CSS

Assignment - 2

Q1. Difference between flash events and DOS

→ Flash events a type of attack that is characterized by a large number of requests or message sent to a server in a very short period of time This sudden surge in traffic can overwhelm the server, causing it to crash or become unresponsive. Flash events are typically launched using botnets, which are network of compromised computers that are controlled by a single attacker.

- Denial of Service (DOS) attacks, on the other hand, are designed to disrupt or disable a computers system or network by flooding it with traffic or sending it malformed packets. The goal of a DOS attack is to prevent legitimate users from accessing the targeted systems or service. DOS attacks is to prevent legitimate from accessing the targeted systems or service. DOS attacks can be launched using a variety of methods such as flooding the target with requests, exploiting ~~its~~ vulnerabilities in the target's software, or overloading its network capacity.

Q2. Explain SSL

→ SSL (Secure Socket Layer) is a security protocol that provides secure communication over the internet. It is designed to protect sensitive data, such as passwords credit card numbers, and other personal information from being intercepted and stolen by hackers. SSL works by establishing a secure connection between a web server and a web browser, This is done by using a combination of encryption and authentication technologies to ensure that the data being transmitted is protected from unauthorized access. When a user connects a website using SSL, their web browser sends a request to the web server to initiate a secure connection. The web server responds by sending a digital certificate, which contains a public key that can be used to encrypt data, to the user's web browser.

By using SSL, websites can provide a secure environment for ~~user~~ users to transmit sensitive information without the risk of interception or theft by hackers.

Q3. ~~Vuln~~ Vulnerabilities in ~~Unix~~ Unix and Windows OS.

→ Both Unix and Windows OS are susceptible to vulnerabilities which can be exploited by attackers to gain unauthorized access systems, steal data, or cause disruption. Here are some examples of vulnerabilities that are commonly ~~named~~ found in Unix and Windows OS.

Unix

→ (i) Privilege Escalation

(ii) Buffer Overflow

(iii) Remote Code Execution

(iv) Authentication Bypass

(v) Misconfiguration

Windows Vulnerabilities →

(i) Malware

(ii) Remote Code Execution

(iii) ~~Privilege~~ Privilege Escalation

(iv) DLL Hijacking

(v) Zero-day exploits

Q4. Note on Database security

Database security is the practice of protecting databases and the data they contain from unauthorized access, use disclosure, disruption, modification, or destruction. Databases store sensitive information such as financial records, personal data and confidential business information making them a valuable target for attackers.

Database security involves various measures to protect databases from unauthorized access and ensure data confidentiality, integrity and availability. These measures include →

(i) Access control
(ii) Encryption
(iii) Backup and recovery
(iv) Auditing and Monitoring
(v) Patching and Upgrades.

Q5. Explain SET

SET (Secure Electronic Transaction) is a protocol that is used to secure credit card transactions over the internet. It was developed by Visa and MasterCard to provide a ~~secu~~ secure method for online transactions and prevent credit card. SET works by establishing a secure channel between the customer, the merchant and the banks involved in the transaction. This is done by using digital certificates to authenticate the parties involved and encryption to protect the data being transmitted. By using SET, online transactions are protected from interception and fraud using encryption and digital certificates.

write short note on

① User authentication and session management

User authentication is the process of verifying the identity of a user who is attempting to access a system, network or application. It is a critical component of information security and is used to prevent unauthorized access to sensitive information or resources.

(i) Password-based authentication.

(ii) Multi-factor authentication

(iii) Biometric authentication.

Session management is the process of managing users sessions to ensure that they are secure and protected from unauthorized access. A session is a period of time during which a user has access to a system, network or application.

Session management involves

(i) Session ID generation.

(ii) Session timeout

(iii) Session encryption.

(iv) Session hijacking prevention

② Short note on Cookies

Cookies are small text files that are stored on a user's device (such as a computer or a mobile device) by a website. They are used to remember used preferences and track ~~us~~user activity on a website analytics, advertising and personalization. When a user ~~vits~~ visits a website, the website may send a cookie to the user's device. The cookie contains information about the user's activity on the website, such as their login information or the items they added to their shopping cart. The next time the users visits the website, the website can read the cookie and provide a personalised experience based on the user's activity.

Different types of cookies :-

(i) Session cookies
(ii) Persistent cookies
(iii) First-party cookies
(iv) Third-party cookies.

3. Cross site request forgery

Cross-site Request Forgery (CSRF) is a type of web attack in which a malicious actor tricks a users into performing an action on a website without their knowledge or consent. This is achived by exploiting the user's trust in the website and their browser's ability to automatically send request requests to the website. In a CSRF attack, the attacker creates a web page that contains a form or a script that performs an action on a website without the user's knowledge.

4. Session hijacking and management

Session hijacking is a type of attack in which an attacker gains access to a user's session on a website or application without their knowledge or consent. This is typically done by stealing the user's session ID, which is a unique identifier that is used to keep track of the user's activity on the website. Once the attacker has the user's session ID, they can use it to impersonate the user and perform actions on the website as application on their behalf. This can include accessing the user's account information, making purchases or even changing the user's password

5. Phishing technique

→ Phishing is a social engineering technique used by cybercriminals to trick users into revealing sensitive information, such as login credentials, financial information or personal data. This is typically done by sending emails or messages that appear to be from a legitmate source, such as bank, social media platform or government agency but are actually fake

6. DNS Attack

A DNS attack is a type of cyber attack that targets the Domain Name System (DNS) infrastructure, which is responsible for translating domain names into IP addresses that can be used by computers to access the internet.

There are several types of DNS attacks →

I. DNS Spoofing

II. DNS Cache Poisoning

III. DNS Amplification

IV. DNS Tunneling

Q6- What are different types of firewalls?

→ Firewalls are an important network security tool that can be used to protect against unauthorized access and cyber attacks. There are several types of firewalls each with their own strengths and weaknesses:-

(i) Packet filtering firewall - This type of firewall examines each packet of data that enters or exits a network and blocks any packets that do not meet predefined security rules. Packet ~~fte~~ filtering firewalls are simple and fast, but they may not provide granular control over network traffic.

(ii) Stateful inspection firewall

(iii) Proxy firewall

(iv) ~~Net~~ Next-generation firewall

(v) Cloud firewall

Q 8. How penetration testing is carried out.

Penetration testing also known as pen testing, is a method of assessing the security of a system or network by simulating an attack from a malicious actor. Penetration testing is typically carried out in the following steps →

(i) Planning and reconnaissance.

(ii) Scanning

(iii) Enumeration

(iv) Exploitation

(v) Post-exploitation

(vi) Reporting.