

Lab 5: Searchsploit and MSF Basics

Preliminaries

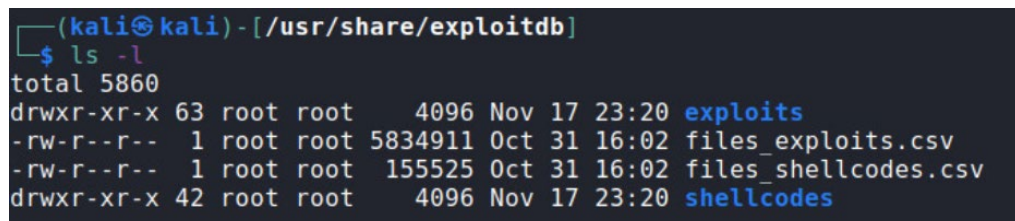
Refer to Lecture slides in Week 5.

Tasks

Turn on Kali VM and Metasploitable2 VM. Log into Kali VM, and start a terminal. Then, complete the following tasks. Write your answers for all questions to your lab report.

1. The 'searchsploit' command.

- 1.1 In a Kali terminal, enter a sequence of commands to achieve a screenshot similar to the one below. Write your sequence of commands into your report.



```
(kali㉿kali) - [/usr/share/exploitdb]
$ ls -l
total 5860
drwxr-xr-x 63 root root 4096 Nov 17 23:20 exploits
-rw-r--r-- 1 root root 5834911 Oct 31 16:02 files_exploits.csv
-rw-r--r-- 1 root root 155525 Oct 31 16:02 files_shellcodes.csv
drwxr-xr-x 42 root root 4096 Nov 17 23:20 shellcodes
```

- 1.2 Examine the contents of files_exploits.csv with a text editor such as nano, vi, mousepad, etc.
- General knowledge: what is a csv file? (You can google this)
 - What are contained in the first line of files_exploits.csv?
 - What is the purpose of files_exploits.csv? (please give an educated guess based on its contents)
- 1.3 Explore what is contained in the directory 'exploits'.
- Name three directories under the directory 'exploits'
 - Name three directories under the directory 'exploits/windows'
 - Look at the content of the Python file 'exploits/windows/local/10240.py'. According to the comments in this file, which computer program it is used to exploit?
- 1.4 Suppose you want to search for exploits from the local installation of exploit-db at Kali to attack the FTP server program VSFTPD version 2.3.2.
- What is your command line for this?
 - Include a screenshot on the output of your command line.
 - Which exploit from the output you will select?
- 1.5 The exploit code you choose in Task 1.4 should be 'exploits/linux/dos/16270.c'. Copy this file to '/home/kali/Downloads' directory for possible use in future.
- Write your commands to achieve this into your lab report. (Hint: studying the 'cp' command in Linux)
 - Include a screenshot to prove that '16270.c' is now under the 'home/kali/Downloads' directory.

2. MSF: attacking VSFTPD 2.3.4 (NB: different version number from Task 1.4).

2.1 The GVM report for Metasploitable2 obtained last week shows the 'vsftpd Compromised Source Packages Backdoor Vulnerability' on TCP port 21.

- a) According to the report, what is the CVSS score for this vuln?
- b) Which section in the vuln details reveals the vsftpd version number affected by this vuln?

2.2 Follow the 'VSFTPD' section in the following blog article: <https://tehaorum.wordpress.com/2015/06/14/metasploitable-2-walkthrough-an-exploitation-guide/> to exploit this vuln.

- a) Include every step with the command lines involved into your lab report.
- b) Include a screenshot on your success. This screenshot should include the results of executing the following commands: 'id' and 'hostname'.

Note: if the web link above doesn't work, please refer to the exploitation guide pdf accompanying this lab spec on vUWS.

Hint: You should set payload and options as shown in the blog before executing 'exploit' or 'run'.

3. MSF: attacking Unreal IRC daemon.

3.1 Follow lecture slides to conduct this attack. The difference is that you should set the 'cmd/unix/reverse_perl' as the payload instead.

- a) Include every step with the command lines involved into your lab report.
- b) Include a screenshot on your success. This screenshot should include the results of executing the following commands: 'whoami' and 'ip a show dev eth0'.

Hints:

- You need to set both the RHOSTS option and the LHOST option. For RHOSTS, you should give the IP address of the target; for LHOST, you should give the IP address of the attacker machine.
- To quit the gained shell, you should hit Ctrl+c.

3.2 Repeat the above attack, but set the 'cmd/unix/reverse' as payload this time.

- a) Include every step with the command lines involved into your lab report.
- b) Include a screenshot on your success. This screenshot should include the results of executing the following commands: 'whoami' and 'ip a show dev eth0'.

Last but very important: First shutdown and then power off all your three VMs. Our school's cloud is under heavy load, as you can see your VMs may not respond to you quickly. Therefore, if you are not using them, you should have them shutdown and power off.