# ISEC 325 Homework 03

Answer the following questions based on your reading of the text books, the module key points, and the instructor’s presentation this week.

1. [4 points] Briefly list and describe each of the network *logical* topologies. What is the difference between a logical and physical topology?

The two logical topologies are bus and star. The bus has a straight-line communication channel where the nodes connect to the same line and the messages are being transmitted one at a time meaning the nodes must wait their turn before they can send the message. The star has a central node that is connected to each other node within the topology. The nodes will transmit message to the center node where the message is received then retransmitted to everyone of the attached nodes. The major difference between logical and physical topology is their focus. The physical topology looks at networks and how they are cabled as well as more physical attributes. The logical topology looks at the network and determines how to functions. It can be looked at like a what and why line of thought. The physical topology asks the question of what the network needs to run while the logical topology asks why the network is running in the first place and its purpose.

1. [3 points] Name and describe three error detection and/or correction techniques used in network transmissions.

The first technique is the repetition scheme where data is repeated in transmission multiple times. The second is the redundancy scheme which will look at and calculate parities for blocks instead of the individual bytes. This is also split into two different types of redundancy checking called longitudinal and vertical redundancy. The third is the message authentication codes which will use a hashing algorithm to make a one-way function with a radically changing range when there is a small change in the domain.

1. [2 points] How is analog information placed on an analog signal? A digital signal?

Analog information is place on an analog signal using amplitude, frequency, and phase like telephone networks or radio stations. To be place on a digital signal, the analog frequencies will be used to encode bits by measuring the signal height.

1. [2 points] How is digital information placed on onto an analog signal? A digital signal?

Digital information on an analog signal is done using shifting keys. The keys will shift the information from its digital state into amplitude, frequency, and phase. The digital information uses a network interface card to connect to the digital signal, it uses current turned into voltage levels to encode binary data.

1. [3 points] Briefly describe and contrast LANs, MANs, and WANs.

LAN is the local area network which would be the immediate area around its center point. MAN is the metropolitan area network which is larger and will cover a county or district. WAN is set up to cover an even larger area such as states, countries, or even the planet itself like the internet. We can contrast them through the use of two-player games. To connect with another person they need a connection and the networks will determine who can play. LAN lets a person play with the immediate people so if they are in their house, it would be their family or visiting friends. MAN lets a person play with their friend who is in the same county such as a school friend. WAN is where a person can play with someone on the other side of the planet and meet new people.

1. [3 points] What differentiates black-hat and white-hat “hackers?”

The main difference between the two hats is their intention. The black-hat hackers will start with the first four-penetration testing phases; reconnaissance, scanning, exploitation, and maintaining access like the white-hat hacker. The black-hat hackers will then go to the fifth which is to cover their tracks and remove anything that can be linked back to them. Depending on their reason for being in the system and what they are looking for or exploiting, the exploited party may not know the hack took place for a long while or until that accessed information leads to trouble for them like blackmail or threats. The white-hat hackers will take each of the steps and make a report so they can help their client with determining where the weaknesses in their systems are and how they were able to get in. They tend to share their experience and path so that the client can fix problems and be protected against less morally good hackers.

1. [4 points] Name and describe the four (or five) stages of a white-hat penetration test. Where does a penetration test fit in an overall enterprise information security plan?

The first stage is the reconnaissance where the hat will gather information that is available to the public. The next step is using the port scanners to identify the computers that are active on the network and what ports can be used. There are other scanners that follow such as the active vulnerability scanners. Once all information from scanning is gathered, the next step is the exploitation which is where the hat will start breaking into the systems itself to get further access. After this is the maintaining access where the person will do penetration testing to make sure they still have access. The fifth step for the white-hat hackers is writing a report on how they completed the penetration testing. The penetration test fits into an enterprise information security plan in the network security where they will run tests after their systems have been running for a while or if they have been updated to check for any possible holes in the security.

1. [4 points] Describe several techniques for passive reconnaissance in a penetration test.

Passive reconnaissance tends to be looking at the public sources of information that can be found without looking directly at IP addresses and searching their website offline. This would be more passive ways like using a search engine to find information on the target or using open source intelligence to gather information for you.

1. [5 points] In two to three paragraphs of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered in the class session this week. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about.  In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Feel free to ask questions in this as well since it will be returned to you with answers.

This week we looked at different information about networks. I remember touching some of these topics when I took a cyber security class, so it is nice to be able to see the information come back like the topologies. There is also some topics that I know where lightly touched on in other places but were expanded here like modulation and how to takes on four different forms. I do not have the best memory so it is nice to know that with seeing some of this information again, I can remember when I learned about it prior. My question is out of the different types of security which is your favorite?