Enterprise Security exam (18/01/2021)

Question 1

1. Habibzadeh et. al. suggests that, “Security level in smart cities is responsible for the vulnerabilities of all other levels”. In your opinion, are present security management frameworks apt for validating the security level of smart cities? Discuss with the help of at least two examples. (4 points)
2. Taking into account the discussion in Habibzadeh et. al. answer the following question: Use an attack tree to analyse the steps an attacker may take to impact the confidentiality & integrity of IT systems in a smart city. In your opinion, what measures can smart city management take in order to defend against attacks on confidentiality & integrity. (6 points)

Question 2

1. We have learnt from interviews of burglars that their actions are aimed at:

   - Minimizing effort.
   - Maximizing gains.
   - Minimizing risks.

   In your opinion, does EBIOS assume that the actions of cyber criminals are also aimed at the above mentioned objectives? Explain by analysing the steps of EBIOS risk analysis method. (5 points)

2. What is the distinction between cyber attack, cyber crime and cyber terrorism? Should a small & medium enterprise’s security strategy be aimed at defending against all three of them? Why? (5 points)

Question 3

1. There exist symmetric and asymmetric techniques for ensuring data integrity and data confidentiality.

   A. Give for each combination (i.e., Symmetric and data integrity, symmetric and data confidentiality, asymmetric and data integrity, asymmetric and data confidentiality) an example algorithm together with an example use-case. (2 points)

2. Assume a communication system with 100 participants where each participant should be enabled to securely communicate with every other participant of the system. (3 points)

    A. Explain the difference between symmetric and asymmetric cryptography. (2 points)
    B. For this specific communication system, compare the number of required keys based on a design using only symmetric cryptography with a design using asymmetric as well cryptography. (1 point)

3. With the advent of quantum computing, asymmetric cryptography that is currently used in real systems can be broken. For example, an attacker with access to quantum computers can calculate the private key given only the public key. (3 points)

    A. With that knowledge, evaluate the threat of quantum computing on existing systems. Distinguish between digital signatures and public key encryption in your evaluation. Take the factor of time into your evaluation, that is, the point in time the quantum computer is available and the effect on the protected data. (2 points)
    B. Explain how you would address this upcoming threat. (1 point)

4. "On the server, passwords should be stored in encrypted form using a hash function."

    A. Discuss this sentence and put it into context where this should be applied. (2 points)

Question 4

1. Explain the components of costs incurred by organisations due to cyber-crime. In your opinion, which one of these components account for the biggest proportion of costs for a medium sized internet service provider (such as Speak-up)? Give at-lease two reasons (with references) in support of your answer. (5 points)
2. One of the biggest security decisions faced by organisations is weather to build security competencies inhouse or to outsource them. Explain, in your words, what factors should organisations consider in order to make this decision. Can return on security investments (ROSI) be used as a metric to make this decision? If yes, explain how? If no, explain why not? (5 points)

Question 5

A website can be targeted by different attacks. In the following, all questions refer to a website (and the corresponding web server hosting the website) that is assumed to be attacked.

1. “Cross-Site scripting vulnerabilities are not severe since they do not target the server but only the client.” (2 points)

    A. What is Cross-Site scripting (XSS)? (1 point)
    B. Do you agree with that statement? (1 point)

2. DoS attacks are another common attack that target web servers. (3 points)

    A. Explain what a DoS attack is. (1 point)
    B. What does a DoS attack target on the CIA triad? (1 point)
    C. How does BGP blackholing help to deal with DoS attacks? (1 point)

3. Websites rely on stored data and this data is often stored in a MySQL database. A vulnerability for such systems is called MySQL injection (SQLi) (2 points) .

    A. Briefly explain what SQLi is and how it can be mitigated. (1 point)
    B. Give an example, what an attacker can achieve with SQLi. (1 point)

4. Rank the three attacks from in this question: XSS, DoS, SQLi for the example scenario of a website. You are free in the metric choice for this ranking. Explain your metric and also the reasoning for your ranking based on this metric. (3 points)