CEH Module 4: Enumeration
Assignment - 02
(Marepalli Rakesh)

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

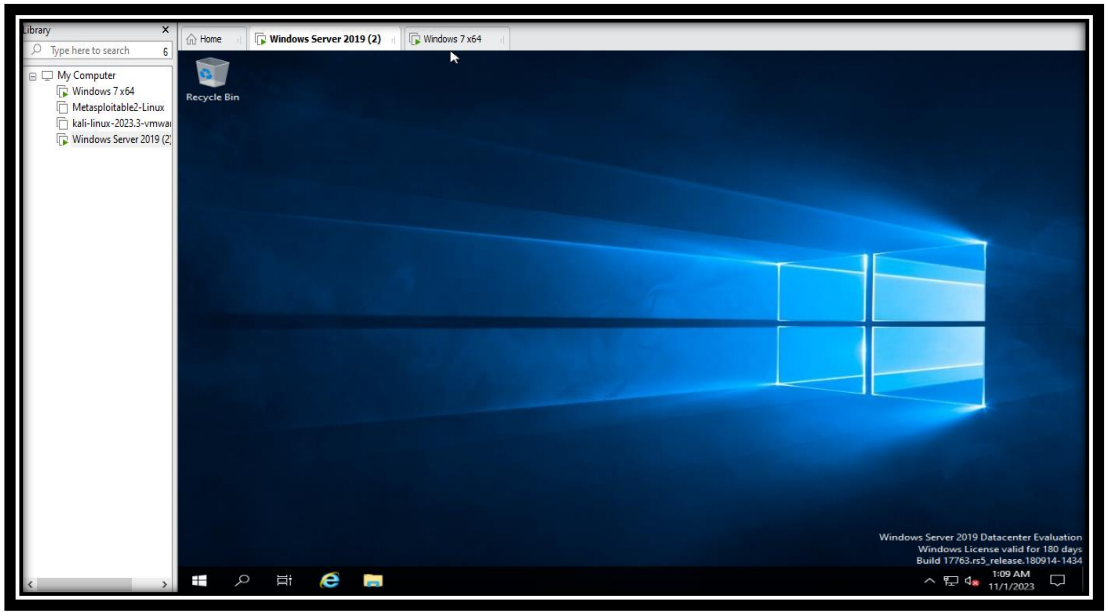
NetBIOS Enumeration:

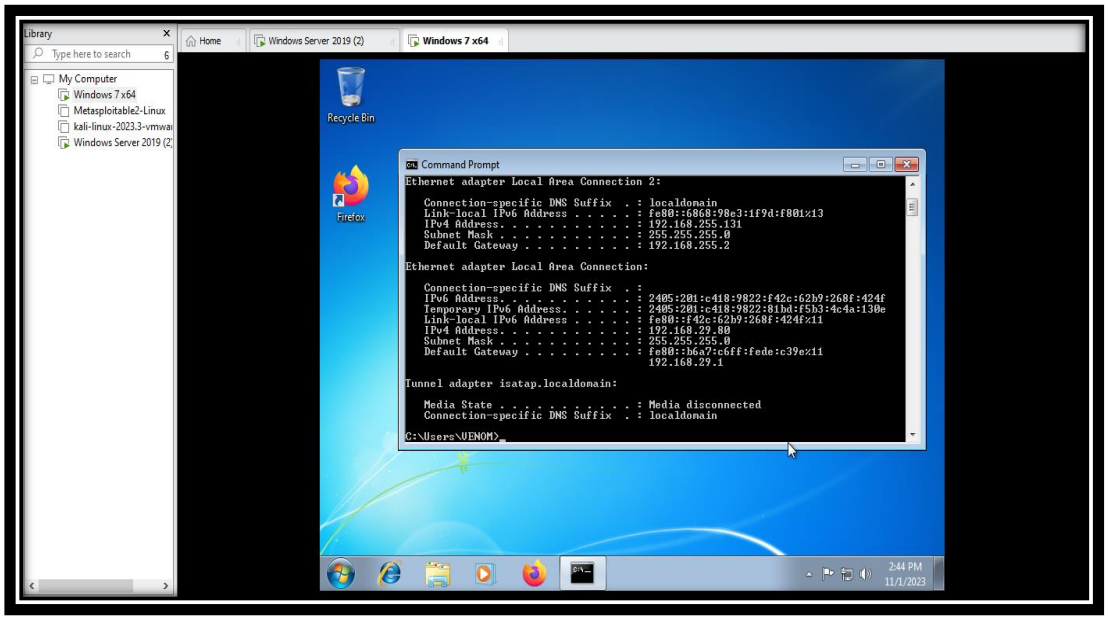
- NetBIOS is an acronym that stands for Network Basic Input Output System. It enables computer communication over a LAN and the sharing of files and printers. TCP/IP network devices are identified using NetBIOS names (Windows).
- An attacker who discovers a Windows OS with port 139 open can investigate what resources are accessible or viewable on the remote system. To enumerate the NetBIOS names, the remote system must have file and printer sharing enabled. Depending on the availability of shares, NetBIOS enumeration may allow an attacker to read or write to the remote computer system or launch a (Dos).
- 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

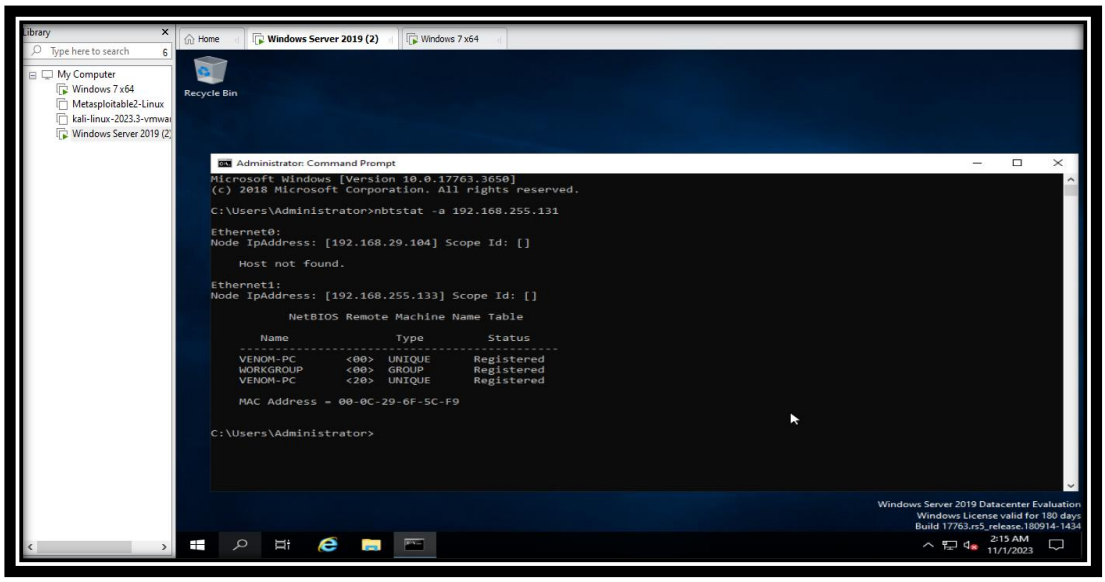
Perform NetBIOS enumeration using Windows command-line utilities

- In order to accomplish this, I set up the necessary environment within VMware, launching both a Windows Server 2019 VM and a Windows 7 VM. The initial step involved identifying the IP address of the Windows 7 VM, which was crucial for subsequent actions. After switching to the Windows 7 VM and opening the Command Prompt, I executed the '**ipconfig**' command to reveal that the IP address of the Windows 7 VM was 192.168.255.131.

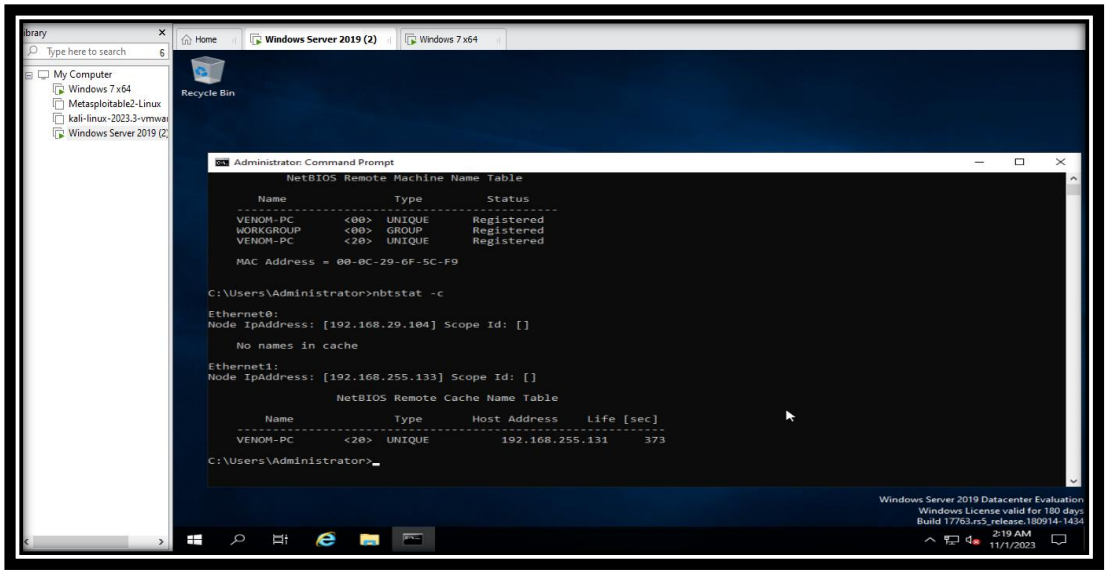




- Following this, I switched to the Windows Server 2019 VM and opened the Command Prompt. In the Command Prompt, I initiated the retrieval of NetBIOS name tables of the remote Windows 7 VM using the **nbtstat -a 192.168.255.131** command. This allowed me to view the NetBIOS name tables associated with the remote computer.



- In the same Command Prompt window, I proceeded to list the contents of the NetBIOS name cache of the remote computer with the **'nbtstat -c'** command. This action revealed the contents of the NetBIOS name cache, comprising a comprehensive table of NetBIOS names and their corresponding resolved IP addresses.

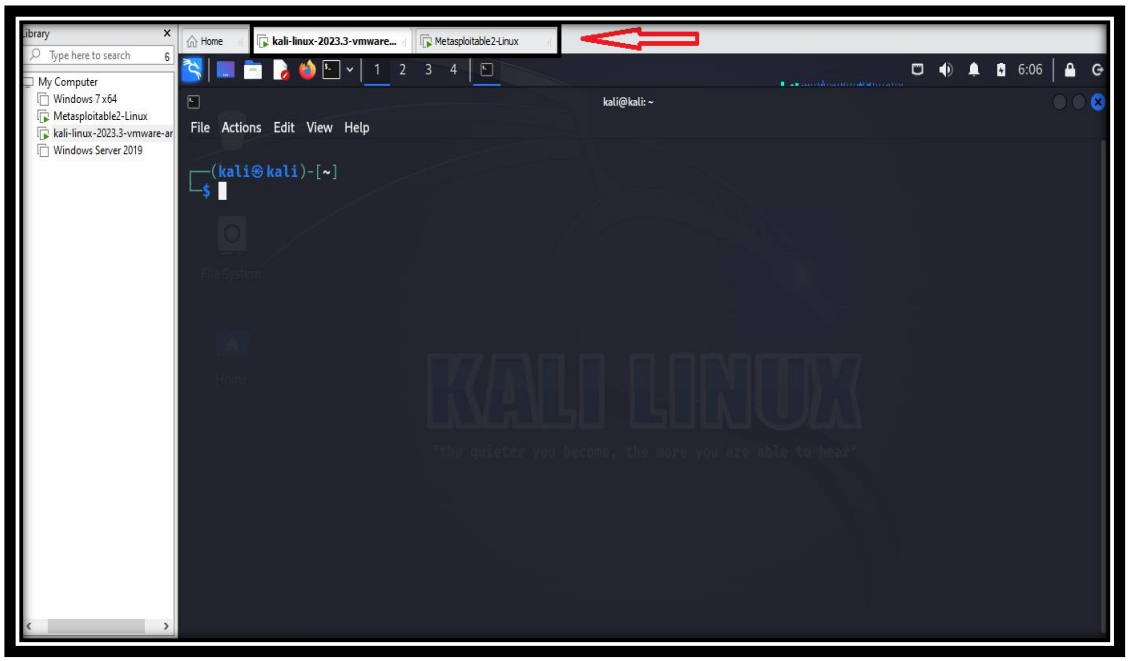


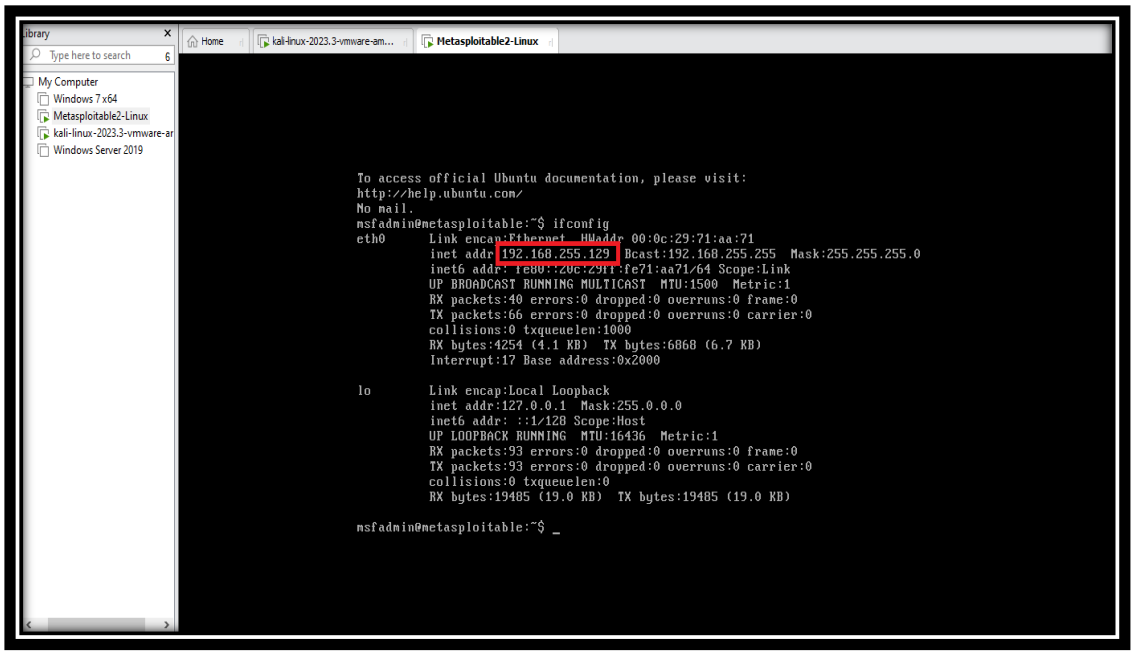
- In summary, this assignment demonstrated the process of performing NetBIOS enumeration using Windows command line utilities, primarily the 'nbtstat' command, enabling a clear understanding of the NetBIOS name tables and cache of the remote computer.

Objective: 02

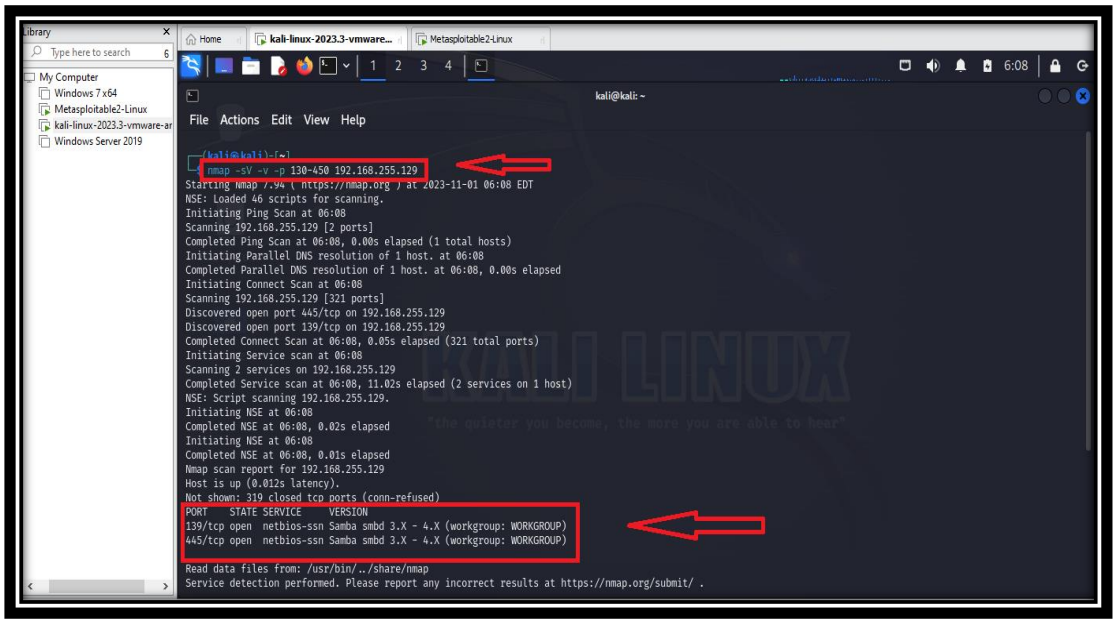
Perform NetBIOS enumeration using an NSE Script

- To start, I opened VMware and launched both the Kali VM and the Metasploitable VM. Afterward, I switched to the Metasploitable VM and used the 'ifconfig' command to determine its IP address, which was found to be 192.168.255.129.

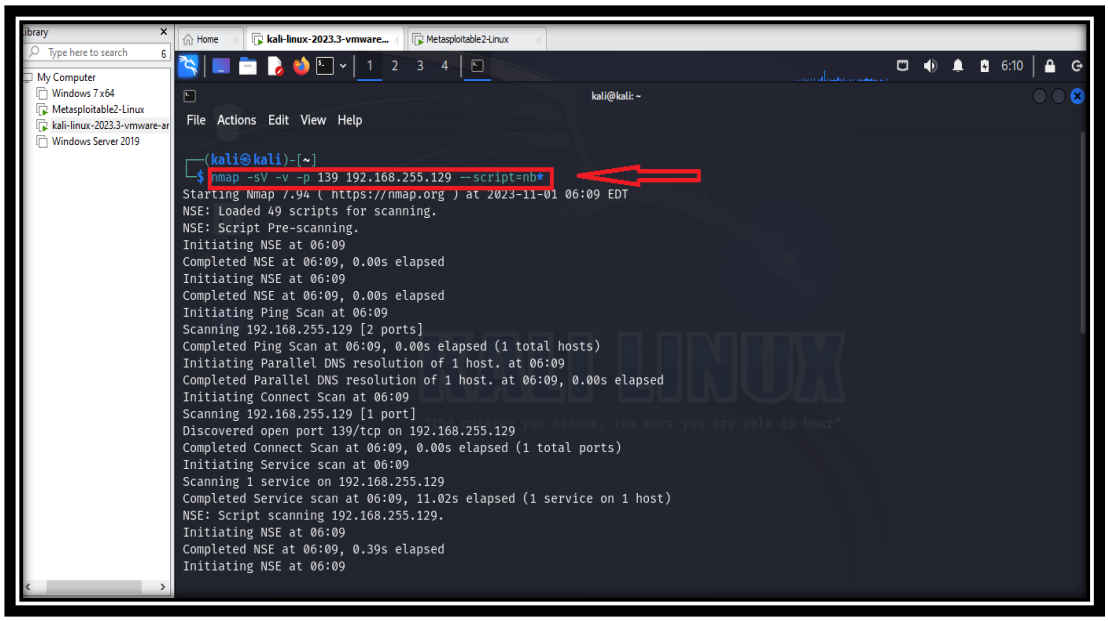


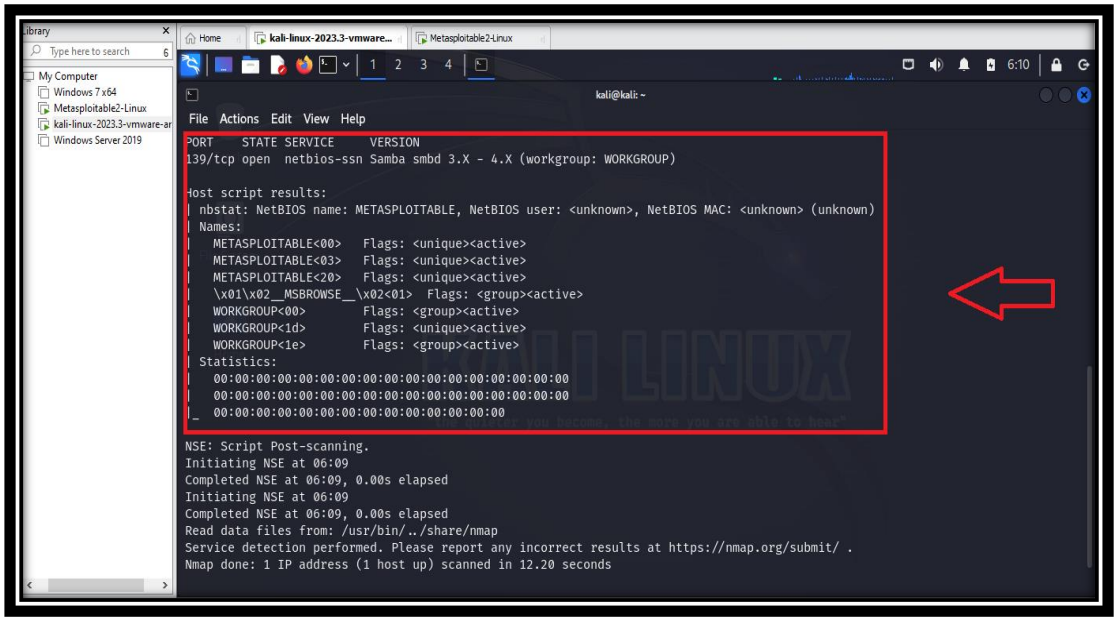


- Next, I moved to the Kali VM and opened a terminal. I executed the command **nmap -sV -v -p 130-450 192.168.255.129**. In this command, '-sV' signified a version scan, '-v' provided verbosity, and '-p' allowed me to specify a range of ports. I focused on ports 130 to 450, as NetBIOS typically runs on ports 139 or 445. Scanning this specific range, rather than the entire spectrum, saved time. The results displayed open ports along with their associated versions. It was confirmed that both ports 139 and 445 were open, running NetBIOS services.



- Continuing with the enumeration process, I utilized the command **nmap -sV -v -p 139 192.168.255.129 --script=nb***. Here, I specified port 139 and ran all available NetBIOS scripts using the '--script=nb*' parameter. The results provided detailed information about the target, including the NetBIOS name, NetBIOS user, and MAC address.
- If the UDP port had been open, I could have performed a UDP scan with the command **nmap -sU -v -p 139 192.168.255.129 --script=nb***. However, in my case, the UDP port was closed.





- 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

Marepalli Rakesh

(Marepalli.rakesh@gmail.com)