Name:Ramya Ajay

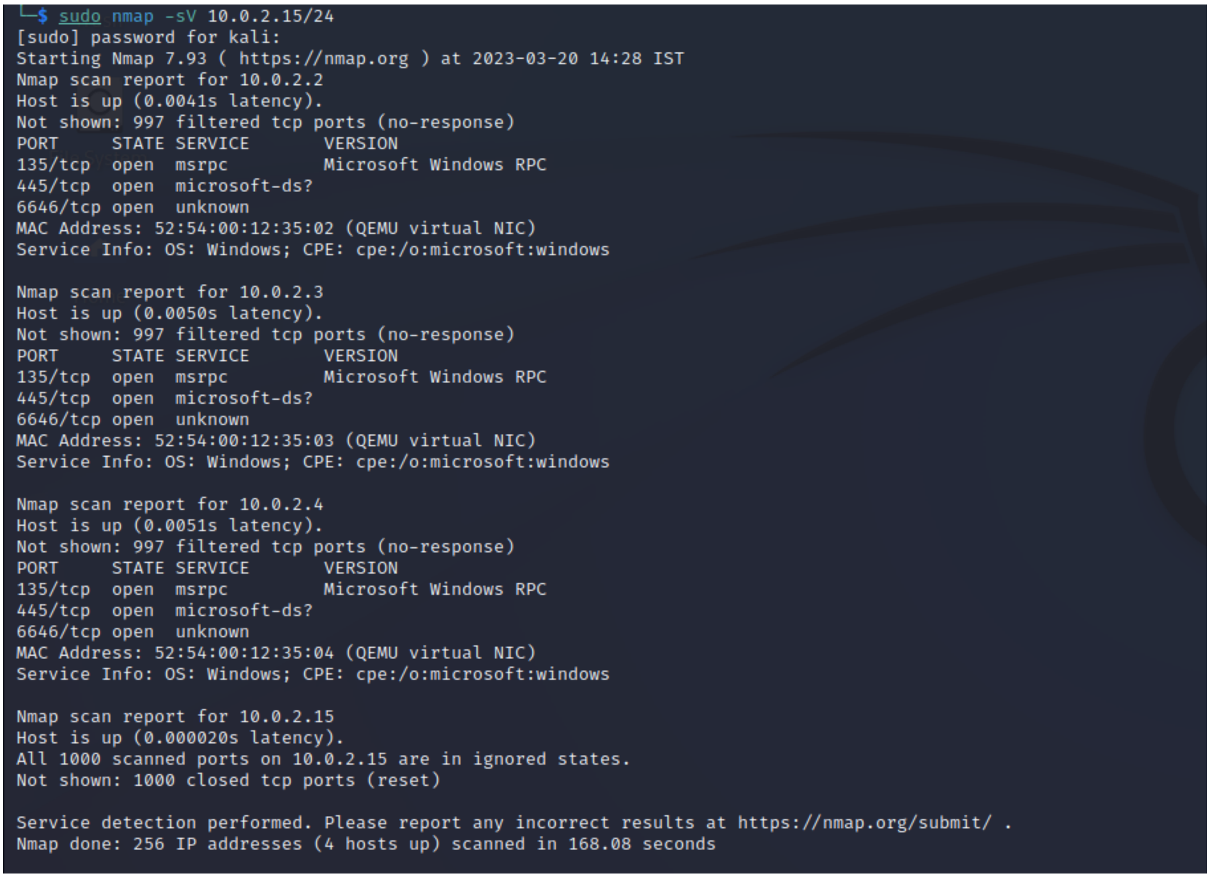
Roll No:CB.EN.P2CYS22004 Lab 2 Assignment Date :20.3.2023

Use the tool NMAP [Command line only] to perform the below task.

a) Explain the subnet and use the NMAP Command to scan the services for the whole subnet.

A subnet is a portion of a network that has been partitioned into smaller networks, each with its own unique IP address range. This is done to improve network performance, security, and manageability. Subnetting allows network administrators to divide a large network into smaller subnetworks, which can be used to group devices that have similar functions or security requirements.

Example - nmap -sV 10.0.2.15/24



```
└─$ sudo nmap -sV 10.0.2.15/24
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 14:28 IST
Nmap scan report for 10.0.2.2
Host is up (0.0041s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.3
Host is up (0.0050s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.4
Host is up (0.0051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
445/tcp  open  microsoft-ds?
6646/tcp open  unknown
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.15
Host is up (0.000020s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 168.08 seconds
```

b) What is a firewall and mention its types. Use the NMAP command to detect that a firewall protects the host.

Firewall

- A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on a set of predefined security rules. Its primary purpose is to protect networks and devices from unauthorized access, attacks, and malicious activity.
- Firewalls can be implemented as software, hardware, or a combination of both. They work by examining the packets of network traffic and comparing them against the set of rules or policies defined by the administrator.
- If a packet matches a rule, it is allowed to pass through the firewall. If it doesn't match any rule, it is either dropped or sent to a different location for further analysis

Types

- Packet filtering firewall
- Stateful inspection firewall
- Application-level gateway firewall
- Next-generation firewall
- Host-based firewall

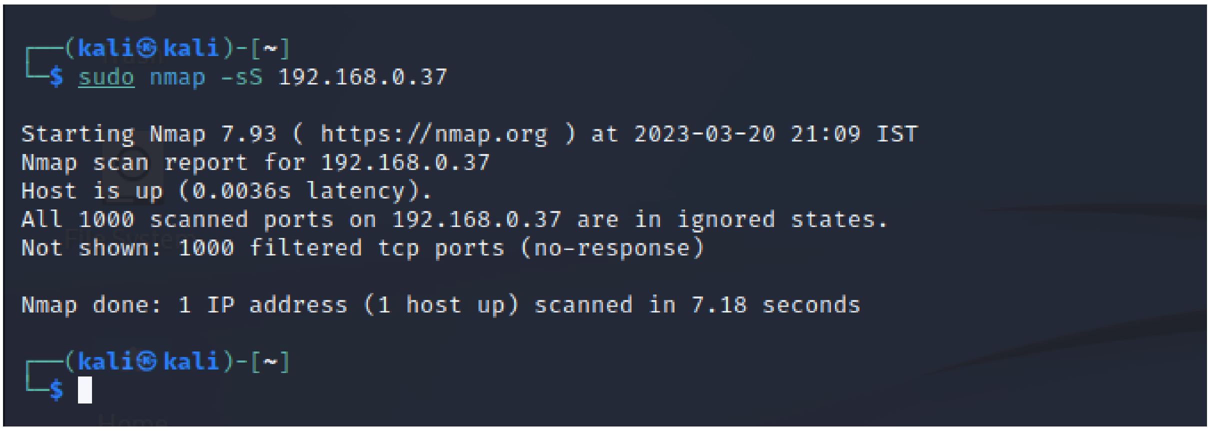
nmap command to identify a firewall -

To identify a firewall we can use the Standard SYN Scan
Reason : The RST packet makes closed ports easy for Nmap to recognize. Filtering devices such as firewalls, on the other hand, tend to drop packets destined for disallowed ports. In some cases they send ICMP error messages (usually port unreachable) instead. Because dropped packets and ICMP errors are easily distinguishable > from RST packets, Nmap can reliably detect filtered TCP ports from open or closed ones, and it does so automatically.

Command - nmap -sS -p- <ip>
If a port is filtered by a firewall, Nmap will not be able to determine if it is open or closed, but will instead report it as "filtered"

where,

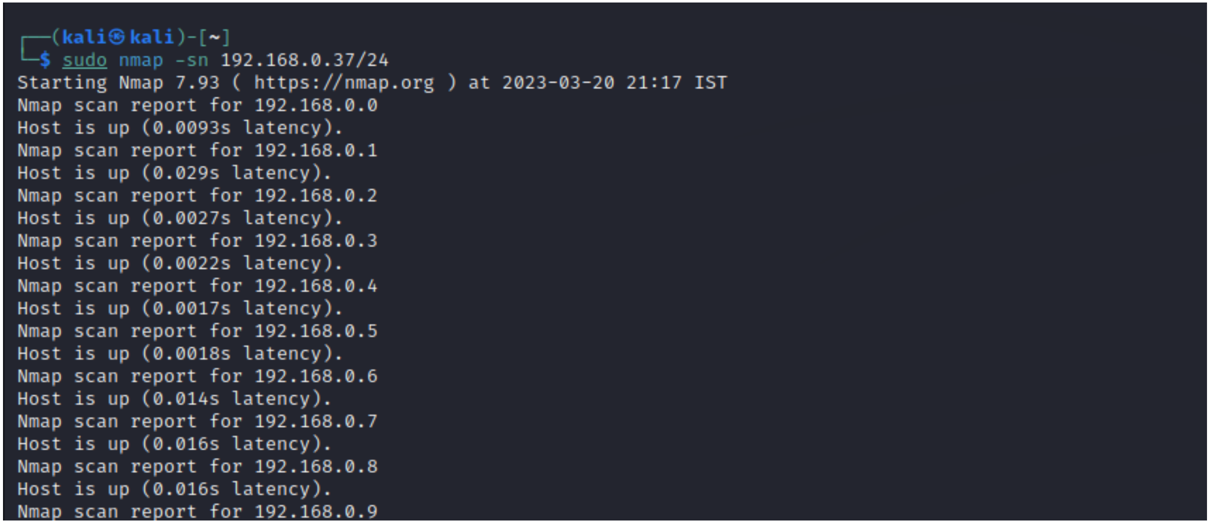
-sS - SYN scan
-p- - all ports



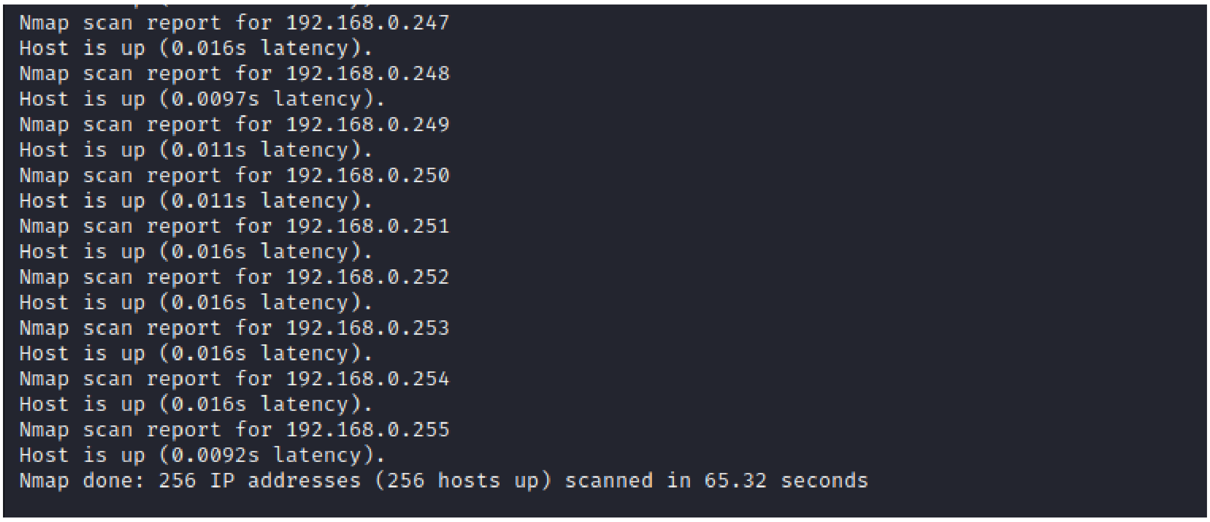
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.0.37

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 21:09 IST
Nmap scan report for 192.168.0.37
Host is up (0.0036s latency).
All 1000 scanned ports on 192.168.0.37 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

c) Use the NMAP command to scan a network and determine which devices are up and running.

Command - nmap -sn <ip>/<CIDR>



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.0.37/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 21:17 IST
Nmap scan report for 192.168.0.0
Host is up (0.0093s latency).
Nmap scan report for 192.168.0.1
Host is up (0.029s latency).
Nmap scan report for 192.168.0.2
Host is up (0.0027s latency).
Nmap scan report for 192.168.0.3
Host is up (0.0022s latency).
Nmap scan report for 192.168.0.4
Host is up (0.0017s latency).
Nmap scan report for 192.168.0.5
Host is up (0.0018s latency).
Nmap scan report for 192.168.0.6
Host is up (0.014s latency).
Nmap scan report for 192.168.0.7
Host is up (0.016s latency).
Nmap scan report for 192.168.0.8
Host is up (0.016s latency).
Nmap scan report for 192.168.0.9
```



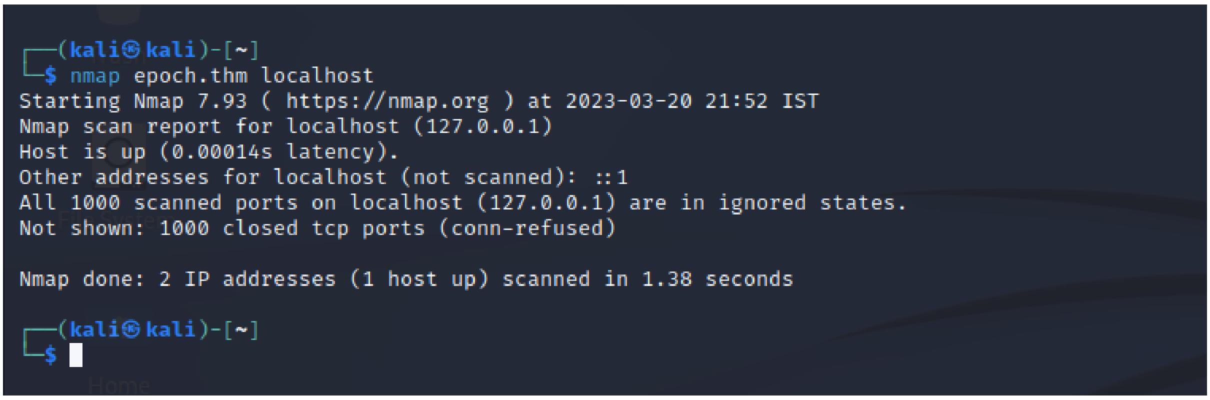
```
Nmap scan report for 192.168.0.247
Host is up (0.016s latency).
Nmap scan report for 192.168.0.248
Host is up (0.0097s latency).
Nmap scan report for 192.168.0.249
Host is up (0.011s latency).
Nmap scan report for 192.168.0.250
Host is up (0.011s latency).
Nmap scan report for 192.168.0.251
Host is up (0.016s latency).
Nmap scan report for 192.168.0.252
Host is up (0.016s latency).
Nmap scan report for 192.168.0.253
Host is up (0.016s latency).
Nmap scan report for 192.168.0.254
Host is up (0.016s latency).
Nmap scan report for 192.168.0.255
Host is up (0.0092s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 65.32 seconds
```

d) What are vertical and horizontal scanning?

- Vertical scanning, also known as **service scanning**, involves **scanning a single host for all the open ports and services** that are running on it. This approach allows for a detailed analysis of the individual host, including the versions of services running, operating system, and other relevant information.
- Horizontal scanning, also known as **port scanning**, involves **scanning multiple hosts for a specific open port or set of ports**. This approach allows for a quick overview of the network or hosts that may have a specific service or vulnerability present.

e) Use the NMAP command to scan multiple hosts. [HINT: Add hosts into a file and scan it].

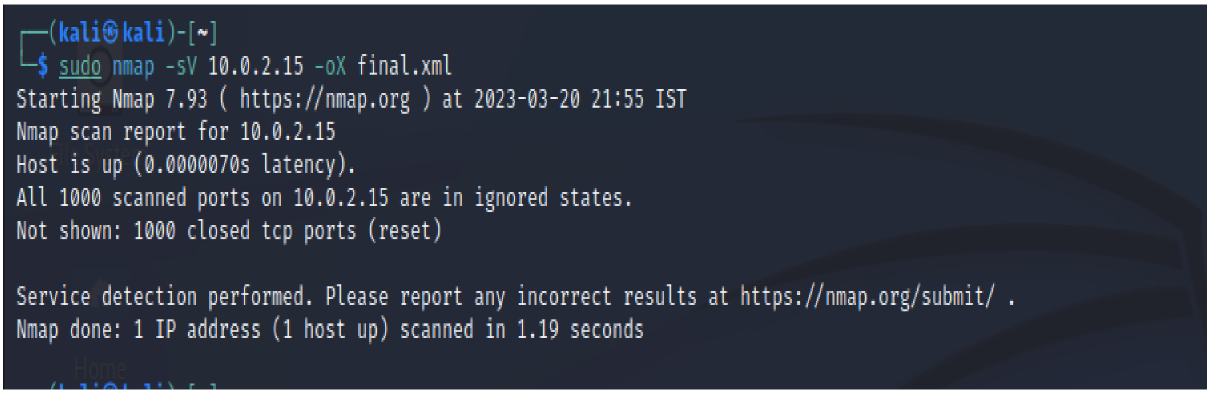
Add the ip address to /etc/hosts file and run the nmap command



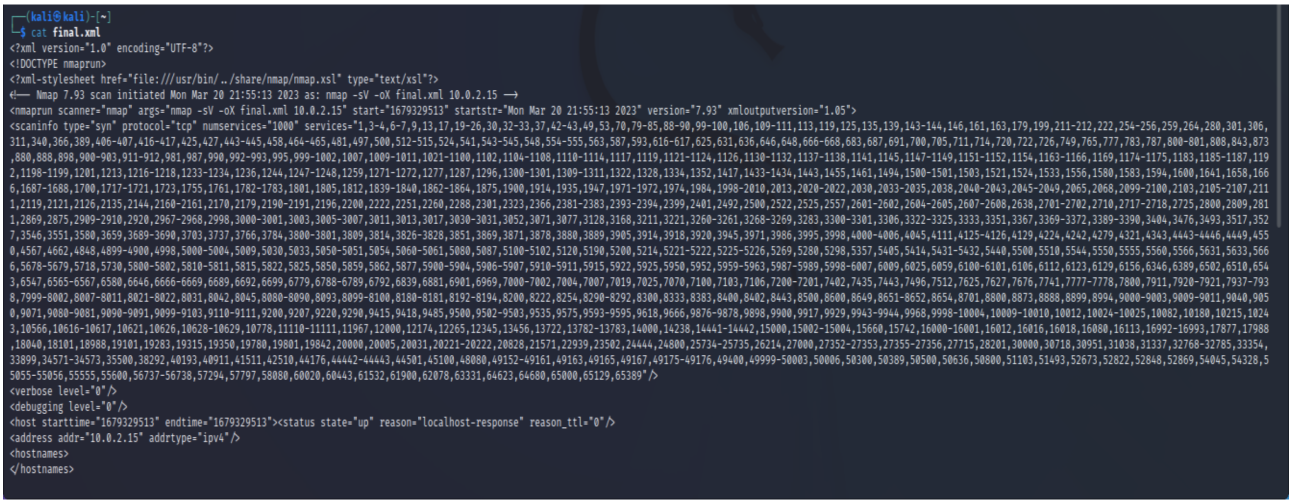
```
┌──(kali㉿kali)-[~]
└─$ nmap epoch.thm localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 21:52 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00014s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 2 IP addresses (1 host up) scanned in 1.38 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

f) Use NMAP commands to export the output in XML format.

We use the -oX flag.



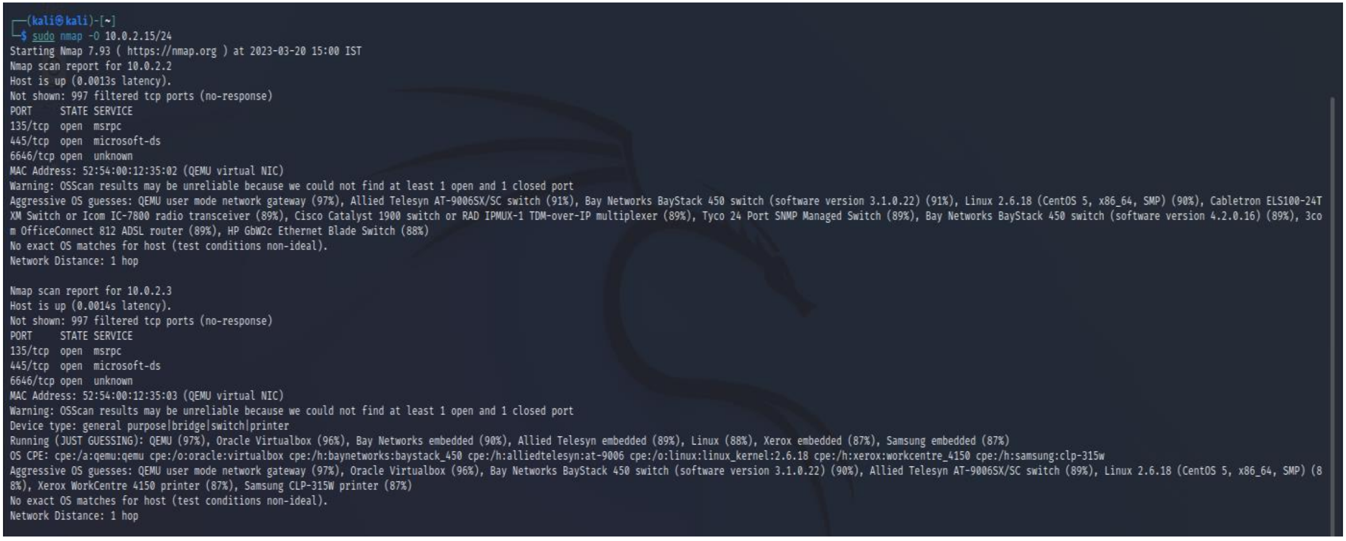
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.0.2.15 -oX final.xml
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 21:55 IST
Nmap scan report for 10.0.2.15
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ cat final.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.93 scan initiated Mon Mar 20 21:55:13 2023 as: nmap -sV -oX final.xml 10.0.2.15 -->
<nmaprun scanner="nmap" args="nmap -sV -oX final.xml 10.0.2.15" start="1679329513" startstr="Mon Mar 20 21:55:13 2023" version="7.93" xmloutputversion="1.05">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,
311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873
,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,119
2,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,166
6,1687-1688,1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,211
1,2119,2121,2126,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,281
1,2869,2875,2909-2910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,352
7,3546,3551,3580,3659,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,455
0,4567,4662,4848,4899-4900,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,566
6,5678-5679,5718,5730,5800-5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,654
3,6547,6565-6567,6580,6646,6666-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-793
8,7999-8002,8007-8011,8021-8022,8031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,905
0,9071,9080-9081,9090-9091,9099-9103,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,1024
3,10566,10616-10617,10621,10626,10628-10629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988
,18040,18101,18988,19101,19283,19315,19350,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,
33899,34571-34573,35500,38292,40193,40911,41511,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,5
5055-55056,55555,55600,56737-56738,57294,57797,58080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1679329513" endtime="1679329513"><status state="up" reason="localhost-response" reason_ttl="0"/>
<address addr="10.0.2.15" addrtype="ipv4"/>
<hostnames>
</hostnames>
```

g) Use the NMAP command to get OS information about a host.

To find the OS information about the host, we use the -O flag .



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.0.2.15/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 15:00 IST
Nmap scan report for 10.0.2.2
Host is up (0.0013s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
6646/tcp open  unknown
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: QEMU user mode network gateway (97%), Allied Telesyn AT-9006SX/SC switch (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (91%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (90%), Cabletron ELS100-24T
XM Switch or Icom IC-7800 radio transceiver (89%), Cisco Catalyst 1900 switch or RAD IPMUX-1 TDM-over-IP multiplexer (89%), Tyco 24 Port SNMP Managed Switch (89%), Bay Networks BayStack 450 switch (software version 4.2.0.16) (89%), 3co
m OfficeConnect 812 ADSL router (89%), HP GbW2c Ethernet Blade Switch (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.3
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
6646/tcp open  unknown
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|bridge|switch|printer
Running (JUST GUESSING): QEMU (97%), Oracle Virtualbox (96%), Bay Networks embedded (90%), Allied Telesyn embedded (89%), Linux (88%), Xerox embedded (87%), Samsung embedded (87%)
OS CPE: cpe:/a:qemu:qemu cpe:/o:oracle:virtualbox cpe:/h:baynetworks:baystack_450 cpe:/h:alliedtelesyn:at-9006 cpe:/o:linux:linux_kernel:2.6.18 cpe:/h:xerox:workcentre_4150 cpe:/h:samsung:clp-315w
Aggressive OS guesses: QEMU user mode network gateway (97%), Oracle Virtualbox (96%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (90%), Allied Telesyn AT-9006SX/SC switch (89%), Linux 2.6.18 (CentOS 5, x86_64, SMP) (8
8%), Xerox WorkCentre 4150 printer (87%), Samsung CLP-315W printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

h) Explain ping sweeping and Perform ping sweeping using Nmap

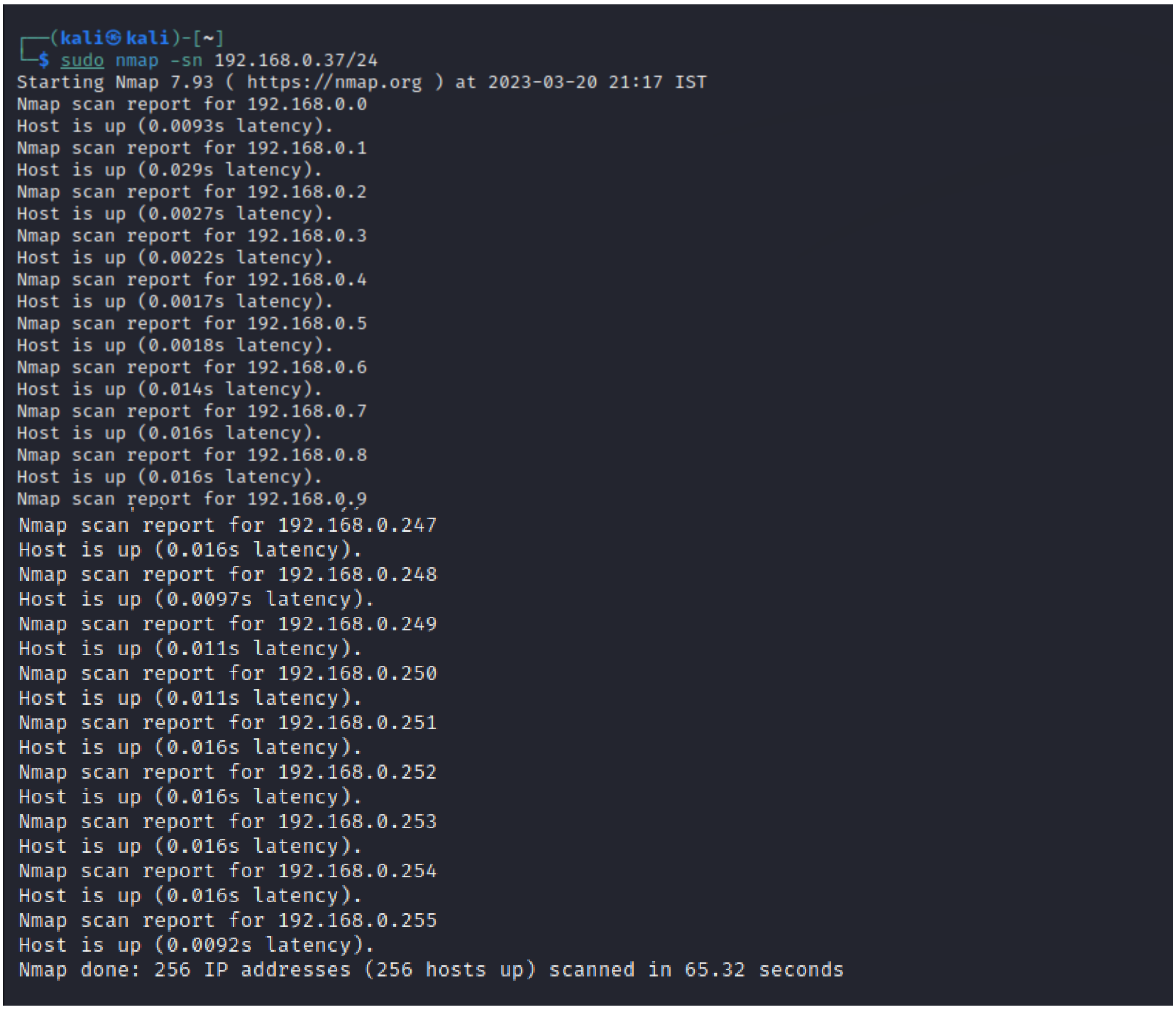
Ping Sweep

Ping sweeping is a network reconnaissance technique used to determine which IP addresses are alive and responsive on a network. It involves sending a series of ICMP echo request messages, also known as pings, to a range of IP addresses, usually in a sequential order, to identify which ones are available and can be reached.

Ping sweeping is often used by network administrators to identify active hosts on a network and to map the network

Nmap command to perform ping sweep - nmap -sn <network address>/<CIDR>.
where,

-sn - allows to perform a ping scan on the target:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 192.168.0.37/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 21:17 IST
Nmap scan report for 192.168.0.0
Host is up (0.0093s latency).
Nmap scan report for 192.168.0.1
Host is up (0.029s latency).
Nmap scan report for 192.168.0.2
Host is up (0.0027s latency).
Nmap scan report for 192.168.0.3
Host is up (0.0022s latency).
Nmap scan report for 192.168.0.4
Host is up (0.0017s latency).
Nmap scan report for 192.168.0.5
Host is up (0.0018s latency).
Nmap scan report for 192.168.0.6
Host is up (0.014s latency).
Nmap scan report for 192.168.0.7
Host is up (0.016s latency).
Nmap scan report for 192.168.0.8
Host is up (0.016s latency).
Nmap scan report for 192.168.0.9
Nmap scan report for 192.168.0.247
Host is up (0.016s latency).
Nmap scan report for 192.168.0.248
Host is up (0.0097s latency).
Nmap scan report for 192.168.0.249
Host is up (0.011s latency).
Nmap scan report for 192.168.0.250
Host is up (0.011s latency).
Nmap scan report for 192.168.0.251
Host is up (0.016s latency).
Nmap scan report for 192.168.0.252
Host is up (0.016s latency).
Nmap scan report for 192.168.0.253
Host is up (0.016s latency).
Nmap scan report for 192.168.0.254
Host is up (0.016s latency).
Nmap scan report for 192.168.0.255
Host is up (0.0092s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 65.32 seconds
```

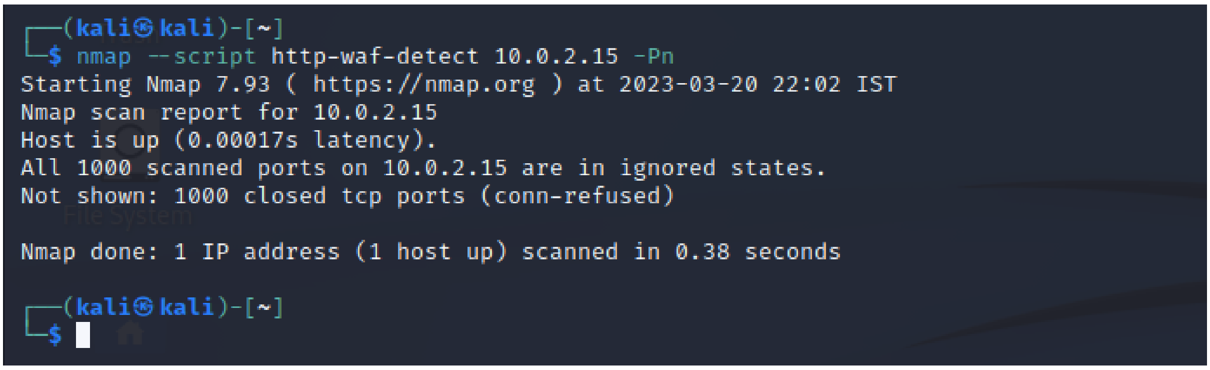
Try these below questions after completing the above commands.

1. What is a web application firewall? How do you use Nmap to detect a WAF? Perform WAF fingerprint detection using NMAP.

- A **web application firewall (WAF)** is a firewall that monitors, filters and blocks data packets as they travel to and from a website or web application.

- A WAF can be either network-based, host-based or cloud-based and is often deployed through a reverse proxy and placed in front of one or more websites or applications.

- Running as a network appliance, server plugin or cloud service, the WAF inspects each packet and uses a rule base to analyze Layer 7 web application logic and filter out potentially harmful traffic that can facilitate web exploits.

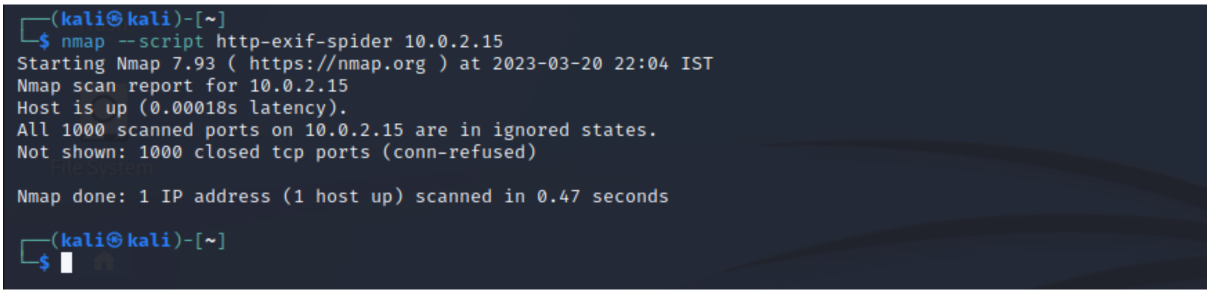


```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-waf-detect 10.0.2.15 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 22:02 IST
Nmap scan report for 10.0.2.15
Host is up (0.00017s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

2. What is EXIF data? Try to find EXIF data of images on a website using NMAP NSE

EXIF DATA

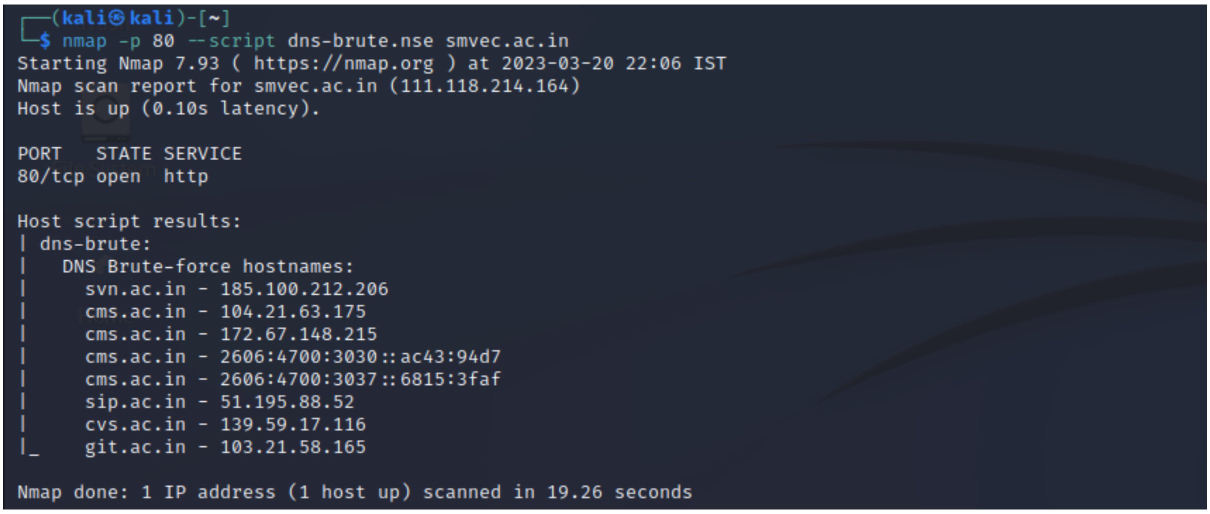
- It is a metadata that is embedded within image files, such as JPEGs, TIFFs, and RAW files. This data includes information about the camera settings used to take the picture, as well as information about the date, time, and location of the image
- Exif data can also include information about the camera's make and model, the lens used, and the exposure settings, such as shutter speed, aperture, and ISO.



```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-exif-spider 10.0.2.15
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 22:04 IST
Nmap scan report for 10.0.2.15
Host is up (0.00018s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

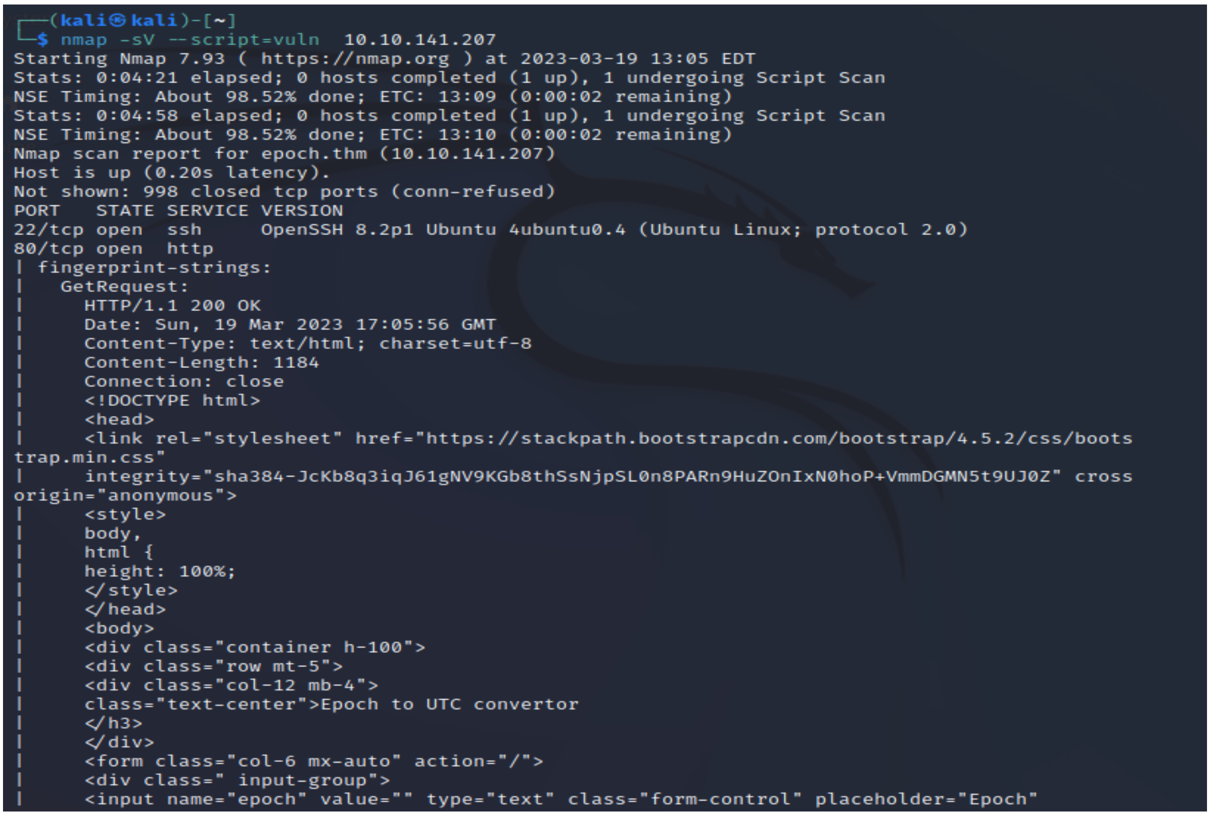
3. Use NMAP NSE to find all subdomains of the website.

All the nse scripts are located in /usr/share/nmap/scripts/
The dns-brute script built into Nmap is designed to enumerate subdomains and their corresponding server IP addresses.



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 --script dns-brute.nse smvec.ac.in
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-20 22:06 IST
Nmap scan report for smvec.ac.in (111.118.214.164)
Host is up (0.10s latency).

PORT   STATE SERVICE
80/tcp open  http

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     svn.ac.in - 185.100.212.206
|     cms.ac.in - 104.21.63.175
|     cms.ac.in - 172.67.148.215
|     cms.ac.in - 2606:4700:3030::ac43:94d7
|     cms.ac.in - 2606:4700:3037::6815:3faf
|     sip.ac.in - 51.195.88.52
|     cvs.ac.in - 139.59.17.116
|_    git.ac.in - 103.21.58.165

Nmap done: 1 IP address (1 host up) scanned in 19.26 seconds
```

4. Perform a vulnerability scan on the target host using NMAP NSE.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vuln  10.10.141.207
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-19 13:05 EDT
Stats: 0:04:21 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.52% done; ETC: 13:09 (0:00:02 remaining)
Stats: 0:04:58 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.52% done; ETC: 13:10 (0:00:02 remaining)
Nmap scan report for epoch.thm (10.10.141.207)
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Sun, 19 Mar 2023 17:05:56 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 1184
|     Connection: close
|     <!DOCTYPE html>
|     <head>
|     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/boots
trap.min.css"
|     integrity="sha384-JcKb8q3iqJ61gNV9KGb8thSsNjpSL0n8PARn9HuZOnIxN0hoP+VmmDGMN5t9UJ0Z" cross
origin="anonymous">
|     <style>
|     body,
|     html {
|     height: 100%;
|     </style>
|     </head>
|     <body>
|     <div class="container h-100">
|     <div class="row mt-5">
|     <div class="col-12 mb-4">
|     class="text-center">Epoch to UTC convertor
|     </h3>
|     </div>
|     <form class="col-6 mx-auto" action="/">
|     <div class=" input-group">
|     <input name="epoch" value="" type="text" class="form-control" placeholder="Epoch"
```