Dated:11/22/2021
Hardeep Kaur Dhalla UWSP, Fall 2021

Assign 11

Alex Smetana

Due Date and time: 11/29/2021 11:59 pm **3 points**

Type in the document and submit to Canvas submission folder.

1. For a given medical/patient record system in Mentcare case study, define an asset, exposure, a vulnerability, attack, threat, and control. 1.5 pts.

Patient database (for example)

Asset – An asset is something that a company would like to protect. Information such as name, address, DOB, social security number, and all medical records would be considered assets in a Mentcare system. Any sort of PII information would be considered as an asset.

Vulnerability – Venerability is a weakness in a computer-based system. An example of this would be a person's password. If an user has a weak password, this has the possibility to expose confidentiality. A way to fix this is to require longer password or use MFA.

Attack – An attack is an exploitation of a systems. For example, a Denial-of-Service Attack is an attack that hurts the Availability in the CIA triad. It prevents a user from accessing information in a timely fashion. This would prove very hurtful in a mentcare system.

Threat – A threat is a circumstance that has the potential to cause harm. An example of a threat is any type of malware. For example, viruses, trojans, rabbits, rats, PUPs, etc. Malware has the potential to wreck a computer and system. In a mentcare system it is crucial to protect against malware. If not protected against, it could have bad consequences.

Control – Is a protective measure that will reduce a systems vulnerability. For example, an access control, which will help limit what information that each user is able to understand. In a mentcare system, limiting the amount of personal data that each employer is able to access will help reduce the possibility of an attack. Some other examples of controls are firewalls and AV software.

2. Suggest how you would go about validating a password protection system for an application that you have developed. Explain the function of any tools that you think may be useful. 1.5 pts.

When implementing a password validation system, I would first start off by requiring a password to have a long length. At least 8+ characters with a minimum of one capitalized letter and a number. This is to ensure that a password wouldn't be able to be brute forced. Doing this would eliminate easy passwords such as, "12345678" or "password." I would require the user to confirm either an email or a phone number and require them to confirm themselves to ensure that this person is real. Finally, I would make sure that every time that a person logged in, that the system requires them to use multi factor authentication to ensure that the information remains safe. If we are dealing with a mentcare system, it is crucial to make sure that all the medical records stay safe.