Assignment 2

Eashwar Shah
60004220126
TY Btech Comps B

Q1 Explain Malware with its types.

Malware short for 'malicious software', refers to any software intentionally designed to cause damage to a computer, server network, or user.

(1) Virus - Programs that replicate themselves by attaching to other files or programs and execute malicious actions when these files are activated.

(2) Worms - Self-replicating malware that spreads across networks by exploiting vulnerabilities in operating systems or applications.

(3) Trojans - Malware disguised as legitimate software or files to trick users into executing them. Once activated, Trojans can create back-doors for attackers, steal sensitive info or cause other malicious activities without the users knowledge

(4) Ransomware - Encrypts files or locks users out of the systems, demanding payments to restore access.

(5) Spyware - Collects sensitive information from infected devices without the users consent, such as login credentials.

(6) Adware - Display unwanted advertisements or redirects users to malicious software, websites, downloads.

daraz
FOR EDUCATIONAL USE
Scanned with CamScanner

Q: Explain & illustrate cross site scripting

Cross site scripting (XSS) is a vulnerability in a web application that allows a third party to execute a script in the users browser on behalf of the web application.

Cross site scripting is one of the most vulnerability present on web today.

The exploitation of XSS against a user can lead to various consequences such as account compromise, account deletion and many more.

Preventing XSS attacks, involves implementing proper input validation and output encoding techniques in web application.

This include filtering and sanitizing, users input to remove or neutralise potentially malicious characters and encoding output to ensure to treated as plain text

Additionally using security mechanisms like: content security policy can help mitigate the risks associated

Depending on content there are two types of XSS

1) Reflected XSS

If the input has to be provided each time to execute such XSS is called reflected.

These attacks are mostly carried out by delivering a payload directly to victim.

2) Stored XSS

When response containing the payload is stored on the server in such a way that the script gets executed on every visit. An example of stored XSS is XSS in the comment thread.

FOR EDUCATIONAL USE

Scanned with CamScanner

Q.3 Explain DOS attack

A Denial of service attacks a floods a target system or network with excessive traffic, rendering it inaccessible to legitimate users.

Attackers exploit vulnerabilities to overwhelm servers, routers or networks, disrupting services and causing down time.

Common types include SYN flood, UDP flood and ICMP flood attacks

DOS attack aim to exhaust resources, leading to system crashes or slowdowns, impacting business operations and user experience.

Mitigation strategies involve implementing network security measures, such as firewalls and intrusions detection systems, to filter and block malicious traffic.

FOR EDUCATIONAL USE

Scanned with CamScanner