Sapience Edu Connect Pvt Ltd

NAME: DEVALLA JWALA NARSIMHA
DOMAIN: CYBER SECURITY

Week 3: Network Scanning, Footprinting and Enumeration

Task3:

1. Identify Target IP Range:

a. Determine the target IP range for scanning

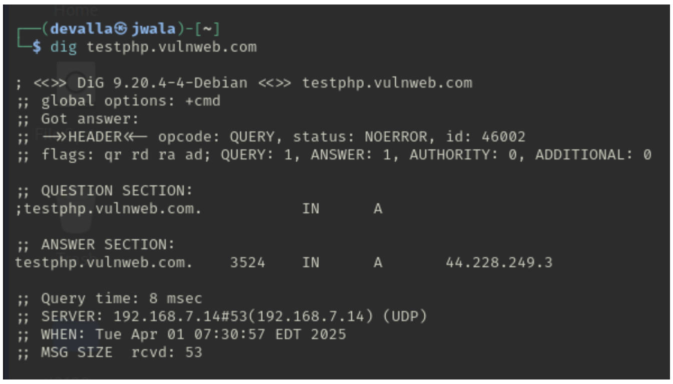
Step 1: Gather Initial Information.

Resolve the Domain to an IP Address

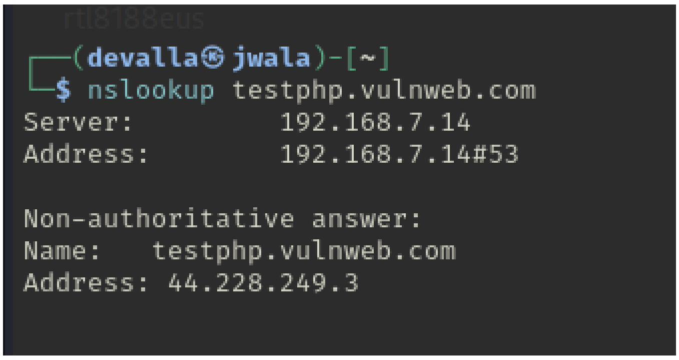
Use a tool like nslookup or dig to resolve the domain name to an IP address.

nslookup testphp.vulnweb.com

dig testphp.vulnweb.com



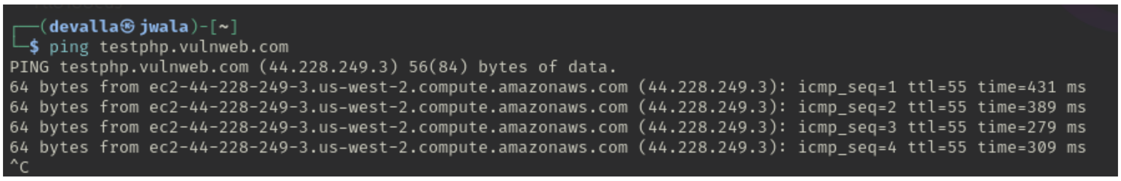
```
┌──(devalla㉿jwala)-[~]
└─$ dig testphp.vulnweb.com

; <<>> DiG 9.20.4-4-Debian <<>> testphp.vulnweb.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46002
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;testphp.vulnweb.com.           IN      A

;; ANSWER SECTION:
testphp.vulnweb.com.    3524    IN      A       44.228.249.3

;; Query time: 8 msec
;; SERVER: 192.168.7.14#53(192.168.7.14) (UDP)
;; WHEN: Tue Apr 01 07:30:57 EDT 2025
;; MSG SIZE  rcvd: 53
```



```
┌──(devalla㉿jwala)-[~]
└─$ nslookup testphp.vulnweb.com
Server:         192.168.7.14
Address:        192.168.7.14#53

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

2 Perform Ping Scan:
a. Toidentify active hosts within the target IP range.

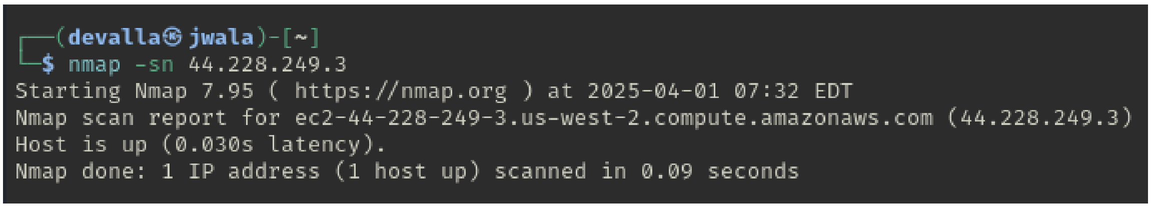
Step1: ping testphp.vulnweb.com



```
┌──(devalla㉿jwala)-[~]
└─$ ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=1 ttl=55 time=431 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=2 ttl=55 time=389 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=3 ttl=55 time=279 ms
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3): icmp_seq=4 ttl=55 time=309 ms
^C
```

Nmap is a powerful network scanning tool that can perform a ping scan to identify active hosts. The command to perform a ping scan is:

nmap -sn 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sn 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 07:32 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.030s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

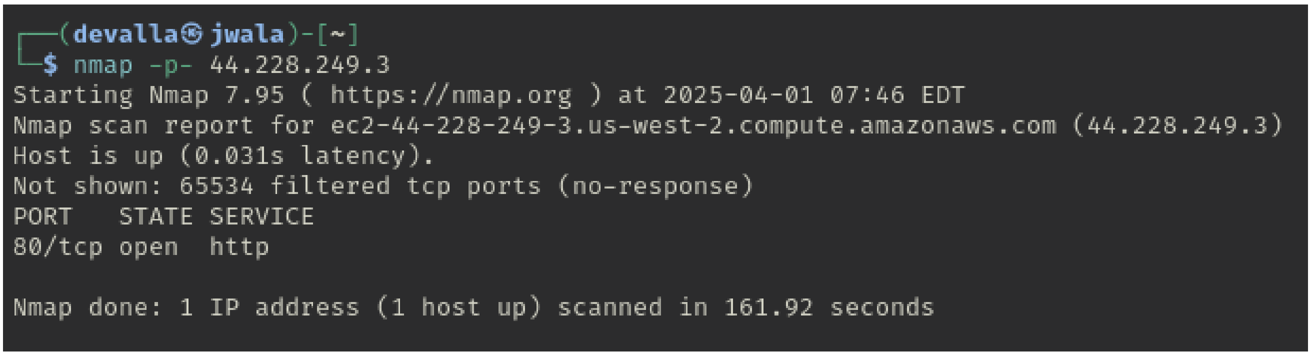
3.Port Scanning:

a. Perform a comprehensive port scan on the identified active hosts to discover open ports

Step1:

Open your terminal and execute the following command to perform a comprehensive port scan on the identified active hosts:

nmap -p- 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -p- 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 07:46 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.031s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 161.92 seconds
```

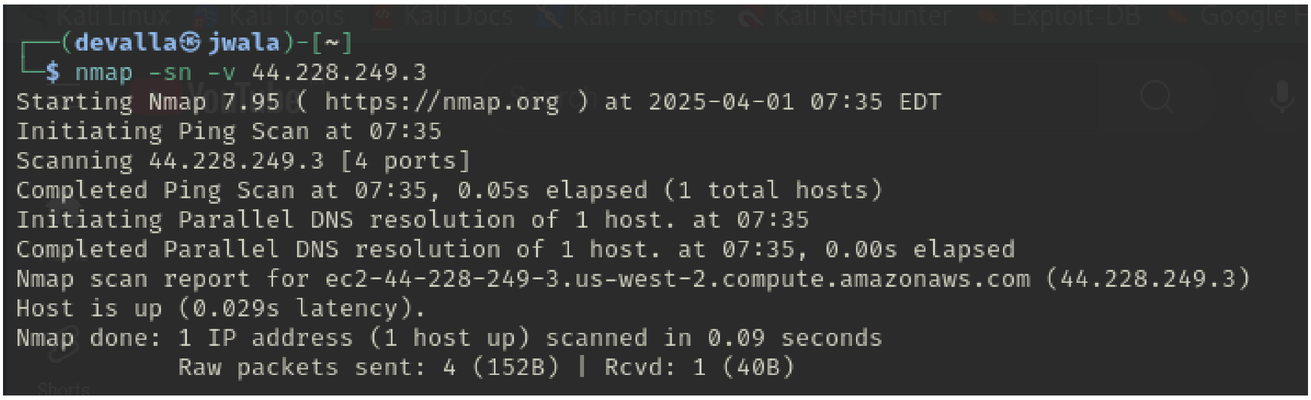
4.Service Enumeration:

a. Toidentify the version of services running on open ports.

Step1:

Identify the version of services running on open ports. Nmap can help with this:

nmap -sn -v 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sn -v 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 07:35 EDT
Initiating Ping Scan at 07:35
Scanning 44.228.249.3 [4 ports]
Completed Ping Scan at 07:35, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:35
Completed Parallel DNS resolution of 1 host. at 07:35, 0.00s elapsed
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.029s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
           Raw packets sent: 4 (152B) | Rcvd: 1 (40B)
```

To determine the version of services running on open ports.

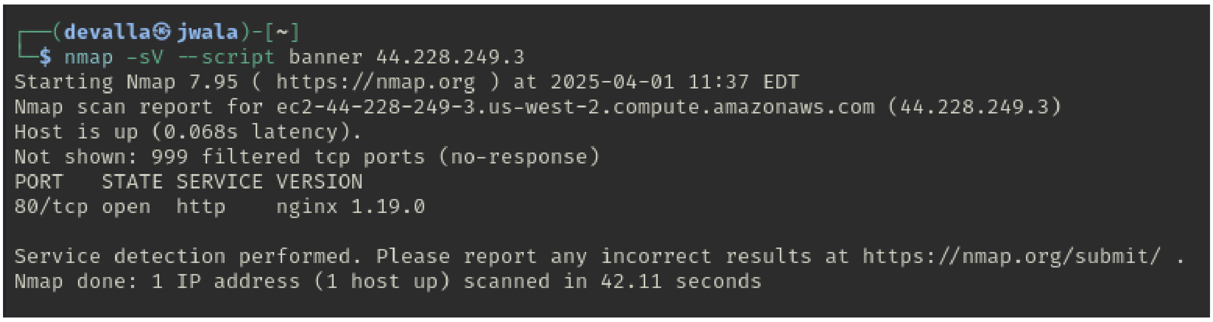
5.Banner Grabbing:

a. Tograb banners from open ports to gather more information about the services.

Step1:

Grab banners from open ports to gather more information about the services. Nmap can also be used for banner grabbing

nmap -sV --script banner 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sV --script banner 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 11:37 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.068s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.11 seconds
```

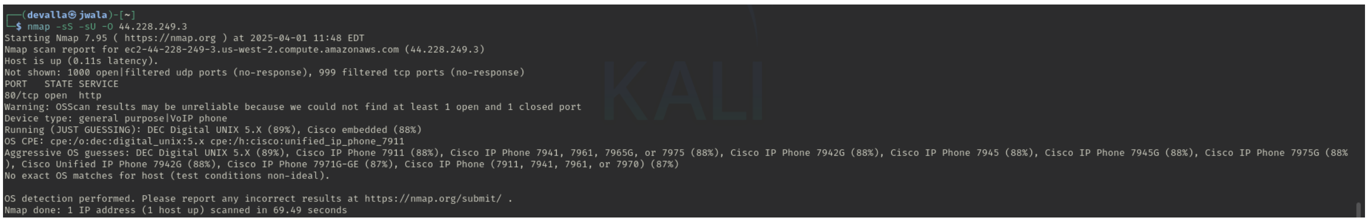
6. OSFingerprinting:

a. Toperform OS fingerprinting on the target machine.

Step1:

Perform OS fingerprinting on the target machine. Nmap can do this:

nmap -sS -sU -O 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sS -sU -O 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 11:48 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.11s latency).
Not shown: 1000 open|filtered udp ports (no-response), 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|VoIP phone
Running (JUST GUESSING): DEC Digital UNIX 5.X (89%), Cisco embedded (88%)
OS CPE: cpe:/o:dec:digital_unix:5.x cpe:/h:cisco:unified_ip_phone_7911
Aggressive OS guesses: DEC Digital UNIX 5.X (89%), Cisco IP Phone 7911 (88%), Cisco IP Phone 7941, 7961, 7965G, or 7975 (88%), Cisco IP Phone 7942G (88%), Cisco IP Phone 7945 (88%), Cisco IP Phone 7945G (88%), Cisco IP Phone 7975G (88%
), Cisco Unified IP Phone 7942G (88%), Cisco IP Phone 7971G-GE (87%), Cisco IP Phone (7911, 7941, 7961, or 7970) (87%)
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 69.49 seconds
```

7.Footprinting:

a. Use tools like whois, dig, and nslookup to gather additional information about the target network and domain.

Step1:

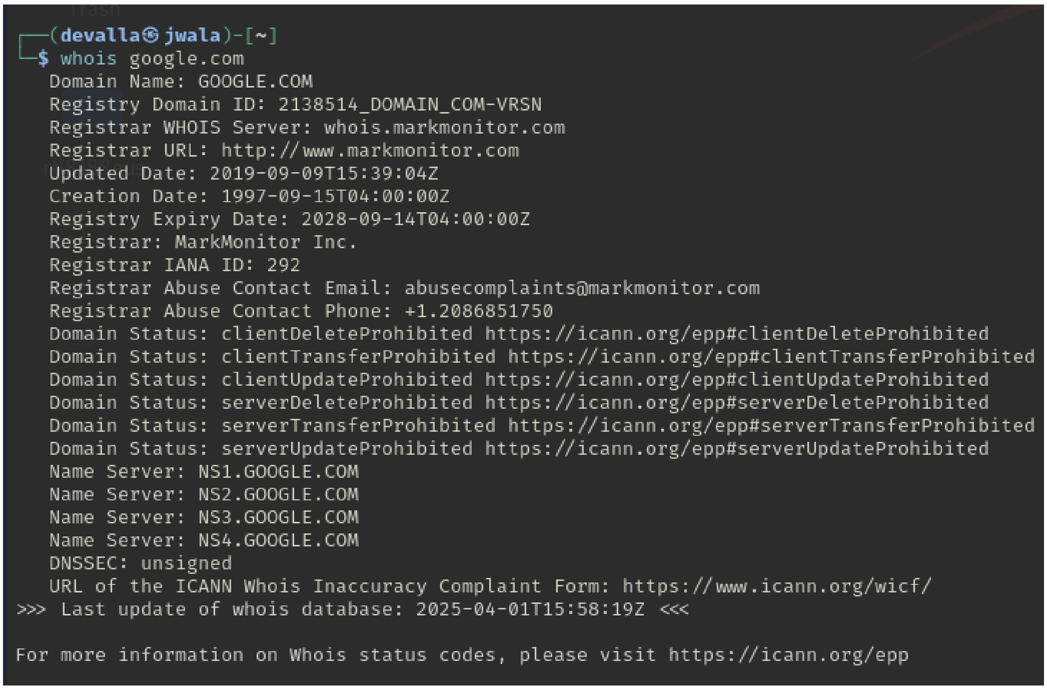
Use tools like whois, dig, and nslookup to gather additional information about the target network and domain.
For example:

whois <domain>

dig <domain>

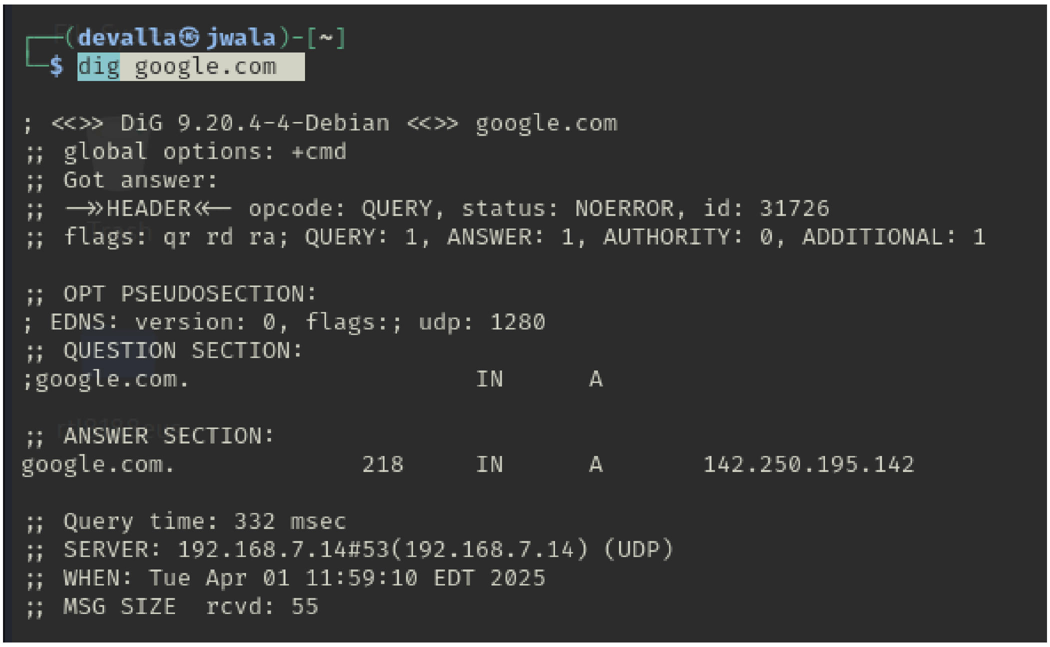
nslookup <domain>

whois google.com



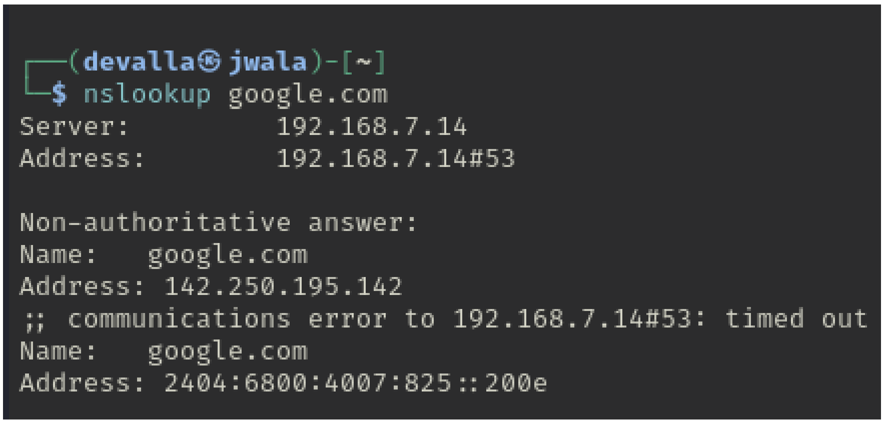
```
┌──(devalla㉿jwala)-[~]
└─$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-04-01T15:58:19Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

dig google.com



```
┌──(devalla㉿jwala)-[~]
└─$ dig google.com

; <<>> DiG 9.20.4-4-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31726
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             218     IN      A       142.250.195.142

;; Query time: 332 msec
;; SERVER: 192.168.7.14#53(192.168.7.14) (UDP)
;; WHEN: Tue Apr 01 11:59:10 EDT 2025
;; MSG SIZE  rcvd: 55
```

nslookup google.com



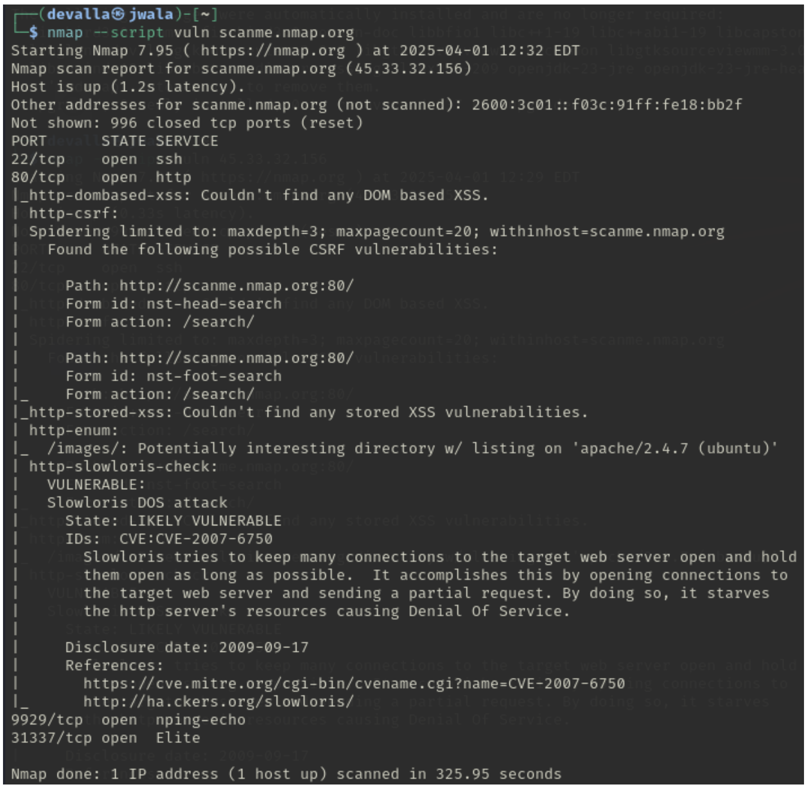
```
┌──(devalla㉿jwala)-[~]
└─$ nslookup google.com
Server:         192.168.7.14
Address:        192.168.7.14#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.195.142
;; communications error to 192.168.7.14#53: timed out
Name:   google.com
Address: 2404:6800:4007:825::200e
```

8.Vulnerability assessment:
a. Toperform Vulnerability assessment using nmap.

Step1:

Perform a vulnerability assessment using Nmap. You can use Nmap scripts for this:

nmap --script vuln scanme.nmap.org



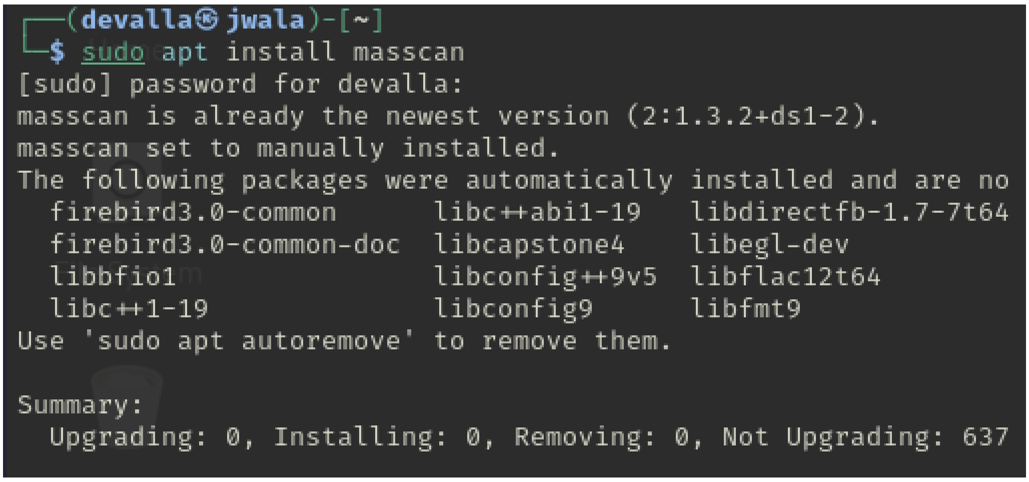
```
┌──(devalla㉿jwala)-[~]
└─$ nmap --script vuln scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 12:32 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (1.2s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-head-search
|     Form action: /search/
|
|     Path: http://scanme.nmap.org:80/
|     Form id: nst-foot-search
|_    Form action: /search/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 325.95 seconds
```

9. Also perform the above tasks with other open source tools and compare the output.

To compare the output, you can use other open-source tools like:

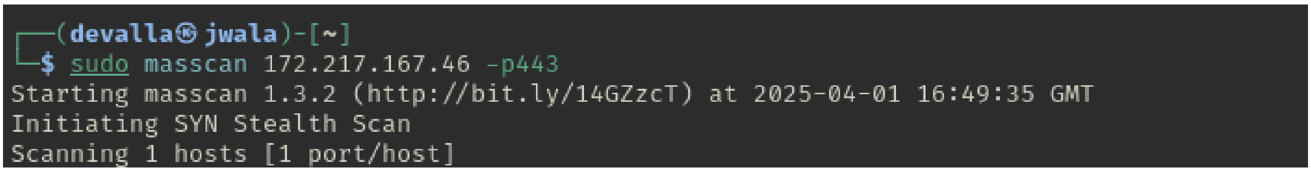
- **Masscan: For fast port scanning.**
- **Zmap: Another fast port scanner.**
- **OpenVAS: For vulnerability scanning.**
- **Nikto: For web server scanning.**

sudo apt install masscan



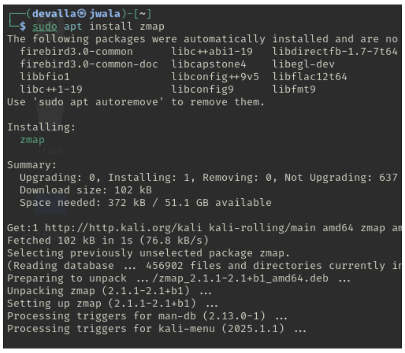
```
┌──(devalla㉿jwala)-[~]
└─$ sudo apt install masscan
[sudo] password for devalla:
masscan is already the newest version (2:1.3.2+ds1-2).
masscan set to manually installed.
The following packages were automatically installed and are no
  firebird3.0-common      libc++abi1-19   libdirectfb-1.7-7t64
  firebird3.0-common-doc  libcapstone4    libegl-dev
  libbfio1                libconfig++9v5  libflac12t64
  libc++1-19              libconfig9      libfmt9
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 637
```

sudo masscan 172.217.167.46 -p443



```
┌──(devalla㉿jwala)-[~]
└─$ sudo masscan 172.217.167.46 -p443
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-04-01 16:49:35 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [1 port/host]
```

Zmap: Another fast port scanner



```
┌──(devalla㉿jwala)-[~]
└─$ sudo apt install zmap
The following packages were automatically installed and are no
  firebird3.0-common      libc++abi1-19   libdirectfb-1.7-7t64
  firebird3.0-common-doc  libcapstone4    libegl-dev
  libbfio1                libconfig++9v5  libflac12t64
  libc++1-19              libconfig9      libfmt9
Use 'sudo apt autoremove' to remove them.

Installing:
  zmap

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 637
  Download size: 102 kB
  Space needed: 372 kB / 51.1 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 zmap am
Fetched 102 kB in 1s (76.8 kB/s)
Selecting previously unselected package zmap.
(Reading database ... 456902 files and directories currently in
Preparing to unpack .../zmap_2.1.1-2.1+b1_amd64.deb ...
Unpacking zmap (2.1.1-2.1+b1) ...
Setting up zmap (2.1.1-2.1+b1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

- **OpenVAS: For vulnerability scanning.**

OpenVAS and Nmap are both powerful tools used in the field of cybersecurity, particularly for vulnerability scanning and network mapping. However, they serve different primary purposes and have distinct features. Here's a comparison to help understand their roles:

OpenVAS

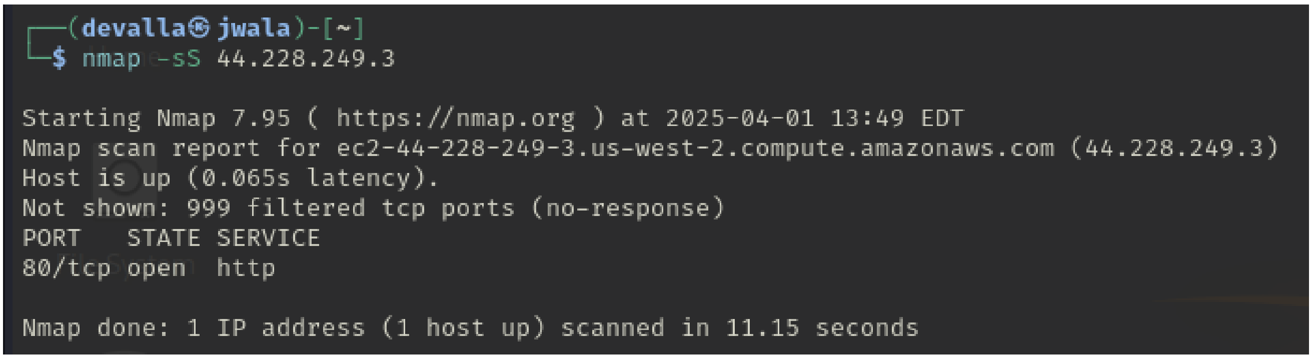
Primary Purpose: Vulnerability Scanning

- **Functionality:** OpenVAS is designed to scan networks for known vulnerabilities. It identifies security issues by comparing the target system against a database of known vulnerabilities.
- **Features:**
  - Extensive vulnerability database.
  - Detailed reporting on identified vulnerabilities.
  - Risk assessment and prioritization.
  - Integration with other security tools.
- **Use Case:** Ideal for comprehensive vulnerability assessments and regular security audits. It helps organizations identify and mitigate potential security risks.

10. Perform 5 more active scans using nmap and record what you had analyzed from it

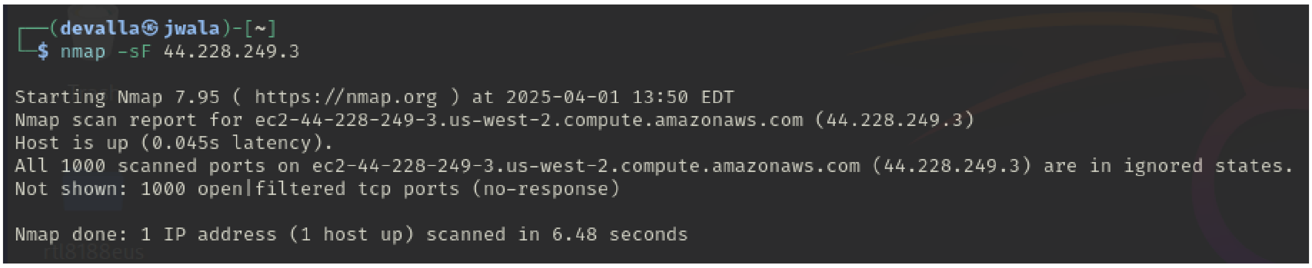
Perform five more active scans using Nmap and record your analysis. Here are some scan types you can try:

1. SYN Scan:
nmap -sS 44.228.249.3



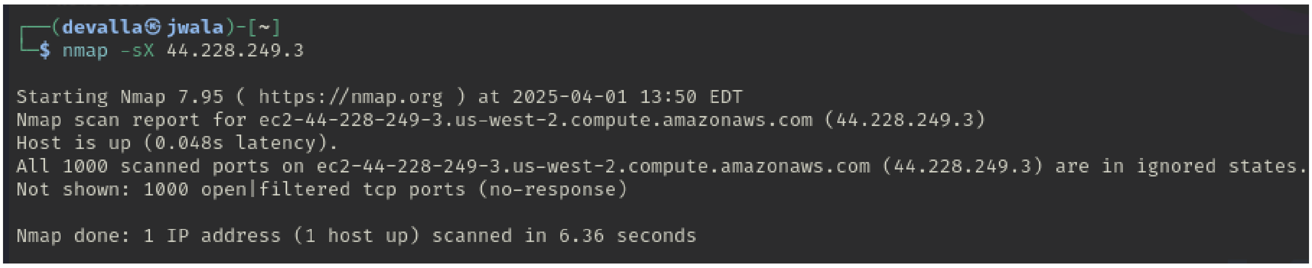
```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sS 44.228.249.3

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 13:49 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.065s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```

2. FIN Scan:
nmap -sF 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sF 44.228.249.3

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 13:50 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.045s 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 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
```

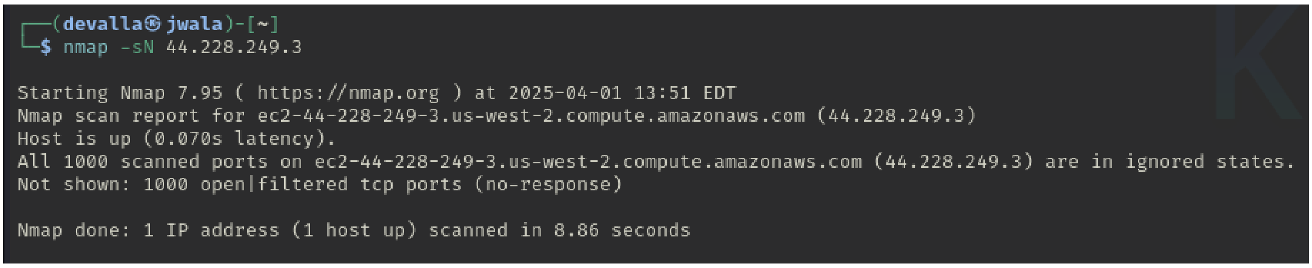
3. Xmas Scan:
nmap -sX 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sX 44.228.249.3

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 13:50 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.048s 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 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 6.36 seconds
```

4. Null Scan:

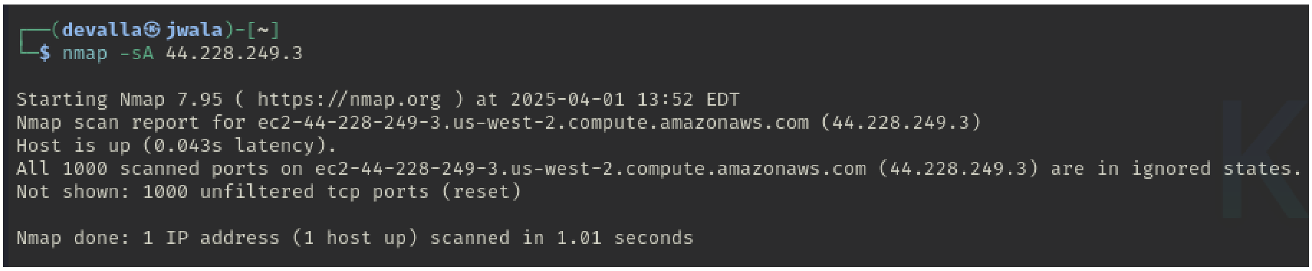
nmap -sN 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sN 44.228.249.3

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 13:51 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.070s 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 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 8.86 seconds
```

5. Ack Scan:

nmap -sA 44.228.249.3



```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sA 44.228.249.3

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-01 13:52 EDT
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.043s 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 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

THANK YOU!