Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Tutorial 5
COMPUTER VIRUSES

Nhat Nam Nguyen
nhatnamcse@gmail.com

25/4/2015

Exercise 1. (2pts)

Explain how they are different between a front-door attack and a back-door attack and give one example of each?

Exercise 2. (2pts)

Explain the difference between a virus, a worm and a Trojan horse?

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

Optional: How are computer viruses like biological viruses?

Exercise 3. (3pts)

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 antivirus 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) Under the Vulnerabilities section, analysis and describe one of type Vulnerabilities.

Exercise 4. (3pts)

a) 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?

b) 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?

c) 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?

Exercise 5. (3pts)

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?

THE END