**CIS3360: Security in Computing**

**Homework 1**

**1. (50 points) Knowledge-based Question:**

a. What are the four criteria to judge whether or not biometrics are 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 could page fault 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. Why do some system admins want monthly password changes?

f. What does ‘Non-executable stack memory’ mean? Why can some programs not run when this option is enabled?

g. Why can ‘Address space layout randomization’ prevent stack overflow?

h. How does ‘Stackguard’ prevent stack overflow? Can stackguard prevent a function pointer overflow attack?

i. Describe the A.A.A concept from Chapter 1 in your words.

j. Describe 3 ways to social engineer an end user to give you an admin password.

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

a. If ‘test’ is a file in a Unix machine and the ‘ls’ command shows that its privilege is: “rwxr-x---“, what does this privilege mean?

b. If ‘cis3360’ is a folder in a Unix machine and the ‘ls’ command shows that its privilege is: “rwx-w----”, what does this privilege mean?

3. **(20 points) 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 in a password?

d. Why it is unsafe to keep around the C:\hiberfil.sys file after a computer has been restored from hibernation?

4. **(20 points) Physical attacks**:

1. Describe 3 ways to break into server room without leaving an obvious trace of the intrusion, provided the room is only protected with a pin tumbler lock.
2. Describe 3 ways to perform a direct attack against a laptop.