Deepali MCA (1 year)

Assignment-1

Date

Answers:

(1). XSS attack (cross site scripting):

It can be used by infused by putting the malicious code (which gets automatically run) in any comment section or feedback section of any webpage, usually a blogging page. This can also hampers the reputation of a site and the attackers may place any private data or personal credentials.

Cross-site scripting (XSS) is a client-code injection attack. The attackers aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for cross-site scripting attacks are forums, message boards, & web pages that allow comments.

(2). Firewall:

It is a type of filter in network security, allowing or disallowing incoming or outgoing activity based on security measures we specify.

It performs 2 basic functions for a network. These are known as packet filtering and acting as an application proxy. A firewall system analyzes network traffic based on rules. A firewall only welcomes those incoming connections that it has been configured to accept. It does so by allowing or blocking specific data packets units of communication we send over digital networks - based on preestablished security rules.

Spiral

Date

(3) - (a) Spear phishing is an e-mail spoofing attack that targets a specific ~~org~~ organization / individual, seeking unauthorised access to sensitive information such as account credentials, credit card.

(b) Man-in-the-middle (MitM) attack occurs when a hacker inserts itself between the communication of a client & a server. The attacker's computer replaces the client's IP address with own IP address and spoofs the client's sequence numbers.

(c) SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, recover the content of a given file and in some cases, issue commands to the OS.

(4) The Reserve Bank of India governor, Raghuram Rajan launched 'sachet portal' sachet.rbi.org.in to check illegal money collection.

(5) Yes, patching prevents ransomware and malware attacks, as a patch is a piece of code that improves a program already installed into your system, & like as an update, i.e, if a bug is found on a program already installed on your machine, a patch would be created to fix this issue without the need of reworking the entire code. As patch management has the most critical & obvious benefit is better sec. network security. By securing your network, ~~your~~ you

Spiral

Date

can avoid data theft, legal issues and lasting reputation damage.