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?

   A topology is a diagram of how a network is set up. Physical topologies show how networks are cabled and logical topologies show how a network functions. The most common logical topologies are bus and star topologies. A bus topology is a linear communication channel where messages are transmitted one at a time from one station or node to another where the nodes take turns. A star topology has a central node that each station transmits to and then is retransmitted to all the attached nodes.

2. [3 points] Name and describe three error detection and/or correction techniques used in network transmissions.

   Repetition schemes can be used in error detection by repeating blocks of data a predetermined number of times if an error doesn't affect each block it may be detected. Parity schemes both odd and even can be used in error detection where an extra bit is added to the data. If the scheme is odd, then if the data's sum is odd the extra bit is given a 0 and if the data is even it is given a 1 to make the sum odd. Even is the same but checks for an even sum. If the data is transmitted with a parity scheme and it is not odd or even, then it can indicate not all the data is there. Message authentication codes are used with hash values of the entire message appended to the message upon delivery the hashes are decrypted by the user's private key and the messages are compared to detected errors.

3. [2 points] How is analog information placed on an analog signal? A digital signal?

   Information is embedded on the analog medium using three characteristics of the analog signal the amplitude, frequency and the phase. By controlling the height, number of times the wave is repeated and the direction of the waves, the waves can be used to transmit data. When analog information is placed on a digital signal pulse amplitude modulation is used where the height of the waves is measured, and the data is encoded on bits.

4. [2 points] How is digital information placed on onto an analog signal? A digital signal?

   Modems embed digital data over airwaves by manipulating the characteristics of the signal. There are three techniques used to embed the data amplitude shift keying, frequency shift keying and phase shift keying. Digital information placed onto a digital signal is done with a network interface card which modulates the current carried over the network into a series of discrete voltage level which are return to zero and non-return to zero.

5. [3 points] Briefly describe and contrast LANs, MANs, and WANs.

    - LAN stands for Local Area Network which indicates that it has less than 3 miles of cabling. A LAN contains a dedicated server that connects systems and provides services over a small geographical space. LANs are typically owned and operated by a single organization.

    - MAN stands for a Metropolitan Area Network is a network that covers an area the size of a municipality, county or district. A MAN is larger than a LAN but smaller than a WAN.

    - WAN stands for Wide Area Network and covers a large geographical area like a state, a country or the planet. A WAN is comprised of both LANs and WANs.

6. [3 points] What differentiates black-hat and white-hat "hackers?"

    There are only grey hat hackers but to answer the question black hat hackers are hackers that act out of greed or personal gain to illegally gain access to systems with out authorization. White hat hackers are sometimes known as penetration testers who utilize the same hacking tools and techniques as a black hat hacker with authorization to test a system or network for vulnerabilities to try and find the vulnerabilities before black hat hackers so that they may be patched or fixed.

7. [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 five steps of a penetration test are Reconnaissance which is the process of information gathering about your target. IP addresses and email addresses may be goals of the reconnaissance phase. Scanning is the next step where the penetration tester uses port scanners like NMAP to find open ports, applications and operating system information. Exploitation is the next phase of penetration testing where the pen tester will use hacking tools like Metasploit to do more intensive scans to uncover vulnerabilities. Metasploit then has a suite of scripts that take advantage of vulnerabilities to give access to the target system. Post exploitation and maintaining access is a debatable step the post exploitation is the part of the test where a report is written to be presented which details security flaws found in the test. In theory a pen tester could attempt to maintain access to determine the severity of the vulnerability but maintaining access shouldn't always be necessary in a pen test. The last phase which is again debatable is removing all traces of your access which shouldn't be necessary for a white hat penetration tester. A penetration tests fits into an overall enterprise security plan by providing information about vulnerabilities so that they may be corrected to prevent a breach.

8. [4 points] Describe several techniques for passive reconnaissance in a penetration test.

    Passive reconnaissance is making use of the information that is on the web. HTTRACK: Website Copier makes an identical copy of a website on your computer where you can go through the website's pages, links and code. Google Directives to search information about your target, by

doing a google search with the name of the directive you want to use a colon and the term you want to use in the directive you can return results on google that can be used in information gathering. Whois is a service which allows access to specific information about a target such as IP addresses or host names of the company's domain name server. Netcraft will return any websites that it is aware of with your search keywords it will provide information about ip addresses and the operating systems of the servers. The Host tool preforms translations of host names to IP addresses.

9. [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.

I enjoyed the material and MEET session this week. It was good to get a refresher about how analog and digital data is transmitted. I tried to explain why vinyl record players have a different sound to my wife awhile back but came up short. I was able to explain it more clearly after this week. Going over the OSI model and the TCP model previously helped me understand how error checking works better. I dug deep into hashes in a previous class and it was cool for me to see how it all fit together.

It was nice to have a refresher on topologies and brushing over them and the material over the LAN, MAN, and WAN makes things easier to understand. I have an associate degree in Network Systems Administration where we covered the topics more in depth but sometimes the essence of the topics can get lost with all the intricacy and detail. In security I know it is important for me to understand how things work so I can protect them.

I really enjoy the penetration testing part of information security. It is too bad it may still get looked at in a bad light. I don't think everyone has to use that knowledge for bad purposes. It seems like a lot of work to go through to exploit people for next to nothing gain in the end. If someone has worked hard to get a degree, they wouldn't want to throw all that away committing crimes on the internet I would think. I really enjoyed the penetration testing labs. If nothing else, it is great to see how systems are exploited so we can understand how to protect them.

References

Engebretson, P. (2013). *Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier Science and Technology Books.

Whitman, M. E. (2012). *Guide to Network Security, 1e.* Cengage Learning.