Krutarth Panchal

CIS 450

Week 8 - Web Application Security and Exploitation

1. Why is it necessary to pen test web applications? (Logic Question)

It is necessary to pen test a web application because web application store, process, and transmit lots of data, where web application pen test can be use to determine any security weakness of the web application and its components which help developer to identify the vulnerabilities and threats.

1. What are three industry verticals that utilize web applications?

The three industry verticals that utilize web applications are Consumers, Commercial / Industrial and Medical.

1. What are seven malware exploits that can compromise Linux systems?

The seven malware exploits that can compromise Linux systems are:

1. Mirai
2. BASHLITE
3. Carna
4. Linuc.Darlloz
5. Linux.Wifatch
6. Bricker Bot
7. Hajime
8. The seven exploits on page 196 cannot be used to compromise IOT (internet of things) devices. (T or F)

True

1. What are the top 10 OWASP web application security risks and their corresponding risk attributes?

The top 10 OWAP web application security risks and their corresponding risk attributes are:

1. Injection: It is the process of adding information into the HTTP requests sent to the server.
2. Broken Authentication: It is the re-use of username and password across all devices, invalid session handling and insecure storage of credentials.
3. Sensitive Data Exposure: It is a process of gathering data in an unencrypted or non-tokenized format, essentially clear-text or encrypted with and already broken algorithm.
4. XML External (XXE): It can occur when a web service is actively accepting XML directly or allows for uploads from untrusted sources.
5. Broken Access Control: It can occur when a user inputs data that fails outside of what may normally be allowed to be passed to the web server.
6. Security Misconfiguration: These vulnerabilities normally stem from lack of any security implementation or forgetting to remove development code from a production service.
7. Cross-Site Scripting (XSS): It is normally occurring when it the server stores user-based input on the webpage itself, which could then be stores on the webpage, and executed by another user visiting the web pages.
8. Insecure Deserialization: it can occurs at the application level of the web server, and the content that they may provide. If an application or its API has objects that can be tampered with, it can lead to object and data structure attack and typical data tampering attacks.
9. Using Components with Known Vulnerabilities: This can be occurs by using outdated modules within the web application or versions of a publicly vulnerable module in a web application.
10. Insufficient Logging & Monitoring: This is occurs when the customers is not monitoring their logs or they are capturing enough logs.