OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 3

Katelynn Johnson

UIN 01108787

Spring 2019

1 SUMMARY

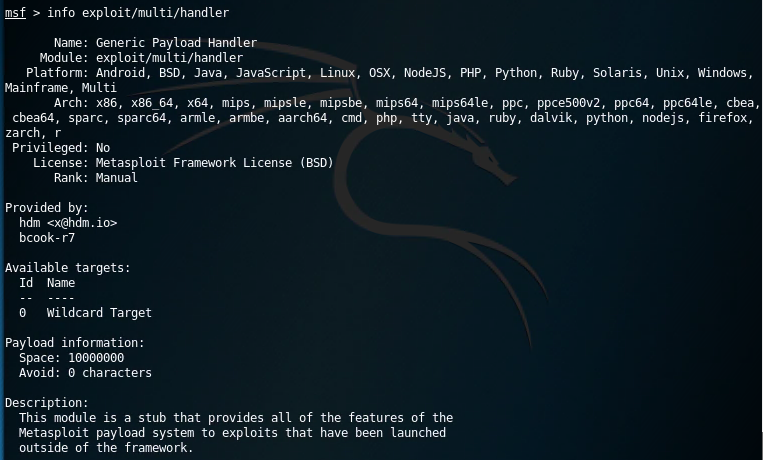
In this module I learned about computer vulnerabilities and ways to take advantage of a host’s vulnerabilities. In order to discover what vulnerabilities a host may have, first, an Nmap scan is run. Running an Nmap scan tells you what ports are open, what services are running on those ports, and version of the services running on those ports. Next is to find exploits associated with services. This is done by using the Metasploit Framework to search for exploits and payloads that will capitalize on the vulnerability of your choosing.

In order for an exploit to work it must have a payload added to it. An exploit by itself is just a way that the payload is delivered. This means that the payload does the actual damage to the system (in our case creating sessions that connect to the target host remotely) the exploit is just a way to get it to the target host. In Metasploit there are three types of payloads, *Singles, Stagers,* and *Stages. Singles* are payloads that are completely standalone payloads. *Stagers* are payloads set up a network connection between the attacker machine and the target victim. *Stages* are payloads components that are downloaded by Stagers modules.

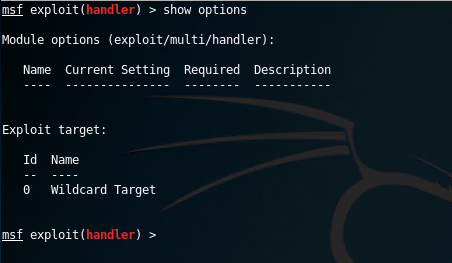
Also in this module, we learned about a reverse shell payload. This type of payload is one that requires the attacker to set up a listener on their host. Next the victim will connect to the attacker’s listener (unknowing). Then the attacker receives a shell on the target machine. This type of attack is good when the target machine is behind a firewall and will block an attacking machine to connect to the victim. In this attack, the victim is that one who connects to the attacking machine with an outward connection, (unlike most attacks where the attacker attempts to connect to its victim).

We also covered what an attacker could do whenever a remote connection is made to the victim. Once a session is made, the attacker is remotely connected to the victim. This means the attacker can access the victim machine as if the attacker was directly logged into the victim’s machine. Depending on the privileges that the attacker has on the victim’s machine, an attacker can do anything that they want to do. Some examples of what an attacker could do include taking a screen shot of the victim’s current desktop, logging the victim’s keystrokes, creating users for the victim’s machine, collect the host’s information to include host name, IP address etc.

2 SCREENSHOTS

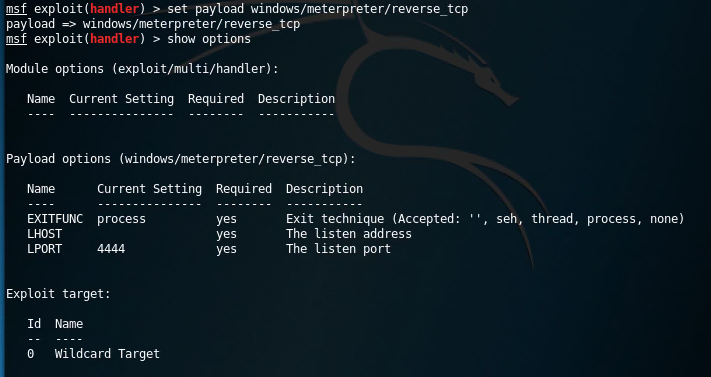
Command: info exploit/multi/handler

Command: show options



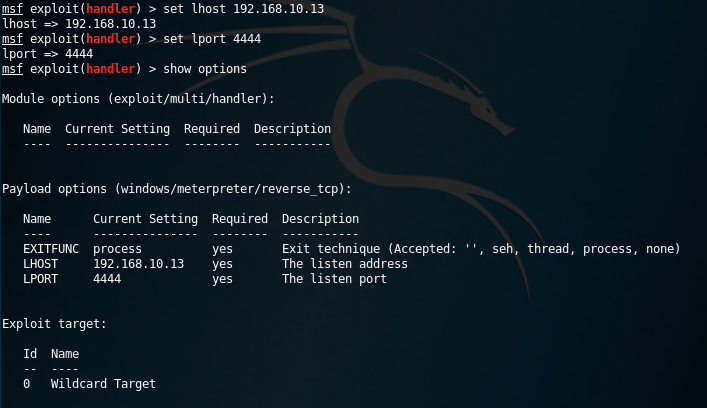
After the windows/meterpreter/reverse\_tcp is added as a payload to handler

Command: show options

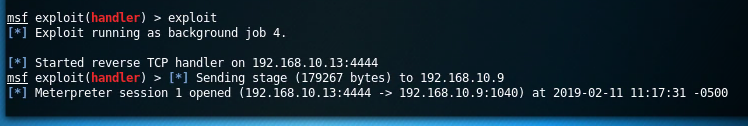


After lhost and lport are set

Command: show options

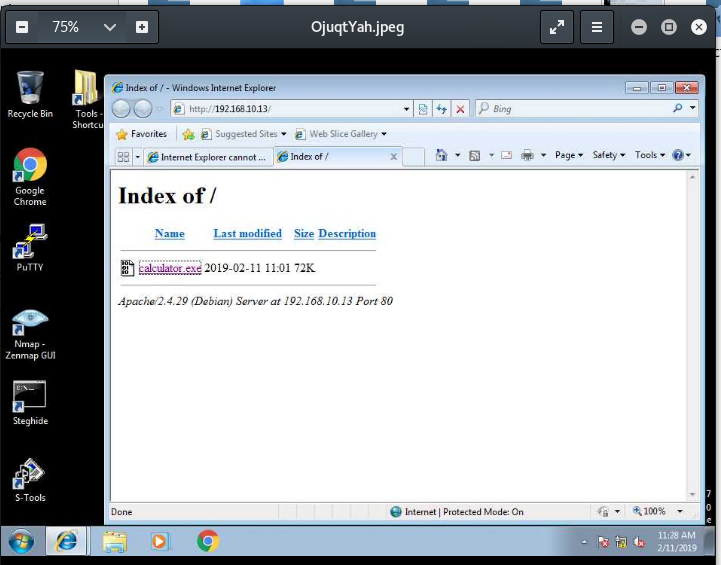


After I opened up an Internet Explorer browser in the Windows 7 VM and typed “http://192.168.10.13” into the browser. I clicked on the calculator.exe and clicked run. I navigated back to my attacker/ webpage host machine which is the internal Kali and this was what my command prompt looked like:

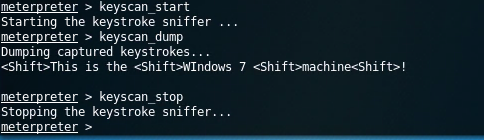


The screenshot captured by my attacker machine of the victim’s machine current desktop.

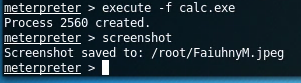
Command: screenshot



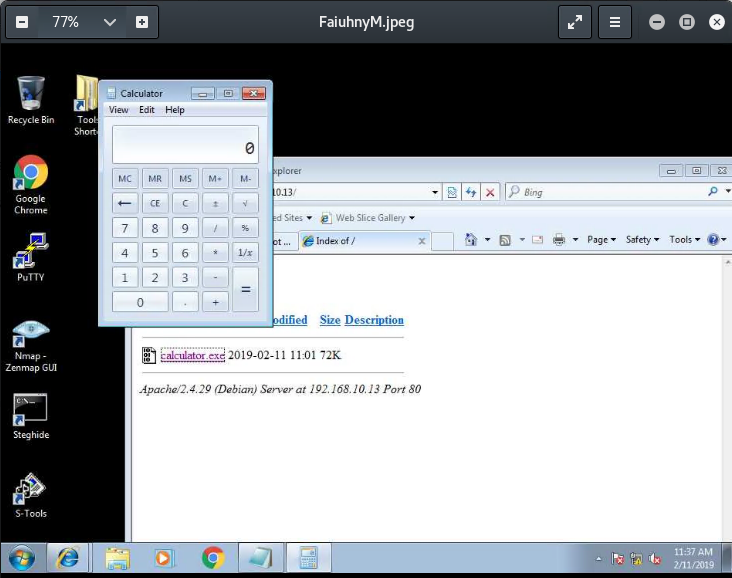
A screenshot of the captured keystrokes on the victim machine.



A screenshot of the commands I ran to open the calculator on the victim’s machine.

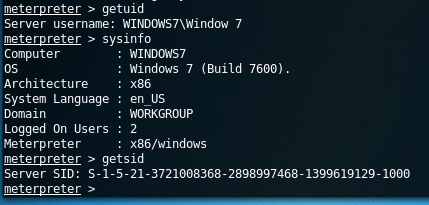


Opening the screen capture of the victim’s machine from the attacker’s machine using the screenshot command as shown in the photo above.

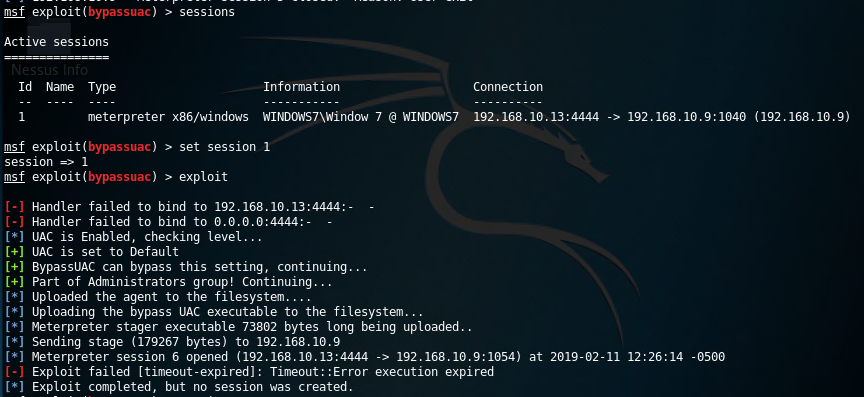
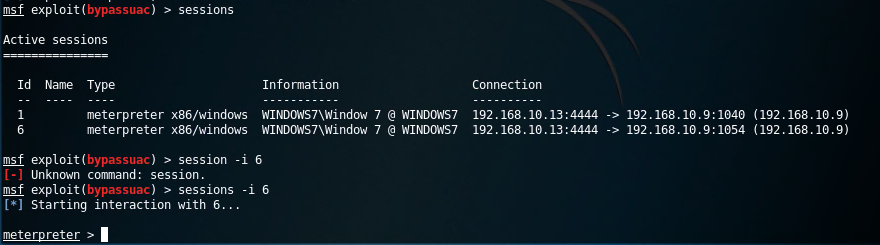


The output of 3 commands run to gather system info.

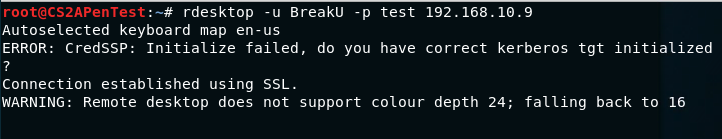
Commands: getuid sysinfo getsid



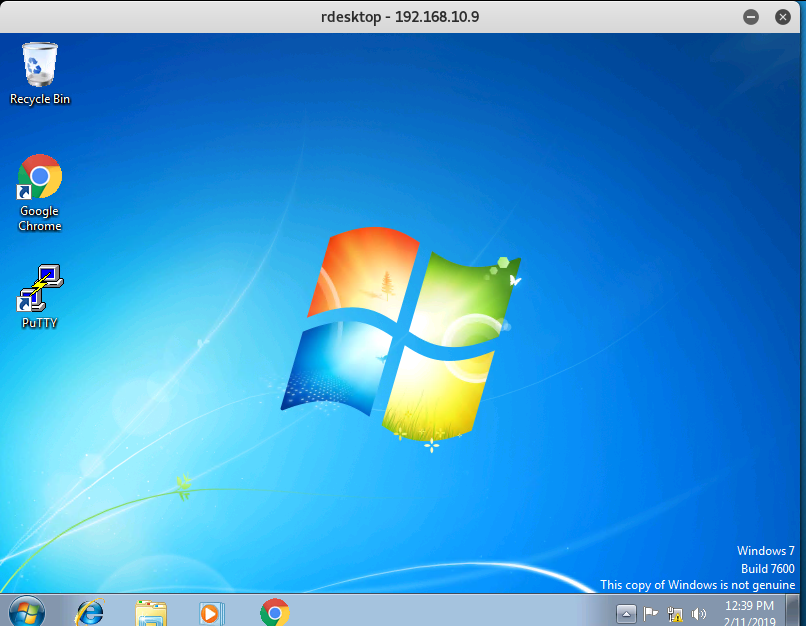
Creating a new session to the victim host with the bypassuac exploit. Then switching to the new session.



Command that I ran to connect to the victim’s machine remotely.



A photo of the remote connection.

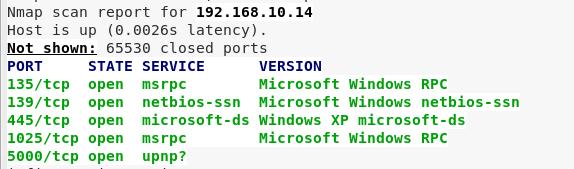


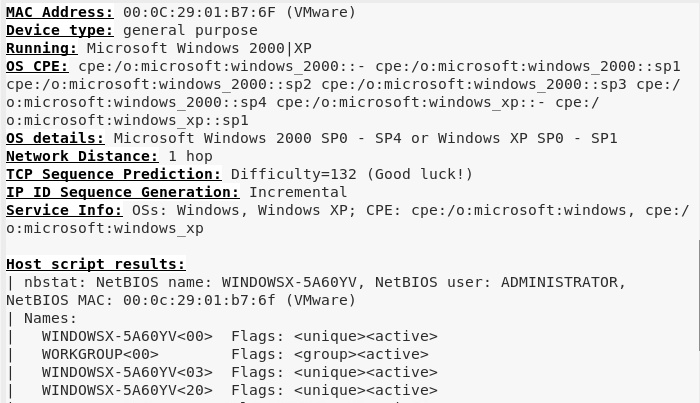
3 EXERCIESE

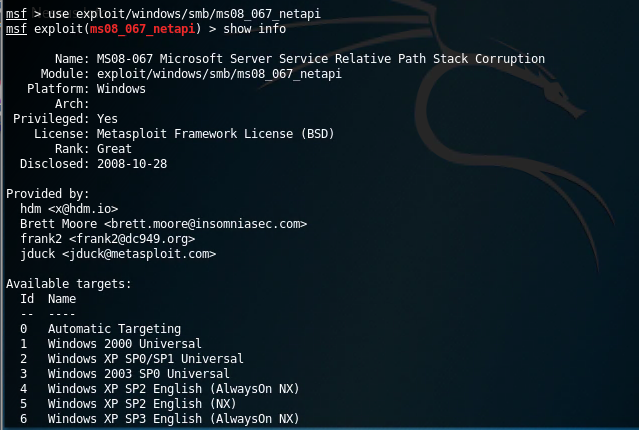
**Exploring other vulnerabilities and exploiting them in the Windows 7 VM**

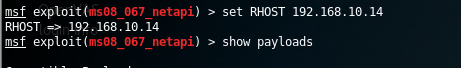
Analyze the vulnerabilities of your target Windows 7 VM (or Windows XP in the VM pool)  and try to use other exploits and payload pairs to set up a session between your attack machine and the target machine. Log the key steps and explain the possible reasons if you fail to step up the connection.  ​ **(25 points)**Hint: ***exploit/windows/*smb*/ms08\_067\_netapi***is been widely used to explore the windows samba service called ms08-67 on Windows XP. If you want to exploit Windows XP, then you need manually connect Windows XP to the pfSense LAN interface.

Create an account with your name as account name and UIN as a password on the target machine. ​ **(10 points)**

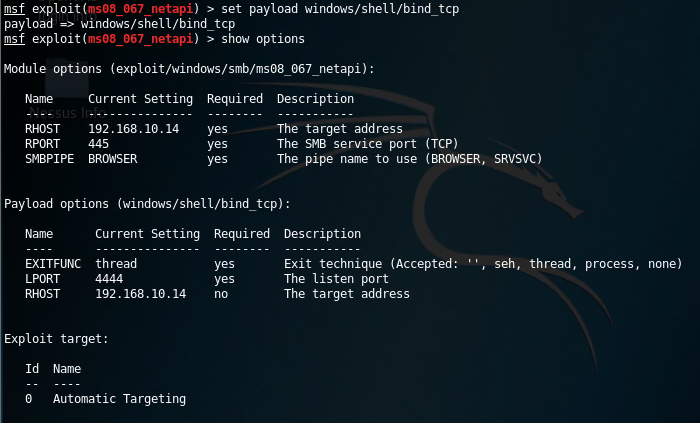
First, I ran an Nmap scan on the Windows XP host to discover open ports and services running on those ports.

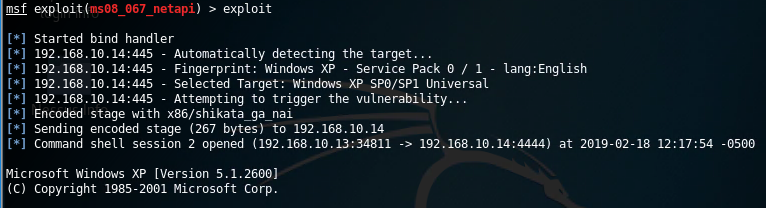


I then set the exploit as the “exploit/windows/smb/ms08\_067\_netapi” and ran a “show info” to make sure this exploit works for my target host that is Windows XP. Samba runs on TCP port 139 or 445 which is shown to be open in the Nmap results in the screen shot above.

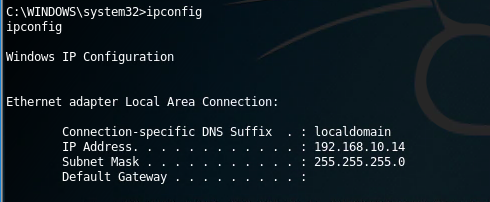
I set the RHOST as the host I intend to connect to. I then ran a “show payloads” command to see what payloads I could use with this exploit. I chose a payload with the description of “Windows command shell, Bind TCP stager Windows x86”. I picked this payload because the Windows XP host is a 32 bit system (x86) and because “Bind” in the description means that we will connect with the target host without them needing to initial the connection.

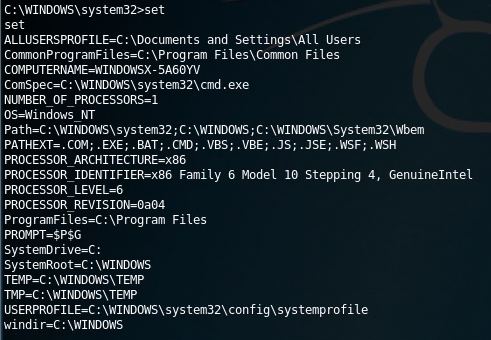
I then made sure that all of the required options were set and then entered “exploit” to run this exploit/payload combination.

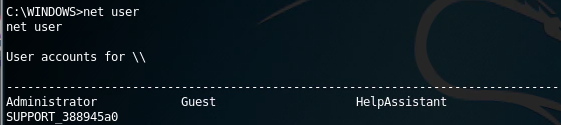


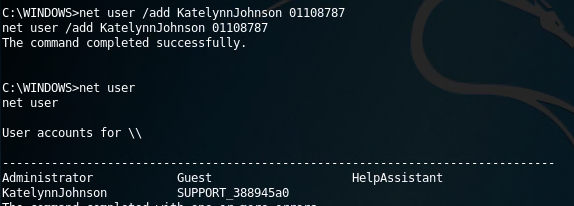


I then ran a few commands on the remote system to verify that I was indeed on the intended targets command prompt (ipconfig and set).





I then viewed what accounts could be used to login to the machine with “net user”.

I then added a new username and password with the command “net user /add KatelynnJohnson 01108787” and verified that this user was created by running the “net user” command again.

I then logged into the Windows XP machine with my newly created credentials.

