CEH Module 4: Assignment 1

Lab Scenario: As a professional ethical hacker or penetration tester, your first step in the enumeration of a Windows system is to exploit the NetBIOS API. NetBIOS enumeration allows you to collect information about the target such as a list of computers that belong to a target domain, shares on individual hosts in the target network, policies, passwords, etc. This data can be used to probe the machines further for detailed information about the network and host resources

Lab Objectives:

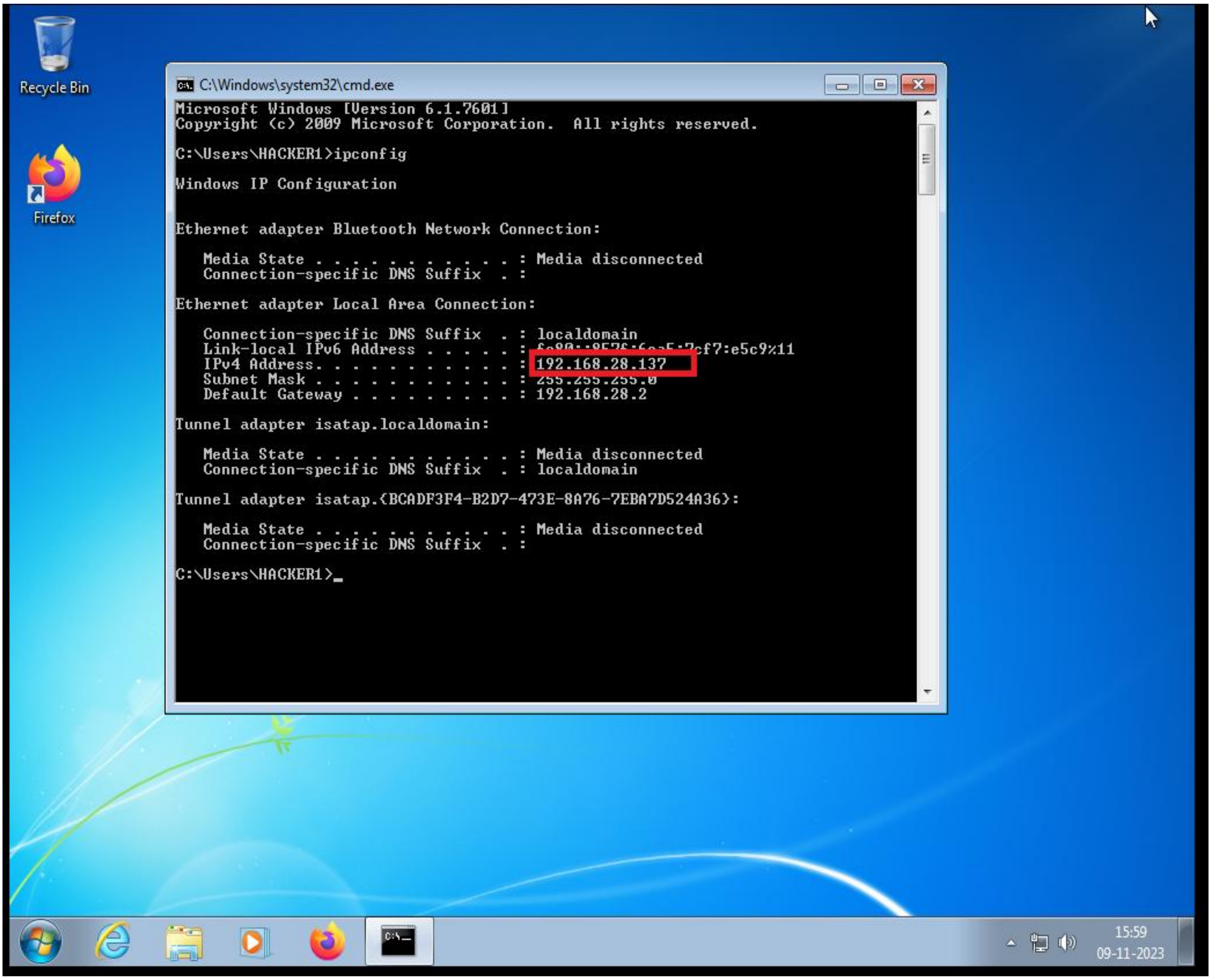
- Perform NetBIOS enumeration using Windows command-line utilities
- Perform NetBIOS enumeration using an NSE Script

• Perform NetBIOS enumeration using Windows command-line utilities

Attacker machine : Windows 10 virtual machine

Target machine : Windows 7 virtual machine

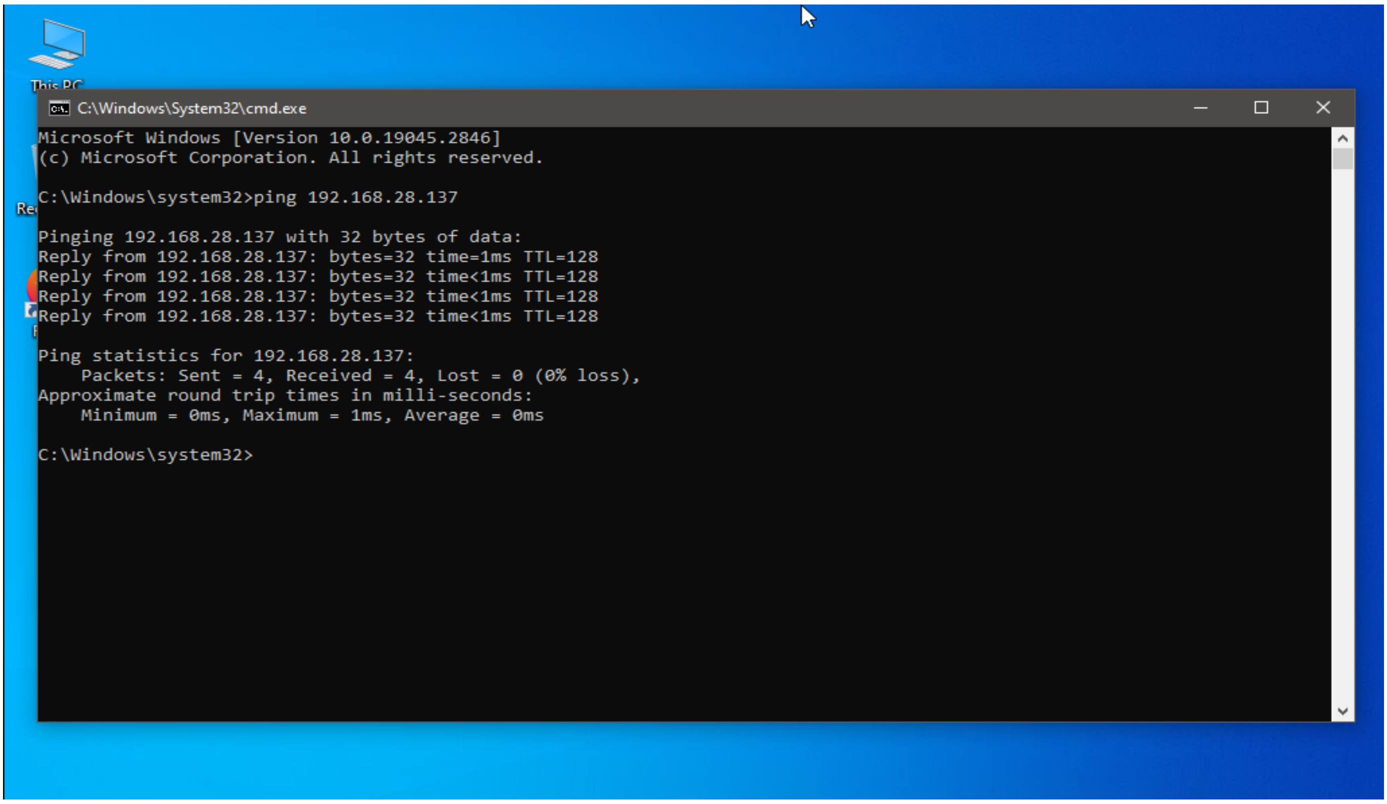
1. Find the ip address of the target machine for advance information



```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\HACKER1>ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

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

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::8576:6aa5:7cf7:e5c9%11
   IPv4 Address. . . . . . . . . . . : 192.168.28.137
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.28.2

Tunnel adapter isatap.localdomain:

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

Tunnel adapter isatap.{BCADF3F4-B2D7-473E-8A76-7EBA7D524A36}:

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

C:\Users\HACKER1>_
```

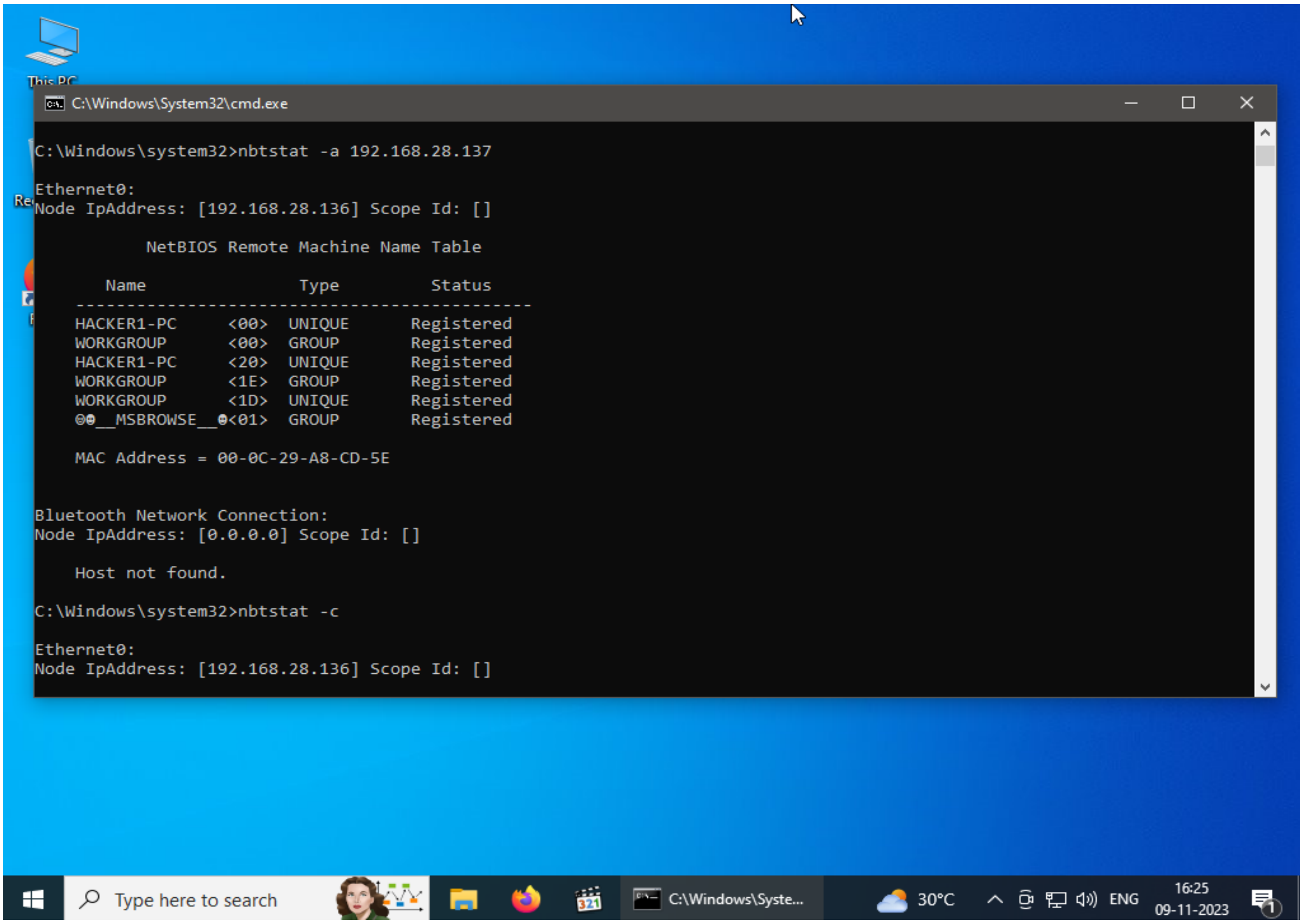
gathering .

2. Now the ip address of the target machine **192.168.28.137**
3. Go to the attacker machine and open the CMD
4. Ping the target ip form the attacker machine **ping 192.168.28.137**



```
Microsoft Windows [Version 10.0.19045.2846]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 192.168.28.137

Pinging 192.168.28.137 with 32 bytes of data:
Reply from 192.168.28.137: bytes=32 time=1ms TTL=128
Reply from 192.168.28.137: bytes=32 time<1ms TTL=128
Reply from 192.168.28.137: bytes=32 time<1ms TTL=128
Reply from 192.168.28.137: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.28.137:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\system32>
```

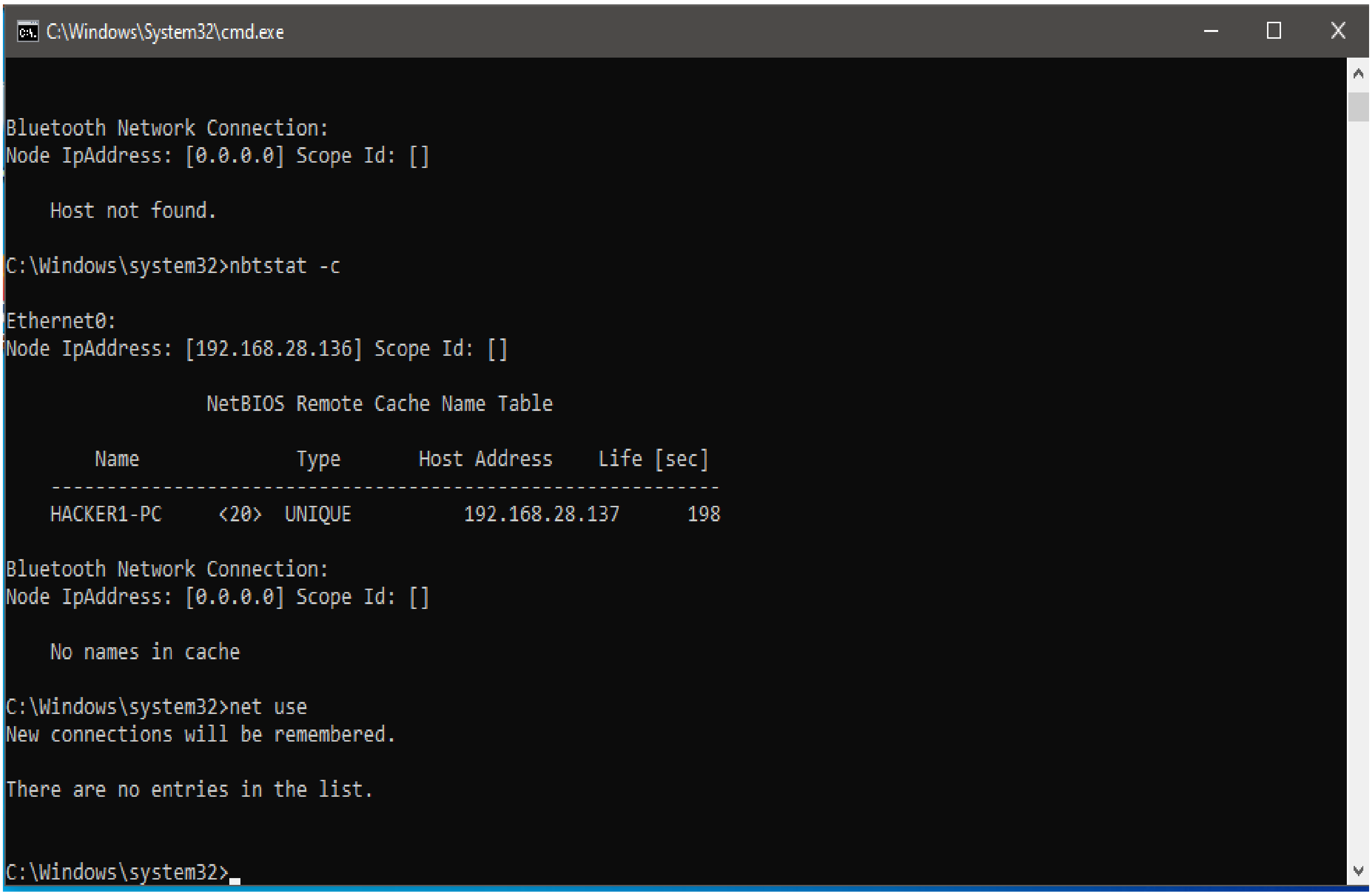
5. ***nbtstat -a 192.168.28.137***



```
C:\Windows\system32>nbtstat -a 192.168.28.137

Ethernet0:
Node IpAddress: [192.168.28.136] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    HACKER1-PC     <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    HACKER1-PC     <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ☺☻__MSBROWSE__☻<01>  GROUP       Registered

    MAC Address = 00-0C-29-A8-CD-5E


Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

C:\Windows\system32>nbtstat -c

Ethernet0:
Node IpAddress: [192.168.28.136] Scope Id: []
```

Gourav-Cybersecurity-Portfolio

6. Nbtstat -c
7. Net Use



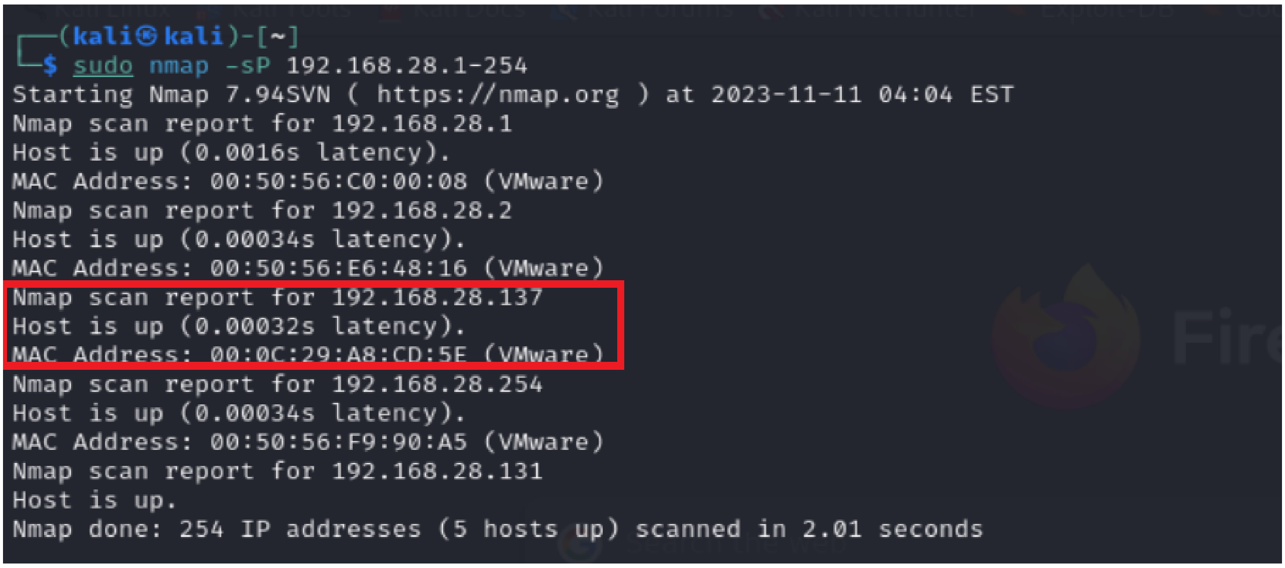
```
Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    Host not found.

C:\Windows\system32>nbtstat -c

Ethernet0:
Node IpAddress: [192.168.28.136] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name              Type       Host Address    Life [sec]
    ------------------------------------------------------------
    HACKER1-PC     <20>  UNIQUE          192.168.28.137      198

Bluetooth Network Connection:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache

C:\Windows\system32>net use
New connections will be remembered.

There are no entries in the list.


C:\Windows\system32>_
```

• Perform NetBIOS enumeration using an NSE Script

Lab Environment:

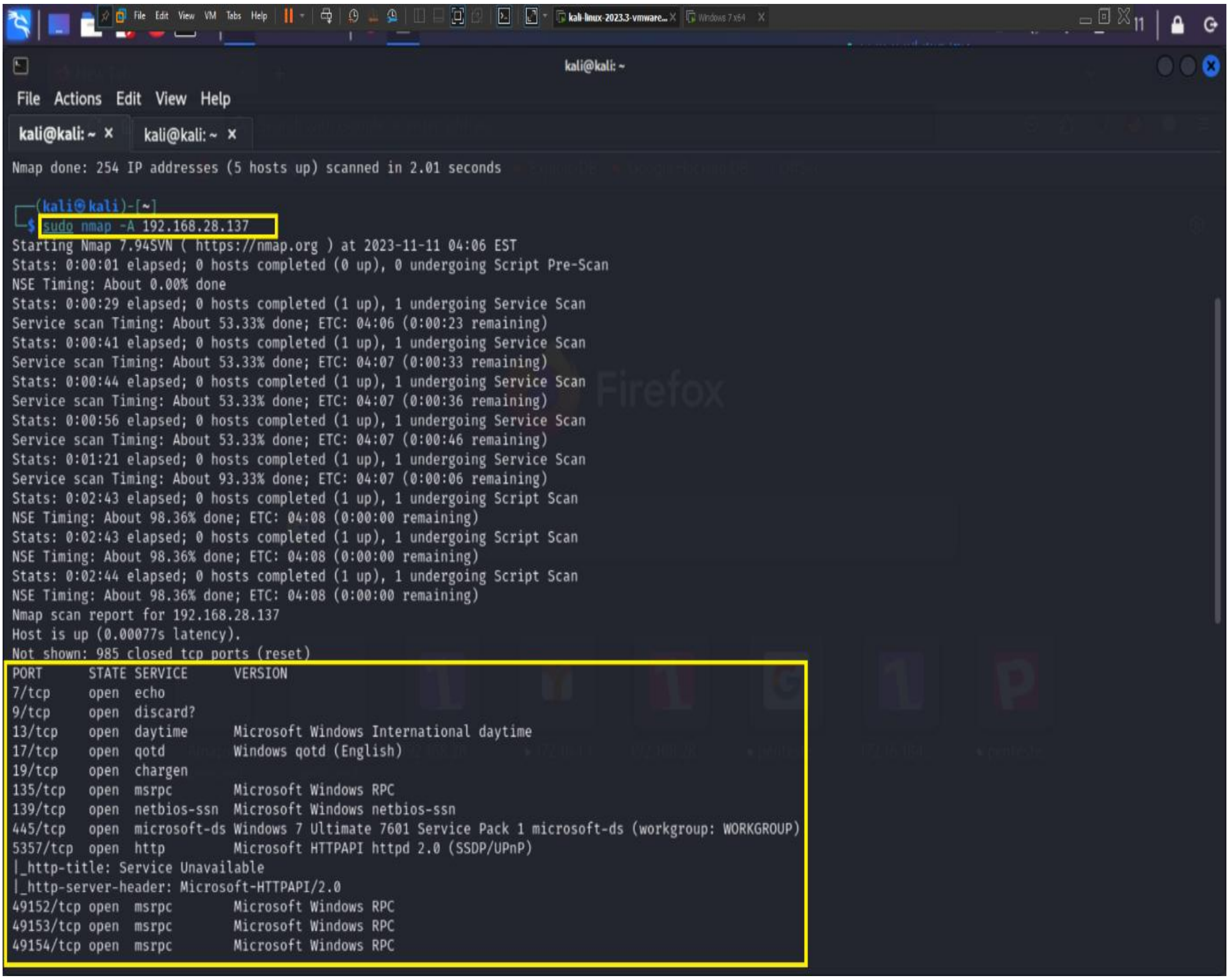
Attacker machine : Kali Linux

Target machine : Windows 7 ultimate

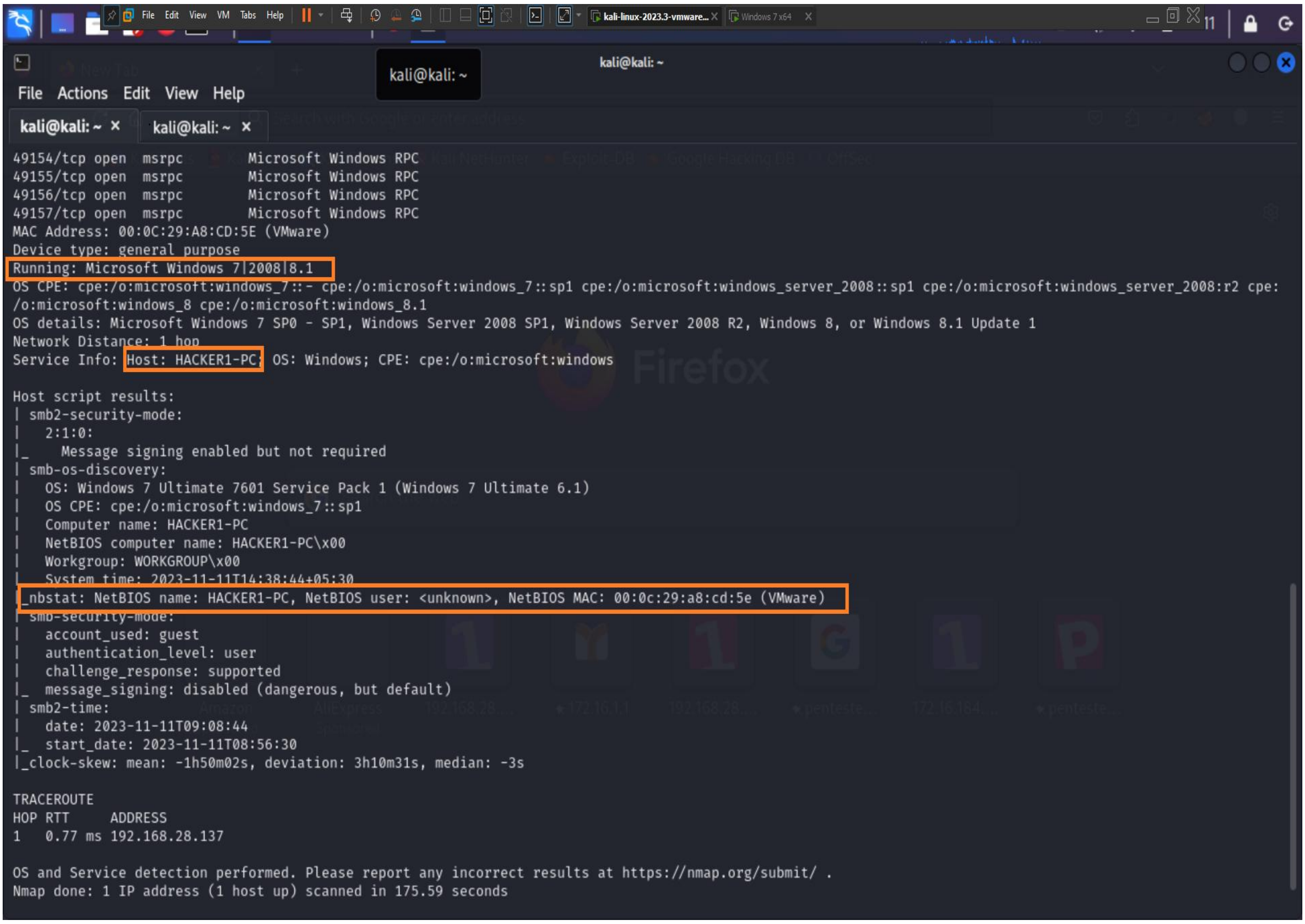


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sP 192.168.28.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 04:04 EST
Nmap scan report for 192.168.28.1
Host is up (0.0016s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.28.2
Host is up (0.00034s latency).
MAC Address: 00:50:56:E6:48:16 (VMware)
Nmap scan report for 192.168.28.137
Host is up (0.00032s latency).
MAC Address: 00:0C:29:A8:CD:5E (VMware)
Nmap scan report for 192.168.28.254
Host is up (0.00034s latency).
MAC Address: 00:50:56:F9:90:A5 (VMware)
Nmap scan report for 192.168.28.131
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 2.01 seconds
```

1. **Find the Victim Server in same server using sudo nmap -sp 192.168.28.1-254**
2. **Now I will try to scan ip 192.168.28.137 and try to gather more information like :**
   a. **What is this ip**
   b. **What is the name of the system**
   c. **What are the open ports**
   d. **Sudo nmap -A 192.168.28.137**

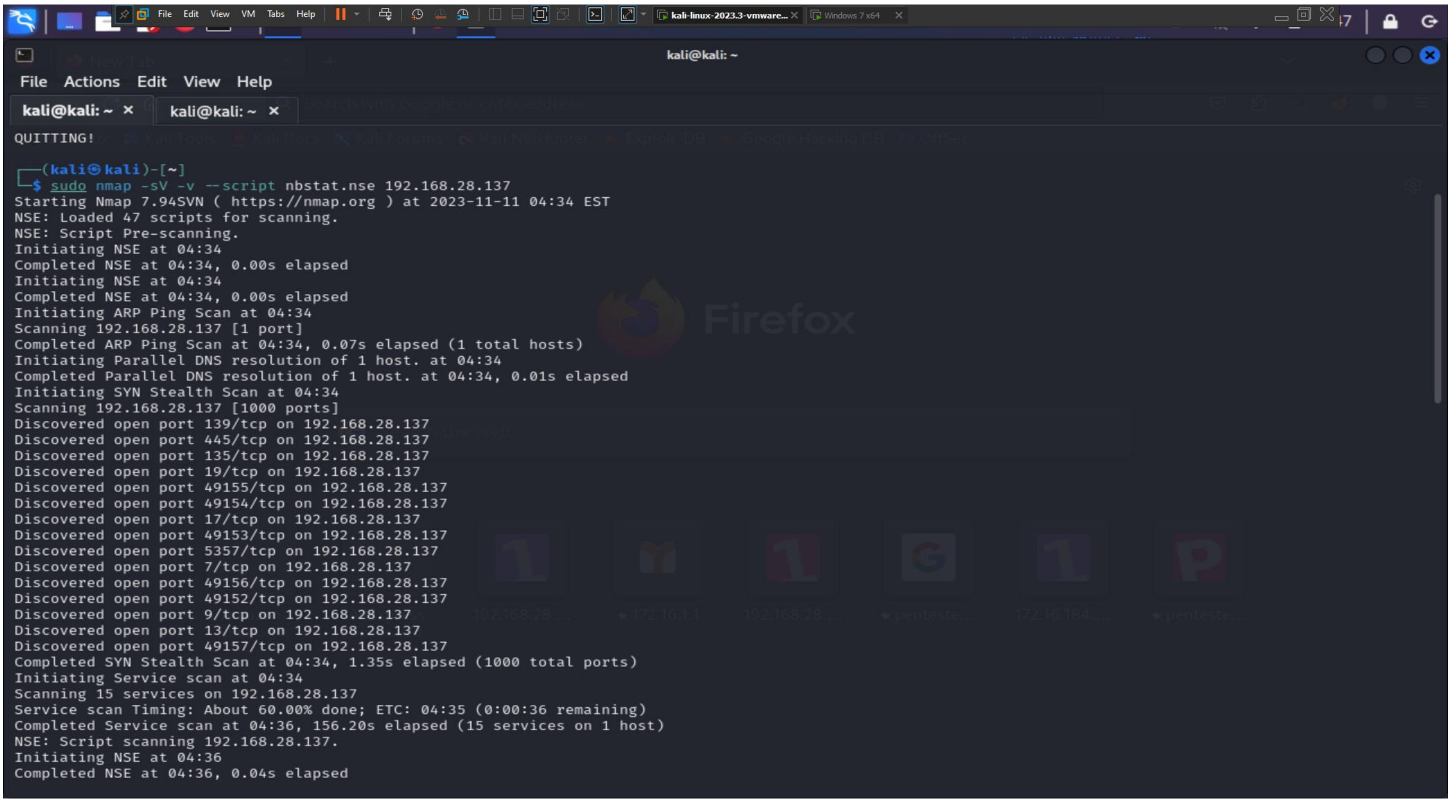


```
Nmap done: 254 IP addresses (5 hosts up) scanned in 2.01 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.28.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 04:06 EST
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 53.33% done; ETC: 04:06 (0:00:23 remaining)
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 53.33% done; ETC: 04:07 (0:00:33 remaining)
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 53.33% done; ETC: 04:07 (0:00:36 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 53.33% done; ETC: 04:07 (0:00:46 remaining)
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 93.33% done; ETC: 04:07 (0:00:06 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.36% done; ETC: 04:08 (0:00:00 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.36% done; ETC: 04:08 (0:00:00 remaining)
Stats: 0:02:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.36% done; ETC: 04:08 (0:00:00 remaining)
Nmap scan report for 192.168.28.137
Host is up (0.00077s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
```

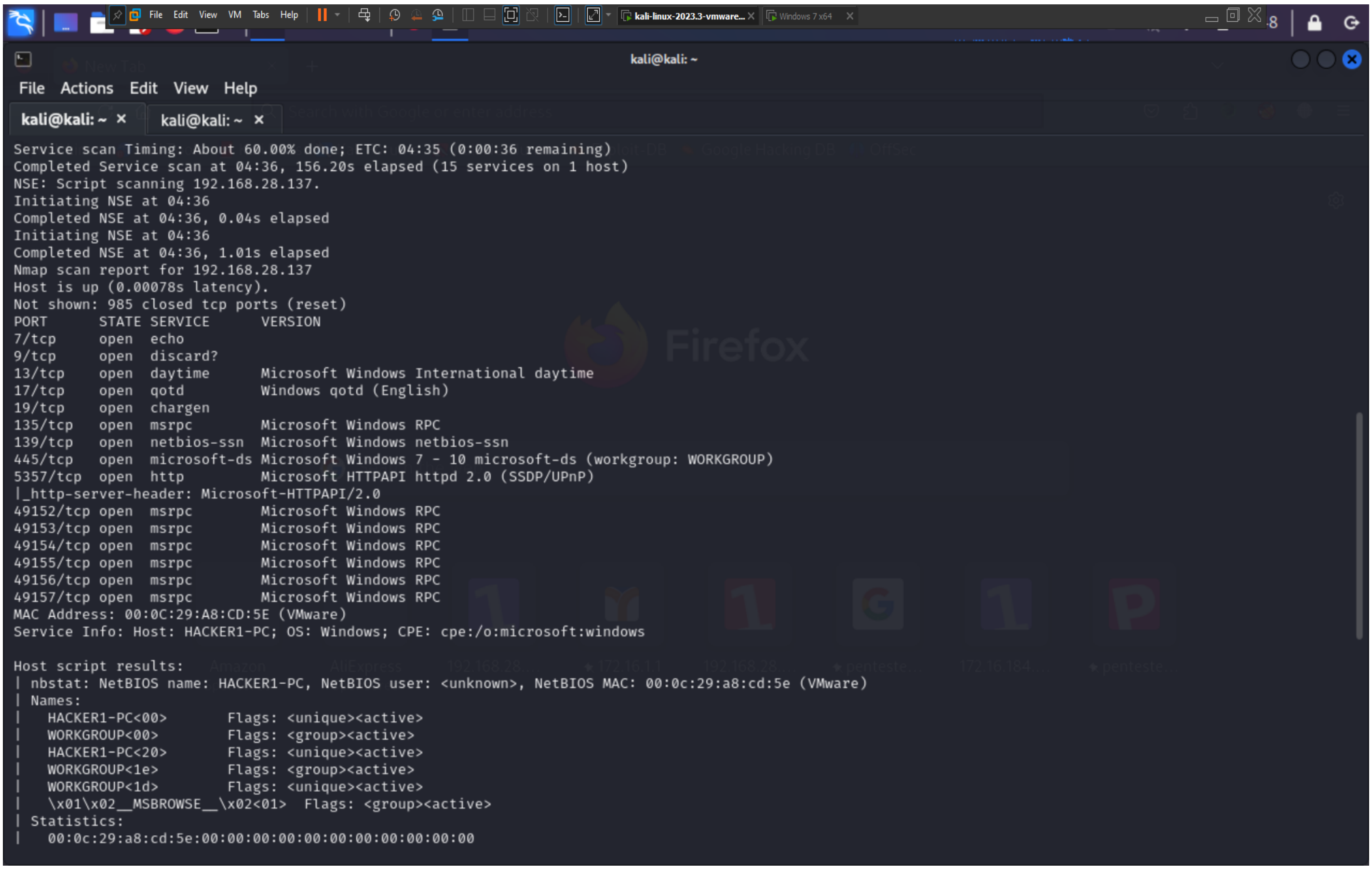


```
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:A8:CD:5E (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:
/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: HACKER1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: HACKER1-PC
|   NetBIOS computer name: HACKER1-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-11-11T14:38:44+05:30
|_nbstat: NetBIOS name: HACKER1-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a8:cd:5e (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-11-11T09:08:44
|_  start_date: 2023-11-11T08:56:30
|_clock-skew: mean: -1h50m02s, deviation: 3h10m31s, median: -3s

TRACEROUTE
HOP RTT     ADDRESS
1   0.77 ms 192.168.28.137

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.59 seconds
```

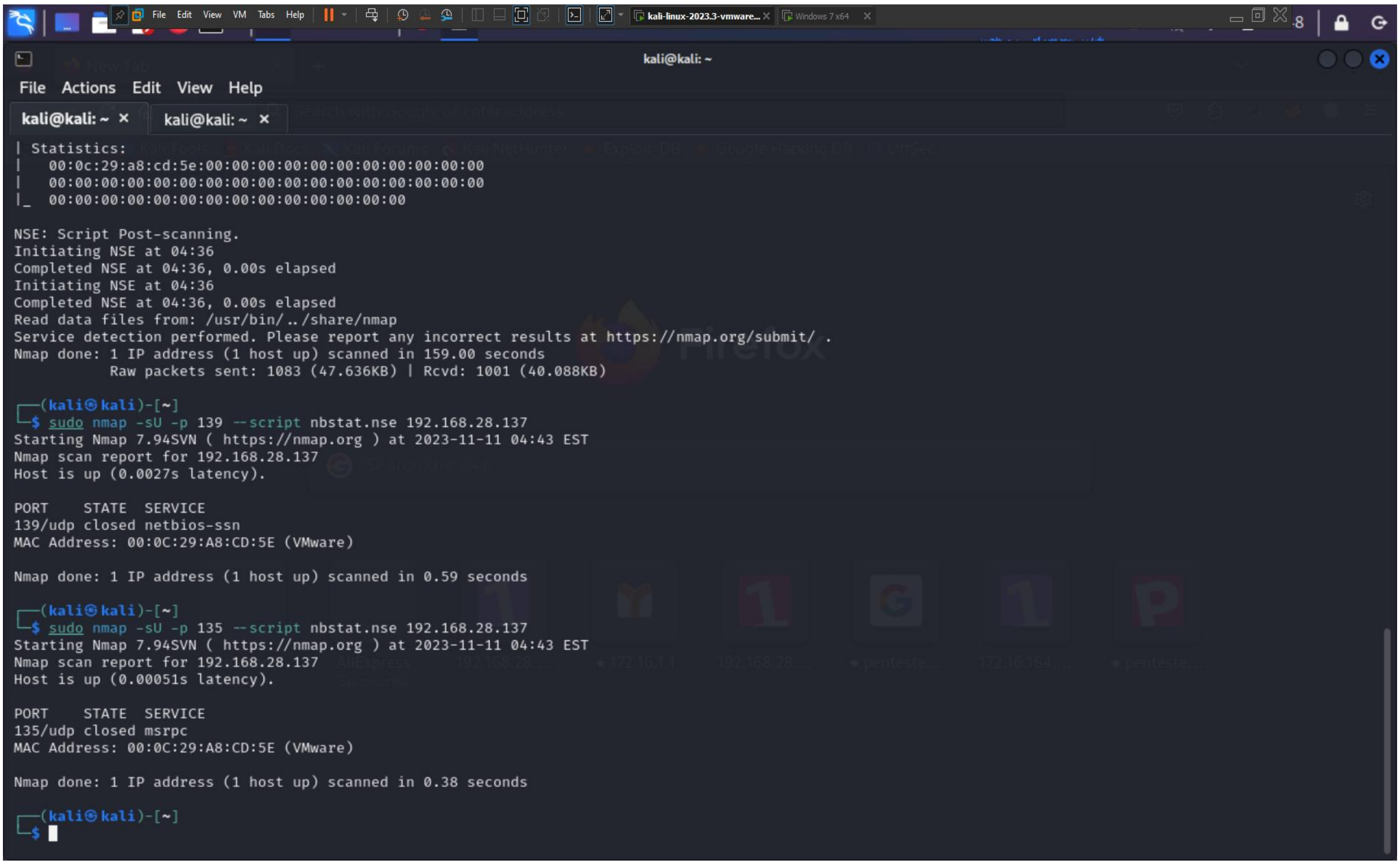
Sudo nmap -sV -v –script nbstat.nse 192.168.28.137



```
QUITTING!

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -v --script nbstat.nse 192.168.28.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 04:34 EST
NSE: Loaded 47 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating ARP Ping Scan at 04:34
Scanning 192.168.28.137 [1 port]
Completed ARP Ping Scan at 04:34, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:34
Completed Parallel DNS resolution of 1 host. at 04:34, 0.01s elapsed
Initiating SYN Stealth Scan at 04:34
Scanning 192.168.28.137 [1000 ports]
Discovered open port 139/tcp on 192.168.28.137
Discovered open port 445/tcp on 192.168.28.137
Discovered open port 135/tcp on 192.168.28.137
Discovered open port 19/tcp on 192.168.28.137
Discovered open port 49155/tcp on 192.168.28.137
Discovered open port 49154/tcp on 192.168.28.137
Discovered open port 17/tcp on 192.168.28.137
Discovered open port 49153/tcp on 192.168.28.137
Discovered open port 5357/tcp on 192.168.28.137
Discovered open port 7/tcp on 192.168.28.137
Discovered open port 49156/tcp on 192.168.28.137
Discovered open port 49152/tcp on 192.168.28.137
Discovered open port 9/tcp on 192.168.28.137
Discovered open port 13/tcp on 192.168.28.137
Discovered open port 49157/tcp on 192.168.28.137
Completed SYN Stealth Scan at 04:34, 1.35s elapsed (1000 total ports)
Initiating Service scan at 04:34
Scanning 15 services on 192.168.28.137
Service scan Timing: About 60.00% done; ETC: 04:35 (0:00:36 remaining)
Completed Service scan at 04:36, 156.20s elapsed (15 services on 1 host)
NSE: Script scanning 192.168.28.137.
Initiating NSE at 04:36
Completed NSE at 04:36, 0.04s elapsed
```



```
Service scan Timing: About 60.00% done; ETC: 04:35 (0:00:36 remaining)
Completed Service scan at 04:36, 156.20s elapsed (15 services on 1 host)
NSE: Script scanning 192.168.28.137.
Initiating NSE at 04:36
Completed NSE at 04:36, 0.04s elapsed
Initiating NSE at 04:36
Completed NSE at 04:36, 1.01s elapsed
Nmap scan report for 192.168.28.137
Host is up (0.00078s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows International daytime
17/tcp    open  qotd         Windows qotd (English)
19/tcp    open  chargen
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:A8:CD:5E (VMware)
Service Info: Host: HACKER1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: HACKER1-PC, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a8:cd:5e (VMware)
| Names:
|   HACKER1-PC<00>       Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   HACKER1-PC<20>       Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00:0c:29:a8:cd:5e:00:00:00:00:00:00:00:00:00:00:00
```



```
| Statistics:
|   00:0c:29:a8:cd:5e:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00

NSE: Script Post-scanning.
Initiating NSE at 04:36
Completed NSE at 04:36, 0.00s elapsed
Initiating NSE at 04:36
Completed NSE at 04:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.00 seconds
           Raw packets sent: 1083 (47.636KB) | Rcvd: 1001 (40.088KB)

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 139 --script nbstat.nse 192.168.28.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 04:43 EST
Nmap scan report for 192.168.28.137
Host is up (0.0027s latency).

PORT    STATE  SERVICE
139/udp closed netbios-ssn
MAC Address: 00:0C:29:A8:CD:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 135 --script nbstat.nse 192.168.28.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 04:43 EST
Nmap scan report for 192.168.28.137
Host is up (0.00051s latency).

PORT    STATE  SERVICE
135/udp closed msrpc
MAC Address: 00:0C:29:A8:CD:5E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds

┌──(kali㉿kali)-[~]
└─$ 
```