

**Day 2 of Learning Cyber Security****Platform: Kali Linux****Name:** Ayesha Nadeem**Topic:** Nmap & Zenmap**Contact Me:** [ayeshanm8@gmail.com](mailto:ayeshanm8@gmail.com)**Date:** 2<sup>nd</sup> July, 2025

Applied Cyber Security © 2025 by Ayesha Nadeem is licensed under CC BY-NC 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>

## Nmap: Reconnaissance & Scanning

### Command 1:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ nslookup nust.edu.pk
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   nust.edu.pk
Address: 172.67.68.211
Name:   nust.edu.pk
Address: 104.26.3.7
Name:   nust.edu.pk
Address: 104.26.2.7
Name:   nust.edu.pk
Address: 2606:4700:20::681a:307
Name:   nust.edu.pk
Address: 2606:4700:20::681a:207
Name:   nust.edu.pk
Address: 2606:4700:20::ac43:44d3
```

### Command 2:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:43 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.25s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 172.67.
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds

(ayeshanadeem@ayeshanadeem)-[~]
$ nmap 104.26.3.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:43 EDT
Nmap scan report for 104.26.3.7
Host is up (0.22s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 18.61 seconds
```

### Command 3:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -sP nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:45 EDT
Nmap scan report for nust.edu.pk (104.26.2.7)
Host is up (0.22s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.3.7 172.67.
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

## Command 4:

```
(ayeshanadeem@ayeshanadeem)~[~]
$ nmap -sT nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:46 EDT
Nmap scan report for nust.edu.pk (172.67.68.211)
Host is up (0.24s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 104.26.
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 17.49 seconds
```

## Command 5:

```
(ayeshanadeem@ayeshanadeem)~[~]
$ nmap -sU nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:47 EDT
Nmap scan report for nust.edu.pk (172.67.68.211)
Host is up (0.12s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 104.26.
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
33459/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 145.01 seconds
```

## Command 6:

```
(ayeshanadeem@ayeshanadeem)~[~]
$ nmap -sV nust.edu.pk --version-intensity 5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:52 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.29s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 172.67.68.
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Cloudflare http proxy
443/tcp   open  ssl/http  Cloudflare http proxy
8080/tcp  open  http      Cloudflare http proxy
8443/tcp  open  ssl/http  Cloudflare http proxy

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 38.61 seconds
```

## Command 7:

```

File Actions Edit View Help
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -sS nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:53 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.24s latency).
Other addresses for nust.edu.pk (not scanned): 172.67.68.211 104.26.3.7
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 17.84 seconds

```

## Command 8:

```

(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -p 8443,2052 nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:53 EDT
Nmap scan report for nust.edu.pk (172.67.68.211)
Host is up (0.083s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.3.7 104.26.2.7 104.26.2.7
PORT      STATE SERVICE
2052/tcp   open  clearvisn
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 0.71 seconds

(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -p [1-65536] nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:55 EDT
Ports specified must be between 0 and 65535 inclusive
QUITTING!

(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -p [1-65535] nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:55 EDT
Nmap scan report for nust.edu.pk (172.67.68.211)
Host is up (0.26s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.3.7 104.26.2.7 104.26.2.7
Not shown: 8364 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
2052/tcp   open  clearvisn
2053/tcp   open  knetd
2082/tcp   open  infowave
2083/tcp   open  radsec
2086/tcp   open  gnunet
2087/tcp   open  eli
2095/tcp   open  nbx-ser
2096/tcp   open  nbx-dir
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
8880/tcp   open  cddbp-alt

Nmap done: 1 IP address (1 host up) scanned in 94.79 seconds

```

## Command 9:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -O nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 09:58 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.30s latency).
Other addresses for nust.edu.pk (not scanned): 172.67.68.211 104.26.2.7 2606:4700:20::681
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Aggressive OS guesses: Apple iOS 14.0 - 15.6 or tvOS 14.3 - 16.1 (Darwin 20.0.0 - 22.1.0)
- 22.4.0) (89%), FreeBSD 11.1-STABLE (89%), FreeBSD 12.0-RELEASE - 12.1-RELEASE (89%), F
E (85%), FreeBSD 11.2-RELEASE - 11.3 RELEASE (85%), FreeBSD 12.0-RELEASE - 13.0-RELEASE (
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 29.97 seconds
```

## Command 10:

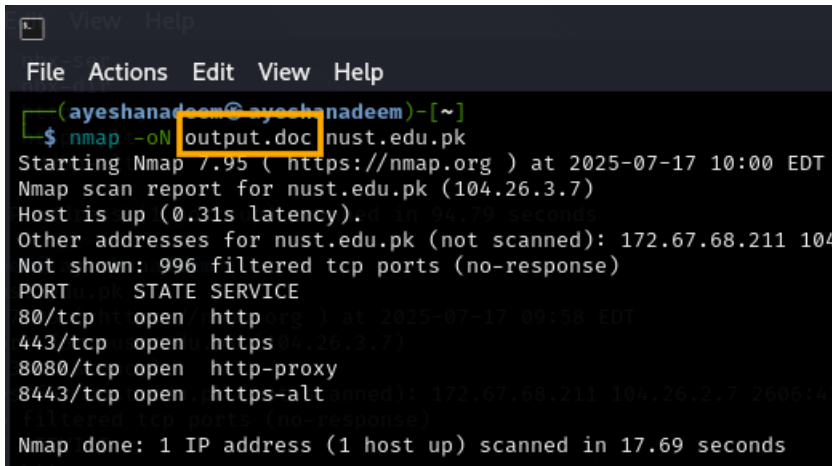
```
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap --script http-vuln* 104.26.3.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 10:19 EDT
Nmap scan report for 104.26.3.7
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 38.92 seconds
```

## Command 11:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ nmap -oN output.txt nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 10:00 EDT
Nmap scan report for nust.edu.pk (172.67.68.211)
Host is up (0.27s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 104.2
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 17.92 seconds
```



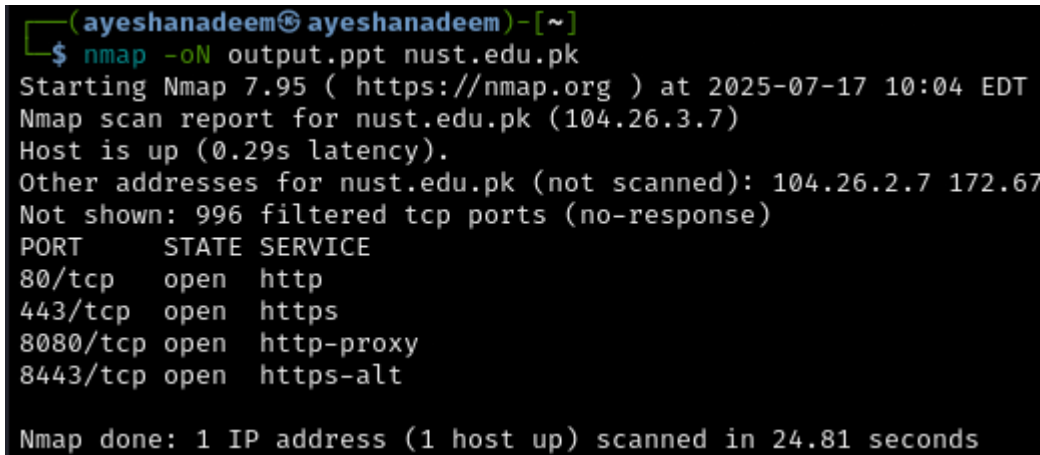
## Command 12:



```

ayeshanadeem@ayeshanadeem:~$ nmap -oN output.doc nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 10:00 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.31s latency).
Other addresses for nust.edu.pk (not scanned): 172.67.68.211 104.26.2.7 260614
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 17.69 seconds
  
```

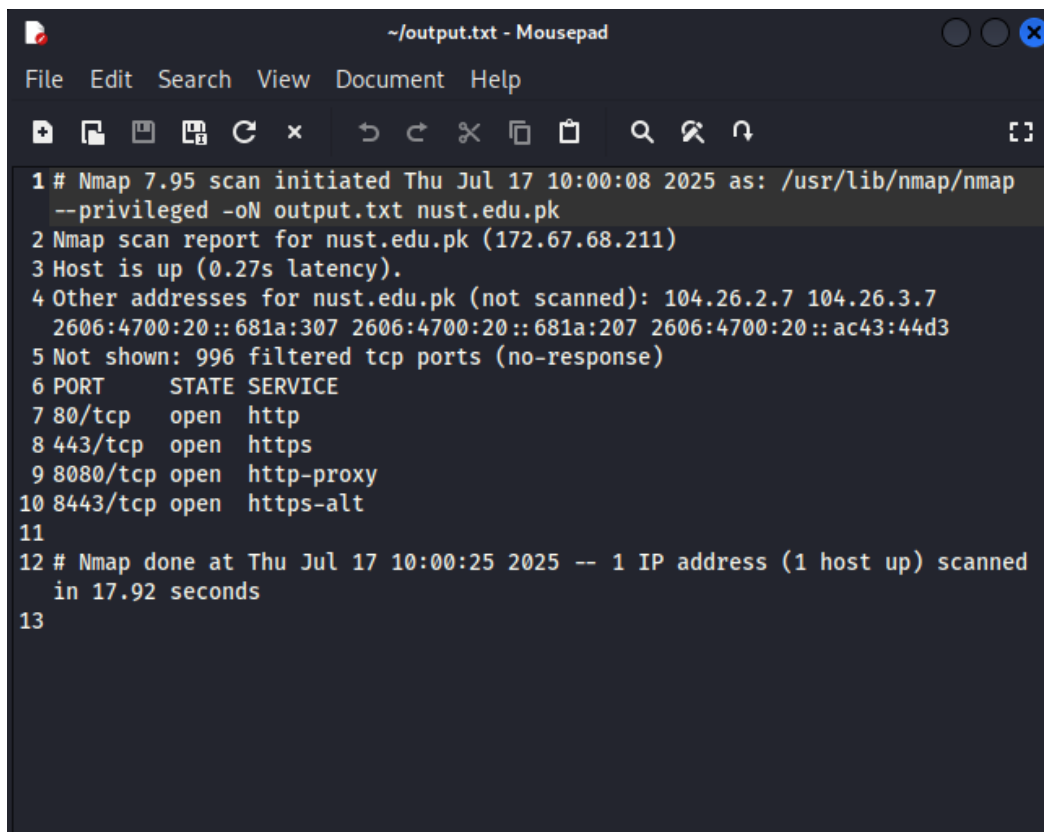
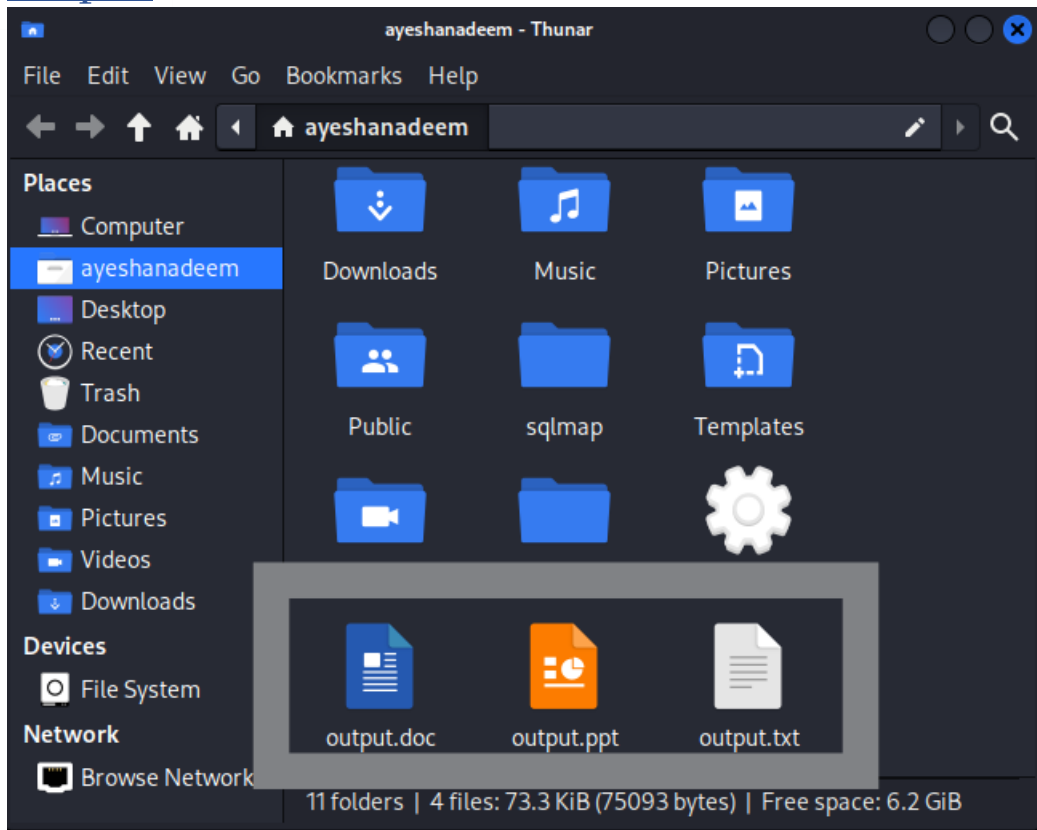
## Command 13:



```

ayeshanadeem@ayeshanadeem:~$ nmap -oN output.ppt nust.edu.pk
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 10:04 EDT
Nmap scan report for nust.edu.pk (104.26.3.7)
Host is up (0.29s latency).
Other addresses for nust.edu.pk (not scanned): 104.26.2.7 172.67.68.211
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 24.81 seconds
  
```

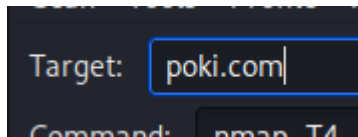
Output:



## Zenmap: Reconnaissance & Scanning

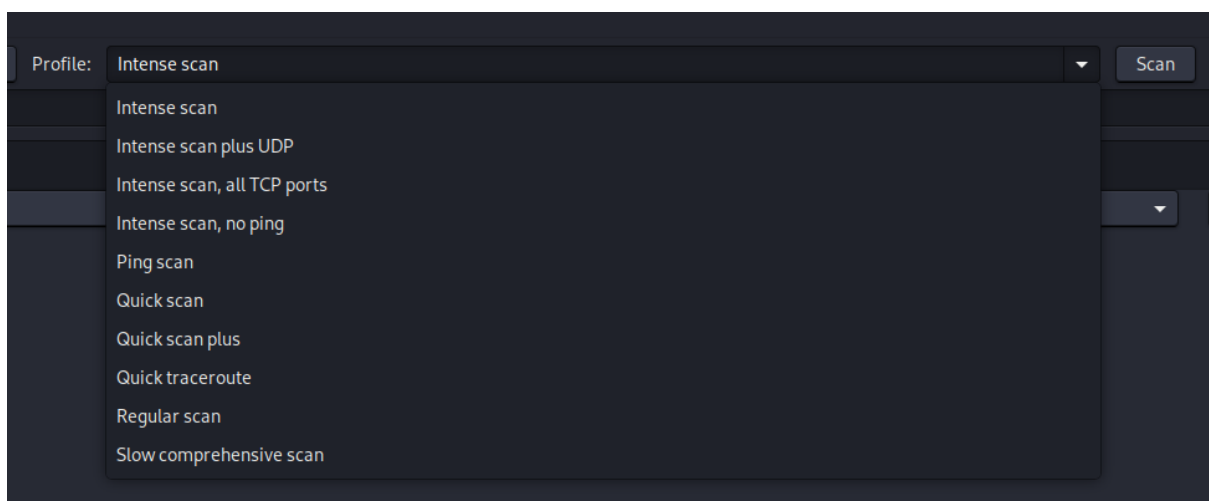
### Step 1:

Set any Target IP/ Target domain name



### Step 2:

Choose any scan type and hit the scan button



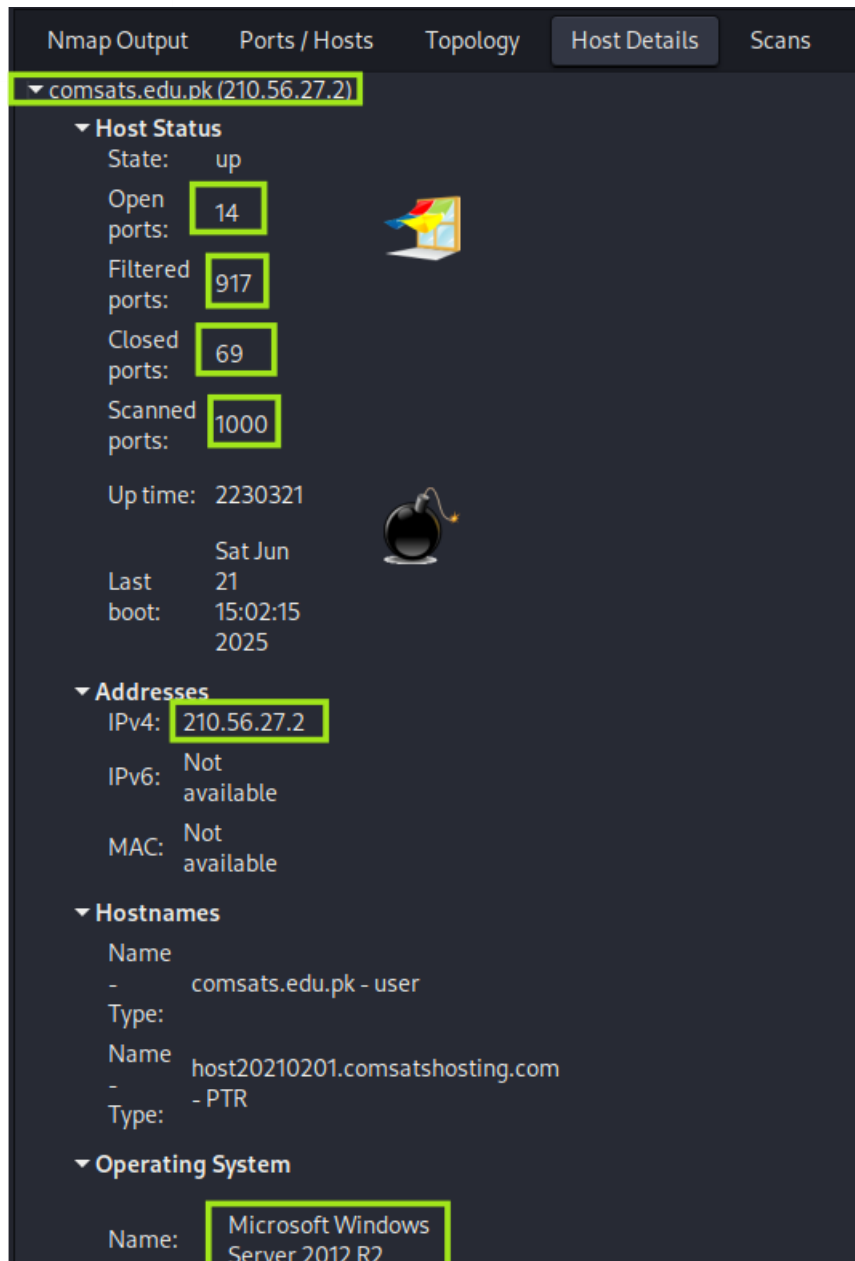
### Outputs:

Hosts		Services		Nmap Output		Ports / Hosts	Topology	Host Details	Scans
OS	Host			Port	Protocol	State	Service	Version	
	daraz.com (8.219)			✓ 21	tcp	open	ftp	Microsoft ftpd	
	poki.com (104.18)			✓ 53	tcp	open	domain	Simple DNS Plus	
	comsats.edu.pk			✓ 80	tcp	open	http	Microsoft IIS httpd 10.0	
				✓ 110	tcp	open	pop3	SmarterMail pop3d	
				✓ 143	tcp	open	imap	SmarterMail imapd	
				✓ 443	tcp	open	http	Microsoft IIS httpd 10.0	
				✓ 465	tcp	open	smtp	IA Mailserver smtpd	
				✓ 587	tcp	open	smtp	IA Mailserver smtpd	
				✓ 993	tcp	open	imap	SmarterMail imapd	
				✓ 995	tcp	open	pop3	SmarterMail pop3d	
				✓ 1433	tcp	open	ms-sql-s	Microsoft SQL Server 2016 13.00.4001.00; SP1	
				✓ 3306	tcp	open	mysql	MariaDB 5.5.5-10.11.8	
				✓ 8443	tcp	open	http	Microsoft IIS httpd 10.0	
				✓ 9998	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	

### *Open Ports Detail*



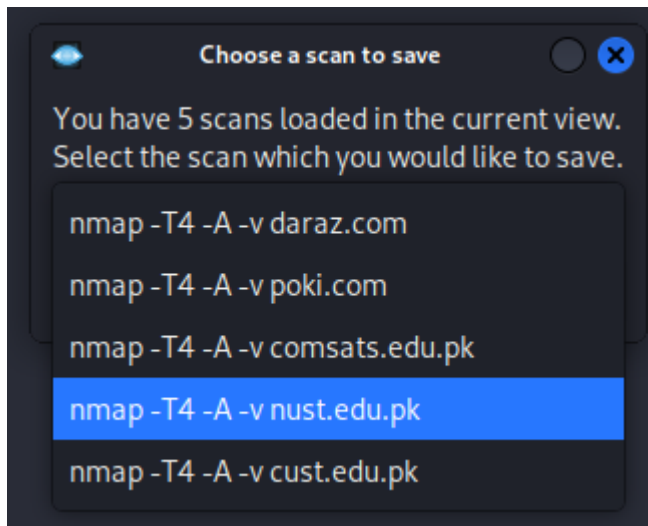
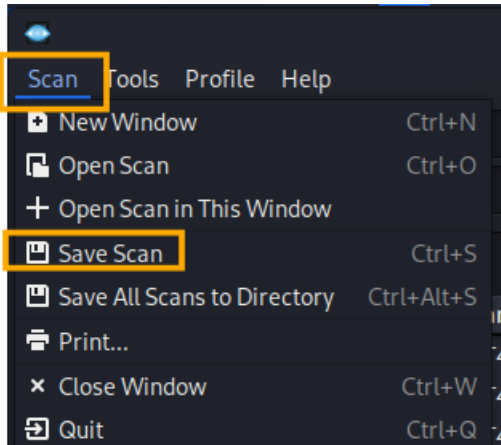




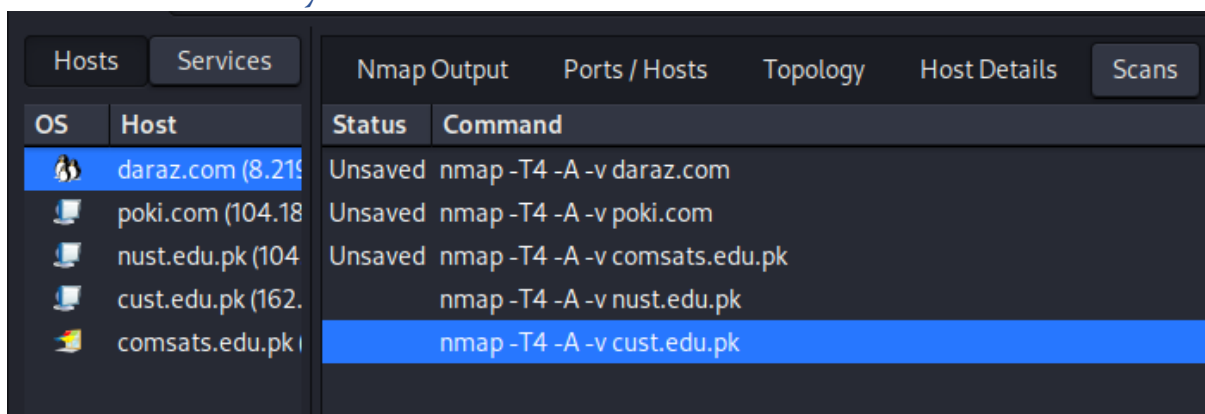
*Some other details*

### Step 3:

Save any two scan

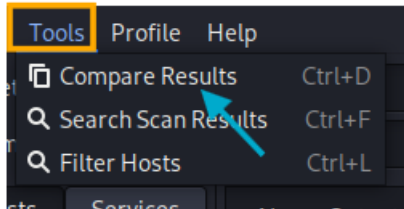


Saved successfully



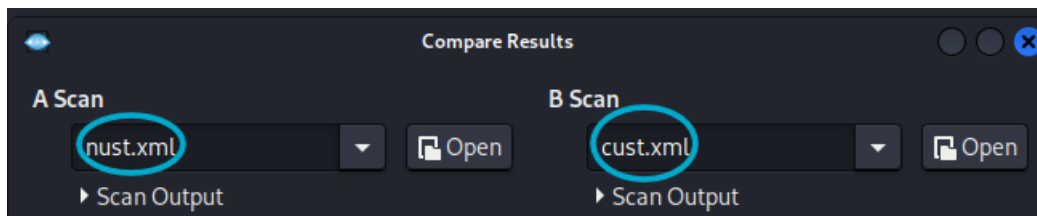
## Step 4:

Compare the outputs



## Step 5:

Upload/Open saved scan files.



## Output:

