CEH Module 4: Enumeration
Assignment - 02
(Sairaj Mothukuri)

Given 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

Given Lab Objectives:

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

Enumeration:

- In enumeration we can gather advance information of the target.
- Enumeration can done when we are inside the **LAN**
- If we do enumeration on target we can extract
    - **Routing information**
    - **SNMP information**
    - **Machine name**
    - **User information**
    - **Group information**

- **Network resource**

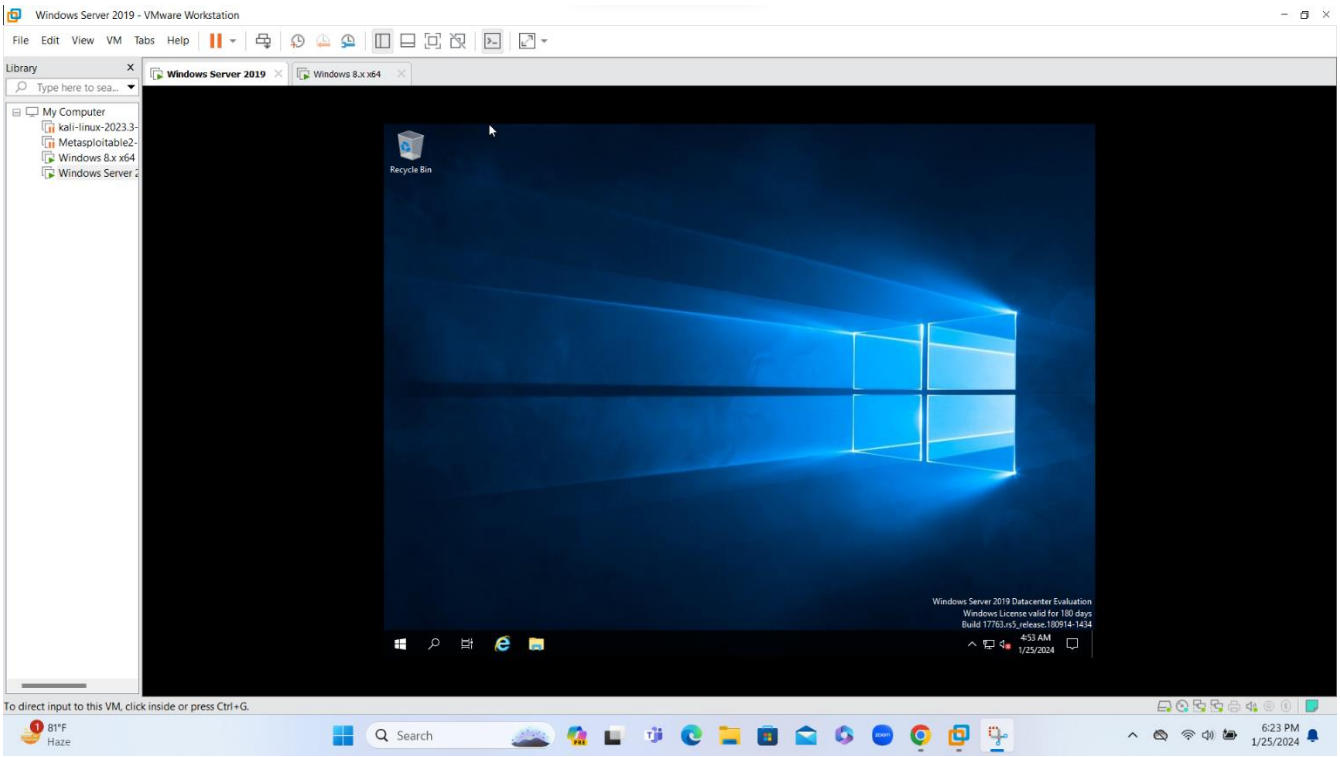
NetBIOS Enumeration:

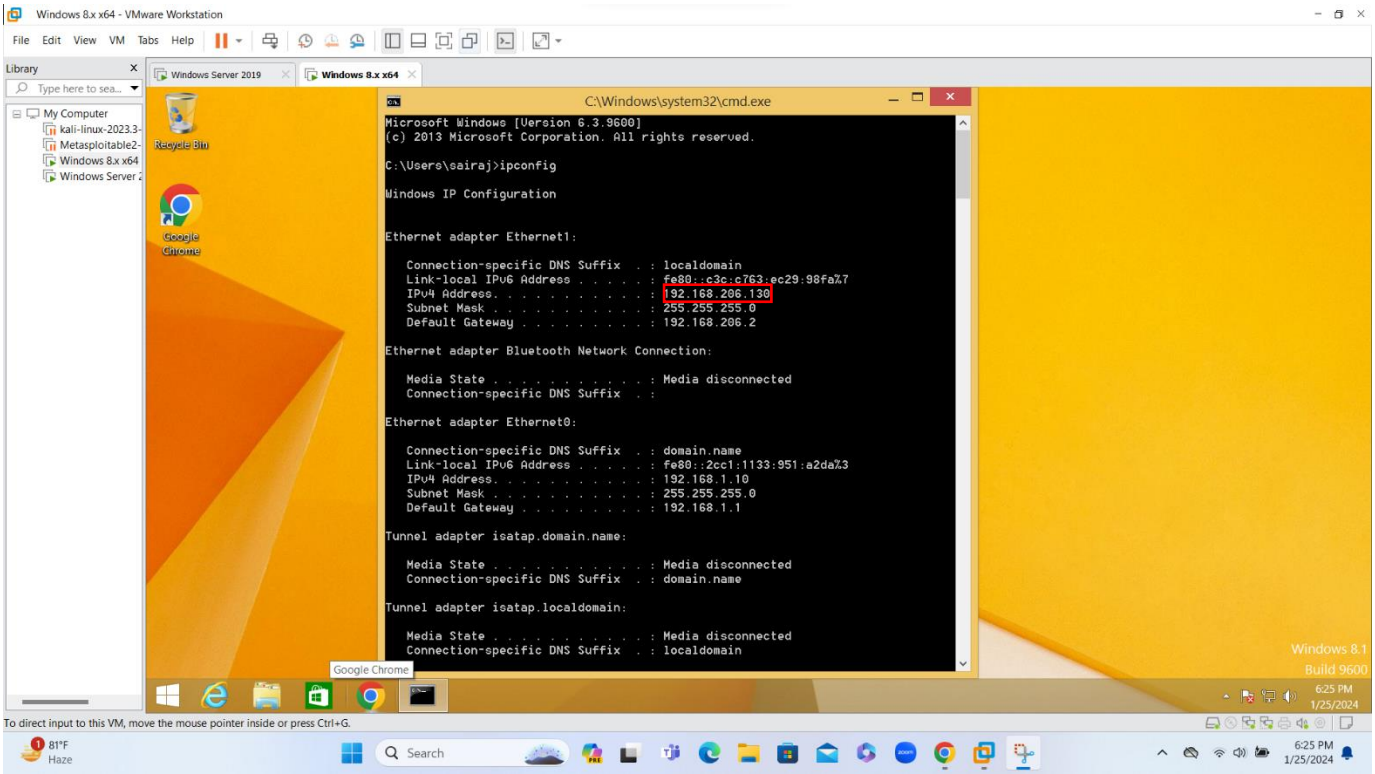
- ✓ NetBIOS is network basic input output system.
- ✓ Basically, it will allow separate computer to communicate with each other over a network.
- ✓ It allows different applications information to different computer {or}
- ✓ It allows a particular application on different computer in network to communicate each other
- ✓ Like Files, printer on the same network.
- ✓ NetBIOS had 16 characters
    - First 15 characters occupies the device name or machine name
    - 16 characters occupies the service information.
- ✓ Attackers use the NetBIOS enumeration to obtain:
    - List of computers that belong to a domain
    - List of shares on the individual hosts on the network
    - Policies and passwords

Objective: 01

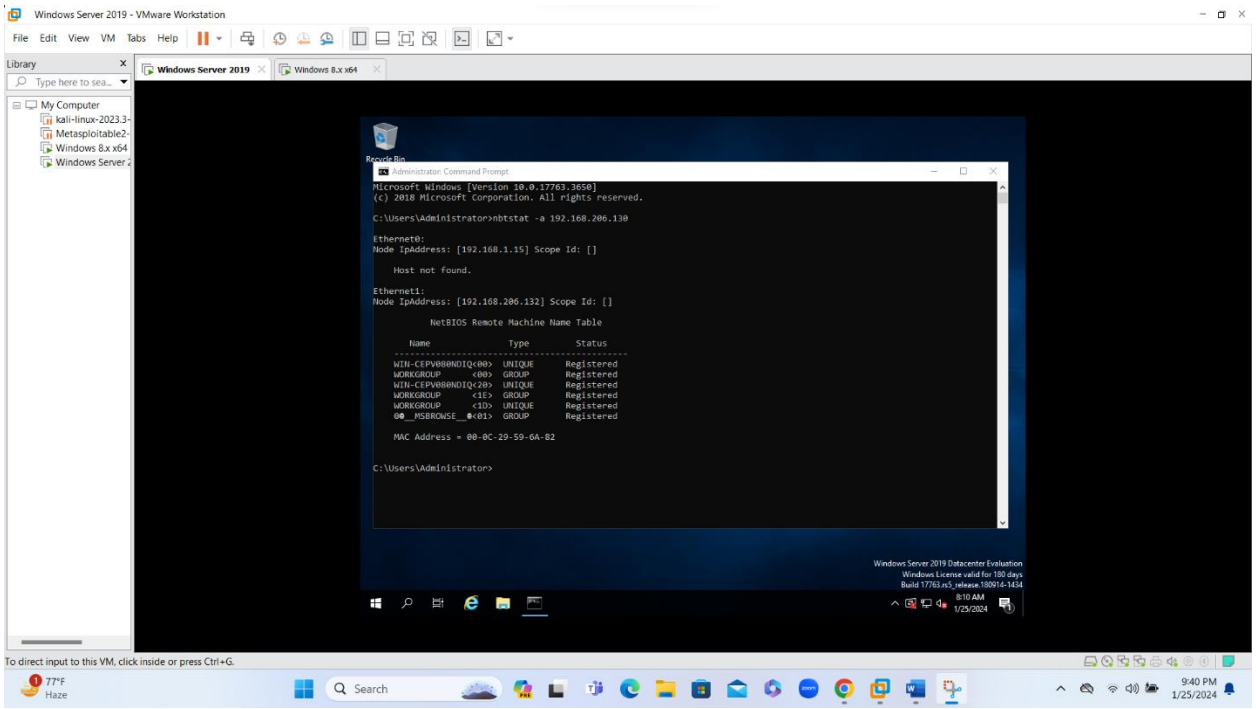
Perform NetBIOS enumeration using Windows command-line utilities

- ❖ In order to complete the lab objectives, I have setup the lab environment with VMware and installing both Windows Server 2019 VM and Windows 8 VM.
- ❖ After the setup of Windows 8 VM, the next step to identifying the IP address of the Windows 8 VM
- ❖ So to identify the IP of windows 8 VM open the command prompt and executed the command **"ipconfig"** to reveal the IP
- ❖ The IP address of windows 8 VM is **192.168.206.130**

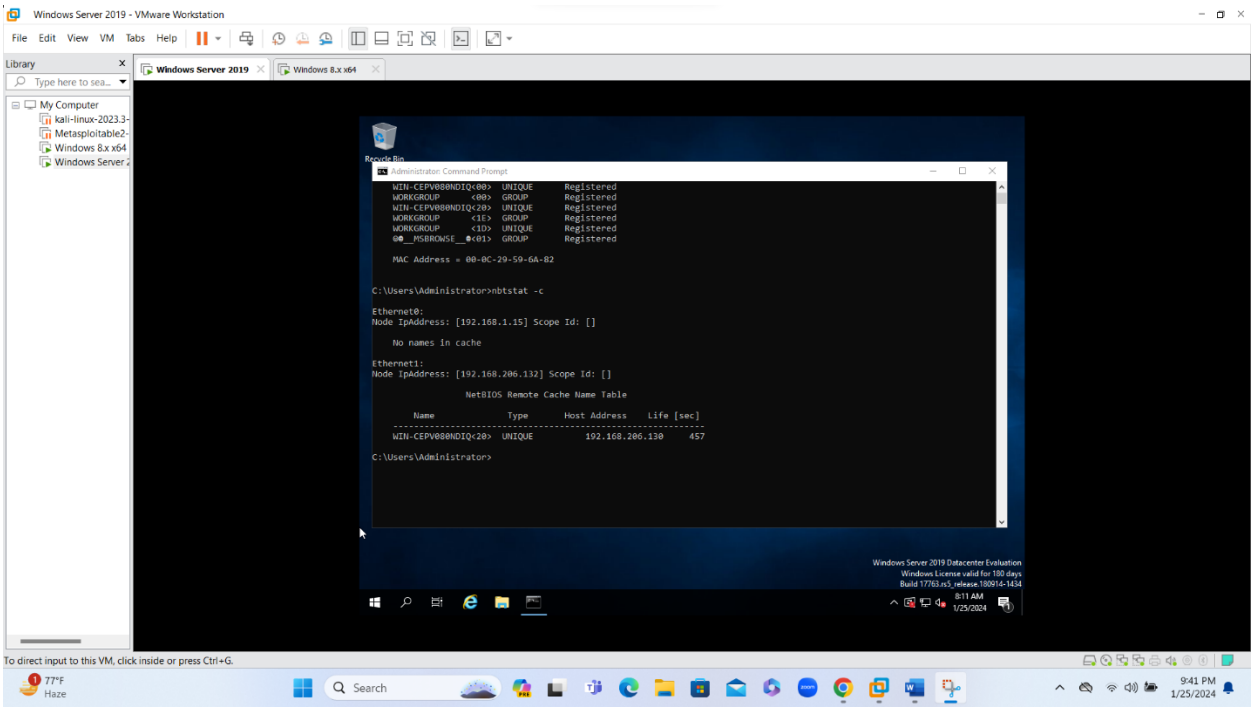

Windows Server 2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Windows Server 2019
Windows 8.x x64
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Recycle Bin
Windows Server 2019 Datacenter Evaluation
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
4:53 AM
1/25/2024
To direct input to this VM, click inside or press Ctrl+G.
81°F
Haze
Search
6:23 PM
1/25/2024


Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Windows Server 2019
Windows 8.x x64
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Recycle Bin
Google Chrome
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\sairaj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet1:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::c3c:c763:ec29:98fa%7
IPv4 Address. . . . . : 192.168.206.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.206.2
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : domain.name
Link-local IPv6 Address . . . . . : fe80::2cc1:1133:951:a2da%3
IPv4 Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Tunnel adapter isatap.domain.name:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : domain.name
Tunnel adapter isatap.localdomain:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Google Chrome
Windows 8.1
Build 9600
6:25 PM
1/25/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
81°F
Haze
Search
6:25 PM
1/25/2024

- After knowing the IP of the Windows 8 VM, I switched to the Windows server 2019 VM and opened the command prompt.
- In the command prompt, then I performed the **nbtstat -a 192.168.206.130** command.
- This allowed me to view the NetBIOS name tables associated with the remote computer.



- In the same command prompt window, I performed **"nbtstat -c"** command to list the name cache of the NetBIOS.
- This action revealed the content of the NetBIOS name cache.

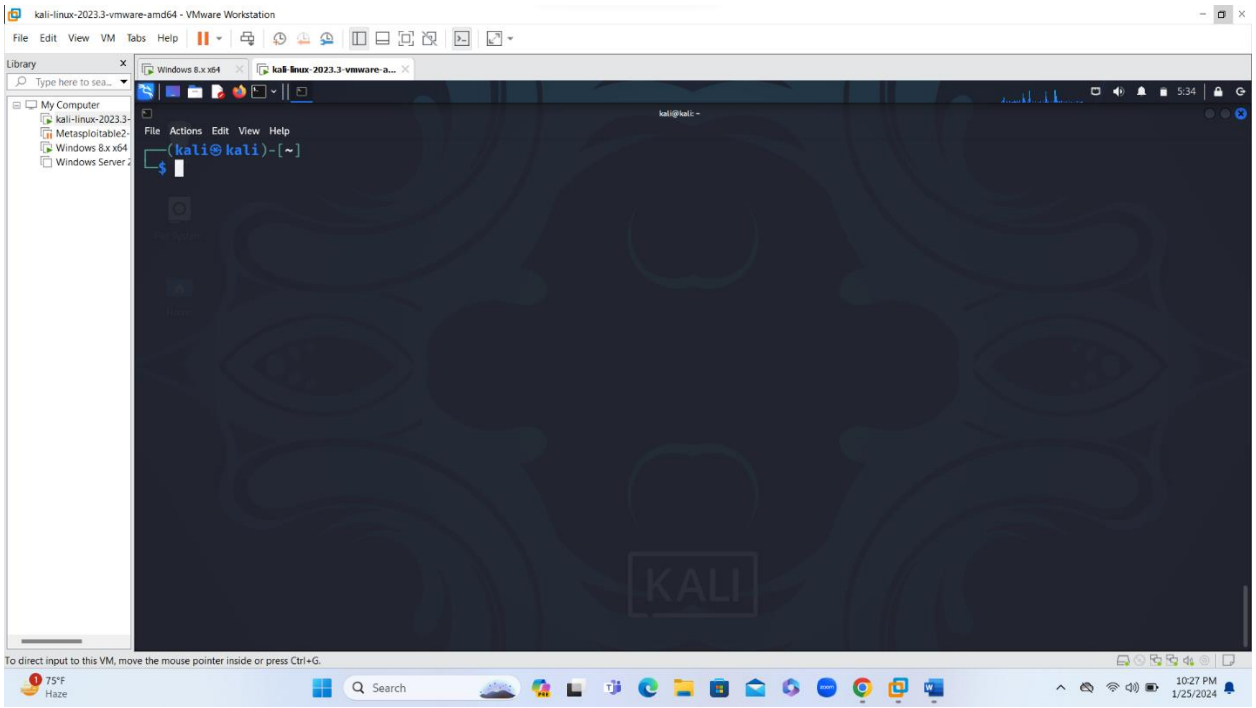


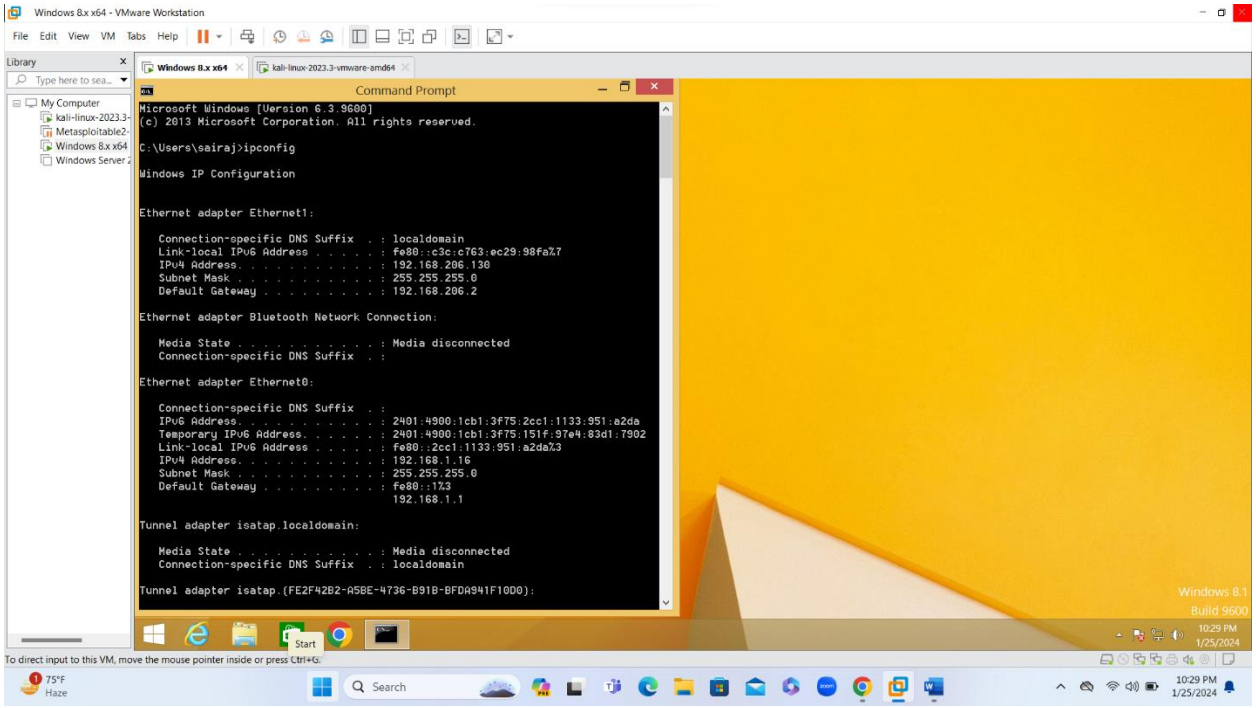
- In summary, this assignment demonstrated the process of performing NetBIOS enumeration using Windows command line utilities, primarily the 'nbtstat' command, enabling a clear understanding of the NetBIOS name tables and cache of the remote computer.

Objective: 02

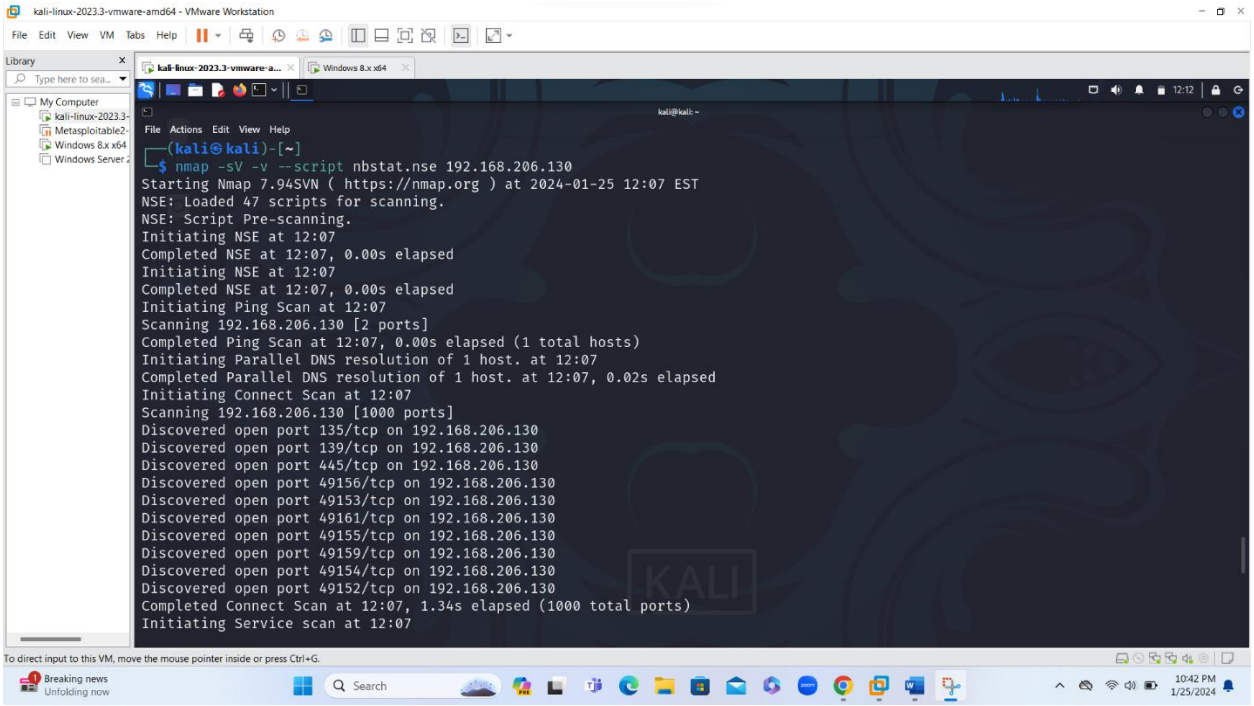
Perform NetBIOS enumeration using an NSE Script

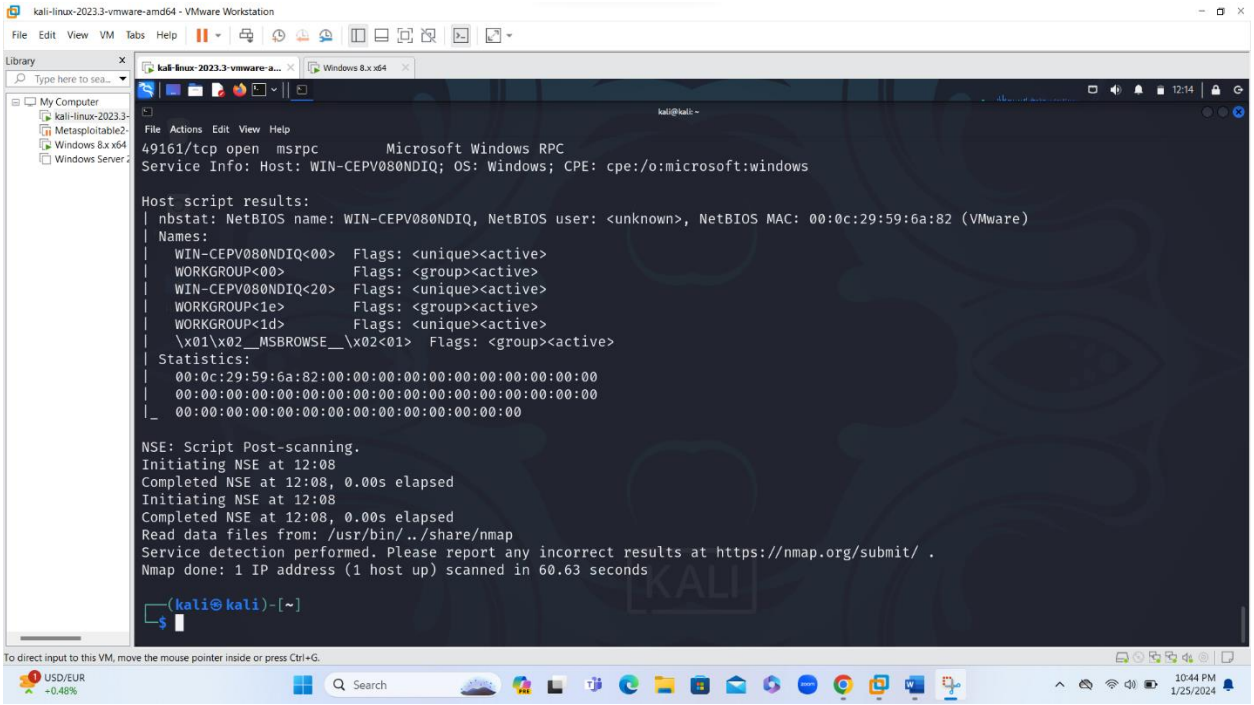
- To perform the Objective, I have opened VMware and launched both Kali VM and windows 8 VM.
- Next, I opened the command prompt in windows 8 VM and performed **"ipconfig"** command to determine its IP address, which the result is **198.168.206.130**


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Windows 8.x x64
kali-linux-2023.3-vmware-a...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
75°F
Haze
Search
10:27 PM
1/25/2024

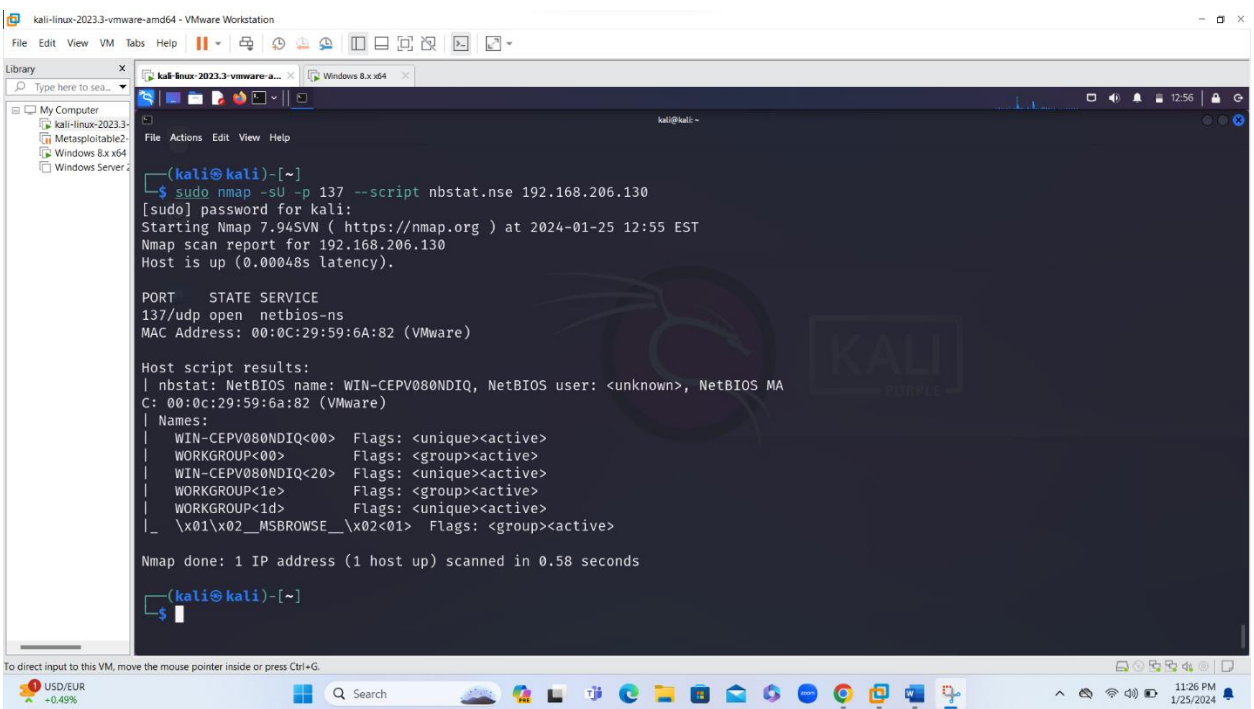

Windows 8.x x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows 8.x x64
Windows Server 2
Windows 8.x x64
kali-linux-2023.3-vmware-amd64
Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\sairaj>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet1:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::e3c:c763:ec29:98fa%7
IPv4 Address. . . . . : 192.168.206.130
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.206.2
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2401:4900:1cb1:3f75:2cc1:1133:951:a2da
Temporary IPv6 Address. . . . . : 2401:4900:1cb1:3f75:151f:97e4:83d1:7902
Link-local IPv6 Address . . . . . : fe80::2cc1:1133:951:a2da%3
IPv4 Address. . . . . : 192.168.1.16
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::1%3
192.168.1.1
Tunnel adapter isatap.localdomain:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
Tunnel adapter isatap.{FE2F42B2-A5BE-473G-B91B-BFDA941F10D0}:
Start
Windows 8.1
Build 9600
10:29 PM
1/25/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
75°F
Haze
Search
10:29 PM
1/25/2024

- After knowing the IP address, I moved to Kali VM and opened the terminal. And executed the command **“nmap -sV -v --script nbstat.nse 192.168.206.130”.**
- In this commands ‘-sV’ signified a version and ‘-v’ provided verbosity
- Here, I specified all the open ports of the IP address and ran all available NetBIOS scripts using **“--script nbstat.nse”** command.
- The result provided detailed information about the target, including the NetBIOS name, NetBIOS user, MAC address.





❖ And next I have performed UDP scan with the command **"sudo nmap -sU -p 137 –script nbstat.nse"**



- After the performing the UDP scan one port has been open and including the NetBIOS name, NetBIOS user, MAC address.

- In summary, this assignment demonstrated the process of performing NetBIOS enumeration using NSE scripts, enabling a clear understanding of the NetBIOS name tables and cache of the remote computer

Submitted By
Sairaj Mothukuri
[sairajmothukuri28@gmail.com]