ENPM809W - Secure Coding

Homework - 1

Author: Syed Mohammad Ibrahim
Directory Id: iamibi

1. Give an example of a repudiation threat in a web server application scenario given in the reading.
A. An attacker deletes or modifies the audit logs.

2. Explain how the repudiation threat example works by giving an example.
A. An attacker if is able to escalate their privileges in the web server and can become an admin with permissions to read/write/update audit logs, may try to cleanup any existence of them on the server so that it can't be traced back to them and also, might cleanup other critical information like how many active user sessions are currently happening.

3. Give an example, not given in the reading, of an elevation of privilege threat in a web server application scenario.
A. An example of elevation of privilege threat is when an attacker executes a XSS (cross-site scripting) attack to gain control of a valid user's session cookies through which they are able to access the compromised user's account and use the privileges that come with it.

4. What is the type of threat from STRIDE in the following scenario?A web server serving application traffic is attacked using an ARP cache poisoning or ARP spoofing attack.
A. ARP Cache Poisoning - Tampering with Data
   ARP Spoofing Attack - Spoofing Identity

5. What is the type of threat from STRIDE in the following scenario? A web server serving application traffic is suddenly brought down by a DDoS attack
A. Denial of Service