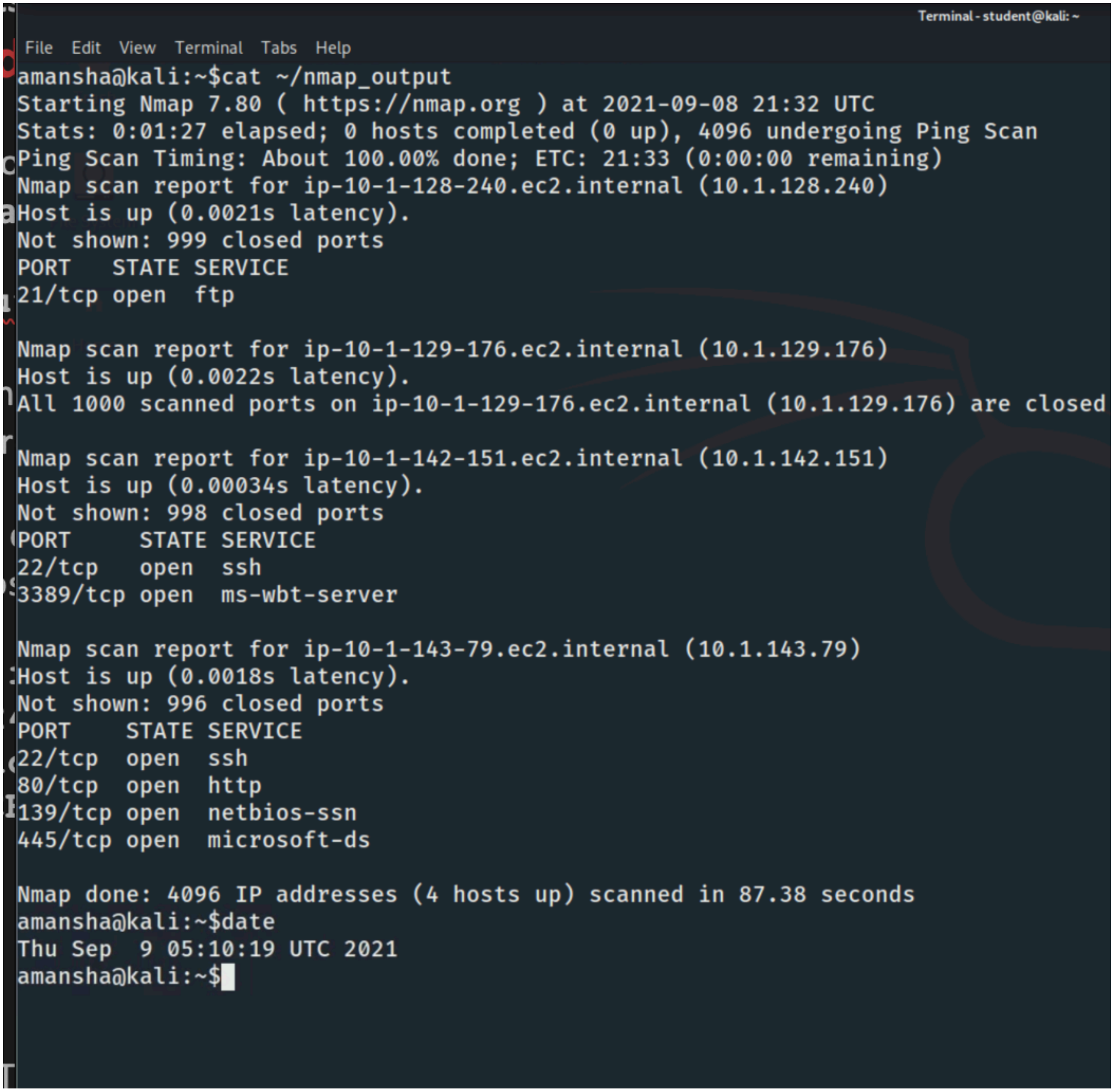
Amir Mansha
Lab 2-2
CYSE 425
Fall 2021

Task 2: Examine the nmap results from the Reconnaissance lab

Used the cat command to pull up the previously saved file.



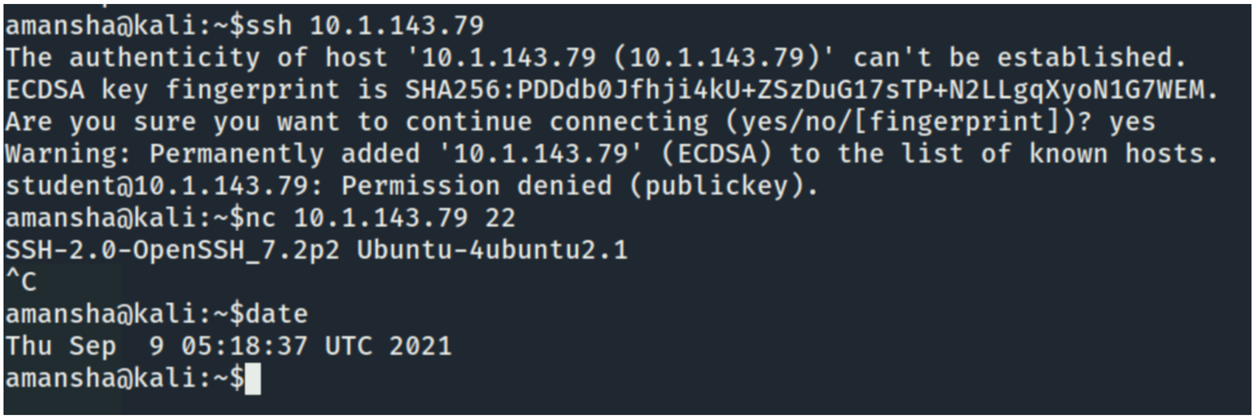
```
amansha@kali:~$cat ~/nmap_output
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-08 21:32 UTC
Stats: 0:01:27 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 21:33 (0:00:00 remaining)
Nmap scan report for ip-10-1-128-240.ec2.internal (10.1.128.240)
Host is up (0.0021s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp

Nmap scan report for ip-10-1-129-176.ec2.internal (10.1.129.176)
Host is up (0.0022s latency).
All 1000 scanned ports on ip-10-1-129-176.ec2.internal (10.1.129.176) are closed

Nmap scan report for ip-10-1-142-151.ec2.internal (10.1.142.151)
Host is up (0.00034s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server

Nmap scan report for ip-10-1-143-79.ec2.internal (10.1.143.79)
Host is up (0.0018s 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 done: 4096 IP addresses (4 hosts up) scanned in 87.38 seconds
amansha@kali:~$date
Thu Sep  9 05:10:19 UTC 2021
amansha@kali:~$
```

Task 3: Enumerate port 22 SSH

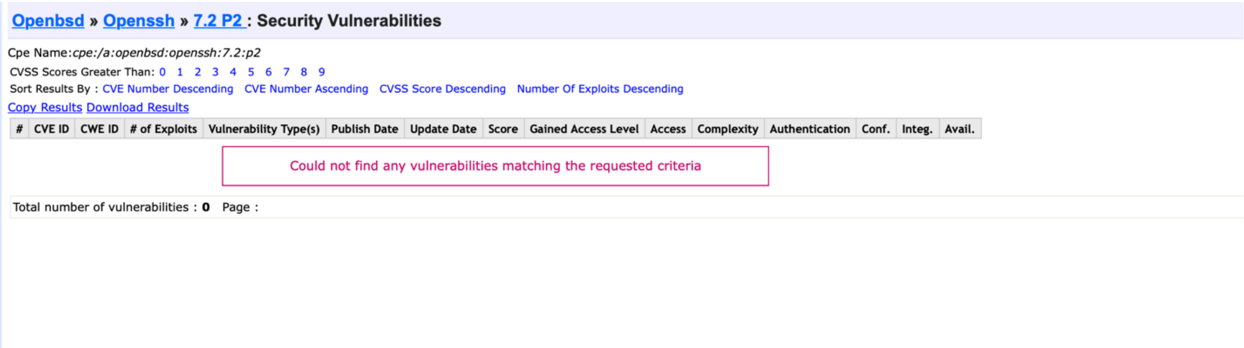
I SSH to the host and got the permission denied message. I then used “netcat” to see if there are any current vulnerabilities. When I used netcat I got a SSH version number in return. Searched that version

Amir Mansha
Lab 2-2
CYSE 425
Fall 2021

number on my web browser and the results showed there was no Vulneabilities.



```
amansha@kali:~$ssh 10.1.143.79
The authenticity of host '10.1.143.79 (10.1.143.79)' can't be established.
ECDSA key fingerprint is SHA256:PDDdb0Jfhji4kU+ZSzDuG17sTP+N2LLgqXyoN1G7WEM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.143.79' (ECDSA) to the list of known hosts.
student@10.1.143.79: Permission denied (publickey).
amansha@kali:~$nc 10.1.143.79 22
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1
^C
amansha@kali:~$date
Thu Sep  9 05:18:37 UTC 2021
amansha@kali:~$
```



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.

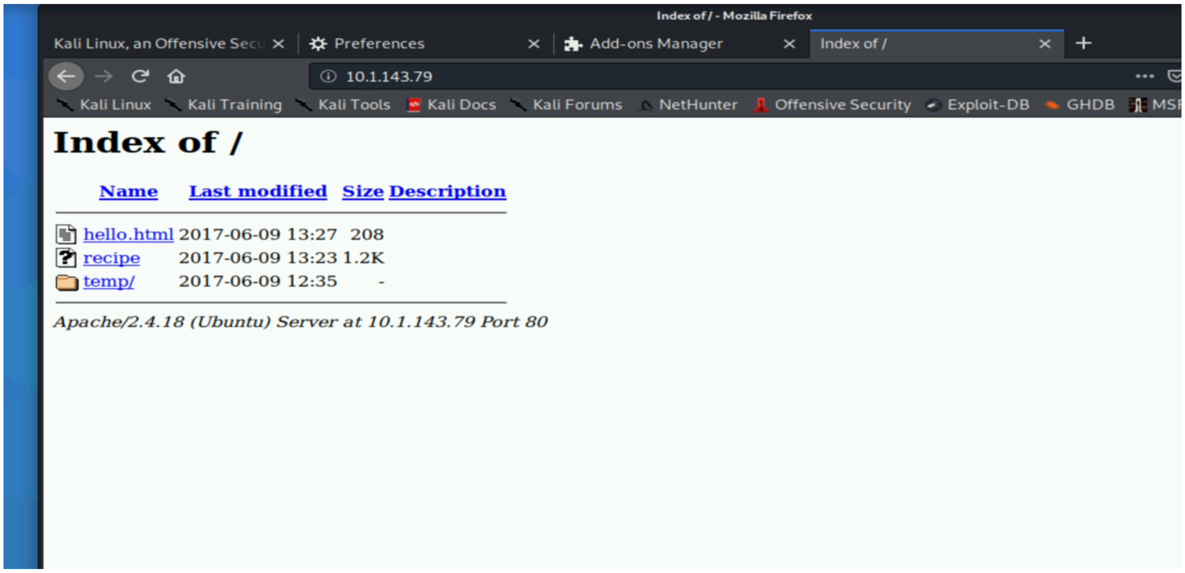
Could not find any vulnerabilities matching the requested criteria

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

Task 4: Enumerate port 80 HTTP

Amir Mansha
Lab 2-2
CYSE 425
Fall 2021

Used kali Linux to pull up a web browser, open its network settings to select the “no proxy” option and then typed in the target ID in the web browser and was presented with the home page down below



Index of /

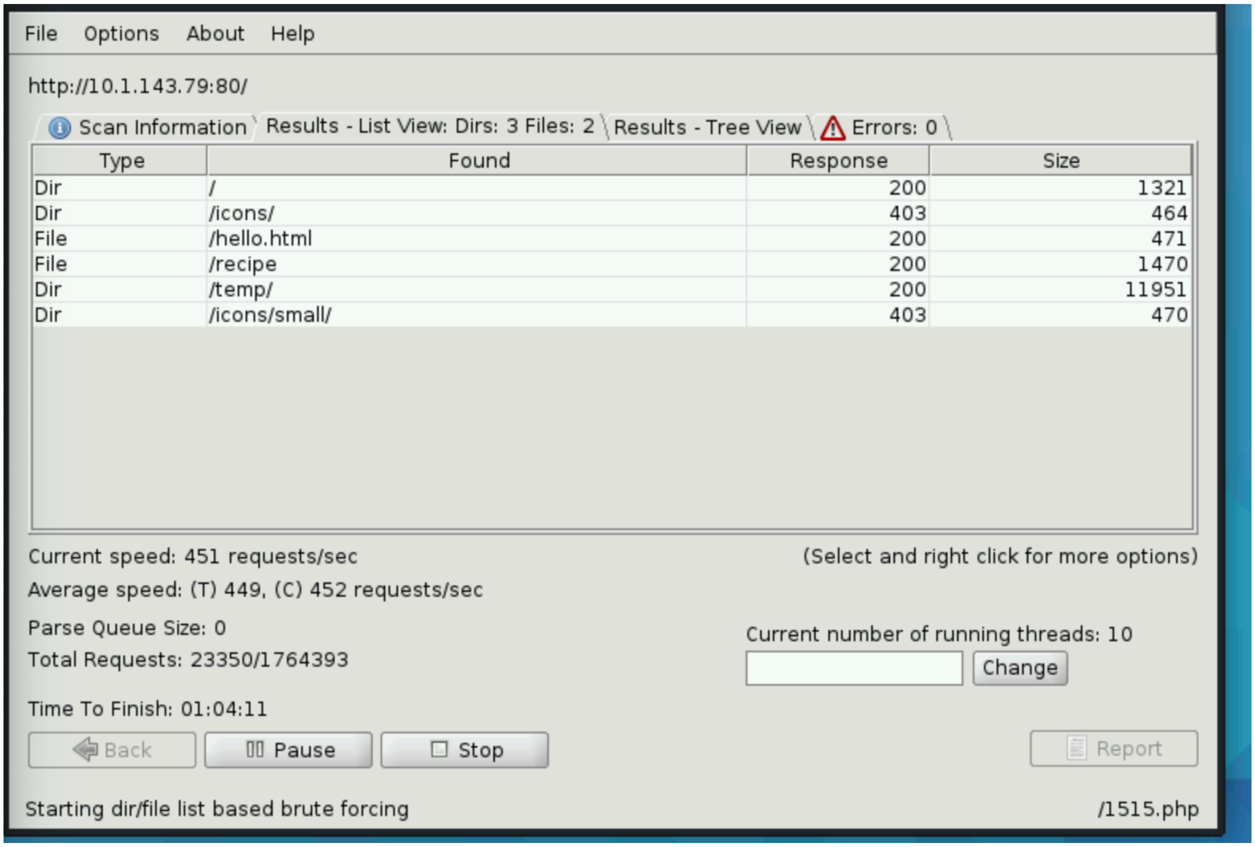
Name	Last modified	Size	Description
hello.html	2017-06-09 13:27	208	
recipe	2017-06-09 13:23	1.2K	
temp/	2017-06-09 12:35	-	

Apache/2.4.18 (Ubuntu) Server at 10.1.143.79 Port 80

Task 5: Web Server directory enumeration using Dirbuster

Opened dirbuster using terminal, after that I conducted a bruteforce search of files. Down below is the picture of the results

Amir Mansha
Lab 2-2
CYSE 425
Fall 2021



http://10.1.143.79:80/

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

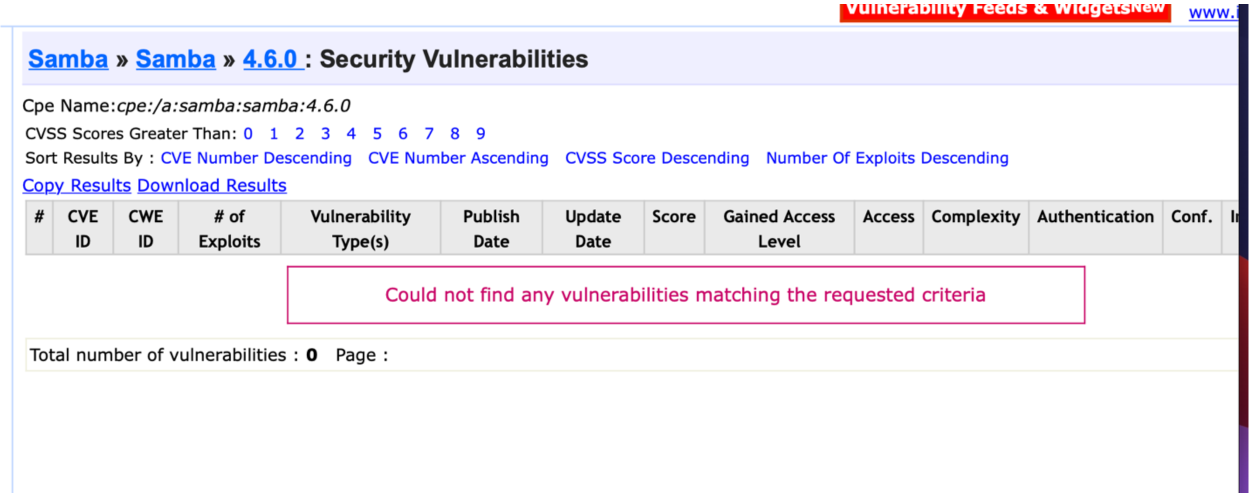
Current speed: 451 requests/sec
(Select and right click for more options)
Average speed: (T) 449, (C) 452 requests/sec
Parse Queue Size: 0
Current number of running threads: 10
Total Requests: 23350/1764393
Time To Finish: 01:04:11
Starting dir/file list based brute forcing
/1515.php

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

I ran the SMB command and got the samba version 4.6.0, once searched online for any vulnerabilities, the rsults I got showed no

Amir Mansha
Lab 2-2
CYSE 425
Fall 2021

vulnerabilities



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

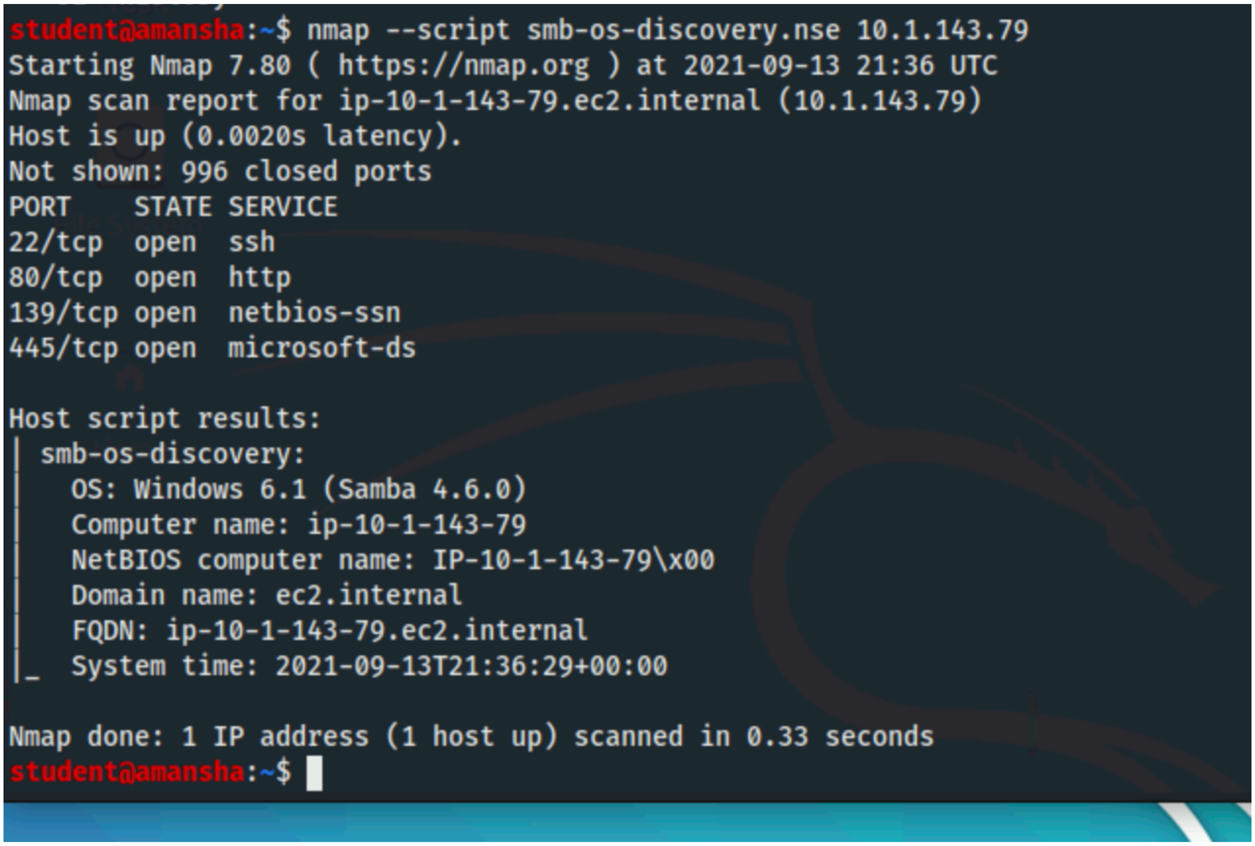
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

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.	I

Could not find any vulnerabilities matching the requested criteria

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



```
student@amansha:~$ nmap --script smb-os-discovery.nse 10.1.143.79
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-13 21:36 UTC
Nmap scan report for ip-10-1-143-79.ec2.internal (10.1.143.79)
Host is up (0.0020s 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-10-1-143-79
|   NetBIOS computer name: IP-10-1-143-79\x00
|   Domain name: ec2.internal
|   FQDN: ip-10-1-143-79.ec2.internal
|_  System time: 2021-09-13T21:36:29+00:00

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
student@amansha:~$ 
```