Homework Assignment #1 (100 points)

1. Explain how a buffer overflow works (10 points)
2. What is the difference between a stack-based buffer overflow and heap-based buffer overflow? (5 points)
   1. Give an example of each used in an exploit (5 points)
3. What is the phishing? What is pharming?  What is the difference between phishing and spear-phishing? (15 points – 5 points each)
4. List the four types of buffer overflows and provide an example of each one (10 points)
5. Biometrics such as fingerprints, retina patterns and voice print are used as part of a multi-factor authentication scheme. Thinking like an attacker – how can a fingerprint scanner be fooled into accepting an unauthorized user as a legitimate user (assuming they know the target user account’s password)? (15 points)
6. Which is more complicated to implement correctly in an operating system, authentication or authorization? (10 points)
7. In 1988 the Morris Worm spread throughout the Internet by exploiting the Sendmail Mail Transfer Agent program that was common throughout UNIX systems.
   1. What type of vulnerability did the Morris Worm exploit? (5 points)
   2. What specific Sendmail command did the Morris Worm use to initiate the attack? (5 points)
   3. What other programs did the Morris Worm use to spread itself across the Internet at that time? (5 points)
8. For the following code, provide a simple exploit that will trigger buffer overflow and have the code print out “you win!” (15 points)

/\* stack1-stdin.c \*

 \* specially crafted to feed your brain by gera \*/

#include <stdio.h>

int main() {

               int cookie;

               char buf[80];

               printf("buf: %08x cookie: %08x\n", &buf, &cookie);

               gets(buf);

               if (cookie == 0x41424344)

                              printf("you win!\n");

}