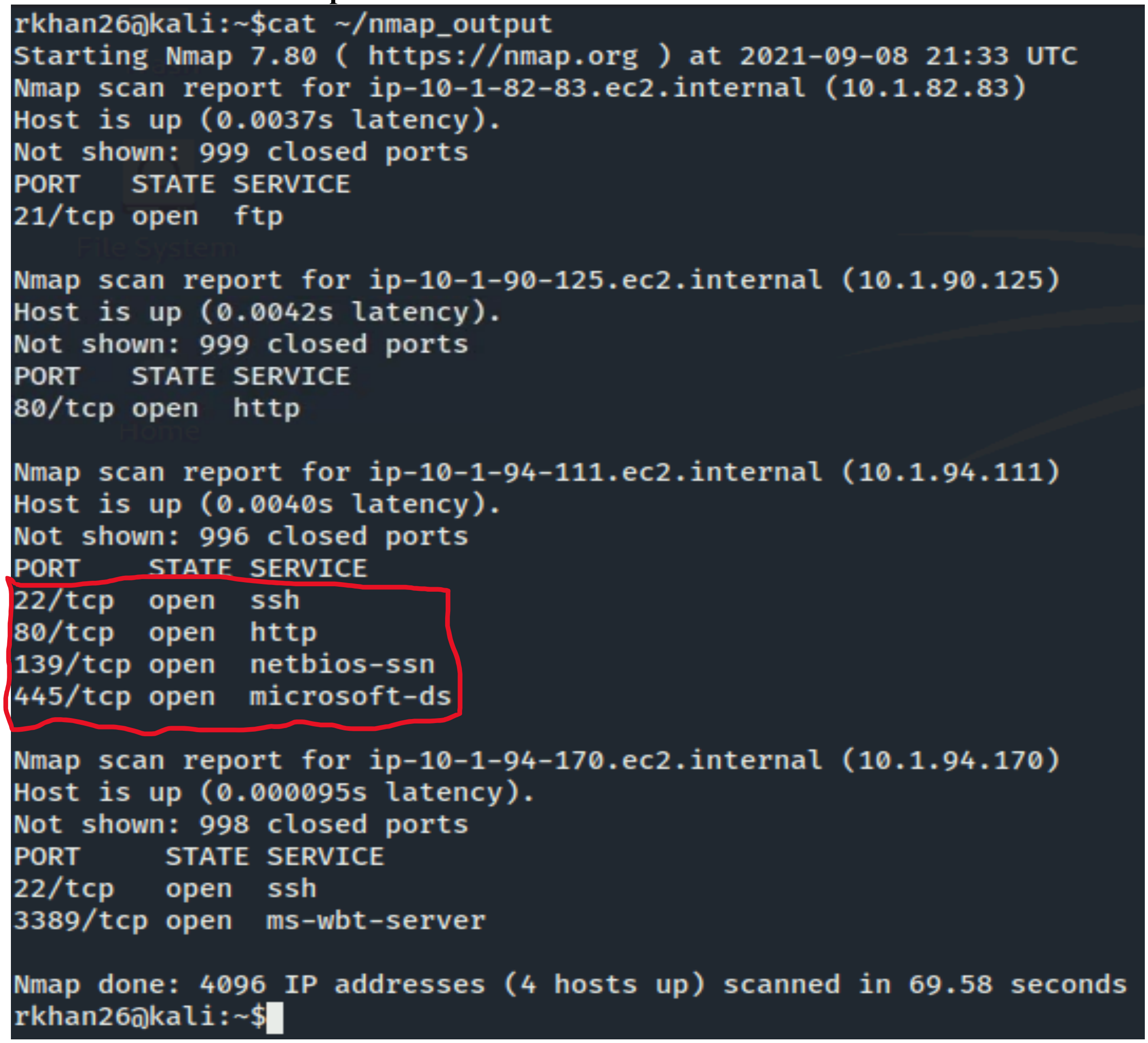
Roozah Khan
Laboratory Exercise 2-2 – Enumeration Lab Exercise

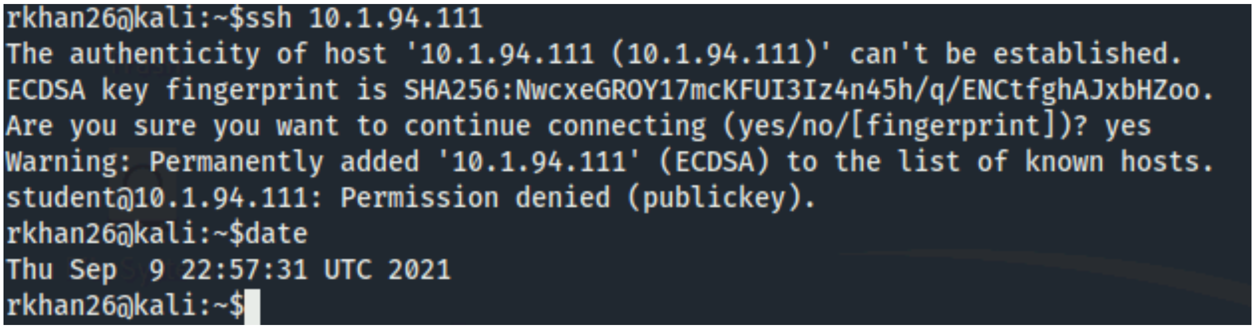
Task 2: Examine the nmap results from the Reconnaissance lab



```
rkhan26@kali:~$cat ~/nmap_output
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:33 UTC
Nmap scan report for ip-10-1-82-83.ec2.internal (10.1.82.83)
Host is up (0.0037s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-90-125.ec2.internal (10.1.90.125)
Host is up (0.0042s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http

Nmap scan report for ip-10-1-94-111.ec2.internal (10.1.94.111)
Host is up (0.0040s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for ip-10-1-94-170.ec2.internal (10.1.94.170)
Host is up (0.000095s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap done: 4096 IP addresses (4 hosts up) scanned in 69.58 seconds
rkhan26@kali:~$
```

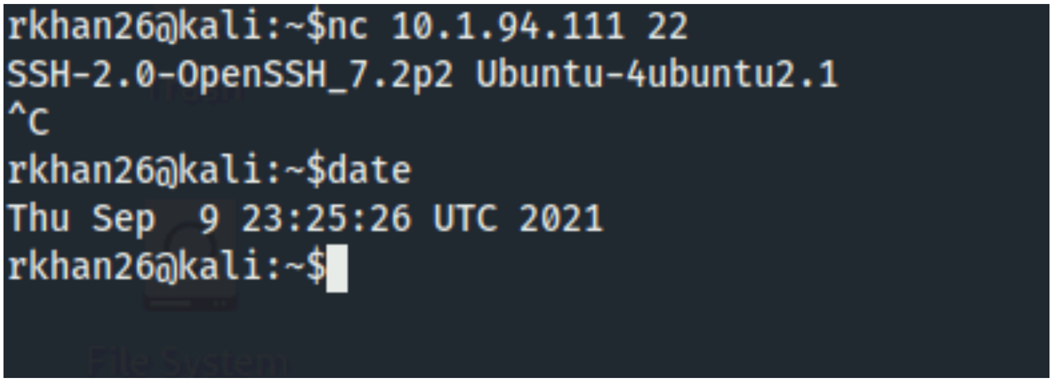
I used the cat command to view the contents of the nmap file and looked for specific host with the ports that are open circled in red.

Task 3: Enumerate port 22 SSH



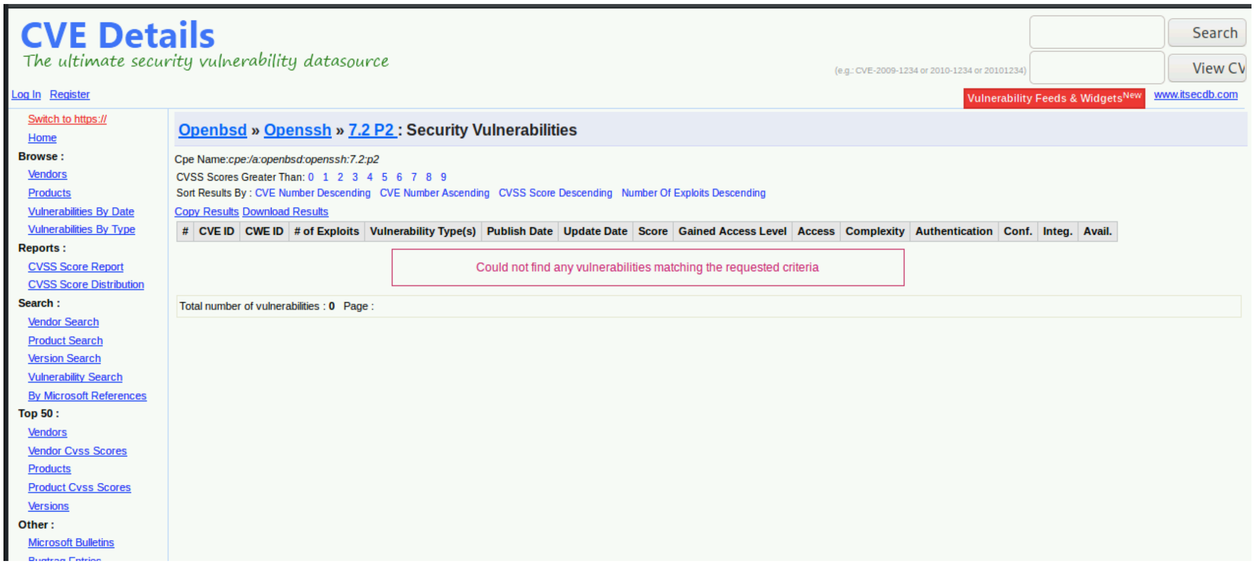
```
rkhan26@kali:~$ssh 10.1.94.111
The authenticity of host '10.1.94.111 (10.1.94.111)' can't be established.
ECDSA key fingerprint is SHA256:NwcxeGROY17mcKFUI3Iz4n45h/q/ENCtfghAJxbHZoo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.94.111' (ECDSA) to the list of known hosts.
student@10.1.94.111: Permission denied (publickey).
rkhan26@kali:~$date
Thu Sep  9 22:57:31 UTC 2021
rkhan26@kali:~$
```

I attempted to ssh to the host with the target IP address.



```
rkhan26@kali:~$nc 10.1.94.111 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1
^C
rkhan26@kali:~$date
Thu Sep  9 23:25:26 UTC 2021
rkhan26@kali:~$
```

I used the nc command to figure out the version of ssh server to see if vulnerabilities exist.



Openbsd » Openssh » 7.2 P2 : Security Vulnerabilities

Cpe Name:*cpe:/a:openbsd:openssh:7.2:p2*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

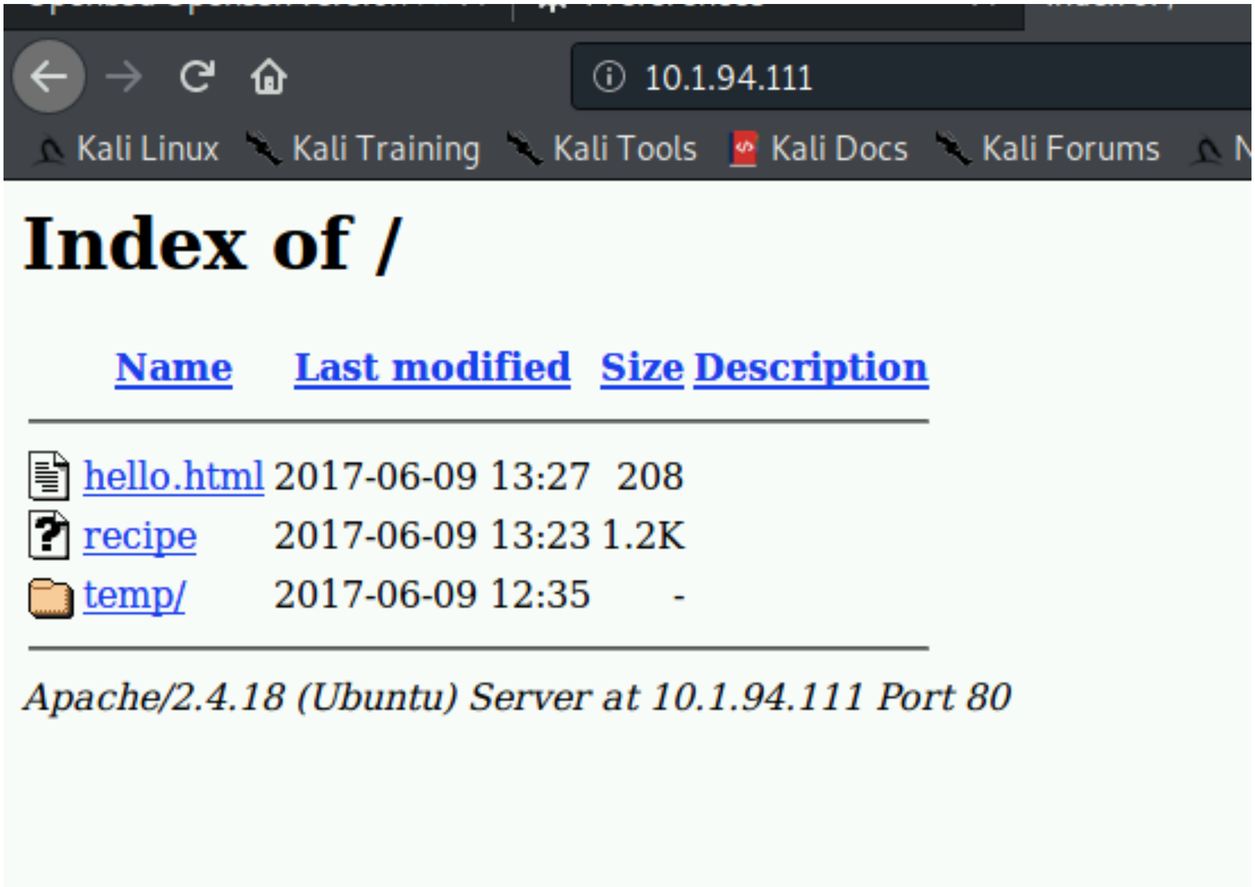
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.

Could not find any vulnerabilities matching the requested criteria

Total number of vulnerabilities : **0** Page :

I used the web browser to find OpenSSH 7.2p2 vulnerabilities on the CVE database. There were not any vulnerabilities listed.

Task 4: Enumerate port 80 HTTP



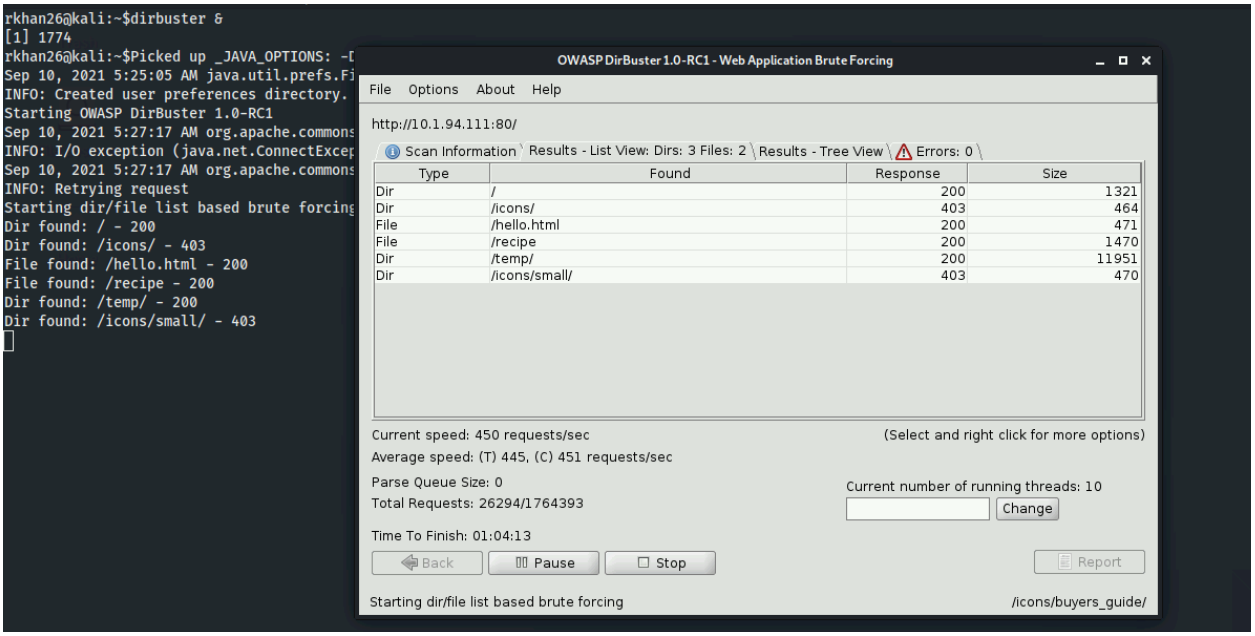
Index of /

Name	Last modified	Size	Description
hello.html	2017-06-09 13:27	208	
recipe	2017-06-09 13:23	1.2K	
temp/	2017-06-09 12:35	-	

Apache/2.4.18 (Ubuntu) Server at 10.1.94.111 Port 80

I opened the web browser preferences and changed the settings to “No proxy” and then typed the target IP address in the search bar to see the version number of the Apache web server.

Task 5: Web Server directory enumeration using Dirbuster



```
rkhan26@kali:~$dirbuster &
[1] 1774
rkhan26@kali:~$Picked up _JAVA_OPTIONS: -D
Sep 10, 2021 5:25:05 AM java.util.prefs.Fi
INFO: Created user preferences directory.
Starting OWASP DirBuster 1.0-RC1
Sep 10, 2021 5:27:17 AM org.apache.commons
INFO: I/O exception (java.net.ConnectExcep
Sep 10, 2021 5:27:17 AM org.apache.commons
INFO: Retrying request
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
File found: /hello.html - 200
File found: /recipe - 200
Dir found: /temp/ - 200
Dir found: /icons/small/ - 403
```

http://10.1.94.111:80/

Type	Found	Response	Size
Dir	/	200	1321
Dir	/icons/	403	464
File	/hello.html	200	471
File	/recipe	200	1470
Dir	/temp/	200	11951
Dir	/icons/small/	403	470

Current speed: 450 requests/sec

(Select and right click for more options)

Average speed: (T) 445, (C) 451 requests/sec

Parse Queue Size: 0

Current number of running threads: 10

Total Requests: 26294/1764393

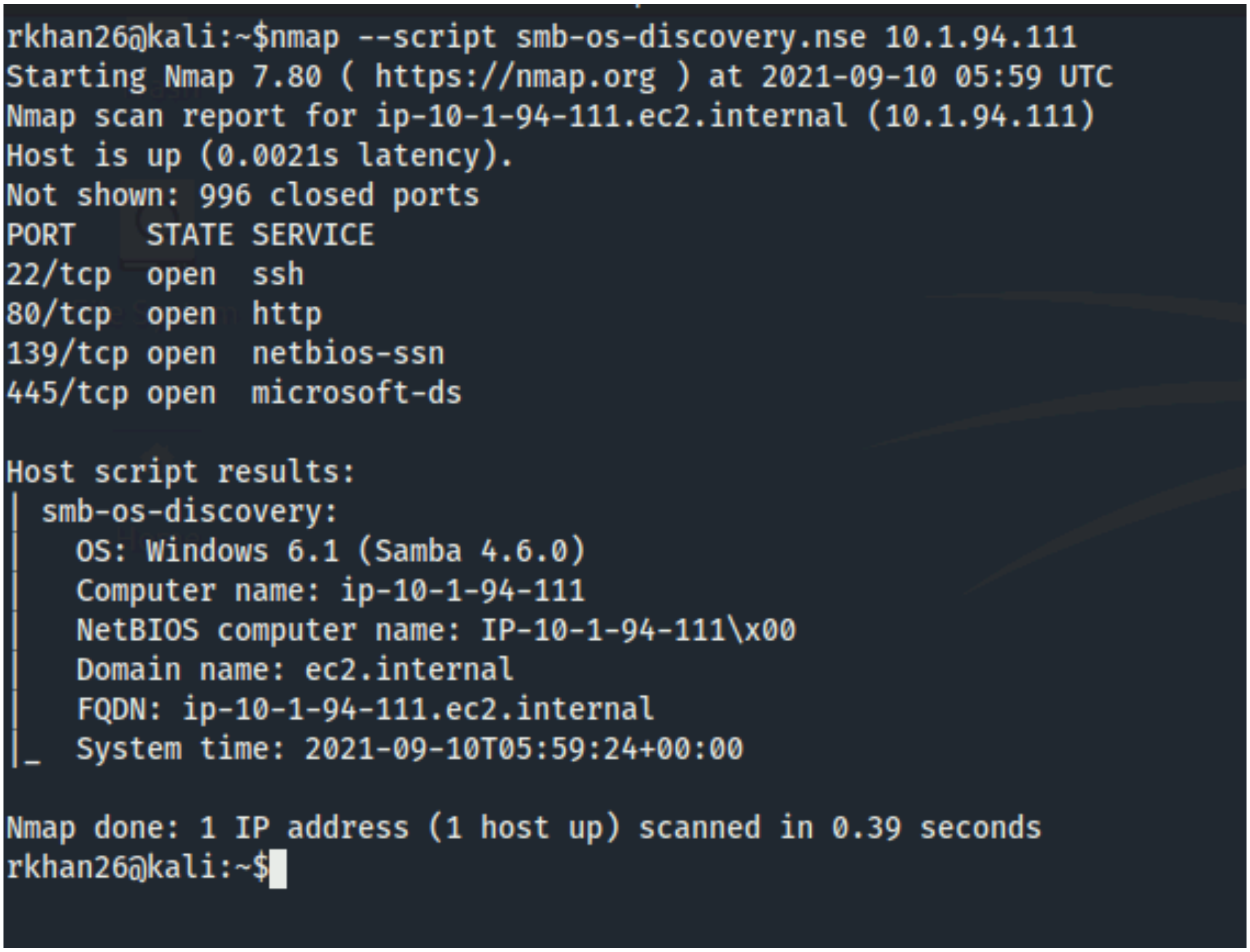
Time To Finish: 01:04:13

Starting dir/file list based brute forcing

/icons/buyers_guide/

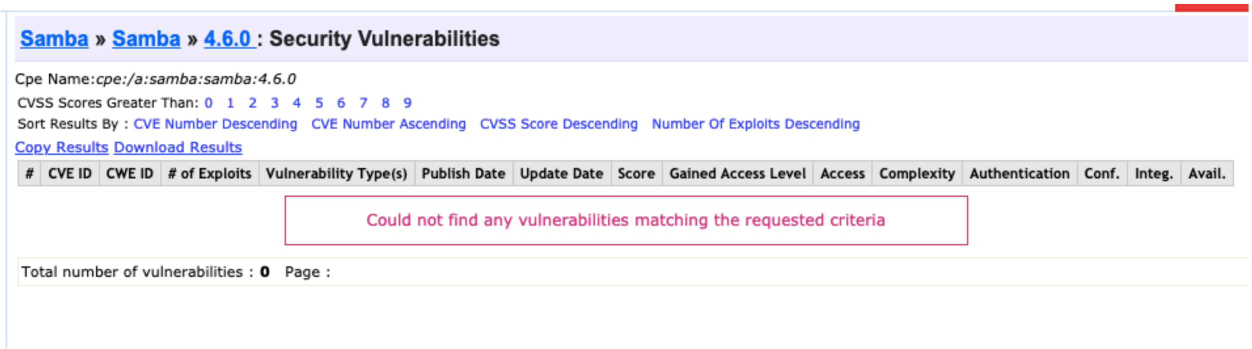
I ran the dirbuster & see it search various files and directories from the target IP address/web server.

Task 6: SMB port 445 enumeration using Nmap Scripting Engine (NSE)



```
rkhan26@kali:~$nmap --script smb-os-discovery.nse 10.1.94.111
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-10 05:59 UTC
Nmap scan report for ip-10-1-94-111.ec2.internal (10.1.94.111)
Host is up (0.0021s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.6.0)
|   Computer name: ip-10-1-94-111
|   NetBIOS computer name: IP-10-1-94-111\x00
|   Domain name: ec2.internal
|   FQDN: ip-10-1-94-111.ec2.internal
|_  System time: 2021-09-10T05:59:24+00:00

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
rkhan26@kali:~$
```

I used the nmap command to enumerate the SMB protocol to view the version number of Samba. I used a web browser to find any vulnerabilities with the 4.6.0 Samba version. I could not find any, so I just clicked on "Samba" and chose the same CVE number that is shown in the lab instructions. As you can see down below, there is one vulnerability that has the score of 10.



Samba » Samba » 4.6.0 : Security Vulnerabilities

Cpe Name:*cpe:/a:samba:samba:4.6.0*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

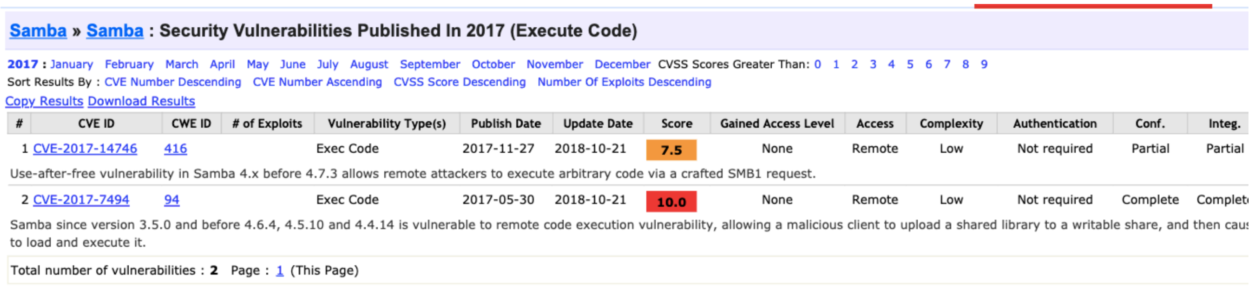
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.

Could not find any vulnerabilities matching the requested criteria

Total number of vulnerabilities : **0** Page :



Samba » Samba : Security Vulnerabilities Published In 2017 (Execute Code)

2017 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

<table>
<tr><th>#</th><th>CVE ID</th><th>CWE ID</th><th># of Exploits</th><th>Vulnerability Type(s)</th><th>Publish Date</th><th>Update Date</th><th>Score</th><th>Gained Access Level</th><th>Access</th><th>Complexity</th><th>Authentication</th><th>Conf.</th><th>Integ.</th></tr>
<tr><td>1</td><td>CVE-2017-14746</td><td>416</td><td></td><td>Exec Code</td><td>2017-11-27</td><td>2018-10-21</td><td>7.5</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Partial</td><td>Partial</td></tr>
<tr><td colspan="14">Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.</td></tr>
<tr><td>2</td><td>CVE-2017-7494</td><td>94</td><td></td><td>Exec Code</td><td>2017-05-30</td><td>2018-10-21</td><td>10.0</td><td>None</td><td>Remote</td><td>Low</td><td>Not required</td><td>Complete</td><td>Complet</td></tr>
<tr><td colspan="14">Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then caus to load and execute it.</td></tr>
</table>

Total number of vulnerabilities : **2** Page : 1 (This Page)