



CyberForge
ACADEMY



NMAP 101

Network Scanning and Analysis



\$ whoami



- Software Engineer & Researcher at CyberForge Academy
- Final year, B. Tech. CSE @ LPU
- Engaged in Research, Creating course content/setups 
- Developing SaaS software and open source tools
- Interned with Web3verse Academy, a Singapore-based startup focused on Web3 education and Namekart, a domain name brokerage firm.
- Interested in Art and craft 



CyberForge
ACADEMY



Table of contents

01

Introduction

02

**Why Network
Scanning ?**

03

**Basic
Functionalities**

04

Nmap Scans

05

Comparison

06

NSE



CyberForge
ACADEMY

What is Nmap ?



Image :Nmap: the Network Mapper -Free Security Scanner

- **Nmap** (Network Mapper)
- Used to discover hosts and services on a target by sending packets and analyzing the responses.
- Released in September 1997 by **Gordon Lyon**
- Free and Open Source
- <https://github.com/nmap/nmap>
- Cross-platform (Windows/Linux/MacOS)

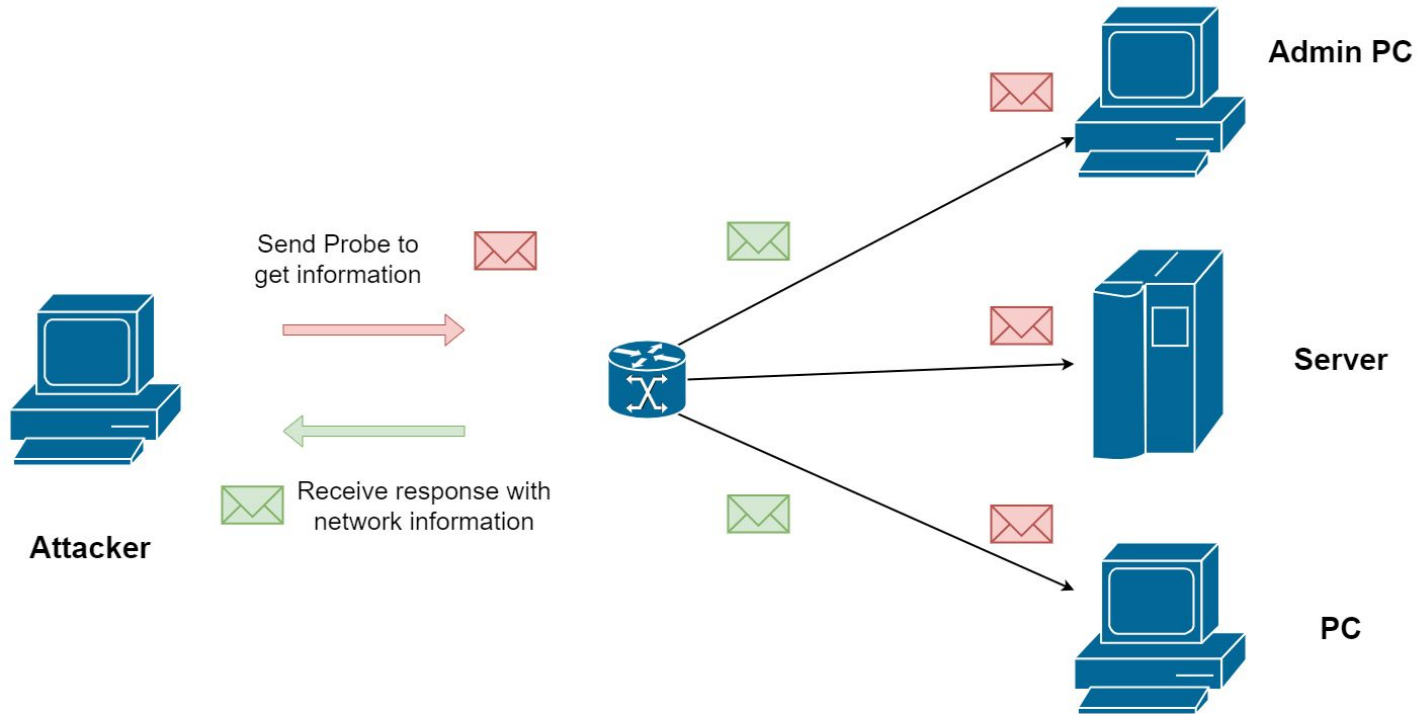


Image : Gordon Lyon -Wikipedia



CyberForge
ACADEMY

Network Scanning



Why Network Scanning?

- Monitoring network health and performance.
- Managing assets effectively.
- Detecting and mitigating security threats efficiently.





```
● student@cyberforgeacademy:~$ nmap -h
```

```
Nmap 7.80 ( 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
```

```
-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
```



CyberForge
ACADEMY

Nmap Default Scan



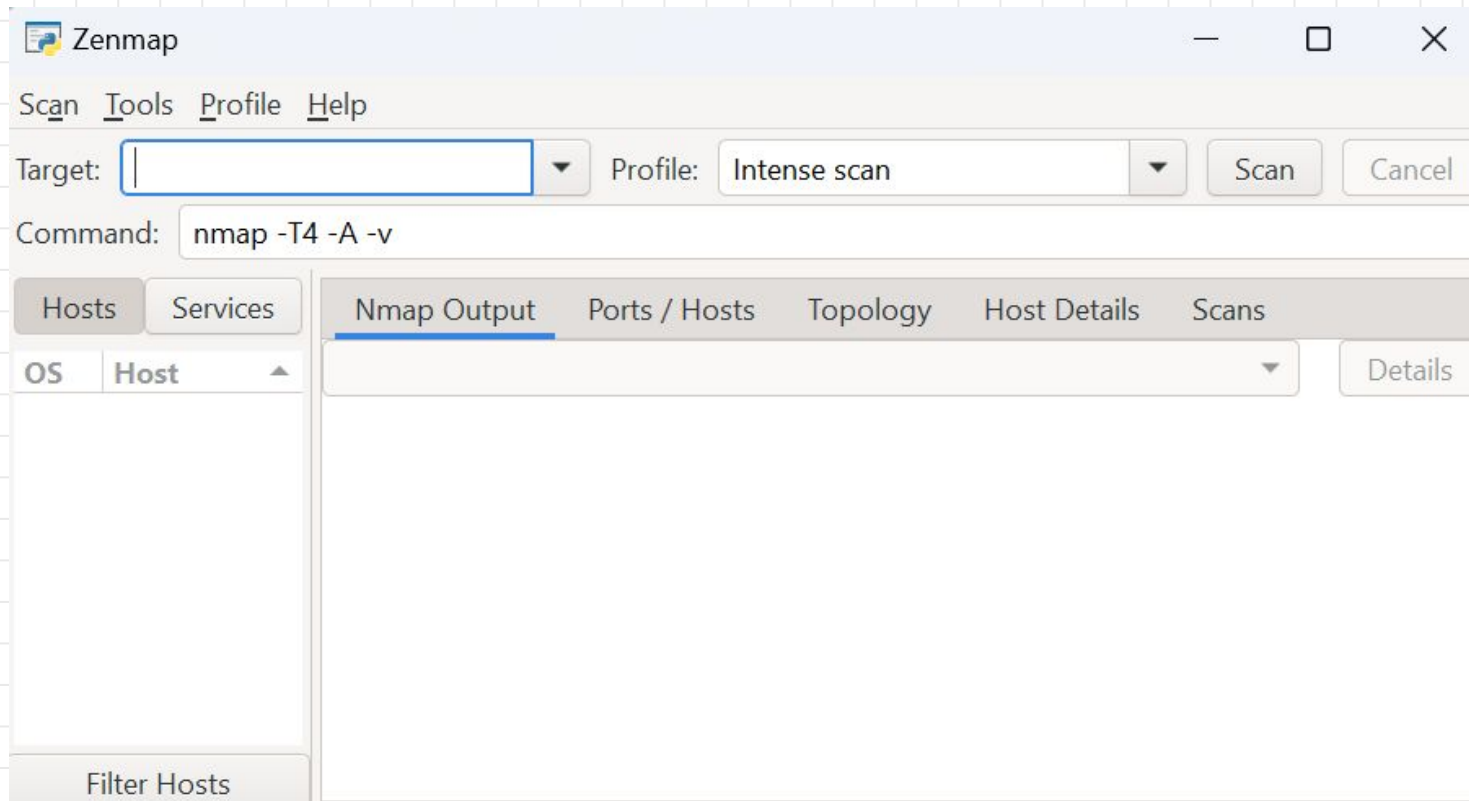
Command: nmap <target_ip>

```
● student@cyberforgeacademy:~$ nmap 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 07:02 IST
Nmap scan report for 172.17.0.2
Host is up (0.00018s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```



Zenmap - Nmap GUI





Scanning Network by Zenmap



CyberForge
ACADEMY

Basic Functionalities

1) Host Discovery

- Determines which hosts are available & responsive
- -sn is used for ping scan to only perform host discovery

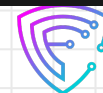
```
● student@cyberforgeacademy:~$ nmap -sn 172.17.0.1-10
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:19 IST
Nmap scan report for cyberforgeacademy (172.17.0.1)
Host is up (0.00013s latency).
Nmap scan report for 172.17.0.2
Host is up (0.00087s latency).
Nmap done: 10 IP addresses (2 hosts up) scanned in 1.47 seconds
```



2) Port Scanning

- Discovers open ports and running services on target devices
- **-p-** used to scan all 65535 ports on the target device

```
● student@cyberforgeacademy:~$ nmap -p- 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06
Nmap scan report for 172.17.0.2
Host is up (0.00022s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
11211/tcp open  memcache
33060/tcp open  mysqlx
```



3) Service Fingerprinting:

- Attempts to determine the version of services running on the open ports
- -sV used for service fingerprinting

```
student@cyberforgeacademy:~$ nmap -sV 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:35 IST
Nmap scan report for 172.17.0.2
Host is up (0.00026s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
3306/tcp  open  mysql        MySQL (unauthorized)
Service Info: Host: 185b11ded85d; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



4) OS Fingerprinting:

- Attempts to determine the operating system of a target
- -O used for OS detection

```
● student@cyberforgeacademy:~$ sudo nmap -O 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:28 IST
Nmap scan report for 172.17.0.2
Host is up (0.00020s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 02:42:AC:11:00:02 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/sul
TCP/IP fingerprint:
```



Nmap Switches

- **-v:** Verbose mode for detailed output.
- **-T:** Timing template for scan speed.
- **-T0 (Paranoid):** Slow, stealthy scan.
- **-T1 (Sneaky):** Slightly faster, cautious scan.
- **-T2 (Polite):** Default balance of speed and stealth.
- **-T3 (Normal):** Faster scan with more network impact.
- **-T4 (Aggressive):** Rapid scan with higher risk of detection.



Type of Scans

1) Intense Scan

- **Packet uses:** SYN-ACK,RST (2919 packets)
- **Total Ports Scan:** 1000 ports
- **Command :** “nmap -A <target>”




```
● student@cyberforgeacademy:~$ nmap -A 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:39 IST
Nmap scan report for 172.17.0.2
Host is up (0.00031s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu L
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: 185b11ded85d, PIPELINING, SIZE 10240000, VRFY, ETRN

| ssl-cert: Subject: commonName=185b11ded85d
| Subject Alternative Name: DNS:185b11ded85d
| Not valid before: 2024-02-20T10:20:07
|_Not valid after:  2034-02-17T10:20:07
| ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
3306/tcp  open  mysql        MySQL (unauthorized)
```



2) Quick Scan

- **Total Ports Scan :** 100 Ports
- **Packet uses:** TCP SYN packet
- **Command :** “nmap -F <target>”

```
● student@cyberforgeacademy:~$ nmap -F 8.8.8.8
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:48
IST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.037s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https


Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
```



Did You Know This Exist ?

← ↻ 🔒 https://dns.google

🔍 ⭐ ⚙️ | 📄 ⭐ 📌 🔄 ...



Google
Public DNS

DNS Name

Resolve

Enter a domain (like example.com) or IP address (like 8.8.8.8 or 2001:4860:4860::8844) here.



3) Ping Scan

- Focuses exclusively on host discovery
- **Packet uses:** ICMP Echo Request packet
- **Total Ports Scan :** 0
- **Command :** “nmap -sn <target>”

```
● student@cyberforgeacademy:~$ nmap -sn 172.17.0.1-10
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:19 IST
Nmap scan report for cyberforgeacademy (172.17.0.1)
Host is up (0.00013s latency).
Nmap scan report for 172.17.0.2
Host is up (0.00087s latency).
Nmap done: 10 IP addresses (2 hosts up) scanned in 1.47 seconds
```



4)Intense Scan, All TCP Ports

- Total Ports: 65535
- Packet uses: TCP SYN packet
- Command : “ nmap -p 1-65535 -A <target>”

```
student@cyberforgeacademy:~$ nmap -p 1-65535 -A 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 06:54 IST
Nmap scan report for 172.17.0.2
Host is up (0.00014s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; pr
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: 185b11ded85d, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
CHUNKING,
|_ssl-cert: Subject: commonName=185b11ded85d
|_Subject Alternative Name: DNS:185b11ded85d
|_Not valid before: 2024-02-20T10:20:07
|_Not valid after: 2034-02-17T10:20:07
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
|_http_server_header: Apache/2.4.52 (Ubuntu)
|_http_title: Apache2 Ubuntu Default Page: It works
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
3306/tcp  open  mysql        MySQL (unauthorized)
11211/tcp open  memcached    Memcached 1.6.14 (uptime 2453 seconds)
33060/tcp open  mysqlx?
```



5) Quick Traceroute

- Combination of a quick ping scan and traceroute
- **Total Ports Scan : 0**
- **Packet uses:** ICMP Echo Request packet
- **Command :** “ **nmap -sn --traceroute <target>**”

```
● student@cyberforgeacademy:~$ sudo nmap -sn --traceroute 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 07:07 IST
Nmap scan report for 172.17.0.2
Host is up (0.000081s latency).
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.08 ms	172.17.0.2

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds



6) Intense Scan, No Ping

- A thorough scan without relying on ping for host discovery
- **Packet uses:** TCP SYN packet
- **Total Ports Scan:** 1000
- **Command :** “ nmap -T4 -Pn <target>”

```
student@cyberforgeacademy:~$ nmap -Pn 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-0
Nmap scan report for 172.17.0.2
Host is up (0.00014s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
```





Comparing Common Scans



CyberForge
ACADEMY

1) Default Scan

- **Packet uses:** SYN , RST, ACK Packets (2020 packets)
- **Total Ports Scan:** 1,000 most common TCP ports
- **Command:** nmap <target>



● **student@cyberforgeacademy:~\$** nmap 172.17.0.2
Starting Nmap 7.80 (<https://nmap.org>) at 2024-02-25 07:02 IST
Nmap scan report for 172.17.0.2

Host is up (0.00018s latency).

Not shown: 993 closed ports

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

25/tcp	open	smtp
--------	------	------

80/tcp	open	http
--------	------	------

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

3306/tcp	open	mysql
----------	------	-------

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds



default_scan.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.17.0.1	172.17.0.2	TCP	74	41368 → 80 [SYN] Seq=6
2	0.000038318	172.17.0.2	172.17.0.1	TCP	74	80 → 41368 [SYN, ACK]
3	0.000049714	172.17.0.1	172.17.0.2	TCP	66	41368 → 80 [ACK] Seq=1
4	0.000104804	172.17.0.1	172.17.0.2	TCP	74	43354 → 443 [SYN] Seq=
5	0.000112700	172.17.0.2	172.17.0.1	TCP	54	443 → 43354 [RST, ACK]
6	0.000136679	172.17.0.1	172.17.0.2	TCP	66	41368 → 80 [RST, ACK]
7	5.471689067	172.17.0.1	172.17.0.2	TCP	74	50608 → 587 [SYN] Seq=
8	5.471722589	172.17.0.2	172.17.0.1	TCP	54	587 → 50608 [RST, ACK]
9	5.471784382	172.17.0.1	172.17.0.2	TCP	74	53692 → 139 [SYN] Seq=
10	5.472330778	172.17.0.2	172.17.0.1	TCP	74	139 → 53692 [SYN, ACK]
11	5.472361076	172.17.0.1	172.17.0.2	TCP	66	53692 → 139 [ACK] Seq=

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface docker0, id 0

Ethernet II, Src: 02:42:a2:96:c7:93 (02:42:a2:96:c7:93), Dst: 02:42:ac:11:00:02 (02:42:ac:11:00:02)

Internet Protocol Version 4, Src: 172.17.0.1, Dst: 172.17.0.2

Transmission Control Protocol, Src Port: 43354, Dst Port: 443, Seq: 0, Len: 0

Source Port: 43354

Destination Port: 443

[Stream index: 1]

[Conversation completeness: Incomplete (37)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (relative): 333571872

default_scan.pcapng

Packets: 2020 - Displayed: 2020 (100.0%)

Profile: Default



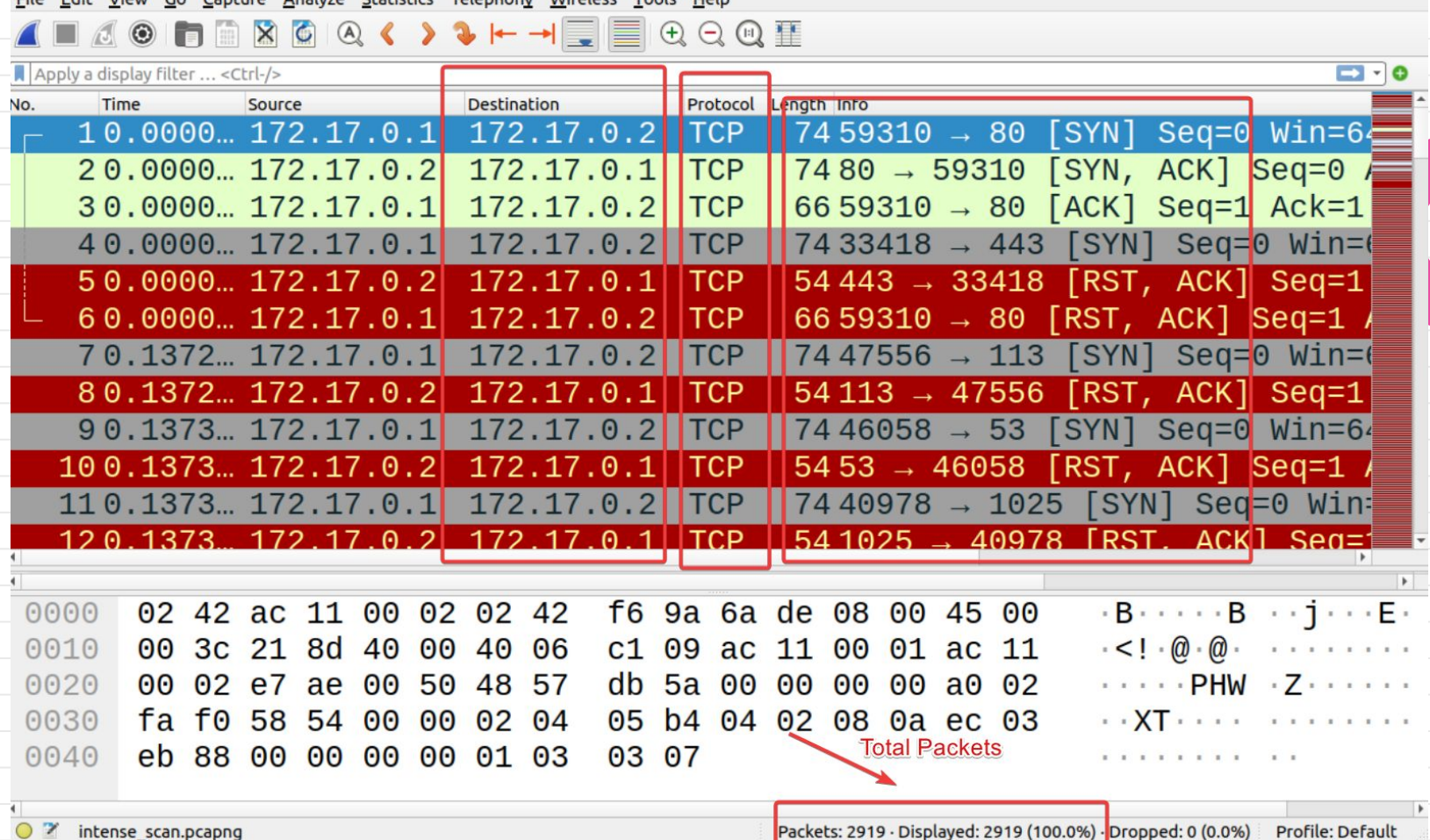
2) Intense Scan

- **Packet uses: SYN Packets (SYN-ACK,RST)(2919 packets)**
- **Total Ports Scan: 1000 ports**
- **Command : nmap -A <target>**



```
● student@cyberforgeacademy:~/CyberForgeAcademy/code/nmap-target$ nmap -A 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-21 17:31 IST
Nmap scan report for 172.17.0.2
Host is up (0.000098s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: 185b11ded85d, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCO
F8, CHUNKING,
|_ssl-cert: Subject: commonName=185b11ded85d
|_Subject Alternative Name: DNS:185b11ded85d
|_Not valid before: 2024-02-20T10:20:07
|_Not valid after: 2034-02-17T10:20:07
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp   open  netbios-ssn Samba smbd 4.6.2
445/tcp   open  netbios-ssn Samba smbd 4.6.2
3306/tcp  open  mysql        MvSQL (unauthorized)
Service Info: Host: 185b11ded85d; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```





4) Specific Port Scan

- Sends packets to specific ports and analyzes responses
- Determines port status (open, closed, or filtered) based on responses
- **Packet uses:** TCP packets targeting specified ports (3 packets)
- **Command:** “nmap -p <port_number> <target>”

```
● student@cyberforgeacademy:~$ nmap -p 22 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-25 07:42 IST
Nmap scan report for 172.17.0.2
Host is up (0.00022s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 5.19 seconds
```



specific_portscan.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.dstport == 22

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.17.0.1	172.17.0.2	TCP	74	50720 → 22 [SYN] Seq=0
2	0.000076448	172.17.0.1	172.17.0.2	TCP	66	50720 → 22 [ACK] Seq=1
3	0.000129453	172.17.0.1	172.17.0.2	TCP	66	50720 → 22 [RST, ACK]

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface docker0, id 0

Ethernet II, Src: 02:42:f6:9a:6a:de (02:42:f6:9a:6a:de), Dst: 02:42:ac:11:00:02 (02:42:ac:11:00:02)

Internet Protocol Version 4, Src: 172.17.0.1, Dst: 172.17.0.2

Transmission Control Protocol, Src Port: 50720, Dst Port: 22, Seq: 0, Len: 0

Source Port: 50720

Destination Port: 22

[Stream index: 0]

[Conversation completeness: Incomplete (37)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 425900277

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

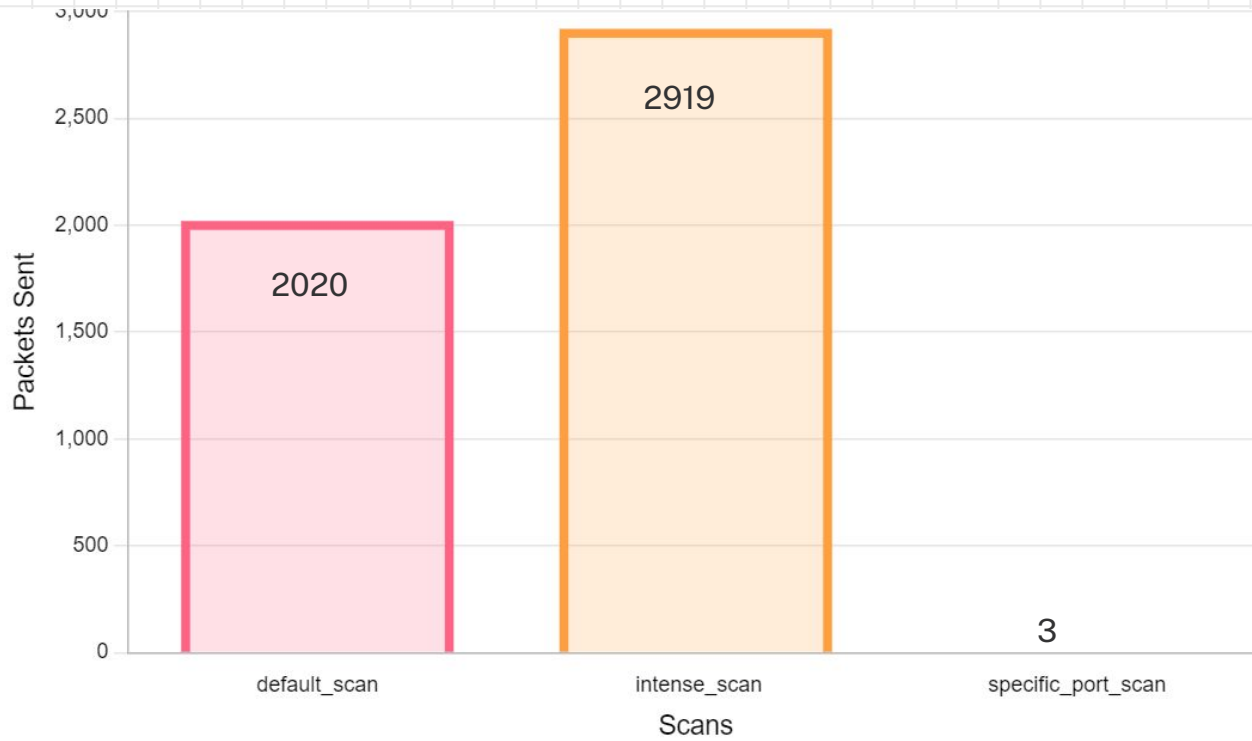
Destination Port (tcp.dstport), 2 bytes

Packets: 3 · Displayed: 3 (100.0%)

Profile: Default



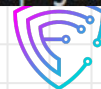
Comparison Between all 3 Scans



Nmap Scripts

- Nmap scripts are Lua programs
- used to automate tasks like vulnerability detection and service enumeration within Nmap scans.
- Run by NSE (Nmap Scripting Engine)

```
student@cyberforgeacademy:~$ cd /usr/share/nmap/scripts/
student@cyberforgeacademy:/usr/share/nmap/scripts$ ls -la
.
..
  nping-brute.nse
  nrpe-enum.nse
acarsd-info.nse
  ntp-info.nse
address-info.nse
  ntp-monlist.nse
afp-brute.nse
  omp2-brute.nse
afp-ls.nse
  omp2-enum-targets.nse
afp-path-vuln.nse
  omron-info.nse
afp-serverinfo.nse
  openlookup-info.nse
afp-showmount.nse
  openvas-otp-brute.nse
ajp-auth.nse
  http-headers.nse
  http-hp-ilo-info.nse
  http-huawei-hg5xx-vuln.nse
  http-icloud-findmyiphone.nse
  http-icloud-sendmsg.nse
  http-iis-short-name-brute.nse
  http-iis-webdav-vuln.nse
  http-internal-ip-disclosure.nse
  http-joomla-brute.nse
  http-jsonp-detection.nse
```

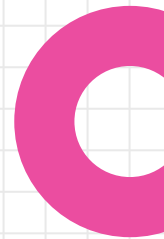


Nmap Scripts-Discovery

- Used to gather information about hosts within a network

Command: `nmap --script discovery <target>`

```
student@cyberforgeacademy:/usr/share/nmap/scripts$ nmap --script discovery 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-22 07:41 IST
Pre-scan script results:
| targets-asn:
|_ targets-asn.asn is a mandatory parameter
Nmap scan report for 172.17.0.2
Host is up (0.00023s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_ banner: 220 (vsFTPd 3.0.5)
22/tcp    open  ssh
|_ banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
|_ ssh2-enum-algos:
|   kex_algorithms: (11)
|   server_host_key_algorithms: (4)
|   encryption_algorithms: (6)
|   mac_algorithms: (10)
|   compression_algorithms: (2)
25/tcp    open  smtp
|_ banner: 220 185b11ded85d ESMTP Postfix (Ubuntu)
|_ smtp-commands: 185b11ded85d, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
|_ smtp-open-relay: Server doesn't seem to be an open relay, all tests failed
```



- Scripts include :
 - **banner:** Connects to an open TCP port and prints any response from the service.

```
21/tcp  open  ftp
|_ banner: 220 (vsFTPd 3.0.5)
22/tcp  open  ssh
|_ banner: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6
|_ ssh2-enum-algos:
|   kex_algorithms: (11)
|   server_host_key_algorithms: (4)
|   encryption_algorithms: (6)
|   mac_algorithms: (10)
|_ compression_algorithms: (2) T
```



- **dns-brute:** Attempts to enumerate DNS hostnames by brute force guessing of common subdomains

Host script results:

```
|_dns-brute: Can't guess domain of "172.17.0.2"; use dns-brute.domain script argument.
```

```
|_fcrdns: FAIL (No PTR record)
```



Nmap Scripts-exploit

- To test for and exploit known vulnerabilities in target systems.
- **Command:** `nmap --script exploit <target>`

```
● student@cyberforgeacademy:/usr/share/nmap/scripts$ nmap --script exploit 172.17.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2024-02-22 07:53 IST
Nmap scan report for 172.17.0.2
Host is up (0.00012s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp    open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open  http
|_ clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
139/tcp   open  netbios-ssn
```


- Scripts include :
 - **smtp-vuln-cve2010-4344**: Checks SMTP servers for vulnerability CVE-2010-4344

```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp open http
```



- **http-csrf:** Tests for CSRF vulnerabilities in HTTP applications
- **http-dombased-xss:** Detects DOM-based XSS vulnerabilities in HTTP apps
- **http-stored-xss:** Identifies Stored XSS flaws in HTTP apps

```
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```





Thanks!

Do you have any questions?

contact@cyberforge.academy

+91 8837537763

<https://cyberforge.academy>

<https://github.com/CyberForgeAcademy/Workshops>

CREDITS: This presentation template was created by [Slidesgo](#), and includes icons by [Flaticon](#), and infographics & images by [Freepik](#)