Computer Security Homework 11 (Due Friday 11/13/20)

1. True or false.

   (a) Java is just as vulnerable to buffer overflows as C.

   (b) Malware took out some Iranian nuclear reactors.

   (c) Most of the worms we looked at targeted Windows.

   (d) In order to create a new virus, you need to be proficient at coding

   (e) Suppose a program claims to convert jpg files to png, but in reality it deletes all your image files. This is a virus.

   (f) Tyler develops a new encryption technique, but in addition to the regular key, he also makes sure that a special 128-bit key that only he knows can be used to decrypt anything encrypted with his technique. This is an example of a backdoor.

   (g) Suppose you click on a link that goes to a site with the URL below. That site is trying to trigger a buffer overflow vulnerability in your web browser.

   `http://www.example.com/%5a%9b%90%49%6b%a8%bb%70%90%43ZZZZZZZZZZZZZZZZZZZZZZ%7f%ff%40%09`

   (h) As long as you update your antivirus software daily, you are safe from viruses.

2. For each of the following, indicate which type of malware best fits the description. Choose from logic bomb, trojan, virus, macro virus, worm, rootkit.

   (a) _____ Joel installs software on the Mount's network such that any time his grade in one of Heinold's classes is not an A, then 30 unpaid parking tickets suddenly show up under Heinold's account.

   (b) _____ Avery downloads the latest version of Python from `downloads.mypython.org` – or at least she thinks it's Python. It actually installs a keylogger and pops up an alert saying the Python installation failed.

   (c) _____ Jack finds a DVD in the computer lab with the label "HeinoldSecurityExam2020". He looks to see what's on the disc, and some code hidden on the DVD attaches itself to several executable files on his hard drive.

   (d) _____ Kaitlyn finds an old server lying around. She puts it on the public internet. Within minutes, there is a malcious program running on the server that exploits a buffer overflow vulnerability in the web server software on the server. That program is now looking for ways to copy itself to other machines on Kaitlyn's local network.

   (e) _____ Ronaldo finds a USB drive in the computer lab. The drive is totally clean except that on it is a MS Excel file entitled Grades2020.xlsm. Ronaldo opens it. He later finds that all of the files from the Fall2020 directory on his computer have been deleted.

   (f) _____ Ryan's computer has been acting up recently. The CPU usage seems to spike at random times. But every time he looks at the list of programs running, he doesn't notice anything unusual using the CPU. It still seems like something must be there, but it's really good at hiding itself.

3. An attacker discovers a buffer overflow vulnerability in the Adobe Flash plugin. Adobe was not aware of this vulnerability. The most common term for a vulnerability like this is

   (a) stealth vulnerability

   (b) proprietary code vulnerability

   (c) zero-day vulnerability

   (d) undetected vulnerability

4. Which of these are things that can be done with a buffer overflow?

   (a) to get to a shell prompt to run commands on a system

   (b) to overwrite other variables in a program to values that help the attacker

   (c) crash the program

   (d) all of these

5. If you download a pdf of Homework 12, that file is (choose all that apply)

   (a) probably safe to download because pdfs are just text

   (b) potentially unsafe to download because it could trigger a buffer overflow in your pdf viewer

   (c) safe to download because Dr. Heinold wouldn't send you something that could harm your computer.

6. In order to get a buffer overflow to run an attacker's code, what is it precisely that the attacker must overwrite?

7. In class, we had a discussion of the Welchia good worm, which infected computers without permission, but which actually patched the computers to protect from a vulnerability. Discuss the ethics of this.