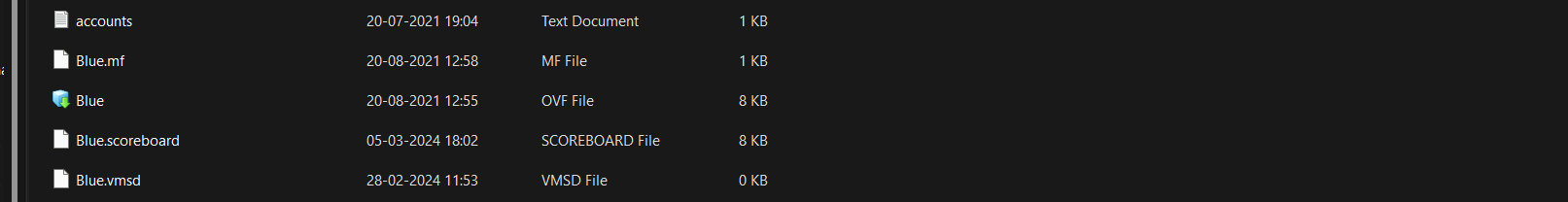
ATTACK ON WINDOWS MACHINE

(BLUE)

INTRODUCTION:

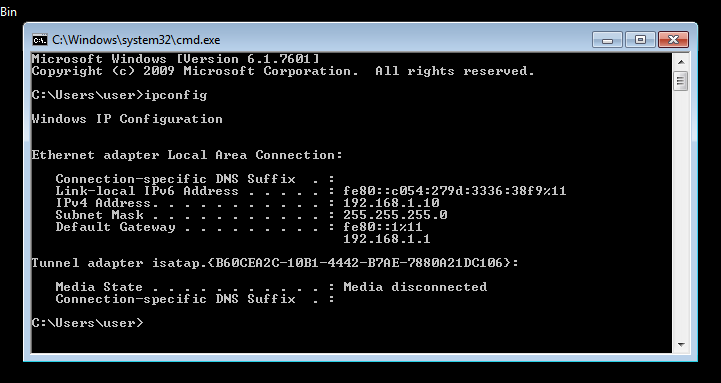
This report is about get remote access to a windows system from a kali linux machine. This machine get remote access to windows user and get exploit to administrator on the machine. The final result on the project is to get remote access to the windows machine by ms17-010 exploit. Thus further details about ms17-010 exploit. MS17-010 is a security vulnerability in Microsoft's implementation of the SMB (Server Message Block) protocol. SMB is a network file sharing protocol that allows applications to read and write to files and request services from server programs in a network. This vulnerability was discovered by the NSA (National Security Agency) and leaked by a group called The Shadow Brokers in April 2017.The MS17-010 vulnerability affects multiple versions of Microsoft Windows operating systems, including Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016. It allows an attacker to execute arbitrary code on the target system, potentially taking control of the system, by sending specially crafted packets to the SMB server.Exploiting this vulnerability typically involves sending a crafted packet to the SMB server, causing a buffer overflow or other memory corruption, which can then be leveraged to execute malicious code. Once exploited, an attacker could install malware, steal data, or perform other malicious actions on the compromised system.The MS17-010 exploit became infamous due to its involvement in the WannaCry ransomware attack that occurred in May 2017. WannaCry leveraged this vulnerability to spread rapidly across networks, encrypting files on infected systems and demanding ransom payments in exchange for decryption keys.Microsoft released security patches to address the MS17-010 vulnerability shortly after its disclosure. It's crucial for users and organizations to apply these patches promptly to protect their systems from potential exploitation. Additionally, network administrators can implement other security measures, such as firewall rules and network segmentation, to mitigate the risk of SMB-related attacks.

STEP 1:



* Download Blue zip file and extract it by using winrar.
* Create a virtual machine Blue in VMware and open it.
* Browse a storage path to open OVF file of the virtual machine in your pc
* Then open it with the given login password from password.txt file.

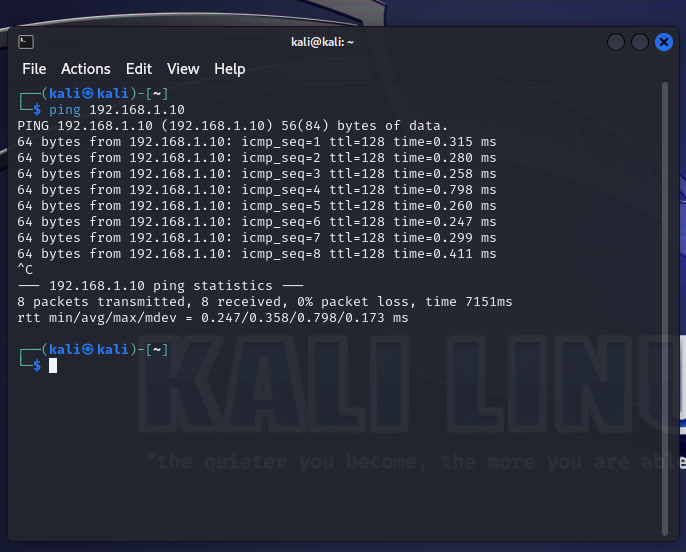
STEP 2:



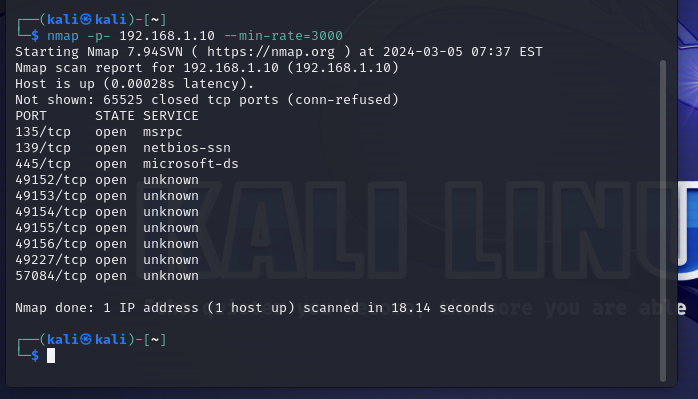
* Open the ipconfig in command prompt of windows machine to know the ipv4 Address of that machine.
* Simultaneously open your kali machine with your login credinals.

STEP 3:

* Ping windows machine from your kali machine.
* Before that ensure both kali machine and the target windows machine need to be connected in a same network.
* Once they both are connected in same network ping them.
* After some time stop the ping process by using Crtl+C.



STEP 4:



* Now use nmap to scan the available ports on the target machine.
* Use command nmap -p- 192.168.1.10 –min-rate=3000.
* This command represents

nmap: This is the command-line utility for network discovery and security auditing.

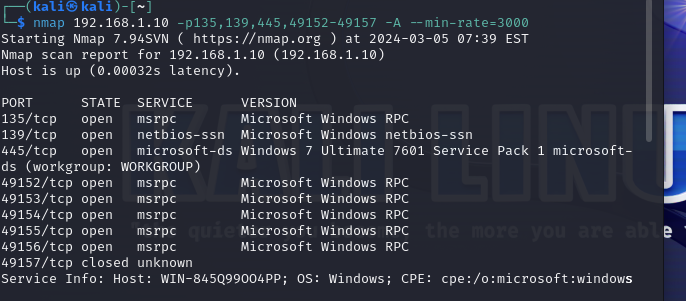
-p-: This option tells Nmap to scan all 65535 TCP ports. The hyphen (-) indicates a range from port 1 to port 65535.

192.168.1.10: This is the target IP address that Nmap will scan.

--min-rate=3000: This option sets the minimum rate of packets sent per second during the scan. In this case, it's set to 3000 packets per second. This can help speed up the scan but may also increase network traffic and raise suspicion if done on networks where scanning activity is monitored.

* Finally it show the number of ports which are open on the target machine.

STEP 5:



* Now use the command nmap again to open the ports that are scanned by this time only open the specific port that are scanned.
* The command nmap 192.168.1.10 -p135,139,445,49152-49157 -A –min-rate=3000.
* It represents

nmap: This is the command-line utility for network discovery and security auditing.

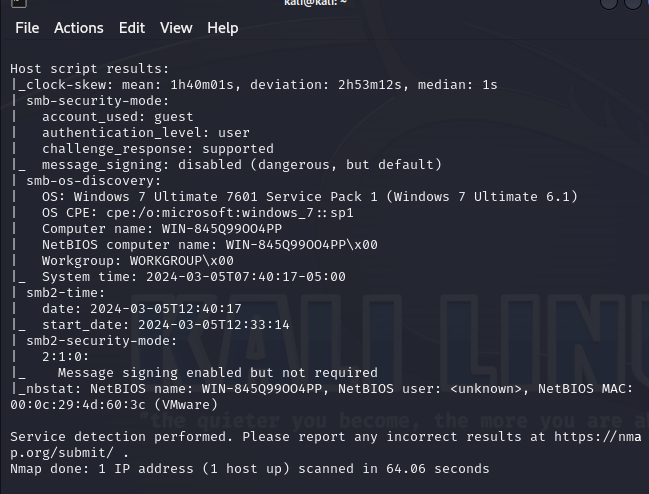
192.168.1.10: This is the target IP address that Nmap will scan.

-p135,139,445,49152-49157: This option specifies a specific list of TCP ports to scan. Ports 135, 139, 445, and the range from 49152 to 49157 will be scanned.

-A: This option enables aggressive scanning, which includes service version detection, OS detection, script scanning, and traceroute.

--min-rate=3000: This option sets the minimum rate of packets sent per second during the scan.

* Now the ports and their services will be open after this command.



STEP 6:

* The step to explore is there any vulnerability in the target machine.
* So use the command sudo nmap -sV –script vuln 192.168.1.10.
* The command represents

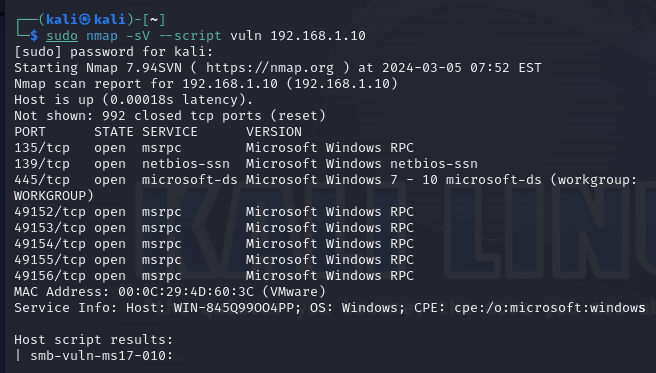
sudo: This command is used to execute the subsequent command with superuser privileges, which may be necessary for certain operations, especially when performing network scans.

nmap: This is the command-line utility for network exploration and security auditing.

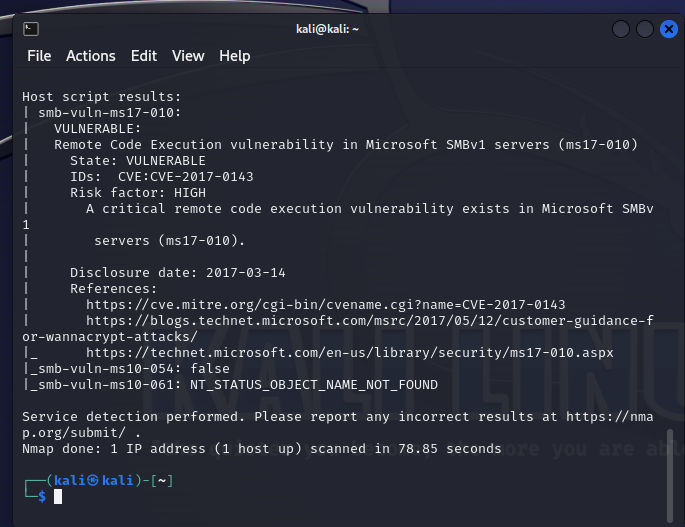
-sV: This option instructs Nmap to perform service version detection. Nmap will attempt to determine the versions of services running on open ports by analyzing their responses to specific probes.

--script vuln: This option specifies that Nmap should run vulnerability scripts against the target. Nmap has a collection of scripts designed to detect known vulnerabilities in various services and applications.

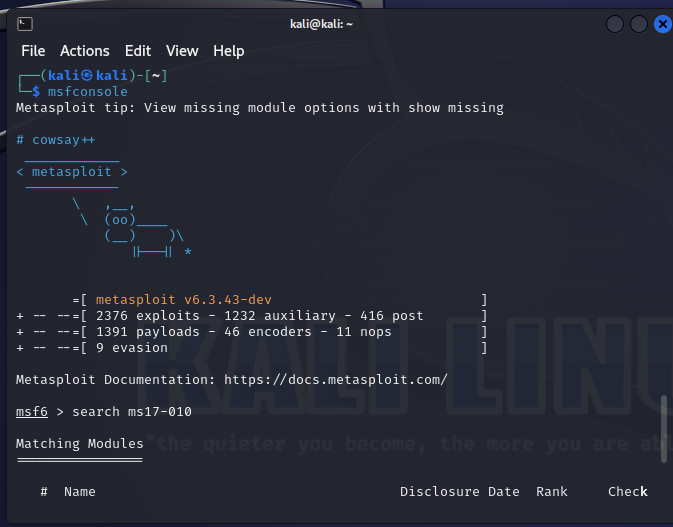
192.168.1.10: This is the target IP address that Nmap will scan for vulnerabilities.



* Now the command shows there is ms17-010 vulnerability found on the target machine.
* This command confirm that attack can be further continue as it have ms17-010 vulnerability in the machine.
* Exploiting this vulnerability typically involves sending a crafted packet to the SMB server, causing a buffer overflow or other memory corruption, which can then be leveraged to execute malicious code. Once exploited, an attacker could install malware, steal data, or perform other malicious actions on the compromised system.
* In this report I have use metasploit to exploit the vulnerability.

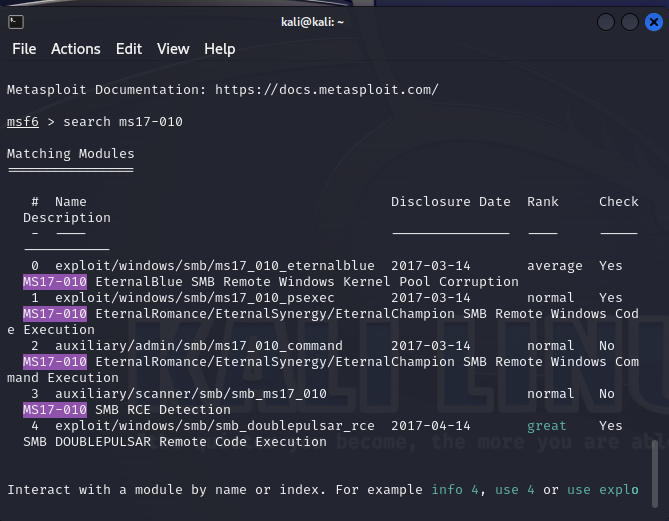


STEP 7:



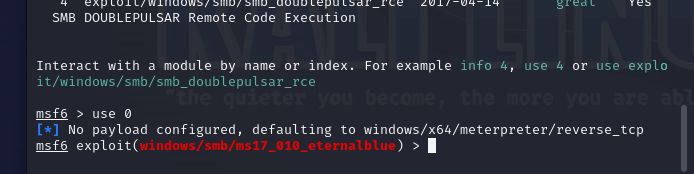
* Use msfconsole in your linux to trigger Metasploit and explore more on ms17-010 vulnerability.

STEP 8:



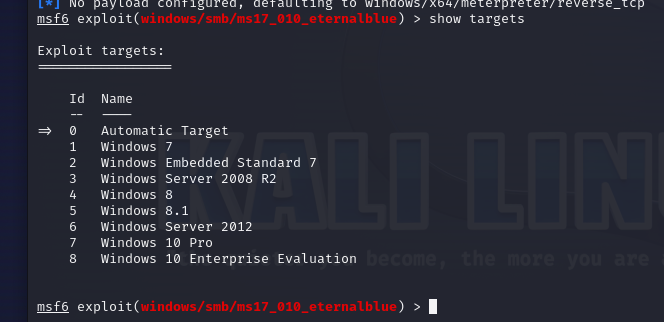
* Search ms17-010 on msf6 to find the machines with that vulnerability.
* Then it is found that eternal blue (Target machine) is available on the matching modules.

STEP 9:



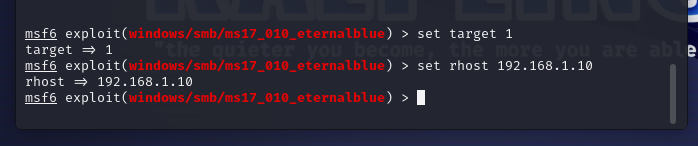
* Now use 0 which shows the target machine that we need to be exploit by using meta sploit.

STEP 10:



* Use command show targets it will display available machines on that eternal blue.

STEP 11:



* Set target 1 (because the target machine is windows 7)
* Set RHOST with target machine ip.

STEP 12:

* Now use exploit command.
* This command now made remote access of target machine in your attacker machine.
* By now we can explore all the files available in the windows (Target machine).



STEP 13:

* Now use command ls ‘C:\Users’ it display all the files in C disk of the target machine
* Here we found Administrator and user files with remote access.

