GROUP 23

INTRODUCTION TO NMAP

A Network Scanning and Security Auditing Tool

GROUP 23

WHAT IS NMAP

🤔 What is NMAP ?

- Nmap (Network Mapper) is a powerful, free and open-source tool.
- Primarily used for network discovery and security auditing.
- Often described as a "**noisy scanner**" because firewalls and server can detect scanning from nmap.

The mission is how to anonymously use the tool instead of using it only.

KEY FUNCTIONS

Host Discovery

Identifies active hosts on a network for initial reconnaissance.

Port Scanning

Determines the state of TCP/UDP ports on target systems.

Service/Version Detection

Pinpoints applications and their versions running on open ports.

OS Detection

Fingerprints the operating system via TCP/IP stack analysis.

Vuinerability Scanning

Leverages the NSE to detect common vulnerabilities.

THE HISTORY OF NMAP

1997

Initiated by Gordon Lyon (Fyodor), first release in Phrack magazine.

1998

Nmap version 2.00 was released, introducing OS detection.

2000

Introduced several new scan methods, and became officially available on Microsoft Windows for the first time.

2006

The Nmap Scripting Engine (NSE) is released.

2007

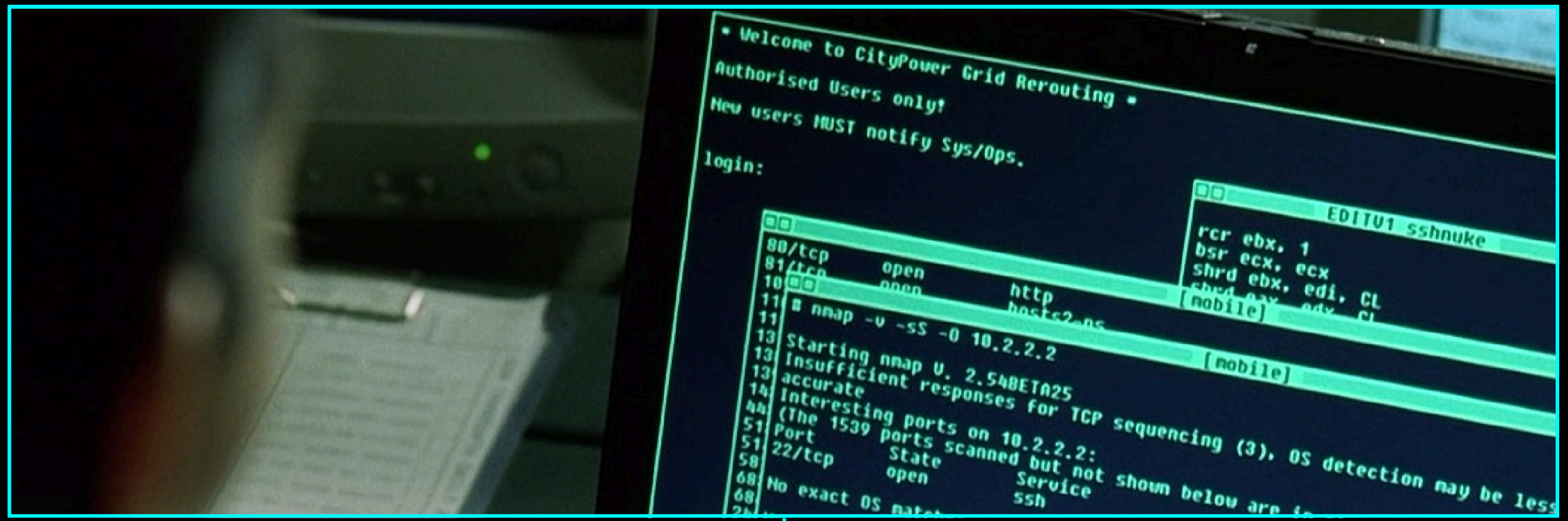
The Zenmap GUI is integrated into Nmap, replacing the older NmapFE

Ongoing

Continuous Updates & Community Support

NMAP IN THE MOVIES

- **The Matrix Reloaded (2003)** – Trinity realistically uses Nmap 2.54BETA25 to find a vulnerable SSH server on the city's power grid, then exploits it to save the day, becoming Nmap's most famous movie appearance.
- **The Bourne Ultimatum (2007)** – CIA agents use Zenmap to scan a newspaper's mail server, revealing SSH, Postfix SMTP, and DNS services.
- **Fantastic Four (2015)** – Sue Storm uses Nmap (with IPSCAN, TRACEROUTE, PORTSCAN) to locate a companion.



Testing Environment

A safe and legal target provided by the creators of Nmap for learning and experimentation:

scanme.nmap.org

Basic Commands

- nmap --help: Display all available options.
- nmap -V: Show the Nmap version.
- nmap <target>: Perform a default scan.

```
ubuntu@ubuntu-lab:~$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-08 08:46 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds
```

Port State

- **Open**: Actively accepting connections.
- **Closed**: Accessible, but no service is listening.
- **Filtered**: A firewall or filter is blocking probes.
- **Unfiltered**: Accessible, but state cannot be determined.
- **Open|Filtered**: Cannot determine if open or filtered.
- **Closed|Filtered**: Cannot determine if closed or filtered.

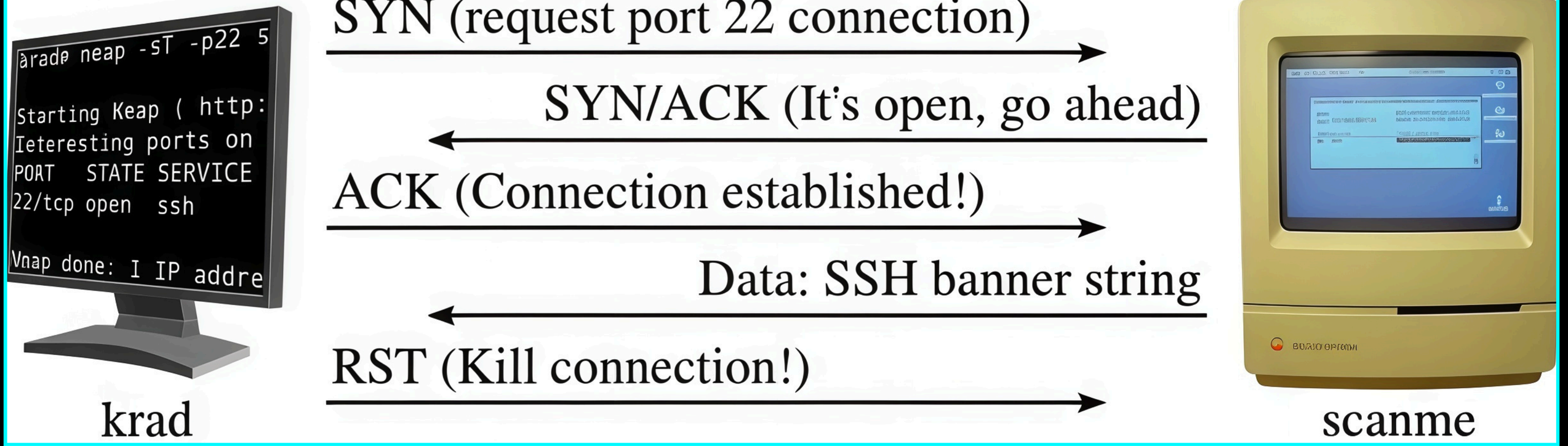
GROUP 23

PORT SCANNING TECHNIQUES

TCP Connect Scan (-sT)

Default (Non-Root) | Full Handshake | Easily Detected

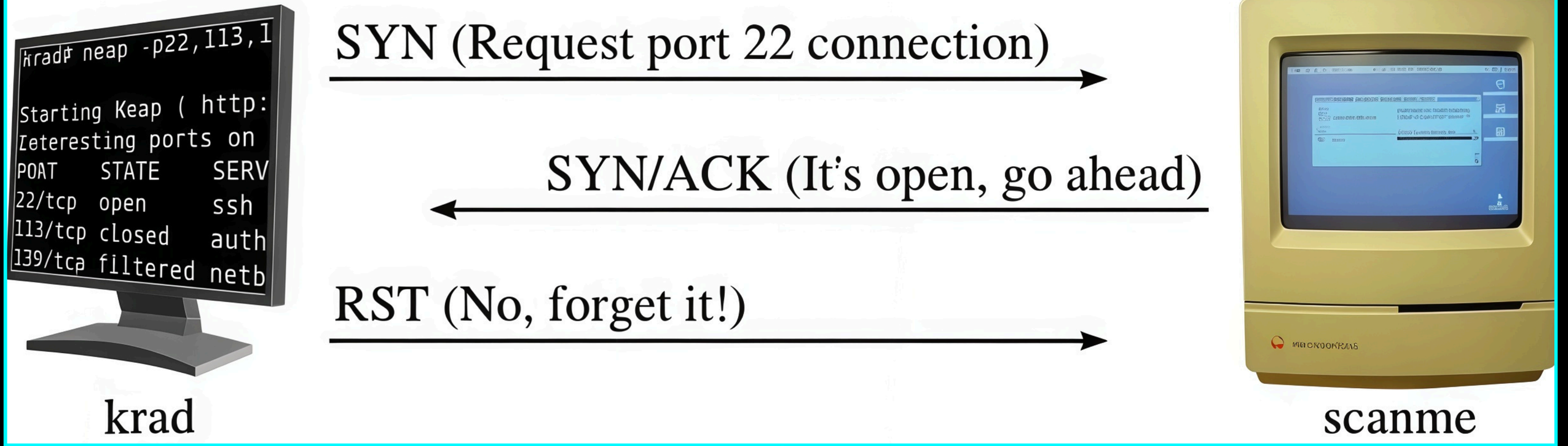
This scan completes the standard three-way TCP handshake (SYN, SYN-ACK, ACK). It's reliable but noisy, as it's logged by target systems and firewalls. It's the default scan when Nmap is not run with root privileges.



TCP SYN "Stealth" Scan (-sS)

Default (Root) | Half-Open | Harder to Detect

Nmap's default and most popular scan with root privileges. It sends a SYN packet and if a SYN-ACK is received, sends an RST packet, preventing a full connection. This "half-open" nature makes it less likely to be logged.



UDP Scan (-sU)

Connectionless | UDP Services | Slower

Scans for UDP services like DNS, SNMP, or DHCP. It sends UDP packets; no response suggests open|filtered, while an ICMP Port Unreachable error indicates a closed port. It is more challenging and slower than TCP scans.

Probe Response	Assigned State
Any UDP response from target port (unusual)	**open**
No response received (even after retransmissions)	**open|filtered**
ICMP port unreachable error (type 3, code 3)	**closed**
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	**filtered**

IP Protocol Scan (-sO)

- Instead of scanning ports, Nmap scans for IP protocols that the target host supports (e.g., ICMP, TCP, UDP, GRE, ESP).
- Useful to detect which protocols are enabled or filtered by firewalls.
- Requires root privileges (because it sends raw IP packets).

```
ubuntu@ubuntu-lab:~$ sudo nmap -sO scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-16 10:53 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 220 closed n/a protocols (proto-unreach), 34 open|filtered n/a protocols
(no-response)
PROTOCOL STATE SERVICE
1        open  icmp
17       open  udp

Nmap done: 1 IP address (1 host up) scanned in 29.37 seconds
```

Firewall Scanning

Flag	Name	Operation	Result
-sA	**ACK Scan**	Sends a TCP ACK packet → if an RST is returned, the port is classified as unfiltered (not blocked); if there is no response, the port is filtered.	Primarily used to map firewall rules.
-sF	**FIN Scan**	Sends a TCP packet with only the FIN flag set. According to RFC 793: a closed port responds with an RST, while an open port remains silent.	Effective only on systems that comply with RFC 793.
-sX	**Xmas Scan**	Sends a TCP packet with the FIN, URG, and PSH flags set.	Similar to the FIN scan; often used to evade intrusion detection systems (IDS).
-sN	**Null Scan**	Sends a TCP packet with no flags set.	According to RFC 793: closed ports reply with an RST, open ports remain silent.

Host Discovery

Command	Objective	Operation
-sn	No port scan	Performs host discovery only (via ICMP, ARP, or TCP/UDP ping), without scanning ports.
-PS	TCP SYN Ping	Sends a TCP SYN packet to a port; if a SYN+ACK is received, the host is considered online.
-PA	TCP ACK Ping	Sends a TCP ACK packet; if an RST is returned, the host is considered online.
-PU	UDP Ping	Sends a UDP packet to a port; if an ICMP response is received, the host is considered online.
-PY	SCTP INIT Ping	Sends an SCTP INIT chunk; used for host discovery over SCTP (Stream Control Transmission Protocol).
-PE	ICMP Echo	Performs a standard ICMP Echo Request (Type 8) and expects an Echo Reply (Type 0).
-PP	ICMP Timestamp	Sends an ICMP Timestamp Request message.
-PM	ICMP Netmask	Sends an ICMP Address Mask Request message.
-PO	IP Protocol Ping	Sends packets with IP protocols other than TCP/UDP to check host responsiveness.
-PR	ARP Ping	Conducts host discovery within a local area network (LAN) using ARP requests.
-Pn	Treat all as up	Skips host discovery and assumes all specified hosts are online.

DNS & Target Specification

-R: Performs reverse DNS resolution on all hosts.
-n: Disables DNS resolution; scans IP addresses directly.
--system-dns: Uses the operating system's DNS resolver.
--dns-servers 8.8.8.8: Specifies a custom DNS server to be used.
-iL file.txt: Reads the list of scan targets from an input file.
--exclude: Excludes specific targets from scanning.
--excludefile: Excludes targets defined in a file.
-iR N: Performs a random scan of N hosts.
-6: Enables scanning over IPv6.
-e eth0: Specifies the network interface to be used for scanning.

GROUP 23

ADVANCED INFORMATION GATHERING WITH NMAP

ⓘ Service Version Detection (-sV)

Purpose: Exploits weaknesses in some firewalls/packet filters that mishandle IP fragments, potentially allowing scans to bypass filtering.
Operation: -f option sends tiny IP fragments (default 8 bytes each). Multiple -f flags increase fragment size; --mtu sets a custom multiple-of-8 size.
Limitations:

- Some OS reassemble fragments before sending; --send-eth can bypass this.
- Works only with Nmap's raw packet features (e.g., TCP/UDP scans, OS detection), not with version detection or NSE scripts.

```
ubuntu@ubuntu-lab:~$ sudo nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-12 10:31 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe
18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE    VERSION
22/tcp    open     ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu L
inux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http       Apache httpd 2.4.7 ((Ubuntu))
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 17.85 seconds
```

```
ubuntu@ubuntu-lab:~$ sudo nmap -O scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-12 10:35 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe
18:bb2f
Not shown: 995 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linu
x 5.0 - 5.5 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.3
9 (93%), Linux 2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 5.0 (
91%), Linux 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nma
p.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.35 seconds
```

Operating System Detection (-O)

Identify a target's operating system remotely using TCP/IP stack fingerprinting.
Nmap sends special TCP/UDP packets to the target. and compares results to **nmap-os-db.**
Prints OS details if matched; otherwise suggests submission for database improvement.
--osscan-limit: just scan OS having at least one open and one closed TCP port

Aggressive Scan (-A)

The `-A` option is a comprehensive and powerful shortcut, designed to accelerate detailed reconnaissance by combining several advanced scanning techniques into a single command. It automatically enables:

- **OS detection** (-O)
- **Version detection** (-sV)
- **Script scanning** (-sC)
- **Traceroute** (--traceroute).

Advantages

- **Comprehensive results** – Combines OS detection, version detection, default scripts, and traceroute in one run.
- **Time-saving**

Limitations

- **Very noisy** – Generates lots of traffic; easy for IDS/IPS to detect.
- **Slower** – Takes more time than basic scans, especially on many targets.
- **Potential service disruption** – NSE scripts may trigger alerts or disrupt fragile services.

GROUP 23

NMAP SCRIPTING ENGINE

What is the Nmap Scripting Engine?

- The Nmap Scripting Engine (NSE) is a powerful component that significantly extends Nmap's core functionality. It allows users to write and execute scripts to automate a wide variety of networking tasks, from basic discovery to complex vulnerability detection.
- Scripts are written in Lua, a lightweight language, making them easy to develop. The Nmap project continuously adds new scripts, demonstrating its rapid growth and strong community contribution.

NSE Script

```
ubuntu@ubuntu-lab:~$ ls /usr/share/nmap/scripts/
acarsd-info.nse                         ip-geolocation-ipinfodb.nse
address-info.nse                        ip-geolocation-map-bing.nse
afp-brute.nse                           ip-geolocation-map-google.nse
afp-ls.nse                              ip-geolocation-map-kml.nse
afp-path-vuln.nse                       ip-geolocation-maxmind.nse
afp-serverinfo.nse                      ip-https-discover.nse
afp-showmount.nse                       ipidseq.nse
ajp-auth.nse                            ipmi-brute.nse
ajp-brute.nse                           ipmi-cipher-zero.nse
ajp-headers.nse                         ipmi-version.nse
ajp-methods.nse                         ipv6-multicast-mld-list.nse
ajp-request.nse                         ipv6-node-info.nse
allseeingeye-info.nse                   ipv6-ra-flood.nse
amqp-info.nse                           irc-botnet-channels.nse
asn-query.nse                           irc-brute.nse
auth-owners.nse                         irc-info.nse
auth-spoof.nse                          irc-sasl-brute.nse
backorifice-brute.nse                   irc-unrealircd-backdoor.nse
backorifice-info.nse                    iscsi-brute.nse
bacnet-info.nse                         iscsi-info.nse
banner.nse                              isns-info.nse
bitcoin-getaddr.nse                     jdwp-exec.nse
bitcoin-info.nse                        jdwp-info.nse
bitcoinrpc-info.nse                     jdwp-inject.nse
bittorrent-discovery.nse                jdwp-version.nse
```

Nmap provides a wide range of NSE (Nmap Scripting Engine) scripts that can be used for different purposes, such as vulnerability detection, service enumeration, or exploitation...

Diverse Applications of NSE Scripts

Vuinerability Detection
Identify specific vuinerabilities, misconfigurations, or backdoors (e.g., Heartbieed, Sheiishock).

Brute-Force Attacks
Automate password guessing against services like SSH, FTP, or HTTP.

Information Gathering
Extract rich detaiis iike HTTP headers, DNS records, or SMB shares.

Maiware & Backdoor Detection
Scan for known maiware or rootkits by checking specific network indicators.

Vuinerability Exploitation
Advanced scripts can expioit vuinerabilities, used in authorized penetration tests.

```
ubuntu@ubuntu-lab:~$ sudo nmap --script http-title -p 80 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-12 10:48 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT   STATE SERVICE
80/tcp open  http
|_http-title: Go ahead and ScanMe!

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
ubuntu@ubuntu-lab:~$ nmap --script http-enum -p 80 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-12 10:48 +07
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (
ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 21.63 seconds
```

GROUP 23

FIREWALL EVASION TECHNIQUES

Packet Fragmentation

Purpose: Instructs Nmap to send packets in tiny, fragmented IP pieces, typically splitting headers into 8-byte chunks.
Evasion: Effective against firewalls/IDS that only inspect the first fragment, allowing subsequent packets with critical data to bypass inspection.
Applicability: Supported by Nmap's raw packet features like TCP/UDP port scans (excluding connect() scans) and OS detection.
-f option sends tiny IP fragments (default 8 bytes each). Multiple -f flags increase fragment size; ***--mtu*** sets a custom multiple-of-8 size.

Decoy Scans

- Sends packets from multiple spoofed IP addresses alongside your real one to mask the true origin.
- Makes it harder for intrusion detection systems (IDS) and firewalls to pinpoint the attacker.
- Example: ***nmap -D RND:10 <target>*** — uses 10 random decoys plus your real IP.
- Limitation: Skilled defenders can still identify the real source through packet timing or traffic analysis.

```
ptn@ptn:~$ sudo nmap -D RND:5 -p 80 10.122.1.176
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-09 12:00 +07
Nmap scan report for 10.122.1.176
Host is up (0.32s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 16:54:75:12:E1:8B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Decoy Scans

```
@sunraku sudo tcpdump -i wlp45s0 'tcp[tcpflags] & tcp-syn != 0 and dst port 80'

[sudo] password for sunraku:
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlp45s0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
12:00:19.133129 IP static-dedicado-200-122-220-188.une.net.co.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
12:00:19.133130 IP 197.30.5.23.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
12:00:19.133130 IP hn.kd.ny.adsl.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
12:00:19.133131 IP 209.60.19.1.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
12:00:19.133131 IP 10.122.4.169.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
12:00:19.133131 IP 154.196.65.104.60772 > trungthe.http: Flags [S], seq 1020820609, win 1024, options [mss 1460], length 0
```

Capture all TCP connection initiation packets (SYN) going to port 80
→ 6 packets from different IP addresses (5 decoys + 1 real IP).

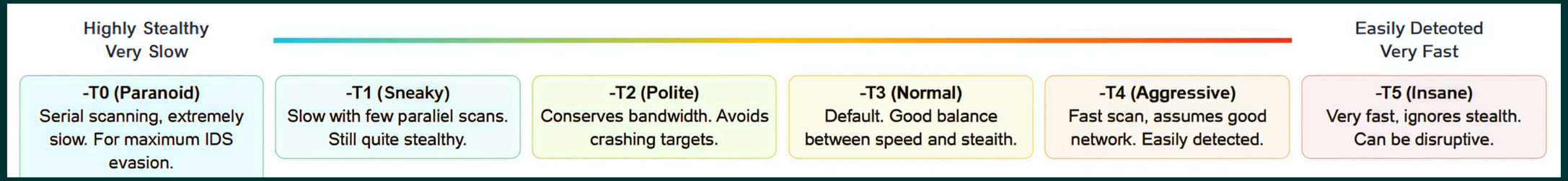
Source Port Manipulation

- Sends scan traffic using a specified source port instead of a random one.
- Can bypass poorly configured firewalls or filters that allow trusted ports (e.g., --source-port 53 for DNS or --source-port 80 for HTTP).
- Useful for evading simple port-based access control.
- Limitation: Ineffective against modern, stateful firewalls and deep packet inspection.

```
# nmap -sS -v -v -Pn 172.25.0.14

Starting Nmap ( https://nmap.org )
Nmap scan report for 172.25.0.14
Not shown: 1658 filtered ports
PORT   STATE  SERVICE
88/tcp closed kerberos-sec

Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds

# nmap -sS -v -v -Pn -g 88 172.25.0.14

Starting Nmap ( https://nmap.org )
Nmap scan report for 172.25.0.14
Not shown: 1653 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1027/tcp open  IIS
1433/tcp open  ms-sql-s

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

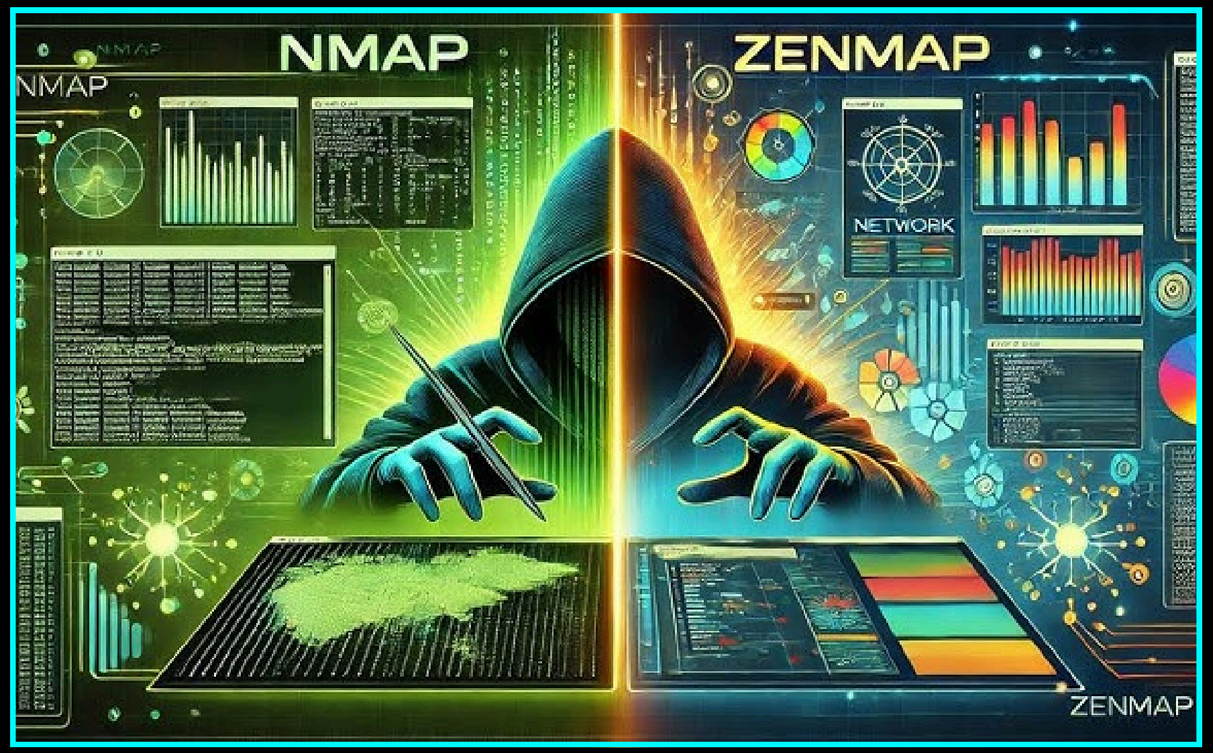
⏱️Timing and Performance

- **Purpose**: Control how quickly Nmap sends packets to balance speed and accuracy.
- **Trade-off**: Faster scans = less stealth & possible incomplete results; slower scans = more accurate but time-consuming.
- -T0 (Paranoid) and -T1 (Sneaky) operate at very slow speeds and are primarily used to evade detection by Intrusion Detection Systems (IDS).
- -T4 (Aggressive) and -T5 (Insane) perform scans at very high speeds but are highly “noisy” and more likely to be blocked.
- The default setting is -T3 (Normal), which provides a balanced trade-off between speed and stealth.



GROUP 23

ZENMAP



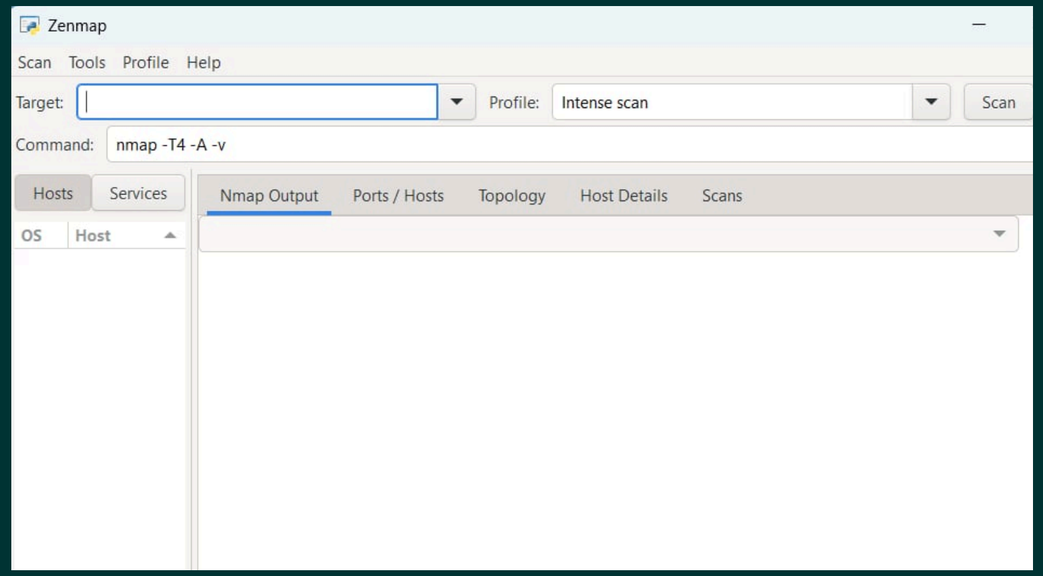
Zenmap – Nmap's Official GUI

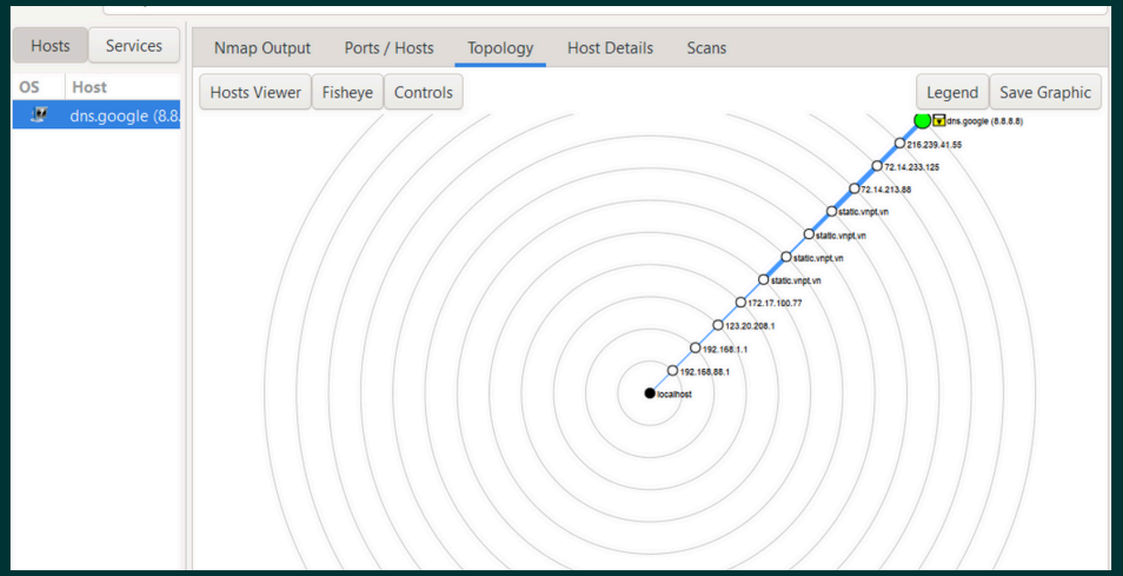
- **Definition**: Zenmap is the official cross-platform Graphical User Interface (GUI) for Nmap.
- **Purpose**: Designed to make Nmap more accessible to beginners while still providing advanced features for experts.
- **Platforms**: Available for Windows, Linux, macOS, and other Unix-like systems.

Main features of Zenmap

- **Profile**: Essentially a saved scan configuration — it stores the scan type, Nmap options, and parameters so you can run the same scan again without re-entering the commands.
- **Command**: Displays the exact Nmap command that will be run based on your chosen profile and settings.
- **Search & Filter**: Allows you to easily find hosts, services, or vulnerabilities within large scan results.
- **Topology View**: Provides a visual network map showing host relationships.
- **Export Options**: Lets you save scan results in XML, plain text, or HTML format for reporting purposes.

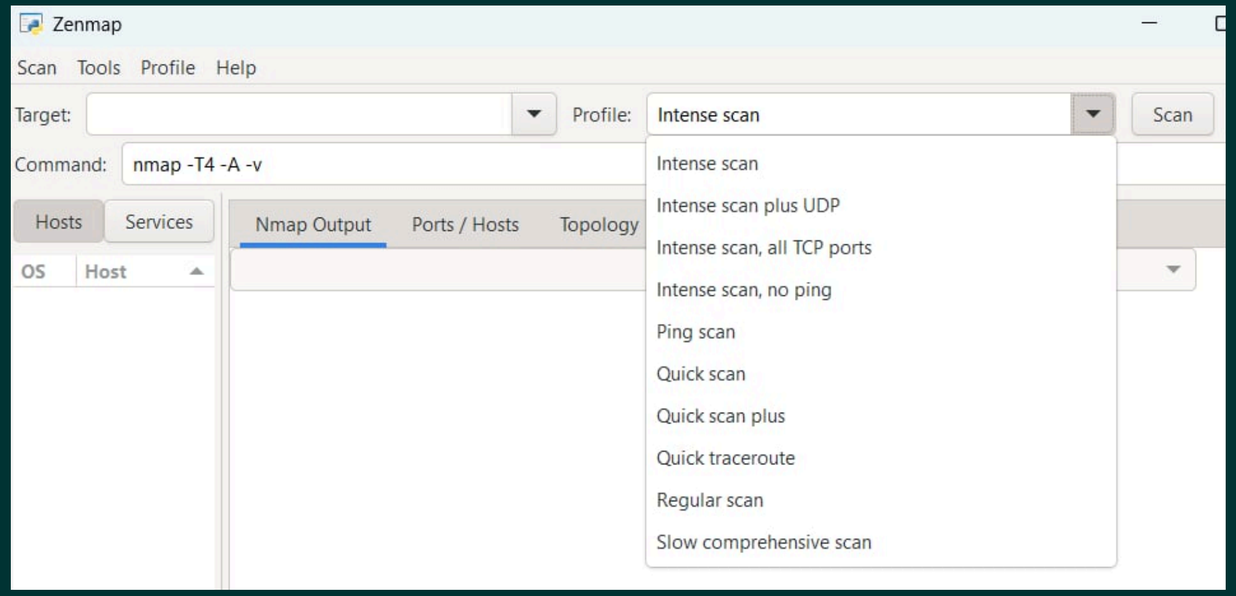
Main features of Zenmap





Some default Zenmap scan profiles

- **Intense Scan**: Runs a comprehensive scan with OS detection, version detection, script scanning, and traceroute.
- **Quick Scan**: A fast scan of common ports using default settings.
- **Intense Scan, All TCP Ports**: Scans all 65,535 TCP ports with full detection features.
- **Ping Scan**: Only checks if hosts are online, without scanning ports.
- **Quick Traceroute**: Performs traceroute without scanning ports.



GROUP 23

DEMO

GROUP 23

THANK YOU FOR LISTENING