CIS3360: Security in Computing (online session, Spring 2012)

Homework 3: Chapter 2, 3, and 4

(assigned 03/19, due on webcourse by 3AM 03/27, i.e., late night in 03/26)

Question 1 should be submitted to Assignment 3.1

1. (55 points) Knowledge-based Question:

a. What are the four criteria to judge whether or not a biometric is suitable for identification? What criteria does the biometric 'weight' violate (which makes it unsuitable for identification)
b. In computer's memory, when stack grows, does the address of the top of stack increase or decrease?
c. What is a 'page fault'? Why page fault could greatly reduce computing performance?
d. What are the two types of virtual machines? What type of VM does Java VM belongs to? What type of VM does VMware belongs to?
e. What are mail 'open relay'? Why it can be used by spammer to send out spam email?
f. What does 'Non-executable stack memory' mean? Why some programs cannot run when this option is enabled?
g. Why 'Address space layout randomization' can prevent stack overflow?
h. How does 'Stackguard' prevent stack overflow? Can stackguard prevent function pointer overflow attack?
i. Why Pharming attack is more difficult to defend than Phishing attack?
j. 'Image and corresponding phrase' has been used by many banks' website. What attack do they prevent?
k. What attacker does the image-based password input method prevent (this technique has been used by many banks' websites)

Question 2-4 should be submitted to Assignment 3.2

2. **(10 points) User privilege.**

a. If 'test' is a file in a Unix machine and 'ls' command shows that its privilege is: "rwxr-x---", what does this privilege mean?
b. If 'cis3360' is a folder under Unix machine and 'ls' command shows that its privilege is: "rwx-w----", what does this privilege mean?

3. **(20)Operating system**:

a. How can multitasking make a single processor look like it is running multiple programs concurrently?
b. Give an example of three Windows operating system services that do not belong in the kernel.
c. What is the purpose of salt password?
d. Why it is unsafe to keep around the C:\hiberfil.sys file after a computer has been restored from hibernation?

4. **(15) Malware**:

a. What are the differences between polymorphic viruses and metamorphic viruses?
b. What is the name of the first widely spreading worm after year 2000?
c. Why Slammer worm spread much much faster than Code Red worm?
d. According to the worm propagation differential equation model, why a worm slows down its infection speed after it infects more than 80% of vulnerable hosts?