Veton Abazovic

NetId: va187

Computer Security

2/6/2019

Assignment 1

Question 1.

What three Internet-enabled vulnerability categories does Paul Rosenzweig identify in his essays on cyberwarfare?

Answer: The three Internet-enabled vulnerability categories that Paul Rosenzweig identifies in his essays on cyberwarfare are:

1. Anonymity- the condition of being anonymous. Paul Rosenzweig talks about how it is difficult to pinpoint the attacker.
2. Lack of Distinction – Rosenzweig describes how it is challenging to determine if something is an attack on the system or not when looking at a bunch of 1's and 0's.
3. Asymmetry of power – Rosenzweig defines this as it is not necessary to require a significant amount of resources to become a threat.

Question 2.

Why are scams with a minuscule chance of success deployed?

Answer: The reason scams with a minuscule chance of success are deployed because the coward is so massive that even if the likelihood of success is small, there is a good possibility that it could work. Another factor is due to the fact they don't require much resources to deploy.

Question 3.

Starting in May 2018, companies doing business in Europe had to comply with the GDPR, the General Data Protection Regulation. This wikipedia article summarizes this regulation and this article specifically focuses on anonymization and pseudonymization.

Briefly explain the difference between anonymization and pseudonymization.

Answer: Anonymization and pseudonymization are both highly recommended by the GDPR to mask data in order to reduce risk. The difference between the two is in the way they categorize personal data. Anonymization techniques are to present the data where is it no longer identifiable by removing all identifying information present. Pseudonymization, on the other hand, improves privacy by replacing a large amount of identifying fields in the data. It does this by dividing the data into two parts identifiable and unidentifiable.

Question 4.

What four components constitute security engineering?

Answer: The four components that constitute security engineering are the following:

1. Policy
2. Mechanism
3. Assurance
4. Incentive