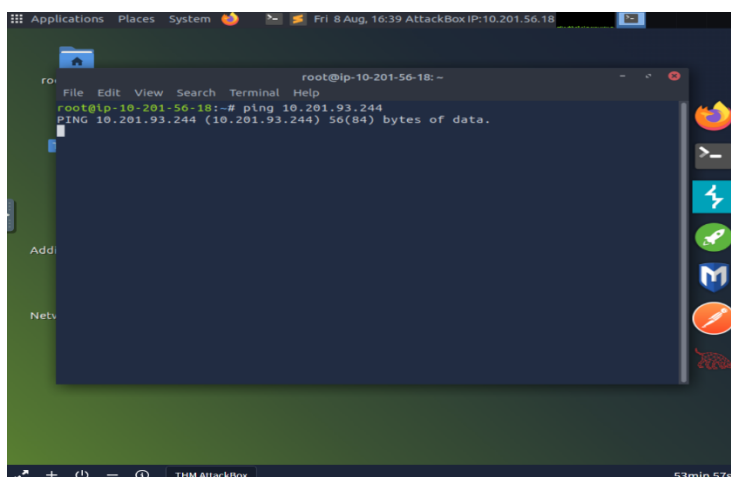


TASK 3 -NMAP ROOM

The third task is to complete the given room on nmap and write a report on that . I did that room long ago. But now ,done it again to write the report.

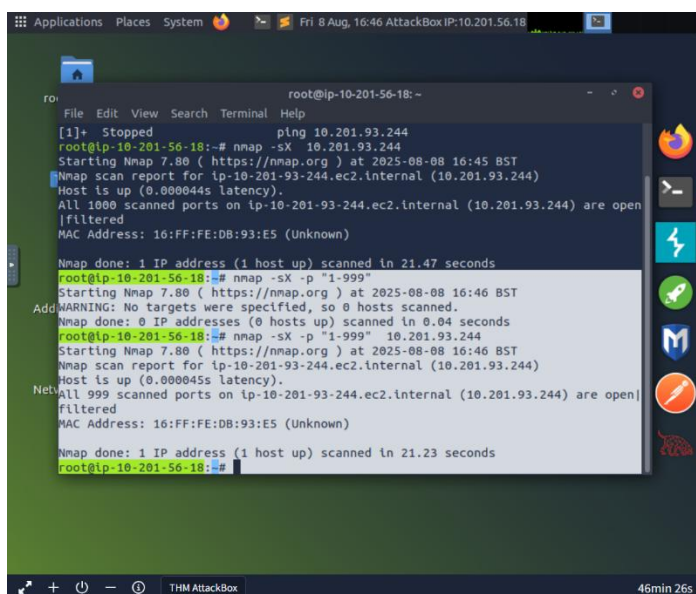
The room says about nmap basics to advanced, nmap commands, from basic commands to advance level like xmas scan...

The first task on that room was to check whether the target IP respond to the ICMP ping request. I used `ping <IP>` to check whether the IP is active.



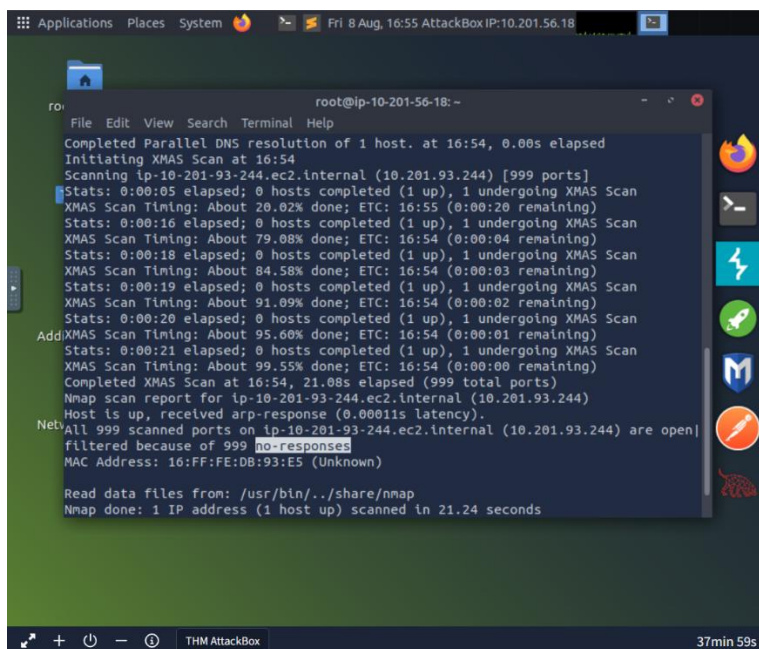
As in this picture, there ain't any response. so the IP isn't active.

Next task was to Perform an Xmas scan on the first 999 ports of the target and check how many ports are shown to be open or filtered

A screenshot of a terminal window on a Linux system. The terminal shows the output of several nmap commands. The first command is 'ping 10.201.93.244', which returns 'Host is up (0.000044s latency)'. The second command is 'nmap -sX 10.201.93.244', which returns 'All 1000 scanned ports on 10.201-93-244.ec2.internal (10.201.93.244) are open | filtered'. The third command is 'nmap -sX -p "1-999" 10.201.93.244', which returns 'All 999 scanned ports on 10.201-93-244.ec2.internal (10.201.93.244) are open | filtered'. The terminal window has a dark background and a light-colored text. The window title is 'root@ip-10-201-56-18: ~'. The window is part of a desktop environment with a taskbar at the bottom showing various icons and the system clock 'Fri 8 Aug, 16:46 AttackBox IP: 10.201.56.18'.

As in this photo, I used `nmap -sX -p "1-999"<IP>` and got that `999 ports` are in filtered state. I have learnt that xmas scan is used to evade firewalls.

Next question is to identify the reason for this filtered ports. I used `-vv` along with the previous xmas command. `vv` stands for very verbose scan which gives an elapsed result about all detailed.

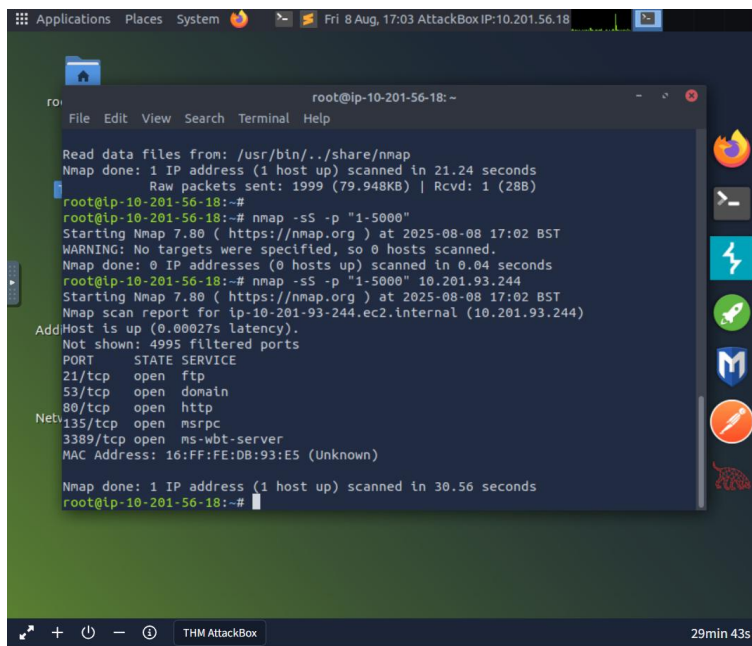
A screenshot of a terminal window titled 'root@ip-10-201-56-18: ~'. The terminal shows the output of an Nmap XMAS scan. The scan is initiated at 16:54 and completes at 16:54, with 21.08s elapsed. The scan target is ip-10-201-93-244.ec2.internal (10.201.93.244) [999 ports]. The output shows that all 999 scanned ports are open, but they are filtered because of 999 'no-responses'. The MAC address is 16:FF:FE:DB:93:ES (Unknown). The terminal also shows the Nmap version (2.8.0) and the scan type (XMAS).

```
root@ip-10-201-56-18: ~  
File Edit View Search Terminal Help  
Completed Parallel DNS resolution of 1 host. at 16:54, 0.00s elapsed  
Initiating XMAS Scan at 16:54  
Scanning ip-10-201-93-244.ec2.internal (10.201.93.244) [999 ports]  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
XMAS Scan Timing: About 20.02% done; ETC: 16:55 (0:00:20 remaining)  
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
XMAS Scan Timing: About 79.08% done; ETC: 16:54 (0:00:04 remaining)  
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
XMAS Scan Timing: About 84.58% done; ETC: 16:54 (0:00:03 remaining)  
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
XMAS Scan Timing: About 91.09% done; ETC: 16:54 (0:00:02 remaining)  
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
Add XMAS Scan Timing: About 95.60% done; ETC: 16:54 (0:00:01 remaining)  
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing XMAS Scan  
XMAS Scan Timing: About 99.55% done; ETC: 16:54 (0:00:00 remaining)  
Completed XMAS Scan at 16:54, 21.08s elapsed (999 total ports)  
Nmap scan report for ip-10-201-93-244.ec2.internal (10.201.93.244)  
Host is up, received arp-response (0.00011s latency).  
Net: All 999 scanned ports on ip-10-201-93-244.ec2.internal (10.201.93.244) are open|  
filtered because of 999 no-responses  
MAC Address: 16:FF:FE:DB:93:ES (Unknown)  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
```

I got “no-response” and identified that it is the reason behind these filtered ports.

Next task is to Perform a TCP SYN scan on the first 5000 ports of the target and find how many ports are shown to be open.

I used the command `nmap -sS -p"1-5000" <IP>`. `-sS` stands for syn tcp scan.



```
root@ip-10-201-56-18: ~  
File Edit View Search Terminal Help  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds  
Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)  
root@ip-10-201-56-18:~#  
root@ip-10-201-56-18:~# nmap -sS -p "1-5000"  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-08 17:02 BST  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds  
root@ip-10-201-56-18:~# nmap -sS -p "1-5000" 10.201.93.244  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-08 17:02 BST  
Nmap scan report for ip-10-201-93-244.ec2.internal (10.201.93.244)  
AddHost is up (0.00027s latency).  
Not shown: 4995 filtered ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
53/tcp    open  domain  
80/tcp    open  http  
135/tcp   open  msrpc  
3389/tcp  open  ms-wbt-server  
MAC Address: 16:FF:FE:DB:93:E5 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 30.56 seconds  
root@ip-10-201-56-18:~#
```

This is the output I obtained. It showed that 5 ports were open.

THANK YOU!