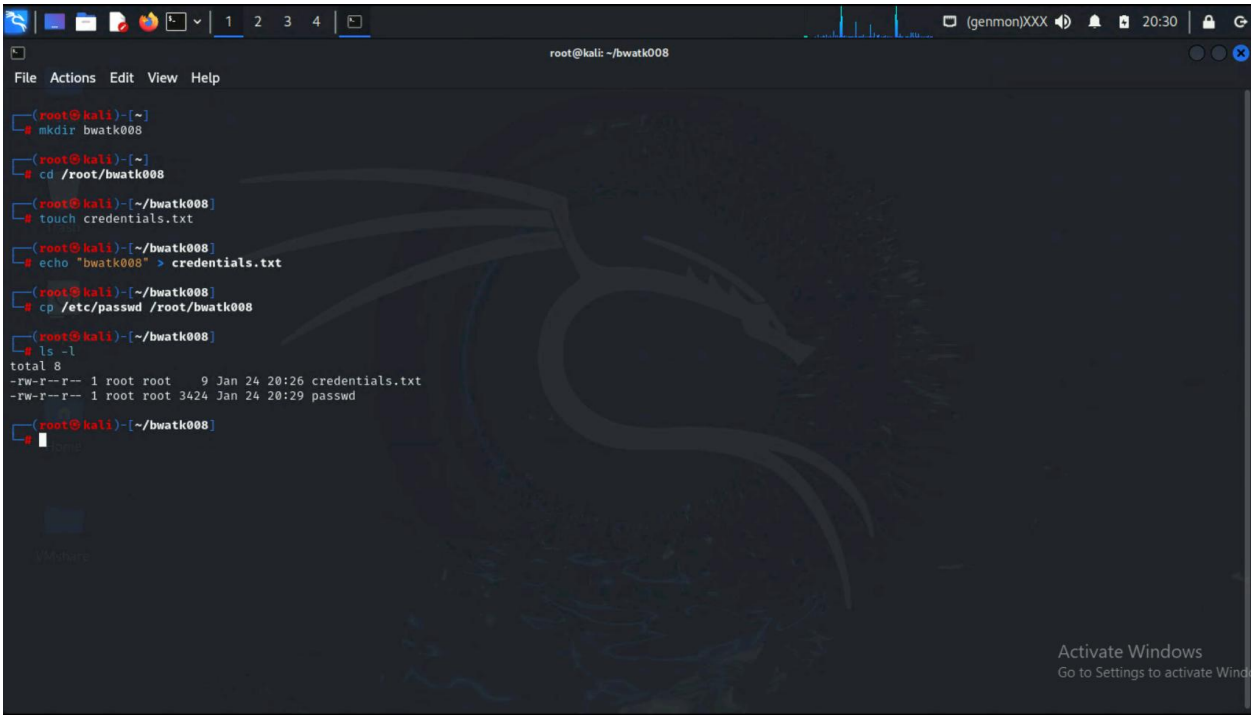
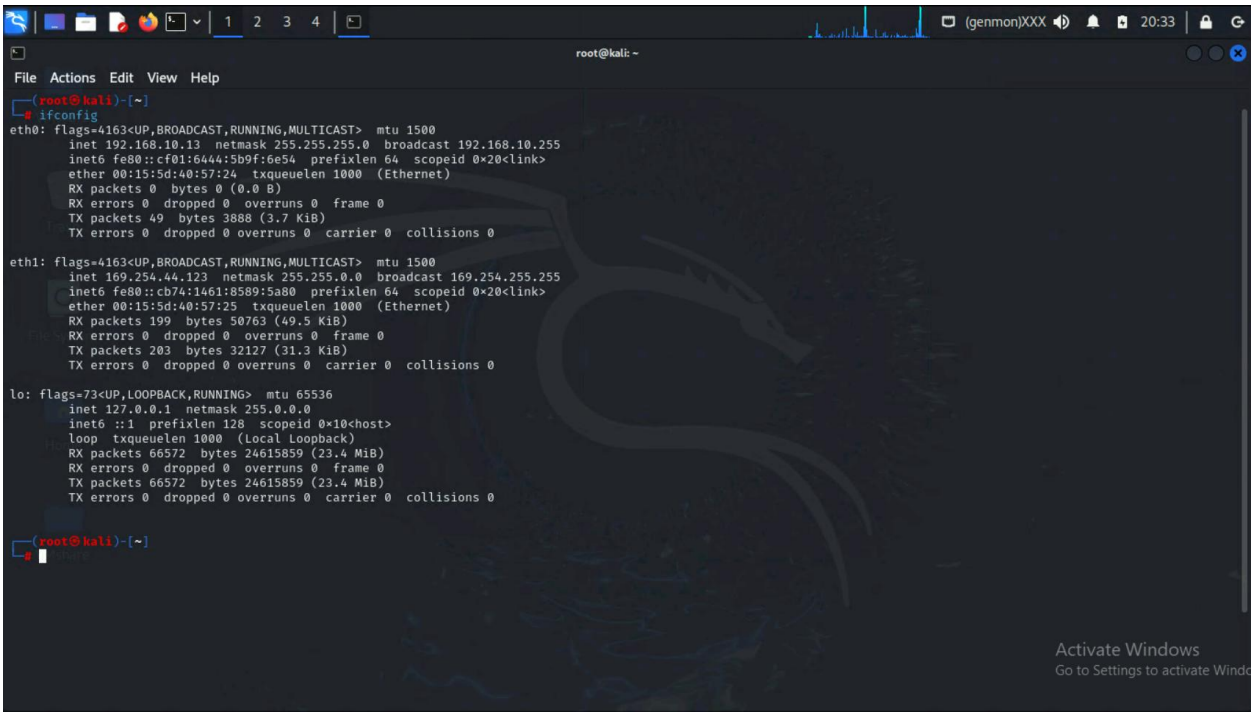
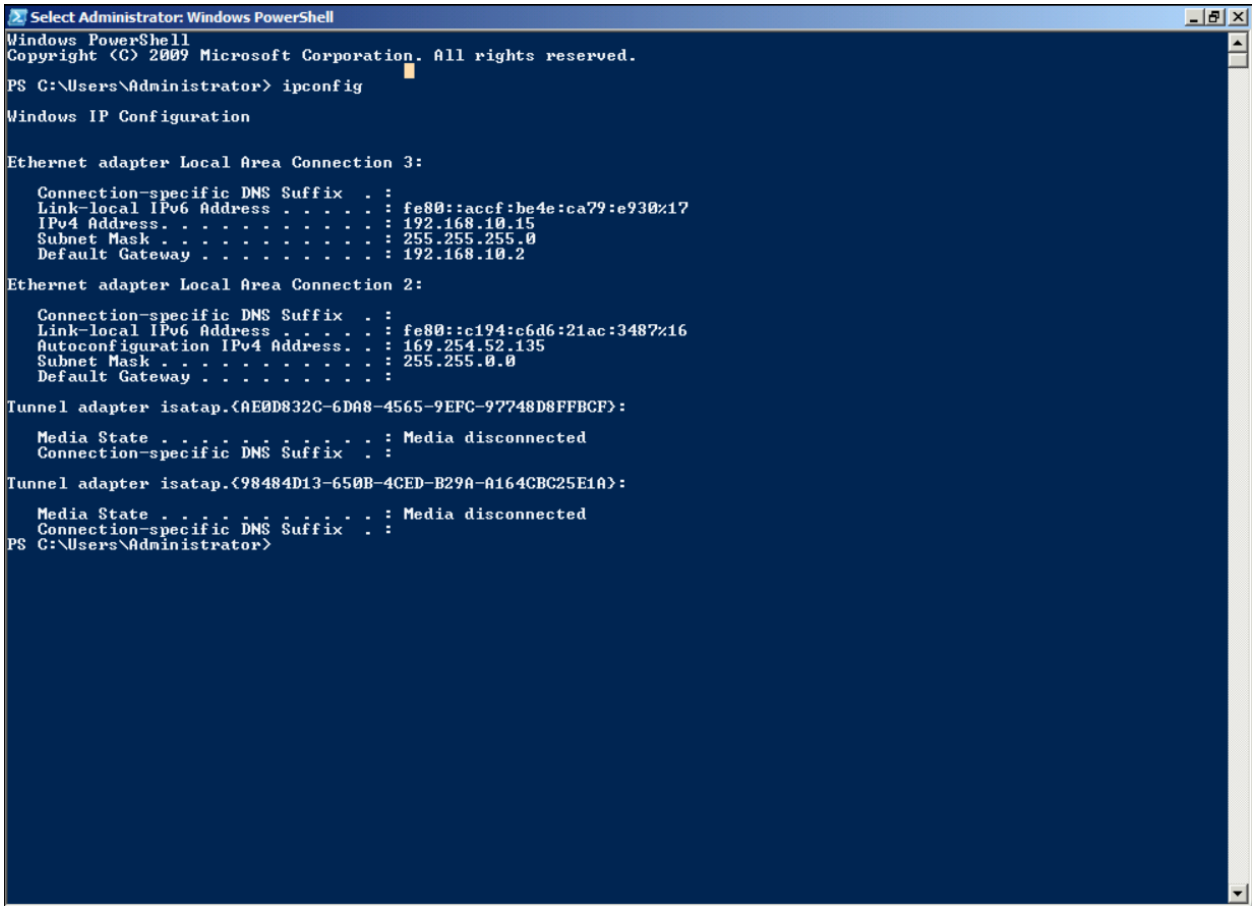
TASK 1

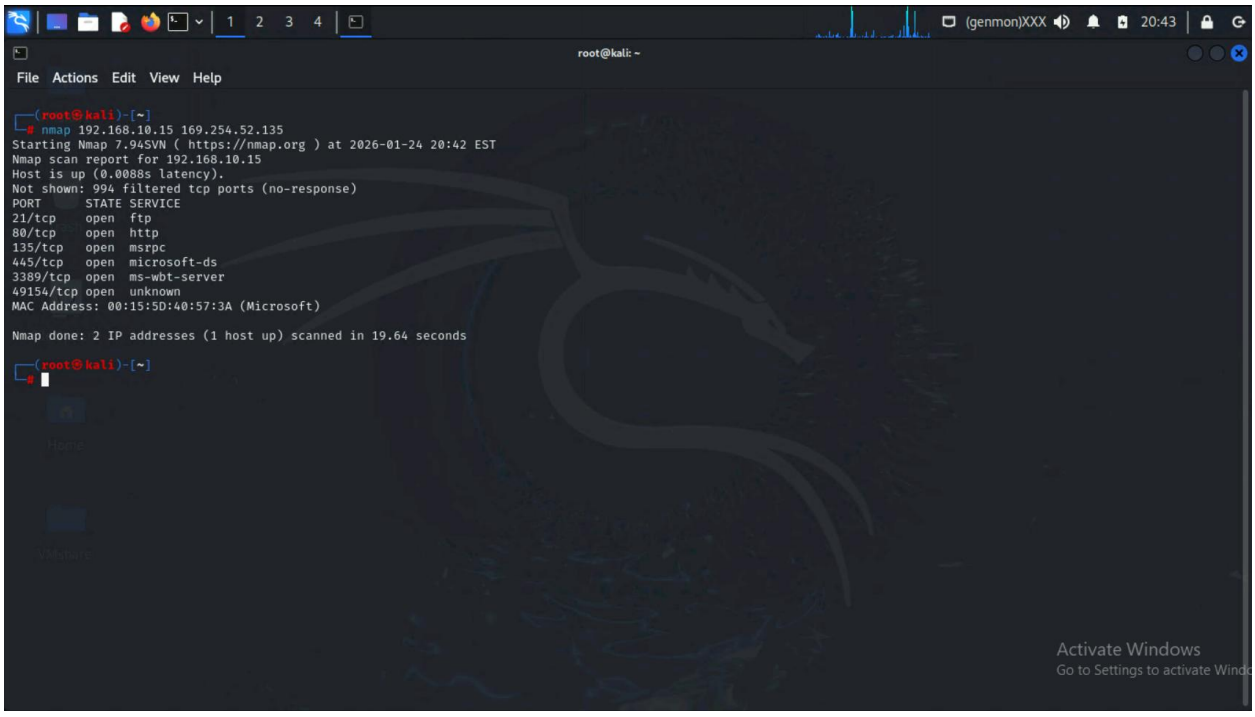

1 2 3 4
(genmon)XXX
20:30
root@kali: ~/bwatk008
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# mkdir bwatk008
┌──(root㉿kali)-[~]
└─# cd /root/bwatk008
┌──(root㉿kali)-[~/bwatk008]
└─# touch credentials.txt
┌──(root㉿kali)-[~/bwatk008]
└─# echo "bwatk008" > credentials.txt
┌──(root㉿kali)-[~/bwatk008]
└─# cp /etc/passwd /root/bwatk008
┌──(root㉿kali)-[~/bwatk008]
└─# ls -l
total 8
-rw-r--r-- 1 root root 9 Jan 24 20:26 credentials.txt
-rw-r--r-- 1 root root 3424 Jan 24 20:29 passwd
┌──(root㉿kali)-[~/bwatk008]
└─#
Activate Windows
Go to Settings to activate Wind

TASK 2

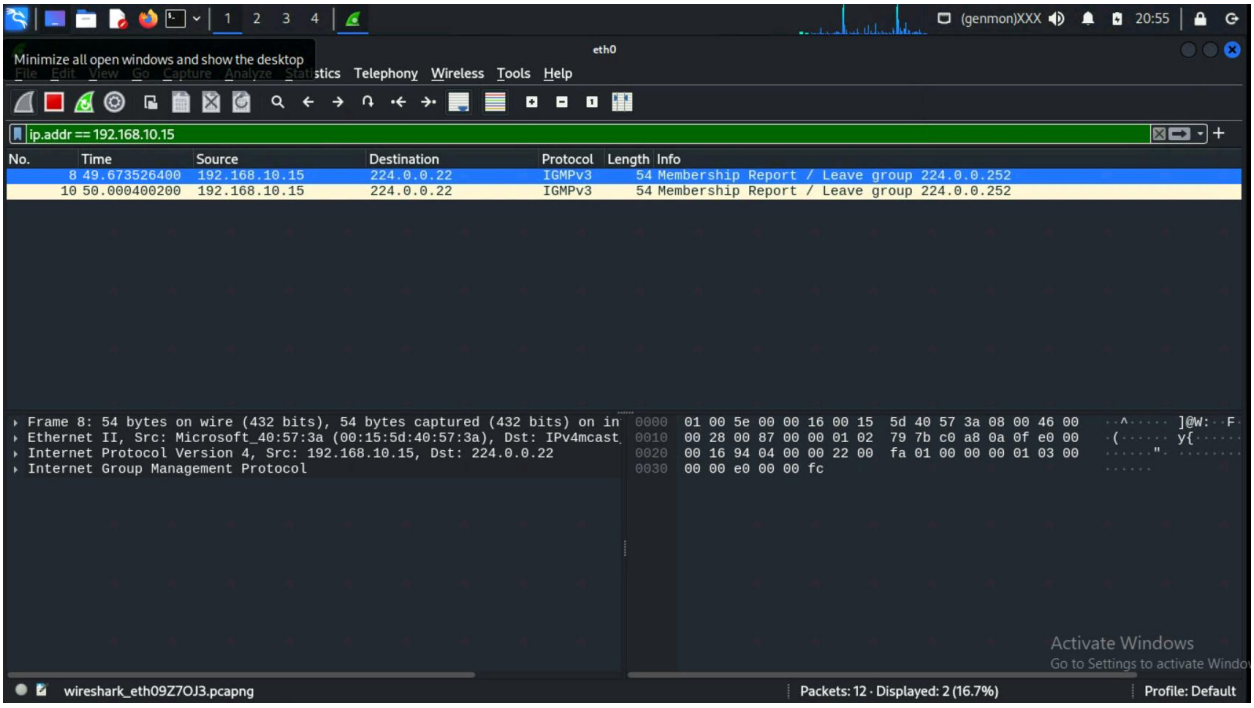

1 2 3 4
(genmon)XXX
20:33
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.10.13 netmask 255.255.255.0 broadcast 192.168.10.255
inet6 fe80::cf01:6444:5b9f:6e54 prefixlen 64 scopeid 0×20<link>
ether 00:15:5d:40:57:24 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 49 bytes 3888 (3.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 169.254.44.123 netmask 255.255.0.0 broadcast 169.254.255.255
inet6 fe80::cb74:1461:8589:5a80 prefixlen 64 scopeid 0×20<link>
ether 00:15:5d:40:57:25 txqueuelen 1000 (Ethernet)
RX packets 199 bytes 50763 (49.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 203 bytes 32127 (31.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 66572 bytes 24615859 (23.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 66572 bytes 24615859 (23.4 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(root㉿kali)-[~]
└─#
Activate Windows
Go to Settings to activate Windo

TASK 2 CONTINUED

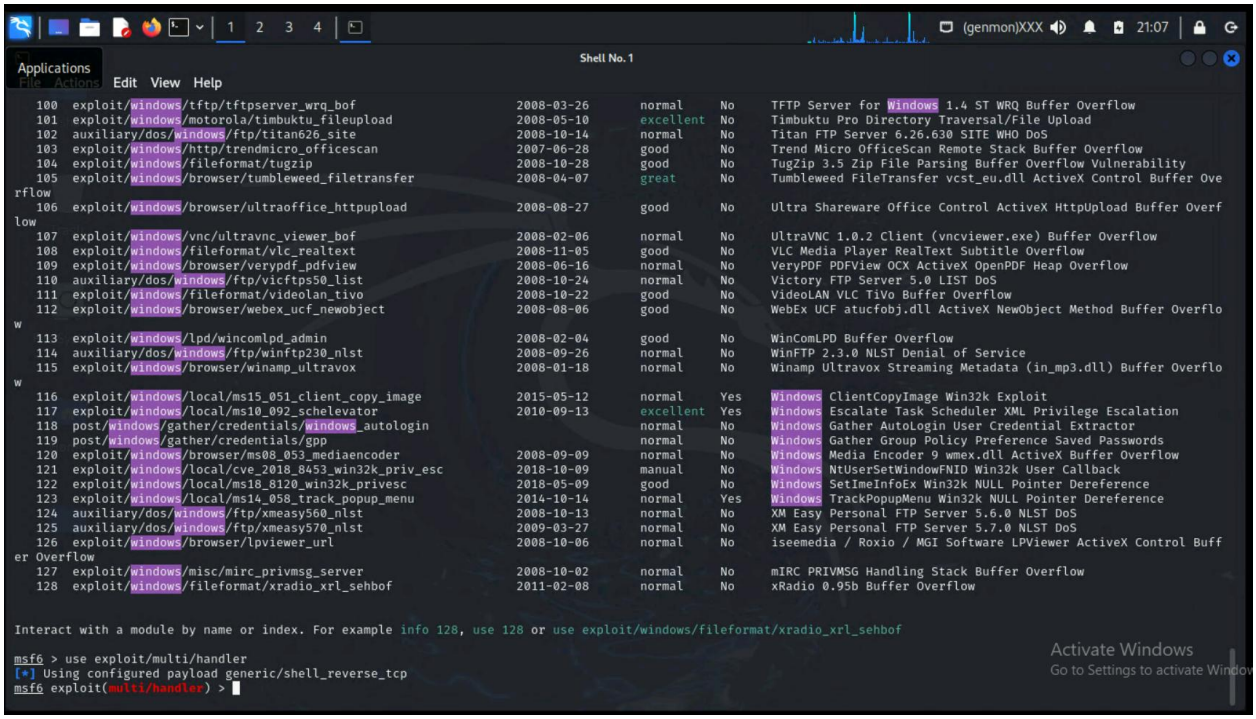




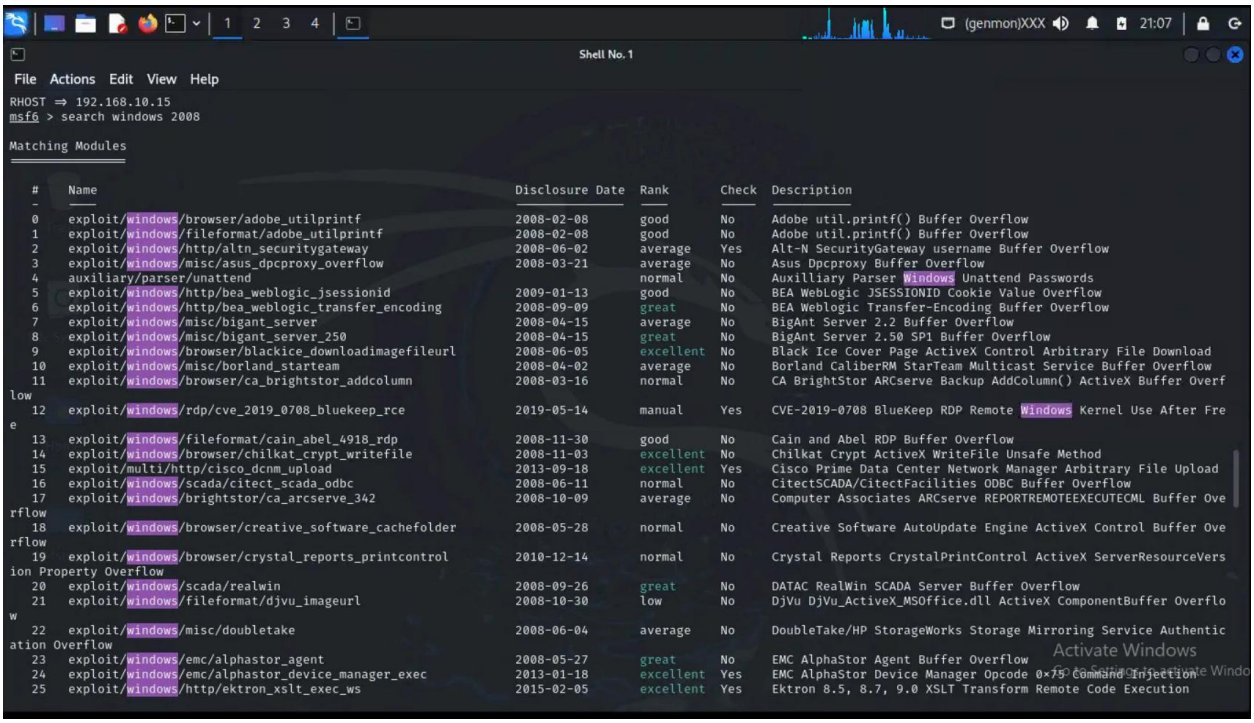
TASK 3



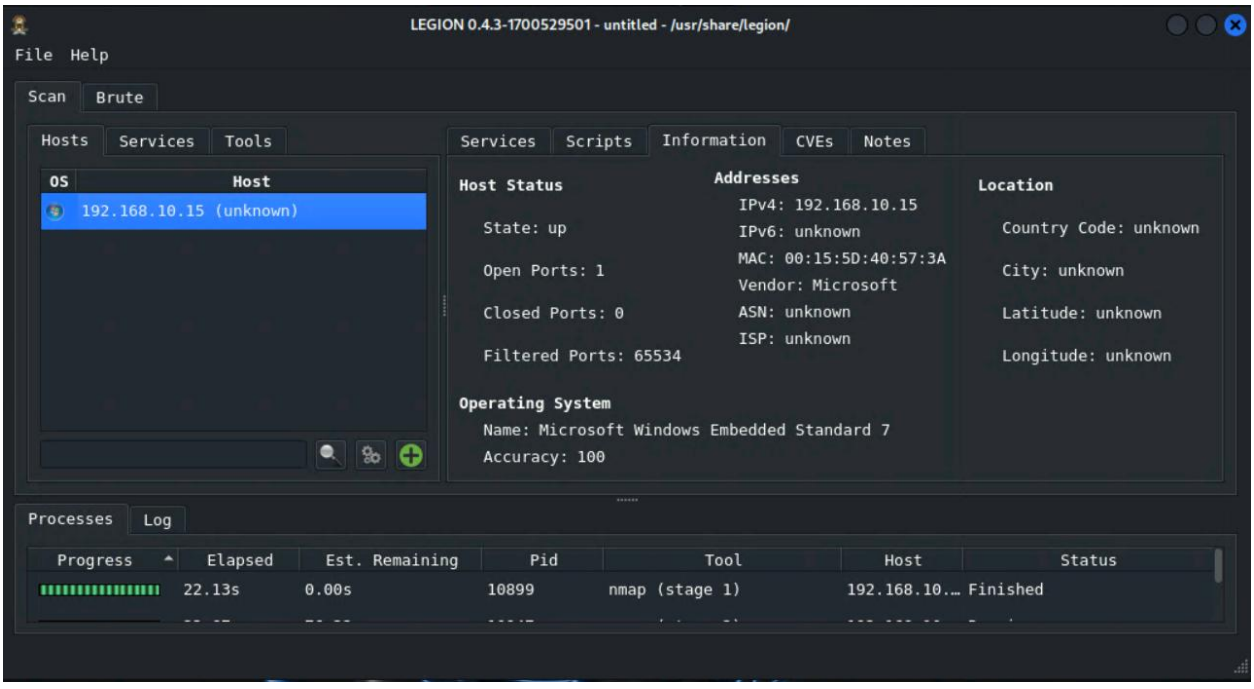
Wireshark – I utilized this tool to conduct monitoring activities on the packet data of 192.168.10.15 (Windows server 2008). There was a total of 12 packets with 2 being displayed.



TASK 3 CONTINUED



Metasploit – I utilized this tool to take steps towards gaining unauthorized access to Windows Server 2008. I successfully set the RHOST (Target) to 192.168.10.15 and selected a specific exploit.



Legion – I utilized this tool to gain insightful information on a potential target (Windows Server 2008). After scanning, the results provided me with some valuable information.

Some results include – IP address, MAC address, number of open ports, state, and operating system.