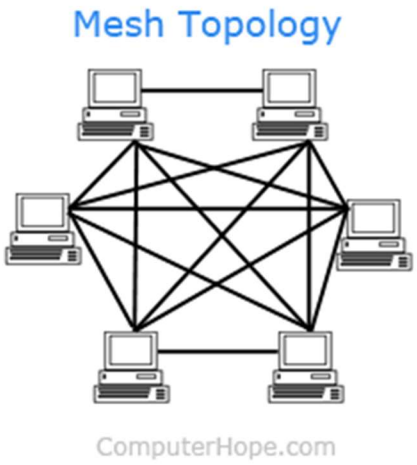
1. Discuss Mesh Topology.

Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

Advantages

Reliable, Fast Communication and Easier Reconfiguration.



2. What is DMZ?

In computer networks, a DMZ, or demilitarized zone, is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet. DMZs are also known as *perimeter networks* or *screened subnetwork*s.

Any service provided to users on the public internet should be placed in the DMZ network. External-facing servers, resources and services are usually located there. Some of the most common of these services include web, email, domain name system, File Transfer Protocol and proxy servers.

Servers and resources in the DMZ are accessible from the internet, but the rest of the internal LAN remains unreachable. This approach provides an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal servers and data from the internet.

3. Explain XSRF attack.

An attacker’s aim for carrying out a CSRF attack is to force the user to submit a state-changing request. Examples include:

- Submitting or deleting a record.
- Submitting a transaction.
- Purchasing a product.
- Changing a password.
- Sending a message.

Social engineering platforms are often used by attackers to launch a CSRF attack. This tricks the victim into clicking a URL that contains a maliciously crafted, unauthorized request for a particular Web application. The user’s browser then sends this maliciously crafted request to a targeted Web application. The request also includes any credentials related to the particular website (e.g., user session cookies). If the user is in an active session with a targeted Web application, the application treats this new request as an authorized request submitted by the user. Thus, the attacker succeeds in exploiting the Web application’s CSRF vulnerability.

4. List types of Bluetooth attacks

1. Bluebugging

Through this Bluetooth attack, hackers can:

- Eavesdrop on phone calls by gaining access to a device.
- Connect themselves to the user’s Internet.
- Receive and send text messages and emails.
- Make calls, when the owner of the device is unaware of it.

This kind of attack generally happens in **phones with older models**.

2. Bluejacking

Bluejacking is not as serious as the other Bluetooth attacks.

It is a common and harmless attack that was earlier used to prank people.

Through this, the hacker can only send text messages to the hacked device. It doesn't give them access to your smartphone or the data in it.

So, to tackle this problem, keep your Bluetooth **settings non-discoverable or invisible**, or just ignore the received messages.

3. Bluesnarfing

Out of the different types of Bluetooth attacks, this is one of the most **dangerous**.

When hackers are within 300 feet of a device, they can conduct a bluesnarfing attack (around 90 meters).

This happens because, even if your device is set to non-discoverable mode, hackers can still attack and access your personal information.

They can also copy the data on your device, including your photos and videos, phone number, contact list, emails, and passwords.

Thus, keep your Bluetooth in **invisible mode**. Since it makes it difficult for hackers to figure out the model and name of your device.

4. Location Tracking

This attack is one of the different types of Bluetooth attacks that occur on locating and tracking devices.

Fitness lovers are more vulnerable to this attack since their fitness devices are always linked to their Bluetooth.

5. Describe GSM algorithms.

GSM uses three different security algorithms called **A3, A5, and A8**. In practice, A3 and A8 are generally implemented together (known as A3/A8). An A3/A8 algorithm is implemented in Subscriber Identity Module (SIM) cards and in GSM network Authentication Centres.

6. What it scripting language? Explain its types.

All scripting languages are programming languages. The scripting language is basically a language where instructions are written for a run time environment. They do not require the compilation step and are rather interpreted. It brings new functions to applications and glue complex system together. A scripting language is a programming language designed for integrating and communicating with other programming languages.

There are many scripting languages some of them are discussed below:

- **bash:** It is a scripting language to work in the Linux interface. It is a lot easier to use bash to create scripts than other programming languages.
- **Node js:** It is a framework to write network applications using **JavaScript**. Corporate users of Node.js include IBM, LinkedIn, Microsoft, Netflix, PayPal, Yahoo for real-time web applications.
- **Ruby:** Its flexibility has allowed to create innovative software.
- **Perl:** A scripting language with innovative features to make it different and popular. Found on all windows and Linux servers

7. What is CAPTCHA and how does it work?

CAPTCHA stands for the Completely Automated Public Turing test to tell Computers and Humans Apart. CAPTCHAs are tools you can use to differentiate between real users and automated users, such as bots. CAPTCHAs provide challenges that are difficult for computers to perform but relatively easy for humans.

Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to identify letters. The letters are distorted so that bots are not likely to be able to identify them. To pass the test, users have to interpret the distorted text,

type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again. Such tests are common in login forms, account signup forms, online polls, and e-commerce checkout pages.

8. How input injection attack is performed? Explain all methods.

During an injection attack, an attacker can provide malicious input to a web application (inject it) and change the operation of the application by forcing it to execute certain commands.

An injection attack can expose or damage data and lead to a denial of service or a full webserver compromise. Such attacks are possible due to vulnerabilities in the code of an application that allows for unvalidated user input.

SQL Injection (SQLi): SQL is a query language to communicate with a database. It can be used to perform actions to retrieve, delete and save data in the database.

Cross-Site Scripting (XSS): Whenever an application allows user input within the output it generates, it allows an attacker to send malicious code to a different end-user without validating or encoding it. XSS takes these opportunities to inject malicious scripts into trusted websites.

Code Injection: In this scenario, an attacker is acquainted with the application code and programming language. By exploiting a vulnerability, they may attempt to inject code into the application to be executed as a command by its web server.

CCS Injection: A CCS injection exploits a vulnerability found in the Change Cipher Spec processing in some versions of OpenSSL.

SMTP/IMAP, Host Header Injection, LDAP Injection and CRLF Injection.

9. Explain different session hijacking and fixation techniques. How session hijacking is done?

Active Session Hijacking : An Active Session Hijacking occurs when the attacker takes control over the active session. The actual user of the network becomes in offline mode, and the attacker acts as the authorized user. They can also take control over the communication between the client and the server.

Passive Session Hijacking : In Passive Session Hijacking, instead of controlling the overall session of a network of targeted user, the attacker monitors the communication between a user and a server.

Hybrid Hijacking : The combination of Active Session Hijacking and Passive Session Hijacking is referred to as Hybrid Hijacking. In this the attackers monitors the communication channel (the network traffic), whenever they find the issue, they take over the control on the web session and fulfill their malicious tasks.

Session Hijacking. Those methods are:

1. Brute Forcing the Session ID
2. Cross-Site Scripting (XSS) or Misdirected Trust
3. Man in the browser
4. Malware infections
5. Session Fixation
6. Session side-jacking

10. Discuss encryption process of mono-alphabetic cipher working.

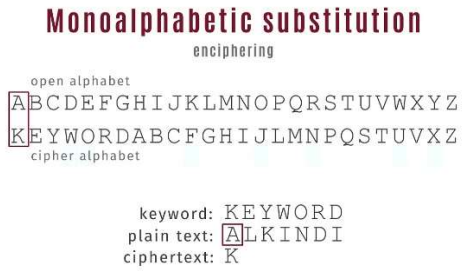
The substitution cipher is the oldest forms of encryption algorithms according to creates each character of a plaintext message and require a substitution process to restore it with a new character in the ciphertext.

This substitution method is deterministic and reversible, enabling the intended message recipients to reverse-substitute ciphertext characters to retrieve the plaintext.

The specific form of substitution cipher is the Monoalphabetic Substitution Cipher, is known as “Simple Substitution Cipher”. Monoalphabetic Substitution Ciphers based on an individual key mapping function K, which consistently replaces a specific character α with a character from the mapping K (α).

A mono-alphabetic substitution cipher is a type of substitution ciphers in which the equivalent letters of the plaintext are restored by the same letters of the ciphertext. Mono, which defines one, it signifies that each letter of the plaintext has a single substitute of the ciphertext.

Caesar cipher is a type of Monoalphabetic cipher. It uses the similar substitution method to receive the cipher text characters for each plain text character. In Caesar cipher, it can see that it is simply for a hacker to crack the key as Caesar cipher supports only 25 keys in all. This pit is covered by utilizing Monoalphabetic cipher.



11. Differentiate between all topologies along with advantages.

Bus topology

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

Advantages of Bus topology:

Low-cost cable, Familiar technology, Moderate data speeds and Limited failure.

Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.

Advantages of Ring topology

Network Management, Product availability, Cost and Reliable.

Star Topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

Advantages of Star Topology

Efficient troubleshooting, Network control, Limited Failure, Familiar Technology, Easily Expandable, Cost Effective and High Data Speeds.

Tree Topology

- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.

Advantages

Support for broadband transmission, Easily expandable, Easily manageable, Error detection Limited failure, Point-to-point wiring

Mesh Technology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

Advantages

Reliable, Fast Communication and Easier Reconfiguration.

Hybrid Technology

- The combination of various different topologies is known as Hybrid topology.
- A Hybrid topology is a connection between different links and nodes to transfer the data.

Advantages

Reliable, Scalable, Flexible and Effective.

12. Explain remote server security attacks? Explain all methods? Explain mitigations.

An attacker could breach a system via remote access by:

- Scanning the Internet for vulnerable IP addresses.
- Running a password-cracking tool.
- Simulating a remote access session with cracked username and password information.

Once inside the system, the attacker may upload malware, copy all sensitive data, and use the compromised system to attack other computers or network within the same environment. The malware will continue to steal data even after the attacker logs out and may go undetected for a long period of time.

DoS attacks

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users.

DNS Poisoning

Using DNS (Domain Name Server) poisoning, hackers can trick the DNS server of any computer into believing that fake data is legitimate and authentic.

Port scanning

Port scanning is used to determine which computer ports are open on a network host. A port scanner is software designed to find such ports.

TCP desynchronization

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number.

SMB Relay

SMB Relay and SMBRelay2 are special programs that are capable of carrying out attacks against remote computers.

ICMP attacks

ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Mitigation, or Attack Mitigation, is the reduction in severity or seriousness of an event. In cybersecurity, mitigation is centered around strategies to limit the impact of a threat against data in custody.

Threats against data can come from outside attackers motivated by profit, activism, retribution, or mischief. Insider threats may have the same motives but could be tied to workplace issues resulting in people abusing their access privileges to inflict harm.

In either case, it is the responsibility of a data owner to protect data from misuse, disclosure, theft, unauthorized exposure, wrongful transmission, and so on while still making the data useful and available to conduct business. To that end, a mitigation strategy should be strict in accordance with risk appetites and realistic enough to allow for the licit use of the data by those authorized.

13.

a) **How CSS attack is performed? Explain methods and solutions.**

To carry out a cross site scripting attack, an attacker injects a malicious script into user-provided input. Attackers can also carry out an attack by modifying a request. If the web app is vulnerable to XSS attacks, the user-supplied input executes as code. For example, in the request below, the script displays a message box with the text “xss.”

http://www.site.com/page.php?var=<script>alert('xss');</script>

There are many ways to trigger an XSS attack. For example, the execution could be triggered automatically when the page loads or when a user hovers over specific elements of the page (e.g., hyperlinks).

Potential consequences of cross site scripting attacks include these:

- Capturing the keystrokes of a user.
- Redirecting a user to a malicious website.
- Running web browser-based exploits (e.g., crashing the browser).
- Obtaining the cookie information of a user who is logged into a website (thus compromising the victim’s account).

Stored XSS. Takes place when the malicious payload is stored in a database. It renders to other users when data is requested—if there is no output encoding or sanitization.

Reflected XSS. Occurs when a web application sends attacker-provided strings to a victim's browser so that the browser executes part of the string as code. The payload echoes back in response since it doesn't have any server-side output encoding.

DOM-based XSS. Takes place when an attacker injects a script into a response. The attacker can read and manipulate the document object model (DOM) data to craft a malicious URL. The attacker uses this URL to trick a user into clicking it.

Solutions

- Never trust user input.
- Implement output encoding.
- Perform user input validation.
- Follow the defense in depth principle.
- Ensure that web application development aligns with OASP's XSS Prevention Cheat Sheet.
- After remediation, perform penetration testing to confirm it was successful.

b) How XML attack is performed? Explain methods and solutions.

XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any back-end or external systems that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (SSRF) attacks.

- Exploiting XXE to retrieve files, where an external entity is defined containing the contents of a file, and returned in the application's response.
- Exploiting XXE to perform SSRF attacks, where an external entity is defined based on a URL to a back-end system.
- Exploiting blind XXE exfiltrate data out-of-band, where sensitive data is transmitted from the application server to a system that the attacker controls.

- Exploiting blind XXE to retrieve data via error messages, where the attacker can trigger a parsing error message containing sensitive data.

Solutions

Leveraging Automation for Identification of XXE

A majority of XXE vulnerabilities are identified reliably, swiftly, and accurately by an intelligent, automated, and hassle-free web application scanner backed with Global Threat Intelligence.

Application Security Testing Performed by Security Experts

Some kinds of XML External Entities are not identified by automated web scanning tools such as blind XXE, file retrievals, and XInclude attacks.

Managed WAF with Custom-Defined Rules

Traditional WAFs are bypassed rather easily by attackers exploiting the XXE vulnerabilities in the application.

Disabling DTD Support

External DTD is designed to be utilized by trusted parties. However, it is a legacy feature and often, leveraged by malicious actors to attack web applications.