

TASK 1

```
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)
#
```

TASK 2

```
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 0x20<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 0x20<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 0x10<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)~)
#
```

TASK 2 CONTINUED

```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::accf:be4e:ca79:e930%17
    IPv4 Address. . . . . : 192.168.10.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.2

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::c194:c6d6:21ac:3487%16
    Autoconfiguration IPv4 Address. . : 169.254.52.135
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{AE0D832C-6DA8-4565-9EFC-97748D8FFBCF}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.{98484D13-650B-4CED-B29A-A164CBC25E1A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 
PS C:\Users\Administrator>
```

```
root@kali: ~
File Actions Edit View Help

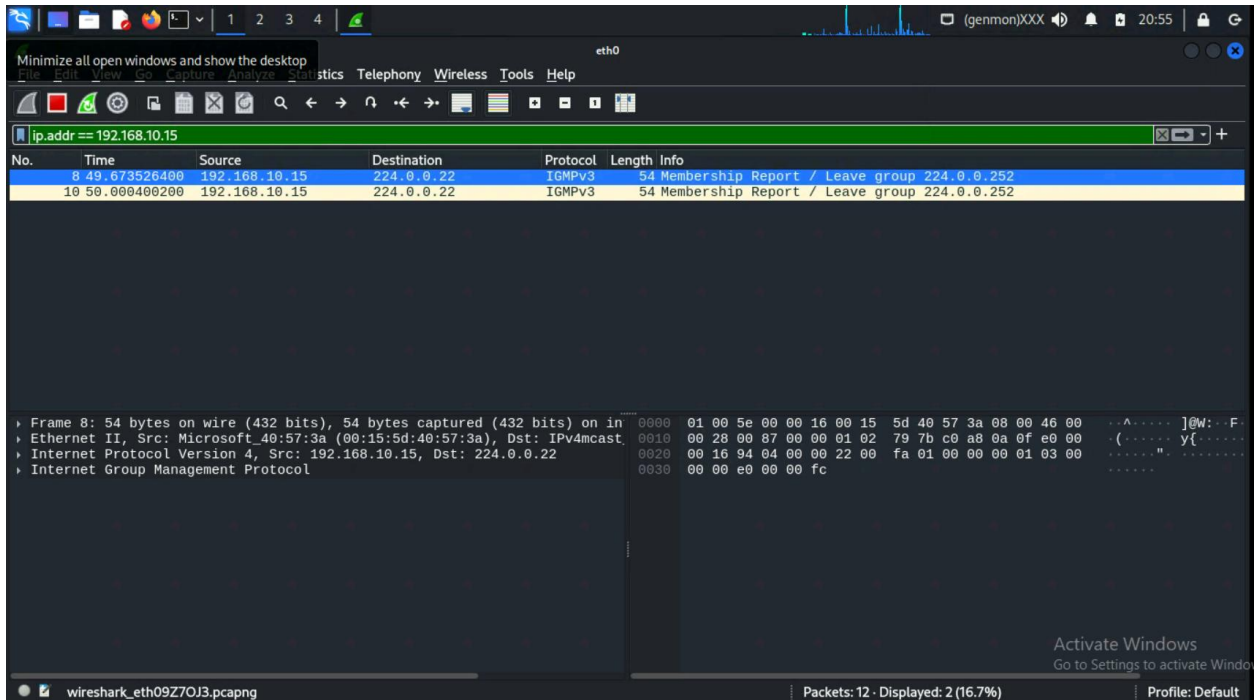
root@kali ~# nmap 192.168.10.15 169.254.52.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-24 20:42 EST
Nmap scan report for 192.168.10.15
Host is up (0.0088s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49154/tcp open  unknown
MAC Address: 00:15:5D:40:57:3A (Microsoft)

Nmap done: 2 IP addresses (1 host up) scanned in 19.64 seconds

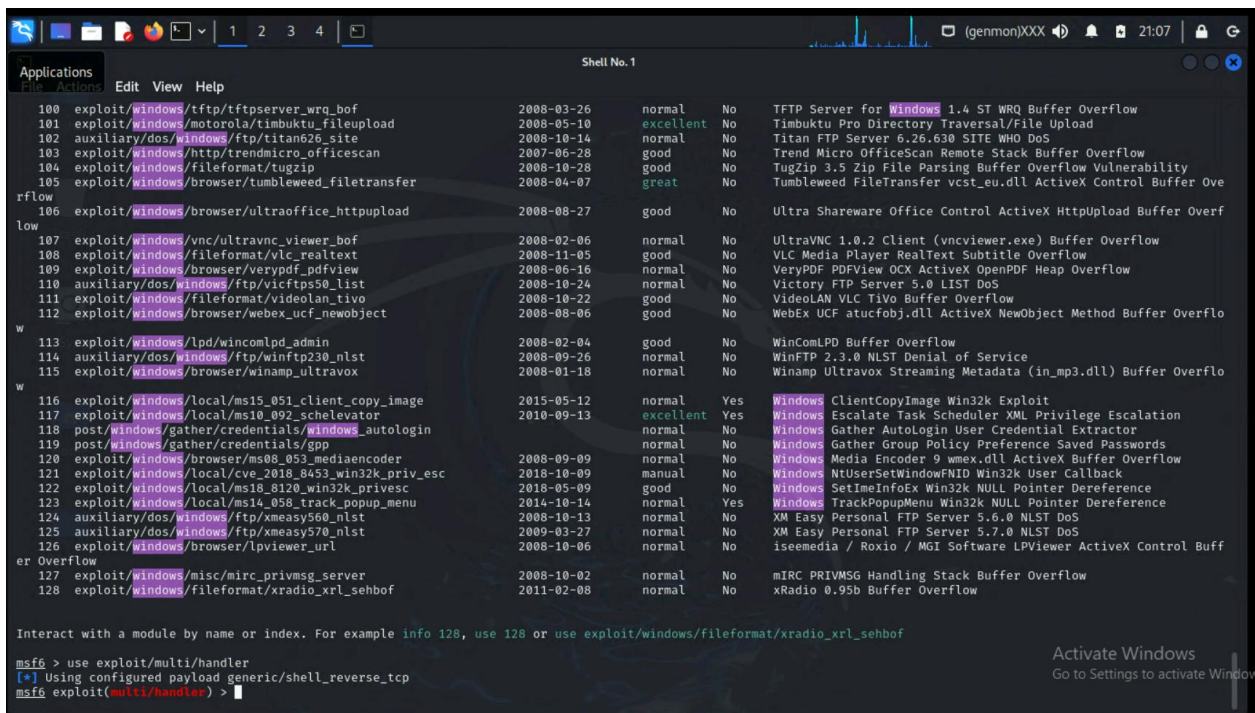
root@kali ~#
```

Activate Windows
Go to Settings to activate Windows

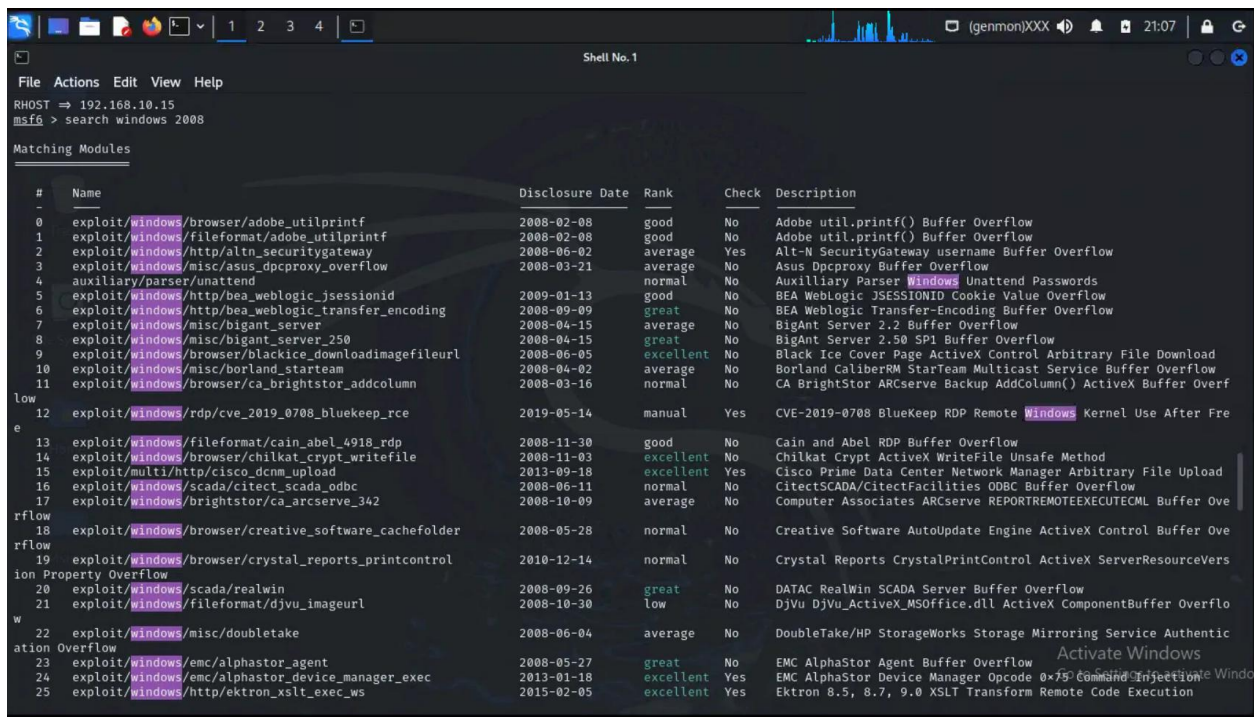
TASK 3



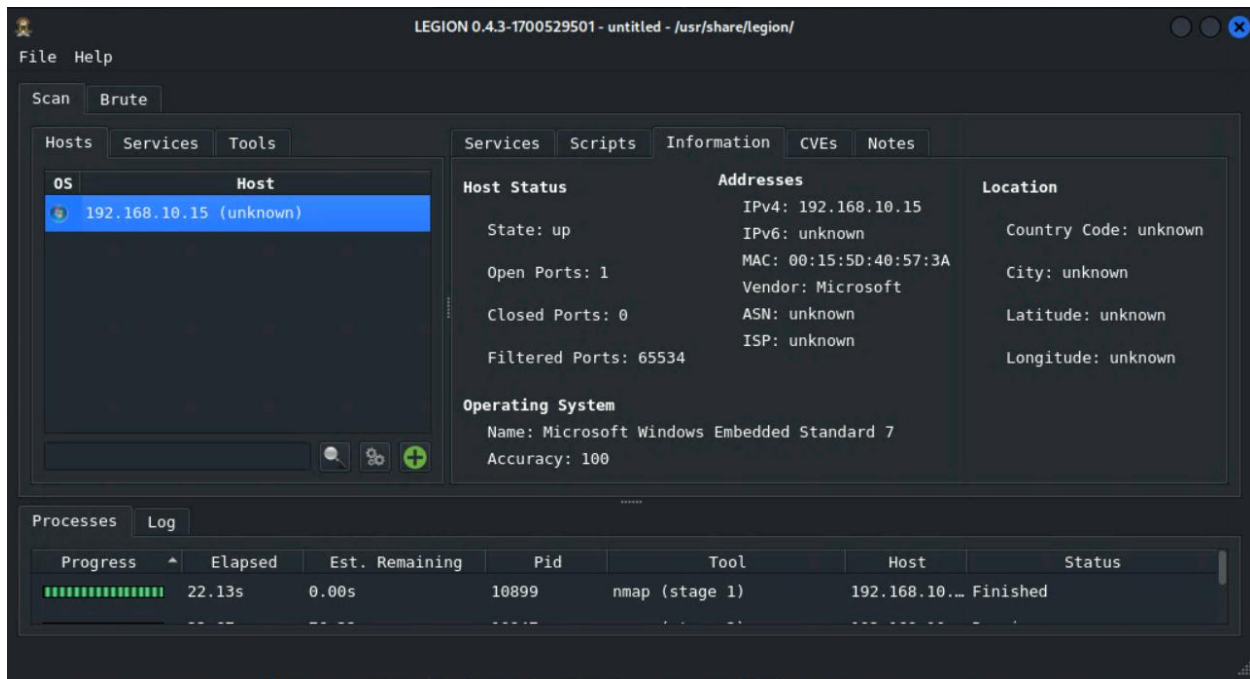
Wireshark – I utilized this tool to conduct monitoring activities on the packet data of 192.168.10.15 (Windows server 2008). There was a total of 12 packets with 2 being displayed.



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.