Question Bank

Web and Mobile Security (20CST-333)

Short Answer Type(2 Marks)

1. **Who are more knowledgeable hackers and why?**

**Ans: -** White hat hackers are types of hackers who're professionals with expertise in cybersecurity. They are authorized or certified to hack the systems. These White Hat Hackers work for governments or organizations by getting into the system. They hack the system from the loopholes in the cybersecurity of the organization

1. **Who are green hat hackers?**

ANS: - Green hat hackers are types of hackers who learn the ropes of hacking. They are slightly different from the Script Kiddies due to their intention. The intent is to strive and learn to become full-fledged hackers. They are looking for opportunities to learn from experienced hackers.

1. **What is DMZ?**

ANS: A demilitarized zone network, or DMZ, is a subnet that creates an extra layer of protection from external attack. Network administrators must balance access and security. Your employees must tap into data outside of the organization, and some visitors need to reach into data on your servers.

1. **What is the use of CAPTCHA?**

Ans:- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of security measure known as challenge-response authentication. CAPTCHA helps protect you from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account.

1. **Define blue-bugging.**

Ans:- Bluebugging is a hacking technique that lets someone get into your device through your discoverable Bluetooth connection. Through bluebugging, a hacker could listen to your calls, read and send messages, and steal your contacts.

1. **What do you mean by blue-snarfing.**

Ans:- Bluesnarfing is the [unauthorized access](https://en.wikipedia.org/wiki/Access_control) of information from a [wireless device](https://en.wikipedia.org/wiki/Wireless_device) through a [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) connection, often between phones, desktops, laptops, and PDAs ([personal digital assistant](https://en.wikipedia.org/wiki/Personal_digital_assistant)).[[1]](https://en.wikipedia.org/wiki/Bluesnarfing#cite_note-1) This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

1. **How blue-jacking is done?**

Ans: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

1. **What are different types of captcha?**

**Text CAPTCHAs**

**Image CAPTCHA**

**Audio CAPTCHA**

1. **What is dictionary attack?**

Ans: A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

1. **Define ping of death attack.**

Ans: Ping of Death (a.k.a. PoD) is a type of [Denial of Service](https://www.imperva.com/learn/application-security/denial-of-service/) ([DoS](https://www.imperva.com/learn/application-security/denial-of-service/)) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.While PoD attacks exploit legacy weaknesses which may have been patched in target systems.

1. **Define directory traversal attack.**

Ans: Directory traversal is a type of HTTP exploit in which a hacker uses the software on a web server to access data in a directory other than the server's root directory. If the attempt is successful, the threat actor can view restricted files or execute commands on the server.

1. **How buffer overflow is used to perform malicious activities?**

Ans: A buffer overflow attack occurs when a hacker exploits the coding error to perform a malicious activity and compromise the impacted system. The cybercriminal modifies the execution path of the app and overwrites elements of its memory, causing existing files to be damaged or confidential information to be exposed

1. **Explain SIM/UICC Security.**

Ans: -

1. **What is browser exploit?**

Ans: A browser exploit is a type of exploit that takes advantage of a web browser vulnerability in order to breach web browser security. Web browsers provide an ideal entry point for hackers to gain access to devices, due to their direct interface with the Internet.

1. **What are canonicalization attacks?**

Ans: - A canonicalization attack is a cyberattack method in which the attacker substitutes various inputs for the canonical name of a path or file. Typically exploited by entering the file path in an input field or webpage or part of a URL, canonical attacks enable attackers to access unauthorized files and directories on a web server.

1. **What are basic security and cryptographic techniques?**

Ans:- **Confidentiality:**   
The degree of confidentiality determines the secrecy of the information

**Authentication:**   
Authentication is the mechanism to identify the user or system or the entity.

**Integrity:**   
Integrity gives the assurance that the information received is exact and accurate

**Non-Repudiation:**   
Non-repudiation is a mechanism that prevents the denial of the message content sent through a network

**Access control:**   
The principle of access control is determined by role management and rule management.

**Availability:**   
The principle of availability states that the resources will be available to authorize party at all times.

       7. **Issues of ethics and law**  
            The following categories are used to categorize ethical dilemmas in the security system.

1. **Discuss the advantages and disadvantages of Mesh topology.**

Ans: Advantages of Mesh Topology :

* Failure during a single device won’t break the network.
* Adding new devices won’t disrupt data transmissions.
* This topology has robust features to beat any situation.
* A mesh doesn’t have a centralized authority.

Disadvantages of Mesh Topology :

* It’s costly as compared to the opposite network topologies i.e. star, bus, point to point topology.
* There is a high risk of redundant connections.
* Each node requires a further utility cost to think about.
* Maintenance needs are challenging with a mesh.

1. **Define security misconfiguration.**

Ans:- Security misconfigurations are security controls that are inaccurately configured or left insecure, putting your systems and data at risk. Basically, any poorly documented configuration changes, default settings, or a technical issue across any component in your endpoints could lead to a misconfiguration.

1. **What is Bluetooth security?**

Ans: Bluetooth security is used to protect services offered by devices as well as enforce exclusivity, permitting only very specific devices to connect. In accomplishing this end, the security troika was introduced consisting of authentication, authorization, and encryption.

1. **Write down the advantages and disadvantages of bus topology.**

Ans: -  **Advantages of Bus Topology :**

* It works very efficiently well when there is a small network.
* The length of cable required is less than a star topology.
* It is easy to understand topology.
* Easy to expand by joining the two cables together.

**Disadvantages of Bus Topology :**

* Bus topology is not great for large networks.
* Identification of problems becomes difficult if the whole network goes down.
* Troubleshooting individual device issues is very hard.
* Need terminators are required at both ends of the main cable.
* Additional devices slow the network down.

1. **Write down the advantages and disadvantages of star topology.**

## Ans: **Advantages of Star Topology**

* It is very reliable – if one cable or device fails then all the others will still work
* It is high-performing as no data collisions can occur
* Easier to put in
* Robust in nature

## **Disadvantages of Star Topology**

* Requires more cable than a linear bus .
* If hub goes down everything goes down, none of the devices can work without hub.
* Hub requires more resources and regular maintenance because it’s the central system of star .
* Extra hardware is required (hubs or switches) which adds to cost

1. **Define X-path injection attack.**

Ans: - XPath Injection enables an attacker to talk directly to the XML database, thus bypassing the application completely. XPath Injection results from the failure of an application to properly sanitize input used as part of dynamic XPath expressions used to query an XML database.