Lab Exercises

Understanding Computer Viruses: What They Can Do, Why People Write Them and How to Defend Against Them

<u>Review Questions</u>

1) In class, we made the distinction between a front-door attack and a back-door attack. Explain how they are different and give one example of each.

2) Give some examples of what malware tries to accomplish.

3) Describe ways that white-hat hackers try to make computer systems more secure.

4) Describe things you can do to secure your computer against attack.

Investigation Questions

1) Use your web browser to investigate the technical difference between a virus, a worm and a Trojan horse. Try typing each of these terms into your favorite Internet search engine.
   a. Do you get better results if you type in each term separately or if you type them in all together? What search strings proved most helpful to you?

      Try looking up these terms on encyclopedia sites such as Wikipedia (http://en.wikipedia.org/wiki/Main_Page) or Webopedia (http://www.webopedia.com/). Was this more or less helpful then using a search engine? Why?

   b. From your investigation, give a short working definition of each of the terms:

      i. Computer virus

      ii. Computer worm

      iii. Trojan horse

c. Optional: Did you find information on where the term “Trojan horse” comes from? If so, briefly explain what you learned.

d. Optional: How are computer viruses like biological viruses?

2) Run “netstat –an” on your own computer. On a computer running Microsoft Windows, open a command prompt. Often this can be done by going to the Start menu, then choosing Programs > Accessories > Command Prompt. The netstat command will actually work on many other operating systems, including Linux.

    a. Consider the following output. How is the output you see the same or different?

Active Connections

```
Proto Local Address                  Foreign Address    State
TCP    0.0.0.0:135                   0.0.0.0:0          LISTENING
TCP    0.0.0.0:445                   0.0.0.0:0          LISTENING
TCP    0.0.0.0:1025                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:1051                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:1067                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:1083                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:2201                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:2207                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:2679                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:3703                  0.0.0.0:0          LISTENING
TCP    0.0.0.0:5000                  0.0.0.0:0          LISTENING
TCP    127.0.0.1:2206                0.0.0.0:0          LISTENING
TCP    127.0.0.1:2206                127.0.0.1:2207     ESTABLISHED
TCP    127.0.0.1:2207                127.0.0.1:2206     ESTABLISHED
TCP    127.0.0.1:5180                0.0.0.0:0          LISTENING
TCP    192.168.0.103:139             0.0.0.0:0          LISTENING
TCP    192.168.0.103:1083            128.153.4.131:22   ESTABLISHED
TCP    192.168.0.103:2201            128.153.3.131:143  ESTABLISHED
TCP    192.168.0.103:12669           0.0.0.0:0          LISTENING
TCP    [::]:135                      [::]:0             LISTENING   0
TCP    [::]:1025                     [::]:0             LISTENING   0
UDP    0.0.0.0:445                   *:*
UDP    0.0.0.0:500                   *:*
UDP    0.0.0.0:1027                  *:*
UDP    0.0.0.0:1063                  *:*
UDP    0.0.0.0:1086                  *:*
UDP    0.0.0.0:4211                  *:*
UDP    127.0.0.1:123                 *:*
UDP    127.0.0.1:1052                *:*
UDP    127.0.0.1:1084                *:*
UDP    127.0.0.1:1085                *:*
UDP    127.0.0.1:1104                *:*
UDP    127.0.0.1:1900                *:*
UDP    192.168.0.103:123             *:*
UDP    192.168.0.103:137             *:*
UDP    192.168.0.103:138             *:*
```

```
 UDP    192.168.0.103:1900        *:*
 UDP    192.168.0.103:10581       *:*
 UDP    192.168.0.103:21210       *:*
```

Notice that each line has the following columns: Proto, Local Address, Foreign Address and State. Let’s examine each one.

The name of the first column, Proto, stands for protocol and is either TCP or UDP. TCP and UDP are two types of network protocols in the Internet. Notice that the TCP lines all end with either ESTABLISHED or LISTENING for a state. ESTABLISHED connections are those that are actively being used to transfer data. The LISTENING connections are not currently being used to transfer data but they represent server software that is ready to accept and respond to requests should they arrive.

The foreign and local address portions of each line are composed of two portions separated by a colon -- an IP address and a port number. The IP address indicates the numerical address of the computer on which the network software is running. The port number indicates the “mailbox” number on that particular computer for that particular service or network conversation.

b. You can investigate each type of server running on your machine. For example, consider the first line:

```
TCP    0.0.0.0:135           0.0.0.0:0             LISTENING.
```

It says that a service is listening on TCP port 135. If I want to know what port 135 is typically used for, I can do a Web search for “TCP port 135”. Do such a Web search. What type of service typically runs on TCP port 135? What are some computer viruses that have exploited flaws in this service?

c. Choose another line of the netstat output and do a similar investigation of what service runs there and what viruses, if any, have targeted that service(If you have multiple people or groups doing this exercise, consider having each choose a different port and then summarize what you learn for each other.)

d. Optional: Doing a complete investigation of each service running on your computer could take a long time. However, it can be a good idea to periodically run netstat and look for new services. If you see a service, you’ve never seen before then investigate it. It could be a sign of a virus. If running on multiple machines, compare your output with others and look for differences.

e. Optional: A group called the Internet Assigned Numbers Authority decides what services run on what ports. Do a web search for “well-known port numbers” and another for the “Internet Assigned Numbers Authority”.

3) If you run anti-virus software at home, you are probably used to getting updated virus signatures. People produce these virus signatures by analyzing new viruses that appear on the Internet and then writing instructions for how to recognize the virus. The anti-virus software then searches all downloaded files to see if they match any known virus signatures. There are several excellent web sites that list detailed information about known viruses -- how they spread, what they do to an infected computer, etc.

   a. Go to the Symmantec Security Response site at: http://securityresponse.symantec.com/

      You should see a list of the latest virus threats. What are the names of the top five?

   b. You can learn a lot about a virus just from its name. For example, many virus names begin with W32, such as in W32.Beagle.BT@mm. W32 indicates that a virus targets the Windows machines or specifically the Windows 32 interface. Some viruses begin with VBS indicating that they are a Visual Basic Script. Some viruses begin with Trojan indicating that they are a Trojan Horse. What things do you suspect about the top five viruses just based on their names?

Choose one of the top five and click on its link to see a detailed report. You should see detailed information about the systems affected, patches to prevent infection, how wide spread infection has become, information about what kind of damage the virus does, how it spreads and technical details about its operations.

c. What is the type of the virus you are reading about? Click on the type for a full definition. What other types are considered?

d. Under the Damage section, what types of damages are considered? Which ones apply to the virus you are reading about?

e. Under the Distribution section, what are the primary distribution methods considered? Which ones apply to the virus you are reading about?

f. Summarize what you learned about the virus you chose. (Consider having each person or group summarize a different virus and present their findings to each other.)

g. You can also search for viruses by name using http://securityresponse.symantec.com/avcenter/search.html. Try searching for the Sasser or Blaster worms. Can you think of any other viruses by name? Try searching for those as well.

Research and Discussion Questions

1) Attacks that are so new to the Internet that they haven’t yet been classified and for which no patches have been written are called “zero-day attacks”. Do some web research on zero-day attacks. What did you learn?

2) How costly is damage done by computer viruses? Search for reports that summarize the impact both in terms on dollar value and the number of people affected. Why do you think good estimates of damage may be so hard to generate?

3) If someone is found guilty of writing and spreading computer viruses, what type of punishment do they typically receive? What do you think should be punishment for writing a virus that affects millions of computer users around the world?

4) In class, we discussed the difference between white-hat and black-hat hackers. Do some research into the distinction between them. What activities are clearly black-hat activities? Clearly white-hat activities? What activities fall into a gray area? How do you feel about these gray-hat activities? Discuss these activities with your classmates. Can you come up with a definition of an ethical hacker? Does a career as a white-hat hacker sound attractive to you – why or why not?