ISEC 325 Homework 02

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

1. [3 points] What is information security and how does it differ from network security? How does network security fit into the McCumber cube (i.e. which cells does it cover)?

   Information security is the protection of information and its critical elements including the systems and hardware that use, store and transmit the information. You are protecting the data in transit and at rest. Network security is the protection of the networking components, connections, and contents. Network security has to do with processing, transmission and storage of data and has to do with the CIA triad protecting the data that is confidentiality, integrity and availability. Where the physical components intersect with each of the tenets of information security would be a control that would have to do with network security. The book uses the example of the intersections of storage and integrity for this the control may be and intrusion detection system. Network security is a part of the entire front part of the McCumber Cube model.

2. [3 points] What is the difference between an exploit and a vulnerability? A threat, a threat agent, and the subject of an attack? An asset and an object of an attack?

   An exploit is a program or code written to take advantage of a vulnerability. A vulnerability is a weakness in your system that opens the possibility for attack. An example of an exploit would be Metasploit a hacking software suite that will identify vulnerabilities such as open ports and provide code to gain access through the ports to set up a backdoor or install malicious code.

   A threat is a category of objects, persons, or other entities that present a danger to an asset. A threat could be a hacker or something like a storm that could knock out your systems. A threat agent is the specific instance of a threat. A specific hacker or a specific storm is considered the threat agent. A computer that is under attack is an example of the subject of an attack, it is what is being attacked. The object of the attack is the computer being used to conduct the attack and the asset is what the attacker is trying to steal, manipulate and gain access to. The asset is the resource you are trying to protect.

3. [3 points] What is management's role regarding information security policies and practices?

   Executive management if information security involves the CIO chief information officer and the CISO chief information security officer who are responsible for advising the chief executive officer, president or company owner on the strategic planning that affects management of information in the organization and the assessment, management and implementation of information security in the organization. The use the security policy, standards and practices.

4. [2 points] What are the components of an effective EISP? How does the EISP differ from the ISSP and the two SysSPs?

   The EISP enterprise information security policy is the general security policy its components may include:

   - The statement or purpose- which answers the question What is this policy for? and provides a framework that helps the reader understand the documents intention.
   - The Information Technology Security Elements which define information security and can lay out security definitions or philosophies to clarify the policy.
   - The Need for Information Security Responsibilities and Roles- Provides information on the importance of information security in the organization and the obligation to protect the assets.
   - The Information Technology Security Responsibilities and Roles which defines the organizations structure designed to support information security, identifies categories of individuals with responsibility for information security and their information security responsibilities.
   - The Reference to Other Information Technology Standards and Guidelines which lists other standards that influence and are influenced by the policy which may include laws.

   The Issue-Specific Security Policy (ISSP) instructs employees on the proper use of technologies and processes like the use of company-owned networks and the Internet. The ESIP is the general security policy and the ISSP is the guidelines on how the equipment is used. The Systems-Specific Policy (SysSPs) are used to target things like implementation and configuration of technology or access control lists which determine what users can access.

5. [2 points] What is a security perimeter and what are the different types of perimeters organizations should look to implement?

   The security perimeter is the boundary between the outer limit of the organization's security and the beginning of the outside world. Different types of perimeters should look to implement are DMZs, firewalls, proxy servers and intrusion detection systems.

6. [4 points] Compare and contrast "spheres of security" (figure 1-10 on page 29) against "defense in depth,"

   Spheres of security presents information security in a sphere graphic to illustrate the different areas of information security needed. The basic shows the asset or information in the middle of the sphere with users on one side and systems, networks and internet on the other which can be broken down even further with the barriers between and around the different area housing controls and policies. Things like firewalls would be found in the barrier between systems and networks and education and training between people and information. Defense in depth is a layered implementation of security which would illustrate your server or asset being protected by layers of security which may include intrusion detection systems, then filtering routers, then a dual homed host which is then behind another external filtering router. So, there are layers of protection before your asset.

7. [8 points] Research the ISO 27000 series of standards and the NIST 800 series of standards. Briefly compare and contrast the two. Include information about the goals of each, the approach each takes, and the applicability of each to, say, a midsize healthcare organization. *Note: I would expect to see some citations in this answer; please go beyond Wikipedia.*

   The ISO 27000 series of standards are a family of standards that are best practices to help an organization improve their information security you must pay for the ISO 27000 series of standards. The NIST 800 comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities. The NIST 800 are free to use. If a midsize healthcare organization were going to use ISO 27000, they would go through each of the parts of the series to set up there EISP. The first step would give them an overview of everything they must do to set up security the following steps address things like the controls (ISO 27002) and how to protect sensitive information (ISO 27017 and 27018). The organization can be audited on the ISO 27001 standard as it serves as a sort of checklist. The midsize healthcare organization would do much the same process with the NIST 800 Publications and use them as a guideline to develop their security program publications like NIST 800-53 defines recommended security controls for federal information systems and organizations.

8. [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 felt comfortable with this week's topics. I have covered them several times before, done my own research reading books and websites and attending security conferences where there are discussions about the topics. I like the way the book we use breaks the subject of network security down into sections that make sense and fit together.

   I tend to lose some interest in the policy and management part of the process although I really read up on it and listened to what you had to say during our MEET session. I guess it's because the actual process of protecting the assets is more interesting to me. I don't mind the mapping of the security network but getting in and configuring routers, firewalls working with intrusion detections systems feels awesome for me. I want to see the attacks and prevent them sort the front lines kind of mentality. I feel slightly put off by the management side of it to be honest. I am not a young guy; I will be 50 this year. I have found that management in my lifetime is often a popularity contest and policy like politics gets to be political. I am very interested to see how it all shakes down in information security because if someone with an ego and popularity goes against the nuts and bolts of securing a network with their own ideas a breach would be very possible. To be fair everyone management person I have met at the security conferences seems to be well put together and someone I would love to work with. In manufacturing masculinity, posturing, bravado, and ego are a real problem. I have a hard time with them because I feel like they get in the way of getting real work done. I see a lot of ego and bravado in my classes as everyone is eager to prove that they are worthy. I understand but hope I am in a position where that stuff doesn't have to be a focal point of conversations and folks can put their brains together to do something great. I feel like people are needed so bad in information security that every conversation doesn't have to be filled with what everyone knows or what they have done but what we can do together. We will see. I appreciate your breakdown of the topics with your experience it gives a good light on them and helps me to understand them from a matter of a fact point of view.

References

Irwin, L. (2019, October 10). *it governance*. Retrieved from What is the ISO 27000 series of standards: https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards

NIST. (2018, May 21). Retrieved from Information Technology Laboratory: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

NIST SP 800 Series and Documents. (n.d.). Retrieved from FLANK protecting your perimeter: https://flank.org/faqs/what-are-the-nist-sp-800-series-publications

Savill, J. (2008). *The Complete Guide to Windows Server 2008.* Addison-Wesley Professional.