**Chapter 9 Homework Questions** - answer the questions below. (2 points for each question - 12 points total)

1. Explain the four goals associated with computer threats.

Attackers are usually concerned with stealing, altering, destroying, or using the information for a malicious purpose. By stealing data, they can gain access to sensitive information and perhaps financial information. When altering, the attackers can erase records for personal gain or just destroy to cause problems. Using information can take the shape of black mail, or using specific information to achieve a goal or cause something private to become public.

2. Explain the main differences between Secret-Key Cryptography and Public-Key Cryptography.

Both keys are usually long complex numbers that make up an encryption for data. A Public-Key is just that, public and can be accessed by anybody via a repository. The Secret-Key is only viewable to that specific person thus is secret. For something to be sent such as an email, the person’s public key will be encrypted with the mail but will require that person’s specific secret key in order to open.

3. What is a digital signature?

This is a strategy to ensure that documents remain authentic during transfer. A digital signature is a type of encryption; password, check sum, cyclic redundancy check, private/public encryption, hashing, and digital certificates.

4. What is a packet sniffer?

A packet sniffer is a program that can view all of the traffic from the Internet and “sniffs” all of the packets to ensure that they contain valid information. This is also used to ensure that there aren’t any breaches in security.

5. Explain the various types of attacks from inside listed in section 9.5 of the text.

There are a lot of different types of attacks but some of the more common ones include eavesdropping, data modification, identity spoofing, password based attacks, denial, and sniffer attacks. Eavesdropping is similar to it’s real world counterpart in that the attacker will “listen” to packets incoming and outgoing in order to gain access to valuable information. Data modification is also just like it sounds, in this type of attack the hacker will attempt to change data within the legitimate user’s system. Identity spoofing is when the attacker will look for information such as an IP to mask their computer to look like the legitimate user’s. Password based attacks rely on looking at the user’s password and username and logging in as them to either amend data, create new user accounts, or look at information. Denial is aimed to deny legitimate users the use of their computers. Sniffer attacks utilize the sniffing of packets to find out information about the system to use against them.

6. Explain the difference between a virus and a worm?

A virus is code that attaches itself to a program or file and can leave a copy of itself on any system that it interacts with. A worm is very similar but it can replicate itself without the aid of the program. A worm will use information stored on your computer to replicate itself such as an email list in which it email itself from.

**Chapter 9 research assignment** (10 points) - Go on the Internet and complete a 1 page summary of three computer viruses of your choice. Submit your summary along with the answers to the questions above in the same Word document.

There have been some very famous viruses in the past that have caused a lot of headaches and have caused billions of dollars in damage, all with varying intentions and scopes. All the viruses have one thing in common and that’s malicious intent. Three viruses in particular stand out in my mind when I think of famous ones: ILOVEYOU worm, the Klez virus, and the Code Red (one and two). These three viruses were big enough to be included in national news and were all worth billions of dollars in damage.

The ILOVEYOU worm originated back in 2001 in the Philippines and spread through corporate companies like wild fire. The worm was an attachment to a email that read “I love you” from a secret admirer that attached a “love letter” to the email. The “love letter” was labeled LOVE-LETTER-FOR-YOU.TXT.vbs. The vbs at the end refers to Visual Basic Scripting, which was what the worm was written in. When opened it would copy itself to different areas of the hard drive, added files to registry files, resent itself through email contacts, and downloaded a boot file that would steal passwords. This worm ripped through big corporate companies who had to spend $10 billion dollars combined to repair all of the damages that it caused. People suspected that the virus had come from a Onel de Guzmen in the Philippines but due to a lack of evidence, he was released.

The Klez virus was very similar in nature to the ILOVEYOU worm but had many different version of it that alluded anti-virus software for years. The virus would attach to an email that when opened would send itself to the user’s address book. The difference came in its ability to be a Trojan horse, a worm, or virus. This caused some problems because anti-virus software had to write code to combat all of the different types. This virus came up in 2001 and caused a lot of damage and still has new versions coming out today. The virus also had the ability to copy people from the address book of the user and place it in the from field to further confuse people who would be seemingly opening an email from a friend or acquaintance.

The last virus is the Code red worms which hit the internet shortly after the Klez in the summer of 2001. The worm only affected machines running Windows NT and 2000 and exploited a buffer overflow problem, which occurs when machine is running and receives more information than the buffers can handle and it starts to overwrite memory. The worm is a backdoor program that is system level, which means the user no longer has control over the system. This is really bad because the virus had the ability to conduct illegal activates through the use of somebody else’s computer. The most media popular instance of this virus occurred when the code red was used to control user’s computers to send info to the white house computers and eventually crash them.