Lab 13: Malware Analysis (Host Analysis)

Aim:

To provide a foundation in understanding of the threats that occur within malware and how to analyse it.

Time to complete: Up to 45 minutes.

Activities:

- **Complete Lab 13**: Malware Analysis (Host/Network).

Leaning Activities:

At the end of these activities, you should understand:

- How to analyse for key threats.
- How to detect threats.

Reflective statements (end-of-exercise):

You should reflect on these questions:

- What methods does the malware writer use to hide the file from the user, and how does it stop them from deleting it?

- What method can a malware writer use to make sure that the malware is loaded ever time that the computer is restarted?

- Without a connection to the Internet, what would you look for, for the malware connecting to a remote server?

- How might an intruder hide their malware from a virus scanner?

- How might a browser search engine redirect be used in a malicious way?

Lab 13: Malware Analysis (Host)

1 Details

Aim: To provide a foundation in understanding malware.

This lab should only be run in a virtual image. Only connect to the network from the Windows XP when told to.

A demo of this lab is here: http://youtu.be/t_P7IkJn748

2 Analysing Malware

L1.1 We are going to investigate a variant of **Worm.Win32.Dorkbot.**

What are the key elements of the malware:

The malware is named DQ.EXE. Can you find any information on this malware?

L1.2 Run the Windows XP image. Now **DISCONNECT THE VM FROM THE NETWORK**. Go to your network adapter and define it with an address of 10.0.0.1 and a gateway of 10.0.0.1.

L1.3 Now try and connect from Windows XP to the Internet from a browser, and MAKE SURE YOU CANNOT CONNECT.

L1.4 Examine your IP address with IPCONFIG MAKE SURE YOUR ADDRESS IS 10.0.0.1 AND THAT YOU DO NOT HAVE ANY PUBLIC IP ADDRESSES.

Can you verify that you are not connect to the Internet?

L1.5 You will now be given DQ.EXE. Please ask you **tutor** for this.

L1.6 Download an MD5 and a SHA program and determine the fingerprint of the program:

Outline the MD5 and SHA signature:

How many characters does MD5 signature have:

How many characters does SHA signature have:

L1.7 Start Wireshark and examine the basic flow of network traffic. There should be very little that is interesting in the traffic.

L1.8 Run the program from the command console.

What can you observe from running the program:

L1.9 Go to the c:\recycler folder. Can you find the malware:

What is the c:\recycler folder normally used for:

How did you find the malware?

Run the attrib *.* command, and determine the attributes on the malware files in c:\recycler folder:

Which command do you need to delete the files:

Make sure you have deleted them … check with dir /ah**. Are they gone?**

L1.10 Go to the registry with REGEDIT.EXE. Now go to:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Where is the malware located within the Registry:

What does the registry entry do on the system:

L1.11 Examine the Wireshark trace.

What can you observe from the trace that the malware has done:

L1.12 Using HexWin, examine the memory. Can you determine anything that you could produce a fingerprint of the malware with:

Possible fingerprint signs:

L1.13 Now clean up the VM:

Did you manage to delete the files in c:\recyler:

Did you manage to delete the registry key:

After you clean up, reboot the VM, and check that malware is not present:

L1.14 Restore the VM to its original state using VM->Restore Snapshot.

L1.15 It is too dangerous in the lab environment to enable the network adapter, so the following is a trace of it running in a real environment:

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

Download and analyse it for:

Identify the basic signs of it when there is a connection to 10.0.0.1:

At which packet number does it manage to resolve the malicious domain:

What is the IP address it connects to:

Outline what it tries to do, and what the result is from the server it communicates with:

L1.16 On reflection, how would you create a detector on the network or on the host to detect this malware:

Outline methods that could be used:

L1.17 From your Windows XP virtual machine, install the software from the following (and accept all the default options):

http://www.jzip.com/

How has the software affected your Web browser:

What traces in Wireshark can you see from your browser of a change:

Can you get rid of the re-direction:

L1.18 From your Windows XP virtual machine, restore your image to the first snapshot. Now install the software from **mixi.dj**. Start Wireshark after the install:

How has the software affected your Web browser:

What traces in Wireshark can you see from your browser of a change:

Can you try and get rid of Delta-search. What steps did you take to get rid of it: