## Lab Exercises

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

**Review Questions**

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.

Front-door attacks require the actions of a legitimate user -- for example, malware that is run when a legitimate user opens an infected email attachment or runs a malicious program the user downloaded from the Internet.

Back-door attacks do not require the actions of a legitimate user. Instead, they target vulnerabilities in the server software that is running a computer. Flaws in server software may cause a server program to respond to an unexpected request in such a way that it gives the attacker access to the computer. A buffer overflow attack is one example of a back-door attack.

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

Malware varies significantly in the actions it takes once it compromises a victim's computer. It can do anything from announcing its presence by displaying a message on the screen to making the computer play sounds. It can also corrupt the system or attempt to attack other machines by sending infected emails, for example.

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

White-hat hackers try to make computer systems more secure by looking for and reporting vulnerabilities so that they can be fixed. They can also help to characterize new viruses and develop patches for them.

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

Run an antivirus program and keep its virus definitions up-to-date. Avoid suspicious email attachments or Internet downloads. Keep your operating system and any services patched and up-to-date. Be aware of what services are running on your computer and consider shutting off any you don't need.

**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?

If you do search for them one at a time, you are likely to get references to biological viruses, earth worms, and historical references to Trojan horses, although the computing usages of these terms will still figure prominently in the list. If you search for them all together, you are likely to narrow in on computing references. Adding the word "computer" is also helpful in this context. In using the Web to research topics, it is important to practice modifying search terms to narrow in on the subject you want.

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?

These sites are probably more helpful for basic, well-rounded definitions. Searching for the terms in search engines will return many references that use the terms in context but do not provide a clear definition. Knowing when to use a general search engine versus a specific reference site is an important skill for Web research. Creating a personal set of links to helpful reference sites can be a good strategy.

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

    i. Computer virus

From Webopedia:
A ***computer virus*** attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels. Much like human viruses, computer viruses can range in severity; some viruses cause only mildly annoying effects while others can damage your hardware, software, or files. Almost all viruses are attached to an executable file, which means the virus may exist on your computer but it cannot infect your computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going. People continue the spread of a computer virus, mostly unknowingly, by sharing infecting files or sending e-mails with viruses as attachments in the e-mail.

ii. Computer worm

From Webopedia:
A ***worm*** is similar to a virus by its design, and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the ability to travel without any help from a person. A worm takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its ability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. One example would be for a worm to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues on down the line. Due to the copying nature of a worm and its ability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers, and individual computers to stop responding. In more recent worm attacks such as the much talked about .Blaster Worm., the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

iii. Trojan horse

From Webopedia:
A ***Trojan Horse*** is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan Horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

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

It is a reference to the Trojan War between the Greeks and the Trojans in which the Greek soldiers pretended to give up the war and offered the gift of a large wooden horse to the city of Troy. The Trojans accepted the gift, took it into the city, and began celebrating the end of the war. However, Greek soldiers had hidden in the wooden horse, and when the Trojans were not expecting it, they came out and took over the city. Therefore a Trojan horse refers to something that appears to be a great gift but really contains something that will hurt you. See the following Web site for more information:
www.stanford.edu/~plomio/history.html#anchor204279

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

From Wikipedia:
A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed infection, and the infected file (or executable code that is not part of a file) is called a host.
http://en.wikipedia.org/wiki/Computer_virus

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?

Microsoft Remote Procedure Call (RPC) or Distributed Component Environment (DCE) locator service, also known as end-point mapper, runs on this port.

The Blaster worm, among others, targeted this port.

http://nsit.uchicago.edu/alert/port-135.html

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".

www.webopedia.com/quick_ref/portnumbers.asp
www.iana.org
www.iana.org/assignments/port-numbers

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?

On June 4, 2008:

W32.Emsenush.A
Downloader.Swif.C
Trojan.Spryct
Trojan.Apisnuf!inf
Trojan.Apisnuf

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?

The choices were Adware, Dialers, Hack Tools, Joke Program, Remote Access, Spyware, Viruses, Worms, Trojan Horses, and Other.

Reading the definitions of each of these is a nice complement to the investigation of viruses, worms, and Trojan horses that we did in an earlier exercise.

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

Under Damage, the categories were:

- Large scale emailing
- Deletes files
- Modifies files
- Degrades performance
- Causes system instability
- Releases confidential information
- Compromises security settings

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

Under the Distribution section, the categories were:

- Subject of email
- Name of attachment
- Size of attachment
- Time stamp of attachment
- Ports
- Shared drives
- Target of infection

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?

www.cybercrime.gov
www.cybercrime.gov/parents.html

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?

http://en.wikipedia.org/wiki/White_hat
http://white-hat.org
www.whitehatsec.com