

## Week 3: Network Scanning, Footprinting and Enumeration

Name: V. Risvanth

### Introduction

In the realm of cybersecurity, reconnaissance and scanning are crucial steps in assessing the security posture of a target network. This report focuses on conducting various scanning techniques to gather critical information about a system, including active hosts, open ports, running services, and potential vulnerabilities. The objective is to identify security gaps that could be exploited by attackers and provide insights for strengthening network defenses.

### Scope of the Task

The study involves performing a series of active scans using **Nmap** and other open-source tools to compare results and gain a comprehensive understanding of the target network.

The tasks include:

- Identifying the target **IP range** for scanning.
- Conducting **ping scans** to detect active hosts.
- Performing **port scanning** to discover open ports.
- Executing **service enumeration** to determine the versions of running services.
- Using **banner grabbing** to extract additional information about these services.
- Conducting **OS fingerprinting** to identify the target operating system.
- Gathering **network footprinting data** using tools like whois, dig, and nslookup.
- Performing a **vulnerability assessment** to detect security flaws.
- Comparing the output of Nmap scans with results from other open-source tools.
- Conducting **five additional active scans** with Nmap and documenting the findings.

### Tools Used

This study employs **Nmap (Network Mapper)**—one of the most powerful open-source tools for network discovery and security auditing. Additionally, other open-source tools will be used for comparative analysis to evaluate differences in scanning accuracy and efficiency.

## Importance of the Nmap

Cyber attackers often leverage the same reconnaissance techniques to gather intelligence before launching an attack. By proactively performing these scanning techniques, organizations can:

- Identify and remediate security vulnerabilities before they are exploited.
- Strengthen their network security posture by understanding potential attack vectors.
- Enhance security monitoring and incident response strategies.

## Commands Used

### 1. Identifying Target IP Range:

- Objective: Determine the target IP range for scanning
- Command: `ip a | grep inet`
- Analysis: Identifies the network subnet for scanning

### 2. Performing Ping Scan :

- Objective: Identify active hosts within the target IP range.
- Command: `nmap -sn 44.228.249.3`
- Analysis: Displays active devices on the network using ICMP packets.

### 3. Performing Port Scanning:

- Objective: Identify open ports on the active hosts
- Command: `nmap -p- 44.228.249.3`
- Analysis: Scans all 65,535 ports to detect open ones.

### 4. Service Enumeration:

- Objective: Detect the version of services running on open ports.
- Command: `nmap -sV 44.228.249.3`
- Analysis: Identifies service versions and helps in vulnerability detection.

#### 5. Banner Grabbing:

- Objective: Extract banners from open ports
- Command: `nmap --script=banner 44.228.249.3`
- Analysis: Provides software details that may contain vulnerabilities.

#### 6. OS Fingerprinting:

- Objective: Identify the operating system of the target.
- Command: `nmap -O 44.228.249.3`
- Analysis: Determines if the target is Windows, Linux, or another OS.

#### 7. Footprinting:

- Objective: Domain Gathering Information
- Command: `dig testphp.vulnweb.com`  
(or)
- Command: `nslookup testphp.vulnweb.com`
- Analysis: Provides domain owner details and DNS records.

#### 8. Vulnerability Assessment:

- Objective: To find the vulnerability using nmap
- Command: `nmap --script=vuln 44.228.249.3`
- Analysis: Identifies security flaws and misconfigurations.

## 9. Comparing Nmap with Other Open Source Tools:

- Nmap - it is used for Scanning, Enumeration, Vulnerability Analysis
- Nikto - it is used for Web vulnerability scanner
- OpenVAS – it is used for full vulnerability assessment
- Metasploit – it is used for Exploit and penetration testing
- Masscan - it is used for high speed network scanning

## 10. Performing 5 More Active Scans and Analysis:

### Scan 1: TCP SYN Scan:

- Command: `nmap -sS 44.228.249.3`
- Analysis: Stealth scan to detect open TCP ports.

### Scan 2: UDP Scan:

- Command: `nmap -sU 44.228.249.3`
- Analysis: Identifies UDP-based services like DNS and SNMP.

### Scan 3: Aggressive Scan:

- Command: `nmap -A 44.228.249.3`
- Analysis: Performs multiple scans in one command.

### Scan 4: Evading Firewalls with Fragmentation:

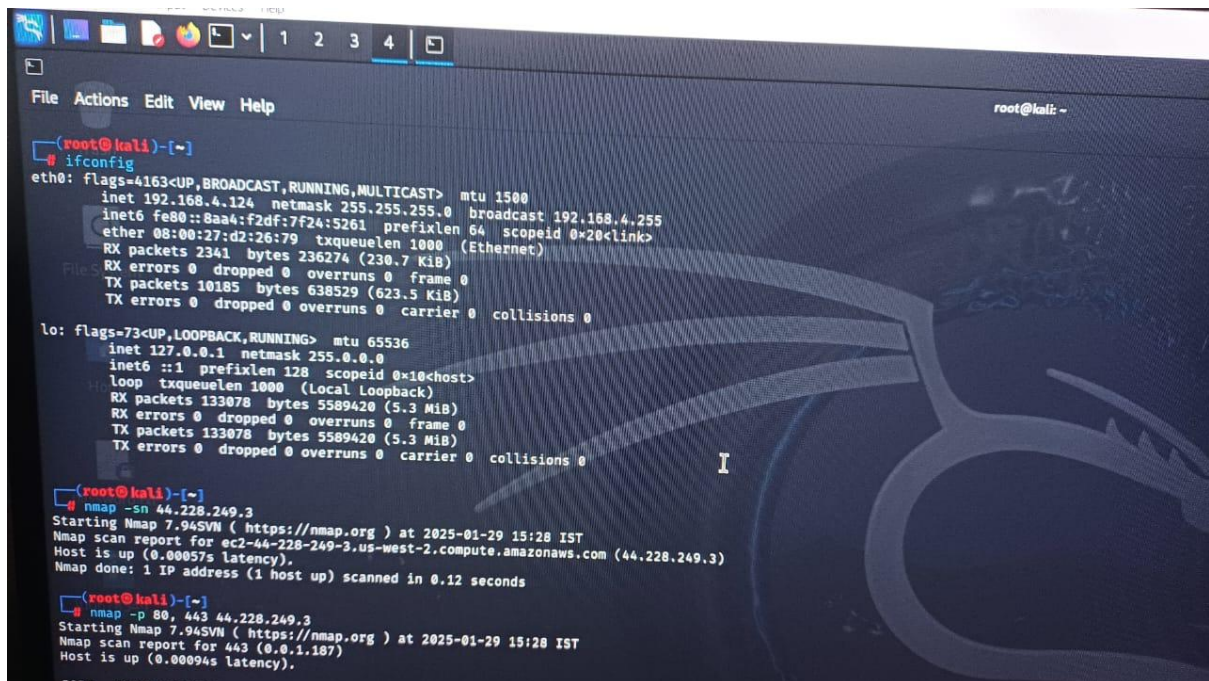
- Command: `nmap -f 44.228.249.3`
- Analysis: Helps bypass intrusion detection systems.

### Scan 5: Spoofing Source IP for Anonymous Scanning

- Command: `nmap -S 192.168.4.124 44.228.249.3`
- Analysis: Hides the real scanner identity.

All the Commands for this task are included with working functionality

### Screenshots



```
(root@kali)~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.4.124 netmask 255.255.255.0 broadcast 192.168.4.255
    inet6 fe80::8aa4:f2df:7f24:5261 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d2:26:79 txqueuelen 1000 (Ethernet)
    RX packets 2341 bytes 236274 (230.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10185 bytes 638529 (623.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 133078 bytes 5589420 (5.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 133078 bytes 5589420 (5.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)~# nmap -sn 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(root@kali)~# nmap -p 80,443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for 443 (0.0.1.107)
Host is up (0.00094s latency).
```

1. Using `ifconfig` command and checked the ip address

```
File Actions Edit View Help
root@kali ~

root@kali:~# nmap -sn 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

root@kali:~# nmap -p 80,443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:28 IST
Nmap scan report for 443 (0.0.1.187)
Host is up (0.00094s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.36 seconds

root@kali:~# nmap -p 443 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:29 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00057s latency).

PORT      STATE SERVICE
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

root@kali:~# nmap -p- 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:29 IST
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.93% done; ETC: 15:32 (0:02:58 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 135.05 seconds
```

```
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 135.05 seconds

root@kali:~# nmap -sV 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:32 IST
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.24% done; ETC: 15:33 (0:00:00 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00096s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http-proxy  DansGuardian HTTP proxy
81/tcp    open  http-proxy  DansGuardian HTTP proxy
443/tcp   open  https?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.22 seconds

root@kali:~# nmap --script-banner 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:33 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 21.05 seconds

root@kali:~# nmap -O 44.228.249.3
```

2. Through Nmap I checked with the Ip address what are the hosts all are alive and checking thee ports which is open



### 1.Performing Ping Scan :

- Objective: Identify active hosts within the target IP range.
- Command: `nmap -sn 44.228.249.3`
- Analysis: Displays active devices on the network using ICMP packets.

## 2. Performing Port Scanning:

- Objective: Identify open ports on the active hosts
- Command: `nmap -p- 44.228.249.3`
- Analysis: Scans all 65,535 ports to detect open ones.

### 3. Service Enumeration:

- Objective: Detect the version of services running on open ports.
- Command: `nmap -sV 44.228.249.3`
- Analysis: Identifies service versions and helps in vulnerability detection.

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 49.22 seconds

(root@kali)~#
# nmap --script-banner 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:33 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 21.05 seconds

(root@kali)~#
# nmap -O 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:34 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (97%), Synology DiskStation Manager 5.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6:32 cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:
Aggressive OS guesses: Linux 4.15 - 5.8 (97%), Linux 5.0 - 5.4 (87%), Linux 5.0 - 5.5 (95%), Linux 5.4 (91%), Linux 2.6:32 (91%), Linux 3.10 - 4.11 (91%), Linux 3
5644 (91%), Linux 2.6:32 - 3.19 (90%)
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 11.70 seconds

(root@kali)~#
# whois testphp.vulnweb.com
No match for "TESTPHP.VULNWEB.COM".
```

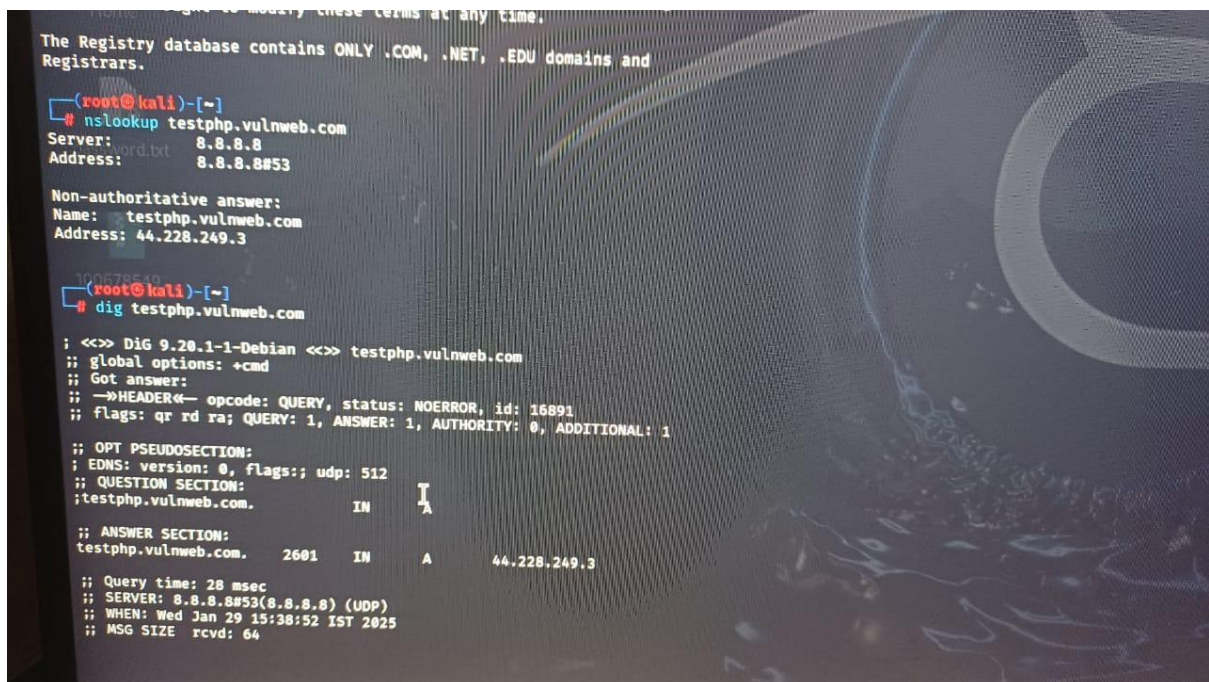
### 1. Banner Grabbing:

- Objective: Extract banners from open ports
- Command: `nmap --script=banner 44.228.249.3`

- Analysis: Provides software details that may contain vulnerabilities.

## 2. OS Fingerprinting:

- Objective: Identify the operating system of the target.
- Command: `nmap -O 44.228.249.3`
- Analysis: Determines if the target is Windows, Linux, or another OS.



```

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

(root@kali)~# nslookup testphp.vulnweb.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   testphp.vulnweb.com
Address: 44.228.249.3

(root@kali)~# dig testphp.vulnweb.com

; <<>> DiG 9.20.1-1-Debian <<>> testphp.vulnweb.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 16891
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;testphp.vulnweb.com.      IN      A
;; ANSWER SECTION:
testphp.vulnweb.com.      2601    IN      A      44.228.249.3

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 29 15:38:52 IST 2025
;; MSG SIZE rcvd: 64

```

## 1. Footprinting:

- Objective: Domain Gathering Information
- Command: `dig testphp.vulnweb.com`  
(or)
- Command: `nslookup teestphp.vulnweb.com`
- Analysis: Provides domain owner details and DNS records.



```
File Actions Edit View Help
;testphp.vulnweb.com.      IN      A
;; ANSWER SECTION:
testphp.vulnweb.com.      2601    IN      A      44.228.249.3

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 29 15:38:52 IST 2025
;; MSG SIZE rcvd: 64

(root@kali)-[~]
# nmap --script=vuln 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:39 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002),
|_  Hosts are all up (not vulnerable).
Stats: 0:01:22 elapsed; 0 hosts completed (1 up); 1 unresolved; 2 bytes
```

```
File Actions Edit View Help
;testphp.vulnweb.com.      IN      A
;; ANSWER SECTION:
testphp.vulnweb.com.      2601    IN      A      44.228.249.3

;; Query time: 28 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Jan 29 15:38:52 IST 2025
;; MSG SIZE rcvd: 64

(root@kali)-[~]
# nmap --script=vuln 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:39 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002),
|_  Hosts are all up (not vulnerable).
Stats: 0:01:22 elapsed; 0 hosts completed (1 up); 1 unresolved; 2 bytes
```



## 1. Vulnerability Assessment:

- Objective: To find the vulnerability using nmap
- Command: `nmap --script=vuln 44.228.249.3`
- Analysis: Identifies security flaws and misconfigurations.

```
Stats: 0:07:39 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.67% done; ETC: 15:47 (0:00:01 remaining)
Stats: 0:08:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.67% done; ETC: 15:48 (0:00:02 remaining)
Stats: 0:10:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.67% done; ETC: 15:50 (0:00:02 remaining)

(root@kali)~# nmap -sS 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:50 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.0020s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.38 seconds

(root@kali)~# nmap -sU 44.228.149.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:51 IST
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.75% done; ETC: 15:57 (0:04:54 remaining)
Stats: 0:03:05 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.85% done; ETC: 16:01 (0:06:55 remaining)
Stats: 0:04:31 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 35.20% done; ETC: 16:04 (0:08:19 remaining)
Stats: 0:05:20 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.40% done; ETC: 16:05 (0:08:156 remaining)
Stats: 0:08:54 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 40.00% done; ETC: 16:06 (0:08:156 remaining)

No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 1.96 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

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 222.25 seconds

(root@kali)~# nmap -F 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 15:59 IST
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.00% done; ETC: 16:04 (0:03:31 remaining)
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 61.00% done; ETC: 16:04 (0:01:52 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.27s latency).
All 1000 scanned ports on ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 284.19 seconds

(root@kali)~# nmap -S 192.168.1.100 44.228.249.3
WARNING: If -S is being used to fake your source address, you may also have to use -e <interface> and -Pn . If you are using it to specify your real source address, you can ignore this warning.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-29 16:07 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.00094s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
81/tcp    open  hosts2-ns
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.77 seconds
```





- Analysis: Stealth scan to detect open TCP ports.

#### Scan 2: UDP Scan:

- Command: `nmap -sU 44.228.249.3`
- Analysis: Identifies UDP-based services like DNS and SNMP.

#### Scan 3: Aggressive Scan:

- Command: `nmap -A 44.228.249.3`
- Analysis: Performs multiple scans in one command.

#### Scan 4: Evading Firewalls with Fragmentation:

- Command: `nmap -f 44.228.249.3`
- Analysis: Helps bypass intrusion detection systems.

#### Scan 5: Spoofing Source IP for Anonymous Scanning

- Command: `nmap -S 192.168.4.124 44.228.249.3`
- Analysis: Hides the real scanner identity.

## Conclusion

The network scanning and security assessment conducted in this task provided valuable insights into the security posture of the target environment. By systematically performing **ping scans, port scans, service enumeration, banner grabbing, OS fingerprinting, footprinting, and vulnerability assessments**, we identified active hosts, open ports, running services, and potential vulnerabilities.

The use of **Nmap** and other open-source tools allowed us to compare outputs, assess tool accuracy, and determine the effectiveness of different scanning techniques. Through **banner grabbing and OS fingerprinting**, we gained deeper visibility into system configurations and potential weaknesses. Additionally, the **footprinting phase** using tools like **whois, dig, and nslookup** helped gather external intelligence on the target domain.

By performing multiple **active scans with Nmap**, we observed various network behaviors and security gaps. These findings emphasize the importance of **regular network scanning and vulnerability assessments** to proactively detect and mitigate security risks.

Overall, this assessment highlights the critical need for **continuous monitoring, proper network hardening, and security best practices** to protect against cyber threats. The insights from this report can be used to strengthen security defenses and improve overall network resilience.

---