

On this page and next few pages current paper
topic mention hain

- **Kali Linux**
- **Virtual Box**

my paper 6 aug 2024.

1. ransomware
2. address space randomization
3. zenmap command for fast scan
4. two best practices of FTPS
5. Info sec k 2 demerits
6. information security mai tenance of OS
7. flags name given flgs btnat thy
8. five operation of 802.11i
9. buffer over flow
- 10.

Short Questions:

1. What are the three phishing technique...
2. What us trojan horse?
3. What are is the basic syntax to scan the web address: scanme.nmap.org
4. What are the IEEE network and standards of wired LAN and Wireless LAN.
5. Table given tha CIS or DISA k good, excellent or satisfaction k words sa difference btana tha..

Long Questions:

1. What are the five common types of pishing attacks by the cyvercriminals?
2. Compare and Contrast the computer forensics and network forensics.
3. What is the syntax of " Togarate.... . Txt in the Linux operating system and what also write the correct syntax to scan this in nmap kxh es type ka question tha.....

- **Virtual Box**
- <https://www.virtualbox.org/wiki/Downloads>
- **Kali Linux**
- <https://www.kali.org/>
- <https://www.osboxes.org/kali-linux/#kali-linux-2022-3-vbox>

Or 1 short Question tha What is the purpose or SSH

Or long mai 1 tha what is working or WEP

Or MCQ's nmap sa related thyn 1 2 or 2 sa 3
CIS benchmark mai sa thyn cybercriminals ki
types sa related 3 4 mcq's thyn or kch forensic
science mai sa thyn and some are from HTTP
means last waly week mai sa b thyn



The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

[DOWNLOAD](#) [DOCUMENTATION](#) 



VirtualBox

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 6.1 packages, see [VirtualBox 6.1 builds](#). Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.6 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [Developer preview for macOS / Arm64 \(M1/M2\) hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

The binaries are released under the terms of the GPL version 2.

See the [changelog](#) for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!

- [SHA256 checksums](#), [MD5 checksums](#)

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.

VirtualBox 7.0.6 Oracle VM VirtualBox Extension Pack

- [All supported platforms](#)

Support VirtualBox RDP, disk encryption, NVMe and PXE boot for Intel cards. See this [chapter from the User Manual](#) for an introduction to this Extension Pack. The Extension Pack binaries are released under the [VirtualBox Personal Use and Evaluation License \(PUEL\)](#). Please install the same version extension pack as your installed version of VirtualBox.

VirtualBox 7.0.6 Software Developer Kit (SDK)

- [All platforms](#)

User Manual

Nmap se thy kuch mcqs or 1 question b tha 5 marks ka flags btany thy or cis and disa ka comparison tha short me

Virus ki types k name thy short me

Shell-code or buffer overflow se related question tha

FTPS wala tha long me

Type of virus

What is DiSa Stigs

Bki week 8 9 10 13 14 imp hyn mostly paper yhan sy Ara hy

Comparison aya tha cis vs disa

Short me

Aik ransomware ki definition thi locard principal of forensic science

Top five error in software

NMap ki definition

Version of CIS CAT

Secure shell k bhry ma pucha hua tha aik

Types of malware

Difference pucha hua tha forensic ur network

forensic

Computer frauds k bhry ma bhi tha koi question

Iso27002:2013 eska bhi aik question tha

Ur ports state bhi thi Nmap ki



[VM IMAGES](#) ▾

[SUPPORT](#) ▾

[BLOG](#)



Oracle VM VirtualBox Manager

File Machine Help



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.



Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).



Snapshots

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.





CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine at the right side of the main tool bar located at the top of the window.

You can

← Create Virtual Machine

Name and operating system

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name:

Type:

Version:

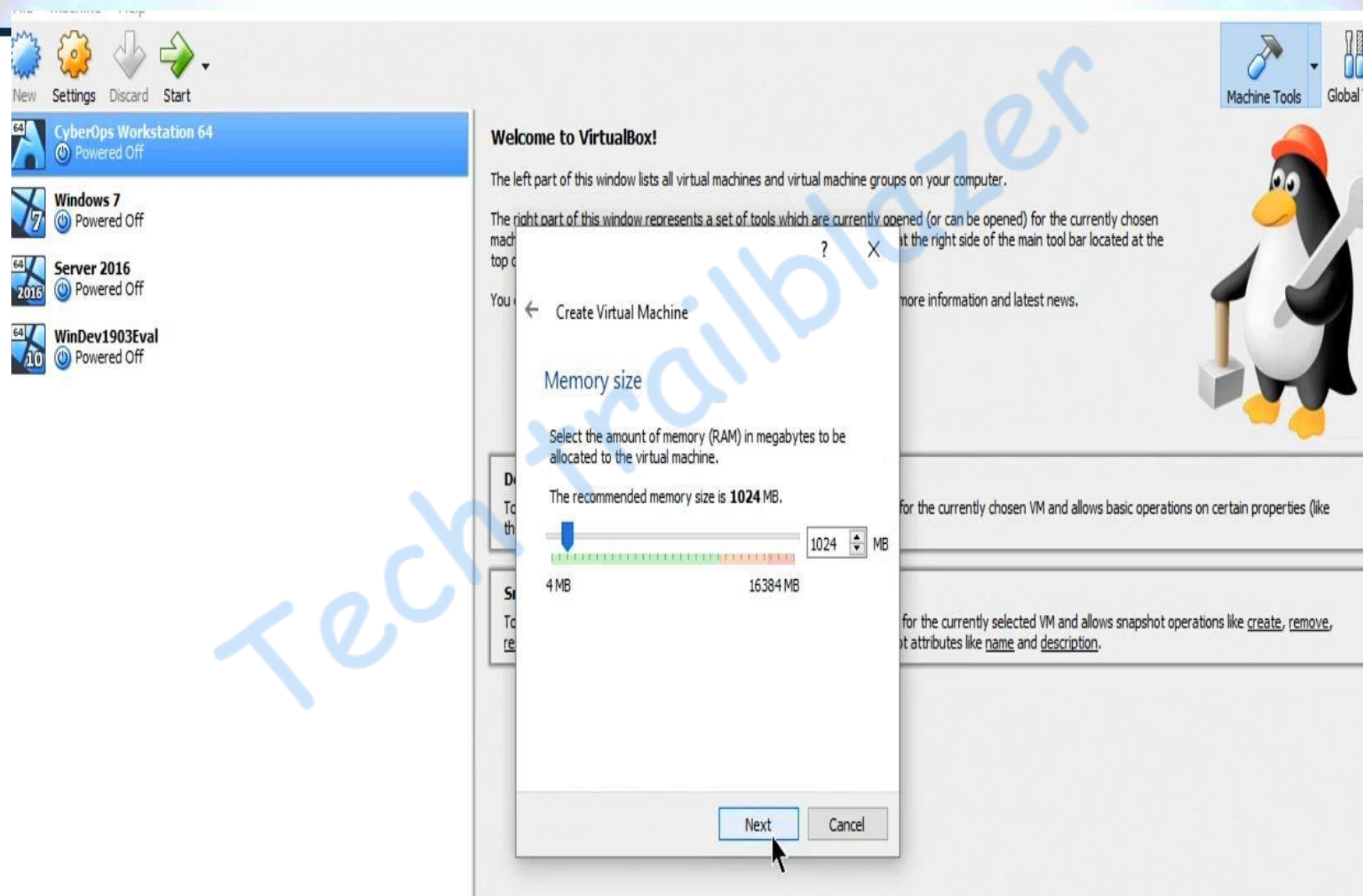
Expert Mode

Next

Cancel

for the currently chosen VM and allows basic operations on certain properties (like

for the currently selected VM and allows snapshot operations like create, remove, at attributes like name and description.





CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off



Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. You can find more information and latest news.

← Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

- ☐ Do not add a virtual hard disk
- ☐ Create a virtual hard disk now
- ☒ Use an existing virtual hard disk file

IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)

Create

Cancel

64 CyberOps Workstation 64
 Powered Off

7 Windows 7
 Powered Off

64 Server 2016
 2016 Powered Off

64 WinDev1903Eval
 10 Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. At the right side of the main tool bar located at the top of the main window, you can find a question mark icon for more information and latest news.



← Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

☐ Do not add a virtual hard disk
☐ Create a virtual hard disk now
☒ Use an existing virtual hard disk file

IE8_-_Win7-disk1.vmdk (Normal, 127.00 GB)

Create Cancel



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine.

Please choose a virtual hard disk file

Navigation: < > << Downloads > Kali > 64bit Search 64bit

Organize New folder

	Name	Date modified	Type
This PC			
3D Objects			
Desktop			
Documents			
Downloads			
Music			
Pictures			
Videos			
Windows (C:)			
RECOVERY (D:)			
MyStorage (F:)			
MyStorage (F:)			

Name	Date modified	Type
Kali Linux 2019.1 (64bit)	5/5/2019 5:37 PM	Virtual

File name: File type: All virtual hard disk files (*.vmd)

Open Cancel



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine.

Please choose a virtual hard disk file

<< Downloads > Kali > 64bit

Search 64bit

Organize

New folder

This PC

3D Objects

Desktop

Documents

Downloads

Music

Pictures

Videos

Windows (C:)

RECOVERY (D:)

MyStorage (F:)

MyStorage (F:)

Name

Date modified

Type

Kali Linux 2019.1 (64bit)

5/5/2019 5:37 PM

Virtual

File name: Kali Linux 2019.1 (64bit)

All virtual hard disk files (*.vmd)

Open

Cancel



certain properties (like

ns like create, remove,



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. You can find the right side of the main tool bar located at the top of the window.

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **8.00 GB**.

- ☐ Do not add a virtual hard disk
- ☐ Create a virtual hard disk now
- ☒ Use an existing virtual hard disk file

Kali Linux 2019.1 (64bit).vdi (Normal, 500.00 GB)

Create

Cancel



for the currently chosen VM and allows basic operations on certain properties (like

for the currently selected VM and allows snapshot operations like create, remove,
not attributes like name and description.

Oracle VM VirtualBox Manager

File Machine Help



CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Kali Linux - Jasper
Powered Off

Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer.

The right part of this window represents a set of tools which are currently opened (or can be opened) for the currently chosen machine. For a list of currently available tools check the corresponding menu at the right side of the main tool bar located at the top of the window. This list will be extended with new tools in future releases.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.



Details

Tool to observe virtual machine (VM) details. Reflects groups of properties for the currently chosen VM and allows basic operations on certain properties (like the machine storage devices).



Snapshots

Tool to control virtual machine (VM) snapshots. Reflects snapshots created for the currently selected VM and allows snapshot operations like create, remove, restore (make current) and observe their properties. Allows to edit snapshot attributes like name and description.





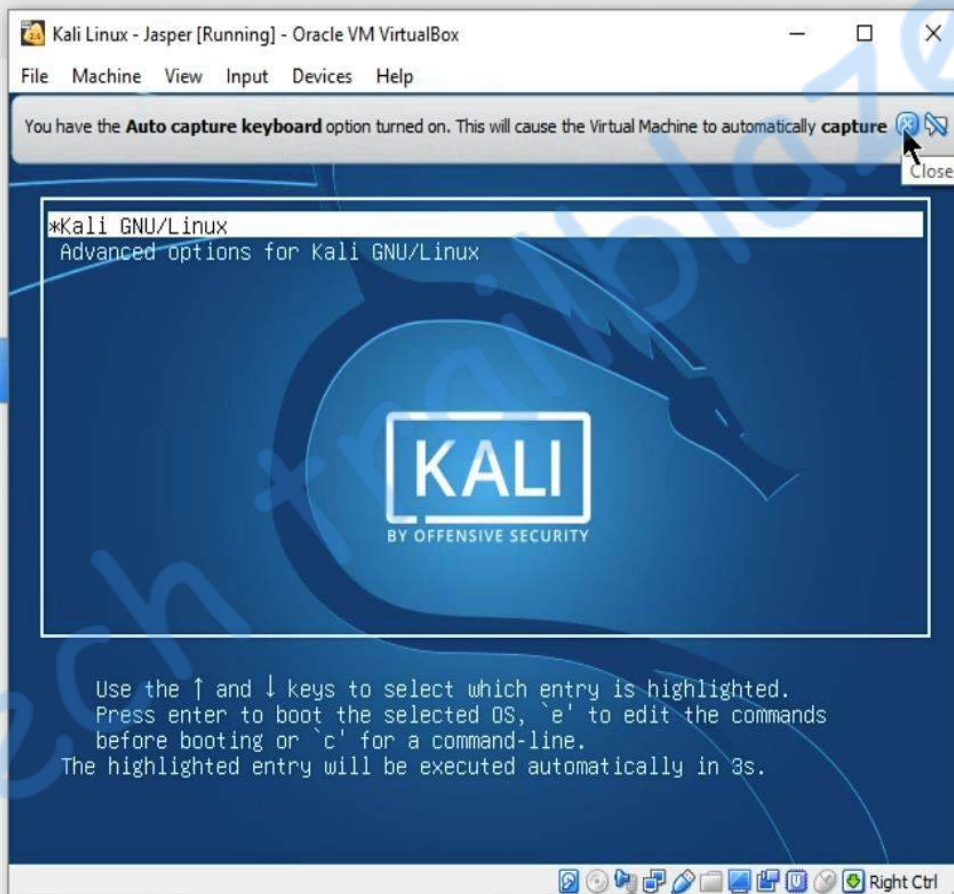
CyberOps Workstation 64
Powered Off

Windows 7
Powered Off

Server 2016
Powered Off

WinDev1903Eval
Powered Off

Kali Linux - Jasper
Running



the currently chosen
bar located at the

WS.

allows basic operations on certain properties (like

and allows snapshot operations like create, remove,
description.

Kali Linux - Jasper [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

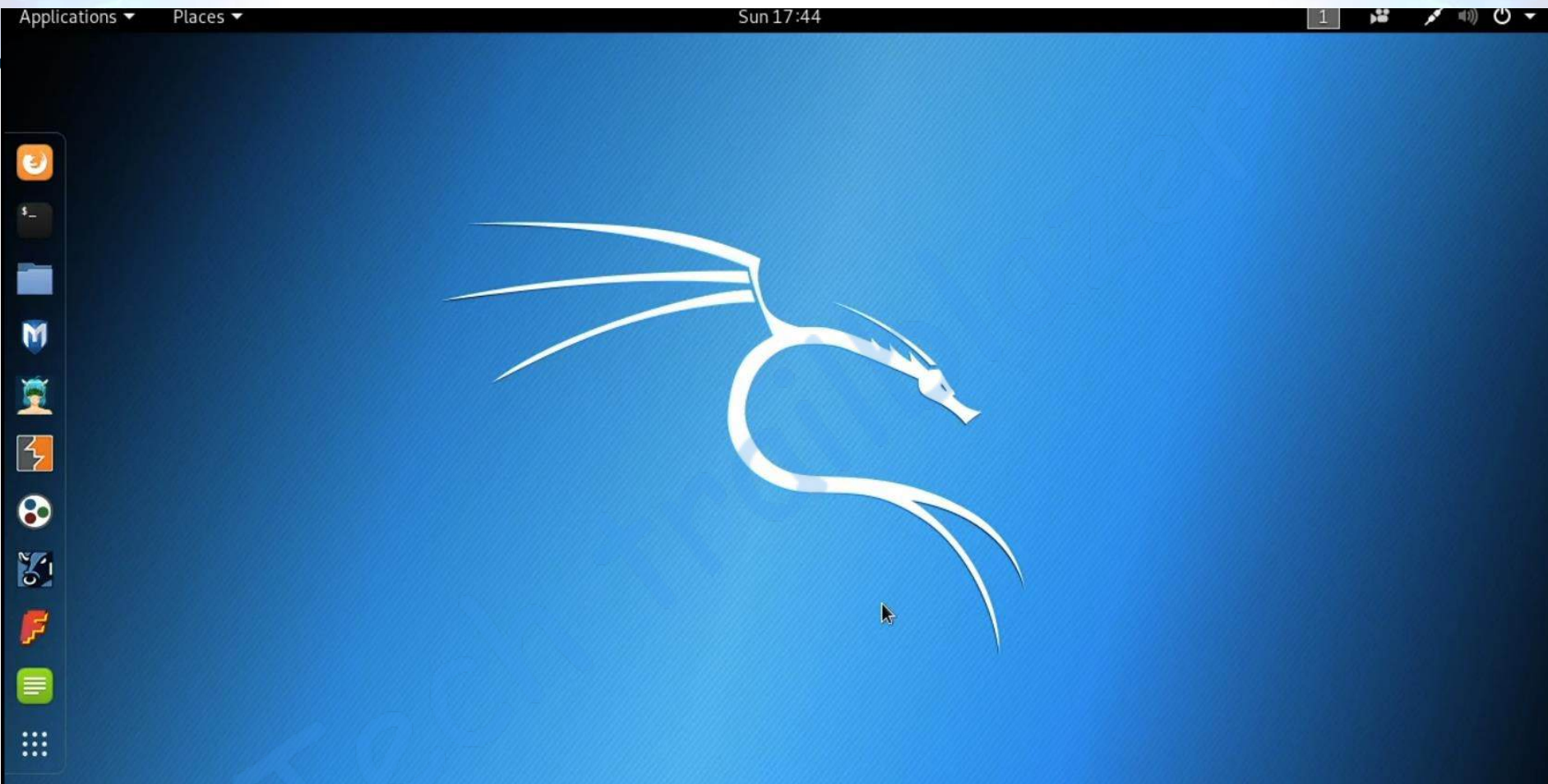
- Full-screen Mode Host+F
- Seamless Mode Host+L
- Scaled Mode Host+C
- Adjust Window Size Host+A
- Auto-resize Guest Display
- Take Screenshot... Host+E
- Video Capture
- Menu Bar
- Status Bar
- Scale Factor
- Virtual Screen 1



Enter your password

Cancel Log In

KALI



Oracle VM VirtualBox Manager

File Machine Help

Tools

kali Linux
Powered Off



General

Name: kali Linux
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Accelerations: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2022.4-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Default
Controller: ICH/AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

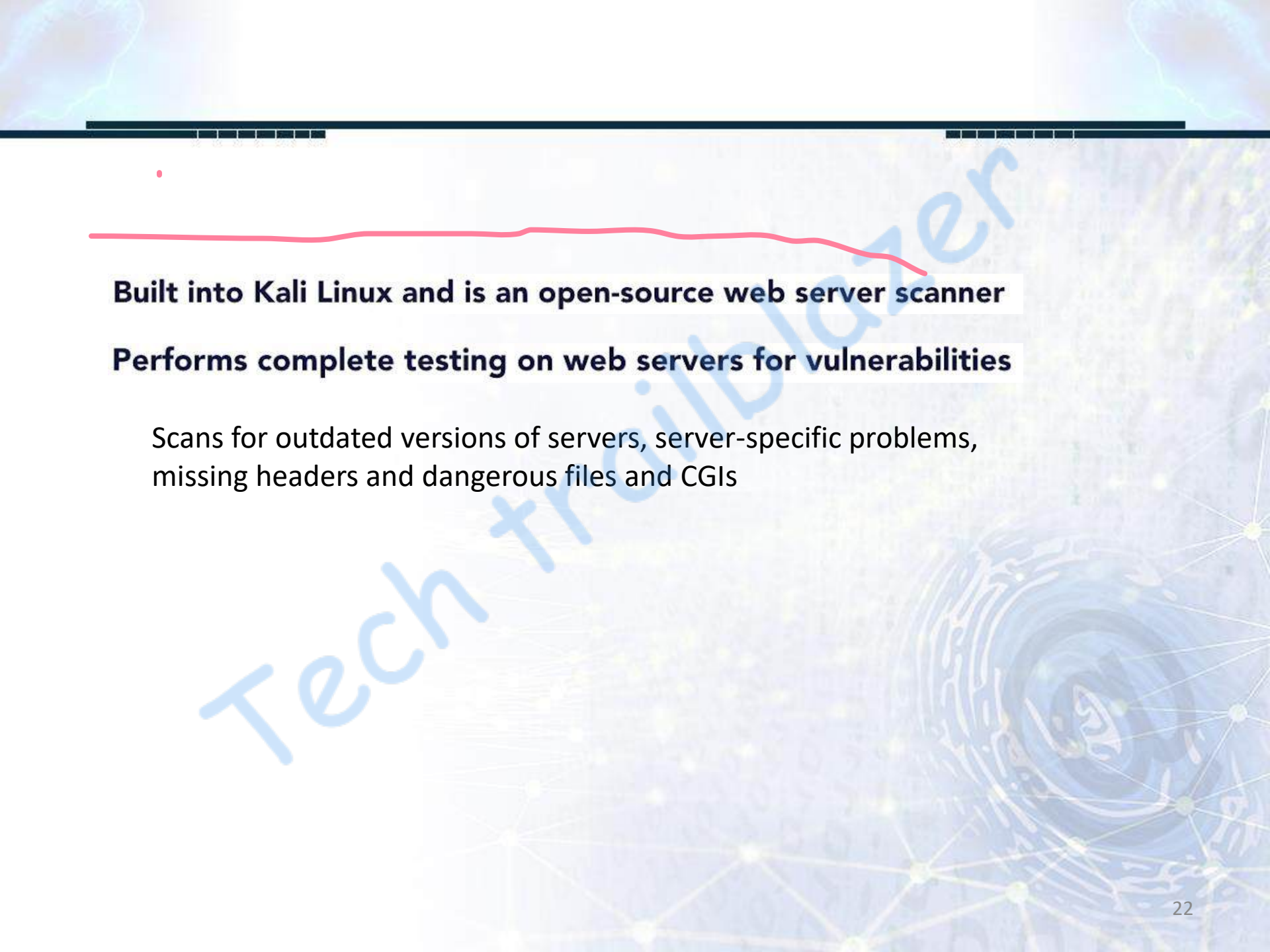
None

Preview



- Nikto

- Web server scanning is a black box test that identifies security vulnerabilities.



Built into Kali Linux and is an open-source web server scanner

Performs complete testing on web servers for vulnerabilities

Scans for outdated versions of servers, server-specific problems, missing headers and dangerous files and CGIs

kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



Search bar:

Favorites

- Recently Used
- All Applications
- Settings
- Usual Applications
- 01 - Information Gathering
- 02 - Vulnerability Analysis
- 03 - Web Application Analysis
- 04 - Database Assessment
- 05 - Password Attacks
- 06 - Wireless Attacks
- 07 - Reverse Engineering
- 08 - Exploitation Tools
- 09 - Sniffing & Spoofing
- 10 - Post Exploitation
- 11 - Forensics
- 12 - Reporting Tools

Applications

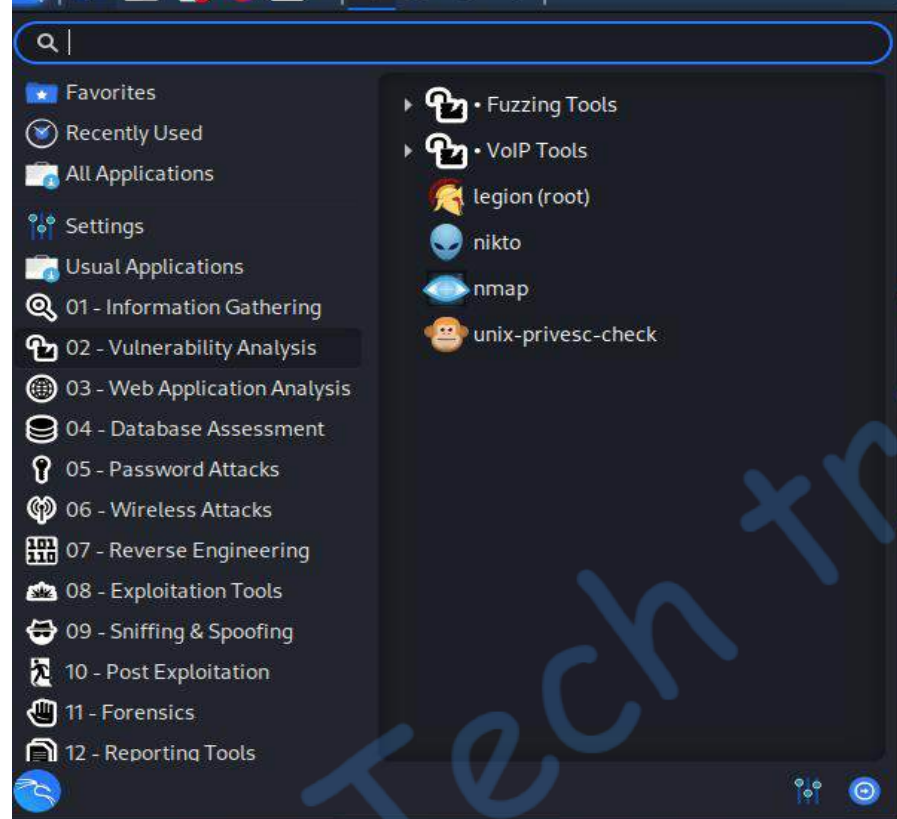
- Terminal Emulator
- Root Terminal Emulator
- File Manager
- Text Editor
- Web Browser
- Kali Linux
- Kali Docs
- Kali Bugs
- Offensive Security Training
- Exploit Database
- VulnHub

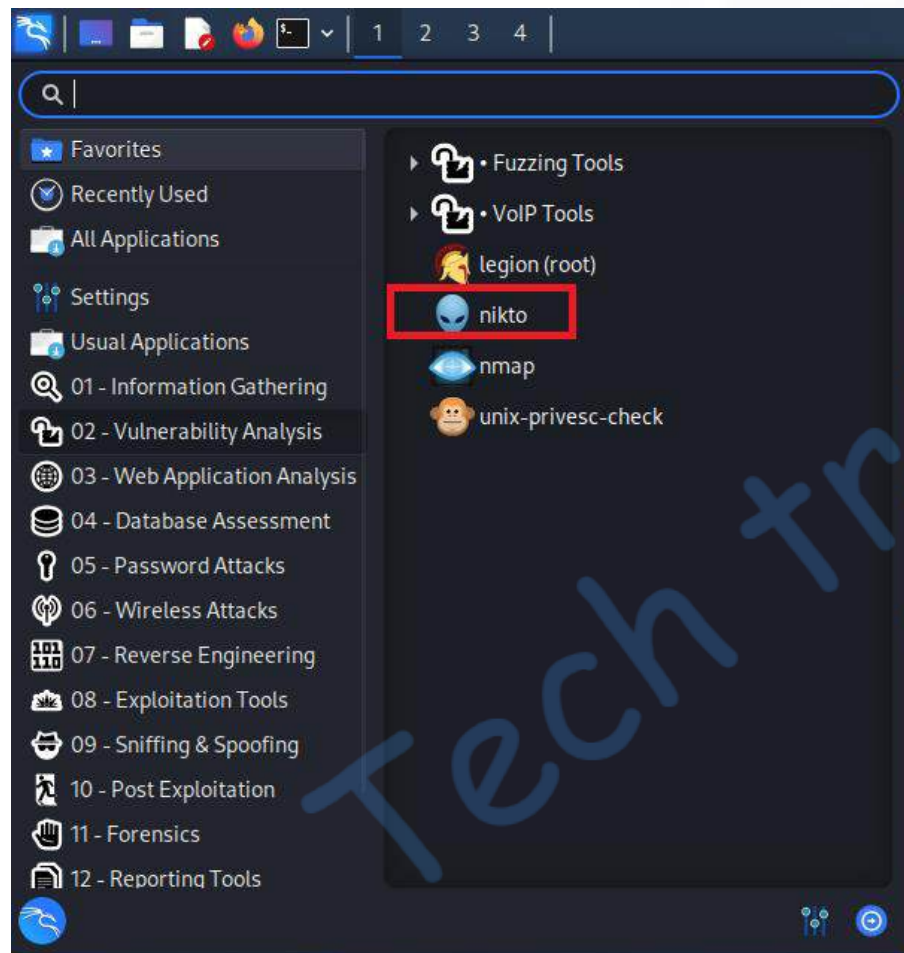
Technical background watermark: Tech + training + lazef

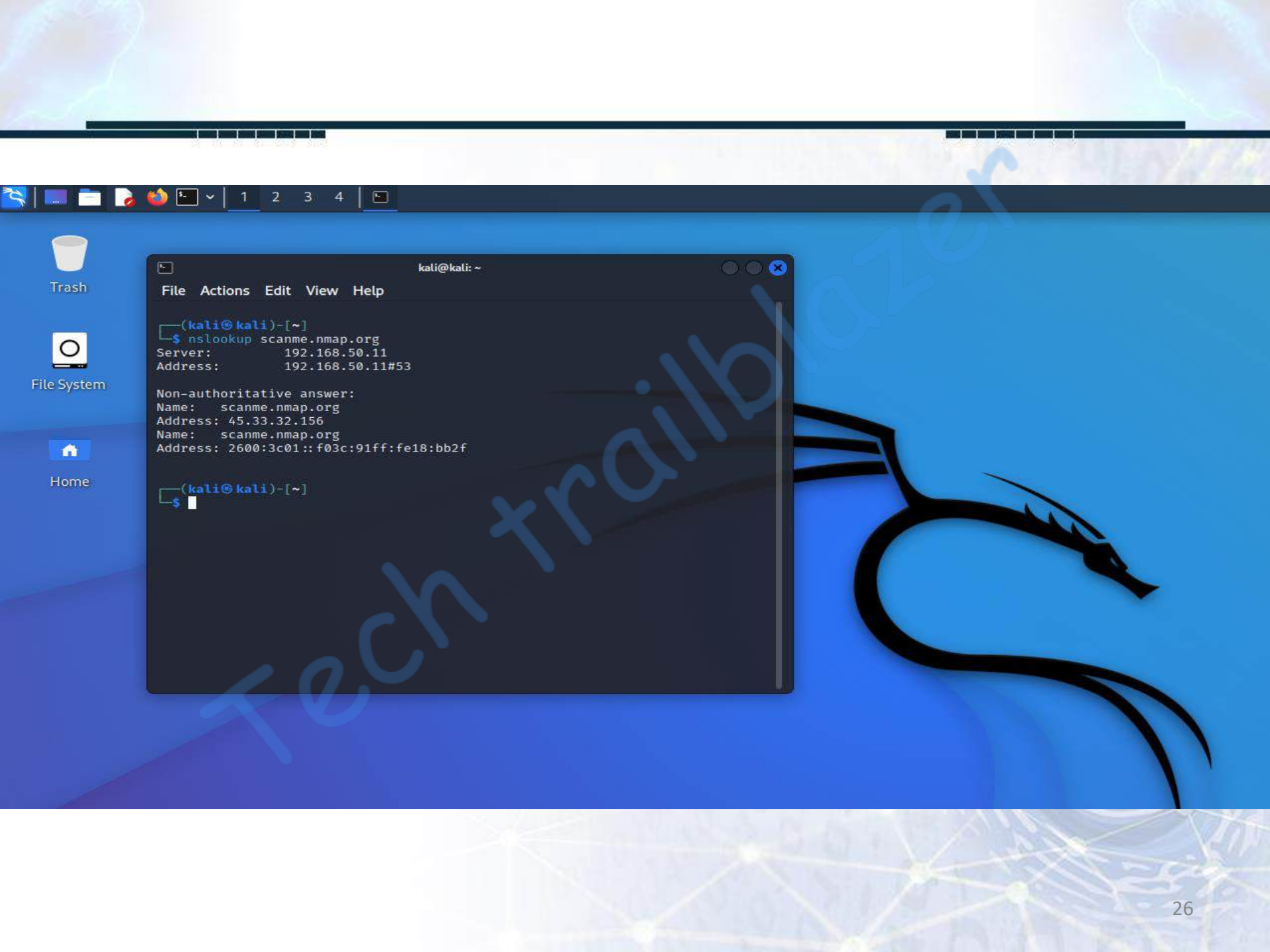


kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help







Trash

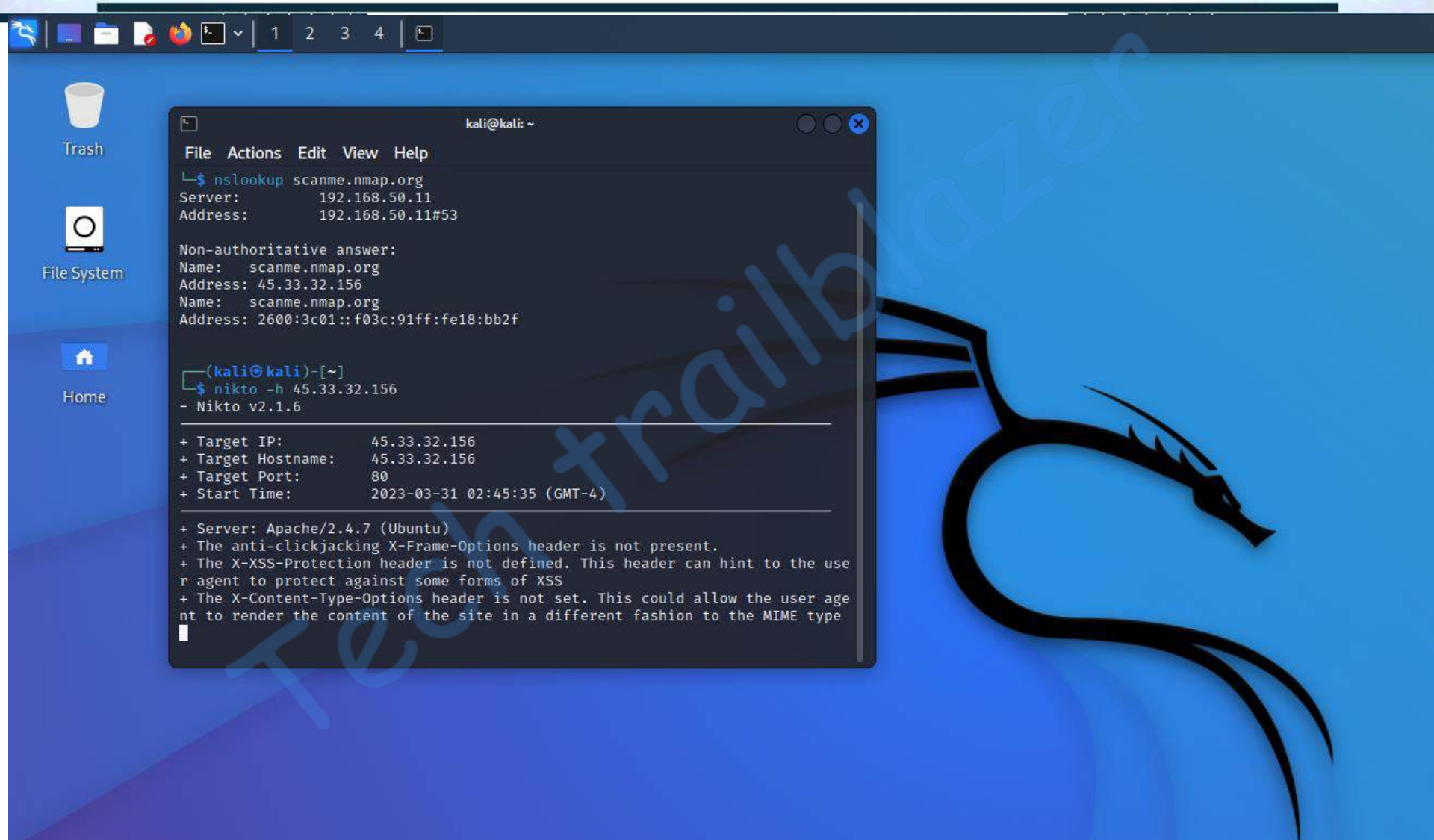


File System



Home

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nslookup scanme.nmap.org  
Server:      192.168.50.11  
Address:     192.168.50.11#53  
  
Non-authoritative answer:  
Name:   scanme.nmap.org  
Address: 45.33.32.156  
Name:   scanme.nmap.org  
Address: 2600:3c01::f03c:91ff:fe18:bb2f  
  
(kali@kali)-[~]  
$
```



Nmap(Network Mapper)

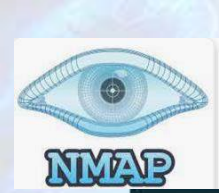


Nmap

Nmap, short for Network Mapper, is a free and open source utility network discovery and security auditing tool.

It is the world's leading port scanner, known for its simple and easy to remember flags that provide powerful scanning options.

- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Discovering connected hosts on a network
- Analyzing free ports on a target host
- Detecting running services on a system along with version number
- Uncovering network vulnerabilities and system loopholes



Nmap

Network administrators often use

- to detect the devices that are presently working on the system
- the port number to which the devices are attached
- the free ports that may be used.
- what services (application name and version) those hosts are offering
- what operating systems (and OS versions) they are running



Nmap

- helpful while performing network penetration testing.
- not only gives network information but also assists in discovering security issues in the system.
- Nmap is platform-agnostic and may be run on various standard operating systems, including Linux, Windows, macOS.
- It is straightforward to use and includes both a command-line interface(CLI) and a graphical user interface(GUI).

Nmap is Used to Scan:

- Enterprise-scale networks
- Small business networks
- Connected devices
- IoT devices and traffic



Nmap Commands

Common Nmap Functions

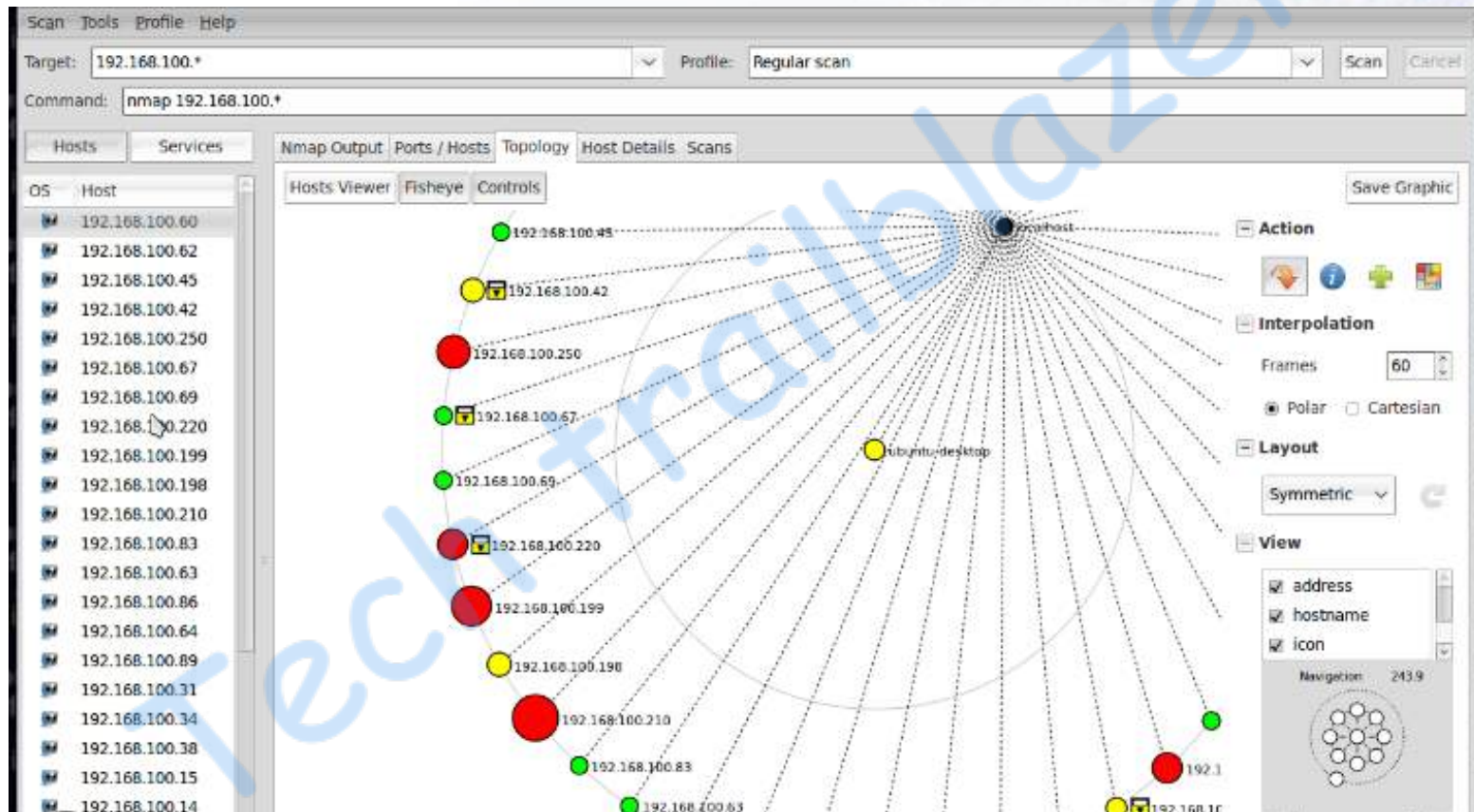


- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution

Zenmap

- Nmap has a graphical user interface called Zenmap. It helps you develop visual mappings of a network for better usability and reporting.

Zenmap GUI





Nmap Commands

- various commands you can use in Nmap along with their flag and usage description with an example on how to use it.

Basic Nmap Scan against IP or host

nmap 1.1.1.1

- Now, if you want to scan a hostname, simply replace the IP for the host, as you see below:

nmap scanme.com



Nmap Commands with flags

Flag	Use	Example
-Pn	only port scan	nmap -Pn 192.168.1.1
-sn	only host discover	nmap -sn 192.168.1.1
-PR	arp discovery on a local network	nmap -PR 192.168.1.1
-n	disable DNS resolution	nmap -n 192.168.1.1

Flag	Use	Example
-p	specify a port or port range	nmap -p 1-30 192.168.1.1
-p-	scan all ports	nmap -p- 192.168.1.1
-F	fast port scan	nmap -F 192.168.1.1

Flag	Use	Example
-sV	detect the version of services running	nmap -sV 192.168.1.1
-A	aggressive scan	nmap -A 192.168.1.1
-O	detect operating system of the target	nmap -O 192.168.1.1

Nmap Benefits and Installation

- Time tested security and networking tool
- Open source package with large community
- Available for most operating systems
- Free!

■ Download Link

<https://nmap.org/download>



Site Search



Download

Reference Guide

Book

Docs

Zenmap GUI

In the Movies

Downloading Nmap

Get the latest Nmap for your system:

- [Windows](#)
- [macOS](#)
- [Linux \(RPM\)](#)
- [Any other OS \(source code\)](#)

Older versions (and sometimes newer test releases) are available from the [Nmap release archive](#) (and really old ones are in [dist-old](#)). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the [sigs directory](#) ([verification instructions](#)). Before downloading, be sure to read the relevant sections for your platform from the [Nmap Install Guide](#). The most important changes (features, bugfixes, etc) in each Nmap version are described in the [Changelog](#). Using Nmap is covered in the [Reference Guide](#), and don't forget to read the other [available documentation](#), particularly the official book [Nmap Network Scanning](#)!

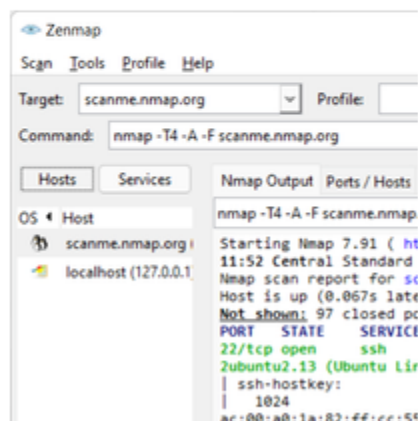
Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

Subscribe to Nmap-hackers

(or subscribe with custom options from the [Nmap-hackers list info page](#))

to get updates by liking [Nmap on Facebook](#) or following us [@nmap on Twitter](#).

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

Latest stable release self-installer: [nmap-7.93-setup.exe](#)

Latest Npcap release self-installer: [npcap-1.73.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the [RPM](#) package management system for quick and easy binary package installation. We have written a detailed [guide to installing our RPM packages](#), though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.93-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.93-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.93-1.x86_64.rpm
```

You can also download and install the RPMs yourself:

Latest stable release:

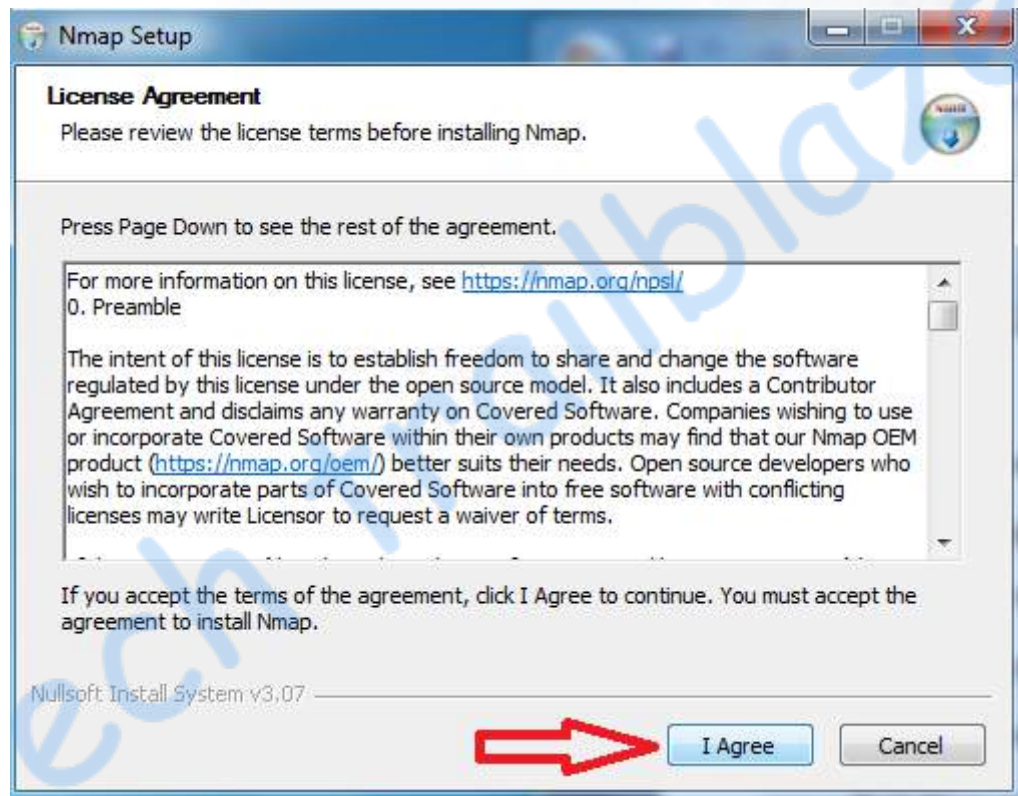
x86-64 (64-bit Linux) [Nmap RPM](#): [nmap-7.93-1.x86_64.rpm](#)

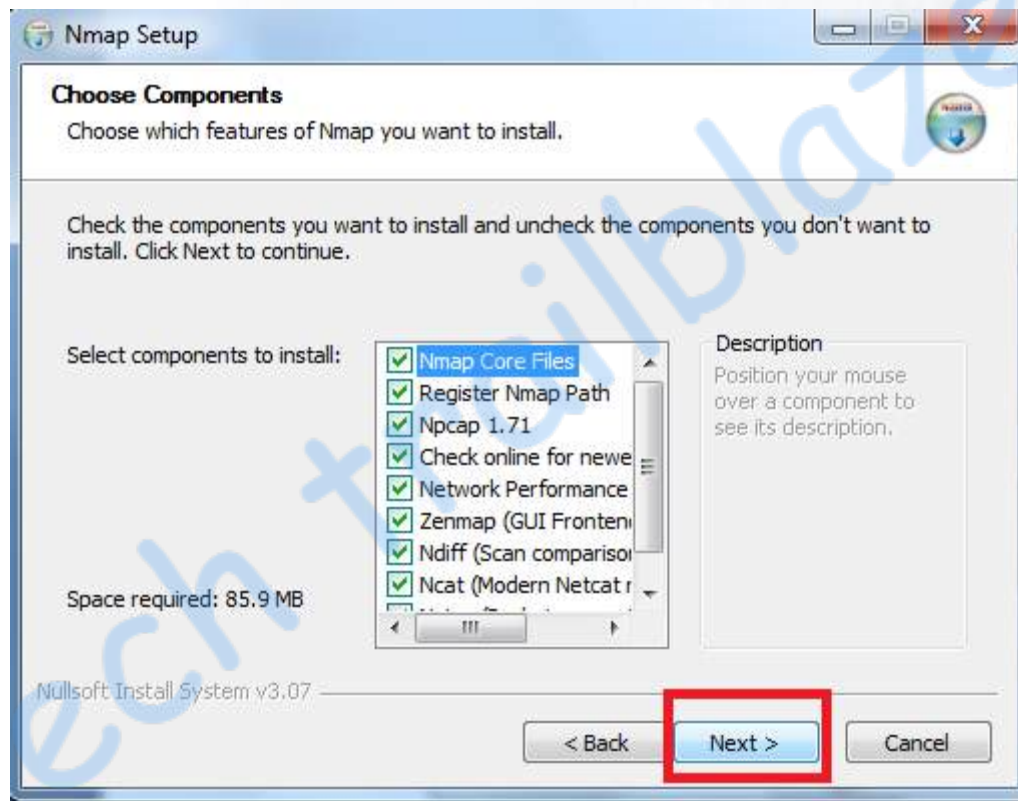
x86-64 (64-bit Linux) [Ncat RPM](#): [ncat-7.93-1.x86_64.rpm](#)

x86-64 (64-bit Linux) [Nping RPM](#): [nping-0.7.93-1.x86_64.rpm](#)

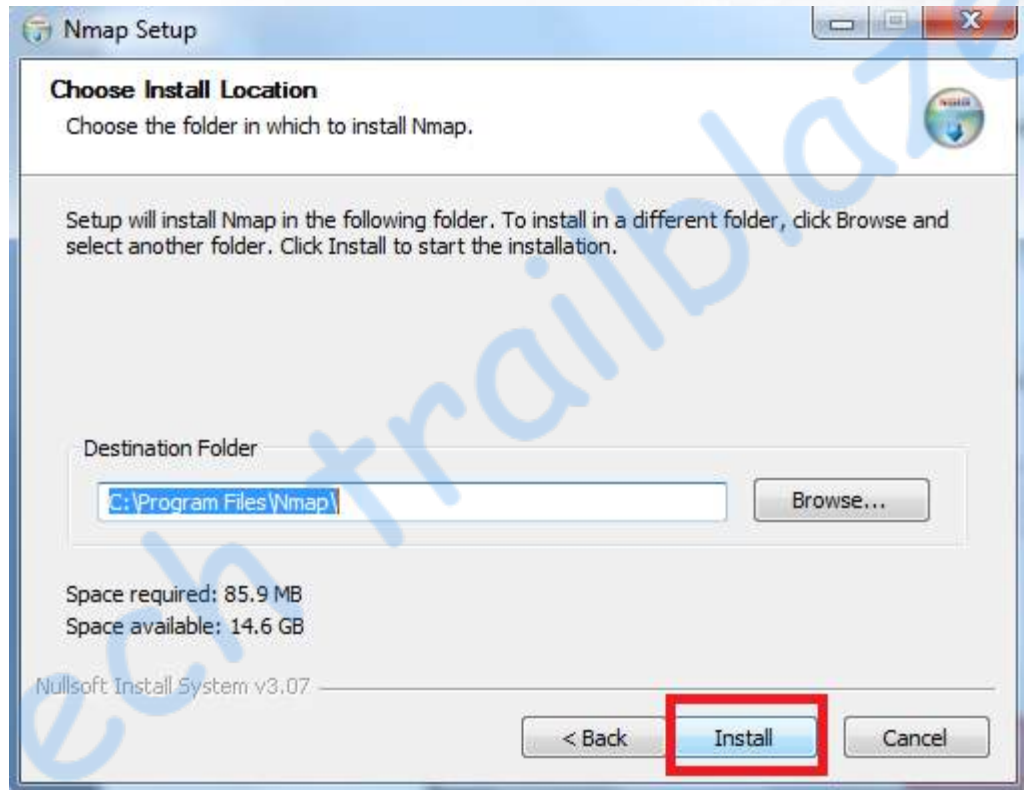
Optional [Zenmap GUI](#) (all platforms): [zenmap-7.93-1.noarch.rpm](#)

Source RPM (includes Nmap, Zenmap, Ncat, and Nping): [nmap-7.93-1.src.rpm](#)





- Nmap core files includes the Nmap scanning engine
- Register Nmap path allows you to execute Nmap from the command line in any directory
- Network performance improvements optimization your system for running scans.
- Zenmap is a graphical front end for Nmap
- Ndiff allows you to compare the results of two Nmap scans.
- Ncat allows you to read and write data to network connections from the command line
- Nping is a packet generation utility that provides enhancements over the basic ping command.





```

D:\>nmap [REDACTED]
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2[,host3[,...]]>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2[,...]]>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)

```

Nmap syntax is the same regardless of the operating system.

```
D:\>nmap -v [REDACTED]  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 22:44 Pakistan Standard Time  
Read data files from: C:\Program Files\Nmap  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds  
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)  
D:\>_
```



```
D:\>nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-31 22:49 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 33.13 seconds
D:\>_
```

Use the Snap container manager to install Nmap on Ubuntu and Debian systems.

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$
```

```
ubuntu@ip-172-31-93-59:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ip-172-31-93-59:~$ nmap -V
Nmap version 7.91 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1 libssh2-1.8.0 libz-1.2.11 libpcre-8.39 libpcap-1.8.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
ubuntu@ip-172-31-93-59:~$
```

Port Stats & Running Simple Namp command

Port Stats in Nmap

State	Description
open	Accepting connection requests
closed	No service responding to requests
filtered	Blocked by a firewall
unfiltered	Accessible, but scanner was unable to determine whether open or closed

VIP

Special cases of port states

- Nmap might be unable to make a definitive statement about the state of the port
- If the Nmap is unsure of the state, it may reports two options.

- Open | filtered means that the port is either open or filtered
- Closed | filtered means that the port is either closed or filtered

Scan with DNS

```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
[ec2-user@ip-172-31-83-84 ~]$
```



```
[ec2-user@ip-172-31-83-84 ~]$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:30 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.072s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.18 seconds
```

- (Microsoft Windows uses **nslookup**, while Mac OS X and Linux use **dig**.)
- Both perform **DNS queries**, and to test out your DNS configuration.
- determine the **IP address** associated with a **domain name**

```
D:\>nslookup scanme.nmap.org
Server: 192.168.1.1
Address: 192.168.1.11

Non-authoritative answer:
Name: scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
          45.33.32.156

D:\>nslookup 45.33.32.156
Server: 192.168.1.1
Address: 192.168.1.11

Name: scanme.nmap.org
Address: 45.33.32.156
```

```
[ec2-user@ip-172-31-83-84 ~]$ dig scanme.nmap.org

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5 <<>> scanme.nmap.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15745
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;scanme.nmap.org.                IN      A

;; ANSWER SECTION:
scanme.nmap.org.                103     IN      A      45.33.32.156

;; Query time: 0 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Mon Jun 14 20:30:33 UTC 2021
;; MSG SIZE rcvd: 60
```


Scan with server IP

```
[ec2-user@ip-172-31-83-84 ~]$ nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 20:31 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.071s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
[ec2-user@ip-172-31-83-84 ~]$
```

```
D:\>nmap scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 14:53 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.32s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 34.77 seconds

D:\>nmap 45.33.32.156
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 15:05 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.34s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 55.42 seconds
```

OS and service Version Detection

- Nmap is able to probe deeper than simply open reports
- Guesses the target OS

Activate operating system detection with the **-O** flag.

```
Mikes-Mac-mini:~ root# nmap -O scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:23 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.080s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (92%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 2.6.39 (91%), Linux 4.0 (90%), Linux 5.4 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 2.6.18 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds
```

```
Mikes-Mac-mini:~ root# nmap -O 192.168.1.54 [REDACTED]
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:27 EDT
Nmap scan report for 192.168.1.54
Host is up (0.012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
28201/tcp  open  unknown
MAC Address: F0:18:98:5A:B1:A0 (Apple)
Device type: general purpose|media device
Running: Apple OS X 10.11.X, Apple iOS 12.X
OS CPE: cpe:/o:apple:mac_os_x:10.11 cpe:/o:apple:iphone_os:12
OS details: Apple Mac OS X 10.11 (El Capitan) or iOS 12.4 - 13.0 (Darwin 15.6.0 - 19.0.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
```

- **Service version detection**

VIP

- Guesses the service versions running on an open port of target system

Activate service version detection with the **-sV** flag.

```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

```
Mikes-Mac-mini:~ root# nmap -sV scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.089s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo   Nping echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds
```

Port selection

Controls scan behavior

- By default, Nmap scans the 1000 most commonly used TCP ports
- Many of those probably are not used on our network
- Scanning each unused port takes some time
- There are 65535 TCP ports on a system

- If a service is running on any of those ports other than the 1000 most commonly used ports then default Nmap scan will miss it
- There are some options that allow us to customize Nmap scan

The **-F** flag requests a fast scan of the top 100 TCP ports.

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3333/tcp  open  dec-notes
5555/tcp  open  freeciv

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
3333/tcp  open      dec-notes
5555/tcp  open      freeciv
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 96 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds
```



```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0074s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
3333/tcp  open      dec-notes
5555/tcp  open      freeciv
```

Nmap done: 1 IP address (1 host up) scanned in 2.98 seconds

```
recording@Mikes-Mac-mini ~ % nmap -F 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:11 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0090s latency).
Not shown: 96 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
```

Nmap done: 1 IP address (1 host up) scanned in 1.44 seconds

The **-p** flag allows us to specify the ports we'd like to scan.

~~MAC ID~~

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
```

```
PORT      STATE SERVICE
80/tcp    open  http
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

```
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```


Scan Service

```
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8008/tcp	closed	http

```
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

```
recording@Mikes-Mac-mini ~ % nmap -p 80 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:12 EDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```
recording@Mikes-Mac-mini ~ % nmap -p 80,443 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:13 EDT
Nmap scan report for 192.168.1.1
Host is up (0.012s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```
recording@Mikes-Mac-mini ~ % nmap -p http,https 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:14 EDT
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
8008/tcp	closed	http

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

The **-p-** flag requests a full TCP scan of the target system(s).

MANCOK

```
recording@Mikes-Mac-mini ~ % nmap -p- 192.168.1.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 14:15 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0078s latency).
Not shown: 65528 closed ports
PORT      STATE      SERVICE
21/tcp    filtered  ftp
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
3333/tcp  open      dec-notes
5555/tcp  open      freeciv
7272/tcp  open      watchme-7272

Nmap done: 1 IP address (1 host up) scanned in 121.38 seconds
```


Specifying Scan Targets

- Single IP address or DNS name
- List of addresses and names, separated by spaces
- Range of IP addresses
- Subnet mask
- File containing addresses and names
- Scan IPv6

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1 192.168.1.3 192.168.1.6 [REDACTED]
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:38 EDT
```

```
Nmap scan report for 192.168.1.1
```

```
Host is up (0.0081s latency).
```

```
Not shown: 994 closed ports
```

PORT	STATE	SERVICE
21/tcp	filtered	ftp
53/tcp	open	domain
80/tcp	open	http
443/tcp	open	https
3333/tcp	open	dec-notes
5555/tcp	open	freeciv

```
Nmap scan report for 192.168.1.3
```

```
Host is up (0.012s latency).
```

```
Not shown: 996 closed ports
```

PORT	STATE	SERVICE
23/tcp	open	telnet
80/tcp	open	http
111/tcp	open	rpcbind
8080/tcp	open	http-proxy

```
Nmap scan report for 192.168.1.6
```

```
Host is up (0.0090s latency).
```

```
Not shown: 998 closed ports
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

```
Nmap done: 3 IP addresses (3 hosts up) scanned in 7.16 seconds
```

```
recording@Mikes-Mac-mini ~ % █
```

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1,3,6 [REDACTED]  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:39 EDT  
Nmap scan report for 192.168.1.1  
Host is up (0.0087s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
21/tcp    filtered ftp  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
3333/tcp  open  dec-notes  
5555/tcp  open  freeciv
```

```
Nmap scan report for 192.168.1.3  
Host is up (0.0087s latency).  
Not shown: 996 closed ports  
PORT      STATE SERVICE  
23/tcp    open  telnet  
80/tcp    open  http  
111/tcp   open  rpcbind  
8080/tcp  open  http-proxy
```

```
Nmap scan report for 192.168.1.6  
Host is up (0.014s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https
```

```
Nmap done: 3 IP addresses (3 hosts up) scanned in 7.75 seconds
```



```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.1-6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:40 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0083s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3333/tcp  open  dec-notes
5555/tcp  open  freeciv
```

```
Nmap scan report for 192.168.1.3
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
8080/tcp  open  http-proxy
```

```
Nmap scan report for 192.168.1.4
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.4 are closed
```

```
Nmap scan report for 192.168.1.5
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.1.5 are closed
```

```
Nmap scan report for 192.168.1.6
Host is up (0.019s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
Nmap done: 6 IP addresses (5 hosts up) scanned in 16.02 seconds
```


Scan subnet

```
recording@Mikes-Mac-mini ~ % nmap 192.168.1.0/29
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0080s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
21/tcp    filtered ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3333/tcp  open  dec-notes
5555/tcp  open  freeciv

Nmap scan report for 192.168.1.3
Host is up (0.010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
111/tcp   open  rpcbind
8080/tcp  open  http-proxy

Nmap scan report for 192.168.1.4
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.4 are closed

Nmap scan report for 192.168.1.5
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.6
Host is up (0.015s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.1.7
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.1.7 are closed

Nmap done: 8 IP addresses (6 hosts up) scanned in 14.75 seconds
```

Scan from file

```
recording@Mikes-Mac-mini ~ % cat scan_targets.txt
192.168.1.1
192.168.1.3
192.168.1.6
192.168.1.8
192.168.1.38
192.168.1.40
192.168.1.42
recording@Mikes-Mac-mini ~ % nmap -iL scan_targets.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:42 EDT
```

```
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
Nmap scan report for 192.168.1.8
Host is up (0.0098s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
5555/tcp   open  freeciv
8009/tcp   open  ajp13
```

```
Nmap scan report for 192.168.1.38
Host is up (0.011s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
9100/tcp  open  jetdirect
```

```
Nmap scan report for 192.168.1.40
Host is up (0.013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp  open  iphone-sync
```

```
Nmap scan report for 192.168.1.42
Host is up (0.010s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
5000/tcp   open  upnp
7000/tcp   open  afs3-fileserver
7100/tcp   open  font-service
49152/tcp  open  unknown
49153/tcp  open  unknown
62078/tcp  open  iphone-sync
```

```
Nmap done: 7 IP addresses (7 hosts up) scanned in 27.92 seconds
```

Scan from file on windows

```
D:\>type scanme.txt
45.33.32.156
18.213.119.84
D:\>more scanme.txt
45.33.32.156
18.213.119.84
```


Nslookup

```
D:\>nslookup scanme.nmap.org
Server:    UnKnown
Address:   192.168.242.235

Non-authoritative answer:
Name:      scanme.nmap.org
Addresses: 2600:3c01::f03c:91ff:fe18:bb2f
           45.33.32.156
```

```
D:\>nslookup scan1.certmike.com
Server:    UnKnown
Address:   192.168.242.235

Non-authoritative answer:
Name:      scan1.certmike.com
Address:   18.213.119.84
```

```
D:\>nmap -iL scanme.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-02 10:19 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.39s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
9929/tcp  open  nping-echo

Nmap scan report for ec2-18-213-119-84.compute-1.amazonaws.com (18.213.119.84)
Host is up (0.23s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 102.17 seconds
D:\>_
```

Scanning IPv6

Nmap is able to scan IPv6 addresses with the **-6** flag.

Tech trailblazer

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ %
```

```
recording@Mikes-Mac-mini ~ % nmap 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:44 EDT
2600:1f18:2763:3000:6b7a:868d:b048:78af looks like an IPv6 target specification -- you have to use the -6 option.
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
recording@Mikes-Mac-mini ~ % nmap -6 2600:1f18:2763:3000:6b7a:868d:b048:78af
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:45 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.16 seconds
recording@Mikes-Mac-mini ~ %
```


Scan Shortcut and Disable DNS option

scanning shortcut

- The **-A** flag offers a scanning shortcut that activate several popular options

-A Options

- Remote operating system detection
- Service and version detection
- Traceroute
- Nmap Scripting engine (NSE)

```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp   filtered  msrpc
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds
9929/tcp  open      nping-echo   Nping echo
31337/tcp open      tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197
4   30.27 ms 96.110.154.133
5   21.36 ms 68.87.231.137
6   30.29 ms be-167-ar01.area4.il.chicago.comcast.net (162.151.144.101)
7   31.34 ms 24.153.89.45
8   31.33 ms be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)

```



```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open  http             Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo       Nping echo
31337/tcp  open  tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 4.0
%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197

```

```
Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
```

```
Host is up (0.079s latency).
```

```
Not shown: 992 closed ports
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)

```
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
```

Namp Scrpiting engine that retrieves the SSH key as presented by the host

```
25/tcp    filtered smtp
80/tcp    open      http      Apache httpd 2.4.7 ((Ubuntu))
```

```
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
```

```
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open      nping-echo Nping echo
31337/tcp open      tcpwrapped
```

```
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 2.6.35 (91%), Linux 3.0 (90%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
```

```
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 16 hops
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE (using port 5900/tcp)
```

HOP	RTT	ADDRESS
1	8.82 ms	192.168.1.1
2	12.34 ms	10.0.0.1
3	20.07 ms	10.128.0.1

```

Mikes-Mac-mini:~ root# nmap -A -T4 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 15:33 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Go ahead and ScanMe!
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 (93%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)
HOP RTT      ADDRESS
1   8.82 ms  192.168.1.1
2   12.34 ms 10.0.0.1
3   30.27 ms 96.120.26.197

```



```

25/tcp    filtered smtp
80/tcp    open      http          Apache httpd 2.4.7 ((Ubuntu))

```

```

|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!

```

```

135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open      nping-echo    Nping echo
31337/tcp  open      tcpwrapped

```

Aggressive OS guesses: Linux 2.6.32 (93%), Linux 2.6.32 or 3.10 (93%), Linux 4.4 (93%), Linux 2.6.32 - 3.0 (90%), Linux 2.6.32 - 3.0 (90%), Linux 3.11 - 4.1 (89%), Linux 3.2 - 3.8 (89%), Linux 5.0 - 5.4 (89%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 16 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 5900/tcp)

HOP	RTT	ADDRESS
1	8.82 ms	192.168.1.1
2	12.34 ms	10.0.0.1
3	30.27 ms	96.120.26.197
4	30.27 ms	96.110.154.133
5	21.36 ms	68.87.231.137
6	30.29 ms	be-167-ar01.area4.il.chicago.comcast.net (162.151.144.101)
7	31.34 ms	24.153.89.45
8	31.33 ms	be-32241-cs04.350ecermak.il.ibone.comcast.net (96.110.40.61)
9	33.63 ms	be-2211-pe11.350ecermak.il.ibone.comcast.net (96.110.33.198)
10	27.18 ms	ae-3-r08.chcgil09.us.bb.gin.ntt.net (129.250.8.65)
11	31.36 ms	ae-4-r23.chcgil09.us.bb.gin.ntt.net (129.250.2.205)
12	96.78 ms	ae-1-r24.snjsca04.us.bb.gin.ntt.net (129.250.5.17)
13	96.79 ms	ae-40-r02.snjsca04.us.bb.gin.ntt.net (129.250.3.121)
14	96.79 ms	ce-0-18-0-1-r02.snjsca04.us.ce.gin.ntt.net (192.80.17.170)
15	96.79 ms	if-1-4.csw6-fnc1.linode.com (173.230.159.83)
16	96.81 ms	scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 20.98 seconds

Mike's Mac mini: root#

- **DNS Resolution**

DNS resolution

- Adds information, but consumes time
- By default, Nmap perform DNS resolution to identify the names of any systems that are scanned by the IP addresses

The **-n** flag disables reverse DNS resolution.

```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
9929/tcp   open  nping-echo
31337/tcp  open  Elite

Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds
```



```
recording@Mikes-Mac-mini ~ % nmap 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:56 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.077s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds

```
recording@Mikes-Mac-mini ~ % nmap -n 45.33.32.156
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 13:57 EDT
Nmap scan report for 45.33.32.156
Host is up (0.079s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds

Zenmap

<https://nmap.org/book/zenmap-results.html>

- Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner.
- Easy for beginners to use while providing advanced features for experienced Nmap users.

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

OS Host

☒ scanme.nmap.org

☒ www.vu.edu.pk (11)

Nmap Output **Ports / Hosts** **Topology** **Host Details** **Scans**

nmap -sn --traceroute scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 09:50 Pakistan
 Nmap scan report for scanme.nmap.org (45.33.32.156)
 Host is up (0.29s latency).

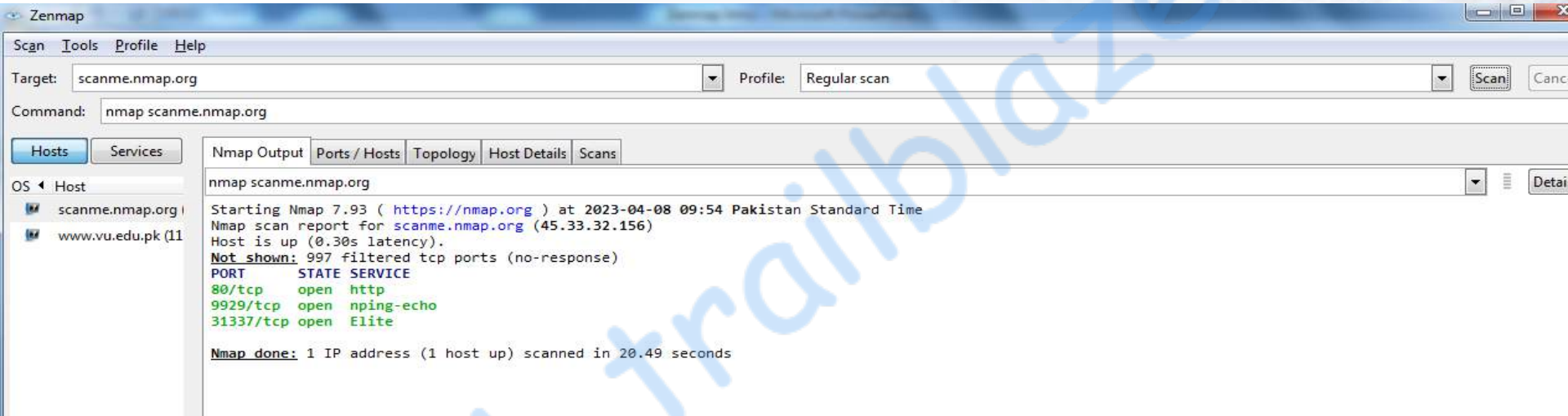
TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
1	2.00 ms	192.168.167.96
2	8.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	16.00 ms	123.108.92.20
5	19.00 ms	119.63.130.252
6	22.00 ms	110.93.252.48
7	25.00 ms	110.93.255.168
8	28.00 ms	110.93.255.230
9	141.00 ms	be5685.ccr22.fra06.atlas.cogentco.com (149.14.211.241)
10	144.00 ms	be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11	150.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	245.00 ms	be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13	244.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	243.00 ms	be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15	253.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	257.00 ms	be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17	266.00 ms	be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)

Profile Menu:

- Quick traceroute
- Intense scan
- Intense scan plus UDP
- Intense scan, all TCP ports
- Intense scan, no ping
- Ping scan
- Quick scan
- Quick scan plus
- Quick traceroute
- Regular scan
- Slow comprehensive scan

zenmap command for fast scsn short question



Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Quick traceroute Scan

Command: nmap -sn --traceroute scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org
www.vu.edu.pk (11)

Nmap Output Ports / Hosts Topology Host Details Scans

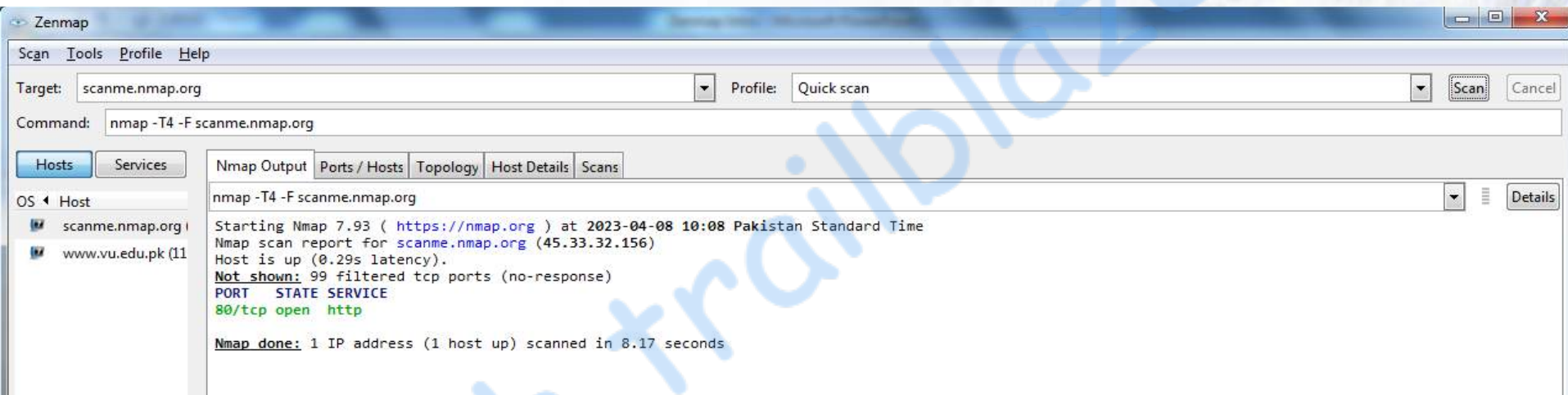
nmap -sn --traceroute scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 09:50 Pakistan Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.29s latency).

TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
1	2.00 ms	192.168.167.96
2	8.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	16.00 ms	123.108.92.20
5	19.00 ms	119.63.130.252
6	22.00 ms	110.93.252.48
7	25.00 ms	110.93.255.168
8	28.00 ms	110.93.255.230
9	141.00 ms	be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10	144.00 ms	be2845.ccr41.fra03.atlas.cogentco.com (154.54.56.189)
11	150.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	245.00 ms	be12194.ccr41.lon13.atlas.cogentco.com (154.54.56.93)
13	244.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	243.00 ms	be2889.ccr21.cle04.atlas.cogentco.com (154.54.47.49)
15	253.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	257.00 ms	be2831.ccr21.mci01.atlas.cogentco.com (154.54.42.165)
17	266.00 ms	be3035.ccr21.den01.atlas.cogentco.com (154.54.5.89)
18	277.00 ms	be3037.ccr21.slc01.atlas.cogentco.com (154.54.41.145)
19	294.00 ms	be3109.ccr21.sfo01.atlas.cogentco.com (154.54.44.137)
20	293.00 ms	be3178.ccr21.sjc01.atlas.cogentco.com (154.54.43.70)
21	295.00 ms	be2063.rcr21.b001848-1.sjc01.atlas.cogentco.com (154.54.1.162)
22	291.00 ms	38.142.11.154
23	307.00 ms	if-1-4.csw5-fnc1.linode.com (173.230.159.81)
24	287.00 ms	scanme.nmap.org (45.33.32.156)

Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds



Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan, no ping

Command: nmap -T4 -A -v -Pn scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

www.vu.edu.pk (11)

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v -Pn scanme.nmap.org

Completed parallel DNS resolution of 22 hosts: at 10:10, 15.00s elapsed

NSE: Script scanning 45.33.32.156.

Initiating NSE at 10:10

Completed NSE at 10:10, 6.04s elapsed

Initiating NSE at 10:10

Completed NSE at 10:10, 1.31s elapsed

Initiating NSE at 10:10

Completed NSE at 10:10, 0.00s elapsed

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.23s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))

|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Go ahead and ScanMe!
|_ http-favicon: Nmap Project
|_ http-server-header: Apache/2.4.7 (Ubuntu)

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 2.6.18 (88%), Linux 4.15 - 5.6 (87%), Linux 2.6.32 or 3.10 (87%), Linux 2.6.35 (87%), Linux 2.6.39 (87%), Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5 (87%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 40.238 days (since Mon Feb 27 04:27:33 2023)

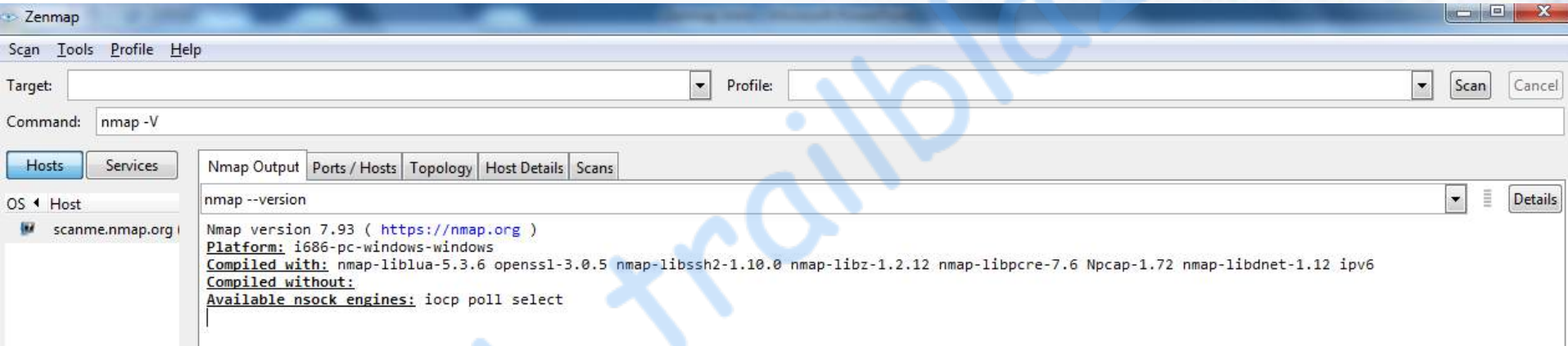
Network Distance: 24 hops

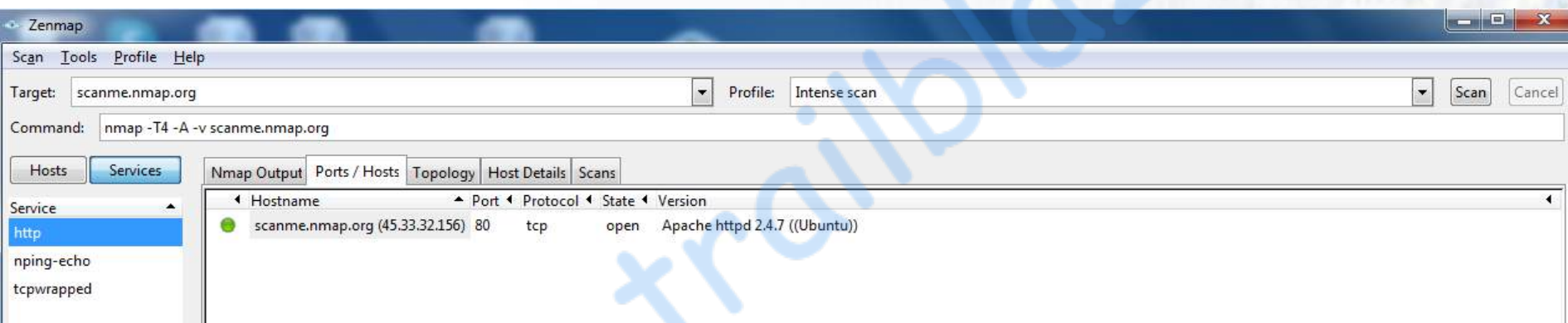
TCP Sequence Prediction: Difficulty=258 (Good luck!)

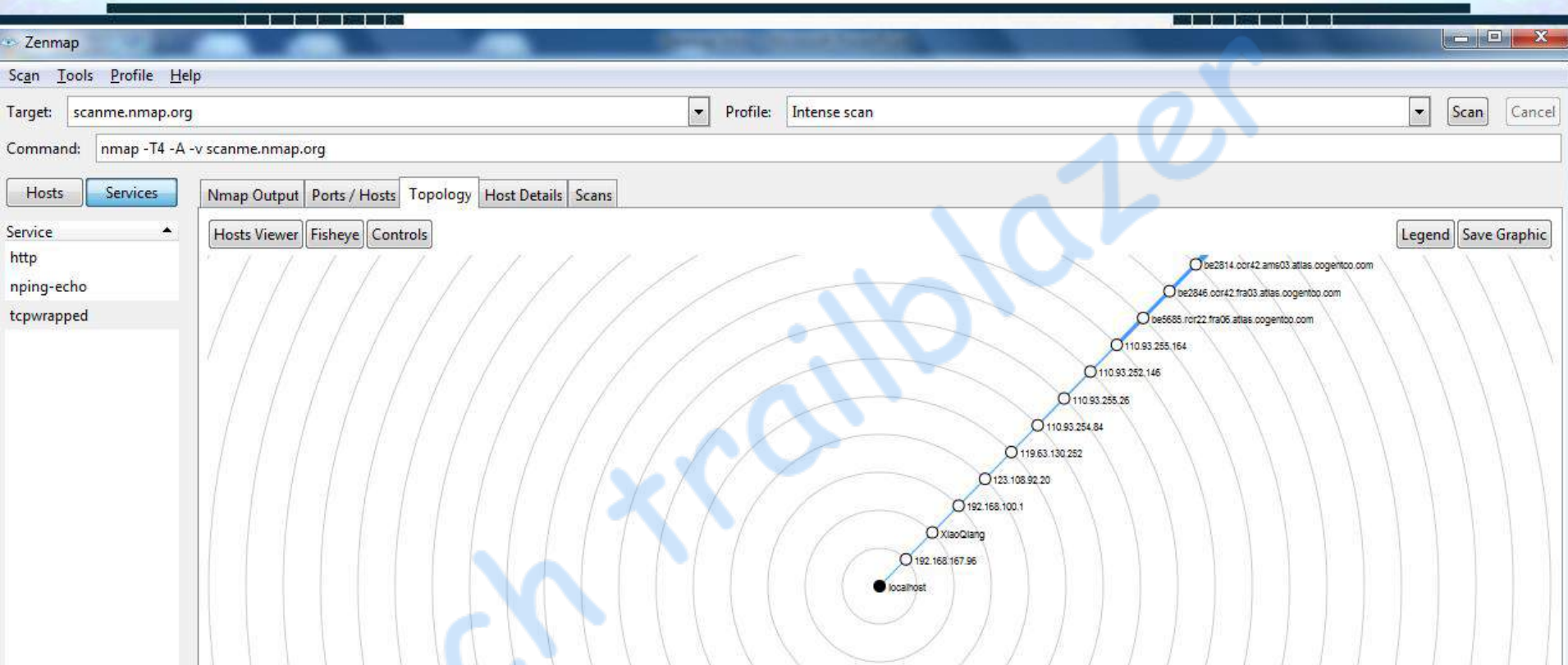
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	3.00 ms	192.168.167.96
2	11.00 ms	XiaoQiang (192.168.31.1)
3	12.00 ms	192.168.100.1
4	12.00 ms	123.108.92.20
5	15.00 ms	119.63.130.252
6	23.00 ms	110.93.252.48







Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v scanme.nmap.org

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

scanme.nmap.org

scanme.nmap.org (45.33.32.156)

- Host Status**
 - State: up
 - Open ports: 3
 - Filtered ports: 997
 - Closed ports: 0
 - Scanned ports: 1000
 - Up time: 3476823
 - Last boot: Mon Feb 27 04:27:33 2023
- Addresses**
 - IPv4: 45.33.32.156
 - IPv6: Not available
 - MAC: Not available
- Hostnames**
 - Name - Type: scanme.nmap.org - user
 - Name - Type: scanme.nmap.org - PTR
- Operating System**
 - Name: Linux 2.6.18
 - Accuracy: 88%
- Ports used**
 - Port-Protocol-State: 80 - tcp - open
 - Port-Protocol-State: 30700 - udp - closed
- OS Classes**
- TCP Sequence**

Filter Hosts

Zenmap

Scan Tools Profile Help

Target: scanme.nmap.org Profile: Intense scan, all TCP ports Scan

Command: nmap -p 1-65535 -T4 -A -v scanme.nmap.org

Hosts Services

OS Host

scanme.nmap.org

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -p 1-65535 -T4 -A -v scanme.nmap.org

Not shown: 65532 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.7 ((Ubuntu))

|_http-title: Go ahead and ScanMe!
 |_http-methods:
 |_Supported Methods: GET HEAD POST OPTIONS
 |_http-favicon: Nmap Project
 |_http-server-header: Apache/2.4.7 (Ubuntu)

9929/tcp open nping-echo Nping echo
 31337/tcp open tcpwrapped

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Linux 2.6.18 (89%), Linux 2.6.32 (88%), Linux 3.10 (88%), Linux 4.15 - 5.6 (88%), Linux 2.6.32 or 3.10 (88%), Linux 2.6.35 (88%), Linux 3.5 (88%), Linux 4.4 (88%), Linux 4.9 (88%), Synology DiskStation Manager 5.1 (88%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 40.252 days (since Mon Feb 27 04:27:34 2023)

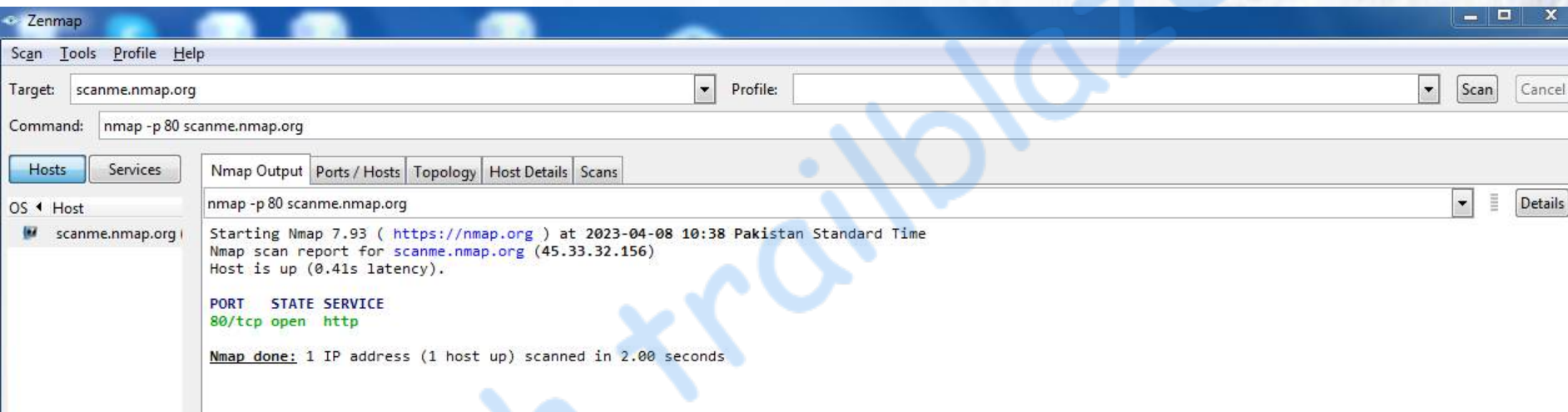
Network Distance: 24 hops

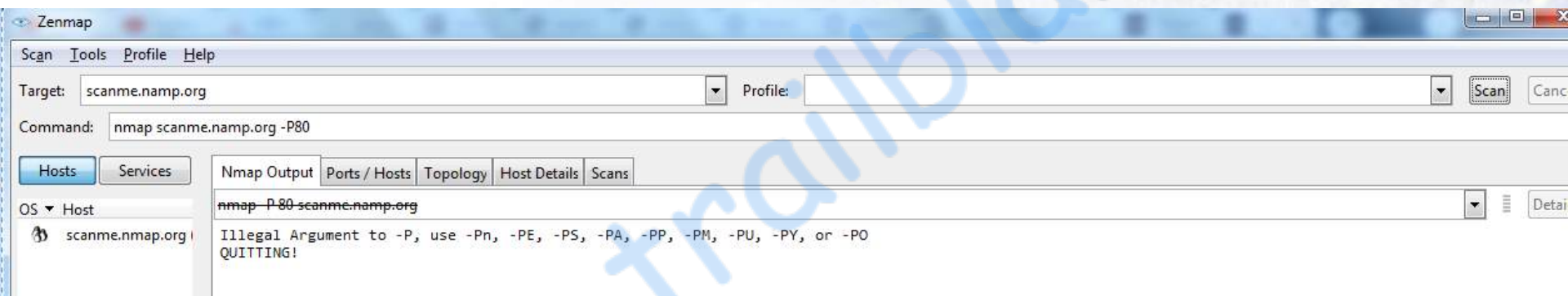
TCP Sequence Prediction: Difficulty=256 (Good luck!)

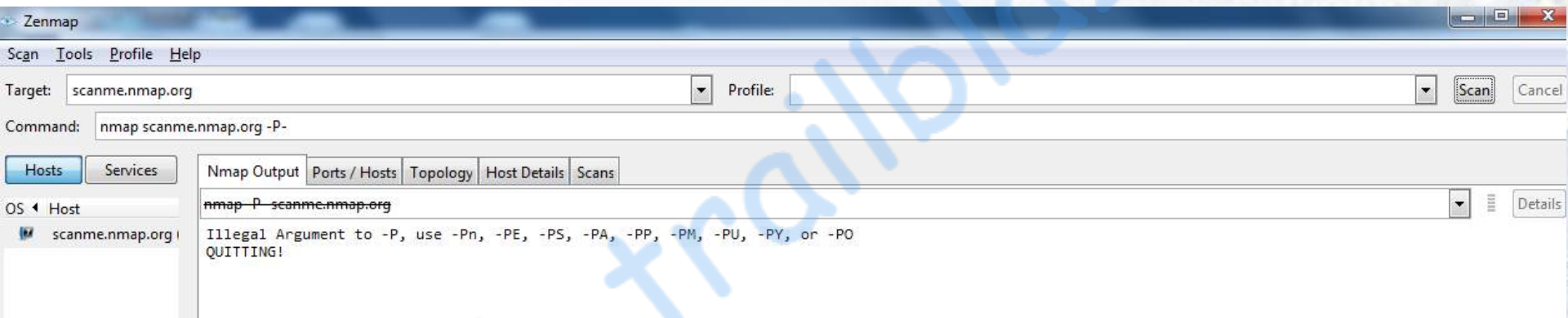
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	12.00 ms	192.168.167.96
2	21.00 ms	XiaoQiang (192.168.31.1)
3	11.00 ms	192.168.100.1
4	12.00 ms	123.108.92.20
5	22.00 ms	119.63.130.252
6	38.00 ms	110.93.252.48
7	32.00 ms	110.93.252.172
8	32.00 ms	110.93.255.164
9	152.00 ms	be5685.rcr22.fra06.atlas.cogentco.com (149.14.211.241)
10	155.00 ms	be2846.ccr42.fra03.atlas.cogentco.com (154.54.37.29)
11	160.00 ms	be2813.ccr41.ams03.atlas.cogentco.com (130.117.0.121)
12	251.00 ms	be12488.ccr42.lon13.atlas.cogentco.com (130.117.51.41)
13	243.00 ms	be2317.ccr41.jfk02.atlas.cogentco.com (154.54.30.185)
14	249.00 ms	be2890.ccr22.cle04.atlas.cogentco.com (154.54.82.245)
15	250.00 ms	be2717.ccr41.ord01.atlas.cogentco.com (154.54.6.221)
16	254.00 ms	be2832.ccr22.mci01.atlas.cogentco.com (154.54.44.169)







Zenmap

Scan Tools Profile Help

Target: 127.0.0.1 Profile: Scan Cancel

Command: nmap -p - 127.0.0.1

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

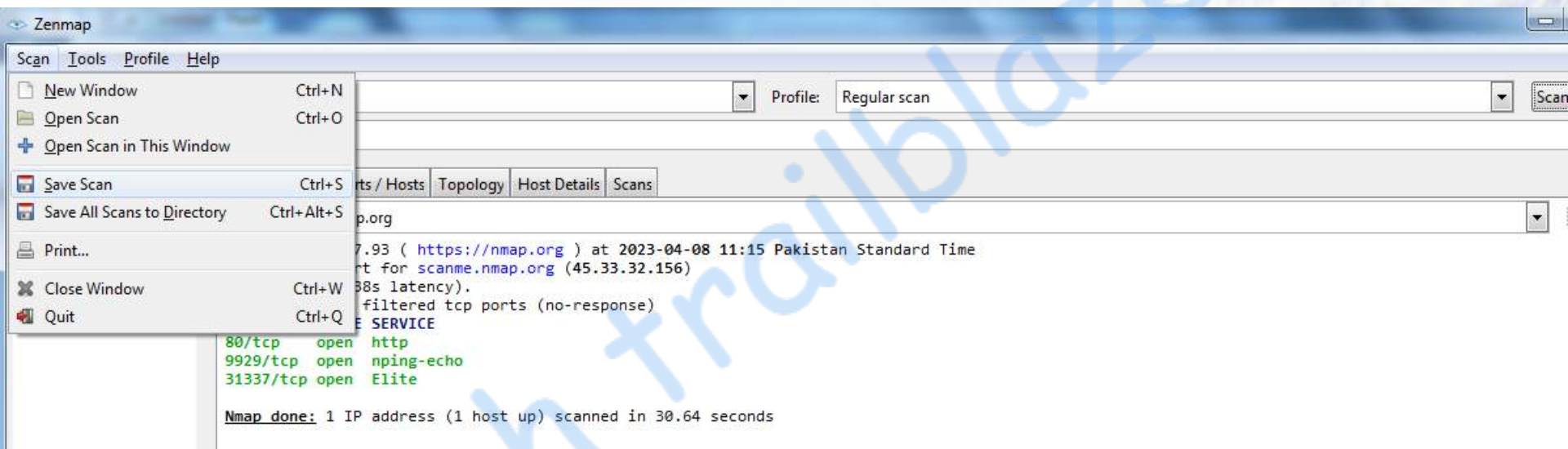
OS Host localhost (127.0.0.1) Details

nmap -p - 127.0.0.1

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 11:10 Pakistan Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0021s latency).
Not shown: 65518 closed tcp ports (reset)

PORT	STATE	SERVICE
135/tcp	open	msrpc
445/tcp	open	microsoft-ds
554/tcp	open	rtsp
895/tcp	open	unknown
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
1027/tcp	open	IIS
1028/tcp	open	unknown
1029/tcp	open	ms-lsa
1030/tcp	open	iad1
1031/tcp	open	iad2
1035/tcp	open	multidrop
1783/tcp	open	unknown
2869/tcp	open	icslap
5939/tcp	open	unknown
10243/tcp	open	unknown
50911/tcp	open	unknown

Nmap done: 1 IP address (1 host up) scanned in 22.52 seconds



nmap scanme.nmap.org

Starting Nmap 7.93 (<https://nmap.org>) at 2023-04-08 11:15 Pakistan Standard Time

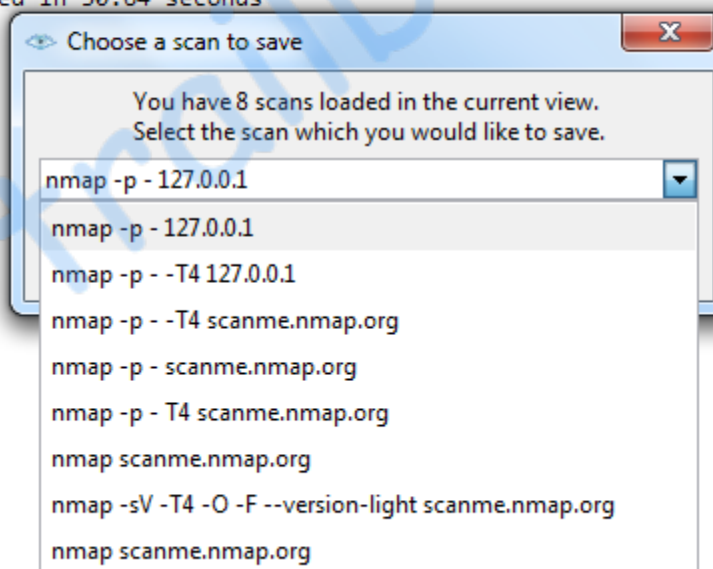
Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.38s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
9929/tcp	open	nping-echo
31337/tcp	open	Elite

Nmap done: 1 IP address (1 host up) scanned in 30.64 seconds



nmap scanme.nmap.org

Starting Nmap 7.93 (<http://nmap.org>) at 2023-04-08 11:45:00 -0400

Nmap scan report for scanme.nmap.org

Host is up (0.38s latency)

Not shown: 997 filtered

PORT STATE SERVICE

80/tcp open http

9929/tcp open nping-echo

31337/tcp open Elite

Nmap done: 1 IP address

Search Scans

Search:

Expressions

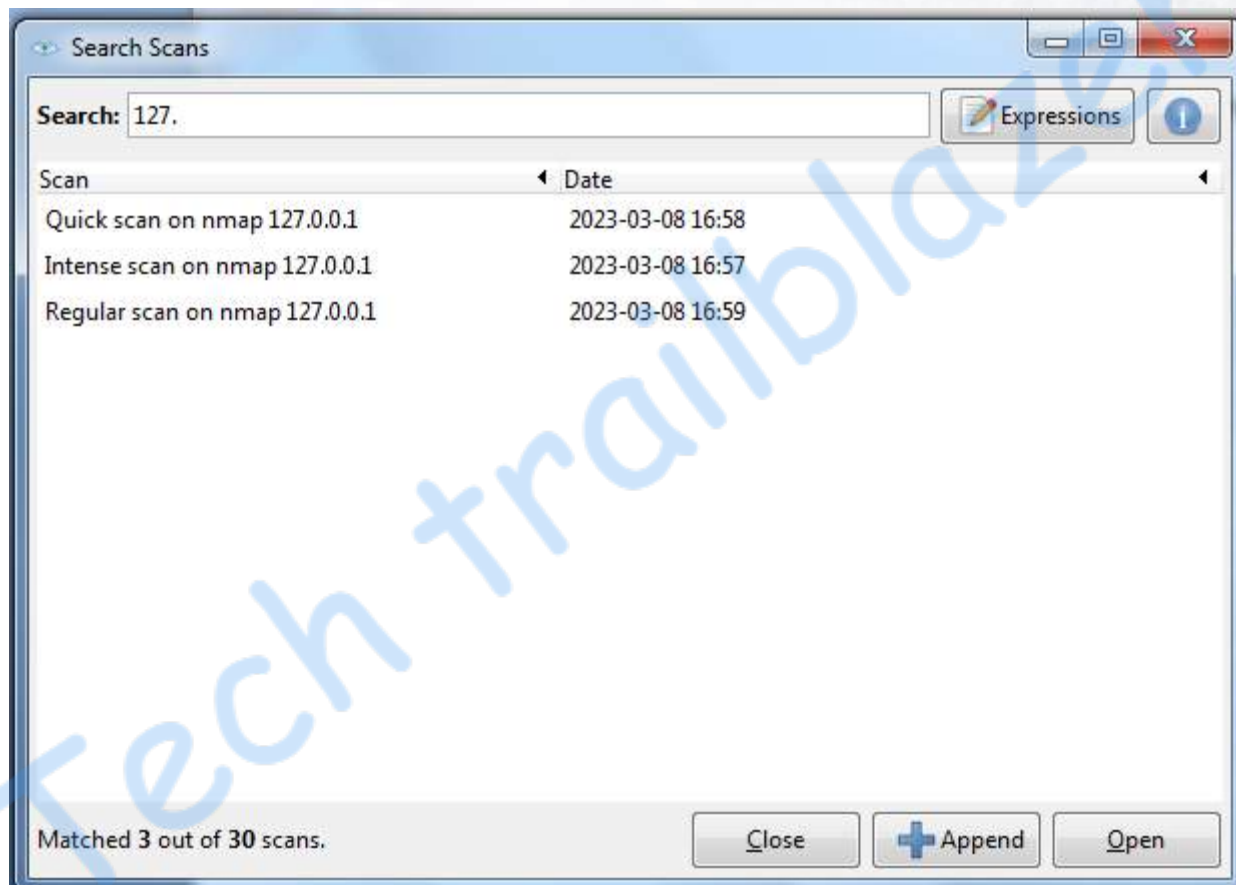
Scan	Date
Quick scan on 192.168.15.62	2023-03-07 15:40
Quick scan on 192.168.15.62	2023-03-07 15:40
Quick scan on www.vu.edu.pk	2023-03-07 16:46
Quick scan on nmap 127.0.0.1	2023-03-08 16:58
Intense scan on nmap 127.0.0.1	2023-03-08 16:57
Regular scan on nmap 127.0.0.1	2023-03-08 16:59
nmap scanme.namp.org	2023-04-08 09:38
Regular scan on scanme.namp.org	2023-04-08 09:39
nmap -T5 www.vu.edu.pk	2023-04-08 09:42
Regular scan on www.vu.edu.pk	2023-04-08 09:49
Ping scan on www.vu.edu.pk	2023-04-08 09:49
nmap -T5 -Pn www.vu.edu.pk	2023-04-08 09:48
Quick traceroute on scanme.nmap.org	2023-04-08 09:50

Matched 30 out of 30 scans.

Close

+ Append

Open



nmap -F nmap 127.0.0.1

Starting Nmap 7.93 (<http://nmap.org>) at 2023-03-08 16:59:00: [Internet Standard Time]

Nmap scan report for localhost

Failed to resolve "nmap":

Host is up (0.00015s latency)

Not shown: 91 closed tcp

PORT	STATE	SERVICE
135/tcp	open	msrpc
445/tcp	open	microsoft
554/tcp	open	rtsp
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	unknown
49157/tcp	open	unknown

Nmap done: 1 IP address

Search Scans

Search: 127

Expressions

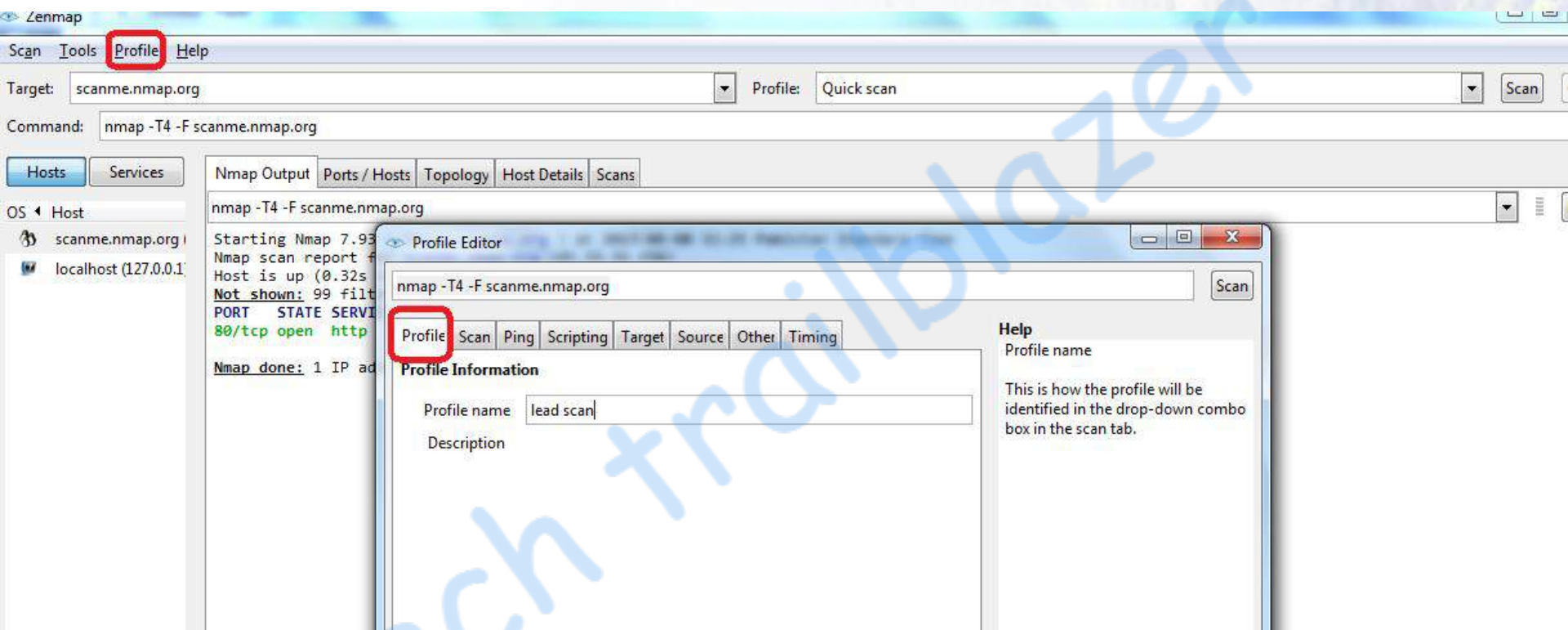
Scan	Date
Quick scan on nmap 127.0.0.1	2023-03-08 16:58
Intense scan on nmap 127.0.0.1	2023-03-08 16:57
Regular scan on nmap 127.0.0.1	2023-03-08 16:59

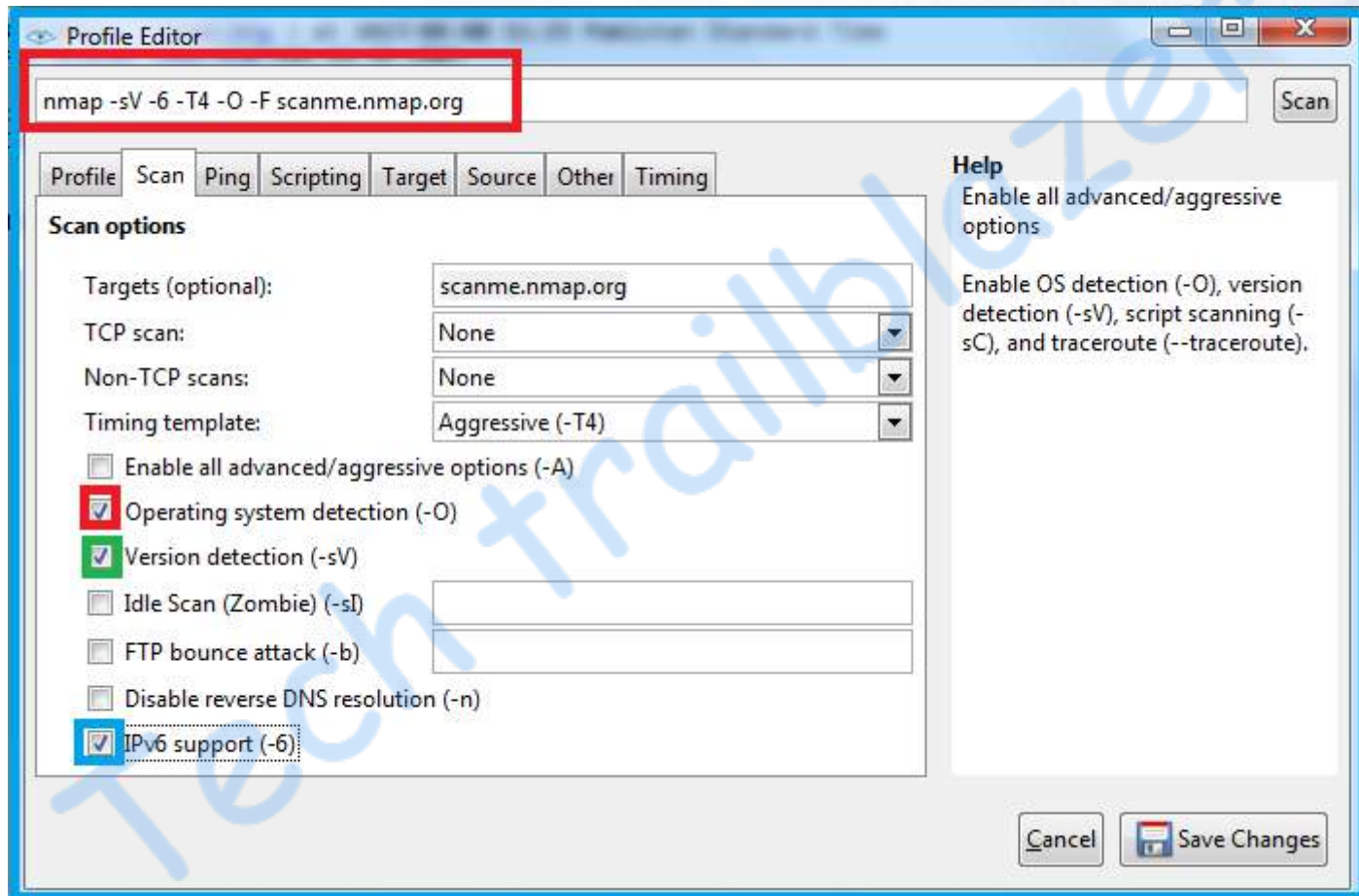
Matched 3 out of 30 scans.

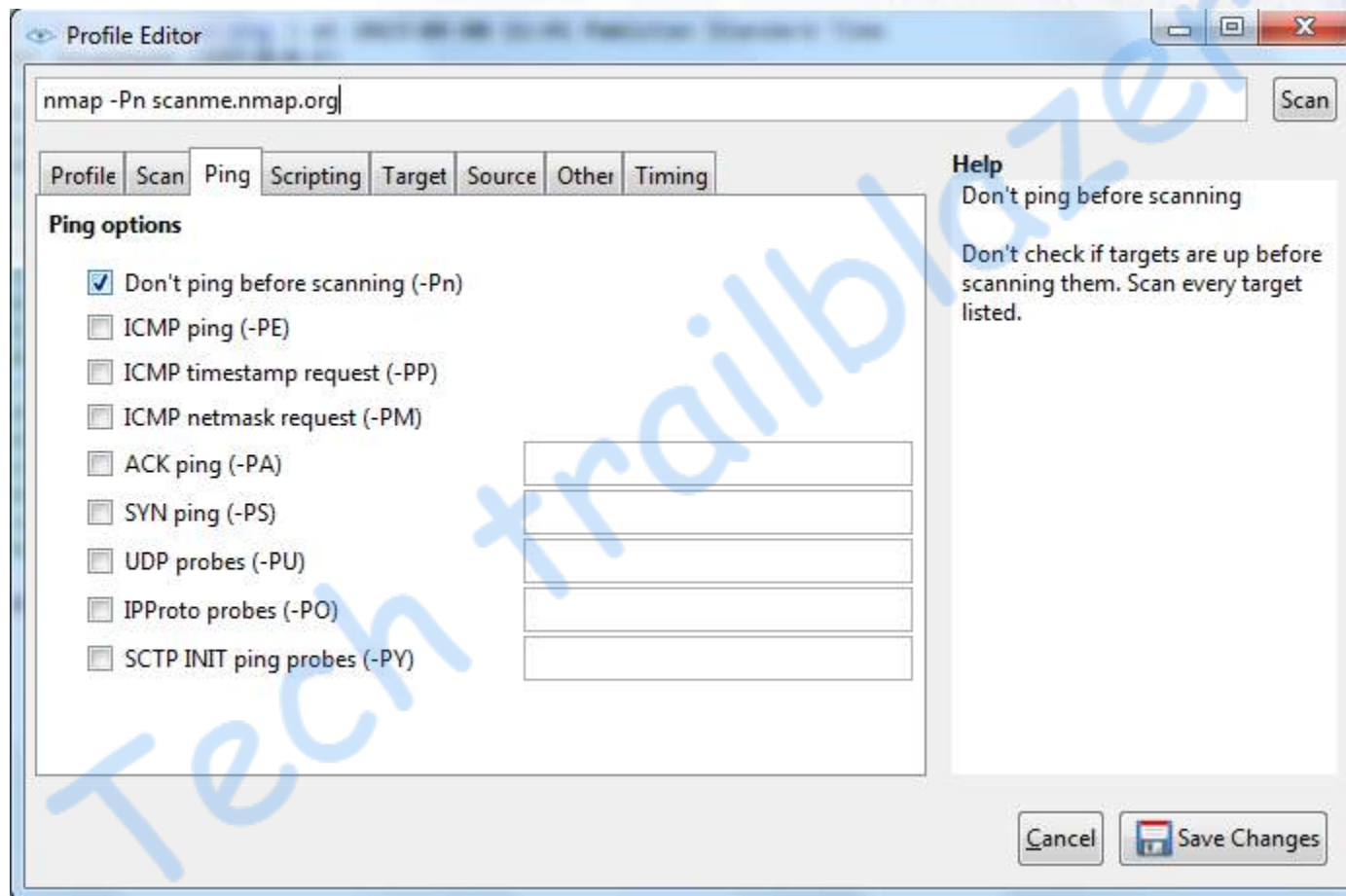
Close

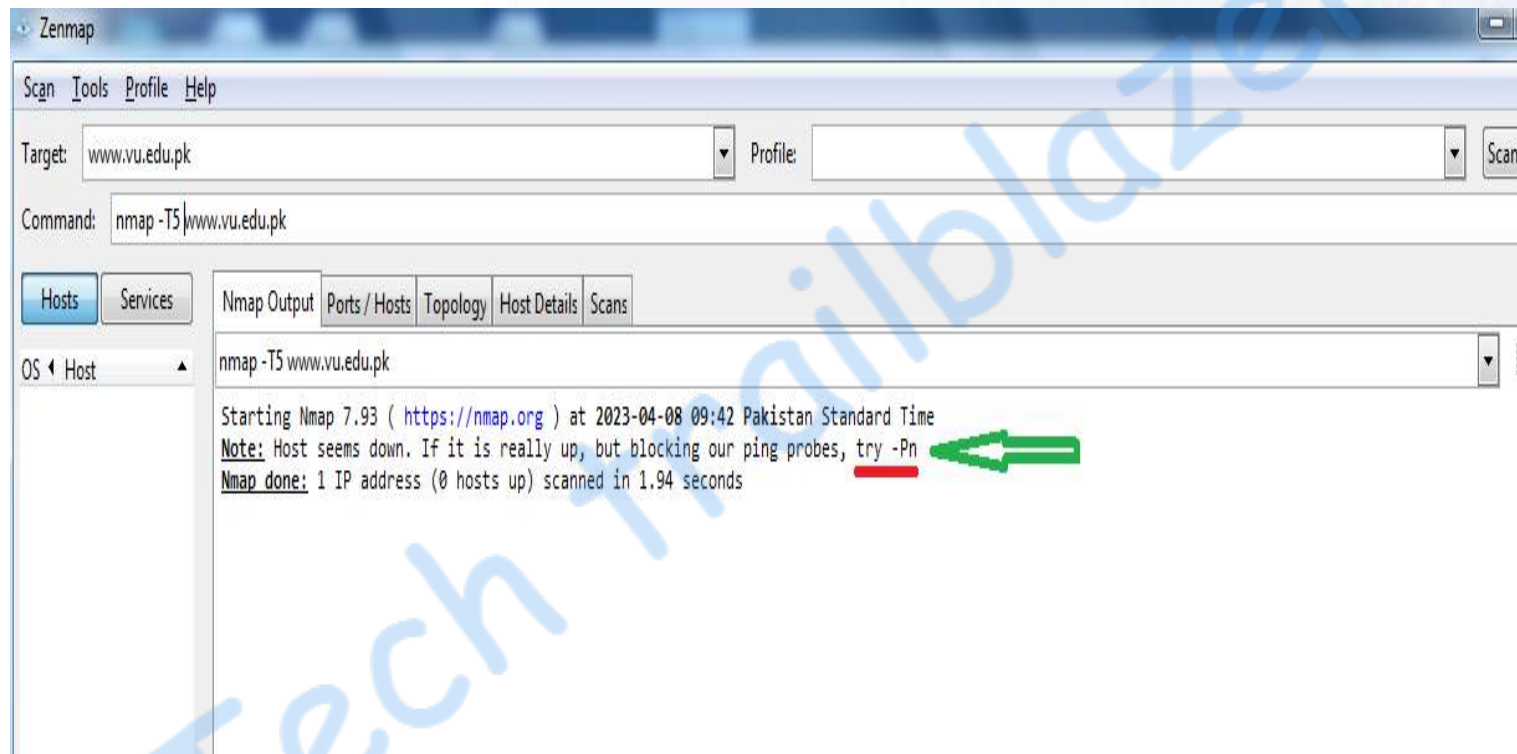
+ Append

Open









in my paper nothing was related to nessus
or qulus

Nessus New scan

Nessus  Scans Settings

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

My Scans

Import New Folder New Scan

1 Scan

☐	Name	Schedule	Last Modified -	
☐	Basic Discovery Scan	Weekly on Tue at 3:00 PM	Today at 2:43 PM	▶ ✕

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Scan Templates

[Back to Scans](#)

Scanner

User Defined

Search Library

**Advanced Scan**

Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**

Audit the configuration of third-party cloud services.

**Badlock Detection**

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**

A full system scan suitable for any host.

**Credentialed Patch Audit**

Authenticate to hosts and enumerate missing updates.

**DROWN Detection**

Remote checks for CVE-2016-0800.

**Host Discovery**

A simple scan to discover live hosts and open ports.

**Intel AMT Security Bypass**

Remote and local checks for CVE-2017-5689.

**Internal PCI Network Scan**

Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**

Scan for malware on Windows and Unix systems.

**MDM Config Audit**

Audit the configuration of mobile device managers.

**Mobile Device Scan**

Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**

Audit the configuration of network devices.

**PCI Quarterly External Scan**

Approved for quarterly external scanning as required by PCI.

**Policy Compliance Auditing**

Audit system configurations against a known baseline.

**SCAP and OVAL Auditing**

Audit systems using SCAP and OVAL definitions.

**Shadow Brokers Scan**

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

**Spectre and Meltdown**

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

**WannaCry Ransomware**

Remote and local checks for MS17-010.

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Scan Templates

[Back to Scans](#)

Scanner

User Defined

**Advanced Scan**

Configure a scan without using any recommendations.

**Audit Cloud Infrastructure**

Audit the configuration of third-party cloud services.

**Badlock Detection**

Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

**Bash Shellshock Detection**

Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

**Basic Network Scan**

A full system scan suitable for any host.

**Credentialed Patch Audit**

Authenticate to hosts and enumerate missing updates.

**DROWN Detection**

Remote checks for CVE-2016-0800.

**Host Discovery**

A simple scan to discover live hosts and open ports.

**Intel AMT Security Bypass**

Remote and local checks for CVE-2017-5689.

**Internal PCI Network Scan**

Perform an internal PCI DSS (11.2.1) vulnerability scan.

**Malware Scan**

Scan for malware on Windows and Unix systems.

**MDM Config Audit**

Audit the configuration of mobile device managers.

**Mobile Device Scan**

Assess mobile devices via Microsoft Exchange or an MDM.

**Offline Config Audit**

Audit the configuration of network devices.

**PCI Quarterly External Scan**

Approved for quarterly external scanning as required by PCI.

**Policy Compliance Auditing**

Audit system configurations against a known baseline.

**SCAP and OVAL Auditing**

Audit systems using SCAP and OVAL definitions.

**Shadow Brokers Scan**

Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

**Spectre and Meltdown**

Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5354.

**WannaCry Ransomware**

Remote and local checks for MS17-010.

Nessus

Scans

Settings

FOLDERS

My Scans

Routine Scans

All Scans

Trash

5

RESOURCES

★ Policies

🔧 Plugin Rules

📄 Customized Reports

🔍 Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Description

Folder

Targets

REQUIRED

My Scans

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Upload Targets

Add File

Save

Cancel

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

General

[Schedule](#)[Notifications](#)

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

Mike's Scan

Description

Folder

My Scans

Targets

172.30.0.0/24

Upload Targets

[Add File](#)

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

- Settings
- Credentials
- Compliance
- Plugins

- BASIC
 - General
 - Schedule
 - Notifications
- DISCOVERY >
- ASSESSMENT >
- REPORT >
- ADVANCED >

Enabled ☒

Frequency

- Once
- Once
- Daily
- Weekly
- Monthly
- Yearly

Starts

15:00

Timezone

k

Summary

ay, January 31st, 2018 at 3:00 PM

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

General

Schedule

• Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Email Recipient(s)

Example: me@example.com, you@example.com

Attach Report

OFF

Result Filters

[Add Filter](#)

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

[Credentials](#)[Compliance](#)[Plugins](#)

BASIC

[General](#)[Schedule](#)• [Notifications](#)

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Email Recipient(s)

mike@certmike.com

Attach Report

ON

Report Type

Nessus

Max Attachment Size

25

Size is in MB and should be less than 50. If the report is larger than this size, it will not be attached.

Result Filters

[Add Filter](#)

Save

Cancel

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

Host Discovery

Port Scanning

Service Discovery

ASSESSMENT

REPORT

ADVANCED

Remote Host Ping

Ping the remote host

ON

General Settings

- ☒ Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls within the target range specified for the scan.
- ☐ Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy network discovery bypasses those additional tests.

Ping Methods

- ☒ ARP
- ☒ TCP
- Destination ports
- ☒ ICMP
- ☐ Assume ICMP unreachable from the gateway means the host is down

Maximum number of retries

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

New Scan / Advanced Scan

[← Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

[Host Discovery](#)• [Port Scanning](#)[Service Discovery](#)

ASSESSMENT

REPORT

ADVANCED

Ports

☐ Consider unscanned ports as closedPort scan range:

Local Port Enumerators

- ☒ SSH (netstat)
- ☒ WMI (netstat)
- ☒ SNMP
- ☒ Only run network port scanners if local port enumeration failed
- ☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

- ☐ TCP
- ☐ Override automatic firewall detection
- ☒ Use soft detection

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

[Host Discovery](#)• [Port Scanning](#)[Service Discovery](#)

ASSESSMENT

REPORT

ADVANCED

Ports

☐ Consider unscanned ports as closedPort scan range:

Local Port Enumerators

☒ SSH (netstat)☒ WMI (netstat)☒ SNMP☒ Only run network port scanners if local port enumeration failed☐ Verify open TCP ports found by local port enumerators

Network Port Scanners

☐ TCP☐ Override automatic firewall detection

FOLDERS

My Scans

Routine Scans5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

General

Brute Force

SCADA

Web Applications

Windows

Malware

Accuracy

Antivirus

SMTP

☐ Override normal accuracy

☒ Avoid potential false alarms

☐ Show potential false alarms

☐ Perform thorough tests (may disrupt your network or impact scan speed)

Antivirus definition grace period (in days):

0

Third party domain

example.com

This domain must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be a SMTP server.

From address

nobody@example.com

To address

postmaster@[AUTO_REPLACED_IP]

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings

Credentials

Compliance

Plugins

BASIC >

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED ✓

General Settings

- ☒ Enable safe checks
- ☐ Stop scanning hosts that become unresponsive during the scan
- ☐ Scan IP addresses in a random order

Performance Options

- ☐ Slow down the scan when network congestion is detected

Network timeout (in seconds)

5

Max simultaneous checks per host

5

Max simultaneous hosts per scan

30

Max number of concurrent TCP sessions per host

Max number of concurrent TCP sessions per scan

Debug Settings

- ☐ Log scan details

- FOLDERS
- My Scans
 - Routine Scans 5
 - All Scans
 - Trash
- RESOURCES
- Policies
 - Plugin Rules
 - Customized Reports
 - Scanners

New Scan / Advanced Scan

[Back to Scan Templates](#)

Disable All

Settings

Credentials

Compliance

Plugins

Show End

STATUS	PLUGIN FAMILY ^	TOTAL	STATUS	PLUGIN NAME
ENABLED	AIX Local Security Checks	11392	No plugin family selected.	
ENABLED	Amazon Linux Local Security Checks	953		
ENABLED	Backdoors	111		
ENABLED	CentOS Local Security Checks	2528		
ENABLED	CGI abuses	3779		
ENABLED	CGI abuses : XSS	644		
ENABLED	CISCO	889		
ENABLED	Databases	563		
ENABLED	Debian Local Security Checks	5309		
ENABLED	Default Unix Accounts	167		
ENABLED	Denial of Service	109		
ENABLED	DNS	170		
ENABLED	F5 Networks Local Security Checks	603		
ENABLED	Fedora Local Security Checks	12295		

Nessus

Scans

Settings

Filter

Search Plugin Families

FOLDERS

My Scans

Routine Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

New Scan / Advanced Scan

Back to Scan Templates

Disable A

Settings

Credentials

Compliance

Plugins

Show E

STATUS	PLUGIN FAMILY -	TOTAL	STATUS	PLUGIN NAME
DISABLED	AIX Local Security Checks	11392		No plugin family selected.
ENABLED	Amazon Linux Local Security Checks	953		
ENABLED	Backdoors	111		
ENABLED	CentOS Local Security Checks	2528		
ENABLED	CGI abuses	3779		
ENABLED	CGI abuses : XSS	644		
DISABLED	CISCO	889		
ENABLED	Databases	563		
DISABLED	Debian Local Security Checks	5309		
ENABLED	Default Unix Accounts	167		
ENABLED	Denial of Service	109		
ENABLED	DNS	170		
DISABLED	F5 Networks Local Security Checks	603		
ENABLED	Fedora Local Security Checks	12295		

Save

Cancel

SETTINGS

About

Advanced

Proxy Server

Remote Link

SMTP Server

Custom CA

ACCOUNTS

My Account

About

Overview

Revert from Pro 7

Software Update

Master Password

Automatic Updates

☒ Update all components☐ Update plugins☐ Disabled

Update Frequency

Daily

Daily

Weekly

Monthly

Update Server

pst.mydomain.com

Save

Cancel

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 1

LOGIN SCREEN

Nessus / Login

https://localhost:8834/#/ Search

 **Nessus**
home

 nahil



☒ Remember Me **Sign In**

 **tenable**
network security

Nessus Demo - 1

DASHBOARD

The screenshot displays the Nessus web interface for the 'Scans' section. The browser's address bar shows the URL 'https://localhost:8834/#/scans'. The interface features a dark header with the 'Nessus' logo and navigation links for 'Scans' and 'Policies'. Below the header, the main content area is titled 'Scans' and includes a 'New Scan' button. A sidebar on the left contains links for 'My Scans', 'Trash', 'All Scans', and 'New Folder'. The 'My Scans' section is currently active, showing a message that 'This folder is empty.'.

Nessus Home / Scans

https://localhost:8834/#/scans

Nessus Scans Policies

Scans

+ New Scan

Scans / My Scans

My Scans

This folder is empty.

Trash

All Scans

New Folder

Nessus Demo - 1

NEW SCAN

Scanner Templates

 Advanced Scan Configure a scan without using any recommendations.	 Audit Cloud Infrastructure Audit the configuration of third-party cloud services. UPGRADE	 Badlock Detection Remote and local checks for CVE-2016-2118 and	 Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and	 Basic Network Scan A full system scan suitable for any host.
 Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	 DROWN Detection Remote checks for CVE-2016-0800.	 Host Discovery A simple scan to discover live hosts and open ports.	 Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.	 Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan. UPGRADE
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers. UPGRADE	 Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM. UPGRADE	 Offline Config Audit Audit the configuration of network devices. UPGRADE	 PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI. UPGRADE
 Policy Compliance Auditing Audit system configurations against a known baseline. UPGRADE	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions. UPGRADE	 Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.	 WannaCry Ransomware Remote and local checks for MS17-010.	 Web Application Tests Scan for published and unknown web vulnerabilities.

Nessus Demo - 1

WANNACRY RANSOMWARE SCAN



Nessus Demo - 1

NEW SCAN WINDOW

New Scan / WannaCry Ransomware

Scan Library > Settings Credentials

BASIC

General

Schedule

Notifications

DISCOVERY

REPORT

ADVANCED

Settings / Basic / General

This policy is used to perform remote and local checks for vulnerabilities exploited by WannaCry Ransomware (MS17-010 / CVE-2017-0144). It can be provided to test via WMI and enumerate missing software updates.

Name

REQUIRED

Description

Folder

My Scans

Targets

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

REQUIRED

Nessus Demo - 1

DASHBOARD VIEW WITH SCANS

Scans

[New Scan](#)

My Scans

Trash

All Scans

New Folder

Scans / My Scans

Upload

Search Scans

☐	Name	Schedule	Last Modified ▲		
☐	LOCAL PC WANNACRY	On Demand	✓ 12:53 AM	▶	×
☐	NAHIL PC	On Demand	📅 N/A	▶	×

Nessus Demo - 1

NEW SCAN...

Scanner Templates



Advanced Scan

Configure a scan without using any recommendations.



UPGRADE

Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.



DROWN Detection

Remote checks for CVE-2016-0800.

Nessus Demo - 1

ENTER SCAN DETAILS

New Scan / Advanced Scan

Scan Library > Settings Credentials Compliance Plugins

BASIC ✓

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name LOCALHOST ADVANCED SCAN

Description ADVANCED SCAN

Folder My Scans

Targets LOCALHOST

Nessus Demo - 1

CREDENTIAL SCAN

LOCALHOST ADVANCED SCAN / Confi...

POLICY: ADVANCED SCAN

Scan > Settings **Credentials** Compliance Plugins

CREDENTIALS

ACTIVE CREDENTIALS

▶ Cloud Services	
▶ Database	
▼ Host	
SNMPv3	1 +
SSH	∞ +
Windows	∞ +
▶ Miscellaneous	
▶ Plaintext Authentication	

Save Cancel

Nessus Demo - 1

COMPLIANCE SCAN

LOCALHOST ADVANCED SCAN / Confi...

POLICY: ADVANCED SCAN

Scan > Settings Credentials **Compliance** Plugins

COMPLIANCE CHECKS	ACTIVE COMPLIANCE
▶ Adtran AOS	
▶ Amazon AWS	
▶ Arista EOS	
▶ BlueCoat ProxySG	
▶ Brocade FabricOS	
▶ Check Point GAiA	
▶ Cisco IOS	
▶ Citrix XenServer	
▶ Database	
▶ Dell Force10 FTOS	

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)

► Unix File Contents	
► VMware vCenter/vSphere	
► WatchGuard	
▼ Windows	
(Upload a custom Windows audit file)	∞ +
CIS Exchange 2007 Enterprise Edge Transport 1...	1 +
CIS Google Chrome L1 v1.1.0	1 +
CIS Google Chrome L2 v1.1.0	1 +
CIS IE 10 v1.1.0	1 +
CIS IE 11 v1.0.0	1 +
CIS IE 9 v1.0.0	1 +
CIS IIS 10 v1.0.0 Level 1	1 +
CIS IIS 10 v1.0.0 Level 2	1 +
CIS IIS 6.0 v1.0.0	1 +
CIS IIS 7 L2 v1.8.0	1 +
CIS IIS 8.0 v1.5.0 Level 1	1 +
CIS IIS 8.0 v1.5.0 Level 2	1 +

Nessus Demo - 1

WINDOWS COMPLIANCE MENU (CIS)...

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0	×
CIS Microsoft Office Outlook 2013 v1.1.0 Level 1	×
CIS Microsoft Office 2013 v1.1.0	×
CIS Microsoft Office Word 2013 v1.1.0	×
CIS IE 10 v1.1.0	×
▶ CIS Google Chrome L1 v1.1.0	×
CIS Microsoft Office PowerPoint 2013 v1.0.1	×
CIS Windows 7 Level 2 v3.0.1	×
▼ DISA STIG Google Chrome V1R8	×

Nessus Demo - 1

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

- Lets take a look at Nessus Demo
- <https://www.tenable.com/products/nessus/nessus-professional/evaluate>
- Download free 7 day trial
- Get activation key from website

Nessus Demo - 2

ADVANCED SCAN / COMPLIANCE

ACTIVE COMPLIANCE CHECKS

CIS IIS 7 L1 v1.8.0	×
CIS Microsoft Office Outlook 2013 v1.1.0 Level 1	×
CIS Microsoft Office 2013 v1.1.0	×
CIS Microsoft Office Word 2013 v1.1.0	×
CIS IE 10 v1.1.0	×
▶ CIS Google Chrome L1 v1.1.0	×
CIS Microsoft Office PowerPoint 2013 v1.0.1	×
CIS Windows 7 Level 2 v3.0.1	×
▼ DISA STIG Google Chrome V1R8	×

Nessus Demo - 2

ADVANCED SCAN / PLUG-INS

LOCALHOST ADVANCED SCAN / Confi... POLICY: ADVANCED SCAN

Disable All Enable All Filter Plugin Families

Scan > Settings Credentials Compliance **Plugins**

Show Enabled | Show All

Status	Plugin Name	Plugin ID
DISABLED	SuSE Local Security Checks	10107
DISABLED	Ubuntu Local Security Checks	3763
DISABLED	Virtuozzo Local Security Checks	130
DISABLED	VMware ESX Local Security Checks	114
DISABLED	Web Servers	1018
DISABLED	Windows	3772
ENABLED	Windows : Microsoft Bulletins	1323
DISABLED	Windows : User management	28
ENABLED	2X ApplicationServer TuxSystem ActiveX ExportSettings() Method Ar...	58484
ENABLED	2X Client TuxClientSystem ActiveX InstallClient() Method Arbitrary M...	58321
ENABLED	3CTftpSvc Long Transport Mode Remote Overflow	23735
ENABLED	3D-FTP Multiple Directory Traversal Vulnerabilities	33218
ENABLED	3DGreetings Player ActiveX Multiple Buffer Overflows	26020
ENABLED	3ivx MPEG-4 < 5.0.2 Buffer Overflow	29749
ENABLED	7-Zip < 16.00 Multiple Vulnerabilities	91230

Save Cancel

Nessus Demo - 2

SCAN...IN PROGRESS

Scans

Upload Search Scans

+ New Scan

Scans / My Scans

☐ Name	Schedule	Last Modified ▲
☐ LOCALHOST ADVANCED SCAN	On Demand	01:32 AM

My Scans 1

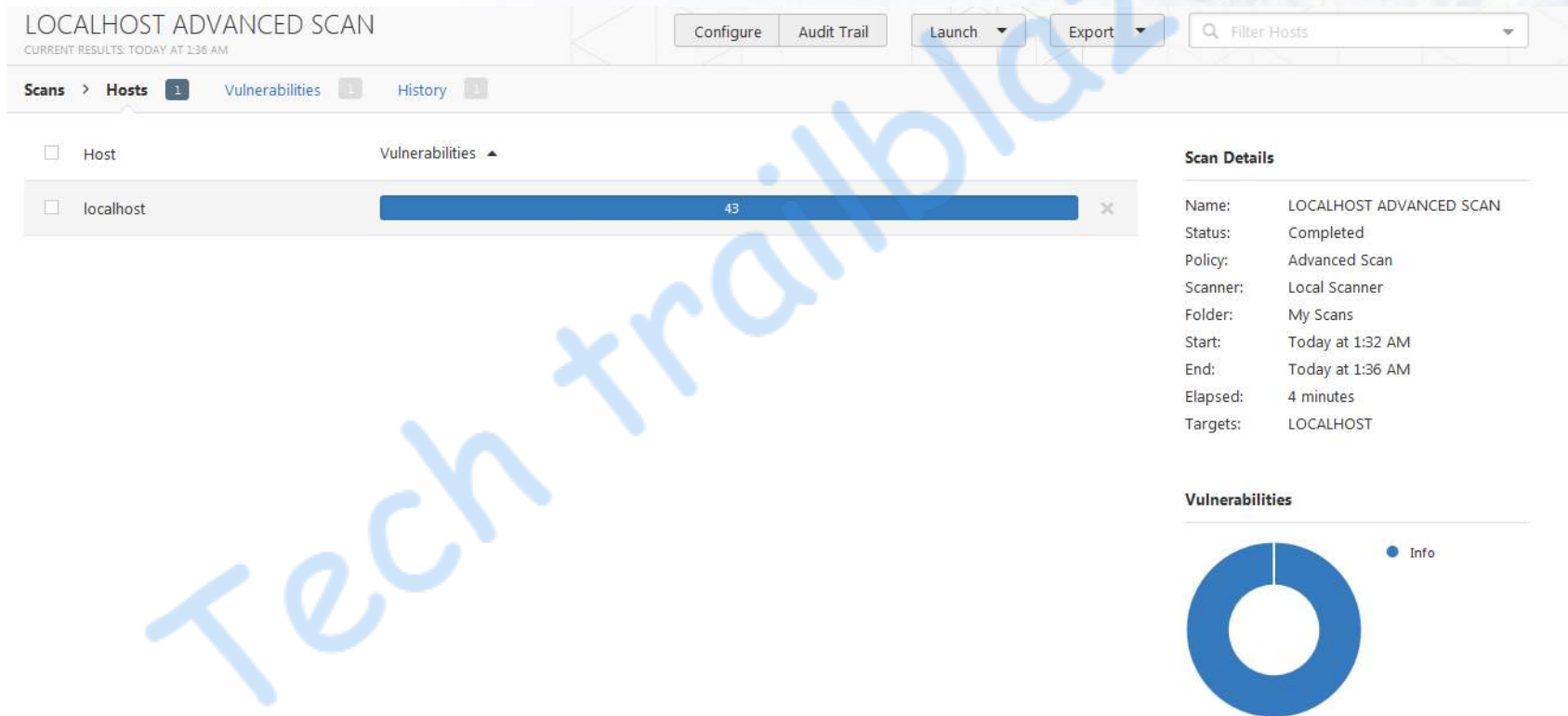
Trash 1

All Scans

New Folder

Nessus Demo - 2

SCAN REPORT [43 INFO]



Nessus Demo - 2

SCAN REPORT [DETAILS]

LOCALHOST ADVANCED SCAN
CURRENT RESULTS: TODAY AT 1:36 AM

Configure

Audit Trail

Launch

Export

Filter Vulnerabilities

Hosts > localhost > Vulnerabilities 1

☐	Severity ▲	Plugin Name	Plugin Family	Count
☐	INFO	Netstat Portscanner (SSH)	Port scanners	43

Host Details

IP: 127.0.0.1
DNS: localhost
OS: Microsoft Windows 7 Home
Start: Today at 1:32 AM
End: Today at 1:36 AM
Elapsed: 4 minutes
KB: [Download](#)

Vulnerabilities

Info



Nessus Demo - 2

SCAN REPORT [DETAILS...]

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost 

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost 

Port 135/tcp was found to be open

Port ▼	Hosts
135 / tcp / epmap	localhost 

Port 137/udp was found to be open

Port ▼	Hosts
137 / udp	localhost 

Nessus Demo - 2

WEB APPLICATION TEST

Audit

ration of
ices.

PCI Quarterly External Scan

Approved for quarterly external
scanning as required by PCI.

omware
checks for
l.



Web Application Tests

Scan for published and unknown
web vulnerabilities.

Nessus Demo - 2

WEB APPLICATION TEST - CREDENTIALS

New Scan / Web Application Tests

Scan Library > Settings Credentials

CREDENTIALS

All credentials in use

ACTIVE CREDENTIALS

HTTP

Authentication method	HTTP login form
Username	admin REQUIRED
Password	REQUIRED
Login page	/login.php REQUIRED
Login submission page	/process_login.php REQUIRED
Login parameters	user=%USER%&pass=%PASS% REQUIRED

If the keywords %USER% and %PASS% are used, they will be substituted with the values above.

Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT



Nessus Demo - 2

CREDENTIALIALED PATCH AUDIT

New Scan / Credentialed Patch Audit

Scan Library > Settings Credentials

CREDENTIALS

- Database
- Host
 - SSH
 - Windows
- Miscellaneous
- Plaintext Authentication

ACTIVE CREDENTIALS

Windows

Authentication method: Password

Username: administrator

Password:

Domain:

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication

Nessus Demo - 2

SCANS DASHBOARD

Scans

New Scan

My Scans 1

Trash 1

All Scans

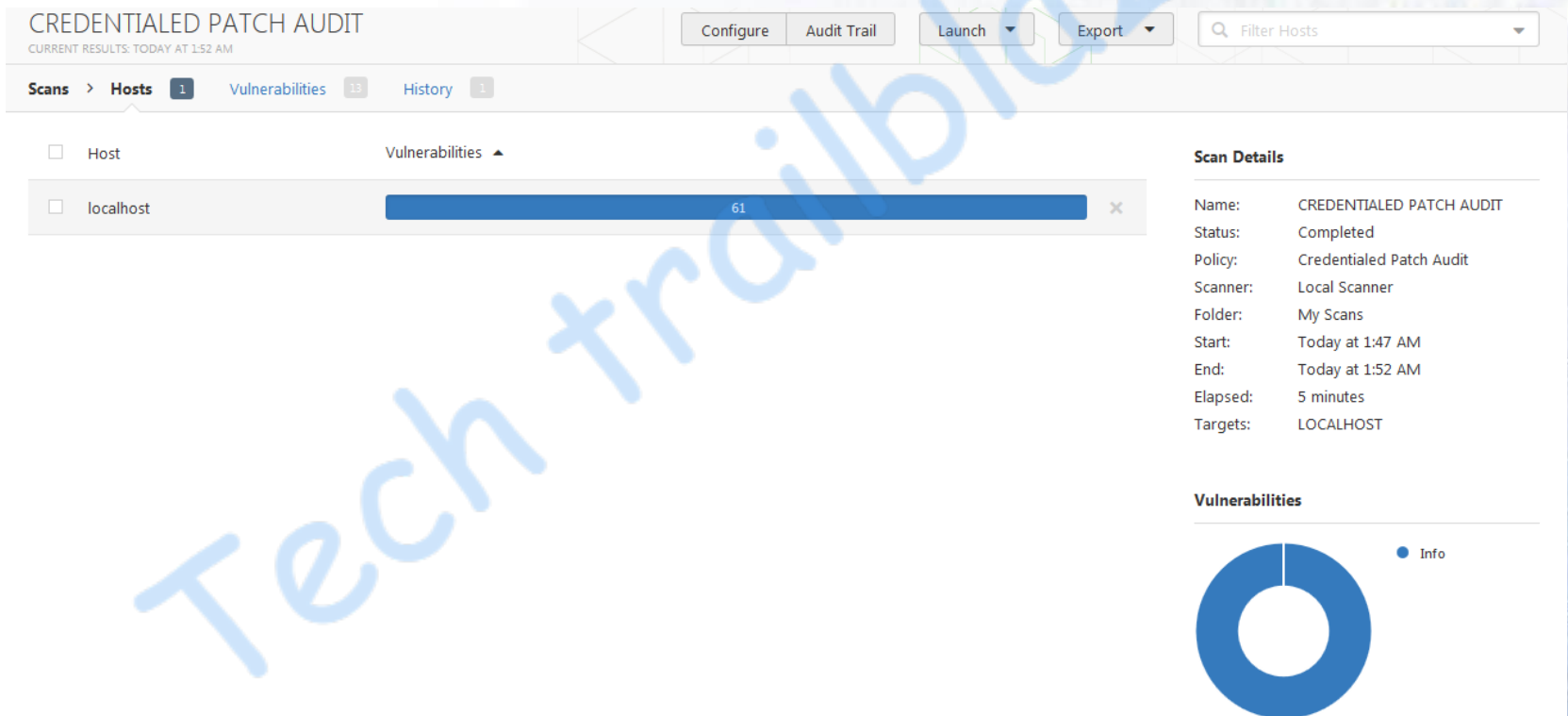
New Folder

Scans / My Scans

☐ Name	Schedule	Last Modified ▲	
☐ CREDENTIALIAED PATCH AUDIT	On Demand	01:47 AM	■
☐ LOCALHOST ADVANCED SCAN	On Demand	01:36 AM	▶ ✕

Nessus Demo - 2

CREDENTIALIAED AUDIT SCAN RESULTS [61 INFO]



Nessus Demo - 2

CREDENTIALIALED AUDIT SCAN RESULTS [61 INFO]

CREDENTIALIALED PATCH AUDIT
CURRENT RESULTS: TODAY AT 1:52 AM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > localhost > Vulnerabilities 13

☐ Severity ▲	Plugin Name	Plugin Family	Count	Host Details
☐ INFO	Netstat Portscanner (SSH)	Port scanners	43	IP: 127.0.0.1
☐ INFO	DCE Services Enumeration	Windows	7	DNS: localhost
☐ INFO	Authenticated Check : OS Name and Installed Package Enumeration	Settings	1	OS: Microsoft Windows 7 Home
☐ INFO	Authentication Failure - Local Checks Not Run	Settings	1	Start: Today at 1:47 AM
☐ INFO	Microsoft Windows NTLMSSP Authentication Request Remote Network Nam...	Windows	1	End: Today at 1:52 AM
☐ INFO	Microsoft Windows SMB Log In Possible	Windows	1	Elapsed: 5 minutes
☐ INFO	Microsoft Windows SMB NativeLanManager Remote System Information Dis...	Windows	1	KB: Download
☐ INFO	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Regi...	Windows	1	
☐ INFO	Microsoft Windows SMB Service Detection	Windows	1	

Vulnerabilities

Info



Nessus Demo - 2

CREDENTIALIAED AUDIT SCAN RESULTS [DETAILS]

INFO Netstat Portscanner (SSH) >

Description

Nessus was able to run 'netstat' on the remote host to enumerate the open ports.

See the section 'plugins options' about configuring this plugin.

See Also

<https://en.wikipedia.org/wiki/Netstat>

Output

Port 68/udp was found to be open

Port ▼	Hosts
68 / udp	localhost

Port 123/udp was found to be open

Port ▼	Hosts
123 / udp	localhost

Port 135/tcp was found to be open

Plugin Details

Severity:	Info
ID:	14272
Version:	1.68
Type:	remote
Family:	Port scanners
Published:	2004/08/15
Modified:	2017/06/16

Risk Information

Risk Factor: None

Nessus Demo - 2

SYSTEM MALWARE SCAN

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.	DROWN Detection Remote checks for CVE-2016-0800.
 Malware Scan Scan for malware on Windows and Unix systems.	 MDM Config Audit Audit the configuration of mobile device managers.
 Policy Compliance Auditing Audit system configurations against a known baseline.	 SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

Nessus Demo - 2

SYSTEM MALWARE SCAN

New Scan / Malware Scan

Scan Library > Settings Credentials

CREDENTIALS

Host
SSH
Windows

ACTIVE CREDENTIALS

Windows

Authentication method Password

Username administrator

Password

Domain

Global Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication
- ☐ Start the Remote Registry service during the scan

Nessus Demo - 2

SCAN DASHBOARD

Scans

+ New Scan

My Scans 1

Trash 1

All Scans

New Folder

Scans / My Scans

☐ Name	Schedule	Last Modified ▲		
☐ WEBSITE	On Demand	02:16 AM		■
☐ SYSTEM MALWARE SCAN	On Demand	✓ 02:10 AM	▶	✕
☐ CREDENTIALED PATCH AUDIT	On Demand	✓ 01:52 AM	▶	✕
☐ LOCALHOST ADVANCED SCAN	On Demand	✓ 01:36 AM	▶	✕

© 1998 - 2017 Tenable Network Security®. All Rights Reserved. Nessus Home v. 6.10.9

Nessus Demo - 2

SYSTEM MALWARE SCAN [2 INFO]

SYSTEM MALWARE SCAN
CURRENT RESULTS: TODAY AT 2:10 AM

Configure Audit Trail Launch Export Filter Hosts

Scans > Hosts 1 Vulnerabilities 2 History 2

☐ Host Vulnerabilities ▲

☐ localhost 2

Scan Details

Name: SYSTEM MALWARE SCAN
Status: Completed
Policy: Malware Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 2:10 AM
End: Today at 2:10 AM
Elapsed: a few seconds
Targets: LOCALHOST

Vulnerabilities

Info



A donut chart representing the distribution of vulnerability information. It consists of a single blue segment that covers the entire circle, indicating that all 2 vulnerabilities are of the 'Info' type. A legend to the right of the chart shows a blue dot next to the label 'Info'.

Nessus Demo - 2

SYSTEM MALWARE SCAN

SYSTEM MALWARE SCAN

CURRENT RESULTS: TODAY AT 2:10 AM

[Configure](#)[Audit Trail](#)[Launch](#)[Export](#)

[Hosts](#) > [localhost](#) > [Vulnerabilities](#) **2**

☐ Severity ▲	Plugin Name	Plugin Family	Count
☐ INFO	Authentication Failure - Local Checks Not Run	Settings	1
☐ INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1

Host Details

IP: 127.0.0.1
DNS: localhost
Start: Today at 2:10 AM
End: Today at 2:10 AM
Elapsed: a few seconds
KB: [Download](#)

Vulnerabilities



Nessus Demo - 2

- Nessus is an easy to use and powerful scanner
- Dozens of scans on dashboard
- Setup a new scan
- Setup a profile as scan template
- Credentialed scan
- Thousands of plugins from CIS/DISA etc

END

Nessus scan Types

Nessus Credentialed scan



Credentialed Scanning

Uses passwords to log into systems

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

My Scans

Import

New Folder

Search Scans



2 Scans

☐	Name	Schedule	Last Modified ▾
☐	Basic Discovery Scan	Weekly on Tue at 3:00 PM	✓ Today at 2:43 PM
☐	Mike's Scan	Daily at 3:00 PM	📁 N/A

Nessus Scans Settings

FOLDERS

- My Scans
- Routine Scans 5
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports
- Scanners

Mike's Scan

[Back to My Scans](#)

Configure

Hosts 0 History 0

No hosts are available.

Scan Details

Name:	Mike's Scan
Status:	Empty
Scanner:	Local Scanner

Nessus

ScansSettings

FOLDERS

My Scans

Routine Scans5

All Scans

Trash

RESOURCES

★ Policies

🔧 Plugin Rules

📄 Customized Reports

🔍 Scanners

Mike's Scan / Configuration

← Back to Scan Report

SettingsCredentialedCompliancePlugins

BASIC

GeneralScheduleNotifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Mike's Scan

Description

Folder

My Scans

Targets

172.30.0.0/24

Upload Targets

Add File

Save

Cancel

Nessus

Scans

Settings

FOLDERS

My Scans

Routine Scans 5

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Scanners

Mike's Scan / Configuration

[Back to Scan Report](#)

Settings

Credentials

Compliance

Plugins

CATEGORIES

Host

Filter Credentials

SNMPv3

SSH

Windows

Save

Cancel

Nessus  Scans Settings

Mike's Scan / Configuration
[Back to Scan Report](#)

Settings Credentials Compliance Plugins

CATEGORIES Host

Filter Credentials

SNMPv3	1
SSH	00
Windows	00

Save Cancel

Nessus Scans Settings

Mike's Scan / Configuration
[Back to Scan Report](#)

Settings Credentials Compliance Plugins

CATEGORIES Host

Filter Credentials

SNMPv3 1

SSH 00

Windows 00

Windows

Authentication method Password

Username vulnerabilityscan

Password

Domain

Global Credential Settings

- ☒ Never send credentials in the clear
- ☒ Do not use NTLMv1 authentication
- ☐ Start the Remote Registry service during the scan
- ☐ Enable administrative shares during the scan

Save Cancel

Qualys Demo - 1

- Lets take a look at Qualys Demo
- Free Qualys tools:
 - BrowserCheck
 - SSL
- Qualys FreeScan
 - Vulnerability
 - OWASP
 - Patch Tuesday
 - SCAP

Qualys Demo - 1

The screenshot shows the Qualys BrowserCheck website. At the top, the Qualys logo is on the left, and navigation links for 'About', 'FAQ', 'Feedback', 'Qualys.com', and 'Try Coinblocker' are on the right. The main heading is 'Check your browser.' followed by a paragraph: 'Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.' Below this, there are two buttons: a green 'Install Plugin' button and a yellow 'Scan without installing plugin' button. A green arrow points to the yellow button. Below the buttons are three columns of content. The first column has a USB icon and the text 'Check your browser and system security' with a subtext 'Click the "Install Plugin" button to enable fast, safe scanning.' The second column has icons for various browsers and the text 'Find vulnerabilities at the click of a button' with a subtext 'Scan and view all security issues in an easy-to-understand detailed list.' The third column has a 'Fix It' button and the text 'Take charge of any issues found' with a subtext 'Follow recommended steps to resolve each vulnerability found.' At the bottom, there is a link 'Learn more about Qualys BrowserCheck'.

Qualys. BrowserCheck

About FAQ Feedback Qualys.com Try Coinblocker

Check your browser.

Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.

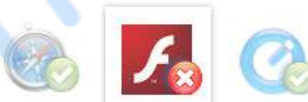
Install Plugin

Scan without installing plugin



Check your browser and system security

Click the "Install Plugin" button to enable fast, safe scanning.



Find vulnerabilities at the click of a button

Scan and view all security issues in an easy-to-understand detailed list.



Take charge of any issues found

Follow recommended steps to resolve each vulnerability found.

Learn more about
Qualys BrowserCheck

<https://www.qualys.com/free-services/>

Qualys® BrowserCheck Summary

Scan start time: **Tue Apr 04 2023, 9:18 AM**

Scan duration: **00:01** (mm:ss)

Congratulations! You passed Qualys BrowserCheck.

We recommend you scan your browser regularly to stay up to date with the latest versions and plugins.

[Re-Scan](#)

INFO: For more comprehensive and automated scans [install Qualys BrowserCheck Plugin](#).



Google Chrome
111.0.0.0

Up To Date

 **Qualys.** BrowserCheck
BUSINESS EDITION

Browser security for
your organization

Monitor all your computers
and check whether they're
staying up-to-date.

Easy, Accurate & FREE!

[Try It Now >](#)



HOW WELL DO YOU KNOW SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.



Test your server »

Test your site's certificate and configuration



Test your browser »

Test your browser's SSL implementation



SSL Pulse »

See how other web sites are doing



Documentation »

Learn how to deploy SSL/TLS correctly

Books



[*Bulletproof SSL and TLS*](#) is a complete guide to deploying secure servers and web applications. This book, which provides comprehensive coverage of the ever-changing field of SSL/TLS and Web PKI, is intended for IT security professionals, system

administrators, and developers, with the main focus on getting things done. [MORE »](#)

News

[LinkedIn Faux Pas Shines Light on Certificate Management](#)

May 24, 2019

[Zombie POODLE and GOLDENDOODLE Vulnerabilities](#)

April 22, 2019

[PCI & SSL/Early TLS QIDs 38601, 42366](#)

March 14, 2019

About SSL Labs

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristić, Qualys

Qualys Demo - 1

SSL LABS REPORT

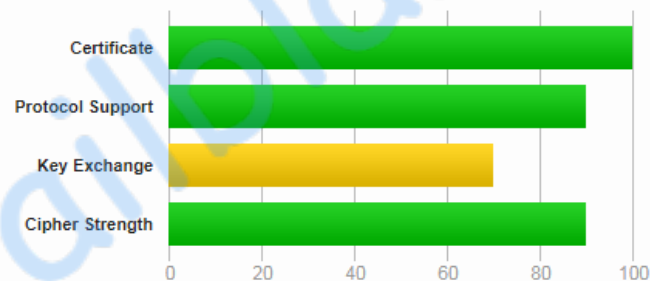


Qualys Demo - 1

SSL LABS REPORT

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)

<https://www.qualys.com/free-services/>
<https://www.ssllabs.com/>

Qualys Demo - 1

PROTOCOL DETAILS

BEAST attack	Not mitigated server-side (more info)	SSL 3: 0xa, TLS 1.0: 0xc014
POODLE (SSLv3)	Vulnerable INSECURE (more info)	SSL 3: 0xa
POODLE (TLS)	No (more info)	
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)	
SSL/TLS compression	No	
RC4	Yes INSECURE (more info)	
Heartbeat (extension)	No	
Heartbleed (vulnerability)	No (more info)	
Ticketbleed (vulnerability)	No (more info)	
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)	
Forward Secrecy	Weak key exchange WEAK	
ALPN	No	

Qualys Demo - 1

QUALYS FREESCAN

New Scan

Scan a URL and receive results on Web Application and Network Vulnerabilities, OWASP Security Risks, and Malware audits. Or, enter an IP address to scan external or internal hosts for Vulnerabilities, authenticated Patch Tuesday audits, or run a SCAP compliance scan.

Choose Scan Type



VULNERABILITY

Network | WAS | MDS Scans



OWASP

Risk Scan



PATCH TUESDAY

Authenticated Scan



SCAP

Compliance Scan

Last Scan Result

OWASP Scan

<http://www.delt...>

Summary: No OWASP Categorie...

16 Jul 2017



Vulnerability Summary

VM(33) WAS(0) MDS(0)



Patch Audit Summary

4 Patches | 4 Vulns Addressed

Last 5 Scan Results

16 Jul 2017	http://www.deltatechglobal.com	
16 Jul 2017	http://www.deltatechglobal.com	View Rescan
16 Jul 2017	http://www.vu.edu.pk	

Qualys Demo - 1



Welcome Nahil

Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

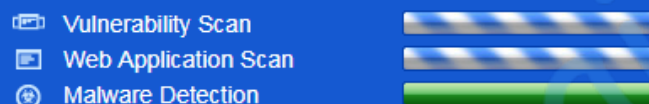
[Back to Home](#)

[Quick Tour](#) | [Upgrade Now](#) | [Nahil Mahmood](#) | [2 Scans](#)

Scan in Progress

[Cancel scan](#)

<http://www.deltatech.com>



In progress
In progress
Scan complete

Scan in Progress

[Cancel scan](#)

<http://www.deltatech.com>



Scan complete
In progress
Scan complete

OWASP Scan rename

Summary: No OWASP Categories Found.

Threat Summary: 33 Vulnerabilities Found

Patch Report Summary: 4 Patches Available

<http://www.deltatech.com>
16 July 2017 at 1:25AM (GMT+0500)



[View Report >](#)

Qualys Demo - 1

OWASP SCAN PATCH REPORT



OWASP Scan [rename](#)

No Authentication Used

16 July 2017 at 11:25AM (GMT+0500)

4

Patches
Required

4

Vulnerabilities
Addressed

<http://www.deltatech.com>

www.deltatech.com

Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (4)

Microsoft (0)

Oracle (0)

Adobe (0)

Others (4)

Patches

1 - 4 of 4 < >

OpenSSH LoginGraceTime Denial of Service Vulnerability	1
OpenSSH Commands Information Disclosure Vulnerability	1
OpenSSH J-PAKE Session Key Retrieval Vulnerability	1
OpenSSH "X SECURITY" Bypass Vulnerability	1

OpenSSH LoginGraceTime Denial of Service Vulnerability

QID: 42413

Published: 09 February 2013

Vendor ID: OpenSSH

CVE: CVE-2010-5107

Solution:

Customers are advised to upgrade to [OpenSSH 6.2](#) and apply the associated server configuration settings to remediate this vulnerability.

1 Vulnerabilities Addressed

QID: 42413

Published: 09 February 2013



OpenSSH LoginGraceTime Denial of Service Vulnerability

Qualys Demo - 1

THREAT REPORT

View by:

OWASP Report

Patch Report

Threat Report

Print Report ▼



OWASP Scan [rename](#)

External Host Vulnerability Report

16 July 2017 at 1:25AM (GMT+0500)

33

Vulnerabilities
Detected

0

HIGH
Risk

10

MED
Risk

23

LOW
Risk

78

INFO
Gathered

<http://www.deltatechglobal.com>

www.deltatechglobal.com

Ubuntu / Linux 2.6.x

Rescan URL

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID



All Scan Results

1 - 25 of 111

Mail Server Accepts Plaintext Credentials	
Discovery of Unix Account Names Vulnerability	
Web Server Stopped Responding	
Discovery of Unix Account Names Vulnerability	
POP3 Server Allows Plain Text Authentication Vulnerability	

Mail Server Accepts Plaintext Credentials

QID: 74147

CVE Base: 5.3

Port: 587

CVSS Temporal: 4.8

Category: Mail
services

CVE ID: -

Threat:

Your Mail Server responds to the EHLO command which implies that it uses the ESMTP protocol. ESMTP uses the AUTH command which indicates an authentication mechanism to the server. If the server supports the requested authentication mechanism, it performs an authentication protocol exchange to

Qualys Demo - 1

THREAT REPORT

Filter by:

All (33)

Level 5 (0)

Level 4 (0)

Level 3 (10)

Level 2 (20)

Level 1 (3)

Info (78)

Search for Title, Category, CVE ID or QID



All Scan Results

1 - 10 of 10

	Mail Server Accepts Plaintext Credentials	
	Discovery of Unix Account Names Vulnerability	
	Web Server Stopped Responding	
	Discovery of Unix Account Names Vulnerability	
	POP3 Server Allows Plain Text Authentication Vulnerability	
	OpenSSH J-PAKE Session Key Retrieval Vulnerability	
	OpenSSH LoginGraceTime Denial of Service Vulnerability	
	OpenSSH Commands Information Disclosure Vulnerability	
	OpenSSH "X SECURITY" Bypass Vulnerability	
	Apache Partial HTTP Request Denial of Service Vulnerability	

Discovery of Unix Account Names Vulnerability

QID: 5001

CVE Base: 3.3

Port: 80



CVSS Temporal: 3

Category: Brute Force Attack

CVE ID: CVE-2001-1013

Threat:

When a request for a user is made (<http://your.host/~user>), certain servers (such as Apache Versions 1.3.12 and 1.3.9) return a different reply depending on whether the account user exists on the host or not.

If a request is made for an account that exists on the host, a 403 error is returned. If a request is made for a non-existent account, then a 404 error is returned.

Impact:

Unauthorized remote users can implement brute force attacks on the Web server to guess a valid account name on the server. Even though they may be successful in obtaining a valid account, they will still have to guess the password. However, if user passwords are weak, some services may also be brute forced.

Solution:

Disable the default-enabled "UserDir" directive. To do so, add the following line to the httpd.conf file:

UserDir Disabled

Qualys Demo - 1

- Qualys is a powerful cloud-based vulnerability management tool
- Several online free tools
- Advanced web application security testing

END

QUALYS DEMO - PART 3

- Lets have a look at some further features of Qualys:
- Qualys Continuous Monitoring

Tech trailblazer

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3

Ruleset Builder Launch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

Description

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types

-  Host
-  Vulnerability
-  Certificate
-  Port / Service
-  Software
-  Ticket

Drag rules here to add them to the ruleset



RULESET BUILDER

QUALYS DEMO - PART 3

Ruleset BuilderLaunch help

Add one or more rules to this ruleset. Each rule describes an event you want to be alerted on.

Title*

Description

This is where you add and customize rules. Your rules can be simple (any new vulnerability) or complex (any new severity 5 vulnerability on a Linux host).

Rule Types


Host


Vulnerability


Certificate


Port / Service


Software


Ticket

Rule 1: New or Fixed or Active or Reopened VulnerabilityRemove

Your selection may result in excessive alerts. Select more filters to get fewer alerts.

When a vulnerability is*☒ New☒ Fixed☒ Active☒ Reopened

 Add Criteria

Rule 2: New or Expired or Expiring CertificateRemove

When a certificate is*☒ New☐ Expiring in 10 days☒ Expired☒ Expiring in 30 days☒ Expiring in 90 days

 Add Criteria

Rule 3: Opened or Changed or Closed Port / ServiceRemove

When a port/service is*☒ Opened☒ Changed☒ Closed

 Add Criteria

RULETYPES & CONFIGURATION

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Help ▾ Nahil Mahmood ▾ Log out

Alerts Configuration

74 days remaining in trial. [Upgrade Now](#)

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ [New Ruleset](#)

2 rulesets ⚙ ▾

☐	Title	# Profiles	Created by	Created on
☐	WEBSITE CHANGES DETECT CHANGES TO WEBSITE	0	detat-nm1	20 Sep 2018 10:56PM GMT+0500
☐	Initial Ruleset (System) With the Initial Ruleset you will receive alerts when a new host is found, a port is open, or an SSL certificate is expired or is about to expire. Use this ruleset as is or save a copy of it to make changes.	0	System	19 May 2018 7:38PM GMT+0500

RULESETS INTERFACE

QUALYS DEMO - PART 3

Welcome to Qualys® Continuous Monitoring

Thank you for signing up to continuously monitor your perimeter network. Receive alerts to threats and unexpected changes as they happen. Make sure you schedule your scans to run on a frequent or continuous basis. [Learn more](#)

Get started with continuous monitoring

[Skip to Dashboard >](#)



Set up rulesets

Tell us the events you want to be alerted on - open ports, expiring certificates, new hosts, software applications, and more. [View the Initial Ruleset](#) provided by Qualys or create a new ruleset.



Configure monitoring profiles

Associate a ruleset with the hosts you want to monitor, and select when and how individuals and teams will be notified of new alerts.



View your alerts

Check out the alerts on your scanned hosts and search for specific alert and host details.

QUALYS CONTINUOUS MONITORING INTERFACE

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 1 of 3

- Hosts** ✓
- Ruleset
- Notifications

Configure a profile for continuous monitoring of your hosts.

Profile for Continuous Monitoring (*) REQUIRED FIELDS

Title*

Choose Target Hosts

Tell us which hosts (IP addresses) you would like to monitor.

☐ Select Tags ☒ Select IPs/Ranges

IPs/Ranges

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

Exclude IPs/Ranges

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

PROFILE CREATION

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 2 of 3

- 1 Hosts
- 2 Ruleset
- 3 Notifications

Choose a set of alert rules to be used for this profile.

Choose Ruleset (*) REQUIRED FIELD

Your ruleset tells us the events you would like to be alerted on. For example: new host found, host changed, SSL certificate expired, vulnerability detected and more.

Alert Ruleset*

WEBSITE CHANGES

Create New

WEBSITE CHANGES [Edit](#)

Description:
DETECT CHANGES TO WEBSITE

Cancel

Previous

Continue

CHOOSE RULESET

QUALYS DEMO - PART 3

Monitoring Profile CreationTurn help tips: On | Off Launch help

Step 3 of 3

- 1 Hosts ✓
- 2 Ruleset ✓
- 3 Notifications ✓

You have the option to set up alert notifications for you and other users.

Frequency (*) REQUIRED FIELD

Tell us how often you want to receive notifications.

Send email alerts

Users

Tell us who should receive alerts. Select from your distribution groups.

Distribution Groups

TECHNICAL (1 email)

NOTIFICATIONS

QUALYS DEMO - PART 3

Continuous Monitoring ▾

Alerts Configuration

Configuration Monitoring Profiles Rulesets License Details

Search...

Actions (0) ▾ New Profile

☐	Title	Ruleset	Notifications	Created by
☐	☒ WEBSITE	WEBSITE CHANGES	daily	detat-nm1

MONITORING PROFILE ACTIVE

QUALYS DEMO - PART 3

- Qualys Continuous Monitoring is very useful for watching critical changes that may impact security

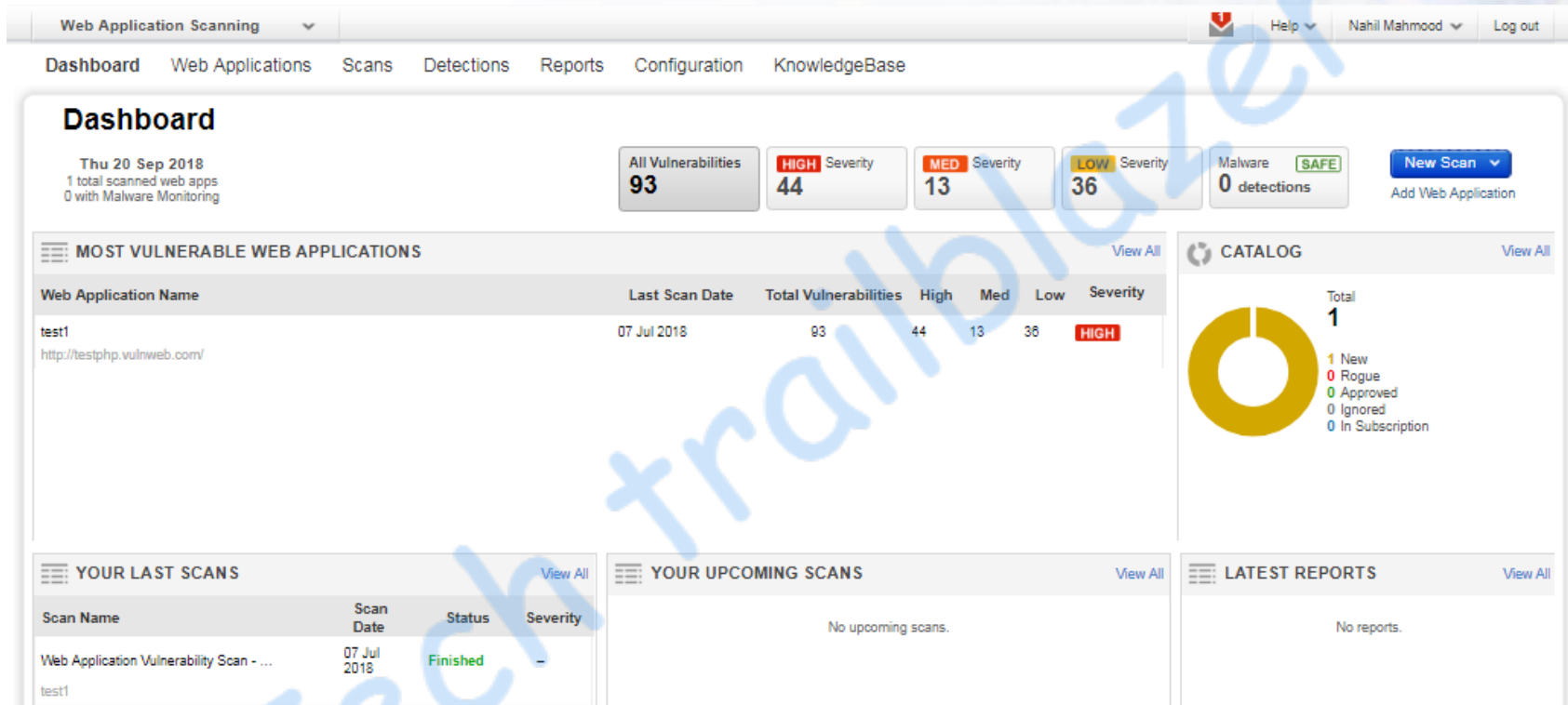
END

QUALYS WEB APPLICATION SCANNING

- Lets have a look at Qualys Web Application Scanning

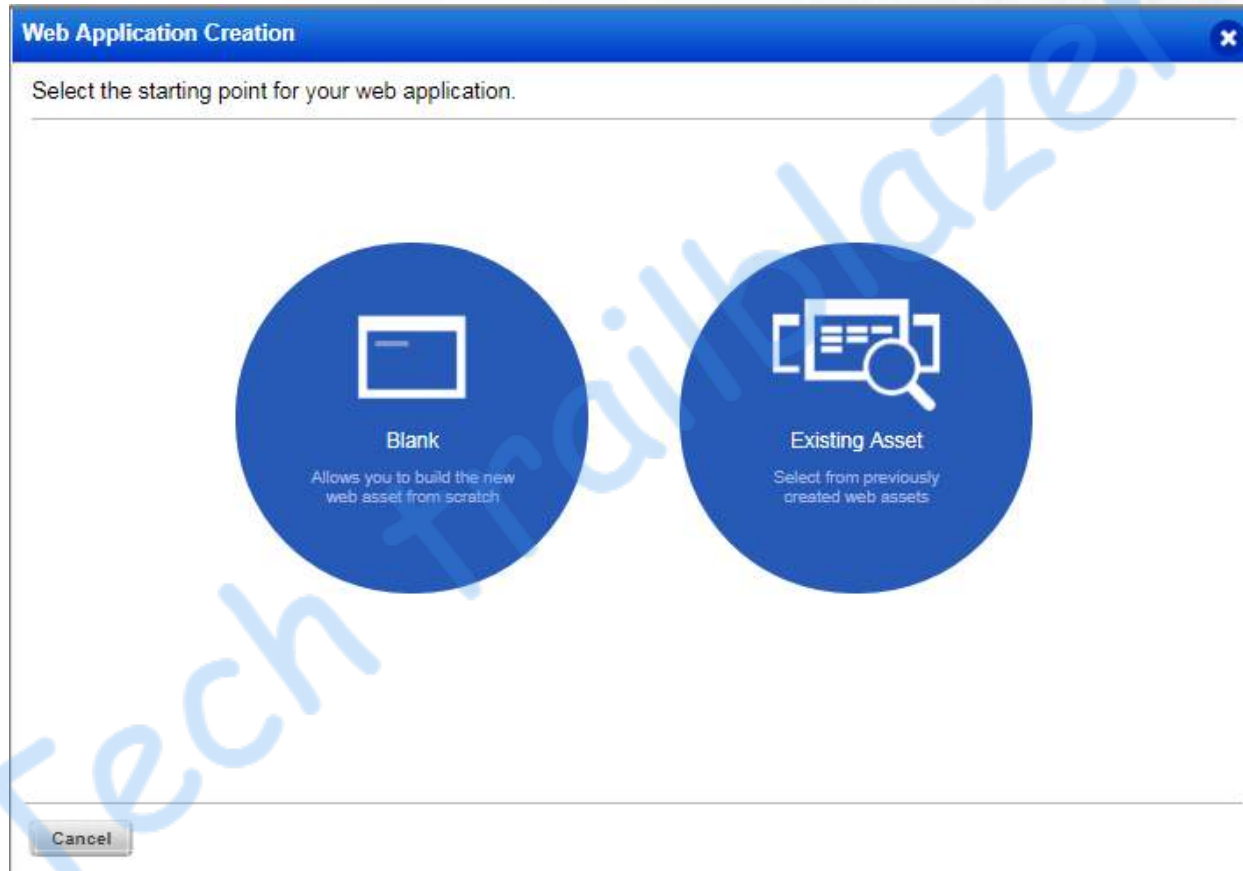
Tech trailblazer

QUALYS WEB APPLICATION SCANNING



DASHBOARD

QUALYS WEB APPLICATION SCANNING



CREATION – BLANK OR EXISTING ASSET

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 1 of 11

- Asset Details** ✓
- Application Details
- Scan Settings
- Crawl Settings
- Redundant Links
- Authentication
- Exclusions
- Advanced Options
- Malware Monitoring
- Comments
- Review And Confirm

Tell us about the asset you want to scan

Definition (*) REQUIRED FIELDS

Let's start with some basic information.

Name*

Target Definition

Web Application URL*

For scanning Swagger-based REST APIs, the Web Application URL should point to the Swagger file. It is your responsibility to verify that you have permission to scan all web applications that you specify as scan targets.

Custom Attributes

Provide attribute information that will help you categorize this web application within your subscription.

Name	Value

Add

Tags

Select tags to apply to the web application

Select | Create | Remove All

Cancel

Continue

ASSET DETAILS

QUALYS WEB APPLICATION SCANNING

Web Application Creation

Turn help

Step 2 of 11

- 1 Asset Details
- 2 Application Details
- 3 Scan Settings
- 4 Crawl Settings
- 5 Redundant Links
- 6 Authentication
- 7 Exclusions

Tell us about the web application you want to scan

Target Definition

Web Application URL

Crawl Scope*

Limit to content located at or below URL subdirectory

Limit at or below URL hostname (www.i' .com)

Limit to content located at or below URL subdirectory

Limit to URL hostname and specified sub-domain

Limit to URL hostname and specified domains

CRAWL SCOPE

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch help

Step 3 of 11

- 1 Asset Details ✓
- 2 Application Details ✓
- 3 Scan Settings ✓
- 4 Crawl Settings
- 5 Redundant Links
- 6 Authentication
- 7 Exclusions
- 8 Advanced Options
- 9 Malware Monitoring
- 10 Comments
- 11 Review And Confirm

Tell us the scan settings you'd like to use

Default Scan Options(*) REQUIRED FIELD

Choose the default scan settings for your web application. You can change the defaults for each scan.

Option Profile

WEB SCANNING PROFILE (Default) View Create

Scanner Appliance

Choose the default scanner appliance for your web application. You can change the defaults for each scan

☒ External ☐ Individual ☐ Tags (Scanner pool)

☒ Lock this scanner appliance for this web application.

Duration

Cancel the scan after N hours or at a certain time. By default the scan will run until it completes, or the maximum scan time is reached.

When selecting Cancel After, the scan will cancel after the time period set once it begins running and may not reflect the time the scan was submitted. This may be due to scan queues or scanner availability. To end scan at a precise time, please use the option Cancel At and select the desired time the scan should end regardless of queues, scanner availability or submittal/run time.

Cancel Option

Cancel Scan After 1 hour

Cancel

PreviousContinue

SCAN SETTINGS

QUALYS WEB APPLICATION SCANNING

Web Application CreationTurn help tips: On | Off Launch the

Step 9 of 11

- 1 Asset Details ✓
- 2 Application Details ✓
- 3 Scan Settings ✓
- 4 Crawl Settings ✓
- 5 Redundant Links ✓
- 6 Authentication ✓
- 7 Exclusions ✓
- 8 Advanced Options ✓
- 9 Malware Monitoring ✓**
- 10 Comments
- 11 Review And Confirm

Malware Monitoring

By enabling Malware Monitoring on this web application, you will allow QualysGuard to perform a regular scan for malware on your external web site. The application owner will receive an email notification when malicious software is detected. Note Malware Monitoring is available for external sites only.

Status

☒ Enable Malware Monitoring for this web application.

Recurrence

Mode*

Launch Information

Start Date

Time*

Time Zone*

Notification

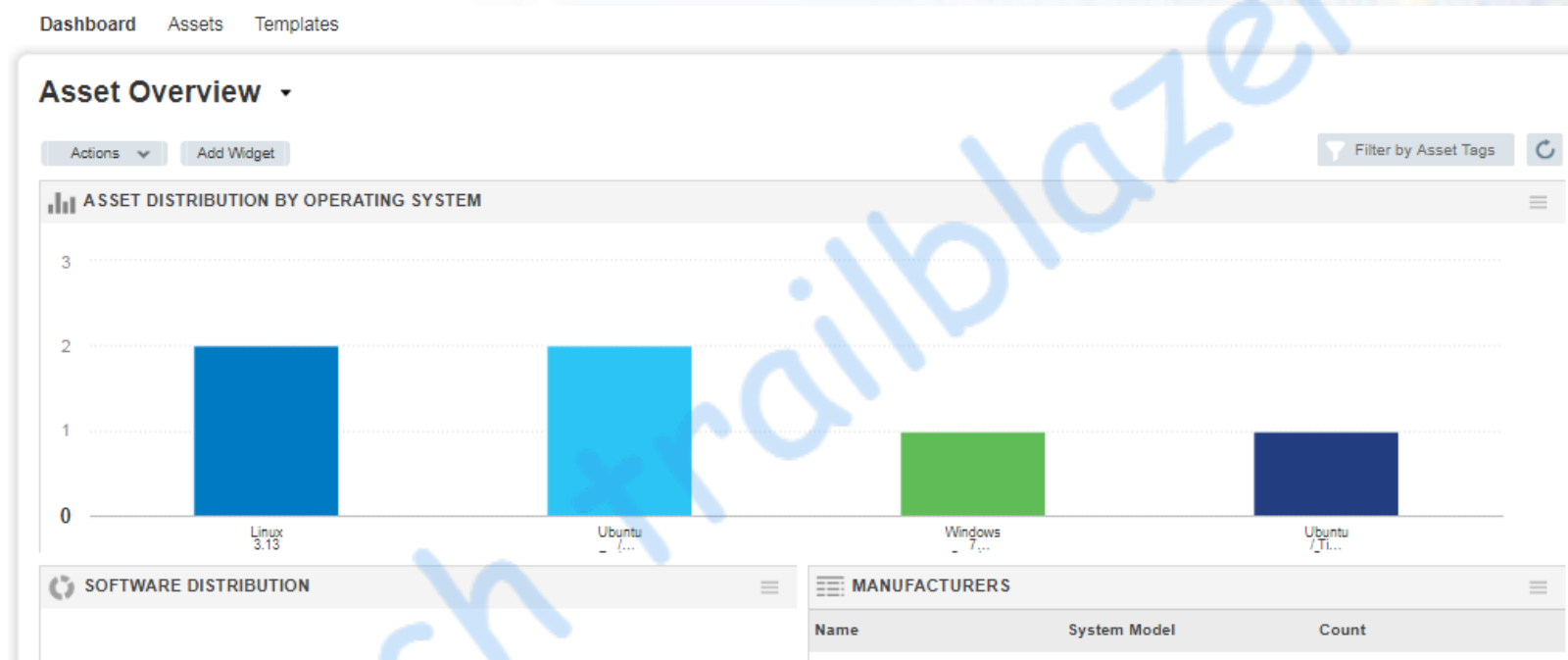
Choose to send notifications about malware scans to the web application owner.

MALWARE MONITORING

ASSET MANAGEMENT THROUGH QUALYS

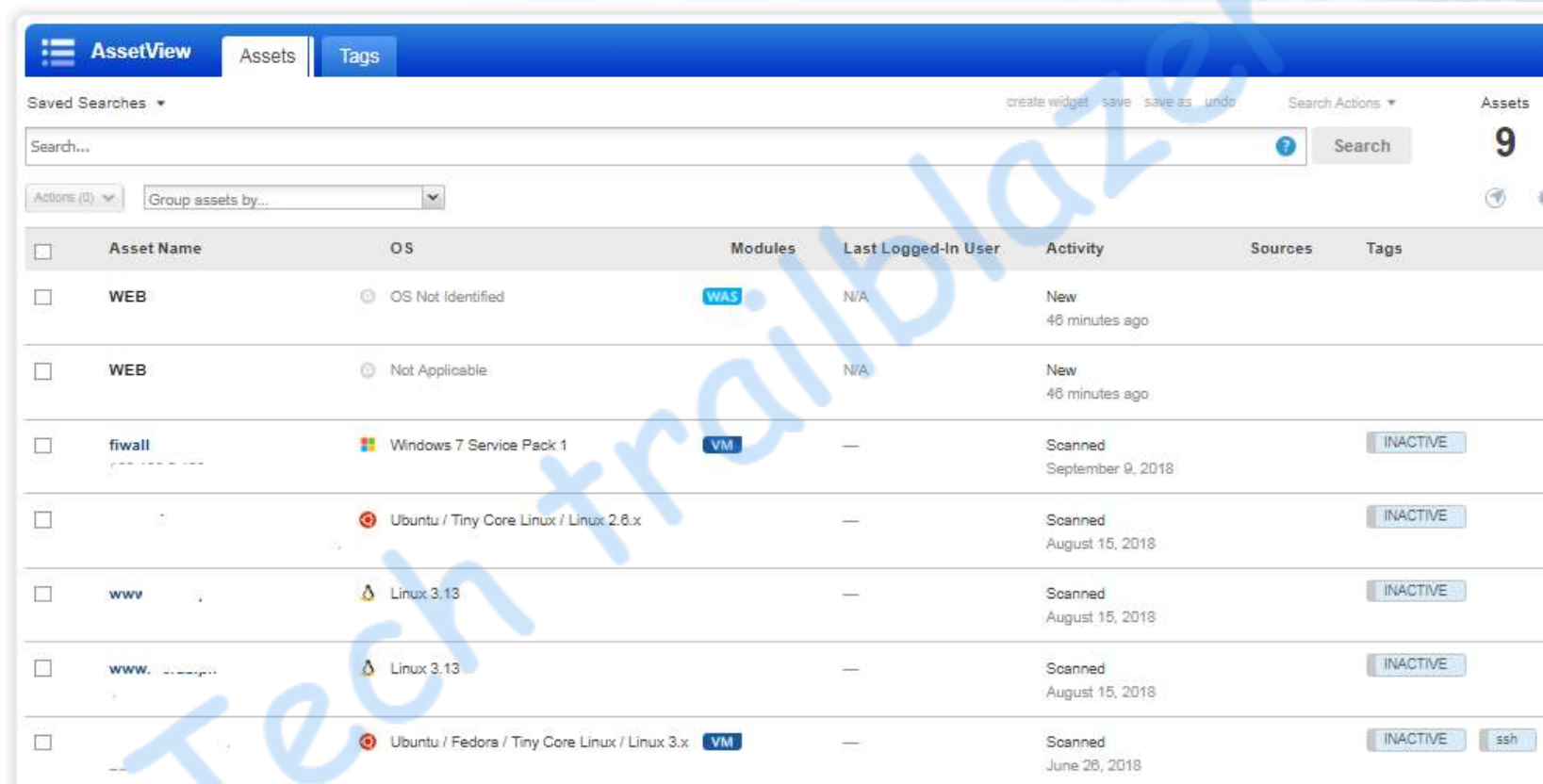
- Lets have a look at Qualys asset management capabilities

ASSET MANAGEMENT THROUGH QUALYS



QUALYS ASSET OVERVIEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



☐	Asset Name	OS	Modules	Last Logged-In User	Activity	Sources	Tags
☐	WEB	OS Not Identified	WAS	N/A	New 46 minutes ago		
☐	WEB	Not Applicable		N/A	New 46 minutes ago		
☐	firewall	Windows 7 Service Pack 1	VM	—	Scanned September 9, 2018		INACTIVE
☐		Ubuntu / Tiny Core Linux / Linux 2.6.x		—	Scanned August 15, 2018		INACTIVE
☐	www	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐	www	Linux 3.13		—	Scanned August 15, 2018		INACTIVE
☐		Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	VM	—	Scanned June 28, 2018		INACTIVE ssh

ASSETS LIST

ASSET MANAGEMENT THROUGH QUALYS

Add a new widget to your dashboard

Templates

Search

All22

Threat13

Assets5

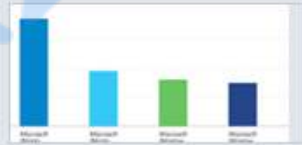
Shared0

Pick a preconfigured widget to add to your dashboard or [create a custom widget](#)

You can also create and customize your own widgets.

Assets with exploits available

A column chart displaying your assets which have an exploit available, broken down by operating system.



Assets with Qualys TOP-10 external vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 external vulns.

ASSETS WITH QUALYS TOP 10 EXTERNAL VULNERABILITIES
116

Assets with Qualys TOP-10 internal vulnerabilities

See how many assets contain vulnerabilities listed amongst Qualys TOP-10 internal vulns.

ASSETS WITH QUALYS TOP 10 INTERNAL VULNERABILITIES
69

Latest Threat Feeds

View the Latest Threats as provided by the Qualys threat intelligence feed. Get correlation data with your existing assets and measure the threat severity.

LATEST THREATS FROM LIVE FEED

Title	Impa...	Seve...	Publi...
Adobe Flash Player under ne...	101	HIGH	4/3/2018
Latest Adobe 0-day now in An...	101	HIGH	3/26/2018
Oracle patches 0-day in Java	118	HIGH	3/24/2018

Custom Count

ASSETS WITH HINDATFABLE

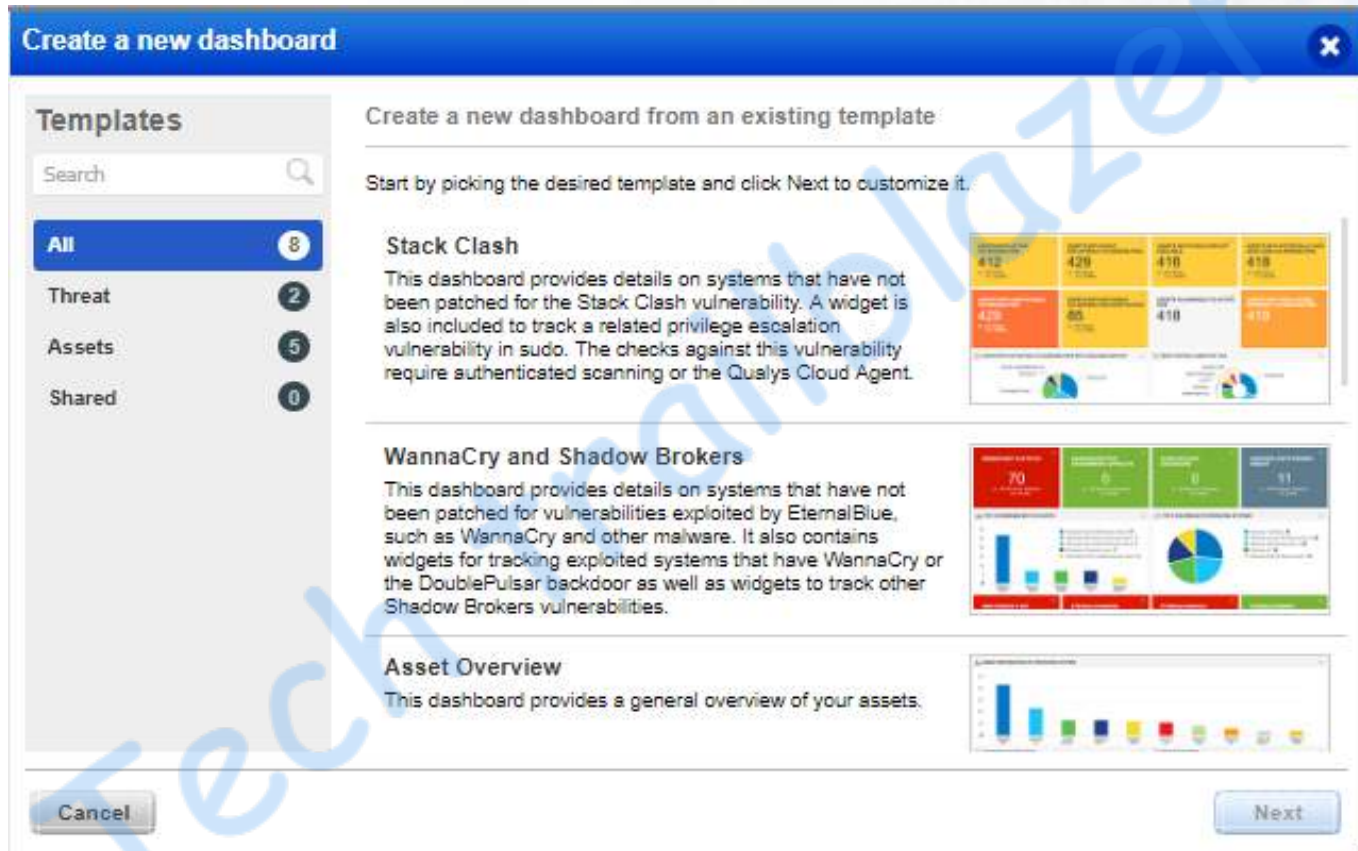
Cancel

Add to Dashboard

ADD NEW ASSET WIDGET TO DASHBOARD

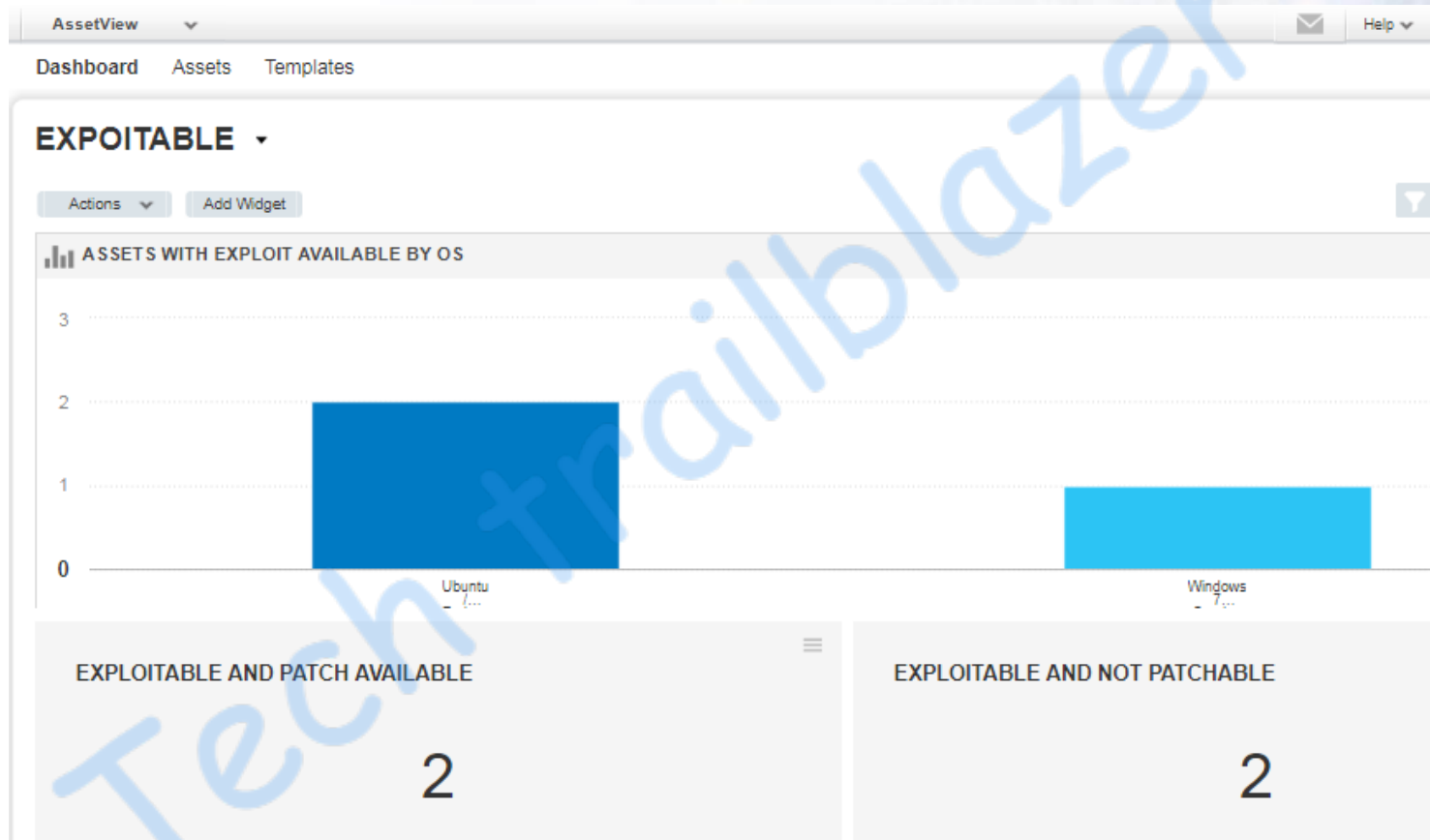
228

ASSET MANAGEMENT THROUGH QUALYS



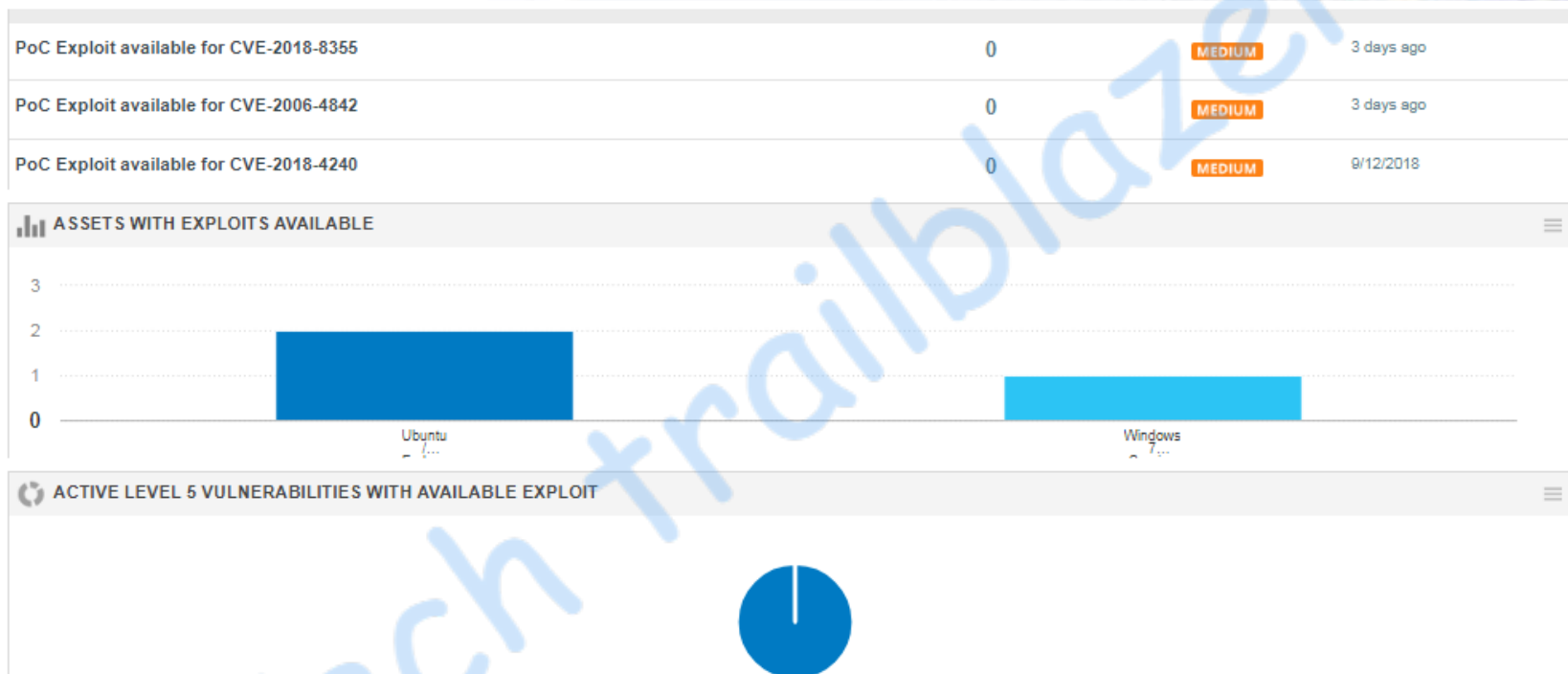
CREATE A NEW DASHBOARD

ASSET MANAGEMENT THROUGH QUALYS



NEW DASHBOARD CREATED

ASSET MANAGEMENT THROUGH QUALYS



ASSETS WITH EXPLOITS AVAILABLE

ASSET MANAGEMENT THROUGH QUALYS

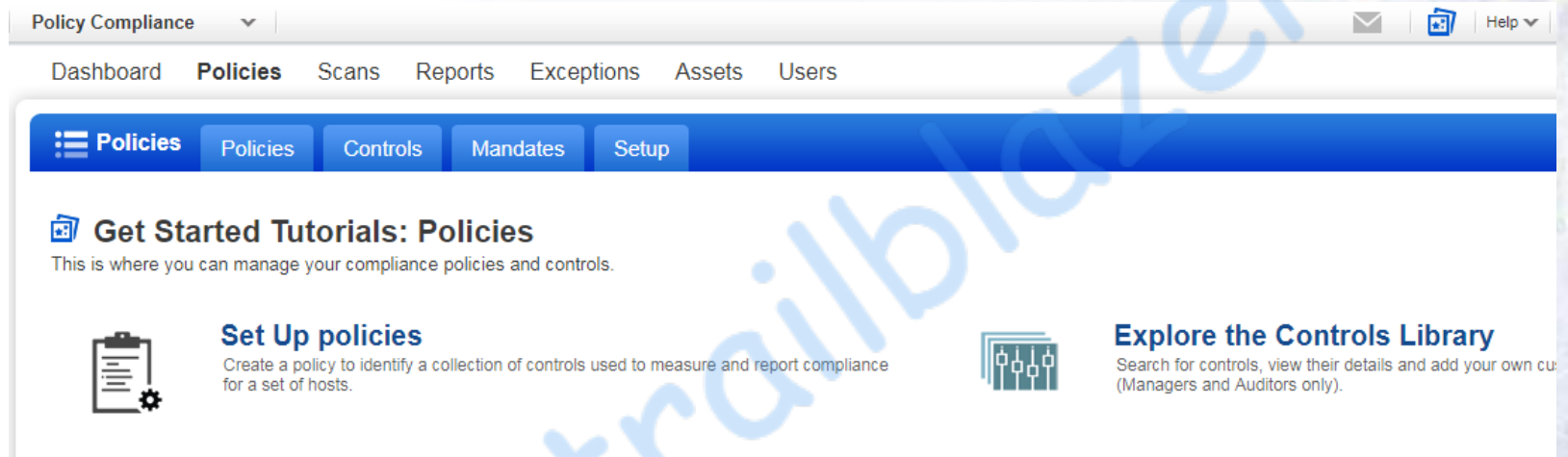
- Qualys allows various reporting and views on assets and their characteristics

END

QUALYS POLICY LIBRARIES

- Lets have a detailed look at Qualys built-in libraries for creating scanning policies
- CIS
- QUALYS
- MANDATE
- DISA
- VENDOR

QUALYS POLICY LIBRARIES



The screenshot displays the Qualys Policy Compliance web interface. At the top, there is a navigation bar with a 'Policy Compliance' dropdown menu, a mail icon, a help icon, and a 'Help' dropdown. Below this is a secondary navigation bar with links for 'Dashboard', 'Policies', 'Scans', 'Reports', 'Exceptions', 'Assets', and 'Users'. A third navigation bar features a 'Policies' icon and buttons for 'Policies', 'Controls', 'Mandates', and 'Setup'. The main content area is titled 'Get Started Tutorials: Policies' and includes the text 'This is where you can manage your compliance policies and controls.' Below this, there are two featured sections: 'Set Up policies' with a clipboard icon and a description 'Create a policy to identify a collection of controls used to measure and report compliance for a set of hosts.', and 'Explore the Controls Library' with a server rack icon and a description 'Search for controls, view their details and add your own controls (Managers and Auditors only)'.

Policy Compliance

Dashboard Policies Scans Reports Exceptions Assets Users

Policies Policies Controls Mandates Setup

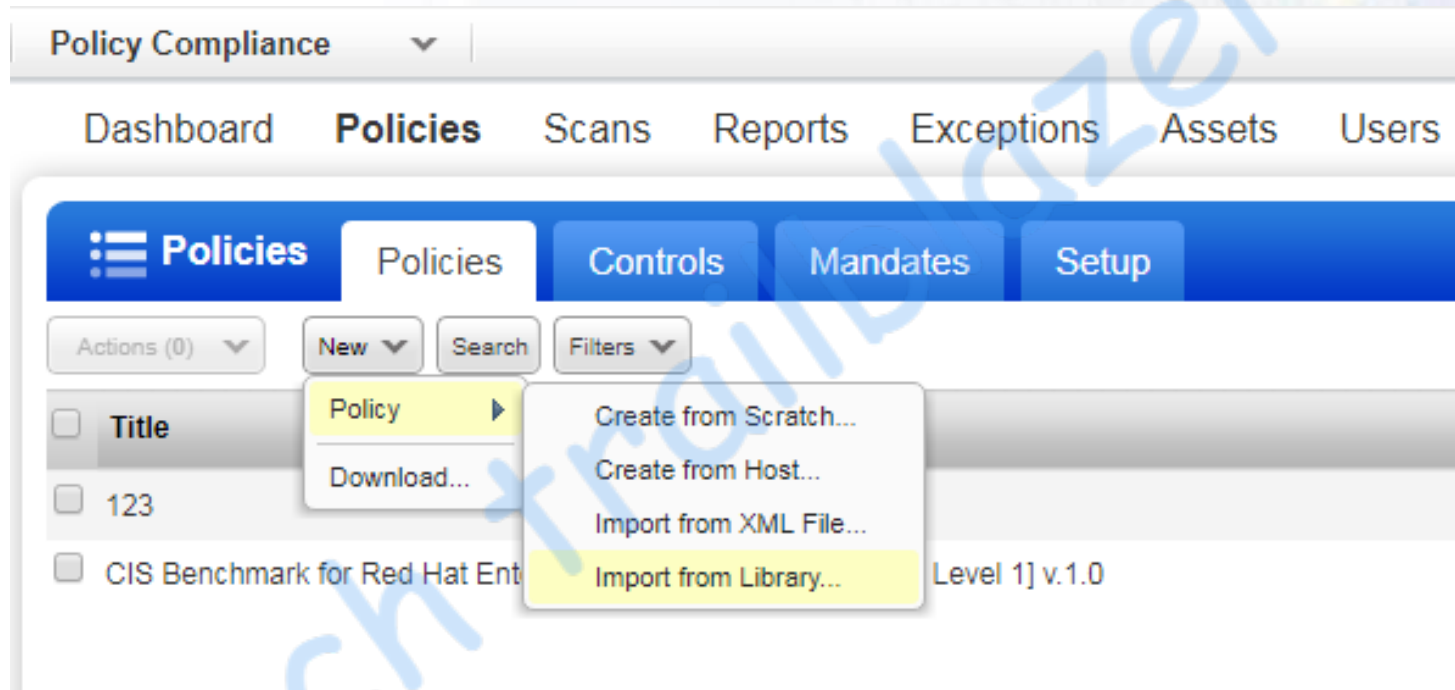
 **Get Started Tutorials: Policies**
This is where you can manage your compliance policies and controls.

 **Set Up policies**
Create a policy to identify a collection of controls used to measure and report compliance for a set of hosts.

 **Explore the Controls Library**
Search for controls, view their details and add your own controls (Managers and Auditors only).

EXPLORE THE CONTROLS LIBRARY

QUALYS POLICY LIBRARIES



CREATE NEW POLICY > IMPORT FROM LIBRARY

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor

Technologies

- ☐ AIX 6.x
- ☐ AIX 7.x
- ☐ Amazon Linux 2 AMI
- ☐ Amazon Linux AMI
- ☐ Apache HTTP Server 2.2.x
- ☐ Apache HTTP Server 2.4.x
- ☐ Apache Tomcat 6.x
- ☐ Apache Tomcat 7.x
- ☐ Apache Tomcat 8.x
- ☐ CentOS 6.x
- ☐ CentOS 7.x
- ☐ Checkpoint Firewall
- ☐ Cisco ASA 8.x
- ☐ Cisco ASA 9.x

Policies (260)

-  CIS Benchmark for SuSE Enterprise Linux Server 10.x v2.0 [Scored]
Version 2.0 02/10/2016 [View Description](#) | [View Policy](#) 
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]
Version 2.0 12/01/2017 [View Description](#) | [View Policy](#) 
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 and Level 2]
Version 2.0 12/01/2017 [View Description](#) | [View Policy](#) 
-  CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]

[Back](#)

Choose Source

[Next](#)

CREATE A NEW POLICY

QUALYS POLICY LIBRARIES

Labels

- All
- New
- Updated
- CIS**
- Qualys
- Mandate
- DISA STIG
- Vendor

Technologies

- ☐ MS IIS 7.x
- ☐ MS IIS 8.x
- ☐ MySQL 5.x
- ☐ Oracle 11g
- ☐ Oracle 12c
- ☐ Oracle Enterprise Linux 6.x
- ☐ Oracle Enterprise Linux 7.x
- ☐ PaloAlto Networks PAN-OS
- ☐ Red Hat Enterprise Linux 5.x
- ☐ Red Hat Enterprise Linux 6.x
- ☒ Red Hat Enterprise Linux 7.x
- ☐ Solaris 10.x
- ☐ Solaris 11.x

Policies (3)

-  CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#) 
-  CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#) 
-  CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 2]
Version 1.0 06/20/2018 [View Description](#) | [View Policy](#) 

CIS > RED HAT ENT. LINUX 7.X

QUALYS POLICY LIBRARIES

Policy Compliance

Dashboard **Policies** Scans Reports Exceptions Assets Users

Policies Policies Controls Mandates Setup

Actions (1) New Search Filters

☐	Title	
☒	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0	
☐	CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1] v.1.0	

CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

ID: 372295

Policy Title: CIS Benchmark for Red Hat Enterprise Linux 7, v2.2.0 [Scored, Level 1 and Level 2] v.1.0

Lock Status: Locked at Import

Active: Active

Evaluate Now: No

Created By: Nahil Mahmood (detat-nm1)

POLICIES DASHBOARD

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All
New
Updated
CIS
Qualys
Mandate
DISA STIG
Vendor

Technologies

- ☐ MS IIS 10.x
- ☐ MS IIS 7.x
- ☐ MS IIS 8.x
- ☐ Red Hat Enterprise Linux 5.x
- ☐ Red Hat Enterprise Linux 6.x
- ☐ Red Hat Enterprise Linux 7.x
- ☐ Windows 10
- ☐ Windows 2008 Active Directory
- ☐ Windows 2008 Server
- ☐ Windows 2012 R1/R2 Active Directory
- ☐ Windows 2012 Server
- ☐ Windows 2016 Active Directory

Policies (18)



DISA Security Technical Implementation Guide (STIG) for Internet Explorer 10, V1R15

Version 4.0 07/24/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows 8.1, V1R20

Version 1.0 08/02/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows Server 2008 (non-R2) DC, V6R39

Version 1.0 08/02/2018 [View Description](#) | [View Policy](#)



DISA Security Technical Implementation Guide (STIG) for Windows Server 2012 (non-R2)

[Back](#)

[Choose Source](#)

[Next](#)

DISA STIG

QUALYS POLICY LIBRARIES

Create a New Policy



Policy from Library: Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

All

New

Updated

CIS

Qualys

Mandate

DISA STIG

Vendor

Technologies

- ☐ Oracle Enterprise Linux 6.x
- ☐ Oracle Enterprise Linux 7.x
- ☐ Oracle WebLogic Server 11g
- ☐ Oracle WebLogic Server 12c
- ☐ Pivotal tc Server 3.x
- ☐ PostgreSQL 9.x
- ☐ Red Hat Enterprise Linux 6.x
- ☐ Red Hat Enterprise Linux 7.x
- ☒ SAP Adaptive Server Enterprise 16
- ☐ vFabric tc Server 2.9.x
- ☐ Windows 10
- ☐ Windows 2000
- ☐ Windows 2000 Active Directory

Policies (1)



Qualys - Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0

Version 2.0 07/24/2018 [Hide Description](#) | [View Policy](#)

This policy for 'Security Configuration and Compliance Policy for SAP Adaptive Server Enterprise 16.0' is based on the 'CIS benchmark for Sybase ASE 15.0, v.1.1.0'. The Policy contains Level 1 and Level 2 'Scored' types of checks from the benchmark. The controls within the policy are configured on the basis of values specified by CIS benchmark.

[Back](#)

Choose Source

[Next](#)

QUALYS SAP ADAPTIVE SERVER ENT 16

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor**

Technologies

- ☐ VMware ESX/ESXi 4.x
- ☐ VMware ESXi 5.x
- ☐ VMware ESXi 6.x
- ☐ Windows 10
- ☐ Windows 2008 Active Directory
- ☐ Windows 2008 Server
- ☐ Windows 2012 Server
- ☐ Windows 2016 Server
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012 R2

Policies (17)



VMWare vSphere Security Hardening Guide for ESXi 6.x

 Version 3.0 03/01/2018 [View Description](#) | [View Policy](#)

VMware



Microsoft Security Compliance Manager (SCM) Baseline for Windows Server 2012 R2 [Member Server]

 Version 2.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 8.1

 Version 3.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 10 version 1511

[Back](#)

Choose Source

[Next](#)

VENDOR POLICIES

QUALYS POLICY LIBRARIES

Create a New Policy

 **Policy from Library:** Choose from one of the policies in our library.

Find the policy that best suits your needs. Our Compliance Policy Library contains several sample policies based on popular compliance frameworks, including SOX, HIPAA, CoBIT and more. Click on one of the policies below, and then click Next to import it.

Labels

- All
- New
- Updated
- CIS
- Qualys
- Mandate
- DISA STIG
- Vendor**

Technologies

- ☐ VMware ESX/ESXi 4.x
- ☐ VMware ESXi 5.x
- ☐ VMware ESXi 6.x
- ☐ Windows 10
- ☐ Windows 2008 Active Directory
- ☐ Windows 2008 Server
- ☐ Windows 2012 Server
- ☐ Windows 2016 Server
- ☐ Windows 7
- ☐ Windows 8
- ☐ Windows 8.1
- ☐ Windows Server 2012 R2

Policies (17)



VMWare vSphere Security Hardening Guide for ESXi 6.x

 Version 3.0 03/01/2018 [View Description](#) | [View Policy](#)

VMware



Microsoft Security Compliance Manager (SCM) Baseline for Windows Server 2012 R2 [Member Server]

 Version 2.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 8.1

 Version 3.0 09/20/2016 [View Description](#) | [View Policy](#)





Microsoft Security Compliance Manager (SCM) Baseline for Windows 10 version 1511

[Back](#)

Choose Source

[Next](#)

VENDOR POLICIES

QUALYS POLICY LIBRARIES

- Qualys has a vast number of options for Compliance Scans, and these should be fully explored through the Qualys trial

END

A Look At CIS Security Benchmarks (1)

CIS stand for
mcqs

- Center for Internet Security (CIS)
 - <https://www.cisecurity.org/cis-benchmarks/>
 - Fill out your details and will receive an email with link

A Look At CIS Security Benchmarks (1)



CIS Benchmarks

You now have access to all of our CIS Benchmark PDFs. Feel free to download as many as you like!

If you have any issues accessing the files, please let us know at learn@cisecurity.org.

Looking for a previous version of a CIS Benchmark? See our [archive](#).

Operating Systems

Distribution Independent Linux 

CIS Distribution Independent Linux Benchmark v1.0.1

[Download PDF](#)

Microsoft Windows Desktop 

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

[Download PDF](#)

A Look At CIS Security Benchmarks (2)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

how many cis bench
msrk

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS	TOTAL
1	DISTRIBUTION INDEPENDENT LINUX	1
2	MICROSOFT WINDOWS DESKTOP	5
3	DEBIAN LINUX	2
4	UBUNTU LINUX	3
5	AMAZON LINUX	1
6	CENTOS LINUX	2
7	ORACLE LINUX	2

A Look At CIS Security Benchmarks (1)

#	OPERATING SYSTEMS (CONTD)...	TOTAL
8	REDHAT LINUX	3
9	SUSE LINUX	2
10	APPLE OS (UNIX)	5
11	IBM AIX (UNIX)	1
12	ORACLE SOLARIS (UNIX)	3
13	MS WINDOWS SERVER	6
	TOTAL BENCH MARKS OPERATING SYSTEMS	36

A Look At CIS Security Benchmarks (1)

Microsoft Windows Desktop

Microsoft Windows

CIS Microsoft Windows 10 Enterprise Release 1607 Benchmark v1.2.0

CIS Microsoft Windows 8.1 Workstation Benchmark v2.2.1

CIS Microsoft Windows 7 Workstation Benchmark v3.0.1

CIS Microsoft Windows XP Benchmark v3.1.0

CIS Microsoft Windows 8 Benchmark v1.0.0

A Look At CIS Security Benchmarks (1)

Microsoft Windows Server

Microsoft Windows

CIS Microsoft Windows Server 2016 RTM (Release 1607) Benchmark v1.0.0

CIS Microsoft Windows Server 2008 (non-R2) Benchmark v3.0.1

CIS Microsoft Windows Server 2008 R2 Benchmark v3.0.1

CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1

CIS Microsoft Windows Server 2012 (non-R2) Benchmark v2.0.1

CIS Microsoft Windows Server 2003 Benchmark v3.1.0

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE	TOTAL
1	MICROSOFT IIS (WEB SERVER)	3
2	VMWARE (VIRTUALIZATION)	2
3	MONGODB (DATABASE SERVER)	3
4	IBM DB2 (DATABASE SERVER)	3
5	BIND (DNS SERVER)	1
6	APACHE TOMCAT (WEB SERVER)	2
7	MICROSOFT SQL SERVER (DB SERVER)	3

A Look At CIS Security Benchmarks (1)

#	SERVER SOFTWARE (CONTD)...	TOTAL
8	APACHE (HTTP SERVER)	2
9	DOCKER (VIRTUALIZATION)	5
10	ORACLE (DATABASE SERVER)	3
11	KUBERNETES (VIRTUALIZATION)	1
12	MIT KERBEROS (AUTHENTICATION)	1
13	ORACLE MySQL (DB SERVER)	4
	TOTAL BENCH MARKS SERVER SOFTWARE	33

A Look At CIS Security Benchmarks (1)

Microsoft SQL Server Database Server

CIS Microsoft SQL Server 2008 R2 Benchmark v1.4.0

CIS Microsoft SQL Server 2012 Benchmark v1.3.0

CIS Microsoft SQL Server 2014 Benchmark v1.2.0

A Look At CIS Security Benchmarks (1)

#	CLOUD PROVIDERS	TOTAL
1	AMAZON WEB SERVICES	2
	TOTAL CLOUD PROVIDERS	2

A Look At CIS Security Benchmarks (1)

- Next module...remaining categories

END

A Look At CIS Security Benchmarks (2)

- Mobile devices, network devices, desktop software, multifunction print devices

A Look At CIS Security Benchmarks (2)

#	MOBILE DEVICES	TOTAL
1	APPLE IOS	5
2	GOOGLE ANDROID	3
	TOTAL BENCH MARKS MOBILE DEVICES	8

A Look At CIS Security Benchmarks (2)

#	NETWORK DEVICES	TOTAL
1	CISCO	4
2	PALO ALTO NETWORKS	2
	TOTAL BENCH MARKS NETWORK DEVICES	6

A Look At CIS Security Benchmarks (2)

#	DESKTOP SOFTWARE	TOTAL
1	MICROSOFT OFFICE	13
2	GOOGLE CHROME (WEB BROWSER)	1
3	MS EXCHANGE SERVER	3
4	MS INTERNET EXPLORER	2
5	MOZILLA FIREFOX	2
	TOTAL BENCH MARKS DESKTOP SOFTWARE	21

A Look At CIS Security Benchmarks (2)

#	MULTIFUNCTION PRINT DEVICES	TOTAL
1	MULTIFUNCTION DEVICE	1
	TOTAL BENCH MARKS MULTIFUNCTION PRINT DEVICES	1

A Look At CIS Security Benchmarks (2)

Apple iOS

CIS Apple iOS 10 Benchmark v2.0.0

CIS Apple iOS 9 Benchmark v1.0.0

CIS Apple iOS 8 Benchmark v1.0.0

CIS Apple iOS 7 Benchmark v1.1.0

CIS Apple iOS 6 Benchmark v1.0.0

A Look At CIS Security Benchmarks (2)

Google Android

CIS Google Android 7 Benchmark v1.0.0

CIS Google Android 4 Benchmark v1.0.0

CIS Google Android 2.3 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Cisco

CIS Cisco Firewall Benchmark v4.0.0

CIS Cisco IOS 12 Benchmark v4.0.0

CIS Cisco IOS 15 Benchmark v4.0.0

CIS Cisco Wireless LAN Controller 7 Benchmark v1.1.0

A Look At CIS Security Benchmarks (2)

Microsoft Office **Productivity Software**

CIS Microsoft Office 2016 Benchmark v1.1.0

CIS Microsoft Office PowerPoint 2016 Benchmark v1.0.1

CIS Microsoft Office PowerPoint 2013 Benchmark v1.0.1

CIS Microsoft Office Excel 2016 Benchmark v1.0.1

CIS Microsoft Office Excel 2013 Benchmark v1.0.1

CIS Microsoft Office Access 2016 Benchmark v1.0.1

CIS Microsoft Office Access 2013 Benchmark v1.0.1

A Look At CIS Security Benchmarks (2)

CIS Microsoft Office 2013 Benchmark v1.1.0

CIS Microsoft Office Word 2016 Benchmark v1.1.0

CIS Microsoft Office Word 2013 Benchmark v1.1.0

CIS Microsoft Office Outlook 2016 Benchmark v1.1.0

CIS Microsoft Office Outlook 2013 Benchmark v1.1.0

CIS Microsoft Outlook 2010 Benchmark v1.0.0

A Look At CIS Security Benchmarks (3)

- CIS Benchmarks
example (Network
Devices)

A Look At CIS Security Benchmarks (3)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

CIS Benchmarks

- The CIS Benchmarks are prescriptive **configuration recommendations** for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

CIS Benchmarks

CIS Benchmarks from the Center of Internet Security (CIS)

- a set of **globally recognized and consensus-driven** best practices to help security practitioners implement and manage their cybersecurity defenses.
- Developed with a **global community of security experts**, the guidelines help organizations **proactively safeguard against emerging risks**.
- Companies implement the CIS Benchmark **guidelines to limit configuration-based security vulnerabilities** in their digital assets.

CIS Benchmarks

When you implement CIS Benchmarks, you can better secure your legacy systems against common and emerging risks by taking steps such as these:

- Disabling unused ports
- Removing unnecessary app permissions
- Limiting administrative privileges

CIS levels

- **Level 1:** Basic easily implementable configurations designed to lower the attack surface without impacting performance.
- **Level 2:** Configuration recommendations that may create system conflicts and are intended to provide “defense in depth” for environments that need enhanced security

Domain Controller& Memeber Server

- A computer with a server OS and Active Directory installed is a Domain Controller.
- Any other computer with a server OS or for example with SQL Server installed, which works as a server and is joined to the domain can be called a member server. A member server does not have Active Directory installed.
- If a computer has DHCP or DNS, but not Active Directory, it's a member server.

Scored and Unscored

- Each recommendation is either 'scored' or 'not scored'.
- **'Scored'** recommendations are **mandatory** to achieve CIS compliance, and if not met, they lower the total benchmark score.
- Recommendations that are **'not scored'** have **no impact** on the overall score of the benchmark.

CIS Benchmarks List

The CIS Benchmarks are prescriptive configuration recommendations for more than 25+ vendor product families. They represent the consensus-based effort of cybersecurity experts globally to help you protect your systems against threats more confidently.

[ACCESS ALL BENCHMARKS →](#)

Are you new to the CIS Benchmarks? [Learn More](#)

Find the CIS Benchmark you're looking for



STEP 3

Download your CIS Benchmark.

Download the latest version or learn what other resources are available for this CIS Benchmark.

1 2 3 4

CLOUD PROVIDERS DESKTOP SOFTWARE DEVSECOPS TOOLS MOBILE DEVICES MULTI FUNCTION PRINT DEVICES NETWORK DEVICES OPERATING SYSTEMS SERVER SOFTWARE

Alibaba Cloud

[DOWNLOAD THE BENCHMARK →](#)

<https://www.cisecurity.org/cis-benchmarks>

CIS Critical Security Controls

- Formerly the SANS Critical Security Controls (**SANS Top 20**) these are now officially called the **CIS Critical Security Controls** (CIS Controls).
- CIS Top 20 Critical Security Controls are a **prioritized set of cybersecurity best practices** that can help **protect enterprises** from the **most pervasive and dangerous attacks**.
- <https://www.cisecurity.org/controls>

- The CIS Critical Security Controls (CIS Controls) are a **prescriptive, prioritized, and simplified set of best practices** that you can use to strengthen your cybersecurity posture.
- Thousands of cybersecurity practitioners from around the world use the CIS Controls and/or contribute to their development via a community consensus process.

CIS-CAT

- CIS-CAT Pro Assessor **evaluates the cybersecurity posture** of a system **against recommended policy settings**. The tool helps organizations save time and resources by employing automated content with policy setting recommendations based on 100+ globally recognized CIS Benchmarks.
- The CIS Controls Self Assessment Tool (CSAT) is a companion tool that helps IT security teams **track their implementation of every CIS Control** and Sub-Control
- <https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls>

There are two versions of CIS CSAT.

- The **CIS-hosted CSAT** is free to every organization for use in a non-commercial capacity.
- **CIS CSAT Pro** is an on-premises version that offers additional features and benefits and is only available to CIS SecureSuite Members.

A Look At CIS Security Benchmarks (4)

- CIS Benchmarks
example (Operating
Systems)
 - MS Windows Server
2012-R2

A Look At CIS Security Benchmarks (4)

#	OVERALL CIS BENCHMARK CATEGORIES	TOTAL
1	OPERATING SYSTEMS	36
2	SERVER SOFTWARE	33
3	CLOUD PROVIDERS	2
4	MOBILE DEVICES	8
5	NETWORK DEVICES	6
6	DESKTOP SOFTWARE	21
7	MULTIFUNCTION PRINT DEVICES	1
	GRAND TOTAL CIS BENCHMARKS	107

A Look At CIS Security Benchmarks (4)

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.2.1 - 01-31-2017

- January 31, 2017
- 760 pages PDF doc

A Look At CIS Security Benchmarks (4)

- Profile applicability:
 - Level 1 domain controller
 - Level 1 member server
 - **Level 2 domain controller**
 - **Level 2 member server**

A Look At CIS Security Benchmarks (4)

- Level 1: Items in this profile intend to:
 - be practical and prudent;
 - provide a clear security benefit; and
 - not inhibit the utility of the technology beyond acceptable means

A Look At CIS Security Benchmarks (4)

- Level 2: extends the Level 1 - profile
 - intended for environments or use cases where security is paramount
 - acts as defense in depth measure
 - may negatively inhibit the utility or performance of the technology

A Look At CIS Security Benchmarks (4)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - **Impact**
 - Default value
 - References

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1]: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)
 - Profile applicability:
Level 1 Domain Controller, Level 1 Member Server

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Description:
 - This policy setting defines how long a user can use their password before it expires.
 - Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire.

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Audit:
 - Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

A Look At CIS Security Benchmarks (4)

Remediation:

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
```

A Look At CIS Security Benchmarks (4)

- 1.1.2 [L1] Default Value: 42 days
- 1.1.2 [L1] Reference: CCE-37167-4
 - Common Configuration Enumeration (Unique identifiers for common system config issues)

END

A Look At CIS Security Benchmarks (3)

CIS Cisco Firewall Benchmark

v4.0.0 - 06-29-2016

- June 29, 2016
- 174 pages PDF doc

A Look At CIS Security Benchmarks (3)

- Control content:
 - Profile applicability (ASA 8.X, ASA 9.X)
 - Description
 - Rationale
 - Audit
 - Remediation
 - Default value
 - References

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Profile applicability: Level 1, Cisco ASA9.X
 - Description: Sets the idle timeout for a console session before the security appliance terminates it.

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Rationale: Limiting session timeout prevents unauthorized users from using abandoned sessions to perform malicious activities.

A Look At CIS Security Benchmarks (3)

Audit:

- Step 1: Run the following command to show what the console timeout is set to

```
hostname#sh run console | in timeout.5
```

The output should look like

```
console timeout 5
```

Example:

```
Asa-fw#sh run console | in timeout.5  
console timeout 5
```

Here the session timeout is 5 minutes

- Step 2: If an output is displayed, the system is compliant. If not, there is a finding.

A Look At CIS Security Benchmarks (3)

Remediation:

- Step 1: Run the following command to set the console timeout to less than or equal to 5 minutes

```
hostname(config)# console timeout 5
```

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Default Value: The default timeout is 0, which means the console session will not time out

A Look At CIS Security Benchmarks (3)

- 1.8 (page 88); Session Timeout
 - Reference: CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.1
 - **Here video 6 slides was not in the download file.**

A Look At DISA STIGs (1)

- Defense Information Systems Agency (DISA) provides technical guides referred to as Security Technical Implementation Guides (STIGs).

A Look At DISA STIGs (1)

why use stigs
mcqs

- USA DoD
- Security Technical Implementation Guides (STIGs)
- Most expansive security benchmarks available
- Most regularly updated
- 425 STIGs available

A Look At DISA STIGs (1)

- **STIGs master list (A-Z):**
 - <https://public.cyber.mil/stigs/downloads/>
 - **STIG viewer:**
 - <https://public.cyber.mil/stigs/srg-stig-tools/>

A Look At DISA STIGs (1)

STIGs HOME

The screenshot displays the DISA STIGs HOME website. The top navigation bar includes the DoD CYBER EXCHANGE PUBLIC logo and links for Topics, Training, PKI/PKE, SRGs/STIGs, Resources, and Help. A left sidebar lists various resources under the heading 'SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)', including SRG/STIGs Home, Automation, Control Correlation Identifier (CCI), Document Library, DoD Annex for NIAP Protection Profiles, DoD Cloud Computing Security, Frequently Asked Questions - FAQs, Group Policy Objects, Quarterly Release Schedule and Summary, SRG / STIG Library Compilations, SRG / STIG Mailing List, and SRG/STIG Tools and Viewing Guidance. The main content area features a 'STIGs' section with a shield icon and a 'CRITICAL UPDATES' section. The 'CRITICAL UPDATES' section contains three paragraphs of text regarding system updates, feedback, and contact information. Below this, a 'STIG UPDATES' section lists four recent releases: DISA releases the Red Hat Ansible Automation Controller Security Technical Implementation Guide, Request for comments - DISA releases draft Kubernetes STIG SCAP benchmark for review, DISA releases the VMware vSphere 7.0 Security Technical Implementation Guide, and The SCC Development Team is pleased to announce the release of SCC 5.7.1.

DoD CYBER EXCHANGE PUBLIC

Topics Training PKI/PKE SRGs/STIGs Resources Help

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)

- SRG/STIGs Home
- Automation
- Control Correlation Identifier (CCI)
- Document Library
- DoD Annex for NIAP Protection Profiles
- DoD Cloud Computing Security
- Frequently Asked Questions - FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance

STIGs

CRITICAL UPDATES

To provide increased flexibility for the future, DISA has updated the systems that produce STIGs and SRGs. This has resulted in a modification to Group and Rule IDs (Vul and Subvul IDs).

Test STIGs and test benchmarks were published from March through October 2020 to invite feedback. New and updated STIGs are now being published with the modified content.

New releases of STIGs published prior to this change will include the "legacy" Group and Rule IDs as XCCDF ident elements.

For all questions related to STIG content, please contact the DISASTIG Customer Support Desk at disastig_spt@mail.mil.

STIG UPDATES

- DISA releases the Red Hat Ansible Automation Controller Security Technical Implementation Guide
- Request for comments - DISA releases draft Kubernetes STIG SCAP benchmark for review
- DISA releases the VMware vSphere 7.0 Security Technical Implementation Guide
- The SCC Development Team is pleased to announce the release of SCC 5.7.1.

<https://public.cyber.mil/stigs/>

A Look At DISA STIGs (1)

STIGs Master List

DoD CYBER EXCHANGE PUBLIC

Topics Training PKI/PKE SRGs/STIGs Resources Help

Log in with CAC

[STIGS]

- SRG/STIGs Home
- Automation
- Control Correlation Identifier (CCI)
- Document Library
- DoD Annex for NIAP Protection Profiles
- DoD Cloud Computing Security
- Frequently Asked Questions - FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance
- Sunset Products
- Vendor STIG Development Process
- Help

Show 10 entries Search:

	TITLE	SIZE	UPDATED
	2016-04-21 DoD CIO Memo - Use of Wearable Devices DoD Accredited Spaces with FAQ	541.89 KB	30 Nov 2018
	A10 Networks ADC ALG - Ver 2, Rel 1	523.3 KB	27 Apr 2021
	A10 Networks Application Delivery Controller (ADC) NDM STIG Ver 1	269.56 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) Overview, Ver 1	86.24 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) STIG Ver 1 Release Memo	70.89 KB	30 Nov 2018
	AAA SRG - Ver 1, Rel 2	665.83 KB	16 Jan 2020
	Active Directory Domain STIG - Ver 3, Rel 2	668.75 KB	09 Nov 2022
	Active Directory Forest STIG - Ver 2, Rel B	433.92 KB	30 Nov 2018
	Adobe Acrobat Pro DC STIGs - Release Memo	707.86 KB	30 Nov 2018
	Adobe Acrobat Professional DC Continuous Track STIG - Ver 2, Rel 1	1.33 MB	26 Jul 2021

Showing 1 to 10 of 549 entries

Previous 1 2 3 4 5 ... 55 Next

STIG TOPICS

- ☐ Application Security (187) [-]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SRGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [-]
- ☐ Mobility (26) [-]
- ☐ Network/Perimeter/Wireless (96) [-]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (52) [-]
- ☐ Security Content Application Protocols (SCAP) (52) [-]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (11)
- ☐ Sunset (132) [-]
- ☐ Supplemental Automation Content (19) [-]
- ☐ Vendor Process (2)

<https://public.cyber.mil/stigs/downloads/>

A Look At DISA STIGs (1)

STIGs Viewer



Topics Training PKI/PKE SRGs/STIGs Resources Help

(STIGs)

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions - FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

STIG Viewing Tools

XCCDF formatted SRGs and STIGs are intended be ingested into an SCAP validated tool for use in validating compliance of a Target of Evaluation (TOE). As such, getting to the content of a XCCDF formatted STIG to read and understand the content is not as easy as opening a doc or pdf file and reading it. The process can be a little confusing and trying. Below are tools which can be used to view the STIGs and a Whitepaper describing the STIG Viewing processes.

DISA has produced standalone versions of STIG Viewer for the Windows and Linux platforms on 64-bit x86 processors. With the end of free support for Java 8 in early 2019, Oracle Corporation changed the licensing and distribution model for Java software. Users without supported Java 8 SE environments should use the standalone versions of STIG Viewer. Users with supported Java 8 SE environments may still use the current JAR file. DISA will base future STIG Viewer development on open-source software developed by the OpenJDK and OpenJFX projects.

Show 10 entries

Search:

TITLE	SIZE	UPDATED
 How to Create and SRG-STIG ID Mapping Spreadsheet	298.21 KB	03 Feb 2021
 STIG Sorted by STIG ID	103.46 KB	30 Mar 2015
 STIG Sorted by Vulnerability ID	101.59 KB	30 Mar 2015
 STIG Viewer 2.17	1.14 MB	21 Sep 2022
 STIG Viewer 2.17 Hashes	1.36 KB	21 Sep 2022
 STIG Viewer 2.17-Linux	73.38 MB	21 Sep 2022
 STIG Viewer 2.17-Win64	54.03 MB	21 Sep 2022
 STIG Viewer 2.17-Win64.msi	54.26 MB	21 Sep 2022

<https://public.cyber.mil/stigs/srg-stig-tools/>

A Look At DISA STIGs (1)

STIG Viewer Download



Topics Training PKI/PKE SRGs/STIGs Resources Help

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions - FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG/STIG Library Compilations

SRG/STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

STIG Viewing Tools

XCEDF formatted SRGs and STIGs are intended to be ingested into an SCAP validated tool for use in validating compliance of a Target of Evaluation (TOE). As such, getting to the content of a XCEDF formatted STIG to read and understand the content is not as easy as opening a .doc or .pdf file and reading it. The process can be a little confusing and trying. Below are tools which can be used to view the STIGs and a Whitepaper describing the STIG Viewing processes.

DISA has produced standalone versions of STIG Viewer for the Windows and Linux platforms on 64-bit x86 processors. With the end of free support for Java 8 in early 2019, Oracle Corporation changed the licensing and distribution model for Java software. Users without supported Java 8 SE environments should use the standalone versions of STIG Viewer. Users with supported Java 8 SE environments may still use the current JAR file. DISA will base future STIG Viewer development on open-source software developed by the OpenJDK and OpenJFX projects.

Show 10 entries

Search:

TITLE	SIZE	UPDATED
 How to Create and SRG-STIG ID Mapping Spreadsheet	298.21 KB	03 Feb 2021
 STIG Sorted by STIG ID	103.46 KB	30 Mar 2015
 STIG Sorted by Vulnerability ID	101.59 KB	30 Mar 2015
 STIG Viewer 2.17	1.14 MB	21 Sep 2022
 STIG Viewer 2.17 Hashes	1.36 KB	21 Sep 2022
 STIG Viewer 2.17-Linux	73.38 MB	21 Sep 2022
 STIG Viewer 2.17-Win64	54.03 MB	21 Sep 2022
 STIG Viewer 2.17-Win64.msi	54.26 MB	21 Sep 2022
 STIG Viewer User Guide (Sep 2022)	1.77 MB	21 Sep 2022

A Look At DISA STIGs (1)

STIG Library Compilation



Topics Training PKI/PKE SRGs/STIGs Resources Help

(STIGs)

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions - FAQs

Group Policy Objects

Quarterly Release Schedule and Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

The SRG-STIG Library Compilation .zip files are compilations of DoD Security Requirements Guides (SRGs) and DoD Security Technical Implementation Guides (STIGs), as well as some other content that may be available through the Cyber Exchange web site's STIG pages. Specifically excluded are Security Readiness Review (SRR) Tools (scripts and OVAL Benchmarks), Group policy objects, and draft SRGs and STIGs.

The Library Compilation .zip files will be updated and released during each SRG-STIG Update Release Cycle to capture all newly updated or released SRGs, STIGs, and Tools. New SRG-STIG content released mid cycle will be individually downloadable from IASE as released. These SRGs-STIGs will appear in the subsequent release of the Library Compilation.

See **SRG-STIG Library Compilation READ ME** for more information to include download / extraction instructions and a FAQ.

NOTE: While every attempt will be made to provide a complete set of **currently in force** SRGs, STIGs, and related tools, DISA makes no guarantee as to the completeness of the compilation or the **currently in force** status of the contents.

NOTE: While every attempt will be made to publish updated compilation files on the SRG-STIG Quarterly Update Release date, publication may lag due to competing workloads. Updated Compilation files will be published on or as soon as possible the published date. We apologize for any inconvenience this may impose.

Concerns or questions related to the contents or format of these compilation files should be directed to the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil

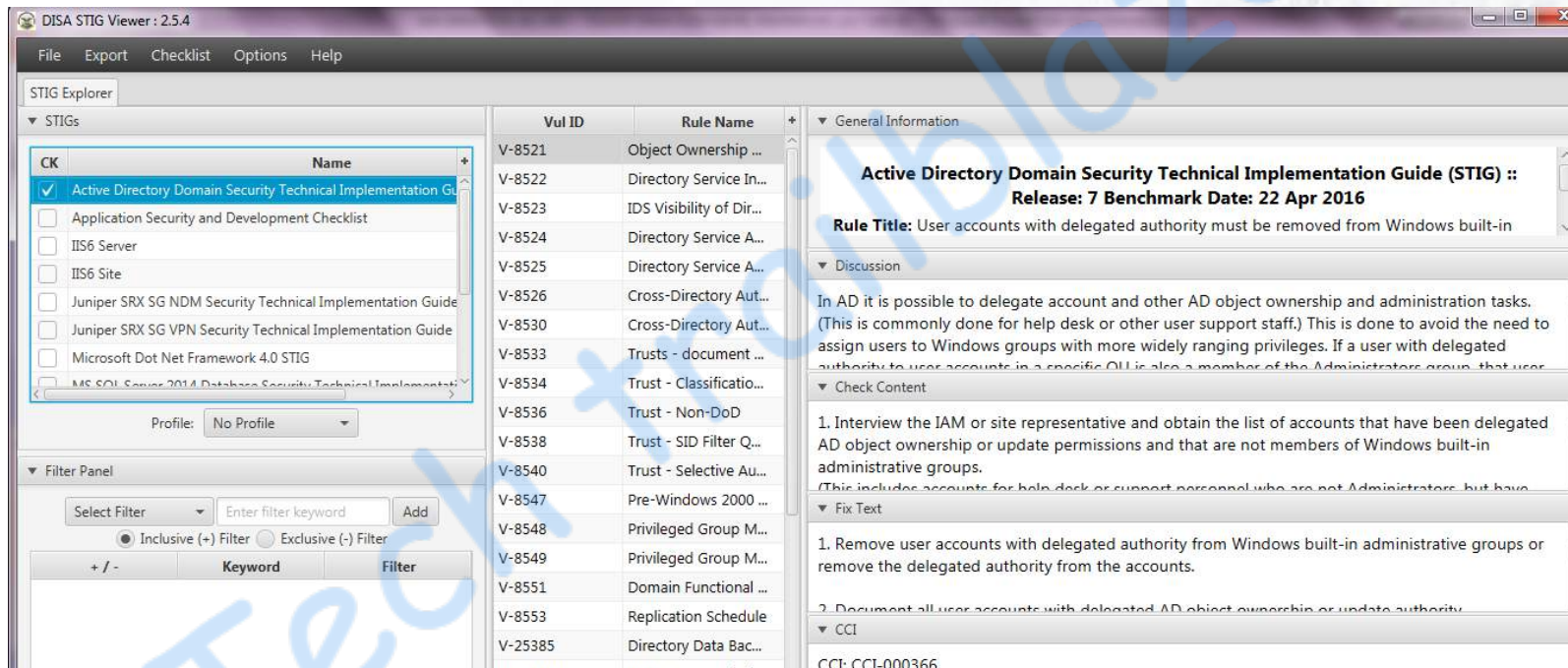
SRG/STIG Compilations

TITLE	SIZE	UPDATED
 Compilation - SRG-STIG Library	260.47 MB	24 Jan 2023
 Compilation - SRG-STIG Library - READ ME	122.17 KB	19 Jun 2019

- There are three categories of severity, ranked on level of risk or vulnerability.
- These are known as Severity Category Codes (CAT), with CAT 1, CAT 2 and CAT 3 levels of risk.
- CAT 1 controls cover the most severe vulnerabilities and risks.
- CAT I weaknesses should receive the highest priority for correction or mitigation.

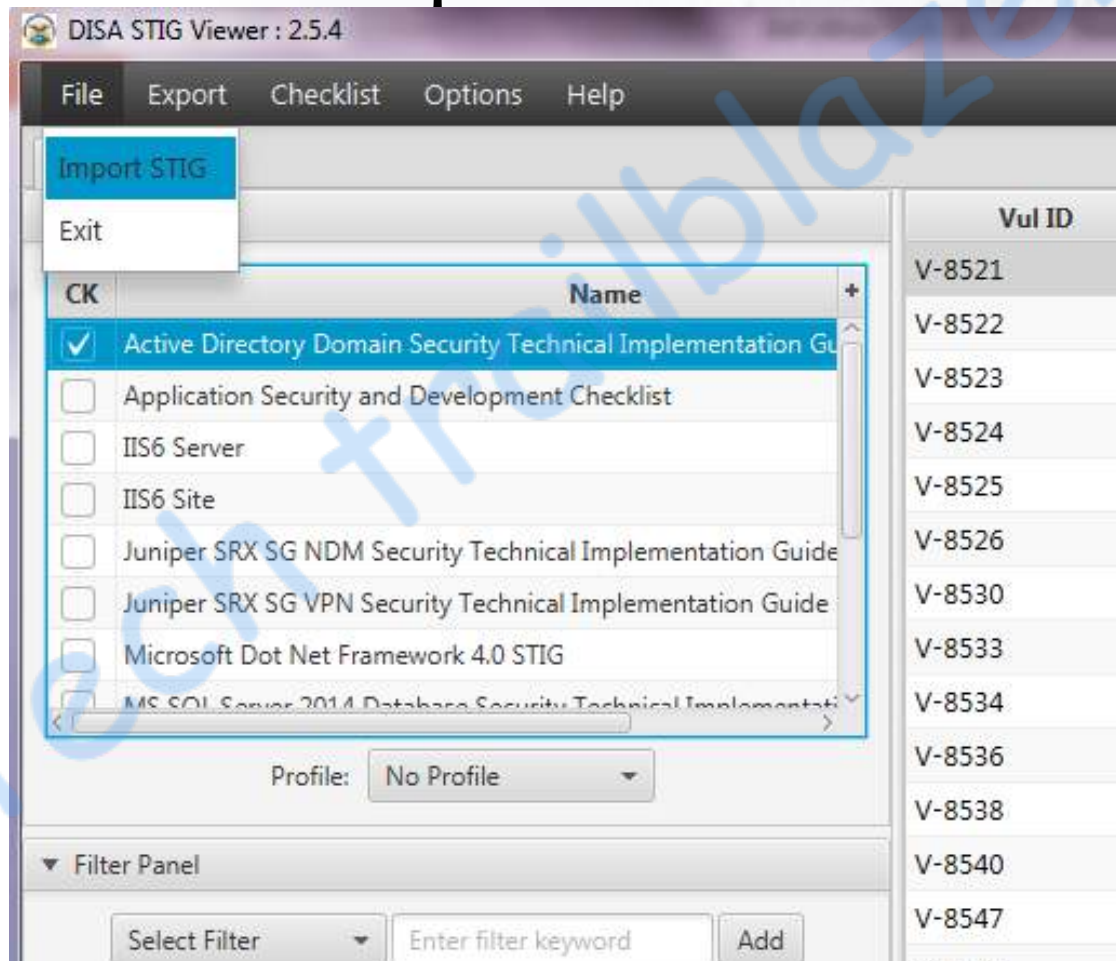
A Look At DISA STIGs (1)

STIG Viewer Window



A Look At DISA STIGs (1)

Import STIG



[HOME](#)[STIGS](#)[DOD 8500](#)[NIST 800-53](#)[COMMON CONTROLS HUB](#)[ABOUT](#)[Microsoft Windows 11](#)[Microsoft Windows 2008 Server Domain Name System](#)[Microsoft Windows 2012 Server Domain Name System](#)[Microsoft Windows Defender Antivirus](#)[Microsoft Windows Firewall with Advanced Security](#)[Microsoft Windows RAW](#)[Microsoft Windows Phone 8.1](#)[Microsoft Windows Server 2012 Domain Controller](#)[Microsoft Windows Server 2012 Member Server](#)[Microsoft Windows Server 2012/2012 R2 Domain Controller](#)[Microsoft Windows Server 2012/2012 R2 Member Server](#)[Microsoft Windows Server 2016](#)[Microsoft Windows Server 2019](#)[Microsoft Windows Server 2022](#)[Microsoft Word 2003](#)[Microsoft Word 2007](#)[Microsoft Word 2010](#)

<https://www.stigviewer.com/stigs>

[HOME](#)[STIGS](#)[DOD 8500](#)[NIST 800-53](#)[COMMON CONTROLS HUB](#)[ABOUT](#)

Microsoft Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide

Overview

Version	Date	Finding Count (330)			Downloads		
3	2022-09-06	CAT I (High): 33	CAT II (Med): 238	CAT III (Low): 59	Excel	JSON	XML

STIG Description

This Security Technical Implementation Guide is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements are derived from the National Institute of Standards and Technology (NIST) 800-53 and related documents. Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil.

Available Profiles

Findings (MAC III - Administrative Sensitive)

Finding ID	Severity	Title	Description
V-225447	High	Anonymous access to the registry must be restricted.	The registry is integral to the function, security, and stability of the Windows system. Some processes may require anonymous access to the registry. This must be limited to properly protect the system.
V-225244	High	Administrative accounts must not be used with applications that access the Internet, such as web browsers, or with potential Internet sources, such as email.	Using applications that access the Internet or have potential Internet sources using administrative privileges exposes a system to compromise. If a flaw in an application is exploited while...
V-225258	High	The Windows 2012 / 2012 R2 system must use an anti-virus program.	Malicious software can establish a base on individual desktops and servers. Employing an automated mechanism to detect this type of software will aid in elimination of the software from the...
V-225547	High	The Act as part of the operating system user right must not be assigned to any groups or accounts.	Inappropriate granting of user rights can provide system, administrative, and other high-level capabilities. Accounts with the "Act as part of the operating system" user right can assume the...
V-225438	High	File Transfer Protocol (FTP) servers must be configured to prevent access to the system drive.	The FTP service allows remote users to access shared files and directories. Access outside of the specific directories of shared data could provide access to system resources and compromise the system.
V-225449	High	Local accounts with blank passwords must be restricted to prevent access from the network.	An account without a password can allow unauthorized access to a system as well as the resources would be exposed. Password policies should protect...

A Look At DISA STIGs (1)

- Completely different mechanism for DISA STIGs

END

A Look At DISA STIGs (2)

- STIG content:
 - General information (title)
 - Discussion
 - Check content
 - Fix text
 - CCI (References)

A Look At DISA STIGs (2)

SEVERITY	DISA CATEGORY CODE GUIDELINES
CAT 1	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT 2	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT 3	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity

A Look At DISA STIGs (2)

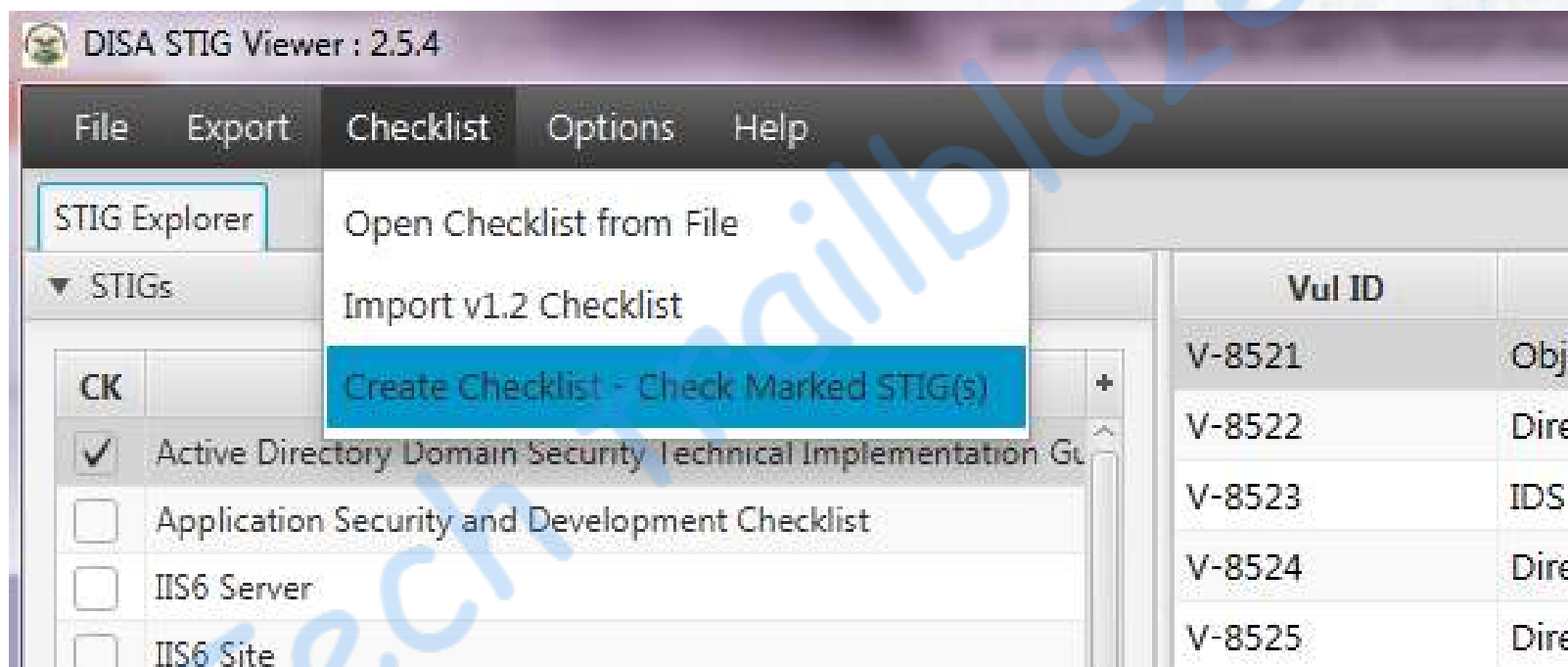
FILTER PANEL

The screenshot shows a 'Filter Panel' window. On the left, a dropdown menu is open, displaying the following options: CAT I, Keyword, Rule Title, STIG ID, Vulnerability ID, Rule ID, IA Control, CAT I (highlighted), CAT II, CAT III, and CCI. To the right of the dropdown, the text 'CAT I' is displayed, followed by an 'Add' button. Below this, there are two radio buttons: 'Filter' (selected) and 'Exclusive (-) Filter'. A table with two columns, 'Keyword' and 'Filter', is visible. The table is currently empty, with the text 'content in table' appearing below it. At the bottom of the panel, there are two buttons: 'Remove Filter(s)' and 'Remove All Filters'.

Keyword	Filter
---------	--------

A Look At DISA STIGs (2)

CREATE CHECKLIST



A Look At DISA STIGs (2)

CHECKLIST

The screenshot displays the DISA STIG Viewer 2.5.4 application interface. The main window is titled "DISA STIG Viewer : 2.5.4" and features a menu bar with "File", "Import", and "Export". Below the menu bar, there are tabs for "STIG Explorer" and "Checklist X", with "Checklist X" being the active tab.

The interface is divided into several sections:

- Totals:** A section showing overall statistics. It includes a table with columns "Overall Totals", "CAT I", "CAT II", and "CAT III". The data shows: Open: 0, Not Reviewed: 42, Not a Finding: 0, and Not Applicable: 0.
- Target Data:** A section for specifying target information. It includes fields for "Host Name", "IP Address", "MAC Address", and "Fully Qualified Domain Name". A "Get Host Data" button is also present.
- Role:** A section for selecting a role. It includes radio buttons for "None", "Workstation", "Member Server", and "Domain Controller", and a checkbox for "Web or Database STIG".
- STIGs:** A section for selecting a specific STIG. It includes a "Name" field and a list of STIGs.
- General Information:** A section for displaying the selected STIG's details. It includes the "Active Directory Domain Security Technical Implementation Guide (STIG) :: Release: 7 Benchmark Date: 22 Apr 2016". The "Rule Title" is "User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts." The "Status" is "Not Reviewed".
- Vuln Information:** A section for displaying vulnerability information. It includes tabs for "Discussion", "Check Content", "Fix Text", "CCI", and "Misc". The "Discussion" tab is active, showing a paragraph about delegating account and other AD object ownership and administration tasks.
- Finding Details:** A section for displaying finding details.
- Comments:** A section for displaying comments.

The bottom of the application shows a taskbar with various icons and a system tray with the date and time (10:21 PM 7/8/2017).

A Look At DISA STIGs (2)

- Checklist screens:
 - Overall totals
 - Target data
 - Role
 - Finding details
 - Comments

A Look At DISA STIGs (2)

- Checklist screens (STATUS):
 - Not reviewed
 - Open
 - Not a finding
 - Not applicable

A Look At DISA STIGs (2)

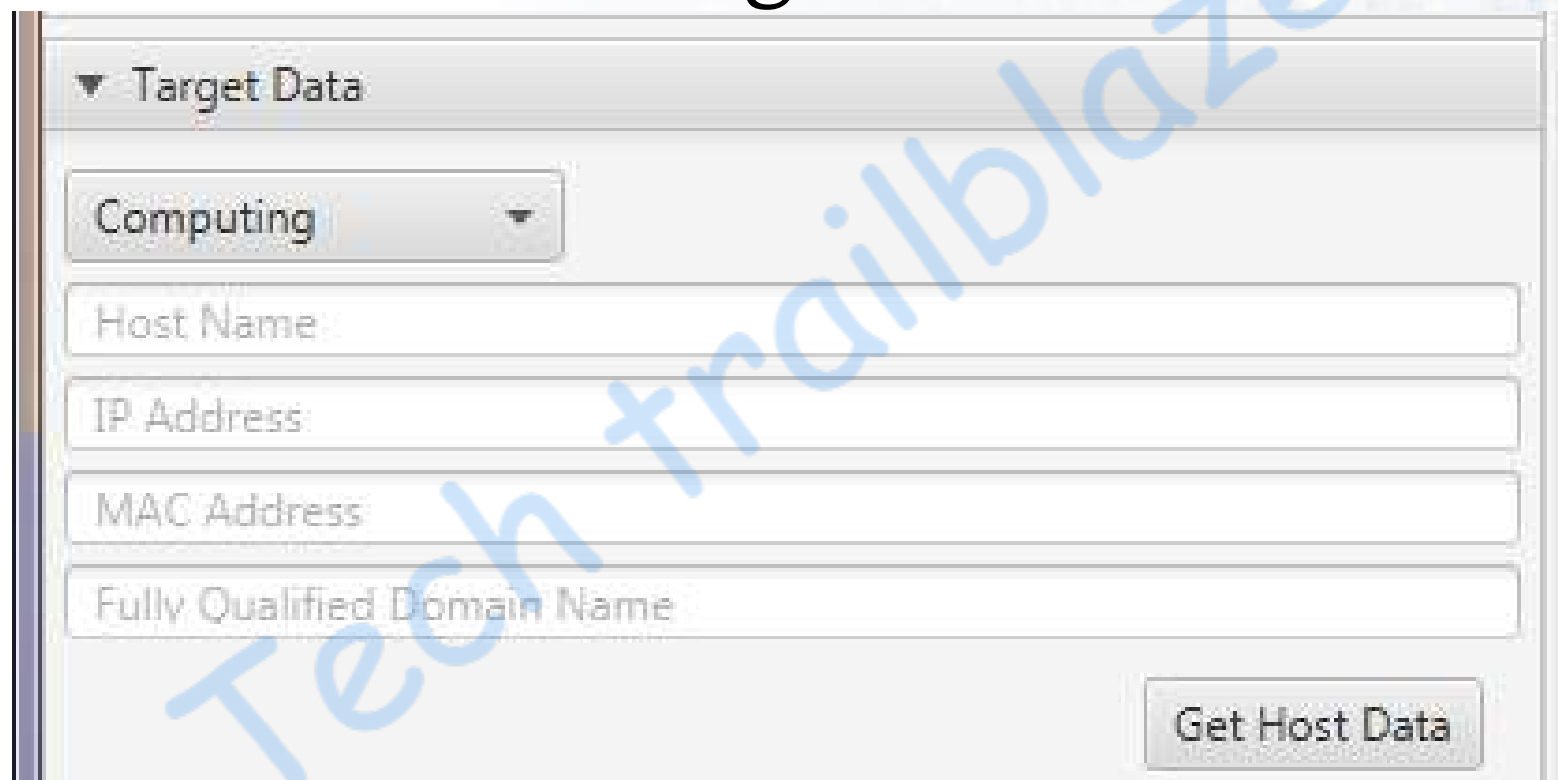
Totals

File Import Export			
STIG Explorer		Checklist X	
▼ Totals			
Overall Totals		CAT I	CAT II
		CAT III	
Open:		1	Not Reviewed: 4
Not a Finding:		0	Not Applicable: 0
Total:		5	
▼ Target Data			

Stat
O
NR
NR
NR
NR

A Look At DISA STIGs (2)

Target Data



The screenshot shows a software window titled "Target Data". Inside the window, there is a dropdown menu currently set to "Computing". Below this menu are four text input fields labeled "Host Name", "IP Address", "MAC Address", and "Fully Qualified Domain Name". At the bottom right of the window is a button labeled "Get Host Data". A large, diagonal watermark reading "Tech trailblazer" is overlaid across the center of the image.

▼ Target Data

Computing ▼

Host Name

IP Address

MAC Address

Fully Qualified Domain Name

Get Host Data

A Look At DISA STIGs (2)

Status

▼ General Information

**Active Directory Domain Security Technical Implementation Guide (STIG) ::
Release: 7 Benchmark Date: 22 Apr 2016**

Rule Title: User accounts with delegated authority must be removed from Windows built-in administrative groups or remove the delegated authority from the accounts.

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable Severity Override ▼

A Look At DISA STIGs (2)

Vuln Information

Review of Hostin...

Status: ☐ Not Reviewed ☒ Open ☐ Not a Finding ☐ Not Applicable Severity Override ▾

▼ Vuln Information

Discussion Check Content Fix Text CCI Misc

In AD it is possible to delegate account and other AD object ownership and administration tasks. (This is commonly done for help desk or other user support staff.) This is done to avoid the need to assign users to Windows groups with more widely ranging privileges. If a user with delegated authority to user accounts in a specific OU is also a member of the Administrators group, that user

A Look At DISA STIGs (2)

- In the next module lets look at further details

END

A Look At STIGs Viewer

<https://public.cyber.mil/stigs/srg-stig-tools/>

Frequently Asked Questions – FAQs

Group Policy Objects

Quarterly Release Schedule and
Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

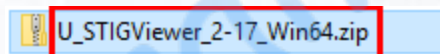
Vendor STIG Development Process

Help

Show 10 entries

	TITLE
	How to Create and SRG-STIG ID Mapping Spreadsheet
	STIG Sorted by STIG ID
	STIG Sorted by Vulnerability ID
	STIG Viewer 2.17
	STIG Viewer 2.17 Hashes
	STIG Viewer 2.17-Linux
	STIG Viewer 2.17-Win64
	STIG Viewer 2.17-Win64 msi
	STIG Viewer User Guide (Sep 2022)
	STIG Viewer Video

Showing 1 to 10 of 11 entries



U_STIGViewer_2-17_Win64.zip

<https://public.cyber.mil/stigs/srg-stig-tools/>

Name	Date modified	Type	Size
app	27/07/2022 2:54 pm	File folder	
runtime	27/07/2022 2:54 pm	File folder	
SWIDTAG	27/07/2022 2:54 pm	File folder	
STIG Viewer	27/07/2022 2:56 pm	Application	592 KB
STIG Viewer	27/07/2022 2:54 pm	Icon	175 KB
ActionLog	11/04/2023 1:04 pm	Text Document	1 KB

DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

▼ STIGs

Filter on STIG name...

CK	Name
No content in table	

Profile: No Profile

▼ Filter Panel

Must match: ☒ All ☐ Any

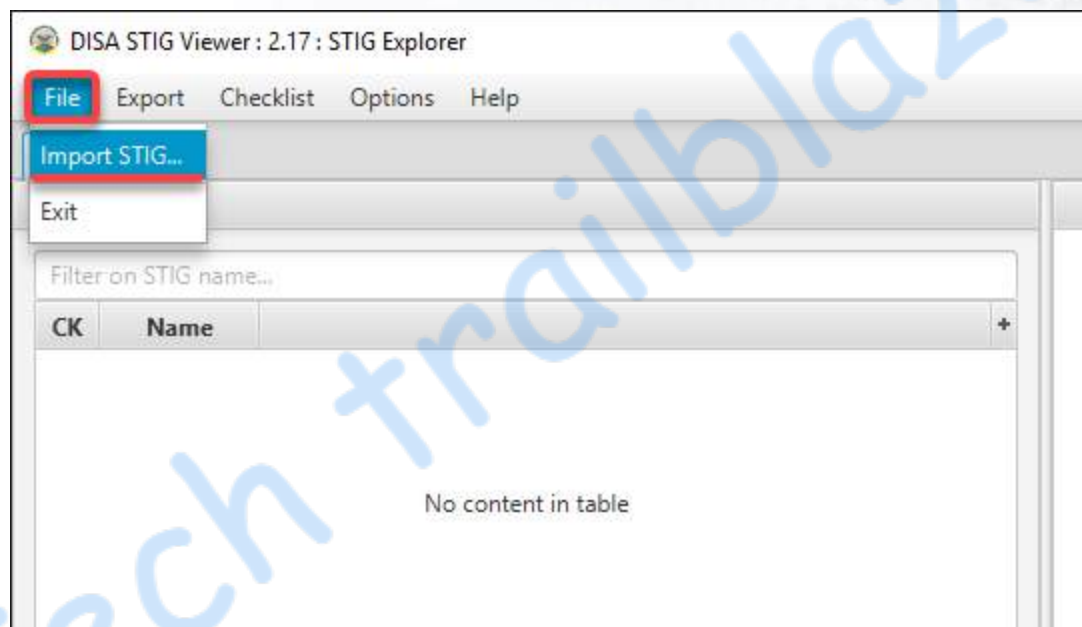
Keyword

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / -	Keyword	Filter
No content in table		

Vul ID	Rule ID	Rule Name
No content in table		

No Rules Selected



A Look At STIGs Viewer

DoD CYBER EXCHANGE PUBLIC

Topics Training PKI/PKE SRGs/STIGs Resources Help

[STIGS]

SRG/STIG Home
Automation
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
DoD Cloud Computing Security
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
Vendor STIG Development Process
Help

Show 10 entries Search:

TITLE	SIZE	UPDATED
Microsoft Sharepoint Designer 2013 STIG - Ver 1, Rel 3	442.79 KB	01 Dec 2018
Microsoft Skype for Business 2016 STIG - Ver 1, Rel 1	352.2 KB	01 Dec 2018
Microsoft Visio 2013 STIG - Ver 1, Rel 4	427.91 KB	01 Dec 2018
Microsoft Visio 2016 STIG - Ver 1, Rel 1	355.78 KB	01 Dec 2018
Microsoft Windows 10 STIG - Ver 2, Rel 5	966.35 KB	09 Nov 2022
Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 7	100.42 KB	13 Jan 2023
Microsoft Windows 11 STIG - Ver 1 Rel 2	948.64 KB	09 Nov 2022
Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1	94.76 KB	17 Nov 2022
Microsoft Windows 2012 and 2012 R2 DC STIG - Ver 3, Rel 5	905.58 KB	09 Nov 2022
Microsoft Windows 2012 and 2012 R2 MS STIG - Ver 3, Rel 5	852.32 KB	09 Nov 2022

Showing 231 to 240 of 549 entries Previous 1 23 24 25 55 Next

STIG TOPICS

- ☐ Application Security (137) [+]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SRGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [+]
- ☐ Mobility (28) [+]
- ☐ Network/Perimeter/Wireless (95) [+]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (52) [+]
- ☐ Security Content Application Protocols (SCAP) (52) [+]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (21)
- ☐ Sunset (132) [+]
- ☐ Supplemental Automation Content (19) [+]
- ☐ Vendor Process (1)

[STIGs]

SRG/STIGs Home

Automation

Control Correlation Identifier (CCI)

Document Library

DoD Annex for NIAP Protection Profiles

DoD Cloud Computing Security

Frequently Asked Questions - FAQs

Group Policy Objects

Quarterly Release Schedule and
Summary

SRG / STIG Library Compilations

SRG / STIG Mailing List

SRG/STIG Tools and Viewing Guidance

Sunset Products

Vendor STIG Development Process

Help

Show 10 entries

Search:

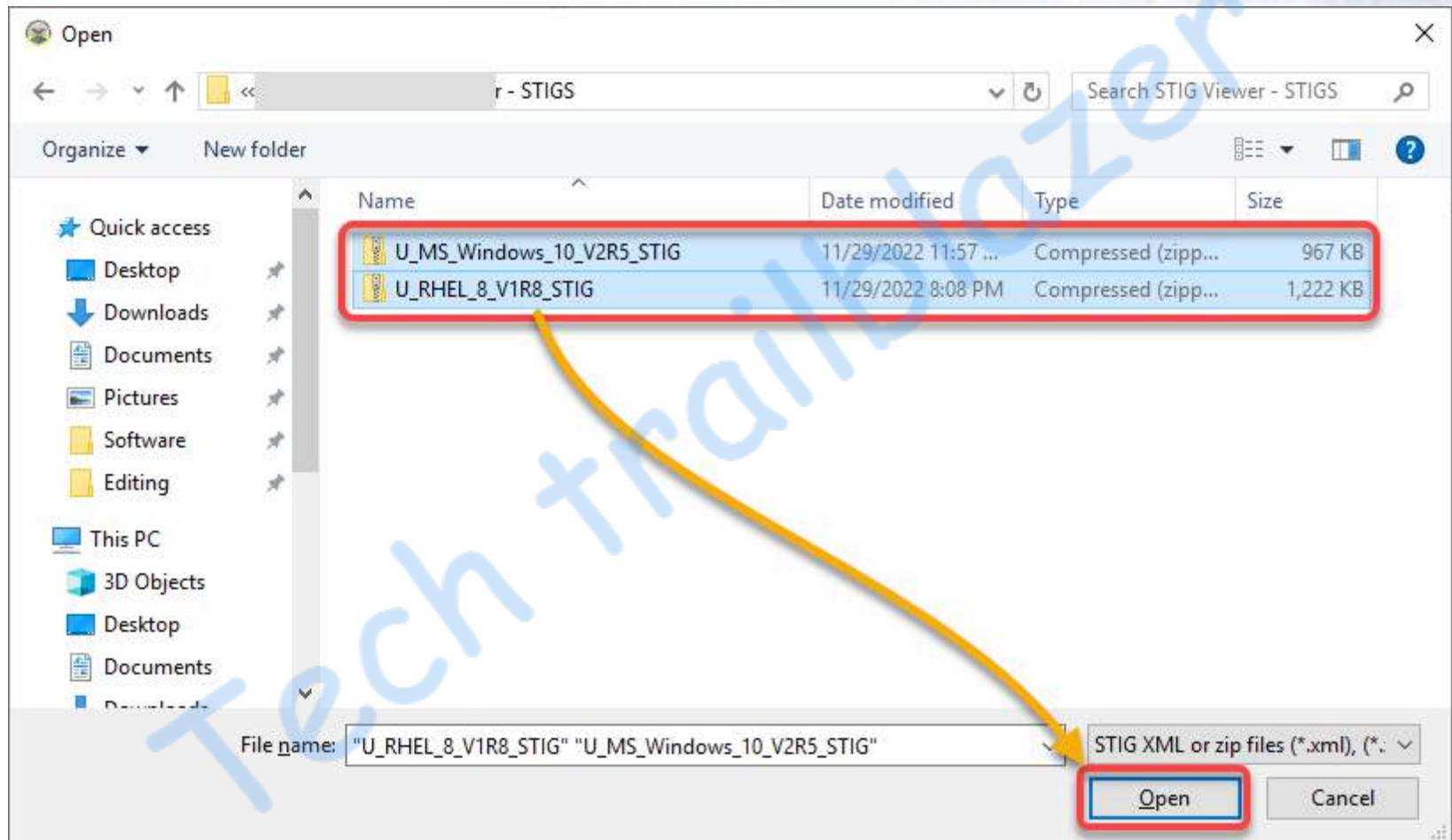
	TITLE	SIZE	UPDATED
	Microsoft Word 2013 STIG - Ver 1, Rel 6	462.31 KB	01 Dec 2018
	Microsoft Word 2016 STIG - Ver 1, Rel 1	361.84 KB	01 Dec 2018
	Mobile Iron Core v9.x Release Memo	65.5 KB	11 Mar 2019
	MobileIron Core v10.x MDM STIG Ver 1 Rel 1	1 MB	06 Jun 2019
	MongoDB Enterprise Advanced 3.x STIG - Ver 2, Rel 1	609.61 KB	19 Apr 2022
	MongoDB Enterprise Advanced 4.x STIG - Ver 1, Rel 2	1.56 MB	21 Oct 2022
	Motorola Android 9.x STIG	2.95 MB	10 Nov 2020
	Motorola Solutions Android 11 - Ver 1, Rel 2	1.68 MB	07 Sep 2022
	Mozilla Firefox for Linux STIG Benchmark - Ver 6, Rel 3	17.52 KB	21 Oct 2022
	Mozilla Firefox for Windows STIG Benchmark - Ver 6, Rel 3	14.8 KB	21 Oct 2022

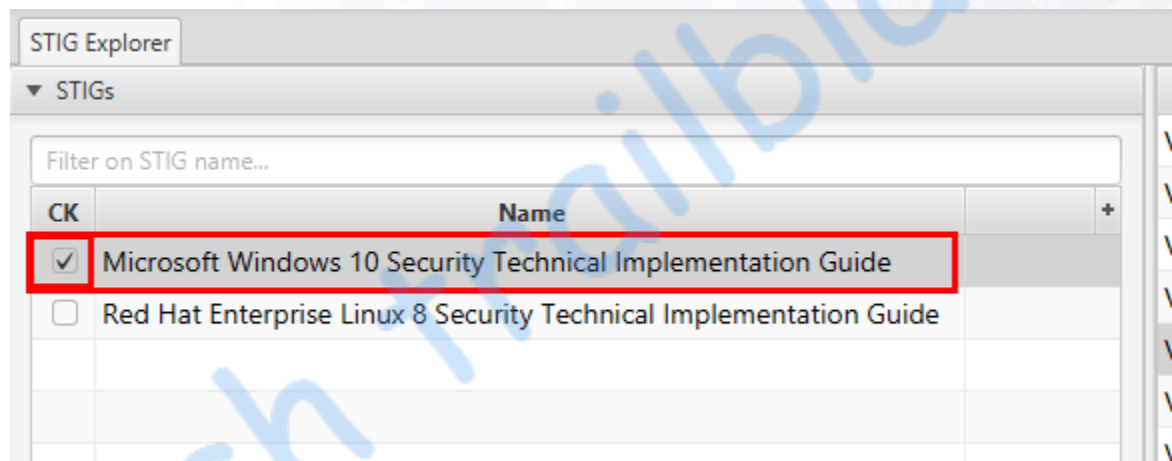
Showing 261 to 270 of 549 entries

Previous 1 26 27 28 55 Next

STIG TOPICS

- ☐ Application Security (167) [+]
- ☐ Cloud Security (4)
- ☐ Control Correlation Identifier (CCI) (4)
- ☐ DoD Cloud Computing Security (DCCS) (5)
- ☐ Draft STIGs/SGs (2)
- ☐ Group Policy Objects (GPO) (1)
- ☐ Host-Based Security Systems (HBSS) (3) [+]
- ☐ Mobility (28) [+]
- ☐ Network/Perimeter/Wireless (96) [+]
- ☐ NIAP Protection Profiles (5)
- ☐ Operating Systems (32) [+]
- ☐ Security Content Application Protocols (SCAP) (52) [+]
- ☐ STIG Compilations (2)
- ☐ STIG Policy (1)
- ☐ STIG Tools (5)
- ☐ STIG Viewing (11)
- ☐ Sunset (102) [+]
- ☐ Supplemental Automation Content (19) [+]
- ☐ Vendor Process (1)





Vul ID	Rule ID	Rule Name	+	M
V-220697	SV-220697r8571...	SRG-OS-000480-...		
V-220698	SV-220698r8571...	SRG-OS-000480-...		
V-220699	SV-220699r5691...	SRG-OS-000480-...		
V-220700	SV-220700r5691...	SRG-OS-000480-...		
V-220701	SV-220701r7931...	SRG-OS-000191-...		
V-220702	SV-220702r8592...	SRG-OS-000185-...		
V-220703	SV-220703r8591...	SRG-OS-000185-...		
V-220704	SV-220704r8592...	SRG-OS-000185-...		
V-220705	SV-220705r8519...	SRG-OS-000370-...		
-----	-----	-----		

Group Title: S

Rule Title: Wi
the following
external scan

Vul ID	Rule ID	Rule Name
V-220697	SV-220697r85...	SRG-OS-00048...
V-220698	SV-220698r85...	SRG-OS-00048...
V-220699	SV-220699r56...	SRG-OS-00048...
V-220700	SV-220700r56...	SRG-OS-00048...
V-220701	SV-220701r79...	SRG-OS-00019...
V-220702	SV-220702r85...	SRG-OS-00018...
V-220703	SV-220703r85...	SRG-OS-00018...
V-220704	SV-220704r85...	SRG-OS-00018...
V-220705	SV-220705r85...	SRG-OS-00037...
V-220706	SV-220706r85...	SRG-OS-00048...
V-220707	SV-220707r79...	SRG-OS-00048...
V-220708	SV-220708r56...	SRG-OS-00008...
V-220709	SV-220709r56...	SRG-OS-00048...
V-220710	SV-220710r56...	SRG-OS-00013...
V-220711	SV-220711r56...	SRG-OS-00011...
V-220712	SV-220712r85...	SRG-OS-00032...
V-220713	SV-220713r56...	SRG-OS-00048...
V-220714	SV-220714r56...	SRG-OS-00009...
V-220715	SV-220715r56...	SRG-OS-00048...
V-220716	SV-220716r56...	SRG-OS-00007...
V-220717	SV-220717r85...	SRG-OS-00031...
V-220718	SV-220718r56...	SRG-OS-00009...
V-220719	SV-220719r56...	SRG-OS-00009...
V-220720	SV-220720r56...	SRG-OS-00009...
V-220721	SV-220721r56...	SRG-OS-00009...
V-220722	SV-220722r56...	SRG-OS-00009...
V-220723	SV-220723r56...	SRG-OS-00048...
V-220724	SV-220724r56...	SRG-OS-00048...
V-220725	SV-220725r56...	SRG-OS-00048...

Showing rule 5 out of 257

Microsoft Windows 10 Security Technical Implementation Guide :: Version 2, Release: 5 Benchmark Date: 14 Nov 2022

Vul ID: V-220701

Rule ID: SV-220701r793197_rule

STIG ID: WN10-00-000025

Severity: CAT II

Classification: Unclass

Legacy IDs: V-63343; SV-77833

Group Title: SRG-OS-000191-GPOS-00080

Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Discussion: An approved tool for continuous network scanning must be installed and configured to run.

Without the use of automated mechanisms to scan for security flaws on a continuous and/or periodic basis, the operating system or other system components may remain vulnerable to the exploits presented by undetected software flaws.

To support this requirement, the operating system may have an integrated solution incorporating continuous scanning using ESS and periodic scanning using other tools, as specified in the requirement.

Check Text: Verify DoD-approved ESS software is installed and properly operating. Ask the site ISSM for documentation of the ESS software installation and configuration.

If the ISSM is not able to provide a documented configuration for an installed ESS or if the ESS software is not properly maintained or used, this is a finding.

Note: Example of documentation can be a copy of the site's CCB approved Software Baseline with version of software noted or a memo from the ISSM stating current ESS software and version.

Fix Text: Install DoD-approved ESS software and ensure it is operating continuously.

References

CCI: CCI-001233: The organization employs automated mechanisms on an organization-defined frequency to determine the state of information system components with regard to flaw remediation.

NIST SP 800-53 :: SI-2 (2)

NIST SP 800-53A :: SI-2 (2).1 (ii)

NIST SP 800-53 Revision 4 :: SI-2 (2)

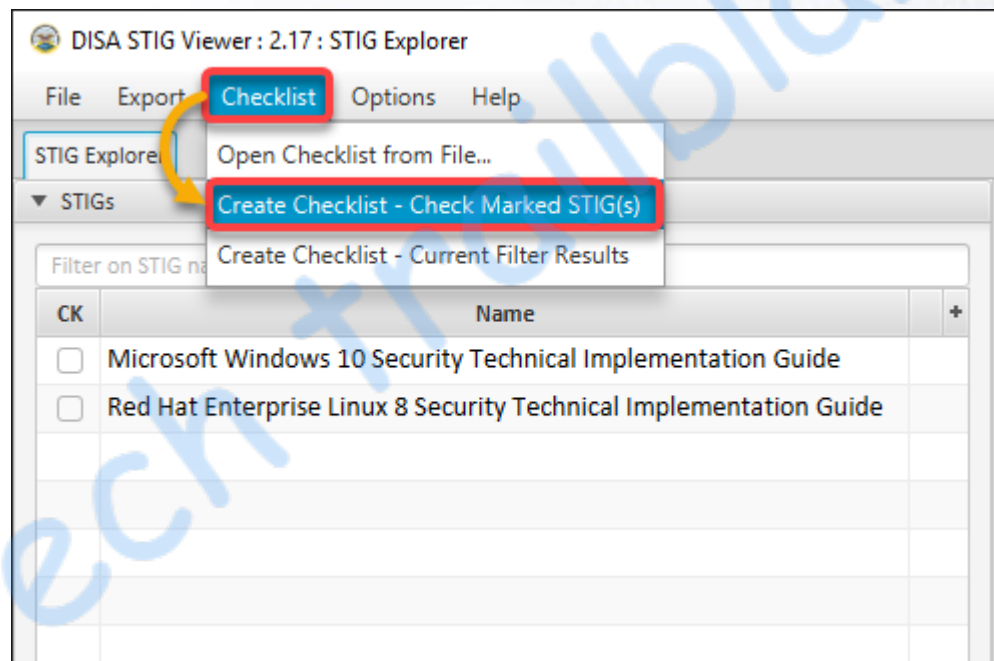
Microsoft Windows 10 Security Technical Implementation Guide :: Version 2. Release: 5 Benchmark Date: 14 Nov 2022

Vul ID: V-220701 **Rule ID:** SV-220701r793197_rule **STIG ID:** WN10-00-000025
Severity: CAT II **Classification:** Unclass **Legacy IDs:** V-63343; SV-77833

Group Title: SRG-OS-000191-GPOS-00080

Rule Title: Windows 10 must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously, where ESS is used; 30 days, for any additional internal network scans not covered by ESS; and annually, for external scans by Computer Network Defense Service Provider (CNDSP).

Discussion: An approved tool for continuous network scanning must be installed and configured to run.



DISA STIG Viewer : 2.17 : *New Checklist

File Import Export Options

STIG Explorer *New Checklist X

▼ Totals

Overall Totals CAT I CAT II CAT III

Open: 0 Not Reviewed: 257
Not a Finding: 0 Not Applicable: 0



▼ Target Data

Computing ▼

CUI
Host Name
IP Address
MAC Address
Fully Qualified Domain Name
Target Comments

Get Host Data

Role

- ☒ None
☐ Workstation
☐ Member Server
☐ Domain Controller
☐ Web or Database STIG

Status	Vul ID	Rule ID	Rule Name
NR	V-220697	SV-220697r857...	SRG-OS-000480...
NR	V-220698	SV-220698r857...	SRG-OS-000480...
NR	V-220699	SV-220699r569...	SRG-OS-000480...
NR	V-220700	SV-220700r569...	SRG-OS-000480...
NR	V-220701	SV-220701r793...	SRG-OS-000191...
NR	V-220702	SV-220702r859...	SRG-OS-000185...
NR	V-220703	SV-220703r859...	SRG-OS-000185...
NR	V-220704	SV-220704r859...	SRG-OS-000185...
NR	V-220705	SV-220705r851...	SRG-OS-000370...
NR	V-220706	SV-220706r857...	SRG-OS-000480...
NR	V-220707	SV-220707r793...	SRG-OS-000480...
NR	V-220708	SV-220708r569...	SRG-OS-000080...
NR	V-220709	SV-220709r569...	SRG-OS-000480...
NR	V-220710	SV-220710r569...	SRG-OS-000138...
NR	V-220711	SV-220711r569...	SRG-OS-000118...
NR	V-220712	SV-220712r851...	SRG-OS-000324...
NR	V-220713	SV-220713r569...	SRG-OS-000480...
NR	V-220714	SV-220714r569...	SRG-OS-000095...
NR	V-220715	SV-220715r569...	SRG-OS-000480...
NR	V-220716	SV-220716r569...	SRG-OS-000076...
NR	V-220717	SV-220717r851...	SRG-OS-000312...
NR	V-220718	SV-220718r569...	SRG-OS-000095...
NR	V-220719	SV-220719r569...	SRG-OS-000096...
NR	V-220720	SV-220720r569...	SRG-OS-000095...
NR	V-220721	SV-220721r569...	SRG-OS-000096...

A Look At DISA STIGs (4)

- Firewall Security
Technical
Implementation Guide
- Vulnerability ID: V-3967
- Rule name: The console
port does not timeout
after 10 mins

A Look At DISA STIGs (4)

The screenshot displays the STIG Explorer application interface. The main window is divided into several panes:

- STIG Explorer** (Top Left): A tree view showing the hierarchy of STIGs. The selected STIG is "Firewall Security Technical Implementation Guide - Cisco".
- Filter Panel** (Bottom Left): A panel for filtering rules. It includes a "Select Filter" dropdown, a text input for "Enter filter keyword", and buttons for "Add", "Inclusive (+) Filter", and "Exclusive (-) Filter". Below this is a table with columns "Keyword" and "Filter", which is currently empty with the message "No content in table".
- Rule List** (Center): A table listing rules with columns "Vul ID" and "Rule Name". The rule "V-3967 The console port does not timeout after 10 minutes." is highlighted.
- General Information** (Right): A pane showing details for the selected rule. It includes the title "Firewall Security Technical Implementation Guide :: Release: 22 Benchmark Date: 28 Apr 2017", the rule title "Rule Title: The network devices must time out access to the console port at 10 minutes or less of inactivity.", the STIG ID "NET1624", and a "Discussion" section.

Rule List Data:

Vul ID	Rule Name
V-3966	More than one local account is defined.
V-3967	The console port does not timeout after 10 minutes.
V-3969	Network element must only allow SNMP read access.
V-3982	L2TP is terminated in the private network.
V-4382	Authentication required for console access.
V-4619	Firewall is not operating on a STIG'd OS.
V-5611	Management connections are not restricted.
V-5612	SSH session timeout is not 60 seconds or less.
V-5613	SSH login attempts value is greater than 3.
V-5646	Devices not configured to filter and drop half-open conn..
V-5731	Perimeter is not compliant with DOD Instr. 8551.1
V-7011	The auxiliary port is not disabled.
V-14637	IPv6 Router Advertisements must be suppressed.
V-14643	Firewall inspection is not performed adequately
V-14644	Firewall must block loopback address
V-14646	Alerts generated at 75% log storage capacity.
V-14647	No FW log dump procedures
V-14648	FA is not informed of critical alerts.
V-14649	FW alert not written to remote console.
V-14653	Audit record must display violation
V-14655	Alerts must remain until acknowledged.
V-14656	FW acknowledge messages must be recorded
V-14667	Key expiration exceeds 180 days.

General Information Details:

Firewall Security Technical Implementation Guide ::
Release: 22 Benchmark Date: 28 Apr 2017

Rule Title: The network devices must time out access to the console port at 10 minutes or less of inactivity.

STIG ID: NET1624

Discussion:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes or less increases the

Check Content:

Review the configuration and verify a session using the console port will time out after 10 minutes or less of inactivity.

If console access is not configured to timeout at 10 minutes or less, this is a finding.

Fix Text:

Configure the timeout for idle console connection to 10 minutes or less.

A Look At DISA STIGs (4)

- General Information:
 - **Rule Title:** The network devices must time out access to the console port at 10 minutes or less of inactivity
 - **STIG ID:** NET1624
 - **Severity:** CAT II

A Look At DISA STIGs (4)

- Discussion:
 - Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console...

A Look At DISA STIGs (4)

- Discussion...:
 - port that has been left unattended. In addition quickly terminating an idle session will also free up resources committed by the managed network device. Setting the timeout of the session to 10 minutes

A Look At DISA STIGs (4)

- Discussion...:
 - or less increases the level of protection afforded critical network components

Tech trailblazer

A Look At DISA STIGs (4)

- Check Content:
 - Review the configuration and verify a session using the console port will time out after 10 mins or less of inactivity.
 - If console access is not configured to timeout at 10 minutes or less, this is a finding.

A Look At DISA STIGs (4)

- Fix Text:
 - Configure the timeout for idle console connection to 10 minutes or less.

Video 11 slides was not available in the downloaded file.

A Look At DISA STIGs (3)

- Windows Server 2012 R2 Member Server
 - Import STIG
 - V1099 (Lockout duration)

Tech trailblazers

A Look At DISA STIGs (2)

STIG Explorer

File Export Checklist Options Help

▼ STIGs

CK	Name
☐	MS SQL Server 2014 Database Security Technical Implementation Guide
☐	Firewall Security Technical Implementation Guide - Cisco
☐	Firewall Security Technical Implementation Guide
☐	SharePoint 2010 Security Technical Implementation Guide (STIG)
☐	Windows Server 2008 R2 Member Server Security Technical Implementation Guide
☐	Layer 2 Switch Security Technical Implementation Guide - Cisco
☐	Layer 2 Switch Security Technical Implementation Guide
☒	Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide

Profile: No Profile

▼ Filter Panel

CAT I CAT I Add

☒ Inclusive (+) Filter ☐ Exclusive (-) Filter

+ / - Keyword Filter

Vul ID	Rule Name
V-1070	Physical security
V-1072	Shared User Accounts
V-1073	Unsupported Service Packs
V-1074	WIN00-000100
V-1075	Display Shutdown Button
V-1076	System Recovery Backups
V-1081	NTFS Requirement
V-1089	Legal Notice Display
V-1090	Caching of logon credentials
V-1093	Anonymous shares are not restricted
V-1097	Bad Logon Attempts
V-1098	Bad Logon Counter Reset
V-1099	Lockout Duration
V-1102	User Right - Act as part of OS
V-1104	Maximum Password Age

A Look At DISA STIGs (2)

Vul ID ▲	Rule Name	+	▼ General Information
V-1070	Physical security		
V-1072	Shared User Accounts		
V-1073	Unsupported Service Packs		
V-1074	WIN00-000100		
V-1075	Display Shutdown Button		
V-1076	System Recovery Backups		
V-1081	NTFS Requirement		
V-1089	Legal Notice Display		
V-1090	Caching of logon credentials		
V-1093	Anonymous shares are not restricted		
V-1097	Bad Logon Attempts		
V-1098	Bad Logon Counter Reset		
V-1099	Lockout Duration		Windows Server 2012/2012 R2 Member Server Security Technical Implementation Guide :: Release: 8 Benchmark Date: 28 Apr 2017 Rule Title: The lockout duration must be configured to require an
V-1102	User Right - Act as part of OS		▼ Discussion The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number of failed logon attempts. A value of 0 will require an administrator to unlock the account.
V-1104	Maximum Password Age		▼ Check Content Verify the effective setting in Local Group Policy Editor. Run "gpedit.msc".
V-1105	Minimum Password Age		Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account
V-1107	Password Uniqueness		▼ Fix Text Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes, "Account is locked out until administrator unlocks it".
V-1112	Dormant Accounts		▼ CCI
V-1113	Disable Guest Account		
V-1114	Rename Built-in Guest Account		
V-1115	Rename Built-in Administrator Account		

A Look At DISA STIGs (3)

- Rule Title:
 - The lockout duration must be configured to require an administrator to unlock an account
 - Severity: CAT II

A Look At DISA STIGs (3)

- Discussion:
 - The account lockout feature, when enabled, prevents brute-force password attacks on the system. This parameter specifies the period of time that an account will remain locked after the specified number

A Look At DISA STIGs (3)

- Discussion...:
 - of failed logon attempts. A value of 0 will require an administrator to unlock the account.

A Look At DISA STIGs (3)

- Check Content:
 - Verify the effective setting in Local Group Policy Editor.
Run "gpedit.msc".

A Look At DISA STIGs (3)

- Check Content:
 - Navigate to Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy.

A Look At DISA STIGs (3)

- Check Content...:
 - If the "Account lockout duration" is not set to "0", requiring an administrator to unlock the account, this is a finding.

A Look At DISA STIGs (3)

- Fix Text:
 - Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy -> "Account lockout duration" to "0" minutes,

A Look At DISA STIGs (3)

- Fix Text...:
 - "Account is locked out until administrator unlocks it".
- CCI: NIST SP 800-53
Revision 4 :: AC-7 b

END

Security Hardening – Case Study – Win 10

- Windows 10
- DISA, Release 9
 - 28 April 2017

Security Hardening – Case Study – Win 10

STIGVIEWER WINDOW

The screenshot shows the DISA STIG Viewer 2.5.4 application. The interface includes a menu bar (File, Export, Checklist, Options, Help) and a toolbar. The main window is divided into three panes:

- STIG Explorer:** A list of STIGs with checkboxes. The "Windows 10 Security Technical Implementation Guide" is selected.
- Table:** A table listing rules with columns "Vul ID" and "Rule Name".
- General Information:** A pane showing details for the selected rule, including the title, release date, and rule title.

Table Data:

Vul ID	Rule Name
V-63325	WN10-CC-000315
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63361	WN10-00-000070
V-63377	WN10-00-000100
V-63379	WN10-EM-000005
V-63429	WN10-AC-000045
V-63651	WN10-CC-000155
V-63667	WN10-CC-000180
V-63671	WN10-CC-000185
V-63673	WN10-CC-000190

General Information:

Windows 10 Security Technical Implementation Guide ::
Release: 9 Benchmark Date: 28 Apr 2017
Rule Title: The Windows Installer Always install with elevated privileges must be disabled.

Discussion:
Standard user accounts must not be granted elevated privileges. Enable Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

Check Content:
If the following registry value does not exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Installer\

Security Hardening – Case Study – Win 10

- General Information:
 - **Rule Title:** The antivirus program must be configured to update signature files on a daily basis.
 - **STIG ID:** WN10-00-000046
 - **Severity:** CAT I

Security Hardening – Case Study – Win 10

- Discussion:
 - Virus scan programs are a primary line of defense against the introduction of viruses and malicious code that can destroy data and even render a computer inoperable. Using a virus scan program provides the ability to...

Security Hardening – Case Study – Win 10

- Discussion...:
 - ...detect malicious code before extensive damage occurs. Updated virus scan data files help protect a system, as constantly changing malware is identified by the antivirus software vendors

Security Hardening – Case Study – Win 10

- Check Content:
 - This requirement is NA if McAfee VirusScan Enterprise (VSE) is used. It will be addressed with the corresponding McAfee VSE STIG.
 - Configurations will vary depending on the product.

Security Hardening – Case Study – Win 10

- Fix Text:
 - Configure the antivirus program to update signature files at least daily. Ensure the updates are occurring on timely basis and are not more than a week old.

Security Hardening – Case Study – Win 10

- CCI (Control Correlation Identifier):

- CCI: 000366

The org implements the security config settings.

NIST SP 800-53 :: CM-6 b

NIST SP 800-53A :: CM-6.1 (iv)

NIST SP 800-53

Revision 4 :: CM-6

END

Comparison of CIS Vs DISA

Comparison of CIS Vs DISA

- Many controls are common
- Approaches are different
- Organization styles are different

Comparison. was in long question
2nd question tabke give. tha just data input
krna tha like good and satisfactory

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL COVERAGE	GOOD	EXCELLENT
ORG SUITABILITY	SMALL AND MEDIUM ORGS	LARGE ORGS
USER FRIENDLINESS	GOOD	SATISFACTORY
UNUSABLE TERMINOLOGY	NO	YES
CONTROL DETAIL	GOOD	SATISFACTORY
TOOLS	CAT (COMMERCIAL)	SCAP (MILITARY USE)

Comparison of CIS Vs DISA

FEATURE	CIS	DISA
CONTROL PRIORITIZATION	LEVEL 1, LEVEL 2	CAT I - CAT III
TRACKING EASE	CAT TOOL (COMMERCIAL)	FREE STIG VIEWER (CHECKLIST)
FREQUENCY OF UPDATES	FAIR	QUARTERLY
INDUSTRY CREDIBILITY	HIGH	VERY HIGH
INDUSTRY ADOPTION	HIGH	MODERATE

Comparison of CIS Vs DISA

- How to select CIS/DISA:
 - Size of organization
 - IT infrastructure extent
 - Nature of business
 - Security program goals
 - Maturity of IT & security staff

Comparison of CIS Vs DISA

- Rule of thumb:
 - Smaller orgs use CIS
 - Larger orgs use DISA
 - CIS is part of Homeland Security, DISA is part of US Military
 - DISA more frequently updated and maintained with wider coverage

END

ISMS:Leading InfoSec Governance Framework

- ISO27001:2013 (ISMS)
 - Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system
 - Ten short clauses
 - Long annex

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 MANDATORY CLAUSES

Reference		Description
Mandatory	Clause 4	Context of the organization
	Clause 5	Leadership
	Clause 6	Planning
	Clause 7	Support
	Clause 8	Operation
	Clause 9	Performance evaluation
	Clause 10	Improvement

<https://chapters.theiia.org/bermuda/Events/ChapterDocuments/Information%20Security%20Management%20System%20%28ISMS%29%20Overview.pdf>

ISMS:Leading InfoSec Governance Framework



ISO27001:2013 DISCRETIONARY CONTROLS

Reference	Description	Control Total
Discretionary	A5 Information security policies	2
	A6 Organization of information security	7
	A7 Human resource security	6
	A8 Asset management	10
	A9 Access control	13
	A10 Cryptography	2
	A11 Physical and environmental security	15
	A12 Operations security	14
	A13 Communications security	7
	A14 System acquisition, development and maintenance	13
	A15 Supplier relationships	5
	A16 Information security incident management	7
	A17 Information security aspects of business continuity management	4
	A18 Compliance	8

TOTAL: 113

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Exceptional framework with comprehensive coverage of mandatory requirements (clauses 4-10) and discretionary controls (annex)

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Highly beneficial as a framework for security program
 - Covers all domain areas
 - Provides a structure and organized sequence for security controls

ISMS:Leading InfoSec Governance Framework

- Merits of ISO27001:2013 (ISMS):
 - Complements security transformation model as serves as a reference and guideline for activities and controls

ISMS:Leading InfoSec Governance Framework

Short question of
demerits

- **De-merits of ISO27001:2013 (ISMS):**
 - Very broad
 - Generic framework – leaves it to organization how to implement the measures and controls
 - Not suited for orgs that are new to security program

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - Implement security transformational model
 - Cap off security transformation project with ISO27001:2013 (ISMS) certification

ISMS:Leading InfoSec Governance Framework

- How to best use advantages of ISO27001:2013 (ISMS):
 - ISMS as a complementary reference and checklist rather than main framework

How to Use ISO27002:2013

- What is ISO27002:2013 ?
 - Information technology -- Security techniques -- Code of practice for information security controls
 - Renamed from ISO 17799

How to Use ISO27002:2013

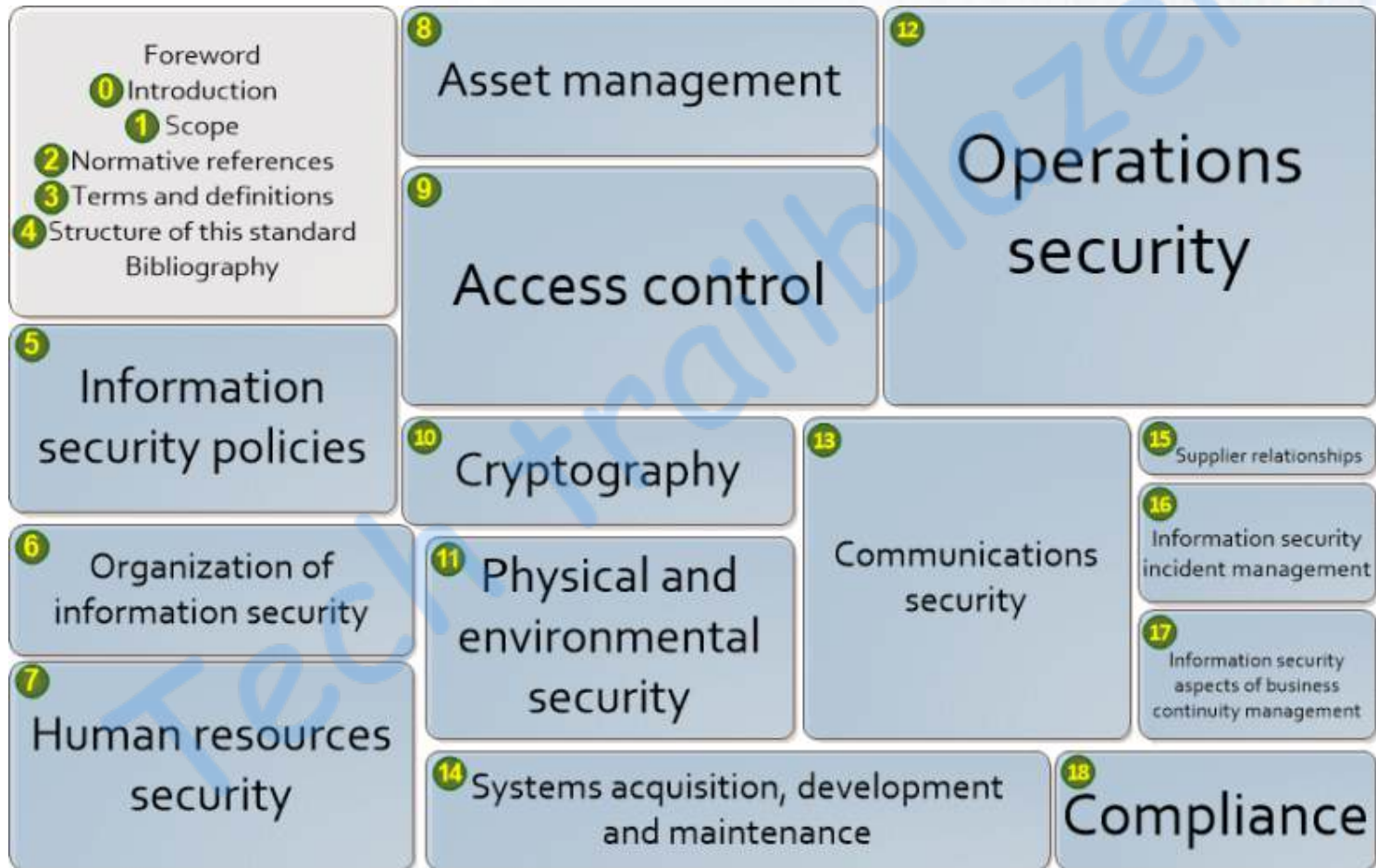
- 0.1 Background & Context
 - This Int'l Standard is designed for orgs to use as a **reference** for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001;

How to Use ISO27002:2013

- 0.1 Background & Context
 - or as a **guidance document** for organizations implementing commonly accepted information security controls.

How to Use ISO27002:2013

STRUCTURE OF ISO27002:2013



<http://www.iso27001security.com/html/27002.html>

How to Use ISO27002:2013

- Lets have a look at control A.5.1.2 (**Review Of The Policies Of Information Security**)

Tech trailblazers

How to Use ISO27002:2013

ISO27001:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFORMATION SECURITY	Control: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
---------	---	---

How to Use ISO27002:2013

ISO27002:2013

TITLE

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

CONTROL

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

How to Use ISO27002:2013

ISO27002:2013

5.1.2 Review of the policies for information security

Control

The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Implementation guidance

Each policy should have an owner who has approved management responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the organization's policies and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

27002 IMPLEMENTATION GUIDANCE

How to Use ISO27002:2013

ISO27002:2013

A.5.1.2	REVIEW OF THE POLICIES FOR INFOSEC	<i>27002: Implementation Guidance:</i> Each policy should have an owner who has approved mngmt responsibility for the development, review and evaluation of the policies. The review should include assessing opportunities for improvement of the org's policies and approach to managing Infosec in response to changes to the org environment, business circumstances, legal conditions or tech environment.
---------	--	---

How to Use ISO27002:2013

- Practically:
 - ISO27001:2013 controls are brief and generic
 - 27002 clarifies further what is being referred to, gives further context & very useful implementation guidance

END

NIST FRAMEWORK

- The Computer Security Resource Center (CSRC) website guides users to NIST resources on **computer, cyber, and information security and privacy.**

NIST FRAMEWORK

- Its content includes **publications, projects, research, news and events** from the NIST Information Technology Laboratory's (ITL) two security divisions

NIST FRAMEWORK

[CONTACT](#) [SITE MAP](#)

Computer Security Division

Computer Security Resource Center

[CSRC Home](#) [About](#) [Projects / Research](#) [Publications](#) [News & Events](#)

Search

Fulltext search of NIST's computer security publications:

 [Advanced Search](#)

Browse Publications

NEW PUBLICATIONS

- SP 800-67 Rev. 2 (Draft)
- SP 800-190 (2nd Draft)
- NISTIR 8179 (Draft)
- SP 800-192
- SP 800-12 Rev. 1

CSRC HOME > PUBLICATIONS > NIST SPECIAL PUBLICATIONS

NIST SPECIAL PUBLICATIONS (SP)

NIST uses three NIST Special Publication subseries to publish computer/cyber/information security and guidelines, recommendations and reference materials:

- **SP 800, Computer Security** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the [NIST Library Catalog](#));
- **SP 1800, NIST Cybersecurity Practice Guides** (2015-present):
A new subseries created to complement the SP 800s; targets specific cybersecurity challenges in the public and private sectors; ***practical, user-friendly guides*** to facilitate adoption of standards-based approaches to cybersecurity;

NIST FRAMEWORK

- **SP 800, Computer Security** (December 1990-present):
NIST's primary mode of publishing computer/cyber/information security ***guidelines, recommendations and reference materials*** (SP 800s are also searchable in the **NIST Library Catalog**);

NIST FRAMEWORK

PUBLICATIONS BY TOPIC/PROJECT

Browse FIPS, Special Publications, NISTIRs and ITL Bulletins *by topic or project*:

Security Concepts

[General IT Security](#)
[Audit & Accountability](#)
[Authentication](#)
[Awareness & Training](#)
[Certification & Accreditation](#)
[Contingency Planning](#)
[Cryptography](#)
[Digital Signatures](#)
[Incident Response](#)
[Maintenance](#)
[Personal Identity Verification \(PIV\)](#)
[Planning](#)
[Privacy](#)
[Public Key Infrastructure \(PKI\)](#)
[Research](#)
[Risk Assessment](#)
[Security Automation](#)
[Services & Acquisition](#)
[Threats & Vulnerability Management](#)
[Usability](#)

Technologies

[Biometrics](#)
[Cloud Computing & Virtualization](#)
[Communications & Wireless](#)
[Mobile](#)
[Smart Cards](#)

Applications

[Cyber-Physical Systems / Smart Grid](#)
[Forensics](#)
[Healthcare](#)
[Internet of Things \(IoT\)](#)
[Public Safety](#)
[Supply Chain](#)
[Voting](#)

Activities

[Annual Reports](#)
[Conferences & Workshops](#)

NIST FRAMEWORK

SP 800s - Computer Security

Number	Date	Title
SP 800-193 (Draft)	May 2017	DRAFT Platform Firmware Resiliency Guidelines ➔ Announcement and Draft Publication
SP 800-192	June 2017	Verification and Test Methods for Access Control Policies/Models 📄 SP 800-192 FAQ doi:10.6028/NIST.SP.800-192 [Direct Link]
SP 800-190 (Draft)	July 2017	DRAFT Application Container Security Guide (2nd Draft) ➔ Announcement and Draft Publication
SP 800-188 (Draft)	December 2016	DRAFT De-Identifying Government Datasets (2nd Draft) ➔ Announcement and Draft Publication
SP 800-187 (Draft)	November 2016	DRAFT Guide to LTE Security ➔ Announcement and Draft Publication
SP 800-185	December 2016	SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash 📄 SP 800-185 FAQ doi:10.6028/NIST.SP.800-185 [Direct Link] 📄 Comments Received on Draft SP 800-185
SP 800-184	December	Guide for Cybersecurity Event Recovery

NIST FRAMEWORK

This publication is available free of charge from <http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST Special Publication 800-147B

BIOS Protection Guidelines for Servers

Andrew Regenscheid

AUGUST 2014
32 PAGES DOC

<http://dx.doi.org/10.6028/NIST.SP.800-147B>

NIST FRAMEWORK

- NIST has a tremendous library of free documentation on a diverse range of topics
- **Relevance is often average, however, depth and detail of material is extraordinary**

END

PCI DSS V3

- PCI Data Security Standard (DSS): 
 - Designed to ensure that ALL companies that accept, process, store or transmit credit card info maintain a secure environment
 - Managed by Security Standards Council

<https://www.pcicomplianceguide.org/pci-faqs-2/>

PCI DSS V3



- PCI DSS:
 - SSC is an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB)
 - 6 Broad goals and 12 requirements

why this was design PCI
DSS mcqa

REF: PCI Best Practices For Implementing
Security Awareness;
[https://www.pcisecuritystandards.org/doc
uments/](https://www.pcisecuritystandards.org/documents/)

PCI DSS V3

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across public networks 
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

<https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

REQUIREMENT

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	

TESTING PROCEDURES

PCI DSS V3

PCI DSS Requirements	Testing Procedures	Guidance
	1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.	Network diagrams describe how networks are configured, and identify the location of all network devices.
	1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.

GUIDANCE

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
7.1.4 Require documented approval by authorized parties specifying required privileges.	7.1.4 Select a sample of user IDs & compare with documented approvals to verify that: -Documented approval exists for the assigned privileges -The approval was by authorized parties -That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.

PCI DSS V3

REQMT	TEST PROCEDURES	GUIDANCE
8.1.4 Remove/disable inactive user accounts within 90 days.	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.

PCI DSS V3

- PCI is specific to the card environment to protect cardholder data
- PCI controls are very specific and in-depth compared to generic and high-level controls of ISO27001

END

COBIT

- COBIT:
 - ISACA framework for IT Governance
 - COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use (ISACA)

COBIT

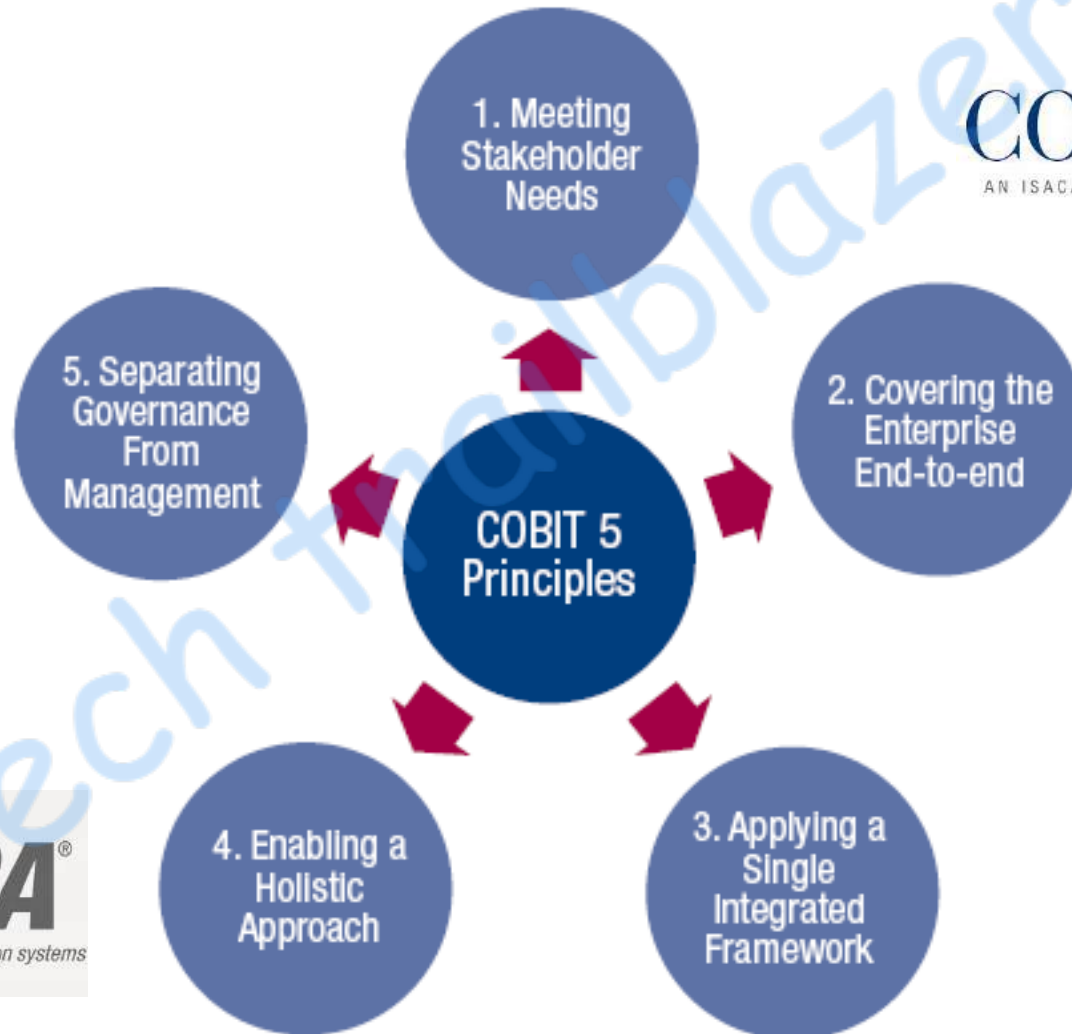


COBIT

- COBIT 5 brings together **five principles** that allow the enterprise to build an effective governance and management framework (ISACA)
- Based on a holistic set of **seven enablers** that optimises IT investment and use for the benefit of stakeholders (ISACA)

COBIT

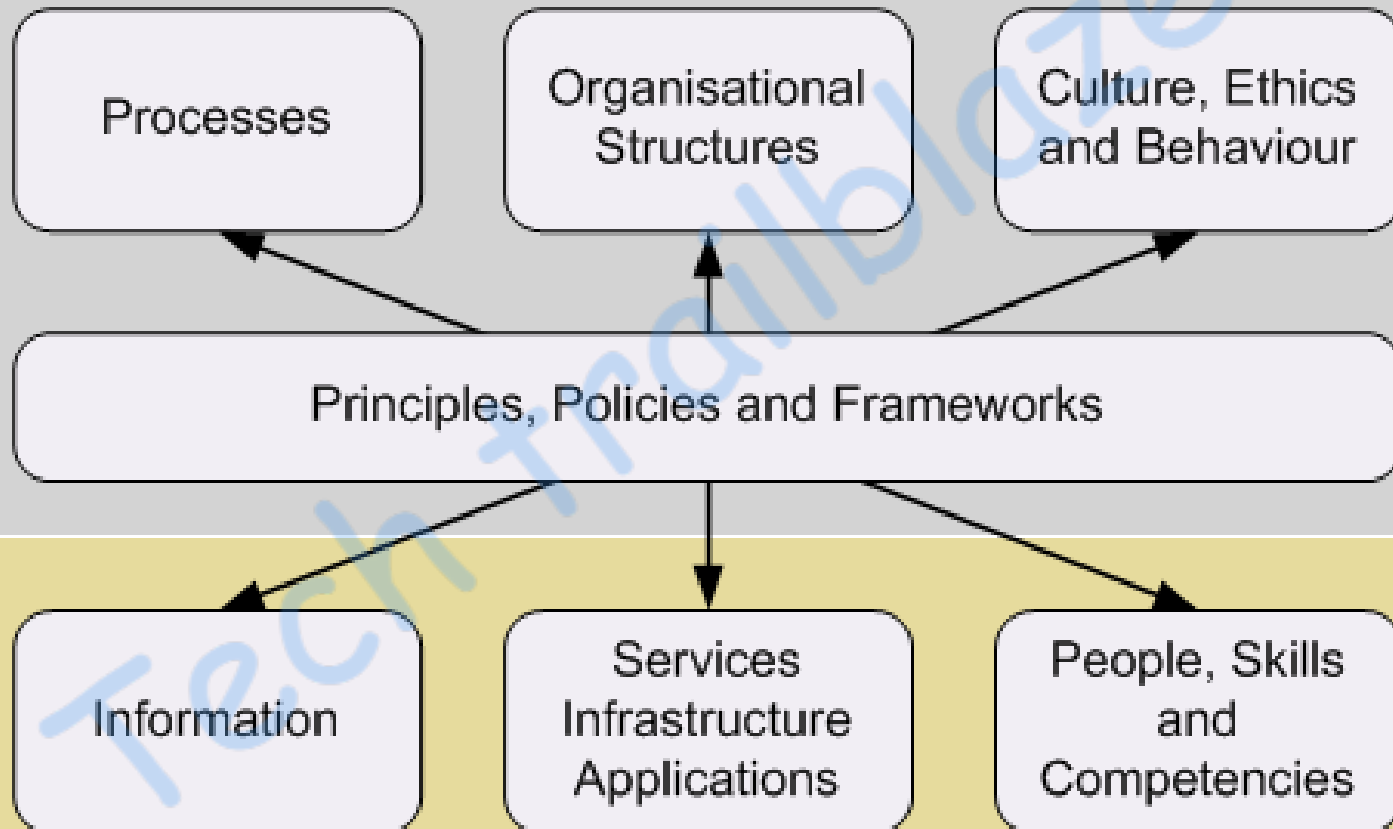
COBIT®
AN ISACA® FRAMEWORK



COBIT



COBIT 5 ENTERPRISE ENABLERS



COBIT

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions & options; setting **direction** through prioritisation & decision making;

COBIT

- ... & **monitoring** performance, compliance and progress against agreed direction and objectives (**EDM**)



COBIT

- **Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (**PBRM**)



COBIT



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 Manage Security

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Changes Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Processes for Management of Enterprise IT

COBIT

- COBIT 5 is a detailed framework for IT governance developed by ISACA which has principles, enablers, and processes
- These tools assist implementers and customer organizations to successfully deploy the framework
- Certifiable framework

END

MALWARE

MALICIOUS SOFTWARE

UUPP

Topic from fornsic, makware, operating system
are imp and computer fraud also

Malware

- Malicious software
- Rogue software
- Rogue
 - Large, destructive, anomalous or unpredictable
 - Operating outside normal or desirable controls

Malware

- Malware (a portmanteau for malicious software) is any software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorized access to information or systems, deprive access to information, or which unknowingly interferes with the user's computer security and privacy.
- Researchers tend to classify malware into one or more sub-types (i.e. computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and keyloggers).
- Malware poses serious problems to individuals and businesses on the Internet.
- According to Symantec's 2018 Internet Security Threat Report (ISTR), malware variants number has increased to 669,947,865 in 2017, which is twice as many malware variants as in 2016.
- Cybercrime, which includes malware attacks as well as other crimes committed by computer, was predicted to cost the world economy \$6 trillion USD in 2021, and is increasing at a rate of 15% per year.
- Since 2021, malware has been designed to target computer systems that run **critical infrastructure** such as the electricity distribution network.
- The defense strategies against malware differ according to the type of malware but most can be thwarted by installing antivirus software, firewalls, applying regular patches to reduce zero-day attacks, securing networks from intrusion, having regular backups and isolating infected systems.
- Malware is now being designed to evade antivirus software detection algorithms.

VIP

Malware Types

- Virus
- Worm
- Trojan
- Logic bomb
- Time bomb
- Drive-by download
- Backdoor
- PUPs(Potentially Unwanted Program)
- Spyware
- Adware
- Scareware
- Ransomware
- FakeAV / Rogue security software
- Malvertising
- APT
- Fileless malware

Software versus Malware

- Writing a typical software
 - Software application (word processor, spreadsheet, graphics)
 - Higher-level programming language
 - Usually independent of OS
- Writing a virus
 - Detailed knowledge of OS

Computer Virus

- Biological virus
 - Latin → Poison
 - Shell filled with genetic material that it injects into a living cell, thereby infecting it
 - The cell then starts manufacturing copies of virus
- Computer virus behaves similarly
 - Injects its contents, a short computer program / instructions, into a host computer and infecting it
 - When the computer executes the virus code, it replicates the code, performs some task(s), usually of a malicious nature

- A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs.
- Computer viruses generally require a host program.
- The virus writes its own code into the host program.
- When the program runs, the written virus program is executed first, causing infection and damage.

- By contrast, a computer worm does not need a host program, as it is an independent program or code chunk.
- Therefore, it is not restricted by the host program, but can run independently and actively carry out attacks.

- Any virus will by definition make unauthorised changes to a computer, which is undesirable even if no damage is done or intended.
- The first page of Dr Solomon's Virus Encyclopaedia explains the undesirability of viruses, even those that do nothing but reproduce.

- The first academic work on the theory of self-replicating computer programs was done in 1949 by John von Neumann who gave lectures at the University of Illinois about the "Theory and Organization of Complicated Automata".
- The work of von Neumann was later published as the "Theory of self-reproducing automata".
- In his essay von Neumann described how a computer program could be designed to reproduce itself.
- Von Neumann's design for a self-reproducing computer program is considered the world's first computer virus, and he is considered to be the theoretical "father" of computer virology.

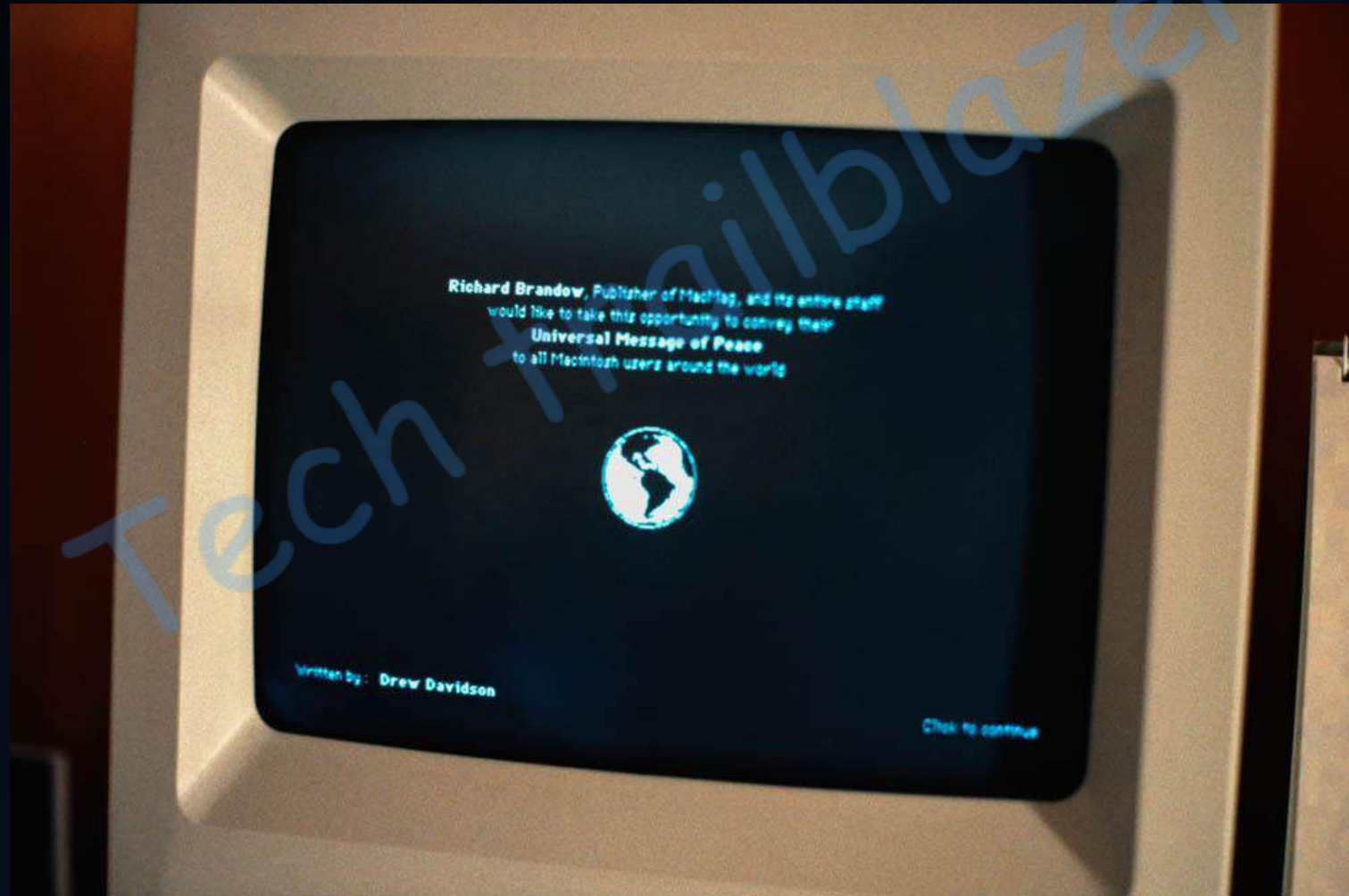
- In 1972, Veith Risak directly building on von Neumann's work on self-replication, published his article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Self-reproducing automata with minimal information exchange).
- The article describes a fully functional virus written in assembler programming language for a SIEMENS 4004/35 computer system.
- In 1980 Jürgen Kraus wrote his diplom thesis "Selbstreproduktion bei Programmen" (Self-reproduction of programs) at the University of Dortmund.
- In his work Kraus postulated that computer programs can behave in a way similar to biological viruses.

Creeper / Reaper

- The Creeper virus was first detected on ARPANET, the forerunner of the Internet, in the early 1970s.
- Creeper was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971.
- Creeper used the ARPANET to infect DEC PDP-10 computers running the TENEX operating system.
- Creeper gained access via the ARPANET and copied itself to the remote system where the message, "I'M THE CREEPER. CATCH ME IF YOU CAN!" was displayed.
- The Reaper program was created to delete Creeper.

- In 1984 Fred Cohen from the University of Southern California wrote his paper "Computer Viruses – Theory and Experiments".
- It was the first paper to explicitly call a self-reproducing program a "virus", a term introduced by Cohen's mentor Leonard Adleman.

This is the MacMag virus 'Universal Peace' message, as displayed on my Mac in March of 1988.



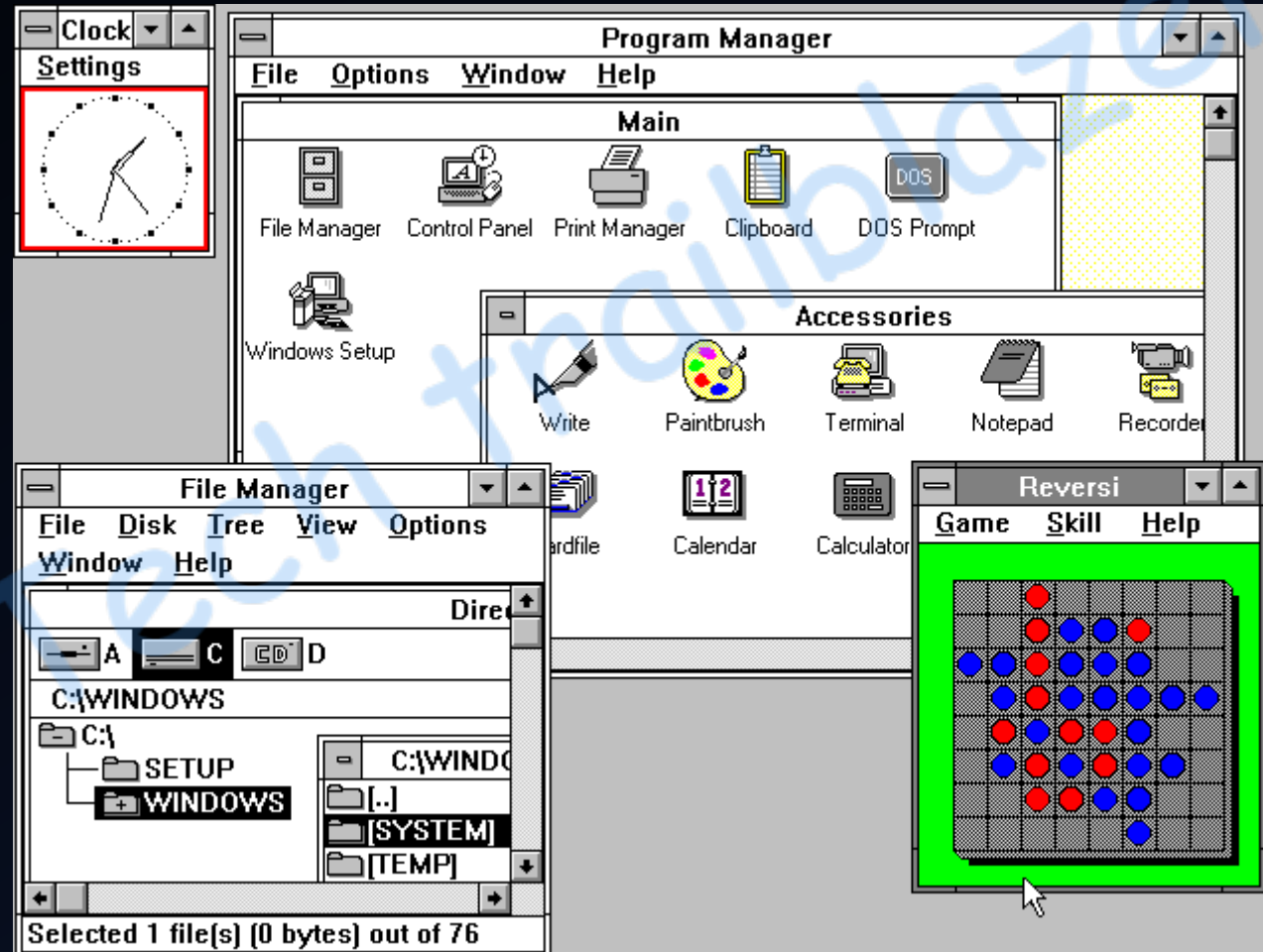
Brain virus

- 26 September 1988: front cover of Time magazine
- Title: “Invasion of the data snatchers”
- The first IBM PC compatible virus in the "wild" was a boot sector virus dubbed (c)Brain, created in 1986 and was released in 1987 by Amjad Farooq Alvi and Basit Farooq Alvi in Lahore, Pakistan, reportedly to deter unauthorized copying of the software they had written.

Hex dump of the Brain virus, generally regarded as the first computer virus for the IBM Personal Computer (IBM PC) and compatibles

Displacement	Hex codes	ASCII value
0000(0000)	FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20	-0J04↑●Π0
0016(0010)	20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F	Welcome to
0032(0020)	20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20	the Dungeon
0048(0030)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0064(0040)	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080(0050)	20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20	(c) 1986 Basit
0096(0060)	26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74	& Amjad (put) Lt
0112(0070)	64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20	d.
0128(0080)	20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20	BRAIN COMPUTER
0144(0090)	53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49	SERVICES.. 730 NI
0160(00A8)	5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41	ZAM BLOCK ALLAMA
0176(00B0)	20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20	.IQBAL TOWN
0192(00C0)	20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52	LAHDR
0208(00D0)	45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E	E-PAKISTAN..PHJN
0224(00E0)	45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 3B	E :430791,443248
0240(00F0)	2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20	,280530.

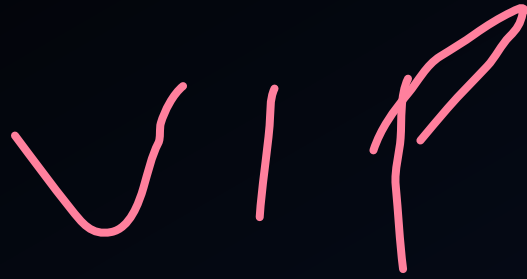
The first virus to specifically target Microsoft Windows, WinVir was discovered in April 1992, two years after the release of Windows 3.0.



Parts of a Virus

- A computer virus generally contains three parts:
 - the infection mechanism, which finds and infects new files
 - the payload, which is the malicious code to execute
 - the trigger, which determines when to activate the payload

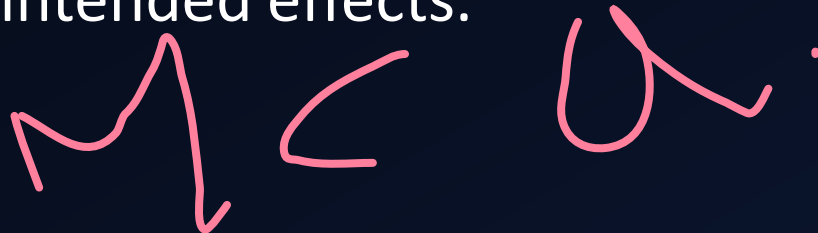
Computer worm



- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers.
- It often uses a computer network to spread itself, relying on security failures on the target computer to access it.
- It will use this machine as a host to scan and infect other computers.
- When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behaviour will continue.

Computer worm

- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time.
- Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- Many worms are designed only to spread, and do not attempt to change the systems they pass through.
- However, as the **Morris worm** and **Mydoom** showed, even these "payload-free" worms can cause major disruption by increasing network traffic and other unintended effects.





0	00	00-6D	73	62	6C	msbl
0	6A	75-73	74	20	77	ast.exe I just w
9	20	4C-4F	56	45	20	ant to say LOVE
0	62	69-6C	6C	79	20	YOU SAN!! billy
0	64	6F-20	79	6F	75	gates why do you
3	20	70-6F	73	73	69	make this possi
0	20	6D-61	6B	69	6E	ble ? Stop makin
E	64	20-66	69	78	20	g money and fix
7	61	72-65	21	21	00	your software!!
0	00	00-7F	00	00	00	♠ δ♥▶ H Δ
0	00	00-01	00	01	00	đ_đ_ © © ©
0	00	00-00	00	00	46	á© L F
C	C9	11-9F	E8	08	00	♦lêèÙ¬¬fþ■
0	00	03-10	00	00	00	+▶H`© ♠♥▶
3	00	00-01	00	04	00	þ♥ ã đ♥ © ♦

important for short question and
mcqs

Ransomware

- Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off.
- While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.
- It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Payment for private key



Private key will be destroyed on
10/13/2013
1:21 PM

Time left
71 : 33 : 17

Choose a convenient payment method and click «Next»:

Bitcoin (most cheap option)



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send **2 BTC** to Bitcoin address

[REDACTED] and specify the Transaction ID on the next page, which will be verified and confirmed.

[Home Page](#)

[Getting started with Bitcoin](#)

<< Back

Next >>



Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT from Monday to Friday

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt

Trojan horse

important for short and
mcqs

- In computing, a Trojan horse is any malware that misleads users of its true intent by disguising itself as a standard program.
- The term is derived from the ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy.

- 
- Once installed, Trojans may perform a range of malicious actions.
 - Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.
 - Since individual Trojans typically use a specific set of ports for this communication, it can be relatively simple to detect them.



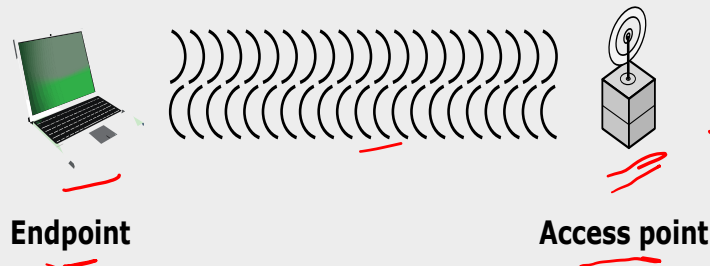
Wireless Network Security

Wireless Networking Components



Wireless Security

- Key factors contributing to higher security risk of wireless networks compared to wired networks include:
- **Channel**
 - Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks
 - Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols
- **Mobility**
 - Wireless devices are far more portable and mobile, thus resulting in a number of risks
- **Limited Resources**
 - Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware
- **Accessibility**
 - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations, thus greatly increasing their vulnerability to physical attacks



IEEE 802.11 Standard

Wired and Wireless LANs

- LANs are designed for use in a **small area** (offices, campuses)
- IEEE **has defined the specifications for a**
 - wired LAN, called IEEE 802.3
 - wireless LAN, called IEEE 802.11,
- These specifications are concerning the physical and data link layers.

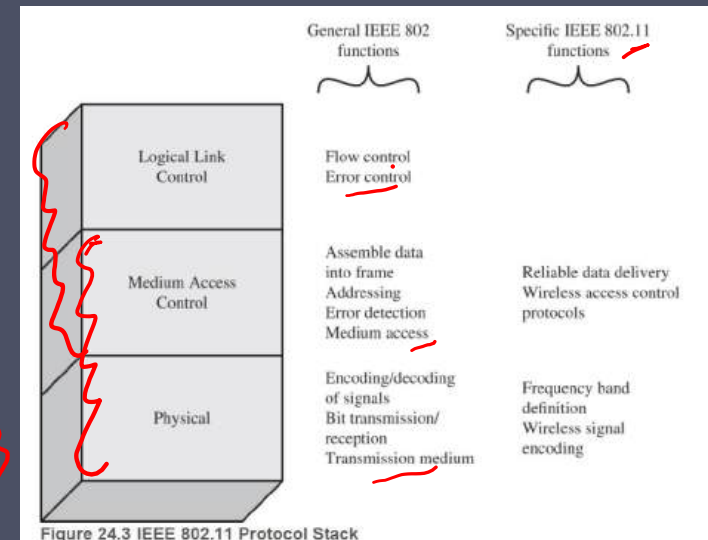
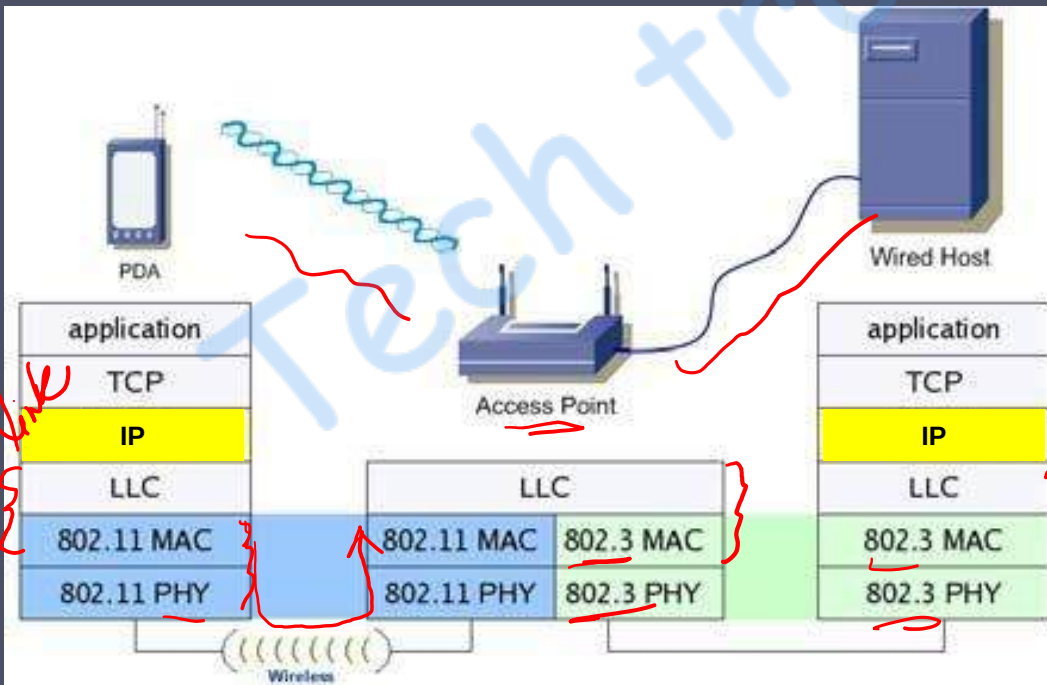


Figure 24.3 IEEE 802.11 Protocol Stack

Brief History of IEEE 802

- Since there are various types of computer system manufacturers, the IEEE's computer society started a project in 1985 called **Project 802** to enable standard communication between various devices.

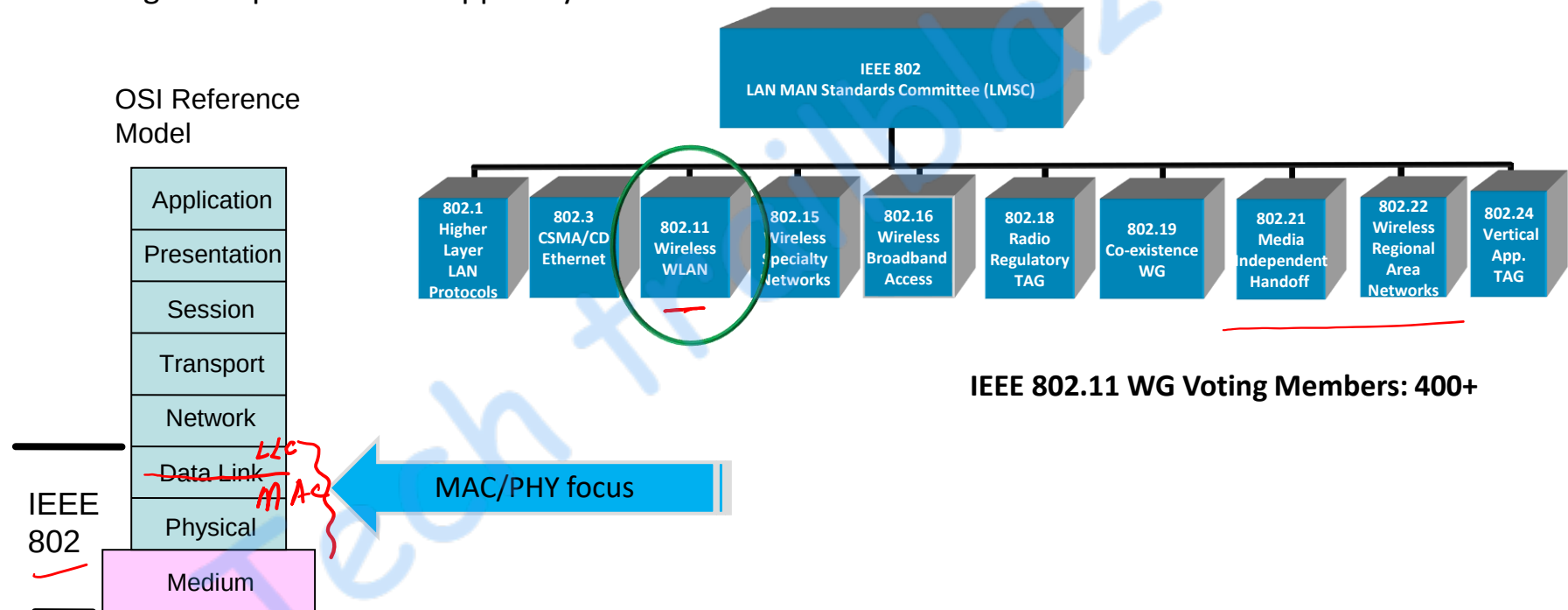


- The **IEEE 802 LAN/MAN Standards Committee (LMSC)** develops and maintains networking standards and recommended practices for **local, metropolitan, and other area networks**, using an open and accredited process, and advocates them on a global basis.

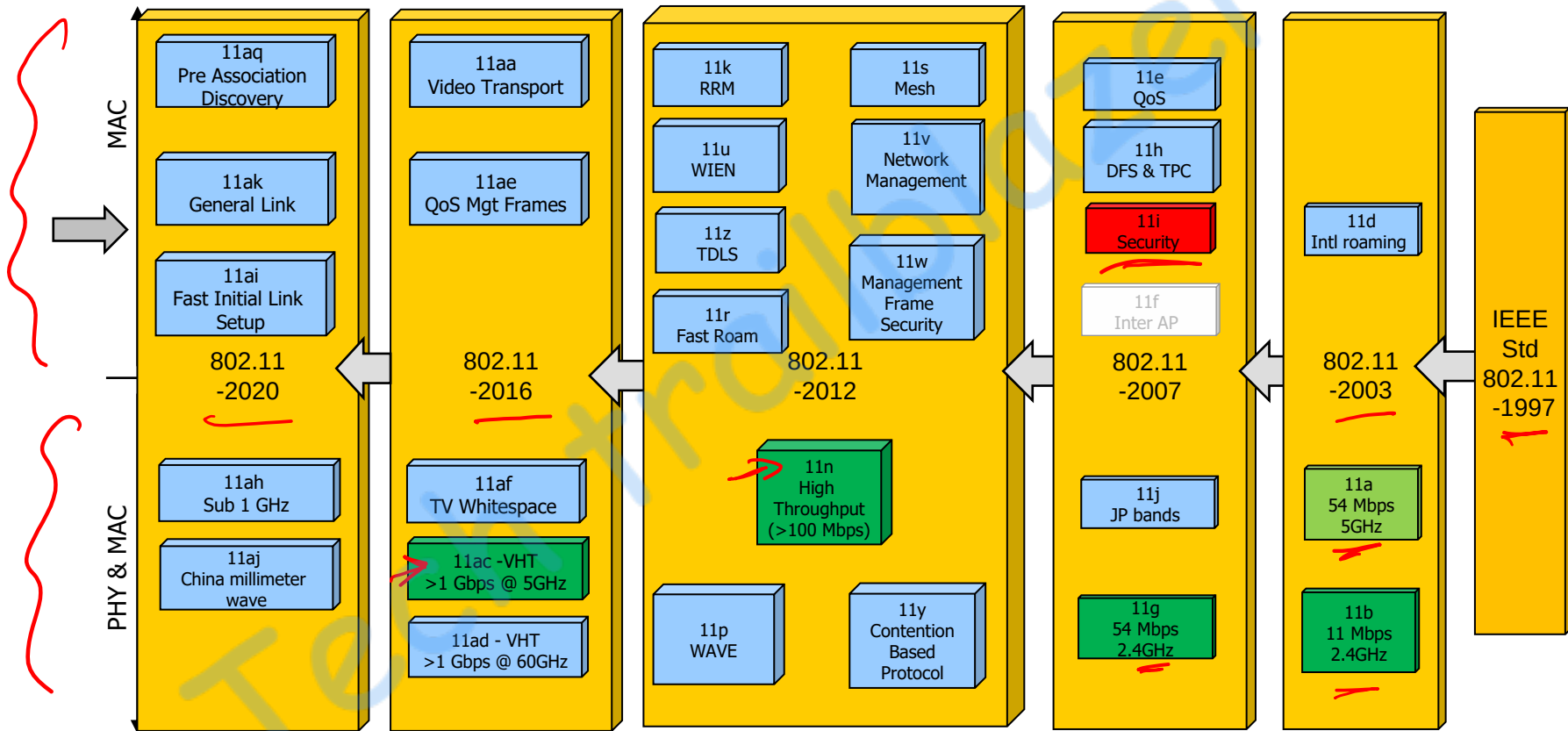
<https://www.ieee802.org/>

The IEEE 802.11 Working Group is one of the most active WGs in 802

- The 802.11 Working Group was established in 1990.
- Focus on **link and physical layers** of the network stack
- Leverage IETF protocols for upper layers



Development of the IEEE 802.11 Standard is ongoing since 1997



IEEE802.11 Wi-Fi standard evolution: 802.11be is under development

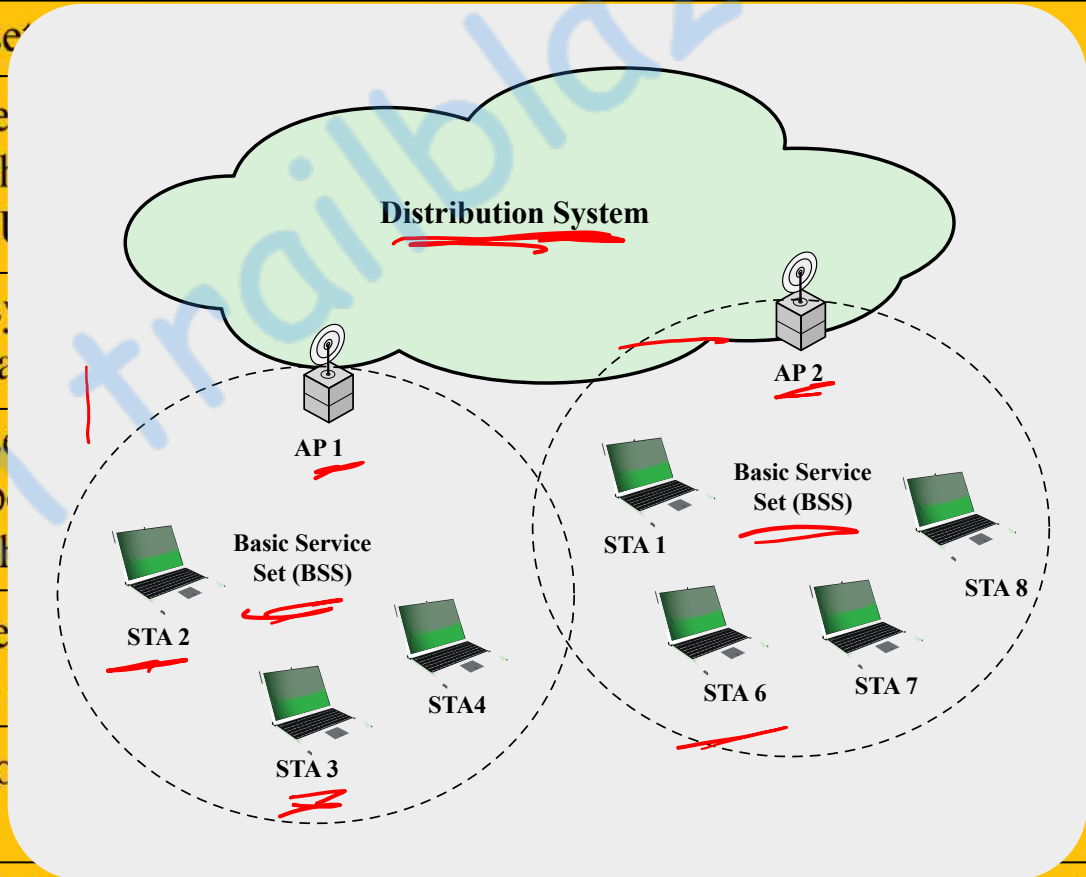
802.11n (2009) <u>Wi-Fi 4</u>	802.11ac (2013) <u>Wi-Fi 5</u>	802.11ax (2021) <u>Wi-Fi 6 E</u>	802.11be (est. 2024) <u>Wi-Fi 7</u>
2.4GHz and 5GHz supported - Wider channels (40MHz) - Better modulation (64-QAM) - Additional streams (Up to 4) - Backward compatibility with 11a/b/g - Standard supports up to 600Mbps	5GHz only - Wider channels (80, 160MHz) - Better modulation (256-QAM) - Additional streams (Up to 8, implemented up to 4) - Backward compatibility with 11a/b/g/n - Standard supports up to 7Gbps	2.4GHz, 5GHz and 6GHz supported - Wider channels (80, 160MHz) - Better modulation (1024-QAM) - Additional streams (Up to 8, implemented) - Backward compatibility with 11a/b/g/n/ac - Standard supports up to 9.6Gbps	2.4GHz, 5GHz and 6GHz supported - Wider channels (40, 80, 160, 240, 320MHz) - Better modulation (4096-QAM) - Backward compatibility with 11a/b/g/n/ac/ax - Throughput minimum of 30Gbps, expect 40Gbps+ - Low latency features - Draft 2.0 now in Working Group Ballot

(Ratification date) Products available in the market typically ~2 years prior

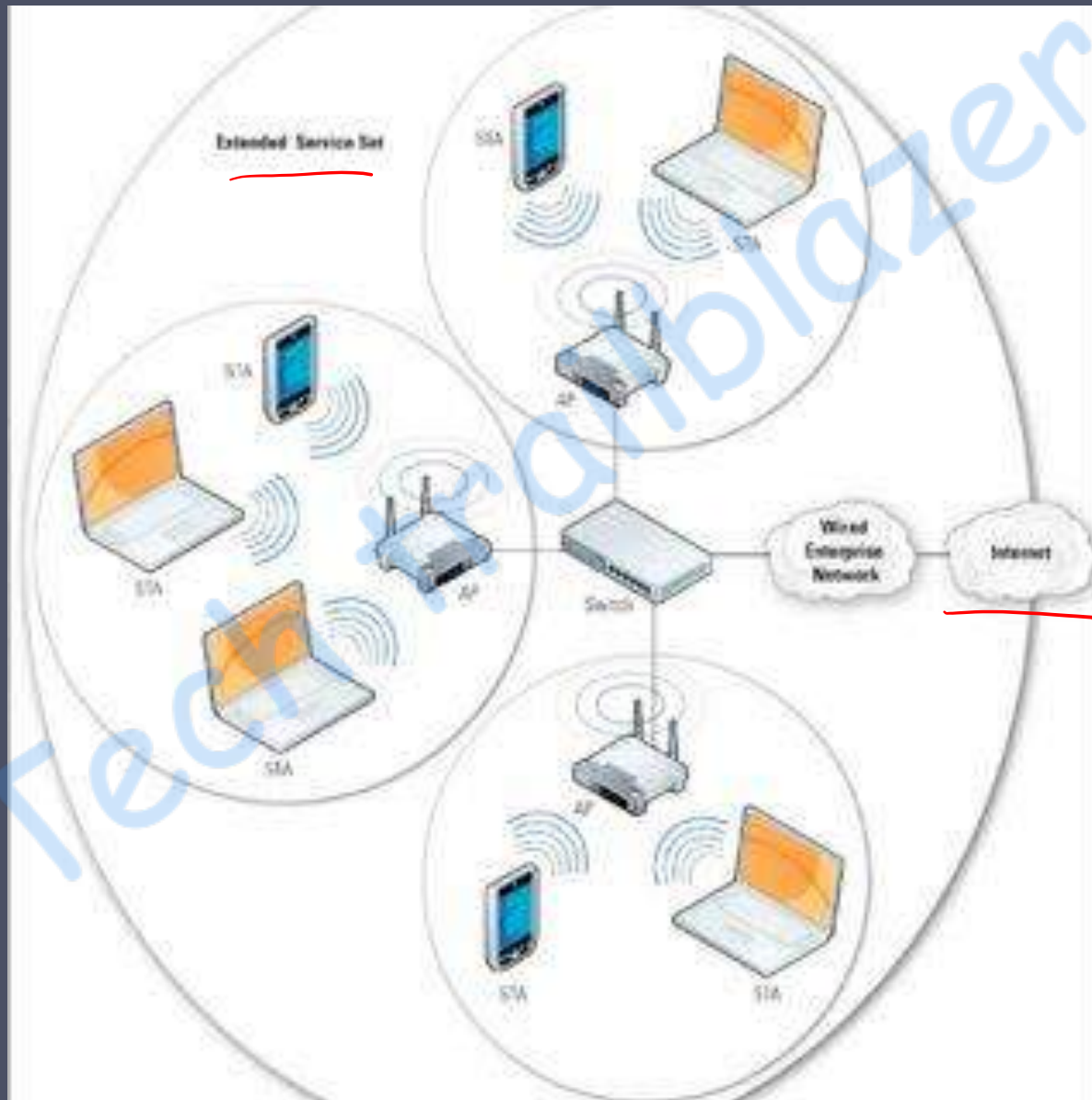
IEEE 802.11 Terminology

IEEE 802.11 Terminology

<u>Access point (AP)</u>	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
<u>Basic service set (BSS)</u>	A set of stations that share the same channel and are able to communicate with each other.
<u>Coordination function</u>	The function performed by the AP to coordinate the access of stations to the distribution system.
<u>Distribution system (DS)</u>	A system that interconnects one or more BSSs and enables them to exchange management frames and data frames.
<u>Extended service set (ESS)</u>	A set of one or more BSSs that share a common system identifier (SSID) and are managed by a single entity.
<u>MAC protocol data unit (MPDU)</u>	The unit of data that is transferred between stations and between a station and an AP.
<u>MAC service data unit (MSDU)</u>	The unit of data that is transferred between stations and between a station and an AP, before it is encapsulated in an MPDU.
<u>Station</u>	Any device that contains an IEEE 802.11 conformant MAC and physical layer.



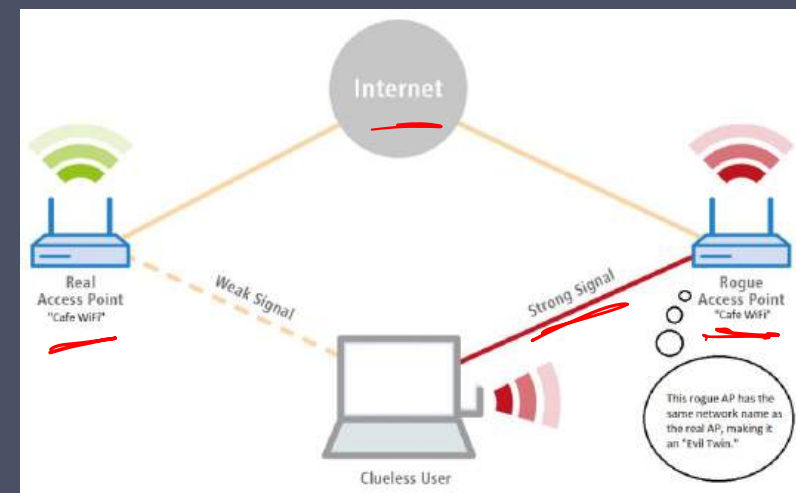
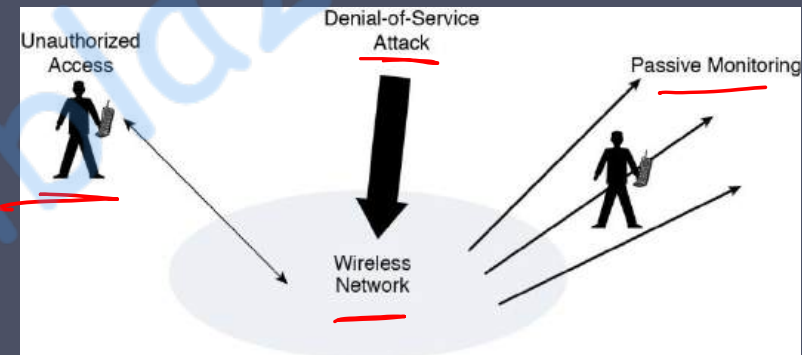
IEEE 802.11 Extended Service Set Example



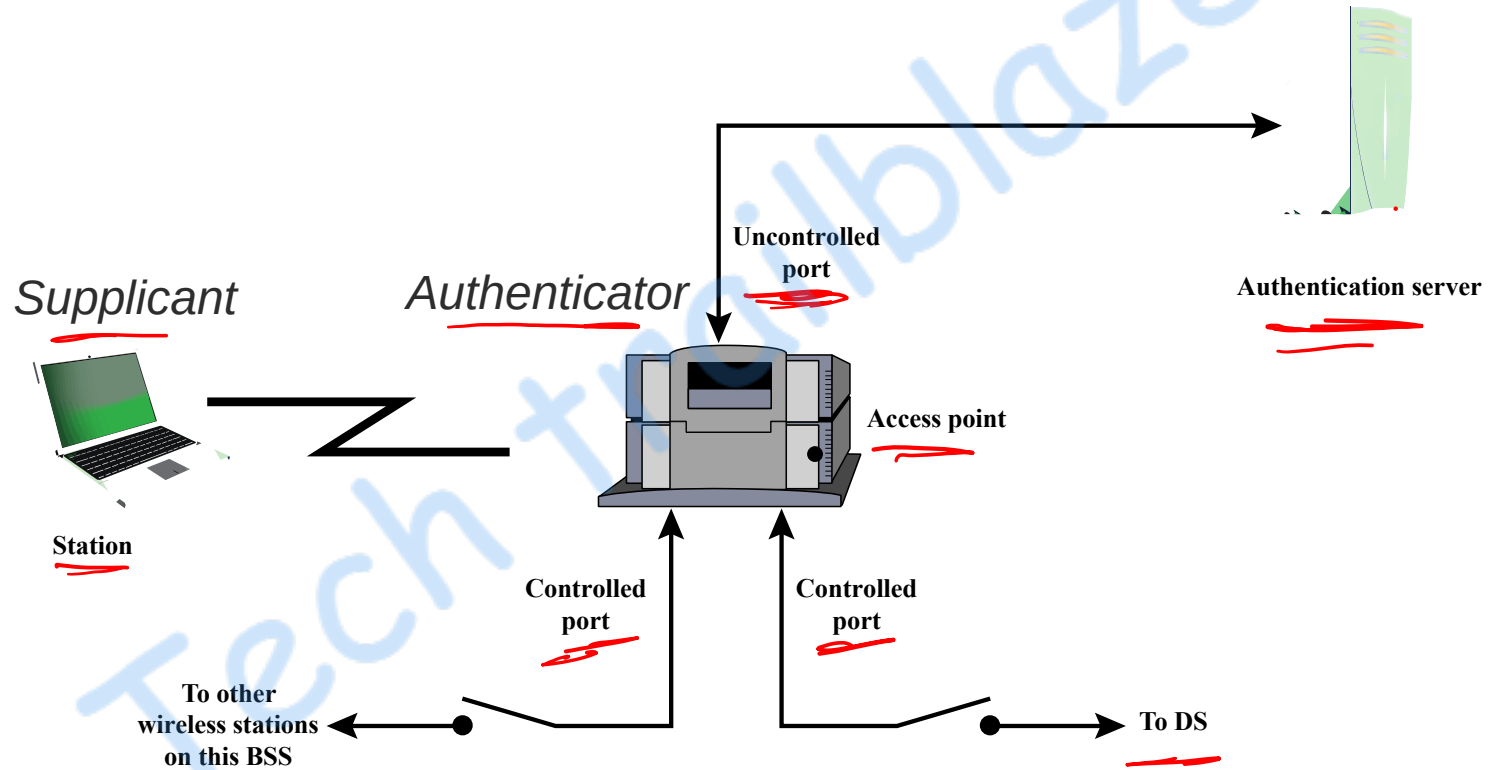
IEEE 802.1x Standard

Securing Wireless Networks

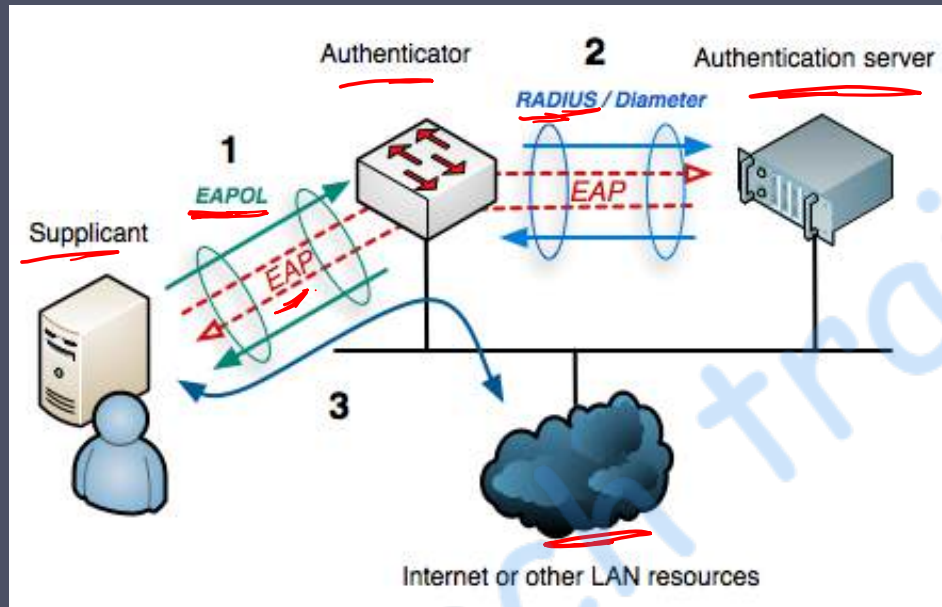
- The main threat involving wireless access points is unauthorized access to the network
- Principal approach for preventing such access is the IEEE 802.1X standard for port-based network access control
 - The standard provides an authentication mechanism for devices wishing to attach to a LAN or wireless network
- Use of 802.1X can prevent rogue access points and other unauthorized devices from becoming insecure backdoors



802.1X Access Control



IEEE 802.1X standard for Securing Wired/Wireless Networks



Extensible Authentication Protocol (EAP) originally designed for Point-to-Point Protocol (PPP)

EAPoL (EAP over LAN)

EAPoW (EAP over Wireless)

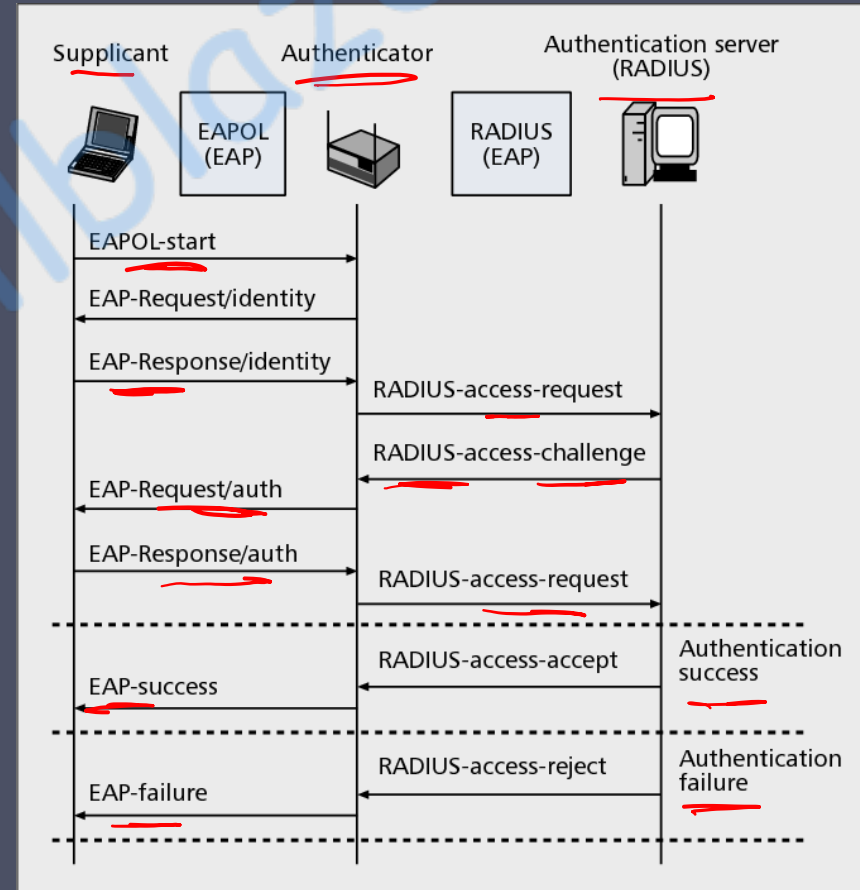


FIGURE 4. A typical 802.1x message flow.

Wireless Fidelity (Wi-Fi) Alliance

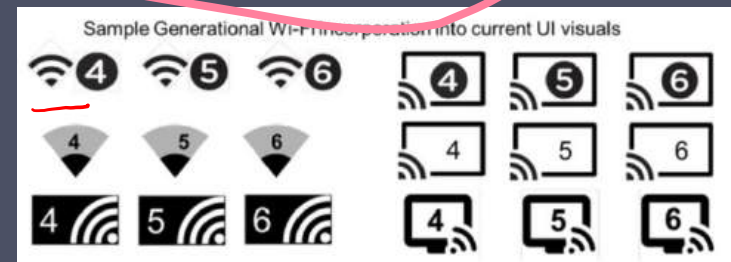
Wireless Fidelity (Wi-Fi) Alliance

<https://www.wi-fi.org/>

- The Wi-Fi Alliance is a non-profit organization that owns the Wi-Fi trademark.
 - Manufacturers may use the trademark to brand products certified for Wi-Fi interoperability.
- 802.11b
 - First 802.11 standard to gain broad industry acceptance
- Wireless Ethernet Compatibility Alliance (WECA)
 - Industry consortium formed in 1999 to address the concern of products from different vendors successfully interoperating
 - Later renamed the Wi-Fi Alliance in 2002
- Term used for certified 802.11b products is Wi-Fi in 1999
- In 2018, the Wi-Fi Alliance introduced simplified Wi-Fi generational numbering to indicate supported 802.11 standard by the equipment e.g.
- Other programs
 - Wi-Fi Direct: In October 2010, the Alliance began to certify Wi-Fi Direct Wi-Fi Easy Connect protocol via QR Code
 - Wi-Fi Passpoint : Wi-Fi Passpoint, alternatively known as Hotspot 2.0 and may others...



Year	WiFi Versions/Protocols	Old name	New name
1999	First Generation	WiFi 802.11b	WiFi 1
1999	Second Generation	WiFi 802.11a	WiFi 2
2003	Third Generation	WiFi 802.11g	WiFi 3
2009	Four Generation	WiFi 802.11n	WiFi 4
2014	Fifth Generation	WiFi 802.11ac	WiFi 5
2019	Sixth Generation	WiFi 802.11ax	WiFi 6

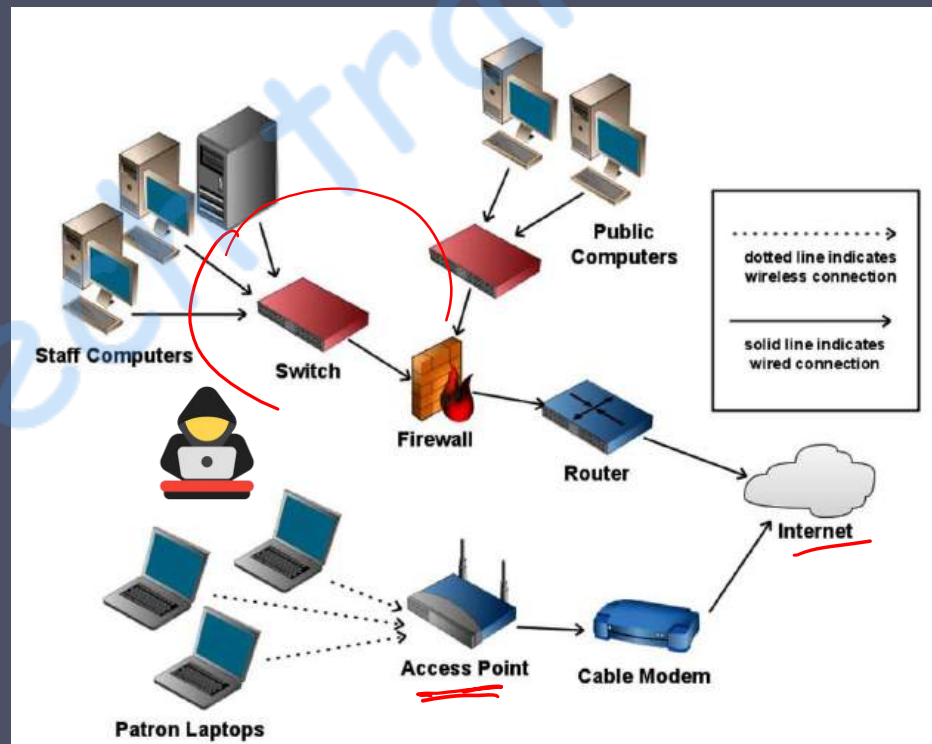


Demo Wi-Fi Info...

Wireless LAN Security

Wireless LAN Security

- There are two characteristics of a wired LAN that are not inherent in a wireless LAN.
 - In order to transmit over a wired LAN, a station must be physically connected to the LAN, which is not the case in Wireless...
 - Similarly, in order to receive a transmission from a station that is part of a wired LAN, the receiving station also must be attached to the wired LAN, which is not the case in Wireless...



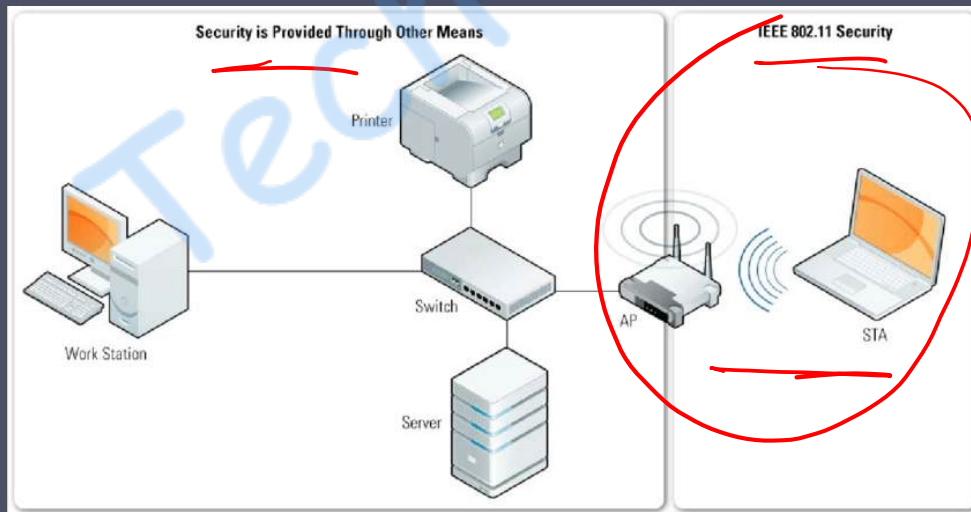
Wireless LAN Security

- The following security measures are often considered as trivial solutions for risk mitigation:
 - Disable the SSID broadcast
 - Maintain a list of authorized MAC addresses and block unauthorized ones from the network
 - Select AP locations in the middle of the building (not close to windows), use  directional antennas and line walls and windows with metal foil to minimize the signal leakage to the outside of the building
- How much security do these measures bring?
- Need something more...real security solutions

Demo AP Setting...

Wireless LAN Security

- The original 802.11 specification included a set of security features for privacy and authentication that were quite weak.
 - For privacy, 802.11 defined the Wired Equivalent Privacy (WEP) algorithm.
 - The privacy portion of the 802.11 standard contained major weaknesses.
- Subsequently, the 802.11i task group has developed a set of capabilities to address the WLAN security issues. In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.
 - WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the trimmed down version of 802.11i standard.
- The final form of the 802.11i standard is referred to as Robust Security Network (RSN).
 - The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.



Demo Wi-Fi Info...

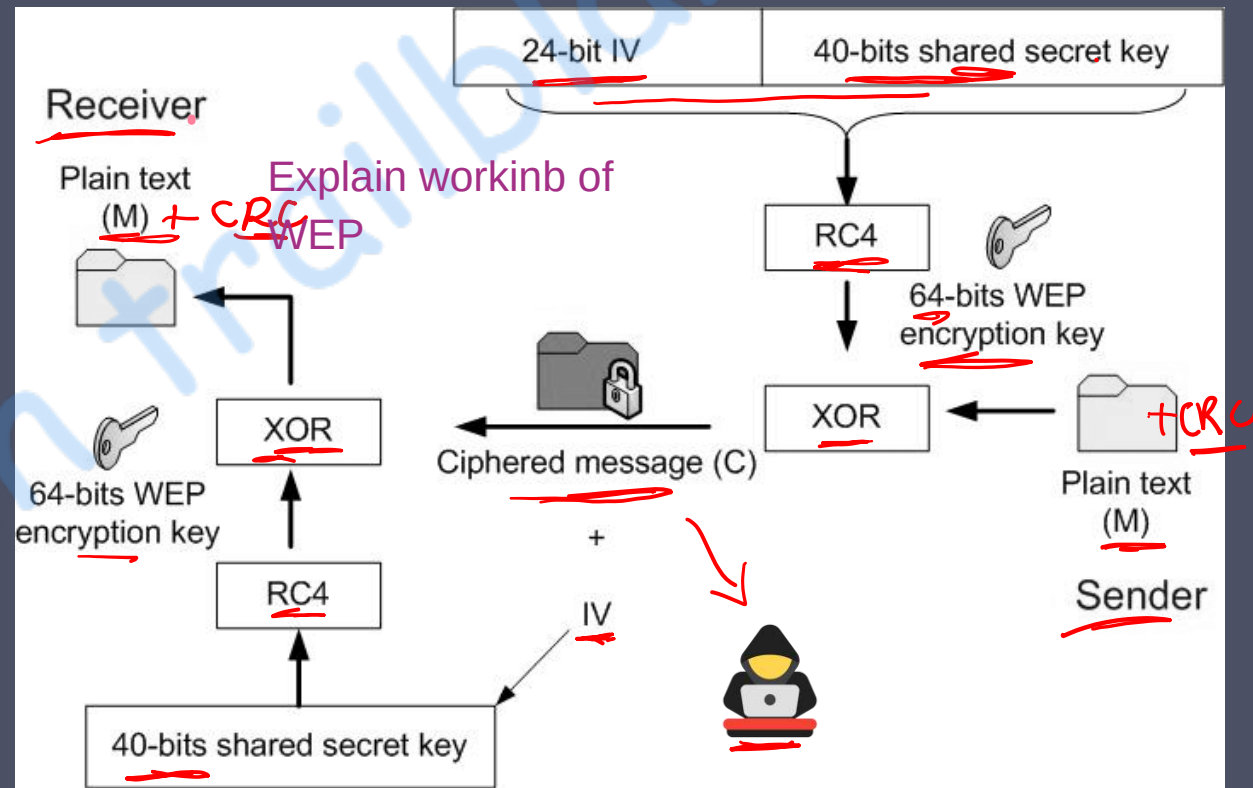
Wired Equivalent Privacy (WEP) Algorithm

Wired Equivalent Privacy (WEP) Algorithm

WEP was part of the IEEE 802.11 standard ratified in 1997.

Provide Support for

- Authentication ✓
- Confidentiality ✓
- Integrity ✓



WEP is notoriously weak...

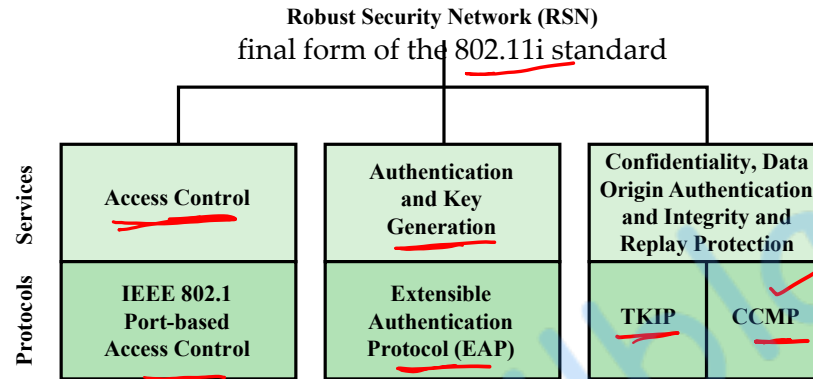
Wi-Fi Protected Access (WPA)

Brief History of Wi-Fi Protected Access (WPA)

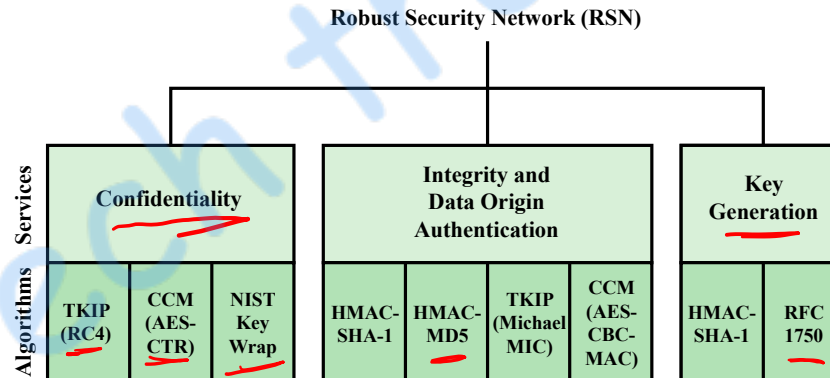
- As WEP was not secure...
- Subsequently, the 802.11i task group has developed a set of capabilities to address the WLAN security issues.
 - In order to accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance promulgated Wi-Fi Protected Access (WPA) as a Wi-Fi standard.
- WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on trimmed down version of 802.11i standard...initially released in 2003.
 - No new/specialized equipment was required...just firmware update
 - Based on TKIP / CCMP for encryption
 - TKIP - Temporal Key Integrity Protocol (TKIP) ✓
 - CCMP - Counter mode CBC-MAC Protocol
- WPA2 is improved version of original WPA released in 2004.
 - Based on CCMP for encryption
- WPA3 comes as a successor to WPA2 - introduced in 2018
 - after July 2020, all Wi-Fi devices that are certified must support it.

WPA2

The Wi-Fi Alliance certifies vendors in compliance with the full 802.11i specification under the WPA2 program.



(a) Services and Protocols



(b) Cryptographic Algorithms

- CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
- CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
- CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
- TKIP = Temporal Key Integrity Protocol

Figure 24.6 Elements of IEEE 802.11i

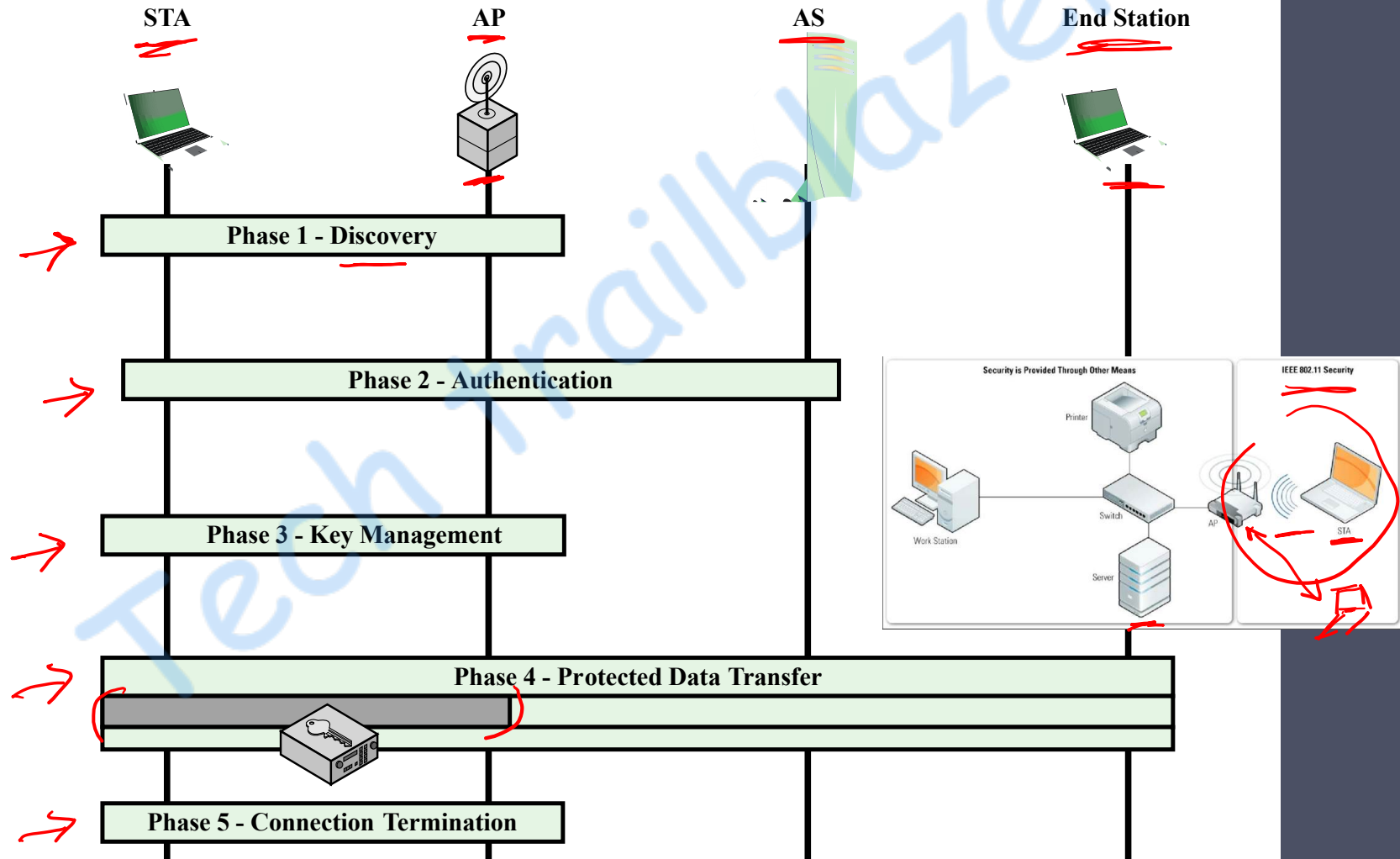
1009

IEEE 802.11i Standard

Phases of Operation

IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol



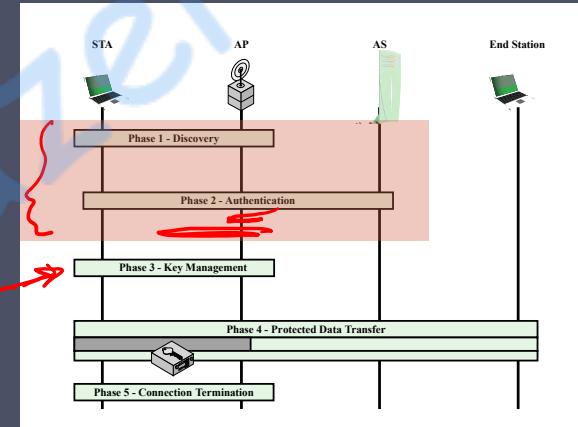
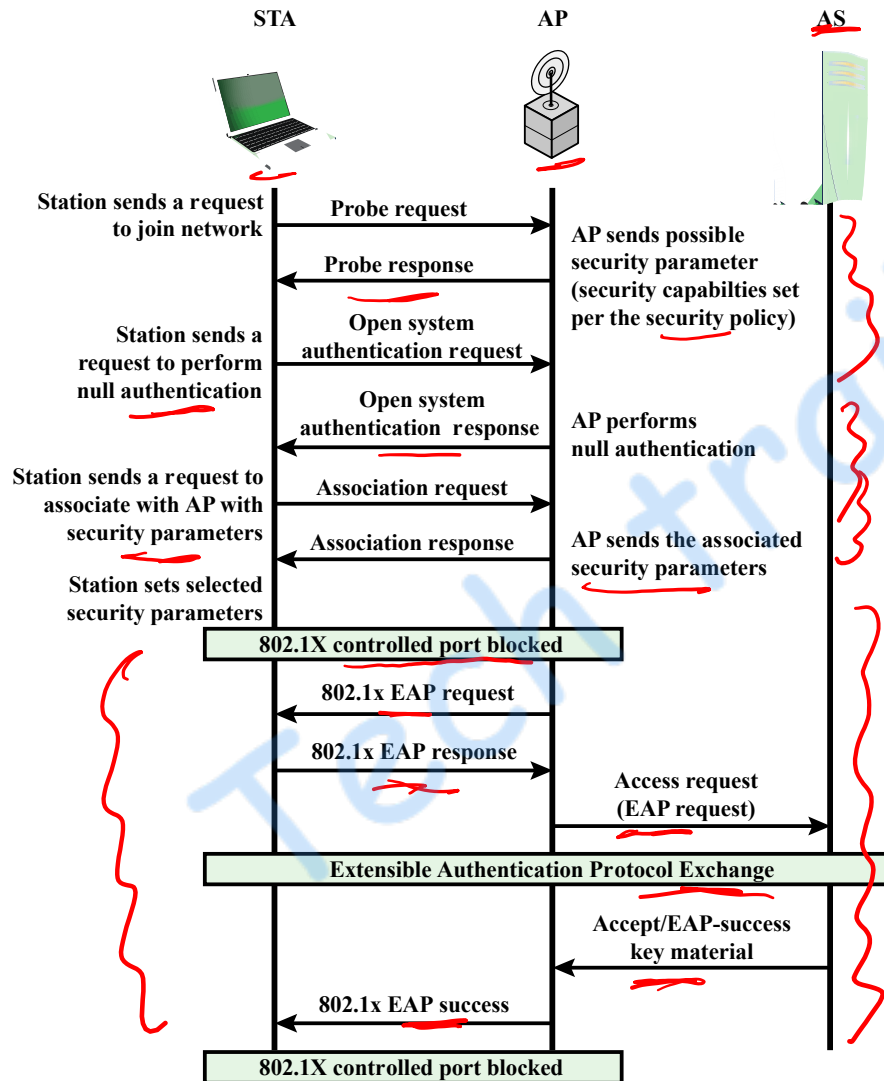
IEEE 802.11i Standard

Phases of Operation

 **Capability Discovery, Association, and Authentication**

IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol

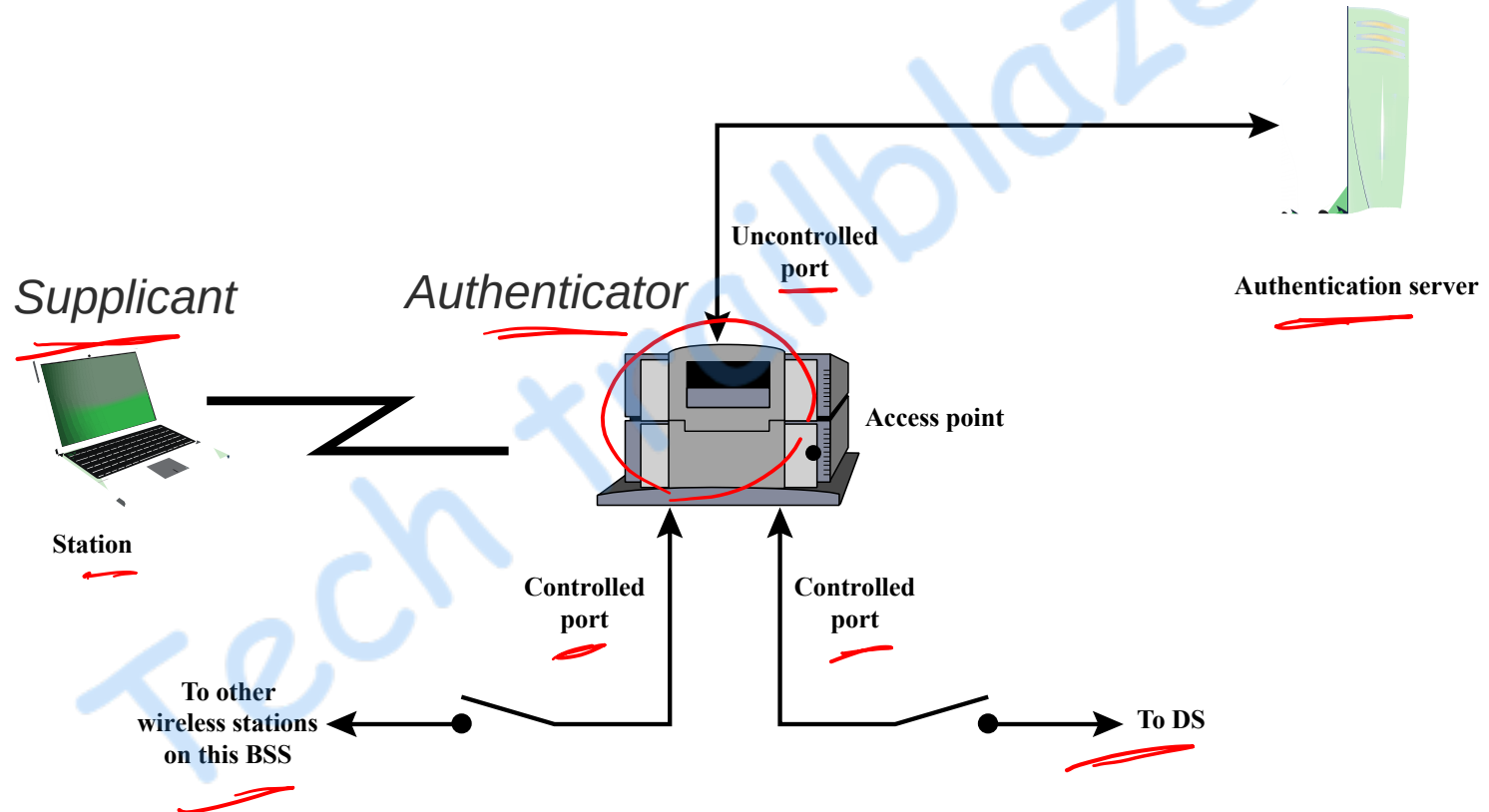


Capability Discovery, Association, and Authentication

Authentication phase consists of three phases:

- **Connect to AS**
 - The STA sends a request to its AS through AP
- **EAP exchange**
 - Authenticates the STA and AS to each other
- **Secure key delivery**
 - On success, the AS generates a Master Session Key and sends it to the STA

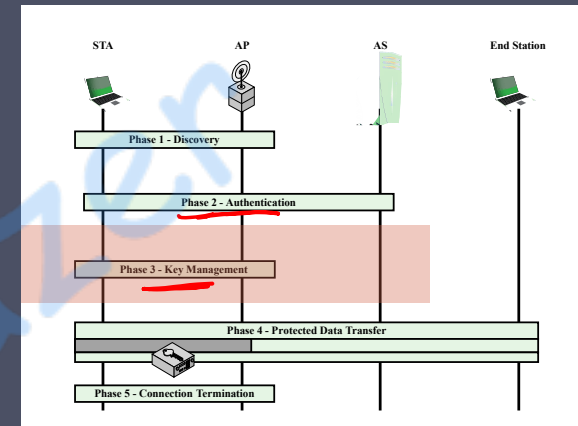
802.1X Access Control



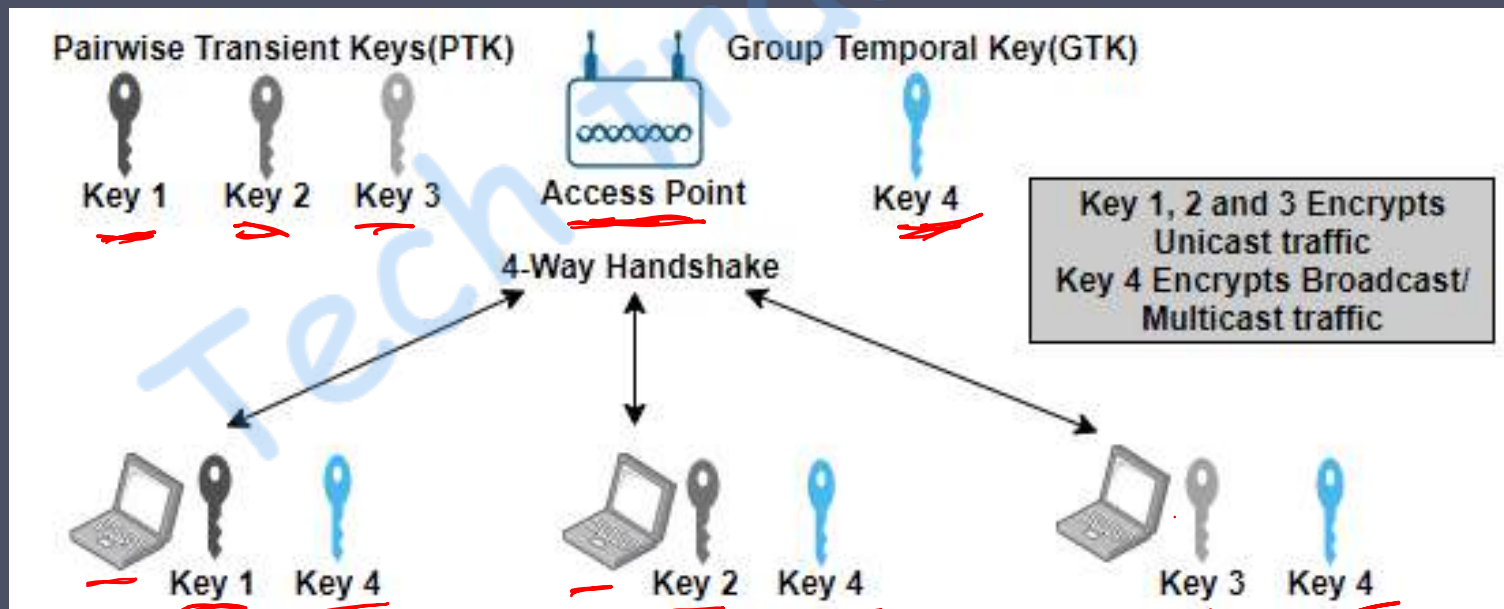
IEEE 802.11i

Key Hierarchies

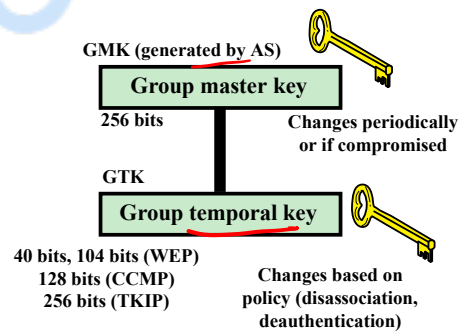
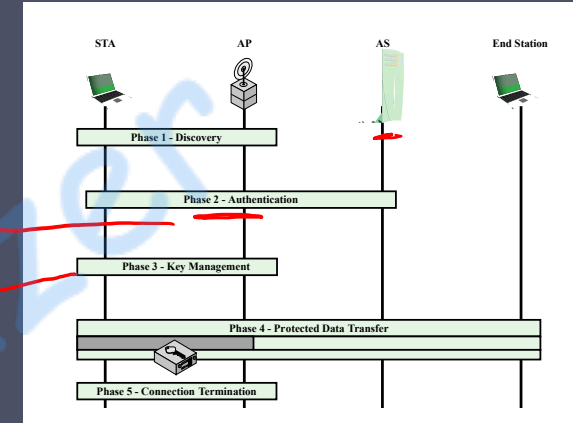
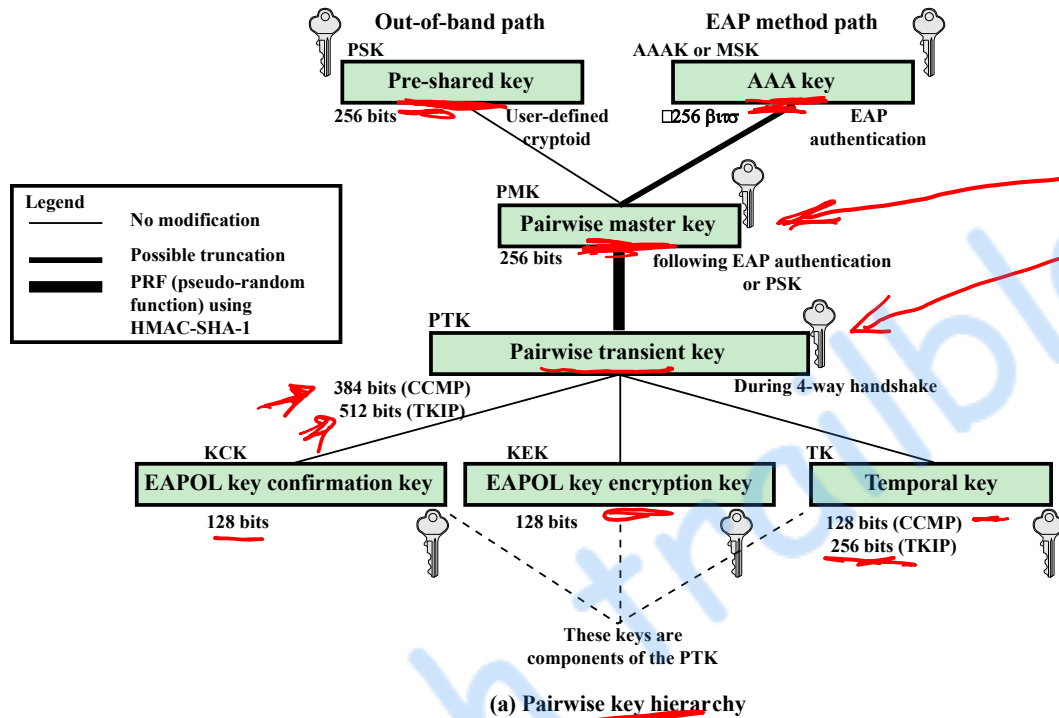
IEEE 802.11i Key Hierarchies



Pairwise keys and Group keys



IEEE 802.11i Key Hierarchies



(b) Group key hierarchy

Abbreviation	Name	Description / Purpose	Size (bits)	Type
<u>AAA Key</u>	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
<u>PSK</u>	Pre-Shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
<u>PMK</u>	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
<u>TK</u>	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
<u>GTK</u>	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

IEEE 802.11i

Keys for Data Confidentiality and Integrity Protocols

IEEE 802.11i Standard

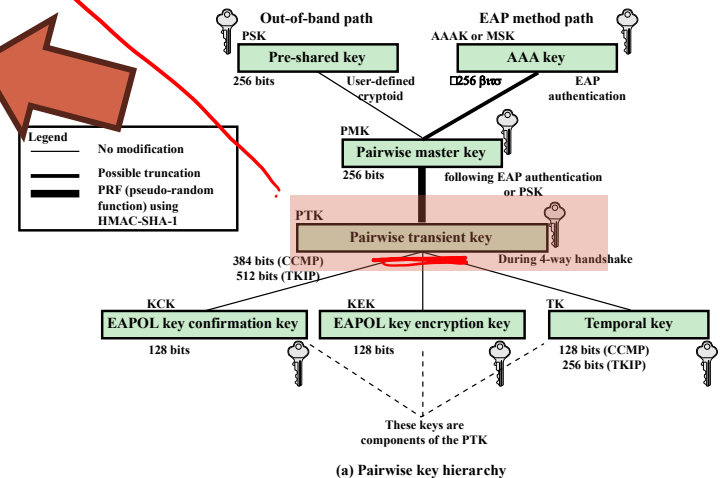
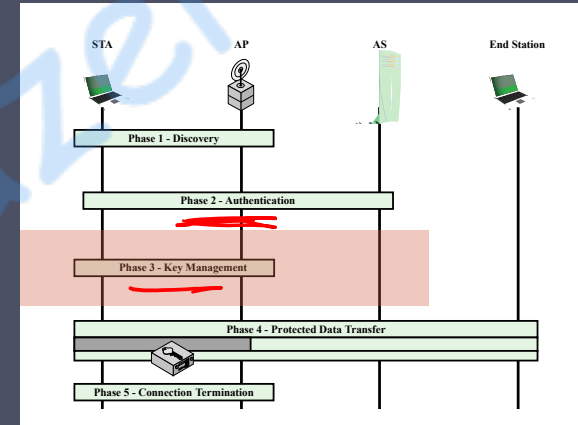
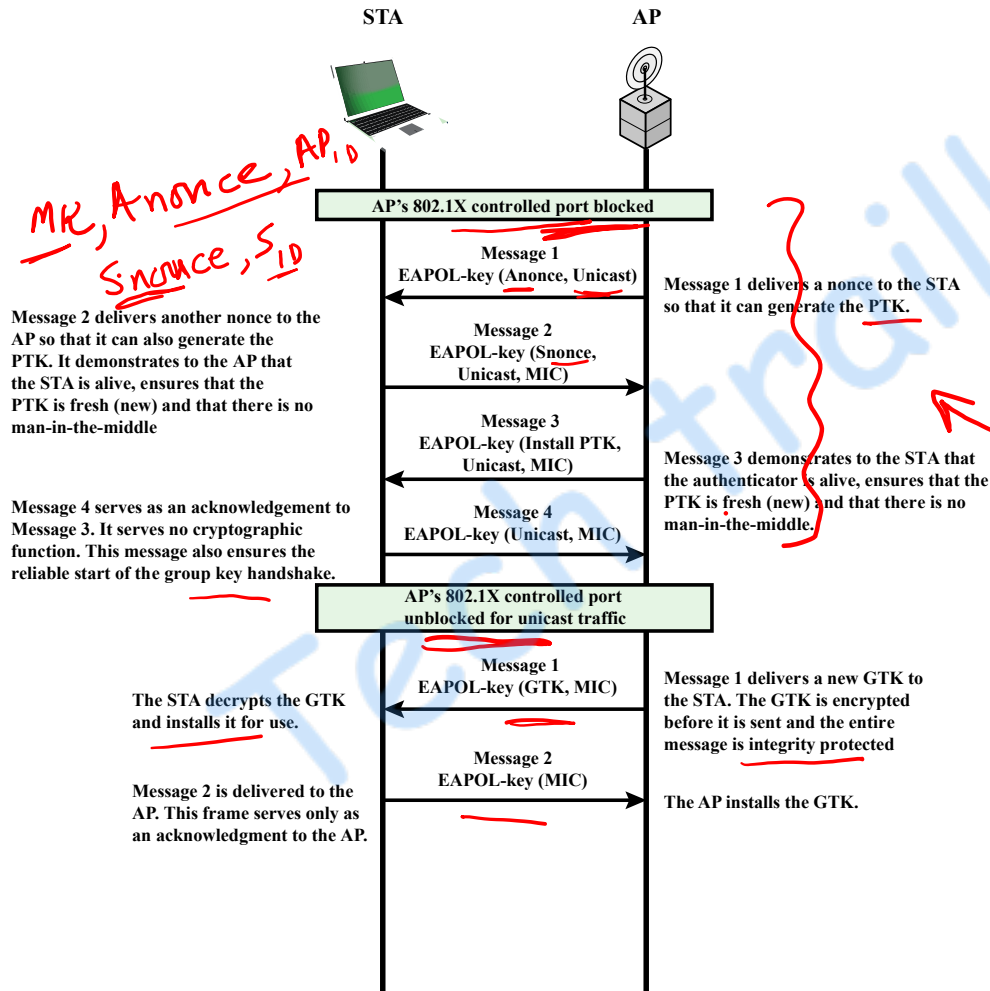
Phases of Operation

→ 4-Way Handshake and Group Key Handshake

IEEE 802.11i Phases of Operation

Essentially the working WPA2 protocol

4-Way Handshake and Group Key Handshake



About Strength of WPA2

- WPA2 ensures that data sent or received over your wireless network is encrypted,
 - only people with your network password have access to it.
- WPA2 use AES to replace the more vulnerable TKIP algorithm used in the original WPA protocol.
- WPA2 uses dynamic key encryption,
 - Regularly changes the key PTK and makes it more difficult to crack.
- However, Pre-Shared Key is derived from passphrase (Wif-Fi password)
 - This is common in Home networks... Enterprise networks use AS and are more safe...
- Weak Wif-Fi passwords can easily be cracked
 - All you need is to capture 4-way handshake exchange messages "airodump-ng"
 - Then use offline dictionary attacks...to crack the password "aircrack-ng"
- That's why we have WPA3 coming as a successor to WPA2...

Buffer Overflow Attacks

important for long short and
mcqs

A Brief History of Some Buffer Overflow Attacks

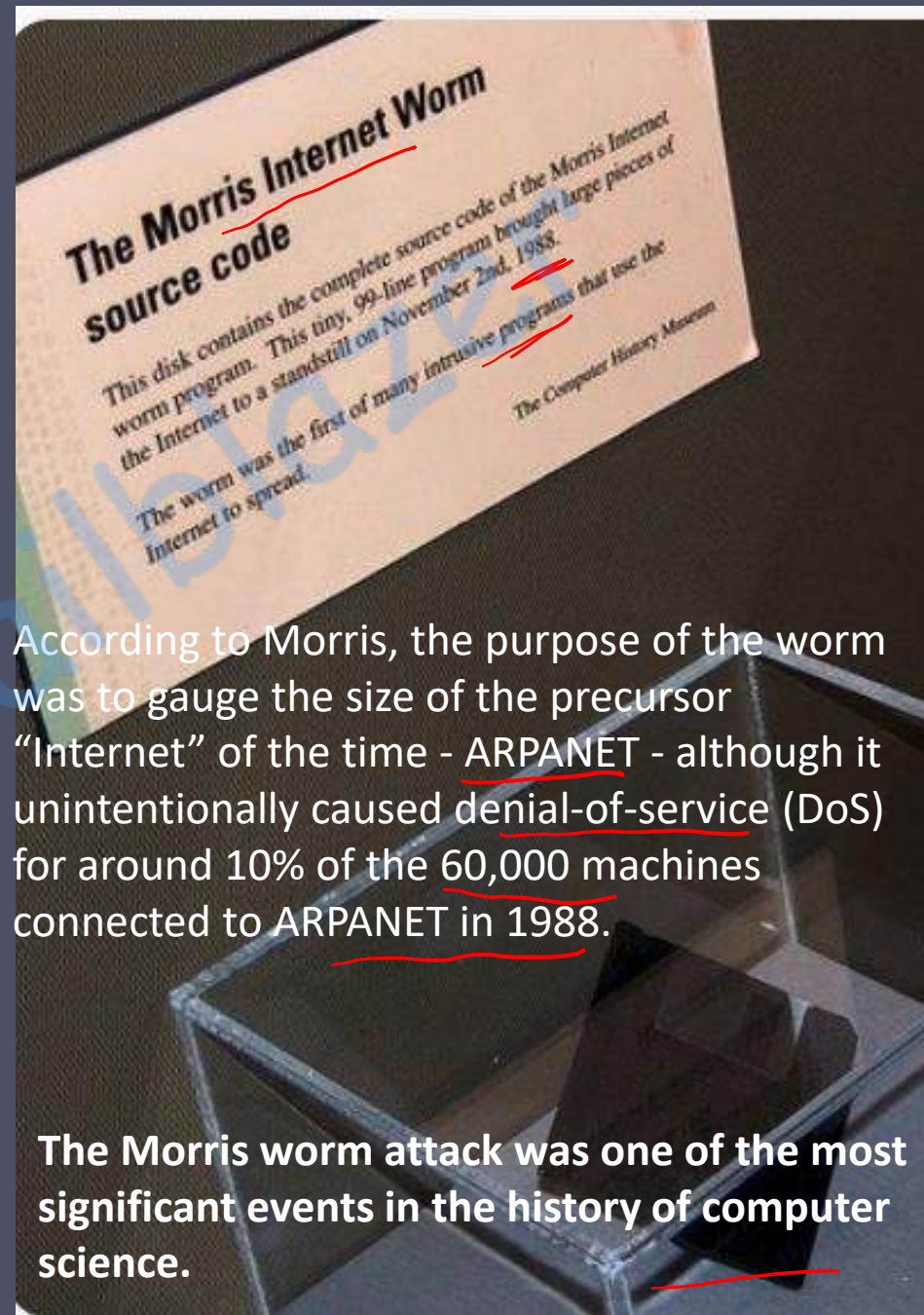
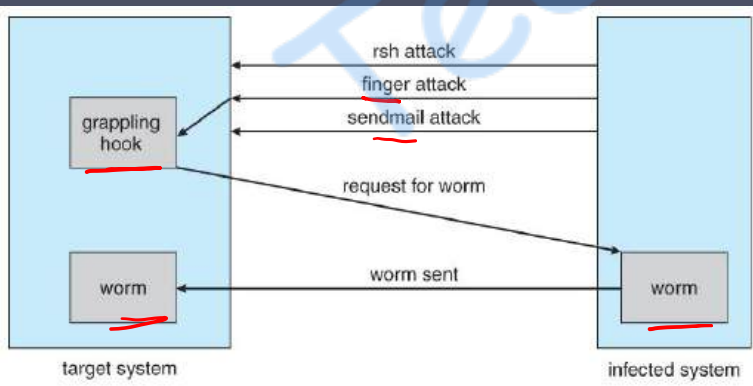
...



Robert Tappan Morris

The Morris worm functioned as a denial-of-service (DoS) attack.

The Morris worm spread by exploiting vulnerabilities in UNIX sendmail (using a backdoor), finger (through buffer overflow), and rsh/rexec (to explore whether it could operate).



According to Morris, the purpose of the worm was to gauge the size of the precursor “Internet” of the time - ARPANET - although it unintentionally caused denial-of-service (DoS) for around 10% of the 60,000 machines connected to ARPANET in 1988.

The Morris worm attack was one of the most significant events in the history of computer science.



mcq
s

Code Red was a computer worm observed on the Internet on July 15, 2001.

This worm targeted Windows-based systems with Microsoft IIS (Internet Information Services for Windows Server) installed exploiting buffer overflow.

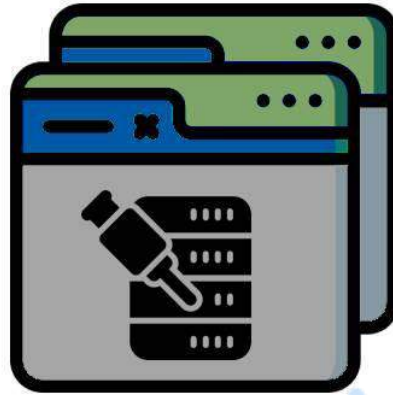
The Code Red worm has three phases

- Discovery and propagation... between day 1 and day 19 of any month ✓
- Attack ...between day 20 and day 27 of any month... DDoS attack on White House Web site
- Dormancy...From day 28 to the end of the month

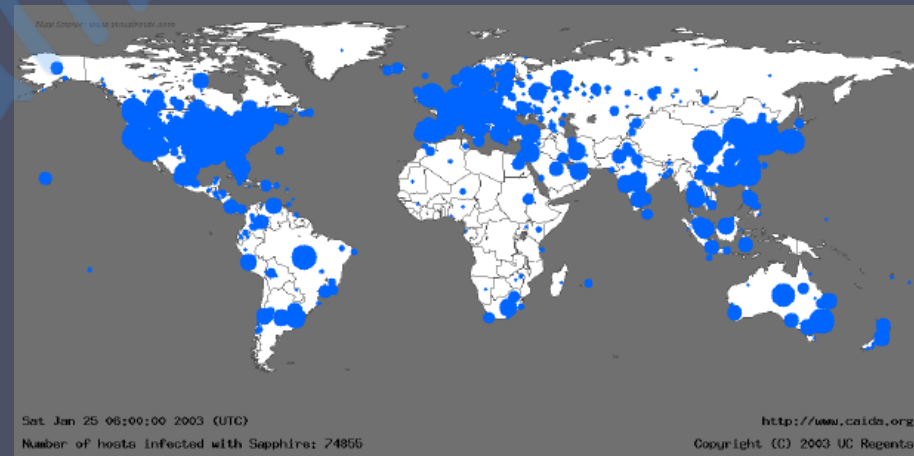
The front page of an infected server might have been changed by the worm to following:



SQL Slammer Virus Attack



SQL Slammer is a 2003 computer worm that caused a denial of service on some Internet hosts and dramatically slowed general Internet traffic and crashing routers all around the world. It spread rapidly, infecting most of its 75,000 victims within 10 minutes.



Slammer exploited a buffer overflow vulnerability in Microsoft SQL server 2000 in order to propagate.



Buffer overflow vulnerability in WhatsApp

On May 14, 2019, a buffer overflow vulnerability was identified in WhatsApp.

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to a boundary error within the WhatsApp VOIP stack when processing SRTCP packets.

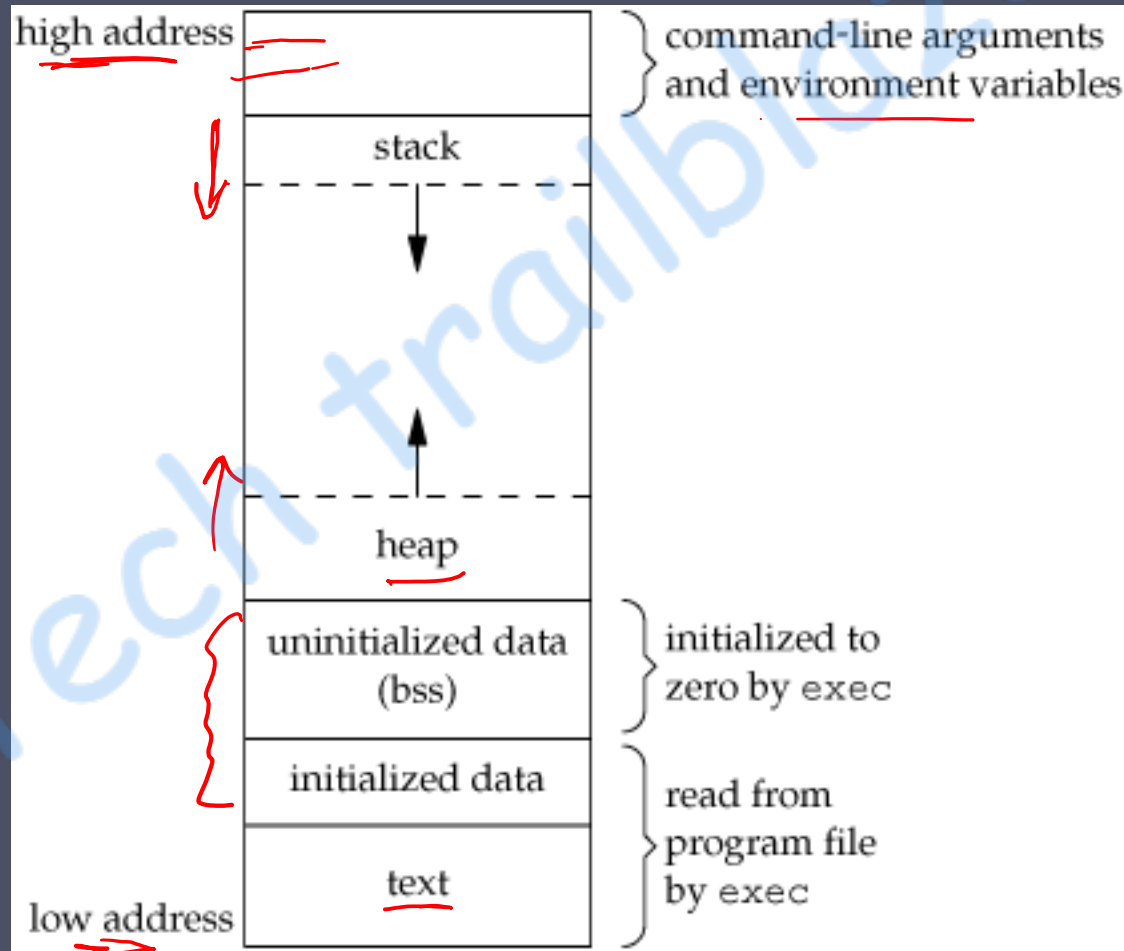
→ A remote attacker can send a series of specially crafted SRTCP packets sent to a target phone number, trigger buffer overflow and execute arbitrary code on the target device.

Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.

✓
https://www.whatsapp.com/security/advisories/archive?lang=en_US

Program Memory Layout and Stack Buffer

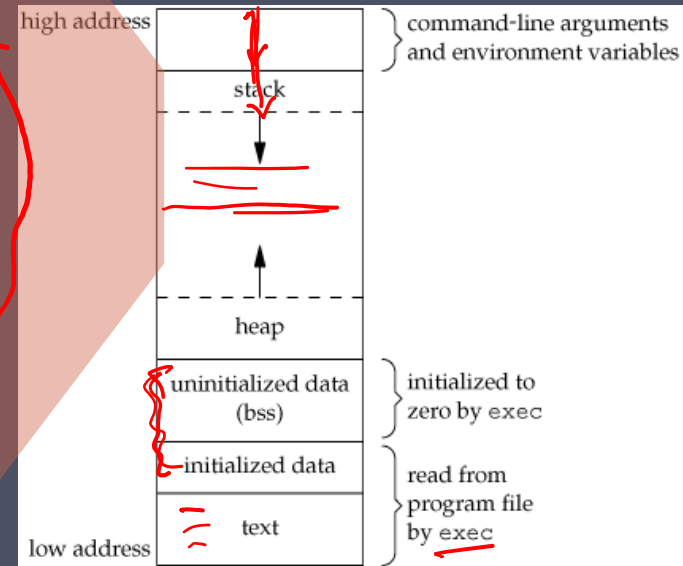
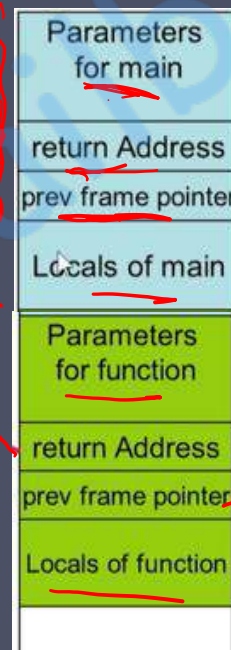
Memory Layout of a C Program



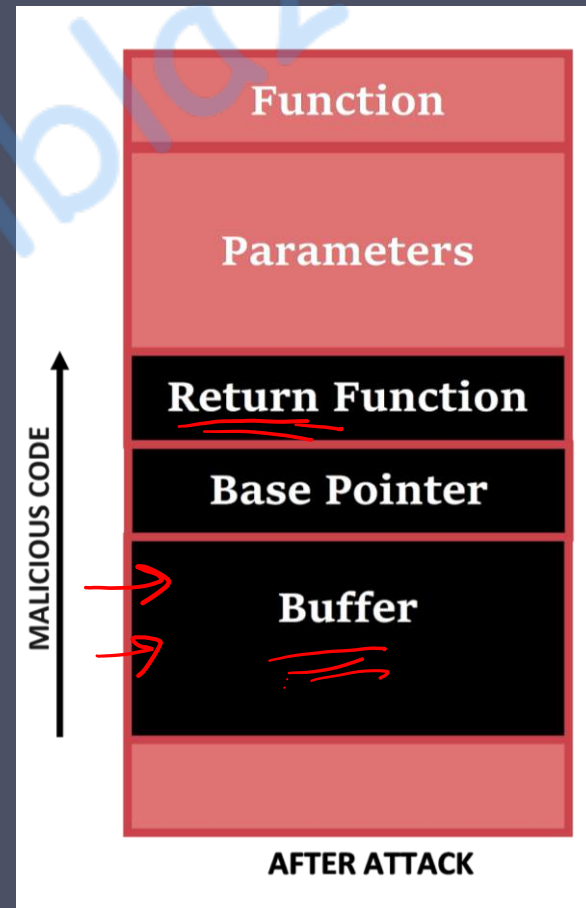
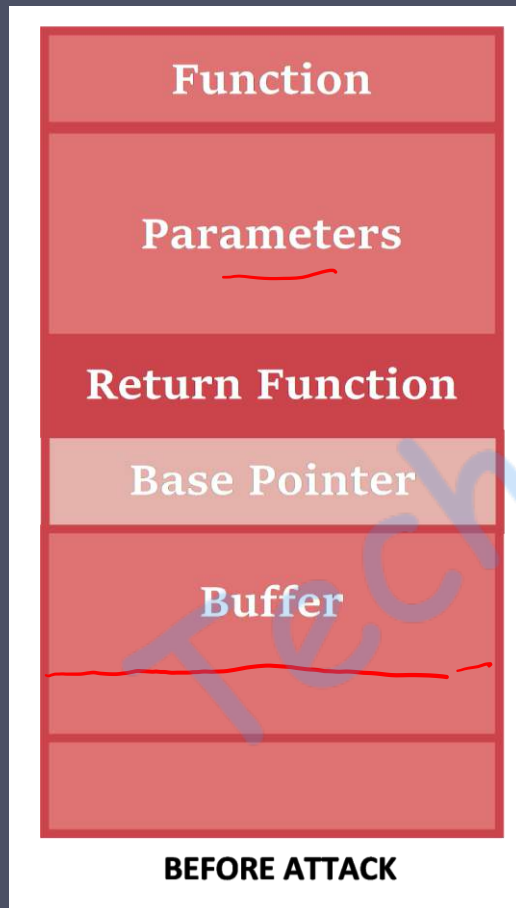
Stack in Program

(when functions are executing)

```
void function(int a, int b, int c){  
    char buffer1[5];  
    char buffer2[10];  
}  
  
int main(int argc, char **argv){  
    function(1,2,3);  
}
```



Buffer Overflow Attack



Buffer Overflow Attack

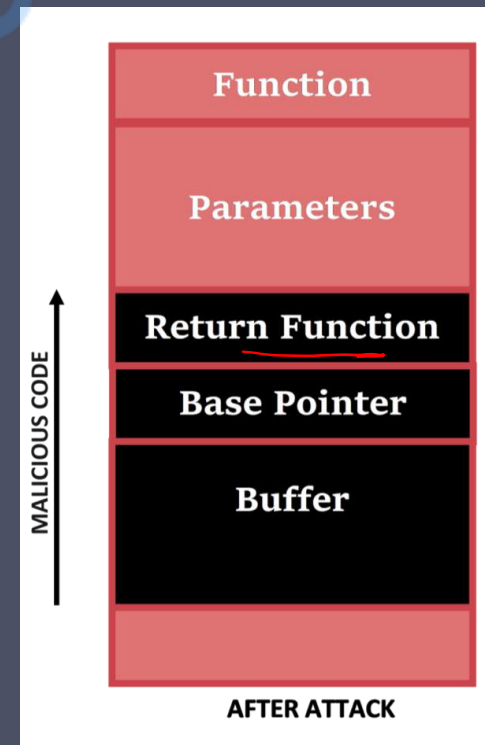
Buffer Overflow Attack

- A very common attack mechanism
 - First widely used by the Morris Worm in 1988
- Prevention techniques known
- Still of major concern
 - Legacy of buggy code in widely deployed operating systems and applications
 - Continued careless programming practices by programmers

Buffer Overflow

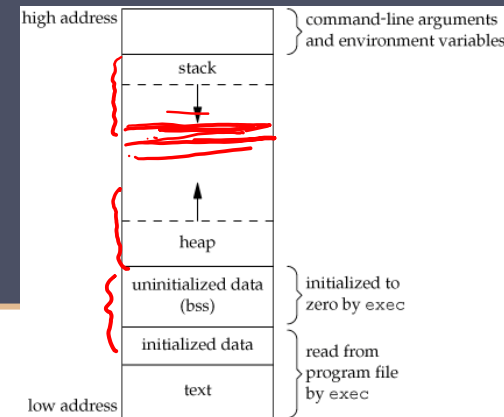
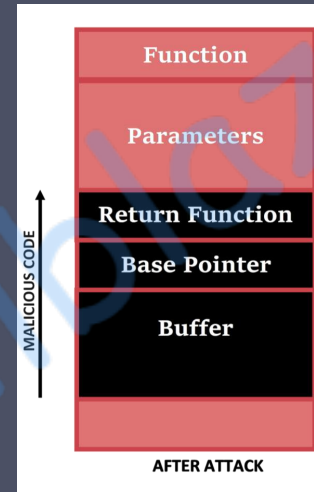
A buffer overflow, also known as a buffer overrun, is defined in the NIST *Glossary of Key Information Security Terms* as follows:

“A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.”



Buffer Overflow Basics

- Programming error when a process attempts to store data beyond the limits of a fixed-sized buffer
- Overwrites adjacent memory locations
 - Locations could hold other program variables, parameters, or program control flow data
- Buffer could be located on the stack, in the heap, or in the data section of the process



Consequences:

- Corruption of program data
- Unexpected transfer of control
- Memory access violations
- Execution of code chosen by attacker

Buffer Overflow Attacks

- To exploit a buffer overflow an attacker needs:
 - To identify a buffer overflow vulnerability in some program that can be triggered using externally sourced data under the attacker's control
 - To understand how that buffer is stored in memory and determine potential for corruption
- Identifying vulnerable programs can be done by:
 - Inspection of program source
 - Tracing the execution of programs as they process oversized input
 - Using tools such as fuzzing to automatically identify potentially vulnerable programs

[Buffer Overflows Made Easy - YouTube](#)

By The Cyber Mentor

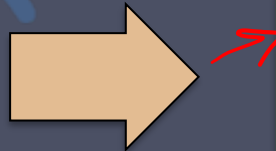
Role of Programming Language in Handling Buffer Overflow Attacks

Programming Language

- At the machine level data manipulated by machine instructions executed by the computer processor are stored in either the processor's registers or in memory
- Assembly language programmer is responsible for the correct interpretation of any saved data value

Modern high-level languages have a strong notion of type and valid operations

- Not vulnerable to buffer overflows
- Does incur overhead, some limits on use



C and related languages have high-level control structures, but allow direct access to memory

- Hence are vulnerable to buffer overflow
- Have a large legacy of widely used, unsafe, and hence vulnerable code

Basic Buffer Overflow Example

```
int main(int argc, char *argv[]) {  
    int valid = FALSE;  
    char str1[8];  
    char str2[8];  
  
    next_tag(str1);  
    gets(str2);  
    if (strncmp(str1, str2, 8) == 0)  
        valid = TRUE;  
    printf("buffer1: str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);  
}
```

(a) Basic buffer overflow C code

```
$ cc -g -o buffer1 buffer1.c  
$ ./buffer1  
START  
buffer1: str1(START), str2(START), valid(1)  
$ ./buffer1  
EVILINPUTVALUE  
buffer1: str1(TVALUE), str2(EVILINPUTVALUE), valid(0)  
$ ./buffer1  
BADINPUTBADINPUT  
buffer1: str1(BADINPUT), str2(BADINPUTBADINPUT), valid(1)
```

(b) Basic buffer overflow example runs

Parameters
for main

return Address
prev frame pointer

Locals of main

Memory Address Before gets(str2) After gets(str2) Contains Value of

....			
<u>bffffbf4</u>	34fcffbf 4...	34fcffbf 3...	<u>argv</u>
<u>bffffbf0</u>	01000000	01000000	<u>argc</u>
			
<u>bffffbec</u>	c6bd0340 ... @	c6bd0340 ... @	<u>return addr</u>
<u>bffffbe8</u>	08fcffbf	08fcffbf	<u>old base ptr</u>
<u>bffffbe4</u>	00000000	01000000	<u>valid</u>
<u>bffffbe0</u>	80640140 . d . @	00640140 . d . @	
<u>bffffbdc</u>	54001540 T .. @	4e505554 N P U T	<u>str1[4-7]</u>
<u>bffffbd8</u>	53544152 S T A R	42414449 B A D I	<u>str1[0-3]</u>
<u>bffffbd4</u>	00850408	4e505554 N P U T	<u>str2[4-7]</u>
<u>bffffbd0</u>	30561540 0 V . @	42414449 B A D I	<u>str2[0-3]</u>
....			

Some Common Unsafe C Standard Library Routines

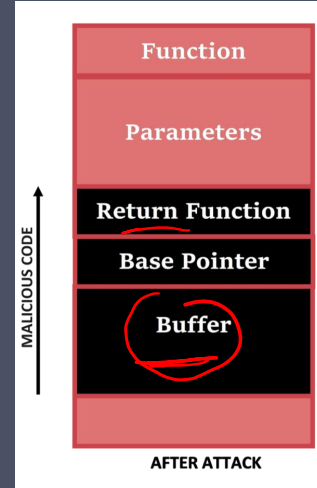
<code>gets(char *str)</code>	read line from standard input into str
<code>sprintf(char *str, char *format, ...)</code>	create str according to supplied format and variables
<code>strcat(char *dest, char *src)</code>	append contents of string src to string dest
<code>strcpy(char *dest, char *src)</code>	copy contents of string src to string dest
<code>vsprintf(char *str, char *fmt, va_list ap)</code>	create str according to supplied format and variables

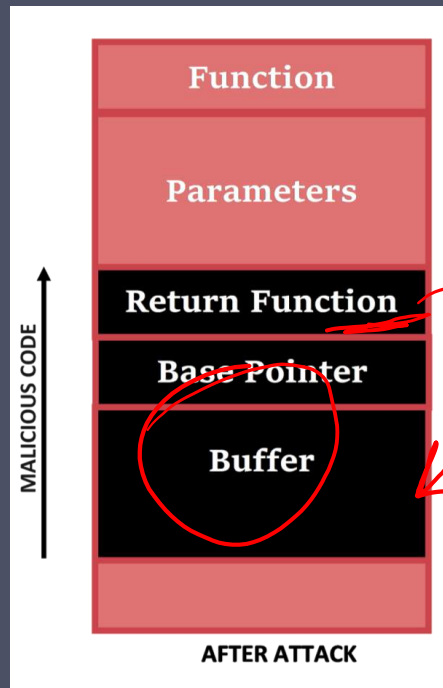
Demo in Visual Studio...

Shellcode

Shellcode

- Code supplied by attacker
 - Often saved in buffer being overflowed
 - Traditionally transferred control to a user command-line interpreter (shell)
- Machine code
 - Specific to processor and operating system
 - Traditionally needed good assembly language skills to create
 - More recently a number of sites and tools have been developed that automate this process
- Metasploit Project
 - Provides useful information to people who perform penetration, IDS signature development, and exploit research





Example UNIX Shellcode

```
int main(int argc, char *argv[])
{
    char *sh;
    char *args[2];

    sh = "/bin/sh";
    args[0] = sh;
    args[1] = NULL;
    execve(sh, args, NULL);
}
```

(a) Desired shellcode code in C

```

nop
nop          // end of nop sled
jmp  find    // jump to end of code
cont: pop    %esi      // pop address of sh off stack into %esi
xor    %eax,%eax      // zero contents of EAX
mov    %al,0x7(%esi)   // copy zero byte to end of string sh (%esi)
lea    (%esi),%ebx     // load address of sh (%esi) into %ebx
mov    %ebx,0x8(%esi)  // save address of sh in args[0] (%esi+8)
mov    %eax,0xc(%esi)  // copy zero to args[1] (%esi+c)
mov    $0xb,%al       // copy execve syscall number (11) to AL
mov    %esi,%ebx      // copy address of sh (%esi) to %ebx
lea    0x8(%esi),%ecx  // copy address of args (%esi+8) to %ecx
lea    0xc(%esi),%edx  // copy address of args[1] (%esi+c) to %edx
int    $0x80          // software interrupt to execute syscall
find: call cont        // call cont which saves next address on stack
sh:    .string "/bin/sh" // string constant
args:  .long 0          // space used for args array
       .long 0          // args[1] and also NULL for env array
```

(b) Equivalent position-independent x86 assembly code

```

90 90 eb 1a 5e 31 c0 88 46 07 8d 1e 89 5e 08 89
46 0c b0 0b 89 f3 8d 4e 08 8d 56 0c cd 80 e8 e1
ff ff ff 2f 62 69 6e 2f 73 68 20 20 20 20 20
```

(c) Hexadecimal values for compiled x86 machine code

Stack Overflow Variants

Target program
can be:



A trusted system
utility



Network service
daemon



Commonly used
library code

Shellcode functions

Launch a remote shell when connected to

Create a reverse shell that connects back to the
hacker

Use local exploits that establish a shell

Flush firewall rules that currently block other
attacks

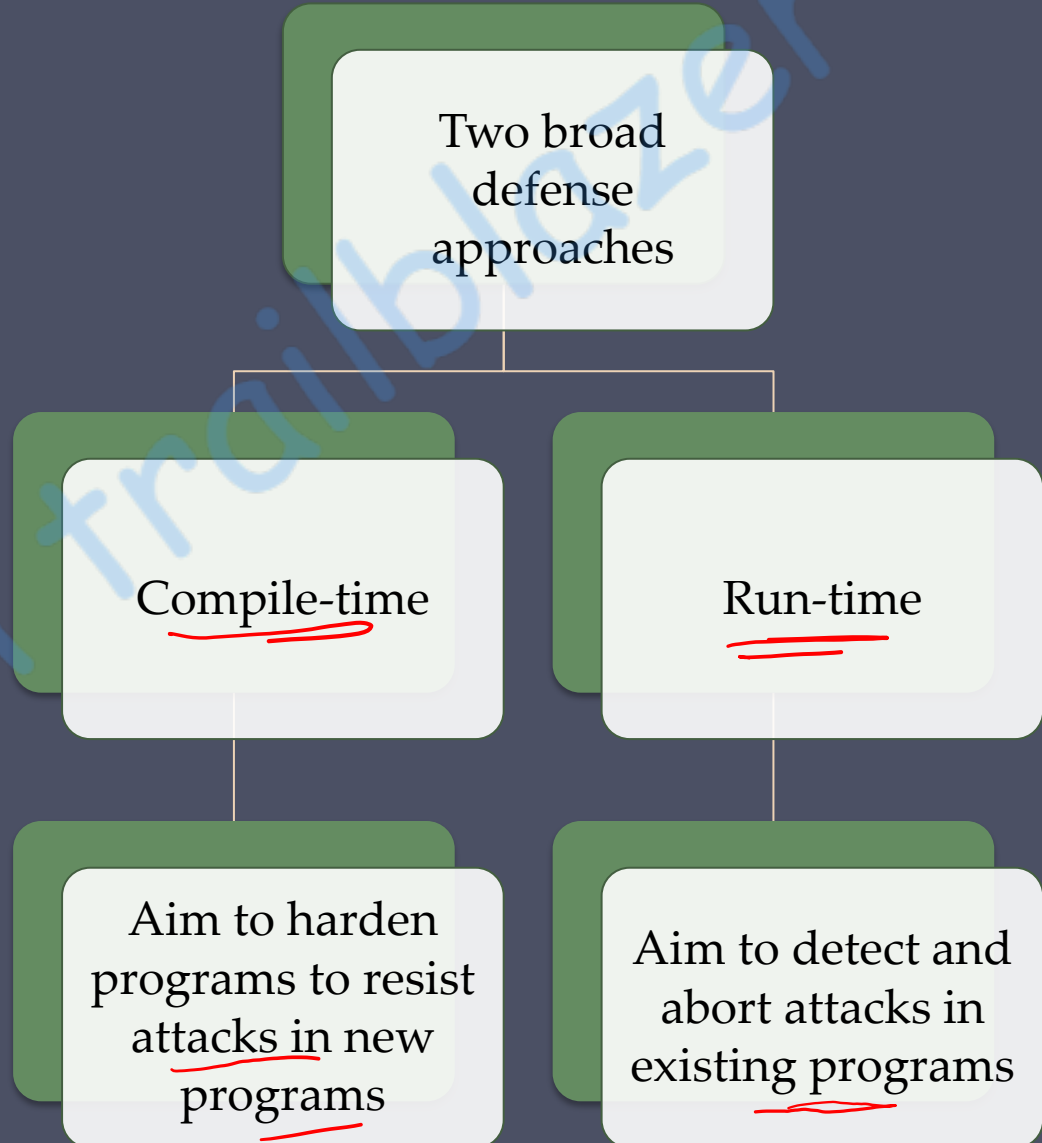


Break out of a chroot (restricted execution)
environment, giving full access to the system

Buffer Overflow Defenses

Buffer Overflow Defenses

- Buffer overflows are widely exploited



Compile-Time Defenses: Programming Language

- Use a modern high-level language
 - Not vulnerable to buffer overflow attacks
 - Compiler enforces range checks and permissible operations on variables

Disadvantages

- Additional code must be executed at run time to impose checks
- Flexibility and safety comes at a cost in resource use
- Distance from the underlying machine language and architecture means that access to some instructions and hardware resources is lost
- Limits their usefulness in writing code, such as device drivers, that must interact with such resources

Compile-Time Defenses: Safe Coding Techniques

- C designers placed much more emphasis on space efficiency and performance considerations than on type safety
 - Assumed programmers would exercise due care in writing code
- Programmers need to inspect the code and rewrite any unsafe coding
 - An example of this is the OpenBSD project
- Programmers have audited the existing code base, including the operating system, standard libraries, and common utilities
 - This has resulted in what is widely regarded as one of the safest operating systems in widespread use

Run-Time Defenses:

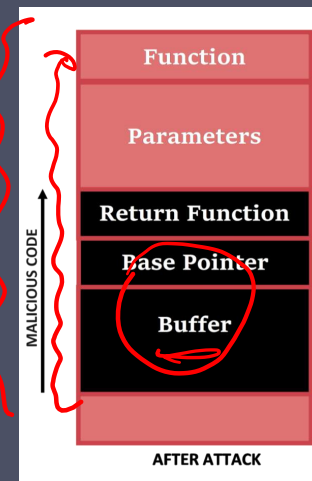
Executable Address Space Protection

Use virtual memory support to make some regions of memory non-executable

- Requires support from memory management unit (MMU)
- Long existed on SPARC / Solaris systems
- Recent on x86 Linux/Unix/Windows systems

Issues

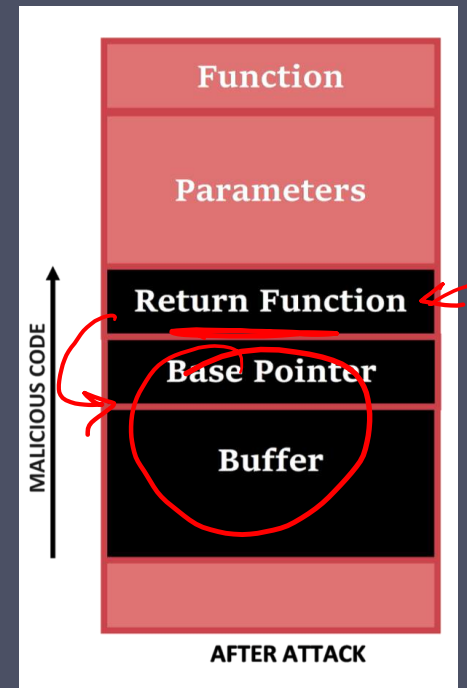
- Support for executable stack code ?
- Special provisions are needed



Run-Time Defenses:

Address Space Randomization

- Manipulate location of key data structures
 - Stack, heap, global data
 - Using random shift for each process
 - Large address range on modern systems means wasting some has negligible impact
- Randomize location of heap buffers
- Random location of standard library functions



Software Security

CWE/SANS TOP 25 Most Dangerous Software Errors (2011)

Software Error Category: Insecure Interaction Between Components

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Unrestricted Upload of File with Dangerous Type

Cross-Site Request Forgery (CSRF) —

URL Redirection to Untrusted Site ('Open Redirect') —

Software Error Category: Risky Resource Management

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') —

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Download of Code Without Integrity Check

Inclusion of Functionality from Untrusted Control Sphere

Use of Potentially Dangerous Function

Incorrect Calculation of Buffer Size

Uncontrolled Format String

Integer Overflow or Wraparound

Software Error Category: Porous Defenses

Missing Authentication for Critical Function

Missing Authorization

Use of Hard-coded Credentials ←

Missing Encryption of Sensitive Data ←

Reliance on Untrusted Inputs in a Security Decision

Execution with Unnecessary Privileges

Incorrect Authorization ←

Incorrect Permission Assignment for Critical Resource ←

Use of a Broken or Risky Cryptographic Algorithm ←

Improper Restriction of Excessive Authentication Attempts ←

Use of a One-Way Hash without a Salt

OWASP Top 10

Web Application Security Risks

Open Web Application Security Project (OWASP)

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



<https://owasp.org/www-project-top-ten/>

Security Flaws

- Critical Web application security flaws include five related to insecure software code
 - Unvalidated input
 - Cross-site scripting
 - Buffer overflow
 - Injection flaws
 - Improper error handling
- These flaws occur as a consequence of insufficient checking and validation of data and error codes in programs
- Awareness of these issues is a critical initial step in writing more secure program code
- Emphasis should be placed on the need for software developers to address these known areas of concern

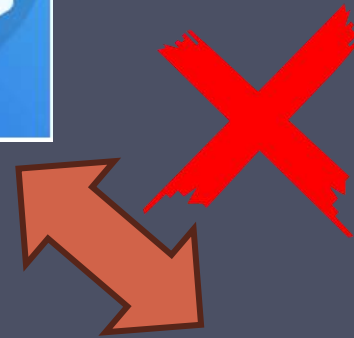
Reducing Software Vulnerabilities

Reducing Software Vulnerabilities

- The NIST report NISTIR 8151 presents a range of approaches to reduce the number of software vulnerabilities
- It recommends:
 - Stopping vulnerabilities before they occur by using improved methods for specifying and building software
 - Finding vulnerabilities before they can be exploited by using better and more efficient testing techniques
 - Reducing the impact of vulnerabilities by building more resilient architectures

Software Security, Quality and Reliability

Software Security, Quality and Reliability



- Software quality and reliability

- Software Security

Software Security, Quality and Reliability

- Software quality and reliability:

- Concerned with the accidental failure of program as a result of some theoretically random, unanticipated input, system interaction, or use of incorrect code
- Improve using structured design and testing to identify and eliminate as many bugs as possible from a program
- Concern is not how many bugs, but how often they are triggered

- Software security:

- Attacker chooses probability distribution, specifically targeting bugs that result in a failure that can be exploited by the attacker
- Triggered by inputs that differ dramatically from what is usually expected
- Unlikely to be identified by common testing approaches

Defensive Programming

Defensive Programming

- Designing and implementing software so that it continues to function even when under attack
- Requires attention to all aspects of program execution, environment, and type of data it processes
- Software is able to detect erroneous conditions resulting from some attack
- Also referred to as secure programming
- Key rule is to never assume anything, check all assumptions and handle any possible error states

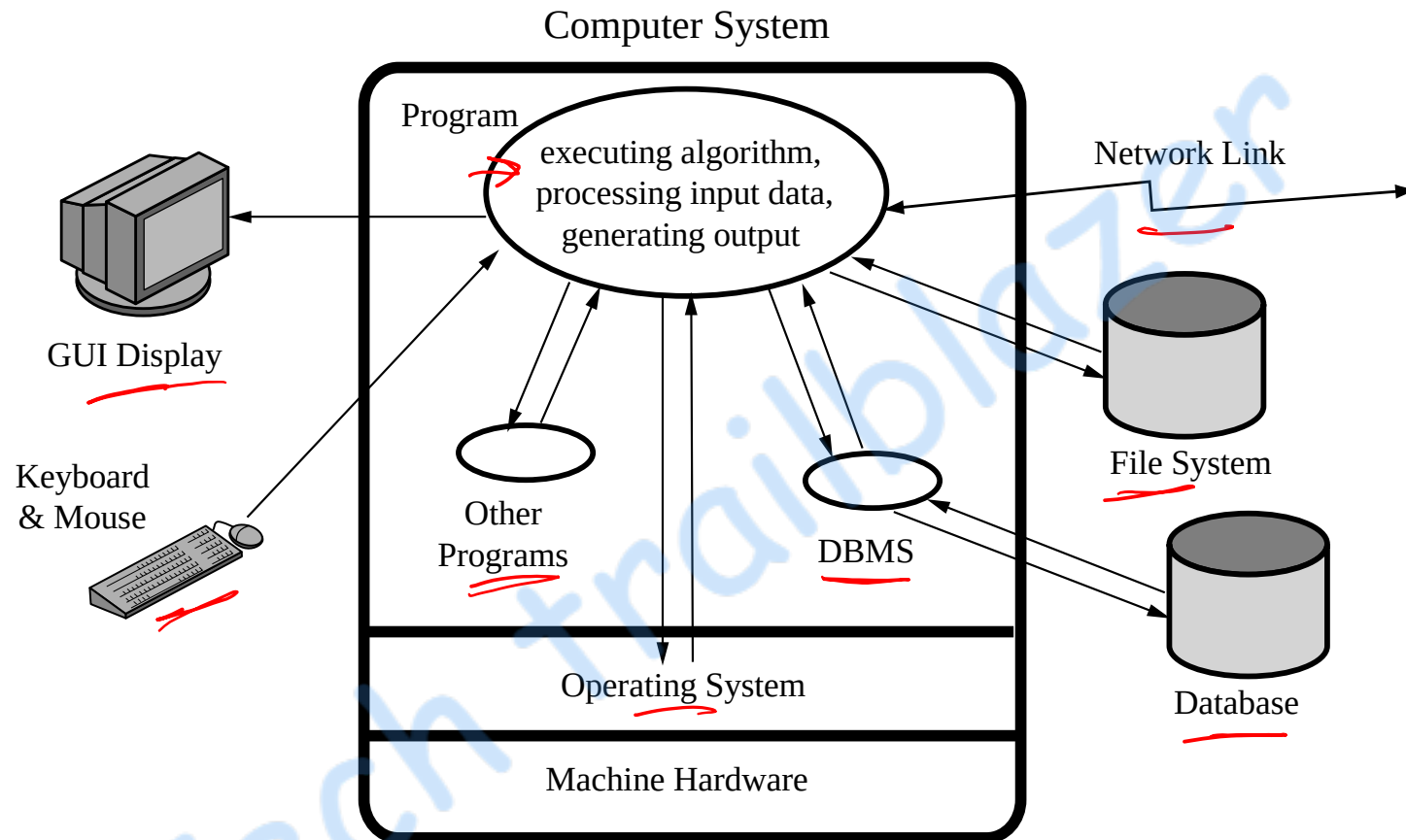


Figure 11.1 Abstract View of Program

Defensive Programming

- Programmers often make assumptions about the type of inputs a program will receive and the environment it executes in
 - Assumptions need to be validated by the program and all potential failures handled gracefully and safely
- Requires a changed mindset to traditional programming practices
 - Programmers have to understand how failures can occur and the steps needed to reduce the chance of them occurring in their programs
- Conflicts with business pressures to keep development times as short as possible to maximize market advantage

Handling Program Input

Handling Program Input

Incorrect handling
of input data is a
very common
failing

Input is any source
of data from
outside and whose
value is not
explicitly known by
the programmer
when the code was
written

Must identify all
data sources

Explicitly validate
assumptions on
size and type of
values before use

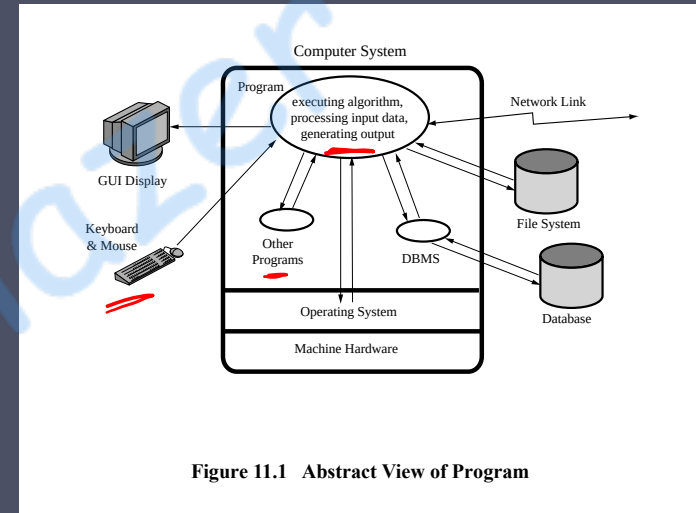


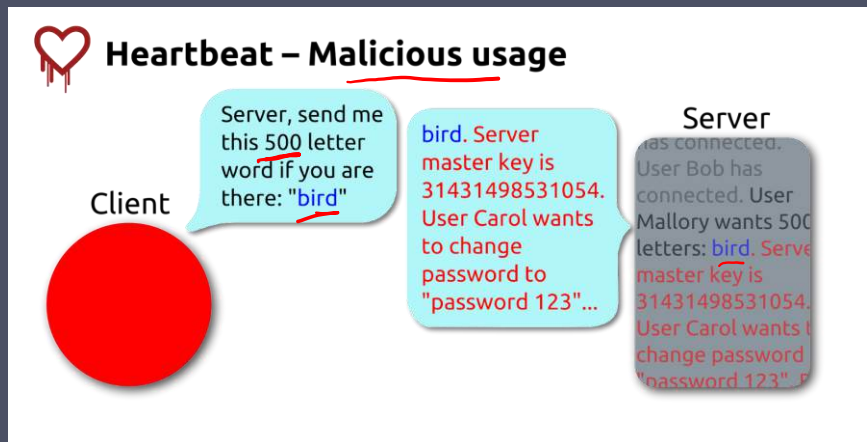
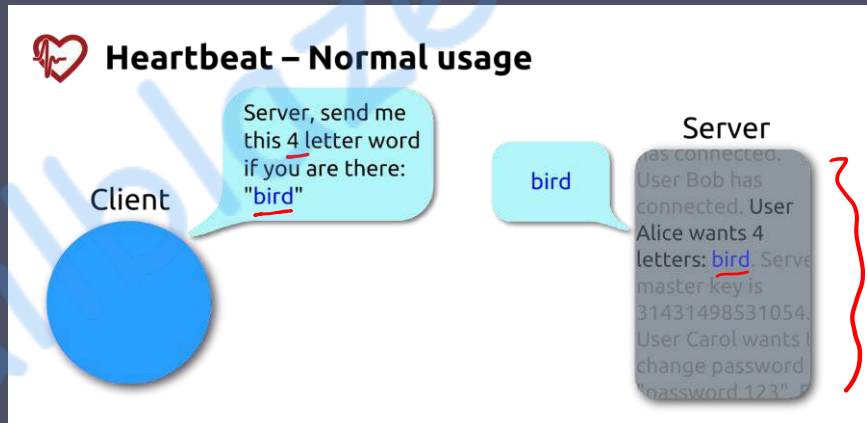
Figure 11.1 Abstract View of Program

Input Size & Buffer Overflow

- Programmers often make assumptions about the maximum expected size of input
 - Allocated buffer size is not confirmed
 - Resulting in buffer overflow
- Testing may not identify vulnerability
 - Test inputs are unlikely to include large enough inputs to trigger the overflow
- Safe coding treats all input as dangerous

Interpretation of Program Input

- Program input may be binary or text
 - Binary interpretation depends on encoding and is usually application specific
- There is an increasing variety of character sets being used
 - Care is needed to identify just which set is being used and what characters are being read
- Failure to validate may result in an exploitable vulnerability
- 2014 Heartbleed OpenSSL bug is a recent example of a failure to check the validity of a binary input value



Injection Attacks

Injection Attacks

- Flaws relating to invalid handling of input data, specifically when program input data can accidentally or deliberately influence the flow of execution of the program

Most often occur in scripting languages

- Encourage reuse of other programs and system utilities where possible to save coding effort

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "'";  
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" .  
    mysql_real_escape_string($name) . "'";  
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

SQL Injection Attack Demo

<https://www.codingame.com/playgrounds/154/sql-injection-demo/sql-injection>

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "'";  
$result = mysql_query($query);
```

(a) Vulnerable PHP code

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" .  
    mysql_real_escape_string($name) . "'";  
$result = mysql_query($query);
```

(b) Safer PHP code

Figure 11.3 SQL Injection Example

query = "SELECT name FROM user where username = '' + username + '' and password = '' + password + ''";

query = "SELECT name FROM user where username = 'admin' and password = 'admin123' "; ✓

query = "SELECT name FROM user where username = 'any' and password = '123' or '1'='1'";

Injected SQL

Forensic Science



- Forensic science, also known as criminalistics, is the application of science to criminal and civil laws.
- During criminal investigation in particular, it is governed by the legal standards of admissible evidence and criminal procedure.
- It is a broad field utilizing numerous practices such as the analysis of DNA, fingerprints, bloodstain patterns, firearms, ballistics, and toxicology.
- Forensic scientists collect, preserve, and analyze scientific evidence during the course of an investigation.
- While some forensic scientists travel to the scene of the crime to collect the evidence themselves, others occupy a laboratory role, performing analysis on objects brought to them by other individuals.
- Still others are involved in analysis of financial, banking, or other numerical data for use in financial crime investigation, and can be employed as consultants from private firms, academia, or as government employees.
- In addition to their laboratory role, forensic scientists testify as expert witnesses in both criminal and civil cases and can work for either the prosecution or the defense.

Origins of forensic science and early methods

- The ancient world lacked standardized forensic practices, which enabled criminals to escape punishment.
- Criminal investigations and trials relied heavily on forced confessions and witness testimony.
- However, ancient sources do contain several accounts of techniques that foreshadow concepts in forensic science developed centuries later.

Locard's Exchange Principle

- In forensic science, Locard's principle holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.
- Dr. Edmond Locard (1877–1966) was a pioneer in forensic science who became known as the Sherlock Holmes of Lyon, France.
- He formulated the basic principle of forensic science as: "Every contact leaves a trace".
- It is generally understood as "with contact between two items, there will be an exchange."
- Paul L. Kirk expressed the principle as follows:
 - Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.
 - Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects.
 - All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.



Edmond Locard's (Sherlock Holmes of France) Principle

Every contact by a criminal
leaves behind a trace.



- **Fragmentary** or **trace evidence** is any type of material left at (or taken from) a crime scene, or the result of **contact** between two surfaces, such as shoes and the floor covering or soil, or fibres from where someone sat on an upholstered chair.
- When a crime is committed, fragmentary (or trace) evidence needs to be collected from the scene.
- A team of specialised police technicians goes to the scene of the crime and seals it off.
- They record video and take photographs of the crime scene, victim/s (if there are any) and items of evidence.
- If necessary, they undertake ballistics examinations.
- They check for foot, shoe, and tire mark impressions, plus hair as well as examine any vehicles and check for fingerprints – whole or partial.

Principle of Exchange

According to this, when a criminal or his instrument of crime come in contact with the victim or the objects surrounding him, they leave traces, and the criminal or his instrument picks up traces from the same contact.

– Edmond Locard

What is computer/digital/cyber forensics?

- Cyber forensics is the discovery, analysis, and reconstruction of evidence extracted from any element of Computer systems, Computer networks, Computer media, and Computer peripherals that allow investigators to solve a crime.
- Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime.
- The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.



Media types used for computer forensic analysis: a Fujifilm FinePix digital camera, two flash memory cards, a USB flash drive, a 5GB iPod, a CD-R or DVD recordable, and a Mini CD.

<https://en.wikipedia.org/wiki/File:PersonalStorageDevices.agr.jpg>



<https://dxhub.calpoly.edu/challenges/digital-evidence/>











Nature of Digital Evidence

- Physical Form
- Virtual Locations / Paths
- Volatile vs Non-volatile

Application and Uses

- Digital forensics investigations have a variety of applications.
- The most common is to support or refute a hypothesis before criminal or civil courts.
- Criminal cases involve the alleged breaking of laws that are defined by legislation and enforced by the police and prosecuted by the state, such as murder, theft, and assault against the person.
- Civil cases, on the other hand, deal with protecting the rights and property of individuals (often associated with family disputes), but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.
- Forensics may also feature in the private sector, such as during internal corporate investigations or intrusion investigations (a special probe into the nature and extent of an unauthorized network intrusion).
- As well as identifying direct evidence of a crime, digital forensics can be used to attribute evidence to specific suspects, confirm alibis or statements, determine intent, identify sources (for example, in copyright cases), or authenticate documents.
- Investigations are much broader in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions), often involving complex time-lines or hypotheses.





- Digital forensics is commonly used in both criminal law and private investigation.
- Traditionally it has been associated with criminal law, where evidence is collected to support or oppose a hypothesis before the courts.
- As with other areas of forensics this is often a part of a wider investigation spanning a number of disciplines.
- In some cases, the collected evidence is used as a form of intelligence gathering, used for other purposes than court proceedings (for example to locate, identify or halt other crimes).
- In civil litigation or corporate matters digital forensics forms part of the electronic discovery (or eDiscovery) process.
- Forensic procedures are similar to those used in criminal investigations, often with different legal requirements and limitations.
- Outside of the courts digital forensics can form a part of internal corporate investigations.
- A common example might be following unauthorized network intrusion.
- A specialist forensic examination into the nature and extent of the attack is performed as a damage limitation exercise, both to establish the extent of any intrusion and in an attempt to identify the attacker.

Subdivisions and Branches

- Digital forensics is the application of proven scientific methods and techniques in order to recover data from electronic / digital media. Digital Forensic specialists work in the field as well as in the lab.
- Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals and small digital devices (e.g. tablets, smartphones, flash drives) are now extensively used.
- Some of these devices have volatile memory while some have non-volatile memory.
- Sufficient methodologies are available to retrieve data from volatile memory, however, there is lack of detailed methodology or a framework for data retrieval from non-volatile memory sources.
- Also, the technical aspect of an investigation is divided into several sub-branches related to the type of digital devices involved:
 - computer forensics, network forensics, forensic data analysis, and mobile device forensics, router forensics.
- Depending on the type of devices, media or artifacts, digital forensics investigation is branched into various types.

Digital Forensic Categories / Subdivisions / Branches

- Computer Forensics
- Mobile Device Forensics
- Network Forensics [Logs]
- Forensic Data Analysis
- Digital Image Forensics
- Database Forensics
- Cloud Forensics
- IoT Forensics
- Dark Web Forensics
- Audio Analysis/Forensics
- Video Analysis/Forensics
- E-Mail Forensics

- **Computer forensics**

- The goal of computer forensics is to explain the current state of a digital artifact; such as a computer system, storage medium or electronic document.
- The discipline usually covers computers, embedded systems (digital devices with rudimentary computing power and onboard memory) and static memory (such as USB pen drives).
- Computer forensics can deal with a broad range of information; from logs (such as internet history) through to the actual files on the drive.
- In 2007 prosecutors used a spreadsheet recovered from the computer of Joseph Edward Duncan to show premeditation and secure the death penalty.
- Sharon Lopatka's killer was identified in 2006 after email messages from him detailing torture and death fantasies were found on her computer.

Vip

- **Mobile device forensics**

- Mobile device forensics is a sub-branch of digital forensics relating to recovery of digital evidence or data from a mobile device.
- Mobile device forensics is the scientific examination and evaluation of evidence found in mobile phones, e.g. Call History and Deleted SMS, and includes SIM Card Forensics.
- It differs from Computer forensics in that a mobile device will have an inbuilt communication system (e.g. GSM) and, usually, proprietary storage mechanisms.
- Investigations usually focus on simple data such as call data and communications (SMS/Email) rather than in-depth recovery of deleted data.
- SMS data from a mobile device investigation helped to exonerate Patrick Lumumba in the murder of Meredith Kercher.
- Mobile devices are also useful for providing location information; either from inbuilt gps/location tracking or via cell site logs, which track the devices within their range.
- Such information was used to track down the kidnappers of Thomas Onofri in 2006.

Vip

- **Network forensics**

- Network forensics is concerned with the monitoring and analysis of computer network traffic, both local and WAN/internet, for the purposes of information gathering, evidence collection, or intrusion detection.
- Traffic is usually intercepted at the packet level, and either stored for later analysis or filtered in real-time.
- Unlike other areas of digital forensics network data is often volatile and rarely logged, making the discipline often reactionary.

Vip Notes

- **Forensic data analysis**
 - Forensic Data Analysis is a branch of digital forensics. It examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from financial crime.
- **Digital image forensics**
 - Digital image forensics (or forensic image analysis) is a branch of digital forensics that deals with examination and verification of an image's authenticity and content.
 - These can range from Stalin-era airbrushed photos to elaborate deepfake videos.
 - This has broad implications for a wide variety of crimes, for determining the validity of information presented in civil and criminal trials, and for verifying images and information that are circulated through news and social media.
- **Forensic video analysis** is the scientific examination, comparison and evaluation of video in legal matters.

VIT

- **Database forensics**

- Database forensics is a branch of digital forensics relating to the forensic study of databases and their metadata.
- Investigations use database contents, log files and in-RAM data to build a timeline or recover relevant information.

- **IoT Forensics**

- IoT forensics is a branch of Digital forensics that has the goal of identifying and extracting digital information from devices belonging to the Internet of things field, to be used for forensics investigations as potential source of evidence.

Digital Forensic Standards & Frameworks

- Since 2000, in response to the need for standardization, various bodies and agencies have published guidelines for digital forensics.
 1. The Scientific Working Group on Digital Evidence (SWGDE) produced a 2002 paper, Best practices for Computer Forensics.
 2. This was followed, in 2005, by the publication of an ISO standard (ISO 17025, General requirements for the competence of testing and calibration laboratories).
 3. NIST

Forensic Lab Setup

- Laws & Regulations
- Types of Incidents
- Important Numbers / Emergency Contacts
- Physical Location
- Team Members & Personnel
- Forensic Expertise
- HVAC & Lighting
- Building Structure
- Tools
- Hardware
 - Forensic Machines
 - Cables & Connectors
- Software
- Write Blocker
- Duplicator
- Storage
 - Data & Equipment

Digital Forensic Process

- The typical forensic process encompasses the **seizure**, forensic **imaging** (**acquisition**), and **analysis** of digital media, followed with the production of a **report** of the collected evidence.



<https://www.uco.edu/programs/microcredentials/digital-evidence>

- A digital forensic investigation commonly consists of 3 stages:
 - acquisition or imaging of exhibits, analysis, and reporting.
- Ideally acquisition involves capturing an image of the computer's volatile memory (RAM) and creating an exact sector level duplicate (or "forensic duplicate") of the media, often using a **write blocking** device to prevent modification of the original.
 - However, the growth in size of storage media and developments such as cloud computing have led to more use of **'live' acquisitions** whereby a 'logical' copy of the data is acquired rather than a complete image of the physical storage device.
 - Both acquired image (or logical copy) and original media/data are **hashed** (using an algorithm such as SHA-1 or MD5) and the values compared to verify the copy is accurate.
- During the analysis phase an investigator recovers evidence material using a number of different methodologies and tools.
 - In 2002, an article in the International Journal of Digital Evidence referred to this step as "an in-depth systematic search of evidence related to the suspected crime."
 - In 2006, forensics researcher Brian Carrier described an "intuitive procedure" in which obvious evidence is first identified and then "exhaustive searches are conducted to start filling in the holes."
 - The actual process of analysis can vary between investigations, but common methodologies include conducting keyword searches across the digital media (within files as well as unallocated and slack space), recovering deleted files and extraction of registry information (for example to list user accounts, or attached USB devices).
 - The evidence recovered is analysed to reconstruct events or actions and to reach conclusions, work that can mostly be performed by specialised staff.
- When an investigation is complete the data is presented, usually in the form of a written report, in lay persons' terms.

DIGITAL FORENSICS

Identification

Where is the evidence? In which country?
Which device(s) does it need to be gathered from?
Is the data "at rest" or "in transit"?



Preservation

How will the data be accessed? Which legislation applies?
Is the action proportionate, lawful, accountable and necessary?



Analysis

Are the required technical and people skills available
to acquire, analyse and exploit the evidence in a
timely manner with full chain-of-custody?

Documentation

Ensure EVERYTHING is documented to prevent losing
evidence due to legal or procedural mistakes



Presentation

Evidence should be presented accurately, concisely
and clearly. Can the judge and/or jury understand it?
Can it be tested and challenged by the defence?

An example of an image's Exif metadata that might be used to prove its origin

https://en.wikipedia.org/wiki/File:En_exif_data.png

Camera manufacturer	Canon
Camera model	Canon EOS 400D DIGITAL
Exposure time	1/80 sec (0.016666666666667)
F-number	f/4.5
ISO speed rating	400
Date and time of data generation	11:06, August 27, 2010
Lens focal length	31 mm
Show extended details	

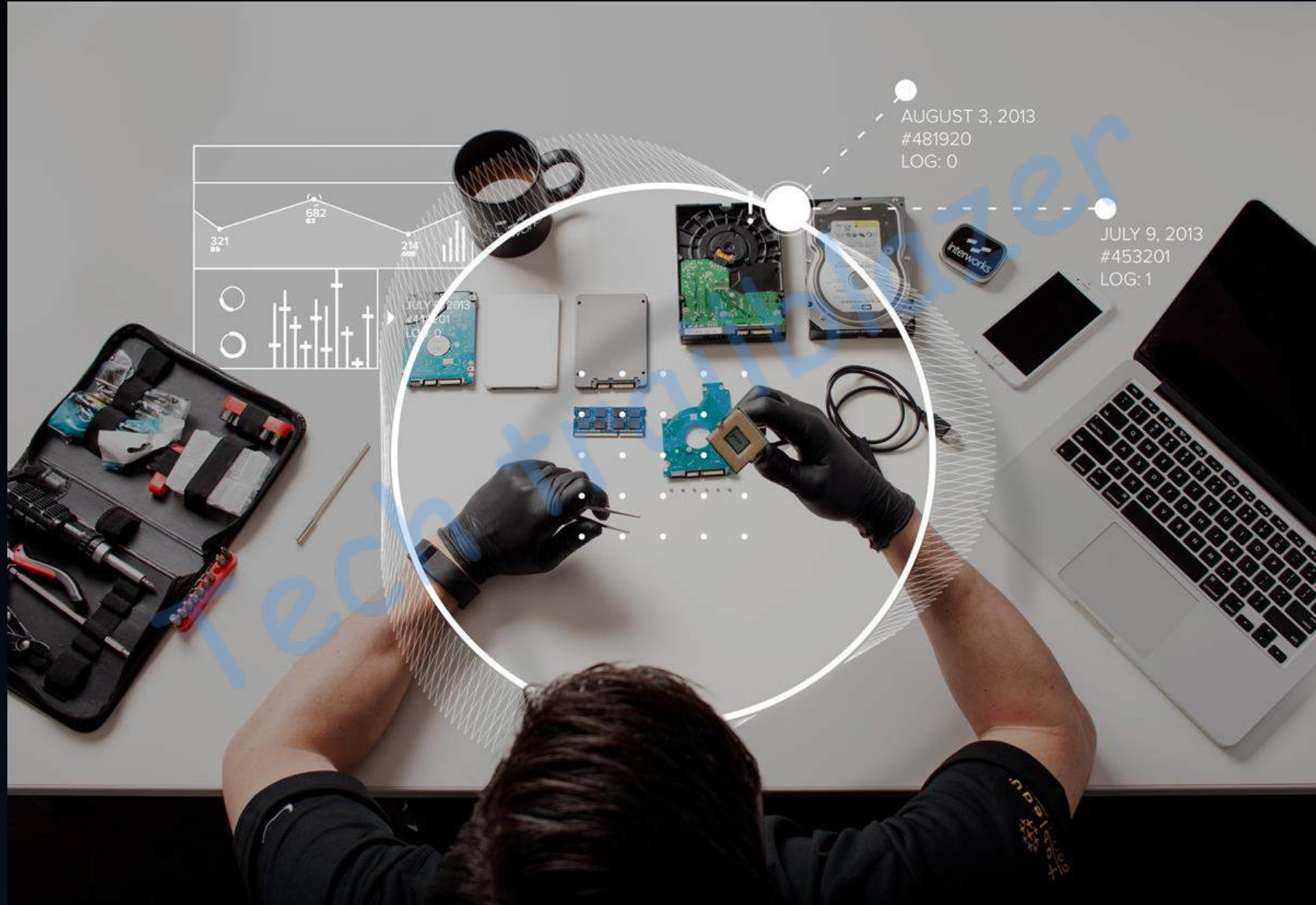
Forensic Report

- Title Page [Case number/title, reporting date, number of pages, examiner name]
- Case Summary
- Evidence Details or Particulars
- Tools Used
- Methodology / Steps
- Forensic Analysis & Findings
- Forensic Investigator/Examiner Signature
- Images of Evidentiary Items
- Chain of Custody

Development of Digital Forensic Tools

- During the 1980s, very few specialized digital forensic tools existed.
- Consequently, investigators often performed live analysis on media, examining computers from within the operating system using existing **sysadmin tools** to extract evidence.
- This practice carried the **risk of modifying data** on the disk, either inadvertently or otherwise, which led to claims of **evidence tampering**.
- A number of tools were created during the early 1990s to address the problem.
- The need for such software was first recognized in 1989 at the Federal Law Enforcement Training Center, resulting in the creation of IMDUMP (by Michael White) and in 1990, SafeBack (developed by Sydex).
- Similar software was developed in other countries; DIBS (a hardware and software solution) was released commercially in the UK in 1991, and Rob McKemmish released Fixed Disk Image free to Australian law enforcement.
- These tools allowed examiners to create an **exact copy** of a piece of digital media to work on, leaving the **original disk intact for verification**.
- By the end of the 1990s, as demand for digital evidence grew, more **advanced commercial tools** such as **EnCase** and **FTK** were developed, allowing analysts to examine copies of media without using any live forensics.
- More recently, a trend towards "live memory forensics" has grown, resulting in the availability of tools such as WindowsSCOPE.
- The same progression of tool development has occurred for **mobile devices**; initially investigators accessed data directly on the device, but soon specialist tools such as **Cellebrite**, **XRY** or Radio Tactics Aceso appeared.

<https://interworks.com/blog/bstephens/2016/02/05/what-digital-forensics/>



Digital Forensic Tools

- Building Structure
- Tools
 - Hardware
 - Forensic Machines
 - Cables & Connectors
 - Software
 - Write Blocker
 - Duplicator
 - Storage
 - Data & Equipment

Mobile phones in an Evidence bag
<https://en.wikipedia.org/wiki/File:Mobiles.JPG>



A portable Tableau write-blocker attached to a hard drive
https://en.wikipedia.org/wiki/File:Portable_forensic_tableau.JPG



Limitations

- Encryption
 - One major limitation to a forensic investigation is the use of encryption; this disrupts initial examination where pertinent evidence might be located using keywords.
 - Laws to compel individuals to disclose encryption keys are still relatively new and controversial but always more frequently there are solutions to brute force passwords or bypass encryption, such as in smartphones or PCs where by means of bootloader techniques the content of the device can be first acquired and later forced in order to find the password or encryption key.
- Steganography
- Cloud Computing/Forensics
 - Jurisdiction
 - Virtualization
 - Elasticity

Anti-Forensic Techniques

- Passwords
- Encryption
- Jurisdiction
- Proxy Chaining
- Steganography
- NTFS Data Streams

Data hiding

- Data hiding is the process of making data difficult to find while also keeping it accessible for future use.
- "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."
- Some of the more common forms of data hiding include encryption, steganography and other various forms of hardware/software based data concealment.
- Each of the different data hiding methods makes digital forensic examinations difficult.
- When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.
- Encryption
- Steganography
- Other forms of data hiding

Data hiding: Encryption

- One of the more commonly used techniques to defeat computer forensics is data encryption.
- In a presentation given on encryption and anti-forensic methodologies, the Vice President of Secure Computing, Paul Henry, referred to encryption as a "forensic expert's nightmare".
- The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key.
 - Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.
- File level encryption encrypts only the file contents.
 - This leaves important information such as file name, size and timestamps unencrypted.
 - Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.
- Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult.
 - Some of these functions include the use of a keyfile, full-volume encryption, and plausible deniability.
 - The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Data hiding: Steganography

- Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight.
- "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)."
- While some experts have argued that the use of steganography techniques is not very widespread and therefore the subject shouldn't be given a lot of thought, most experts agree that steganography has the capability of disrupting the forensic process when used correctly.
- According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current steganalysis programs. It did this through the use of steganography in conjunction with file compression.

Data hiding: Other forms of data hiding

- Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system.
 - Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."
- One of the more well known tools that is often used for data hiding is called Slacker (part of the Metasploit framework).
 - Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software.
- Another data hiding technique involves the use of bad sectors.
 - To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster.
 - The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

Artifact wiping

- The methods used in artifact wiping are tasked with permanently eliminating particular files or entire file systems.
- This can be accomplished through the use of a variety of methods that include disk cleaning utilities, file wiping utilities and disk degaussing/destruction techniques.
- Disk cleaning utilities
- File wiping utilities
- Disk degaussing / destruction techniques

Artifact wiping: Disk cleaning utilities

- Disk cleaning utilities use a variety of methods to overwrite the existing data on disks .
- The effectiveness of disk cleaning utilities as anti-forensic tools is often challenged as some believe they are not completely effective.
- Experts who don't believe that disk cleaning utilities are acceptable for disk sanitization base their opinions of current DOD policy, which states that the only acceptable form of sanitization is degaussing.
- Disk cleaning utilities are also criticized because they leave signatures that the file system was wiped, which in some cases is unacceptable.
- Some of the widely used disk cleaning utilities include DBAN, srm, BCWipe Total WipeOut, KillDisk, PC Inspector and CyberScrubs cyberCide.
- Another option which is approved by the NIST and the NSA is CMRR Secure Erase, which uses the Secure Erase command built into the ATA specification.

Artifact wiping: File wiping utilities

- File wiping utilities are used to delete individual files from an operating system.
- The advantage of file wiping utilities is that they can accomplish their task in a relatively short amount of time as opposed to disk cleaning utilities which take much longer.
- Another advantage of file wiping utilities is that they generally leave a much smaller signature than disk cleaning utilities.
- There are two primary disadvantages of file wiping utilities, first they require user involvement in the process and second some experts believe that file wiping programs don't always correctly and completely wipe file information.
- Some of the widely used file wiping utilities include BCWipe, R-Wipe & Clean, Eraser, Aevita Wipe & Delete and CyberScrubs PrivacySuite.
- On Linux tools like shred and srm can be also used to wipe single files.
- SSDs are by design more difficult to wipe, since the firmware can write to other cells therefore allowing data recovery.
- In these instances ATA Secure Erase should be used on the whole drive, with tools like hdparm that support it.

Artifact wiping: Disk degaussing / destruction techniques

- Disk degaussing is a process by which a magnetic field is applied to a digital media device.
- The result is a device that is entirely clean of any previously stored data.
- Degaussing is rarely used as an anti-forensic method despite the fact that it is an effective means to ensure data has been wiped.
- This is attributed to the high cost of degaussing machines, which are difficult for the average consumer to afford.
- A more commonly used technique to ensure data wiping is the physical destruction of the device.
- The NIST recommends that "physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding and melting.

Trail obfuscation

- The purpose of trail obfuscation is to confuse, disorient, and divert the forensic examination process.
- Trail obfuscation covers a variety of techniques and tools that include "log cleaners, spoofing, misinformation, backbone hopping, zombied accounts, trojan commands."
- One of the more widely known trail obfuscation tools is Timestomp (part of the Metasploit Framework).
 - Timestomp gives the user the ability to modify file metadata pertaining to access, creation and modification times/dates.
 - By using programs such as Timestomp, a user can render any number of files useless in a legal setting by directly calling into question the files' credibility.
- Another well known trail-obfuscation program is Transmogrify (also part of the Metasploit Framework).
 - In most file types the header of the file contains identifying information.
 - A (.jpg) would have header information that identifies it as a (.jpg), a (.doc) would have information that identifies it as (.doc) and so on.
 - Transmogrify allows the user to change the header information of a file, so a (.jpg) header could be changed to a (.doc) header.
 - If a forensic examination program or operating system were to conduct a search for images on a machine, it would simply see a (.doc) file and skip over it.

Attacks against computer forensics

- In the past anti-forensic tools have focused on attacking the forensic process by destroying data, hiding data, or altering data usage information.
- Anti-forensics has recently moved into a new realm where tools and techniques are focused on attacking forensic tools that perform the examinations.
- These new anti-forensic methods have benefited from a number of factors to include well documented forensic examination procedures, widely known forensic tool vulnerabilities, and digital forensic examiners' heavy reliance on their tools.
- During a typical forensic examination, the examiner would create an image of the computer's disks.
 - This keeps the original computer (evidence) from being tainted by forensic tools.
 - Hashes are created by the forensic examination software to verify the integrity of the image.
 - One of the recent anti-tool techniques targets the integrity of the hash that is created to verify the image.
 - By affecting the integrity of the hash, any evidence that is collected during the subsequent investigation can be challenged.

Forensic Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
 - Forensic Examiner / Specialist / Scientist / Manager
- Relevant Degree, Certifications and Experience



Digital Forensic Certifications

- There are several computer forensics certifications available, such as the ISFCE Certified Computer Examiner, Digital Forensics Investigation Professional (DFIP) and IACRB Certified Computer Forensics Examiner.
- The top vendor independent certification (especially within EU) is considered the CCFP - Certified Cyber Forensics Professional.
- Others, worth to mention for USA or APAC are: The International Association of Computer Investigative Specialists offers the Certified Computer Examiner program. The International Society of Forensic Computer Examiners offers the Certified Computer Examiner program.
- Many commercial based forensic software companies are now also offering proprietary certifications on their products.
 - For example, Guidance Software offering the (EnCE) certification on their tool EnCase, AccessData offering (ACE) certification on their tool FTK, PassMark Software offering certification on their tool OSForensics, and X-Ways Software Technology offering (X-PERT) certification for their software, X-Ways Forensics.
- Tool Specific: EnCase, AccessData FTK, Cellebrite
- General: CHFI (Certified Hacking Forensic Investigator by EC-Council), Mile2, eLearnSecurity, SANS GIAC and many more



HTTPS (Hypertext Transfer Protocol Secure)

Securing Web Communication

Introduction to HTTPS

- HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol used for communication between web browsers and web servers.
- HTTPS adds an extra layer of security by encrypting data exchanged between the client and server, ensuring confidentiality and integrity.



How HTTPS Works

HTTPS utilizes the SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocol to establish a secure connection:

Client Request: The client (web browser) initiates a request to the server using the HTTPS protocol.

Server Response: The server responds by presenting its SSL/TLS certificate to the client.

Certificate Verification: The client verifies the authenticity of the server's certificate using trusted Certificate Authorities (CAs).

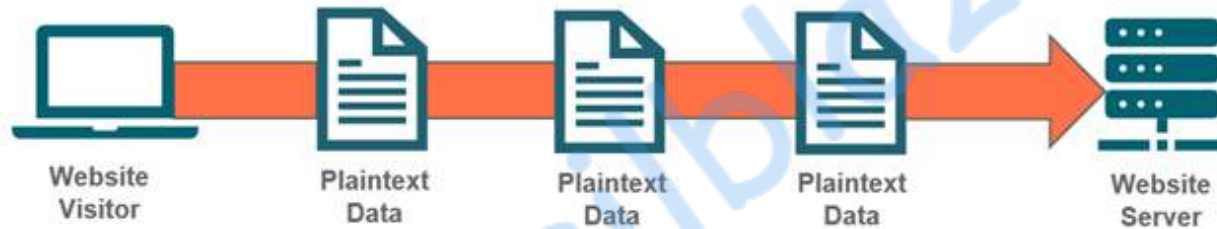
Secure Connection: Once the certificate is validated, a secure connection is established, and data exchange occurs over an encrypted channel.

Encryption and Decryption: The client and server encrypt and decrypt data using symmetric encryption algorithms and a shared session key.

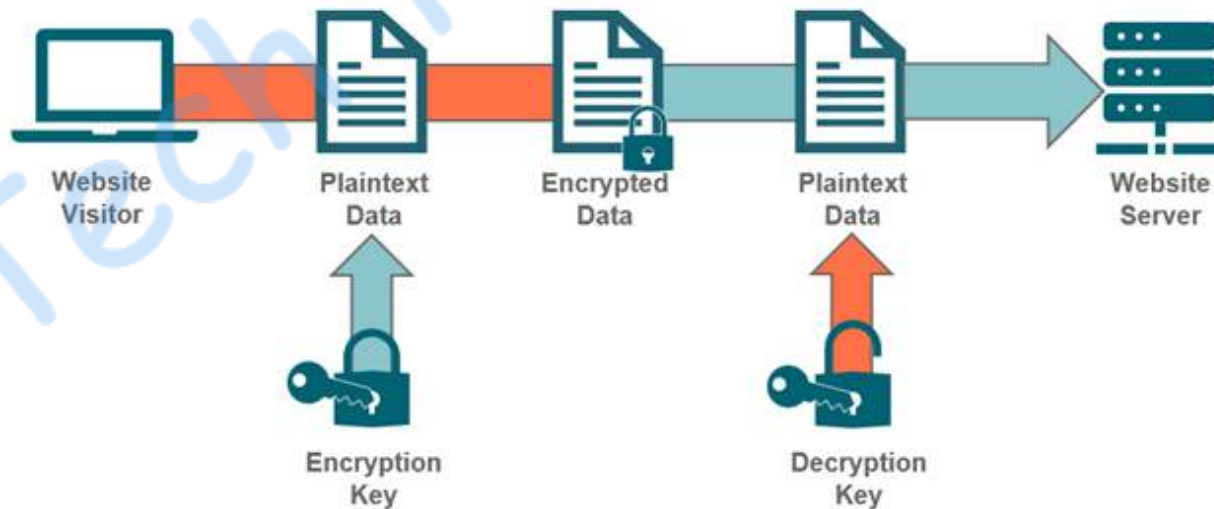
Secure Data Transfer: All subsequent data exchanged between the client and server remains encrypted, protecting it from eavesdropping and tampering.

HTTPS Working

How Insecure Website Communications Work (HTTP)



How Secure Website Communications Work (HTTPS)



Benefits of HTTPS

HTTPS offers numerous benefits for secure web communication:

- **Data Confidentiality:** HTTPS encrypts sensitive information, such as passwords, credit card details, and personal data, preventing unauthorized access.
- **Data Integrity:** HTTPS ensures that data remains intact during transmission, detecting any modifications or tampering attempts.
- **Authentication:** HTTPS verifies the identity of the server through SSL/TLS certificates, preventing impersonation or man-in-the-middle attacks.
- **Trust and User Confidence:** Displaying the padlock symbol and "https" in the URL instills trust in users and reassures them about the security of the website.
- **SEO Benefits:** Search engines consider HTTPS as a ranking signal, incentivizing website owners to implement HTTPS for improved search engine visibility.

Implementing HTTPS

Steps to implement HTTPS on a website:

1. Obtain an SSL/TLS certificate from a trusted Certificate Authority (CA).
2. Install the SSL/TLS certificate on the web server.
3. Configure the server to redirect HTTP traffic to HTTPS.
4. Ensure all web content (images, scripts, stylesheets, etc.) is loaded securely using HTTPS.
5. Test the HTTPS implementation to verify proper functioning and resolve any issues.

HTTPS Best Practices

Best practices for implementing and maintaining HTTPS:

- Use the latest version of the SSL/TLS protocol supported by your infrastructure.
- Enable strong cipher suites and prioritize secure encryption algorithms.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage and prevent downgrade attacks.
- Regularly renew and update SSL/TLS certificates to prevent expiration or revocation.
- Perform security audits and vulnerability scans to identify and address any weaknesses in the HTTPS configuration.

Conclusion

- HTTPS is a crucial technology for securing web communication and protecting sensitive information.
- It ensures data confidentiality, integrity, and authenticity, building trust with users and search engines.
- By implementing HTTPS correctly and following best practices, organizations can enhance the security of their websites and safeguard user data.

SSH (Secure Shell) - Secure Remote Access and File Transfer

Introduction to SSH

- SSH (Secure Shell) is a cryptographic network protocol that provides secure remote access and file transfer between two systems.
- It offers a secure alternative to traditional remote access protocols like Telnet and FTP.
- SSH ensures the confidentiality, integrity, and authenticity of data exchanged between client and server.

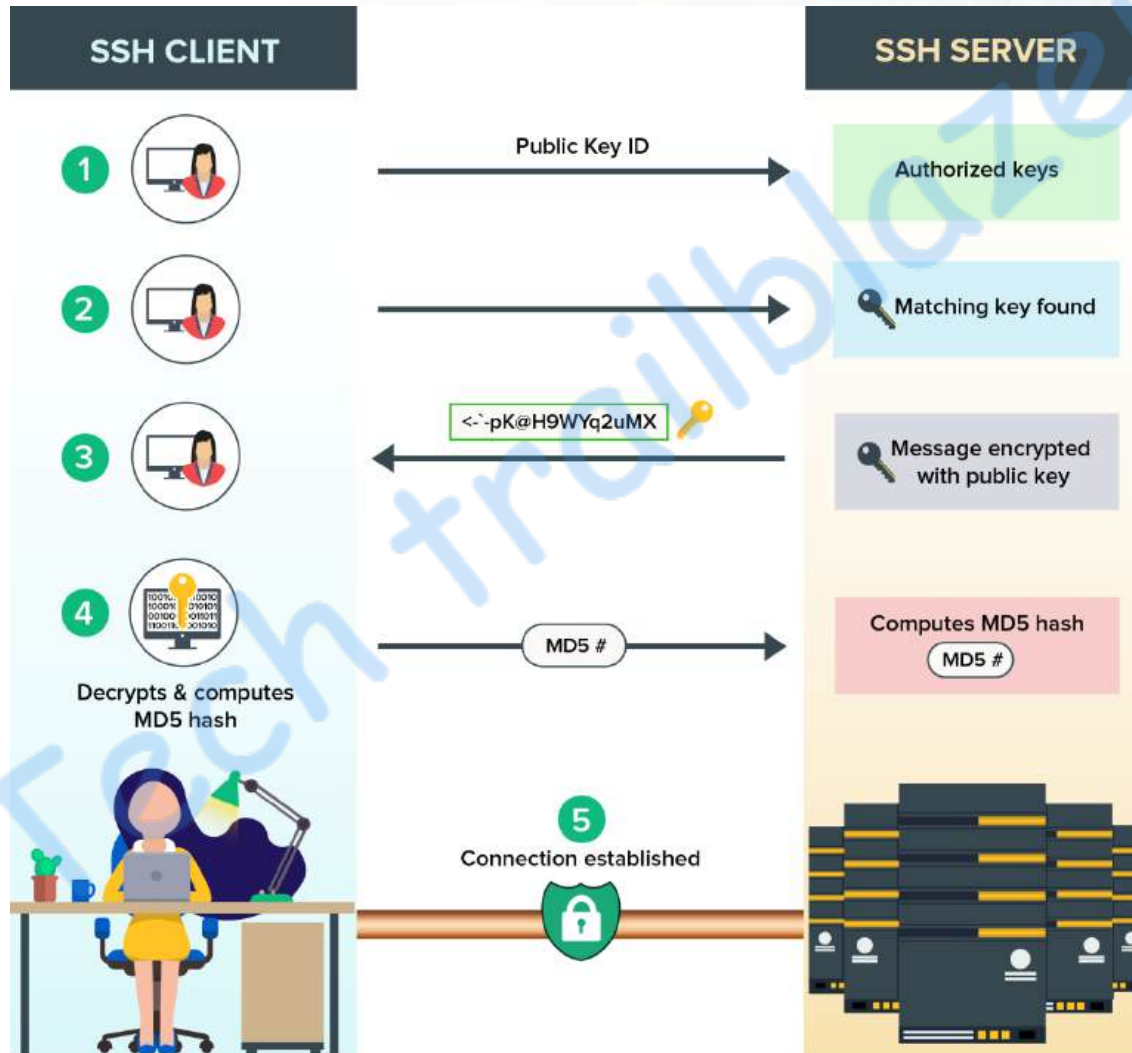


How SSH Works

SSH uses public-key cryptography and encryption to establish a secure connection:

1. **Client Authentication:** The client initiates a connection to the server using SSH and provides its public key.
2. **Server Authentication:** The server presents its public key to the client, which the client verifies to ensure the authenticity of the server.
3. **Session Key Exchange:** Both client and server agree on a session key, which is used for symmetric encryption and decryption of data during the session.
4. **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the session key.
5. **Command Execution and File Transfer:** The client can securely execute remote commands or transfer files to and from the server.

HTTPS Working



Benefits of SSH

SSH offers several advantages for secure remote access and file transfer:

- **Encryption:** All data transmitted over SSH is encrypted, protecting it from unauthorized access or interception.
- **Authentication:** SSH uses public-key cryptography for user authentication, ensuring secure access to remote systems.
- **Data Integrity:** SSH verifies the integrity of data during transmission, preventing tampering or unauthorized modification.
- **Port Forwarding:** SSH allows secure tunneling of other protocols, enabling remote access to services running on a server's local network.
- **Cross-Platform Compatibility:** SSH is available on various operating systems, making it widely accessible for remote administration.

SSH Implementation

Steps to implement SSH for remote access and file transfer:

1. Install an SSH server on the remote system you want to access.
2. Generate an SSH key pair on the client machine.
3. Configure the SSH server to allow remote access using the generated SSH public key.
4. Use an SSH client (e.g., OpenSSH, PuTTY) to establish a secure connection to the remote system using the SSH key pair.

SSH Best Practices

Best practices for implementing and using SSH:

- Use strong and unique SSH key pairs for authentication.
- Disable password-based authentication to enhance security.
- Regularly update SSH software and apply security patches.
- Implement firewall rules to allow SSH access only from trusted IP addresses.
- Monitor SSH logs for suspicious activity and enable two-factor authentication for added security.

Conclusion

- SSH is a critical protocol for secure remote access and file transfer.
- It provides encryption, authentication, and data integrity, ensuring secure communication between client and server.
- By implementing SSH correctly and following best practices, organizations can protect sensitive information and maintain secure remote administration.



SSL (Secure Sockets Layer) - Ensuring Secure Communication

Introduction to SSL

- SSL (Secure Sockets Layer) is a cryptographic protocol that provides secure communication over the internet.
- It ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.
- SSL has been succeeded by Transport Layer Security (TLS), but the term "SSL" is still commonly used.



Secure Sockets Layer

How SSL Works

- SSL handshake process:
- **Client Hello:** The client initiates a connection request to the server, presenting its supported SSL/TLS versions and cipher suites.
- **Server Hello:** The server responds by selecting the appropriate SSL/TLS version and cipher suite from the client's options.
- **Certificate Exchange:** The server sends its SSL certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
- **Client Authentication:** If required, the client presents its own SSL certificate to the server for authentication.
- **Session Key Exchange:** The client and server establish a session key for symmetric encryption and decryption of data during the session.
- **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the session key.
- **Session Closure:** When the session ends, the client and server exchange closure messages to properly terminate the connection.

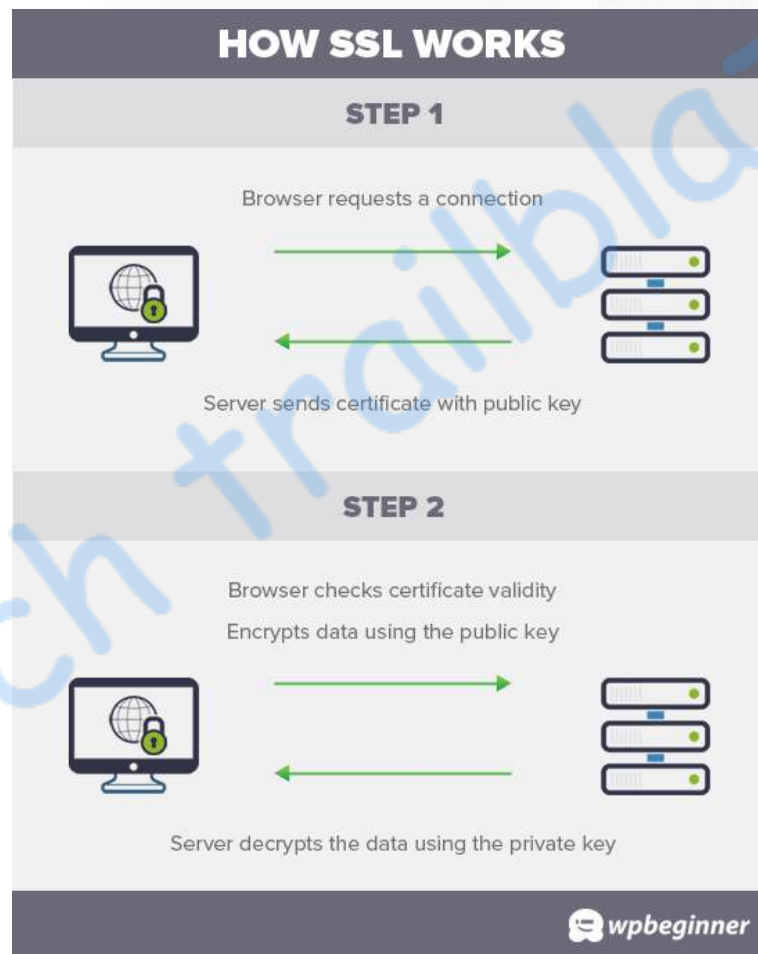
SSL Working



SSL Certificate

- SSL certificates play a crucial role in SSL/TLS communication:
- They are digital files that bind an organization's identity with a public key.
- Issued by trusted Certificate Authorities (CAs), SSL certificates provide authenticity and trust to the SSL/TLS connection.
- SSL certificates contain information such as the domain name, organization name, CA's digital signature, and the public key.

SSL Working with certificate



Benefits of SSL

- SSL provides several advantages for secure communication:
- **Data Encryption:** SSL encrypts sensitive information, such as login credentials and financial details, ensuring their confidentiality.
- **Data Integrity:** SSL ensures that data remains intact during transmission, preventing unauthorized modification.
- **Authentication:** SSL certificates verify the identity of the server, assuring users that they are connecting to the intended website and not an imposter.
- **Trust and User Confidence:** Displaying the padlock symbol and "https" in the URL enhances trust and reassures users about the security of the website.
- **Compliance:** SSL is often required to meet regulatory and compliance standards, such as PCI DSS for secure payment processing.

SSL Implementation

Steps to implement SSL on a website:

- Obtain an SSL certificate from a trusted CA.
- Install the SSL certificate on the web server.
- Configure the server to use SSL/TLS protocols and enable HTTPS.
- Test the SSL implementation to ensure it is functioning correctly.

SSL Best Practices

Best practices for SSL implementation and management:

- Keep SSL certificates up to date and renew them before expiration.
- Use strong encryption algorithms and secure cipher suites.
- Implement HTTP Strict Transport Security (HSTS) to enforce HTTPS usage.
- Regularly monitor and audit SSL configurations for vulnerabilities.
- Educate users on how to identify SSL indicators, such as padlock symbols and "https" in URLs.

Conclusion

- SSL is a vital technology for ensuring secure communication over the internet.
- It provides data encryption, authentication, and integrity, fostering trust and user confidence.
- By implementing SSL correctly and following best practices, organizations can enhance the security of their online services and protect sensitive information.



TLS (Transport Layer Security) - Ensuring Secure Communication

Introduction to TLS

- TLS (Transport Layer Security) is a cryptographic protocol that provides secure communication over the internet.
- It is the successor to SSL (Secure Sockets Layer) and offers enhanced security features.
- TLS ensures the confidentiality, integrity, and authenticity of data transmitted between clients and servers.

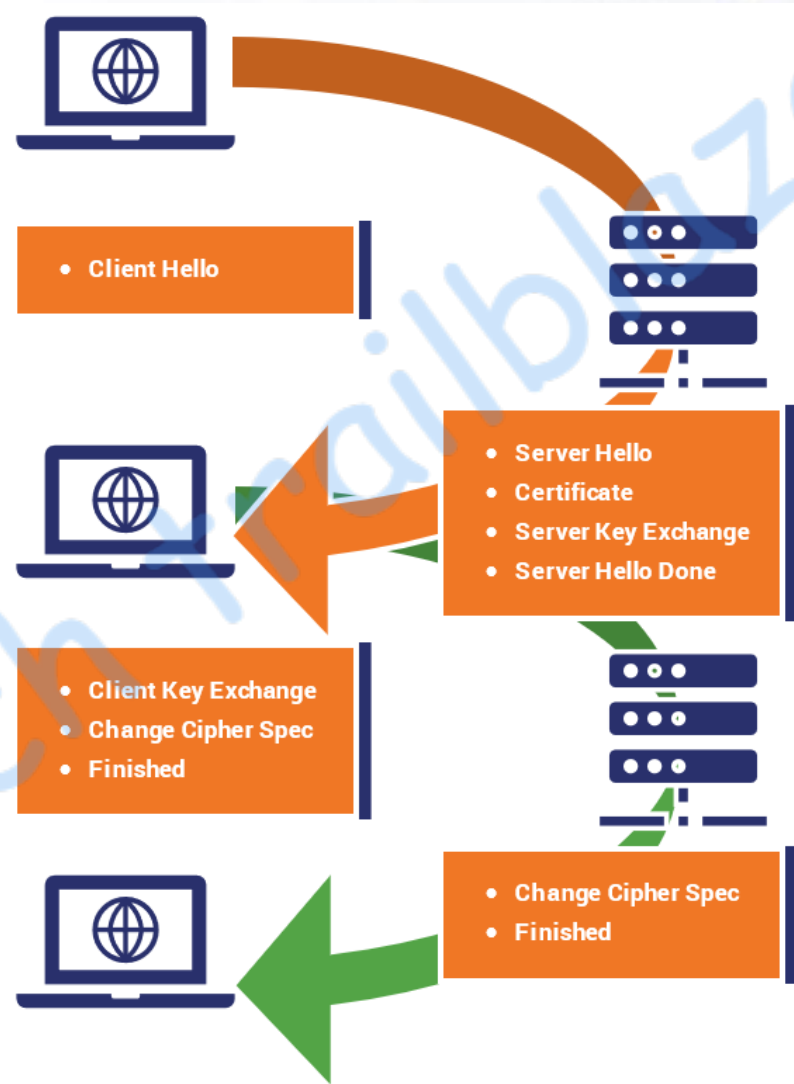


How TLS Works

TLS handshake process:

1. **Client Hello:** The client initiates a connection request to the server, presenting its supported TLS versions and cipher suites.
2. **Server Hello:** The server responds by selecting the appropriate TLS version and cipher suite from the client's options.
3. **Certificate Exchange:** The server sends its TLS certificate to the client, containing the server's public key and digitally signed by a trusted Certificate Authority (CA).
4. **Client Authentication:** If required, the client presents its own TLS certificate to the server for authentication.
5. **Key Exchange:** The client and server negotiate a shared secret key for symmetric encryption and decryption of data during the session.
6. **Secure Data Exchange:** All subsequent data exchanged between the client and server is encrypted using the shared secret key.
7. **Session Closure:** When the session ends, the client and server exchange closure messages to properly terminate the connection.

TSL Working



TLS Versions and Cipher Suites

TLS supports various versions and cipher suites to ensure secure communication:

- **TLS versions:** TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 (the latest version).
- **Cipher suites:** Combinations of encryption algorithms, authentication methods, and key exchange protocols.

Benefits of TLS

TLS provides several advantages for secure communication:

- **Strong Encryption:** TLS uses robust encryption algorithms to protect data from unauthorized access.
- **Data Integrity:** TLS ensures that data remains intact during transmission and detects any tampering attempts.
- **Authentication:** TLS certificates verify the identity of the server, assuring users they are connecting to the correct website.
- **Forward Secrecy:** TLS supports forward secrecy, ensuring that even if a private key is compromised, past communications remain secure.
- **Compatibility:** TLS is widely supported by modern web browsers and applications, enabling secure communication across platforms.

TLS Implementation

Steps to implement TLS on a website:

1. Obtain a TLS certificate from a trusted CA.
2. Install the TLS certificate on the web server.
3. Configure the server to use TLS protocols and enable HTTPS.
4. Regularly update TLS software and libraries to stay protected against vulnerabilities.

TLS Best Practices

Best practices for TLS implementation and management:

- Use the latest TLS version supported by your infrastructure.
- Select strong cipher suites that prioritize security and performance.
- Enable Perfect Forward Secrecy (PFS) to enhance security.
- Implement strict certificate validation and revocation checking.
- Regularly monitor and audit TLS configurations for vulnerabilities.

Conclusion

- TLS is a critical technology for ensuring secure communication over the internet.
- It offers strong encryption, data integrity, and authentication, enhancing the overall security of online services.
- By implementing TLS correctly and following best practices, organizations can protect sensitive information and establish trust with their users.



IPsec (Internet Protocol Security) - Securing Network Communications

Introduction to IPsec

- IPsec (Internet Protocol Security) is a suite of protocols and cryptographic techniques used to secure network communications at the IP layer.
- It provides a robust framework for ensuring the confidentiality, integrity, and authenticity of IP packets transmitted over a network.



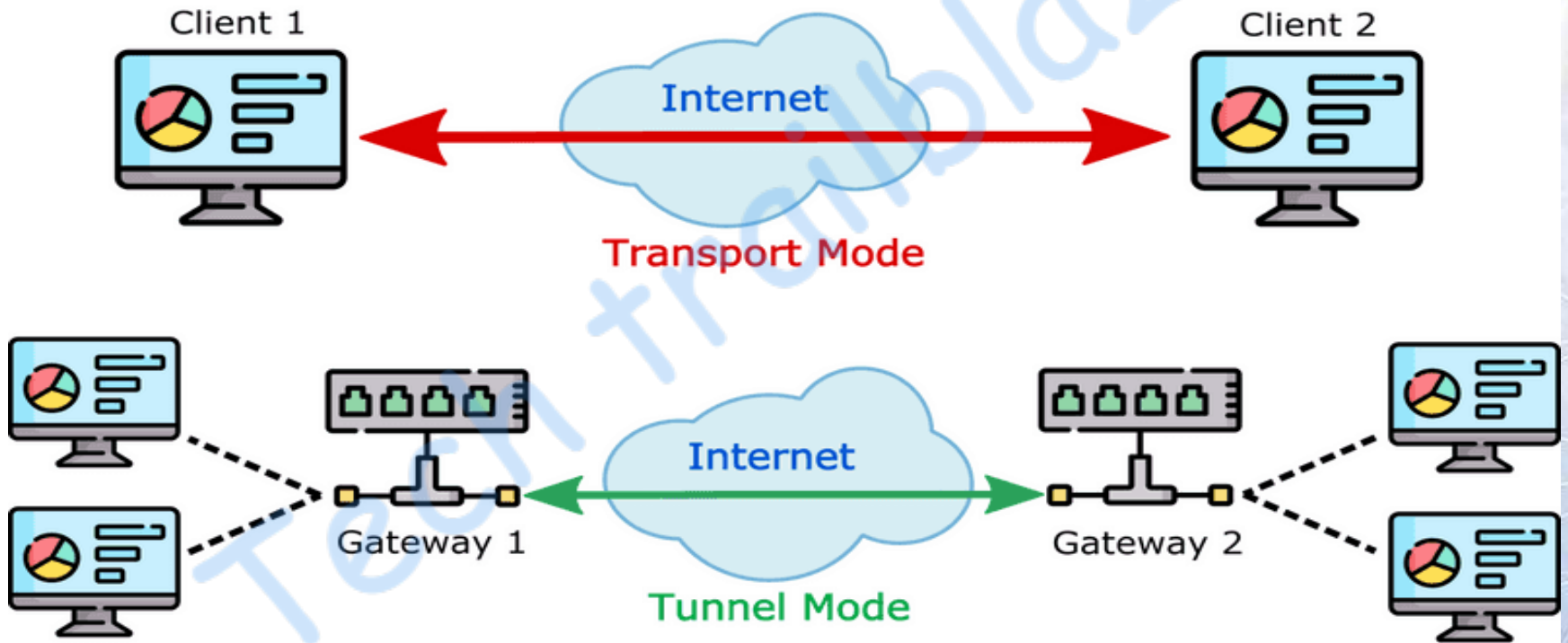
How IPsec Works?

IPsec operates in two main modes: Transport mode and Tunnel mode:

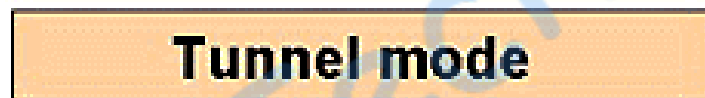
1. **Transport Mode:** Protects the data payload of IP packets, leaving the original IP header intact. It is typically used for end-to-end communication within a network.
2. **Tunnel Mode:** Encrypts the entire IP packet, including the original IP header, and encapsulates it within a new IP packet. It is often used for secure communication between networks.

IPsec Working

IPSec Modes



IPsec Modes

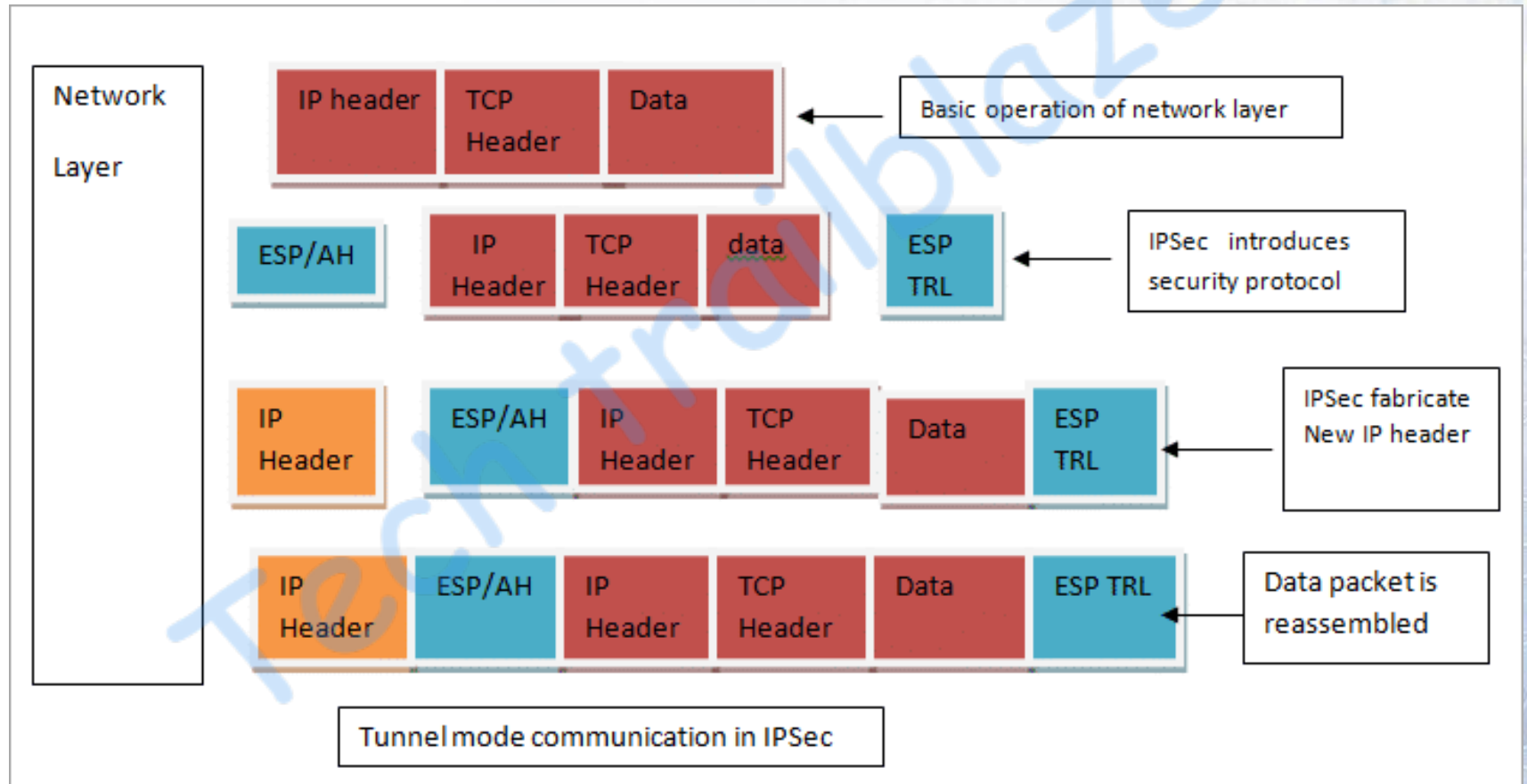


Components of IPsec

IPsec consists of several key components:

1. **Authentication Header (AH):** Provides data integrity and authentication of IP packets.
2. **Encapsulating Security Payload (ESP):** Offers data confidentiality, integrity, and authentication through encryption and encapsulation.
3. **Security Associations (SA):** Establishes the security parameters, including encryption algorithms, authentication methods, and key management, between two communicating entities.
4. **Key Management:** Involves the secure exchange, generation, and management of cryptographic keys used by IPsec for encryption and authentication.

Tunnel Mode Detail



Benefits of IPsec

IPsec offers numerous advantages for securing network communications:

1. **Confidentiality:** Encrypts IP packets, preventing unauthorized access and eavesdropping of sensitive data.
2. **Integrity:** Verifies the integrity of IP packets, ensuring they have not been tampered with during transit.
3. **Authentication:** Authenticates the source of IP packets, preventing spoofing and unauthorized access.
4. **Seamless Integration:** IPsec can be implemented at the network layer, providing security for all applications and protocols that use IP.
5. **Interoperability:** IPsec is a widely supported standard, allowing secure communication between different vendors and platforms.

IPsec Implementation

Steps to implement IPsec in a network:

1. **Assess Network Requirements:** Determine the specific security needs and objectives of the network.
2. **Plan IPsec Policy:** Define security policies, including encryption algorithms, authentication methods, and key management approaches.
3. **Configure IPsec Devices:** Configure IPsec parameters on network devices, such as routers, firewalls, or VPN concentrators, based on the defined policies.
4. **Test and Monitor:** Perform thorough testing to ensure IPsec is functioning correctly and continuously monitor the network for any potential issues or vulnerabilities.

Conclusion

- IPsec is a powerful security protocol suite that protects network communications at the IP layer, ensuring confidentiality, integrity, and authenticity.
- By implementing IPsec correctly and following best practices, organizations can secure their network infrastructure and protect sensitive data from unauthorized access.



SHTTPS (Secure Hypertext Transfer Protocol Secure) - Strengthening Web Security

Introduction to SHTTPS

- SHTTPS (Secure Hypertext Transfer Protocol Secure) is an enhanced version of HTTPS that integrates additional security measures.
- It combines the secure communication features of HTTPS with additional mechanisms to protect against various web security threats.



Why SHTTPS?

- Traditional HTTPS provides secure communication between clients and servers, but SHTTPS further strengthens web security by addressing specific vulnerabilities and attacks.
- SHTTPS aims to mitigate risks related to website tampering, data integrity, and man-in-the-middle attacks.

Key Features of SHTTPS

SHTTPS incorporates the following key features to enhance web security:

- **Subresource Integrity (SRI):**
 - SRI ensures that external resources, such as scripts and stylesheets, loaded by a webpage are not tampered with during transit.
 - It uses cryptographic hashes to verify the integrity of the resources, allowing the browser to block or warn if any modifications are detected.
- **Certificate Transparency (CT):**
 - CT is a framework that provides public auditing and monitoring of SSL/TLS certificates issued by Certificate Authorities (CAs).
 - It aims to detect and mitigate misissued or fraudulent certificates, enhancing trust and accountability in the certificate ecosystem.
- **HTTP Public Key Pinning (HPKP):**
 - HPKP allows website operators to specify a list of cryptographic hashes of their SSL/TLS public keys in the HTTP response header.
 - This helps protect against rogue or compromised CAs by instructing the browser to only accept specific public keys for future connections to the website.

Benefits of SHTTIPS

SHTTIPS offers several advantages for web security:

- **Enhanced Protection:** SHTTIPS strengthens the overall security of websites by addressing specific vulnerabilities and threats.
- **Tamper Detection:** SRI helps ensure the integrity of external resources and prevents unauthorized modifications.
- **Certificate Accountability:** CT provides transparency and oversight of SSL/TLS certificates, reducing the risk of misissued or fraudulent certificates.
- **Key Validation:** HPKP allows website operators to enforce the use of specific public keys, protecting against compromised or unauthorized certificates.
- **User Trust:** Implementing SHTTIPS demonstrates a commitment to web security, enhancing user confidence and trust in the website.

Implementing SHTTPS

Steps to implement SHTTPS on a website:

- **Enable HTTPS:** Ensure that your website is already using HTTPS for secure communication.
- **Subresource Integrity (SRI):** Implement SRI by adding integrity attributes to external resource references (e.g., script and stylesheet tags) in your web pages.
- **Certificate Transparency (CT):** Utilize CT logs and monitoring services to track and validate SSL/TLS certificates issued for your website.
- **HTTP Public Key Pinning (HPKP):** Carefully consider the implications of HPKP, as it requires careful management of public keys and potential risks associated with pinning.

Conclusion

- SHTTIPS is an advanced approach to web security, integrating additional measures to strengthen HTTPS and protect against specific vulnerabilities.
- By implementing SHTTIPS and leveraging its features, website owners can enhance the integrity, trustworthiness, and overall security of their web presence.

FTPS (File Transfer Protocol Secure)

Ensuring Secure and Reliable File Transfers

Whole topic specially best practices
important

Introduction to FTPS

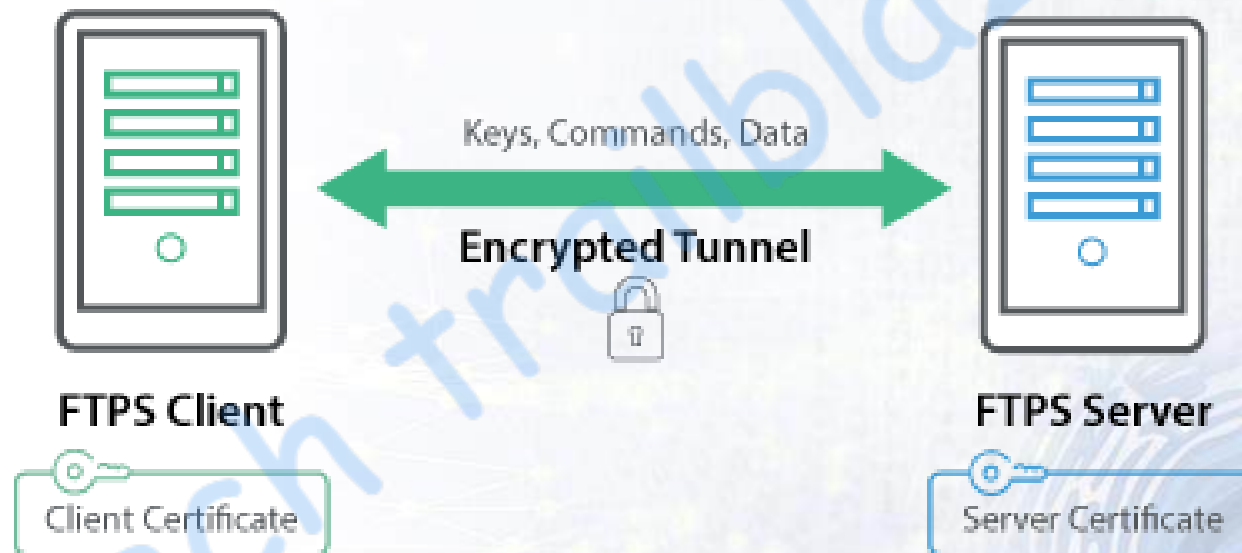
- FTPS is a secure file transfer protocol that combines the traditional FTP protocol with the security features of SSL/TLS encryption.
- It provides a secure and reliable method for transferring files over a network, ensuring data integrity and confidentiality.
- FTPS is widely used in various industries, including banking, healthcare, and e-commerce, where secure file transfers are crucial.



How FTPS Works?

- FTPS utilizes SSL/TLS encryption to secure the communication between the client and the server.
- SSL/TLS establishes a secure and encrypted connection, preventing unauthorized access and eavesdropping.
- FTPS supports both implicit and explicit modes, offering flexibility in choosing the level of security required.

FTPS working



Key Features of FTPS

- **Encryption:** FTPS uses SSL/TLS encryption to protect data during transit, safeguarding it from interception and tampering.
- **Authentication:** FTPS provides strong authentication mechanisms, ensuring that only authorized users can access and transfer files.
- **Data Integrity:** Through SSL/TLS, FTPS guarantees the integrity of transferred files, detecting any unauthorized modifications.
- **Portability:** FTPS is supported by various operating systems and FTP client software, making it widely compatible and accessible.

Benefits of Using FTPS

Enhanced Security: FTPS offers a higher level of security compared to standard FTP, making it suitable for sensitive data transfers.

Compliance with Regulations: FTPS helps organizations meet regulatory requirements for data protection, such as HIPAA and GDPR.

Reliability: FTPS ensures the reliable delivery of files, minimizing errors and interruptions during transfers.

Flexibility: With implicit and explicit modes, FTPS allows organizations to choose the level of security that best suits their needs.

Use Cases for FTPS

- **Banking and Finance:** FTPS enables secure transfer of financial data, such as transactions, statements, and sensitive customer information.
- **Healthcare:** FTPS is used for transferring confidential patient records, medical images, and other sensitive healthcare data.
- **E-commerce:** FTPS ensures secure exchange of product information, inventory updates, and customer data between online retailers and suppliers.



Best Practices for FTPS Implementation

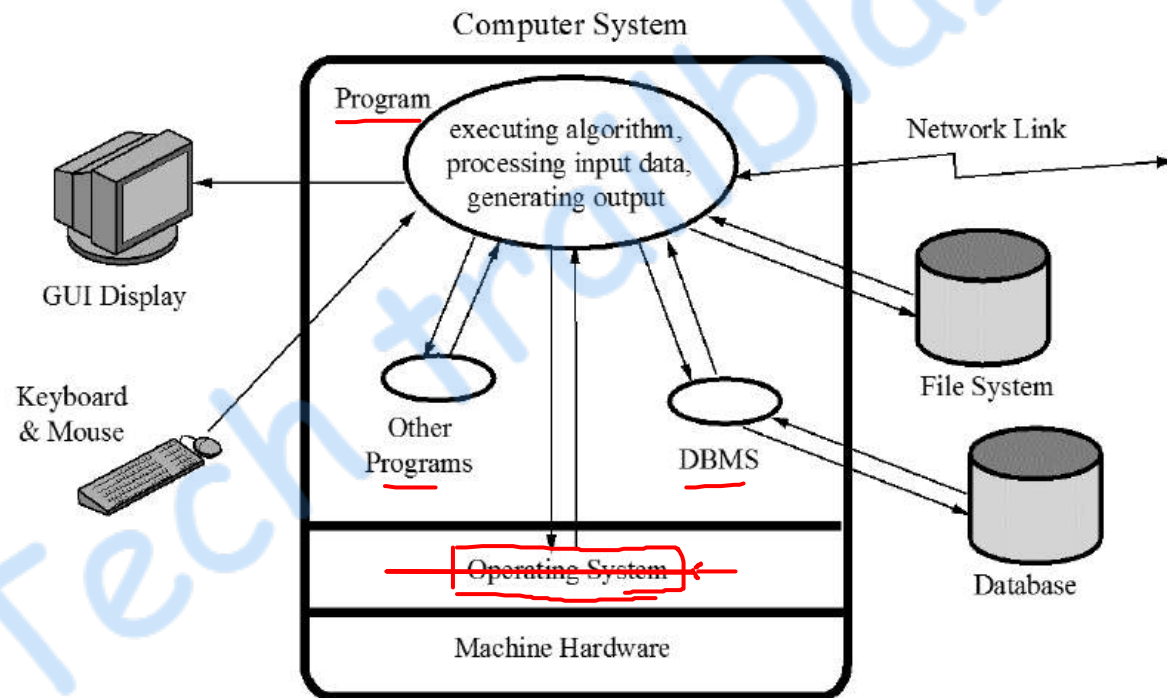
1. **Use Strong Authentication:** Implement strong username/password combinations or consider additional authentication methods like certificates.
2. **Regularly Update SSL/TLS Certificates:** Keep SSL/TLS certificates up to date to maintain the security of the FTPS server.
3. **Employ Access Controls:** Restrict FTPS access to authorized users and employ granular permissions to limit access to specific files and directories.
4. **Monitor and Audit:** Implement logging and monitoring mechanisms to track FTPS activities and detect any suspicious or unauthorized actions.

Conclusion

- FTPS is a secure and reliable file transfer protocol that combines the benefits of FTP with SSL/TLS encryption.
- By implementing FTPS, organizations can ensure the confidentiality, integrity, and secure transfer of sensitive data.
- With its wide compatibility and industry adoption, FTPS remains a trusted solution for secure file transfers in various sectors.

Operating System Security

Recall... Abstract View of Program



Operating System Security

Computer are rarely used in isolation

- Usually connected to some kind of network, Internet etc.

Networked computers

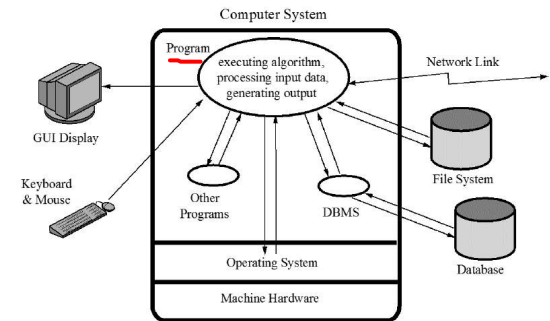
- ensure secure operation in networked environment

New threat?

- Attackers coming from the network.
- Network-facing programs on computers may be buggy.
- Users may be hurt via online communication.

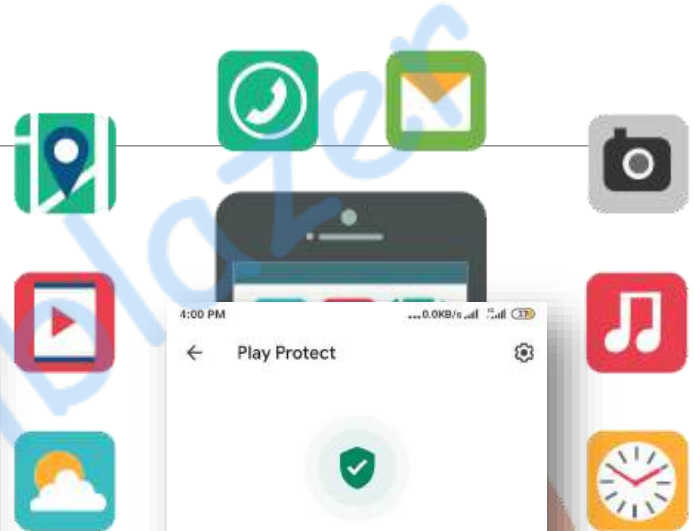
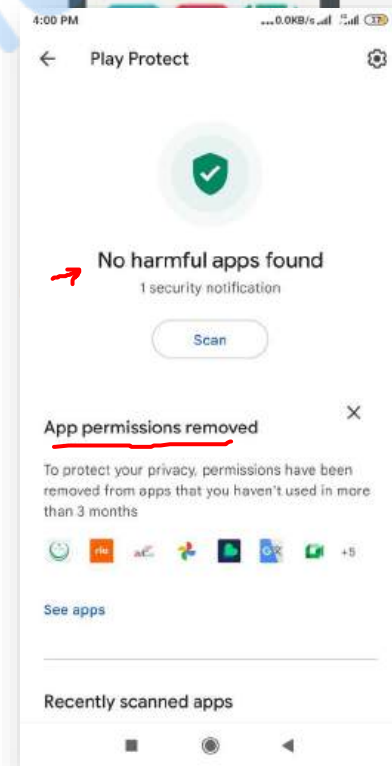
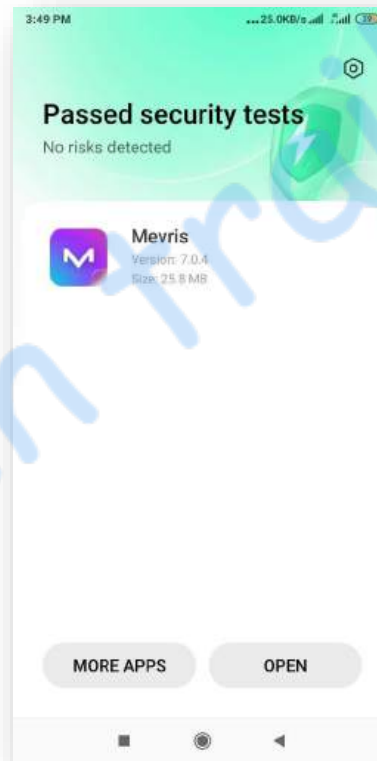
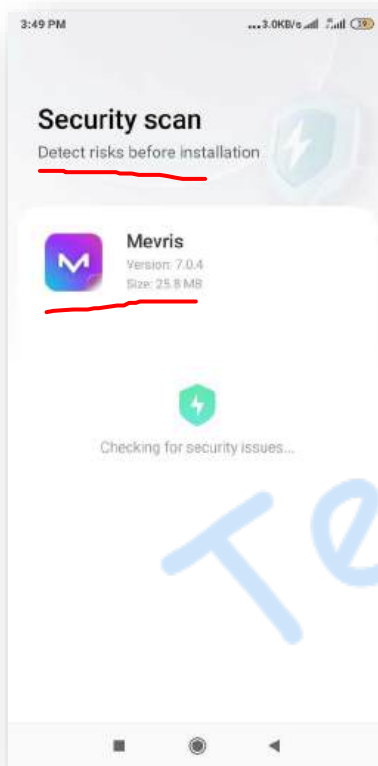
Security mechanisms

- Authentication; Access Control
- Secure Communication (using cryptography)
- Logging & Auditing
- Intrusion Prevention and Detection



Mobile Operating System Security

Mobile computing devices:



Mobile Operating System Security

Mobile computing devices:

New threat?

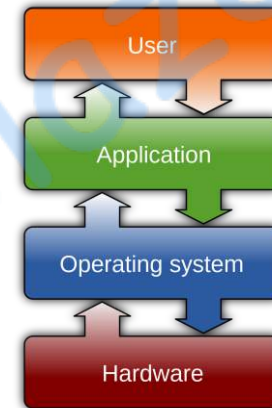
- Apps (programs) may be malicious.
- More tightly connected with personal life of the user e.g. personal health and banking apps.

Security mechanisms?

- ○ Isolation of each app.
- ○ Users assess risks of apps.
- ○ Risk communication.

→ **Google Play Protect**

<https://support.google.com/googleplay/answer/2812853?hl=en>



Use Google Play Protect to help keep your apps safe and your data private

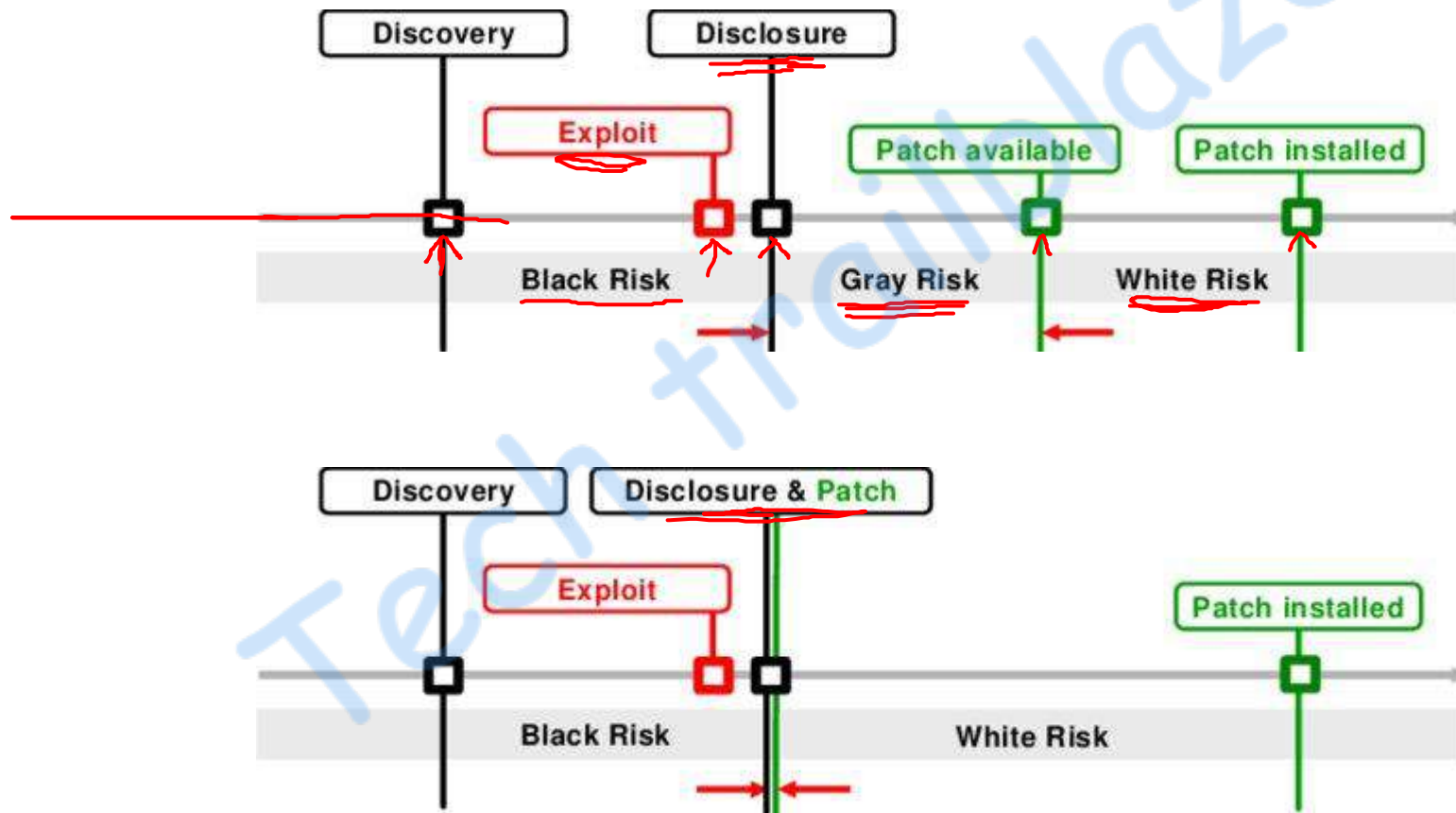
Google Play Protect checks your apps and devices for harmful behavior.

- • It runs a safety check on apps from the Google Play Store before you download them.
- It checks your device for potentially harmful apps from other sources. These harmful apps are sometimes called malware.
- It warns you about potentially harmful apps.
- It may deactivate or remove harmful apps from your device.
- It warns you about detected apps that violate our Unwanted Software Policy by hiding or misrepresenting important information.
- It sends you privacy alerts about apps that can get user permissions to access your personal information, violating our Developer Policy.
- It may reset app permissions to protect your privacy on certain Android versions.

Operating System Hardening

Operating Systems' Risks

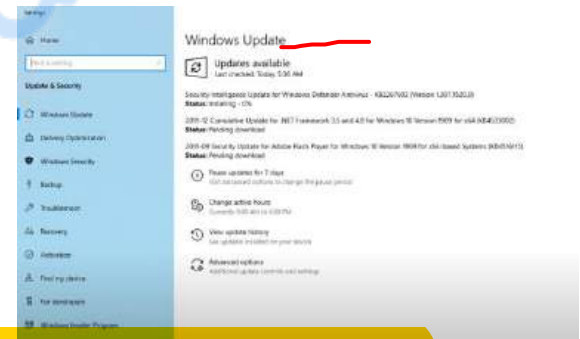
Vulnerability, Exploit, Patch...



Operating Systems Hardening

- The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications.

- Updates in Windows
- Patch Management System in Linux/Unix



- **Basic steps**

- Install and patch the operating system

- Harden and configure the operating system to adequately address the identified security needs of the system by:

- ➔ ■ Removing unnecessary services, applications, and protocols
 - ➔ ■ Configuring users, groups, and permissions
 - ➔ ■ Configuring resource controls

- Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)

- ➔ ○ Test the security of the basic operating system to ensure that the steps taken adequately address its security needs



Remove
Unnecessary
Services,
Applications,
Protocols

• When performing the initial installation the supplied defaults should not be used

○ Default configuration is set to maximize ease of use and functionality rather than security

○ If additional packages are needed later they can be installed when they are required

→ If fewer software packages are available to run the risk is reduced

— System planning process should identify what is actually required for a given system



Configure Users, Groups, and Authentication

Not all users with access to a system will have the same access to all data and resources on that system

→ Elevated privileges should be restricted to only those users that require them, and then only when they are needed to perform a task

→ • System planning process should consider:

→ ○ Categories of users on the system

→ ○ Privileges they have

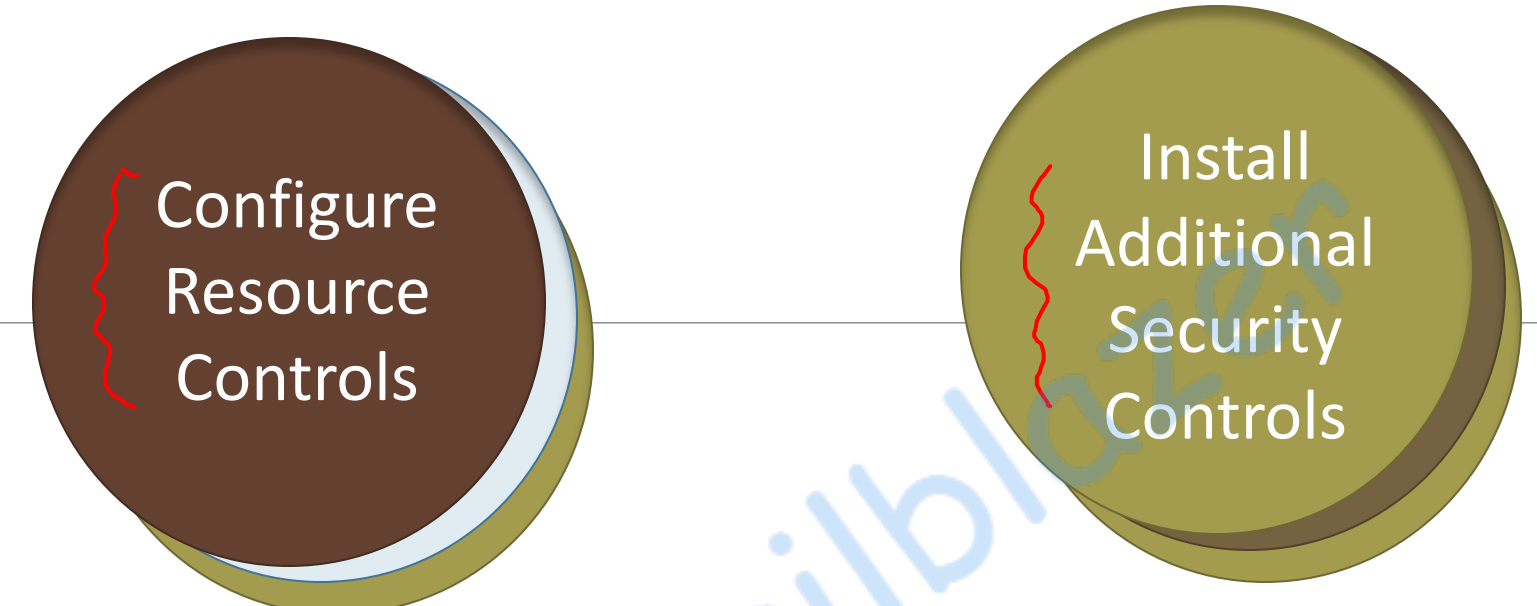
→ ○ Types of information they can access

→ ○ How and where they are defined and authenticated

→ • Default accounts included as part of the system installation should be secured

○ Those that are not required should be either removed or disabled

○ Policies that apply to authentication credentials configured



Configure Resource Controls

Install Additional Security Controls

Once the users and groups are defined, appropriate permissions can be set on data and resources

Many of the security hardening guides provide lists of recommended changes to the default access configuration

- Further security possible by installing and configuring additional security tools:

- Anti-virus software
- Host-based firewalls
- IDS or IPS software
- Application white-listing



Test the System Security

- Final step in the process of initially securing the base operating system is security testing

- Goal:

- Ensure the previous security configuration steps are correctly implemented

- ○ Identify any possible vulnerabilities

- There are programs specifically designed to:

- ○ Review a system to ensure that a system meets the basic security requirements

- Scan for known vulnerabilities and poor configuration practices

- Should be done following the initial hardening of the system

- Repeated periodically as part of the security maintenance process

Security Maintenance

Security Maintenance

Process of maintaining security is continuous

Security maintenance includes:

- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security
- Using appropriate software maintenance processes to patch and update all critical software

Logging

Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

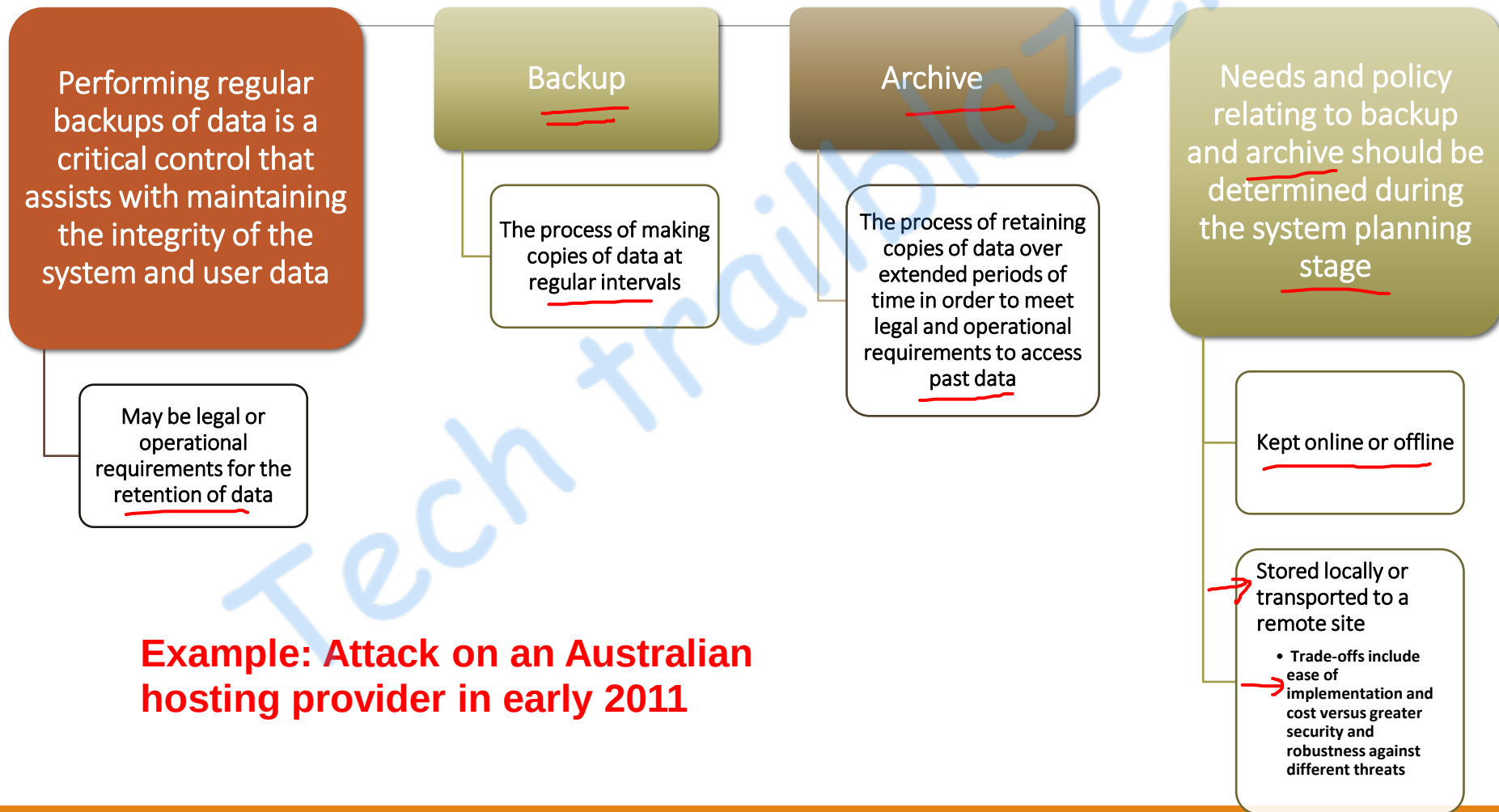
Generates significant volumes of information and it is important that sufficient space is allocated for them

- automatic log rotation

Automated analysis is preferred

Data Backup and Archive

Data Backup and Archive



Linux/Unix Security

Linux/Unix Security



.deb	64 bit	ARM	ARM 64
.rpm	64 bit	ARM	ARM 64
.tar.gz	64 bit	ARM	ARM 64

Patch Management

- Keeping security patches up to date is a widely recognized and critical control for maintaining security
 - Debian based distribution e.g. Ubuntu...include apt-get
 - RPM... Redhat based distribution e.g. Fedora...include up2date or yum
- Application and service configuration
 - Most commonly implemented using separate text files for each application and service
 - Generally located either in the /etc directory or in the installation tree for a specific application
 - ○ Individual user configurations that can override the system defaults are located in hidden “dot” files in each user's home directory
 - ○ Most important changes needed to improve system security are to disable services and applications that are not required

Linux/Unix Security

Users, groups, and permissions

- Access is specified as granting read, write, and execute permissions to each of owner, group, and others for each resource
- These are set using the chmod command.

Understanding The Linux File Permissions

Column: 1 2 3 4

- rwx rwx rwx

Directory/File/Link Information User Rights Group Rights Others Rights

While the first column defines a directory, file or link, the next 3 columns (2, 3, 4) define the permissions for the User, Group and Others (everyone else) groups.

Linux Permissions Made Easy

user group everyone

- rwx rwx rwx

4 2 1 4 2 1 4 2 1

1 1 1 1 1 1 1 1 1

decimal notification
binary notification

7 7 7

decimal notification: add each number to obtain the value ($4 + 2 + 1 = 7$)
binary notification: convert it to decimal then you should have the value ($r-x = 101 \text{ base } 2 = 5 \text{ base } 10$)

```
israr@israr-VirtualBox: ~/Desktop/CS627/Assignment2
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls
AES aes-brute-force-master AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31 سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27 سمير aes-brute-force-master
-rw-rw-r-- 1 israr israr 5661 2021 27 سمير AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 777 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31 سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27 سمير aes-brute-force-master
-rwxrwxrwx 1 israr israr 5661 2021 27 سمير AES.c
```

```
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ chmod 700 AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$ ls -l
total 32
-rwxrwxr-x 1 israr israr 17784 2021 31 سمير AES
drwxrwxr-x 4 israr israr 4096 2021 27 سمير aes-brute-force-master
-rwx----- 1 israr israr 5661 2021 27 سمير AES.c
israr@israr-VirtualBox:~/Desktop/CS627/Assignment2$
```

Linux/Unix Security

○ Guides recommend changing the access permissions for critical directories and files

→ ○ Local exploit

- Software vulnerability that can be exploited by an attacker to gain elevated privileges

→ ○ Remote exploit

- Software vulnerability in a network server that could be triggered by a remote attacker

Windows Security

Windows Security

Patch management

- “Windows Update” and “Windows Server Update Service” assist with regular maintenance and should be used
- Third party applications also provide automatic update support

Users administration and access controls

- Systems implement discretionary access controls resources
- Vista and later systems also include mandatory integrity controls (MIC)
- Objects are labeled as being of low, medium, high, or system integrity level
- System ensures the subject's integrity is equal or higher than the object's level

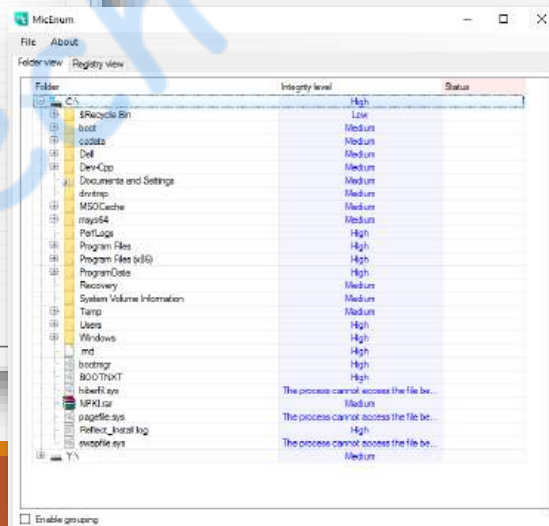
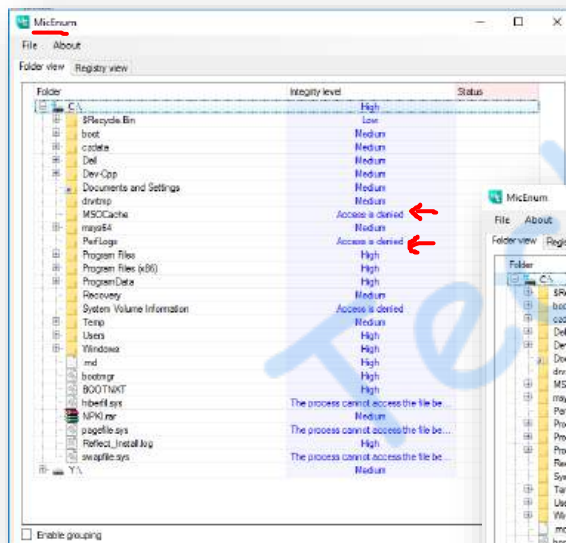
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

Windows Security

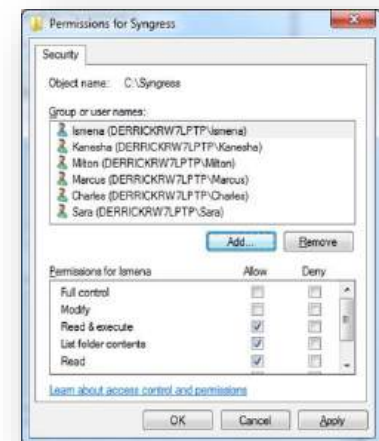
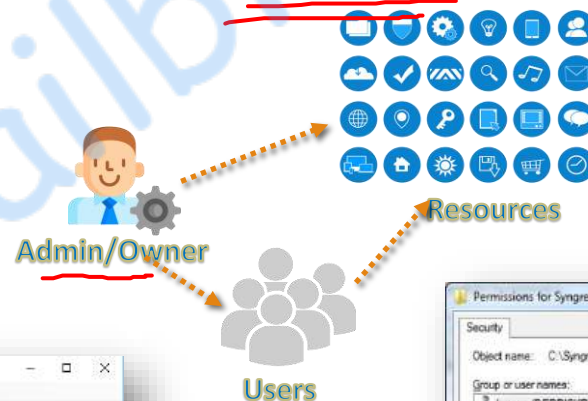
Mandatory Integrity Control (MIC) provides a mechanism for controlling access to securable objects. This mechanism is in addition to discretionary access control and evaluates access before access checks against an object's discretionary access control list (DACL) are evaluated

MANDATORY INTEGRITY CONTROL (MIC)

→ MicEnum Tool, Mandatory Integrity Control Enumerator



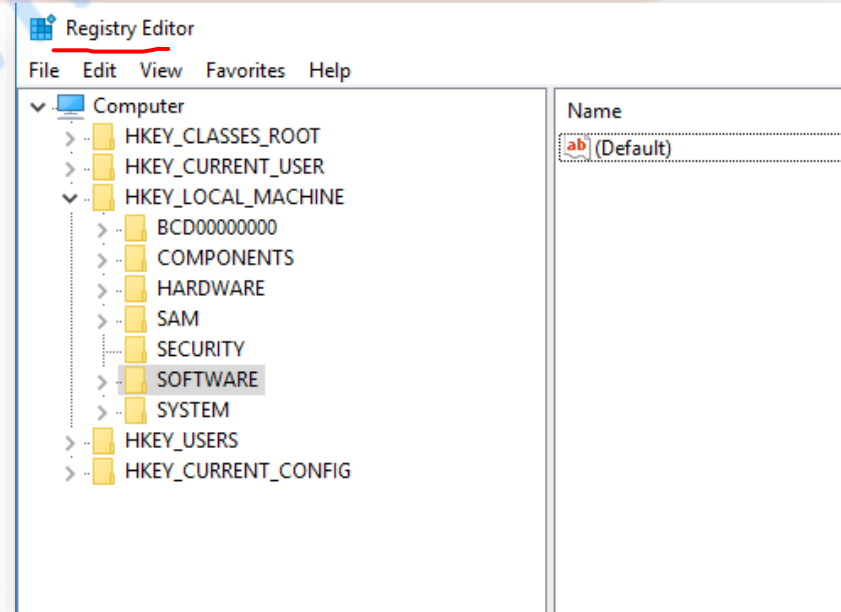
DISCRETIONARY ACCESS CONTROL LIST (DACL)



Windows Security

Application and service configuration

- Much of the configuration information is centralized in the Registry
- Forms a database of keys and values that may be queried and interpreted by applications
- Registry keys can be directly modified using the “Registry Editor”
- More useful for making bulk changes



Oth

- E o p

-

Name	PID	Status	User name	CPU	Memory (p...	Description
jusched.exe	3368	Running	israrullah	00	168 K	Java Update Scheduler
lkads.exe	3532	Running	lkClassAds	00	344 K	NI PSP Service Locator
lktstsvr.exe	3712	Running	SYSTEM	00	524 K	NI Time Synchronization
LMS.exe	10476	Running	SYSTEM	00	664 K	Intel(R) Local Management Service
lsass.exe	712	Running	SYSTEM	00	3,448 K	Local Security Authority Process
MacriumService.exe	2496	Running	SYSTEM	00	1,600 K	Macrium Reflect Utility Service
MpCmdRun.exe	1724	Running	NETWORK SERVICE	00	660 K	Microsoft Malware Protection Command Line Utility
MsMpEng.exe	2356	Running	SYSTEM	00	90,976 K	Antimalware Service Executable
niauth_daemon.exe	696	Running	LOCAL SERVICE	00	184 K	NI Auth Daemon
niDiscSvc.exe	1204	Running	SYSTEM	00	264 K	National Instruments Network Discovery Service
nidmsrv.exe	3732	Running	SYSTEM	00	472 K	NI Domain Service
nierserver.exe	11032	Running	israrullah	00	468 K	NI Error Reporting Server
nimdnsResponder.exe	3968	Running	SYSTEM	00	388 K	National Instruments Zeroconf Service
NisSrv.exe	4904	Running	LOCAL SERVICE	00	5,568 K	Microsoft Network Realtime Inspection Service
nissvcloc.exe	2092	Running	SYSTEM	00	156 K	Service Locator
OhCrosFXService.exe	1960	Running	SYSTEM	00	516 K	CrossFX Live Checker

Week 2 Properties

General | Sharing | Security | Previous Versions | Customize

Week 2

Type: File folder

Location: Y:\VU\CyberSecurity\CS627 CyberSecurity\Final Co

Size: 149 MB (156,515,013 bytes)

Size on disk: 149 MB (156,569,600 bytes)

Contains: 30 Files, 0 Folders

Created: Thursday, April 27, 2023, 11:00:06 AM

Attributes: ☒ Read-only (Only applies to files in folder)
☐ Hidden

Advanced...

OK Cancel Apply

Advanced Attributes

Choose the settings you want for this folder.

When you click OK or Apply on the Properties dialog, you will be asked if you want the changes to affect all subfolders and files as well.

Archive and Index attributes

☐ Folder is ready for archiving

☒ Allow files in this folder to have contents indexed in addition to file properties

Compress or Encrypt attributes

☐ Compress contents to save disk space

☒ Encrypt contents to secure data

[Details](#)

OK **Cancel**

The screenshot displays the Windows Control Panel window titled "BitLocker Drive Encryption". The breadcrumb navigation path is "Control Panel > All Control Panel Items > BitLocker Drive Encryption". The main heading is "BitLocker Drive Encryption" with a subtitle "Help protect your files and folders from unauthorized access by protecting your drives with BitLocker." Below this, there are three sections: "Operating system drive" showing "C: BitLocker off" with a "Turn on BitLocker" button; "Fixed data drives" showing "New Volume (Y:) BitLocker off"; and "Removable data drives - BitLocker To Go" with instructions to insert a USB flash drive. On the left, there are links for "See also", "TPM Administration", "Disk Management", and "Privacy statement".

Full-disk encryption with AES using BitLocker

Cyber Crime

Important for
mcqs.
mcqs

Tech trailblazer

Cyber Crime

- Cybercrime is a type of crime involving a **computer** or a **computer network**.
- The computer may have been **used in committing the crime**, or it may be the **target**.
- Cybercrime may harm someone, someone's security or finances.

Actors and Stakeholders

- Internationally, both **state** and **non-state** actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Cybercrimes **crossing international borders** and involving the actions of at least one nation-state are sometimes referred to as **cyberwarfare**.
- Warren Buffett describes cybercrime as the "number one problem with mankind" and said that it "poses real risks to humanity".

- A 2014 report sponsored by McAfee estimated that cybercrime had resulted in \$445 billion USD in annual damage to the global economy.
- Approximately \$1.5 billion was lost in 2012 to online credit and debit card fraud in the US.
- In 2018, a study by the Center for Strategic and International Studies (CSIS), in partnership with McAfee, concluded that nearly 1 percent of global gross domestic product (GDP), close to \$600 billion, is lost to cybercrime each year.
- The World Economic Forum 2020 Global Risk Report confirmed that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.

Privacy

- There are also many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise.

Tech trailblazer

Cyber Crime Categories

- Computer Fraud
- Cyberterrorism
- Ransomware
- Cybersex Trafficking
- Cyberwarfare
- Obscene / Offensive Content
- Ad-Fraud
- Online Harassment
 - Cyberbullying
 - Online predator
 - Cyberstalking
 - Cyber Racism
 - Internet troll
- Drug Trafficking
- Identity Theft
- Phishing

Computer Fraud

- Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system.
- If computer fraud involves the use of the internet, it can be considered **Internet fraud**.
- The legal definition of computer fraud varies by jurisdiction, but typically involves **accessing a computer without permission or authorization**.
- Forms of computer fraud include **hacking into computers to alter information, distributing malicious code** such as computer **worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams**.
- Other forms of fraud may be committed using computer systems, including **bank fraud, carding, identity theft, extortion, and theft of classified information**.
- These types of crimes often result in the loss of personal or financial information.

Cyberterrorism

- Cyberterrorism are acts of terrorism committed through the use of cyberspace or computer resources.
- Acts of disruption of computer networks and personal computers through viruses, worms, phishing, malicious software, hardware, or programming scripts can all be forms of cyberterrorism.
- Government officials and information technology (IT) security specialists have documented a significant increase in network problems and server scams since early 2001.
- Within the United States, there is an increasing concern from agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).
- Such incidents are part of an organized effort by cyberterrorist foreign intelligence services or other groups to map potential security flaws in critical systems.

Cyberextortion (Ransomware)

- Ransomware is a type of malware used in cyberextortion to restrict access to files, sometimes threatening permanent data erasure unless a ransom is paid.
- The threat of ransomware is a global issue, with more than 300 million attacks worldwide in 2021.
- According to the 2022 Unit 42 Ransomware Threat Report, the average ransom demand in cases handled by Norton climbed 144 percent to \$2.2 million.
- This report included an 85 percent increase in the number of victims who had their personal information shown on dark web information dumps.
- A loss of nearly \$400 million in 2021 and 2022 is just one of the statistics showing the impact of ransomware attacks on everyday people.

Cybersex Trafficking

- Cybersex trafficking is the transportation of victims and then the live streaming of coerced sexual acts or rape on webcam.
- Victims are abducted, threatened, or deceived and transferred to "cybersex dens".
- The dens can be in any location where the cybersex traffickers have a computer, tablet, or phone with an internet connection.
- Perpetrators use social media networks, video conferences, dating pages, online chat rooms, apps, dark web sites, and other platforms.
- They use online payment systems and cryptocurrencies to hide their identities.
- Millions of reports of its occurrence are sent to authorities annually.
- New legislation and police procedures are needed to combat this type of cybercrime.
- There are an estimated 6.3 million victims of cybersex trafficking, according to a recent report by the International Labour Organization and IOM.
- This number includes about 1.7 million child victims.
- An example of cybersex trafficking is the 2018–2020 Nth room case in South Korea.

Cyberwarfare

- The U.S. Department of Defense notes that cyberspace has emerged as a national-level concern through several recent events of geostrategic importance, including the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers.
- In August 2008, Russia again allegedly conducted cyberattacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia.
- Fearing that such attacks may become normalized in future warfare among nation-states, the military commanders intend to adapt the concept of cyberspace operations impact in the future.

Obscene or offensive content

- The content of websites and other electronic communications may be distasteful, obscene, or offensive for a variety of reasons. In some instances, these communications may be illegal.
- The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.
- One area of internet pornography that has been the target of the strongest efforts at curtailment is child pornography, which is illegal in most jurisdictions in the world.

Computer as a tool

- When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target.
- These crimes generally involve less technical expertise.
- Human weaknesses are generally exploited.
- The damage dealt is largely psychological and intangible, making legal action against the variants more difficult.
- These are the crimes which have existed for centuries in the offline world.
- Scams, theft, and the like existed before the development of computers and the internet.
- The same criminal has simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend.

Computer as a tool

- Crimes that use computer networks or devices to advance other ends include:
 - Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime)
 - Information warfare
 - Phishing scams
 - Spam
 - Propagation of illegal obscene or offensive content, including harassment and threats
- The unsolicited sending of bulk email for commercial purposes (spam) is unlawful in some jurisdictions.
- Phishing is mostly propagated via email.
- Phishing emails may contain links to other websites that are affected by malware.
- Or they may contain links to fake online banking or other websites used to steal private account information.

Ad-fraud

- Ad-frauds are particularly popular among cybercriminals, as such frauds are lucrative and less likely to be prosecuted.
- Jean-Loup Richet, a professor at the Sorbonne Business School, classified the large variety of ad-fraud committed by cybercriminals into three categories:
 - identity fraud, attribution fraud, and ad-fraud services.

Ad-fraud

- **Identity fraud** aims to impersonate real users and inflate audience numbers.
- Several ad-fraud techniques relate to this category and include
 - traffic from bots (coming from a hosting company or a data center, or from compromised devices);
 - cookie stuffing;
 - falsifying user characteristics, such as location and browser type;
 - fake social traffic (misleading users on social networks into visiting the advertised website);
 - the creation of fake social media accounts to make the bot appear legitimate.

Ad-fraud

- **Attribution fraud** impersonates the activities of real users, such as clicks and conversations.
- Multiple ad-fraud techniques belong to this category:
 - hijacked devices and the use of infected users (through malware) as part of a botnet to participate in ad fraud campaigns;
 - click farms (companies where low-wage employees are paid to click or engage in conversations and affiliates' offers);
 - incentivized browsing;
 - video placement abuse (delivered in display banner slots);
 - hidden ads (which will never be viewed by real users);
 - domain spoofing (ads served on a website other than the advertised real-time bidding website);
 - clickjacking, in which the user is forced to click on an ad.

Ad-fraud

- **Ad fraud services** are related to all online infrastructure and hosting services that might be needed to undertake identity or attribution fraud.
- Services can involve
 - the creation of spam websites (fake networks of websites created to provide artificial backlinks);
 - link building services;
 - hosting services;
 - creation of fake and scam pages impersonating a famous brand and used as part of an ad fraud campaign.

Online harassment

- Cyberbullying
- Online predator
- Cyberstalking
- Cyber Racism
- Internet troll

- Whereas content may be offensive in a non-specific way, harassment directs **obscenities** and **derogatory comments** at specific individuals focusing, for example, on gender, race, religion, nationality, or sexual orientation.
- There are instances when committing a crime using a computer can lead to an enhanced sentence.
 - For example, in the case of United States v. Neil Scott Kramer, the defendant was given an enhanced sentence according to the **U.S. Sentencing Guidelines Manual §2G1.3(b)(3)** for his use of a cell phone to "persuade, induce, entice, coerce, or facilitate the travel of, the minor to engage in prohibited sexual conduct."
 - Kramer appealed the sentence on the grounds that there was insufficient evidence to convict him under this statute because his charge included persuading through a computer device and his cellular phone technically is not a computer.
 - Although Kramer tried to argue this point, the U.S. Sentencing Guidelines Manual states that the term "computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

- In the **United States**, over 41 states have passed laws and regulations that regard extreme online harassment as a criminal act.
- These acts can be punished on a federal scale, such as **US Code 18 Section 2261A**, which states that using computers to threaten or harass can lead to a sentence of up to 20 years, depending on the action taken.
- Several countries outside the United States have also created laws to combat online harassment.
- In **China**, a country that supports over 20 percent of the world's internet users, the Legislative Affairs Office of the State Council passed a strict law against the bullying of young people through a bill in response to the Human Flesh Search Engine.
- The **United Kingdom** passed the **Malicious Communications Act**, among other acts from 1997 to 2013, which stated that sending messages or letters electronically that the government deemed "indecent or grossly offensive" and/or language intended to cause "distress and anxiety" can lead to a prison sentence of six months and a potentially large fine.
- **Australia**, while not directly addressing the issue of harassment, has grouped the majority of online harassment under the **Criminal Code Act of 1995**.
- Using telecommunication to send threats or harass and cause offense was a direct violation of this act.

- Freedom of Speech:

- Although freedom of speech is protected by law in most democratic societies (in the US this is done by the First Amendment), it does not include all types of speech.
- In fact, spoken or written "true threat" speech or text is criminalized because of "intent to harm or intimidate".
- That also applies to online or network-related threats in written text or speech.

- Cyberbullying:

- Cyberbullying has increased drastically with the growing popularity of online social networking.
- As of January 2020, 44 percent of adult internet users in the United States have "personally experienced online harassment".
- Children who experience online harassment deal with negative and sometimes life-threatening side effects.
- In 2021, reports displayed 41 percent of children developing social anxiety, 37 percent of children developing depression, and 26 percent of children having suicidal thoughts.

- Spying:

- The United Arab Emirates was named in a spying scandal where the Gulf nation along with other repressive governments purchased NSO Group's mobile spyware Pegasus for mass surveillance.
- Prominent activists and journalists were targeted as part of the campaign, including Ahmed Mansoor, Princess Latifa, Princess Haya, and more.
- Ghada Oueiss was one of the many high-profile female journalists and activists who became the target of online harassment.
- Oueiss filed a lawsuit against UAE ruler Mohamed bin Zayed Al Nahyan along with other defendants, accusing them of sharing her photos online.
- The defendants, including the UAE ruler, filed motions to dismiss the case of the hack-and-leak attack.

Drug trafficking

- Darknet markets are used to buy and sell recreational drugs online.
- Some drug traffickers use encrypted messaging tools to communicate with drug mules or potential customers.
- The dark web site Silk Road was the first major online marketplace for drugs, starting operation in 2011.
- It was permanently shut down in 2014 by the FBI and Europol.
- After Silk Road 2.0 went down, Silk Road 3 Reloaded emerged.
- However, it was just an older marketplace named Diabolus Market, that used the name for more exposure from the brand's previous success.

- Darknet markets have had a rise in traffic in recent years for many reasons, one of the biggest contributors being the anonymity offered in purchases, and often a seller-review system.
- There are many ways in which darknet markets can financially drain individuals.
- Vendors and customers alike go to great lengths to keep their identities a secret while online.
- Commonly used tools are virtual private networks (VPN), Tails, and the Tor Browser to help hide their online presence.

- Darknet markets entice customers by making them feel comfortable.
- People can easily gain access to a Tor browser with DuckDuckGo browser that allows a user to explore much deeper than other browsers such as Google Chrome.
- However, actually gaining access to an illicit market is not as simple as typing it in on a search engine like one would with Google.
- Darknet markets have special links that change frequently, ending in .onion as opposed to the typical .com, .net, and .org domain extensions.

- Digital/Virtual Currency:

- To add to privacy, the most prevalent currency on these markets is Bitcoin.
- Bitcoin allows transactions to be anonymous, with the only information available to the public being the record that a transaction occurred between two parties.

- An issue marketplace users face is when vendors or the market itself are exit scamming.
- This is when a vendor with a high rating will act as if they are selling on the market and have users pay for products they will not receive.
- The vendor will then close off their account after receiving money from multiple buyers and never send what was purchased.
- The vendors all being involved in illegal activities have a low chance of not exiting scamming when they no longer want to be a vendor.
- In 2019, an entire market known as Wall Street Market had allegedly exit scammed, stealing \$30 million dollars from the vendors' and buyers' wallets in bitcoin.

- FBI has cracked down on these markets.
- In July 2017, FBI seized one of the biggest markets, commonly called Alphabay, which later re-opened in August 2021 under the control of DeSnake, one of the original administrators.
- Investigators will pose as a buyer and order products from darknet vendors in the hopes that vendors leave a trail the investigators can follow.
- One investigation had an investigator pose as a firearms seller and for six months people purchased from them and provided home addresses.
- The FBI was able to make over a dozen arrests during this six-month investigation.

- Another one of law enforcement's crackdowns was on vendors selling fentanyl and opiates.
- With thousands of people dying each year due to drug overdose, investigators have made it a priority.
- Many vendors do not realize the extra criminal charges that go along with selling drugs online.
- Commonly they get charged with money laundering and charges for when the drugs are shipped in the mail on top of being a drug distributor.
- In 2019, a vendor was sentenced to 10 years in prison after selling cocaine and methamphetamine under the name JetSetLife.
- Although investigators spend large amounts of time tracking down people, in 2018, only 65 suspects who bought and sold illegal goods on some of the biggest markets were identified.
- This is compared to the thousands of transactions taking place daily on these markets.

Famous Incidents:

- Data Leaks
- Celebrity Leaks
- Blackmailing
- Web Defacements
- Hacking / Spying
- Data Stealing
- Impersonation
- Superimposing / Fake Media
- ATM Fraud/Hacking
- Car Hacking
- Cryptocurrency / Forex

Identity Theft

- Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.
- The term identity theft was coined in 1964.
- Since that time, the definition of identity theft has been statutorily defined throughout both the U.K. and the U.S. as the theft of personally identifiable information [PII].
- Identity theft deliberately uses someone else's identity as a method to gain financial advantages or obtain credit and other benefits, and perhaps to cause other person's disadvantages or loss.
- The person whose identity has been stolen may suffer adverse consequences, especially if they are falsely held responsible for the perpetrator's actions.
- Personally identifiable information generally includes a person's name, date of birth, social security number, driver's license number, bank account or credit card numbers, PINs, electronic signatures, fingerprints, passwords, or any other information that can be used to access a person's financial resources.

Phishing

- Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.
- Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim.
- As of 2020, it is the most common type of cybercrime, with the FBI's Internet Crime Complaint Centre reporting more incidents of phishing than any other type of computer crime.
- The term "phishing" was first recorded in 1995 in the cracking toolkit AOHell, but may have been used earlier in the hacker magazine 2600.
- It is a variation of fishing and refers to the use of lures to "fish" for sensitive information.
- Measures to prevent or reduce the impact of phishing attacks include legislation, user education, public awareness, and technical security measures.
- The importance of phishing awareness has increased in both personal and professional settings, with phishing attacks among businesses rising from 72% to 86% from 2017 to 2020.

Phishing Types

- Email phishing
- Spear phishing
- Whaling and CEO fraud
- Clone phishing
- Voice phishing
- SMS phishing
- Page hijacking
- Calendar phishing

Phishing Types

- **Email phishing**

- Phishing attacks, often delivered via email spam, attempt to trick individuals into giving away sensitive information or login credentials.
- Most attacks are "bulk attacks" that are not targeted and are instead sent in bulk to a wide audience.
- The goal of the attacker can vary, with common targets including financial institutions, email and cloud productivity providers, and streaming services.
- The stolen information or access may be used to steal money, install malware, or spear phish others within the target organization.
- Compromised streaming service accounts may also be sold on darknet markets.
- This method of social engineering attack involve sending fraud email or messages that appear to be from a trusted source, such as bank, amazon, or government agency.
- These messages will typically contain a link or attachment that, when you click, will install malware automatically on the targeted device or redirect them to fake login page of any trusted website where they will be promoted to enter their login credential.

Phishing Types

- **Spear phishing**

- Spear phishing is a targeted phishing attack that uses personalized emails to trick a specific individual or organization into believing they are legitimate.
- It often utilizes personal information about the target to increase the chances of success.
- These attacks often target executives or those in financial departments with access to sensitive financial data and services.
- Accountancy and audit firms are particularly vulnerable to spear phishing due to the value of the information their employees have access to.
- Threat Group-4127 (Fancy Bear) targeted Hillary Clinton's 2016 presidential campaign with spear phishing attacks on over 1,800 Google accounts, using the accounts-google.com domain to threaten targeted users.
- A study on spear phishing susceptibility among different age groups found that 43% of 100 young and 58 older users clicked on simulated phishing links in daily emails over 21 days.
- Older women had the highest susceptibility, while susceptibility in young users declined over the study, but remained stable in older users.

Phishing Types

- **Whaling and CEO fraud**

- Whaling attacks use spear phishing techniques to target senior executives and other high-profile individuals[with customized content, often related to a subpoena or customer complaint.
- CEO fraud involves sending fake emails from senior executives to trick employees into sending money to an offshore account.
- It has a low success rate, but can result in organizations losing large sums of money.

Phishing Types

- **Clone phishing**

- Clone phishing is a type of attack where a legitimate email with an attachment or link is copied and modified to contain malicious content.
- The modified email is then sent from a fake address made to look like it's from the original sender.
- The attack may appear to be a resend or update of the original email.
- It often relies on the sender or recipient being previously hacked so the attacker can access the legitimate email.

Phishing Types

- **Voice phishing**
 - Voice over IP (VoIP) is used in vishing or voice phishing attacks, where attackers make automated phone calls to large numbers of people, often using text-to-speech synthesizers, claiming fraudulent activity on their accounts.
 - The attackers spoof the calling phone number to appear as if it is coming from a legitimate bank or institution.
 - The victim is then prompted to enter sensitive information or connected to a live person who uses social engineering tactics to obtain information.
 - Vishing takes advantage of the public's lower awareness and trust in voice telephony compared to email phishing.

Phishing Types

- **SMS phishing (Smishing)**

- SMS phishing or smishing is a type of phishing attack that uses text messages from a cell phone or smartphone to deliver a bait message.
- The victim is usually asked to click a link, call a phone number, or contact an email address provided by the attacker.
- They may then be asked to provide private information, such as login credentials for other websites.
- The difficulty in identifying illegitimate links can be compounded on mobile devices due to the limited display of URLs in mobile browsers.
- Smishing can be just as effective as email phishing, as many smartphones have fast internet connectivity. Smishing messages may also come from unusual phone numbers.

Phishing Types

- **Page hijacking**

- Page hijacking involves redirecting users to malicious websites or exploit kits through the compromise of legitimate web pages, often using cross site scripting.
- Hackers may insert exploit kits such as MPack into compromised websites to exploit legitimate users visiting the server.
- Page hijacking can also involve the insertion of malicious inline frames, allowing exploit kits to load.
- This tactic is often used in conjunction with watering hole attacks on corporate targets.

Phishing Types

- **Calendar phishing**

- Calendar phishing involves sending fake calendar invitations with phishing links.
- These invitations often mimic common event requests and can easily be added to calendars automatically.
- To protect against this form of fraud, former Google click fraud czar Shuman Ghosemajumder recommends changing calendar settings to not automatically add new invitations.

Phishing Techniques

- Link manipulation
- Filter evasion
- Social engineering

Phishing Techniques

- **Link manipulation**

- Phishing attacks often involve creating fake links that appear to be from a legitimate organization.
- These links may use misspelled URLs or subdomains to deceive the user.
- Another tactic is to make the displayed text for a link appear trustworthy, while the actual link goes to the phisher's site.
- To check the destination of a link, many email clients and web browsers will show the URL in the status bar when the mouse is hovering over it.
- However, some phishers may be able to bypass this security measure.

Phishing Techniques

- **Filter evasion**
 - Phishers have sometimes used images instead of text to make it harder for anti-phishing filters to detect the text commonly used in phishing emails.
 - In response, more sophisticated anti-phishing filters are able to recover hidden text in images using optical character recognition (OCR).

Phishing Techniques

- **Social engineering**
 - Phishing often uses social engineering techniques to trick users into performing actions such as clicking a link or opening an attachment, or revealing sensitive information.
 - It often involves pretending to be a trusted entity and creating a sense of urgency, like threatening to close or seize a victim's bank or insurance account.
 - An alternative technique to impersonation-based phishing is the use of fake news articles to trick victims into clicking on a malicious link.
 - These links often lead to fake websites that appear legitimate, but are actually run by attackers who may try to install malware or present fake "virus" notifications to the victim.

Anti-phishing

Tech trailblazer

Combating computer crime

- It is difficult to find and combat cybercrime perpetrators due to their use of the internet in support of cross-border attacks.
- Not only does the internet allow people to be targeted from various locations, but the scale of the harm done can be magnified.
- Cybercriminals can target more than one person at a time.
- The availability of virtual spaces to public and private sectors has allowed cybercrime to become an everyday occurrence.
- In 2018, The Internet Crime Complaint Center received 351,937 complaints of cybercrime, which lead to \$2.7 billion lost.

Combating computer crime

- Investigation
- Prevention
- Legislation
- Penalties
- Awareness
- Intelligence

Cyber Crime Jobs

- Government, Military, Law Enforcement Agencies
- Private sector companies
- Designations:
 - Cyber Crime Analyst / Forensic Examiner / Scientist / Specialist / Investigator
- Relevant Degree, Certifications and Experience



Cyber Crime Agencies and Organizations

- FIA – CCW
- Military
- Government Sector
- Private Companies
- CERTs

Tech trailblazer

Cyber Crime Law in Pakistan

- PECA (2016)
 - Prevention of Electronic Crimes Act
- PPC (Pakistan Penal Code)
- CrPC (Criminal Procedure Code)
- FERA (Foreign Exchange Regulation Act, 1947)
- AMLA (Anti-Money Laundering Act, 2010)
- The Anti-Terrorism Act, 1997

Cyber Crime Reporting in Pakistan

- Modes:
 - Phone
 - Online
 - In-Person
- Required Documents
 - Application / Matter
 - CNIC
 - Proofs
- Process:
 - Application submission
 - Verification
 - Enquiry
 - FIR