UNIT-III

SECURITY ISSUES ON WEB

Cyber criminals use a wide range of methods to exploit web security. Some of the most commonly deployed types of web security threats include:

Phishing

Phishing attacks involve attackers targeting users through email, text messages, or social media messaging sites. They pose as a sender the user trusts to trick them into giving up sensitive information like account numbers, credit card data, and login credentials. A successful phishing attack can also result in cyber criminals gaining unauthorized access to corporate networks, enabling them to steal business data.

Phishing is most commonly committed through email, which remains the most significant attack vector.

Ransomware

Ransomware is a form of malware that results in an attacker holding their victim's data or computer hostage. The attacker threatens to block access to, corrupt, or publish the data unless their victim pays a ransom fee.

Ransomware attacks are typically initiated through phishing emails that contain malicious attachments or links that lead the user's computer to download malware. The device gets infected by the malware, which looks for files to encrypt and prevents users from accessing them. Ransomware is also spread via drive-by downloading, which occurs when users visit an infected website that downloads malware onto their device without them knowing.

SQL Injection

Structured Query Language (SQL) is a computing language used to search and query databases. SQL injection is a web security threat in which attackers exploit vulnerabilities in the application code. Attackers achieve this by inserting an SQL query in standard online form fields, such as login boxes on a website, which are passed to the application's SQL database.

SQL injection attacks have succeeded in exploiting vulnerabilities on shared codebases like WordPress plugins. A vulnerability in the code can lead to hundreds of thousands of websites using the code being hacked. Attackers use this web security issue to steal corporate data, such as customer files and financial information.

Cross-site Scripting

Cross-site scripting (XSS) is a form of web security issue that enables attackers to execute malicious scripts on trusted websites. In an XSS attack, web applications or pages are used to submit malicious code and compromise user interactions. The attacker can then seize a user's

identity to carry out malicious activity, gain authorized access to corporate information, or steal their data.

The script used in XSS attacks prevents users' browsers from identifying malicious activity. The attacker is therefore free to browse the user's cookies, sensitive data, and session tokens stored in their browser.

Distributed Denial-of-service (DDoS) attack

A DDoS attack is a web security threat that involves attackers flooding servers with large volumes of internet traffic to disrupt service and take websites offline. The sheer volume of fake traffic results in the target network or server being overwhelmed, which leaves them inaccessible.

DDoS attacks are often carried out by disgruntled employees or hacktivists who want to cause harm to an organization by taking their server offline. Others are done for the fun of exploiting cyber weakness, and many DDoS attacks are financially motivated, such as certain organizations stealing information from their competitors. They can also be used as part of a ransomware attack.

Viruses and Worms

Viruses and worms are malicious programs that spread through computers and networks. Both exploit software vulnerabilities that allow an attacker to steal data from systems. Viruses and worms also install backdoors into systems that an attacker can use to gain unauthorized access, corrupt files, and inflict broader damage to a company.

Worms, in particular, eat up vast amounts of computer memory and network bandwidth, which leads to servers, systems, and networks overloading and malfunctioning. Worms can operate independently, enabling them to spread between systems, but a virus requires a host computer to carry out malicious activity.

Spyware

Spyware is a form of malware that gathers data from users and their devices then sends it to third-party individuals without consent. Spyware typically collects sensitive information and shares it with advertisers, data collection firms, and cyber criminals, who can use that data to make a profit. It is also used to steal and sell user data like bank accounts, credit card numbers, login credentials, and internet usage information—or to commit broader identity fraud and identity spoofing.

Spyware can be difficult to identify and can cause severe damage to devices and networks. It can also leave a business vulnerable to data breaches, affect device and network performance, and inhibit user activity.

FIREWALL

In simple terms, it acts as an intermediary or wall of separation between the insecure internet and secure internal network which may be a computer, company network, or home network. Separating the internet from your internal network traffic is the default function of most firewalls.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

Importance of Using a Firewall :

The following points listed below are the most relevant in explaining the importance of firewalls is as follows.

Monitoring Network Traffic –

Firewall security starts with effective monitoring of network traffic based on pre-established rules and filters to keep the systems protected. Monitoring of network traffic involves the following security measures.

Source or destination-based blocking of incoming network traffic –

This is the most common feature of most firewalls, whereby the firewalls block the incoming traffic by looking into the source of the traffic.

Outgoing network traffic can be blocked based on the source or destination –

Many firewalls can also filter data between your internal network and the Internet. You might, for example, want to keep employees from visiting inappropriate websites.

Block network traffic based on content –

More modern firewalls can screen network traffic for inappropriate content and block traffic depending on that. A firewall that is integrated with a virus scanner, for example, can prevent virus-infected files from entering your network. Other firewalls work in tandem with e-mail services to filter out unwanted messages.

Report on network traffic and firewall activities –

When filtering network traffic to and from the Internet, it's also crucial to know what your firewall is doing, who tried to break into your network, and who tried to view prohibited information on the Internet. A reporting mechanism of some sort is included in almost all firewalls.

Stops Virus Attacks and spyware –

With cyber thieves creating hundreds of thousands of new threats every day, including spyware, viruses, and other attacks like email bombs, denial of service, and malicious macros, it's critical that you put protections in place to keep your systems safe

Preventing Hacks –

Cyber threats are evolving at a fast pace and are widespread. Firewalls keep hackers out of your data, emails, systems, and other sensitive information. A firewall can either entirely block a hacker or push them to choose a more vulnerable target.

Promotes Privacy –

Having a firewall keeps the data safe and builds an environment of privacy that is trustworthy and a system without a firewall is accepting every connection into the network from anyone. Without a firewall, there would be no way to detect incoming threats.

COMPONENTS OF A FIREWALL SYSTEM

The components of firewall system are explained below −

Perimeter Router

It is used to provide a link to the public networking system like the internet, or a distinctive organization. It performs the routing of data packets with the help of an appropriate routing protocol. It also provides the filtering of packets and addresses translations.

Firewall

The provision of distinctive levels of security and supervises traffic among each level. Most of the firewalls are present near the router that provides security from external threats, but sometimes the firewall is present in the internal network to protect from internal attacks.

Virtual Private Network (VPN)

Its function is to provide a secure connection among two machines or networks. It consists of encryption, authentication, and packet-reliability assurance. It provides the secure remote access of the network, thereafter connecting two WAN networks on the same platform while not being physically connected.

Intrusion Detection System (IDS)

It is used to identify, investigate, and resolve unauthorized attacks. A hacker can attack the network in various ways. It can execute a denial-of-service (DoS) attack or an attack from the backside of the network through some unauthorized access. An IDS solution should be smart enough to deal with these types of attacks.

Transactions Security

- When you go in a market and you use a POS for payment, then a transaction occurs.
- In your mobile phone when you download an android app to order something like the eBay app.
- When you pay something through an online payment service like paypal.com.

Generally a secure transaction happens in an encrypted form which happens between the site that we are connected to and the browser that we are using. It happens through a file in which the website provides its details, which we will deal further in the following sections. A

simpler indication is recognizing the difference between a secure and insecure connection of which **Https://** is a secured site, while **Http://** is not secured.

If you or your users are using Google Chrome, you can push them to always connect securely, if the webpage supports it. Always prefer the HTTPS extension, if you are using a Mozilla Firefox there is an add-on called **HTTPS Everywhere**.

We should do a transaction only through webpages that we know or when they have a good reputation. So, in simple words you should visit those webpages that you trust and even though you trust, it is recommended to do the transactions through payment gateways like PayPal, so you don't transmit bank account details to third parties.

CLIENT-SERVER

The Client-server model is a distributed application structure that partitions task or workload between the providers of a resource or service, called servers, and service requesters called clients. In the client-server architecture, when the client computer sends a request for data to the server through the internet, the server accepts the requested process and deliver the data packets requested back to the client. Clients do not share any of their resources. Examples of Client-Server Model are Email, World Wide Web, etc.

How the Client-Server Model works ?

In this article we are going to take a dive into the Client-Server model and have a look at how the Internet works via, web browsers. This article will help us in having a solid foundation of the WEB and help in working with WEB technologies with ease.

Client: When we talk the word Client, it mean to talk of a person or an organization using a particular service. Similarly in the digital world a Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: Similarly, when we talk the word Servers, It mean a person or medium that serves something. Similarly in this digital world a Server is a remote computer which provides information (data) or access to particular services.

So, its basically the Client requesting something and the Server serving it as long as its present in the database.

There are few steps to follow to interacts with the servers a client.

- User enters the **URL**(Uniform Resource Locator) of the website or file. Th
- Browser then requests the **DNS**(DOMAIN NAME SYSTEM) Server.
- **DNS Server** lookup for the address of the **WEB Server**.

- **DNS Server** responds with the **IP address** of the **WEB Server**.
- Browser sends over an **HTTP/HTTPS** request to **WEB Server's IP** (provided by **DNS server**).
- Server sends over the necessary files of the website.
- Browser then renders the files and the website is displayed. This rendering is done with the help of **DOM** (Document Object Model) interpreter, **CSS** interpreter and **JS Engine** collectively known as the **JIT** or (Just in Time) Compilers.

Advantages of Client-Server model:
- Centralized system with all data in a single place.
- Cost efficient requires less maintenance cost and Data recovery is possible.
- The capacity of the Client and Servers can be changed separately.

Disadvantages of Client-Server model:
- Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.
- Server are prone to Denial of Service (DOS) attacks.
- Phishing or capturing login credentials or other useful information of the user are common and MITM(Man in the Middle) attacks are common.

E-commerce Security Threats

1. Financial frauds

Ever since the first online businesses entered the world of the internet, financial fraudsters have been giving businesses a headache. There are various kinds of financial frauds prevalent in the e-commerce industry, but we are going to discuss the two most common of them.

a. Credit Card Fraud

It happens when a cybercriminal uses stolen credit card data to buy products on your e-commerce store. Usually, in such cases, the shipping and billing addresses vary.

Another form of credit card fraud is when the fraudster steals your personal details and identity to enable them to get a new credit card.

b. Fake Return & Refund Fraud

The bad players perform unauthorized transactions and clear the trail, causing businesses great losses. Some hackers also engage in refund frauds, where they file fake requests for returns.

2. Phishing

Several e-commerce shops have received reports of their customers receiving messages or emails from hackers masquerading to be the legitimate store owners. Such fraudsters present fake copies of your website pages or another reputable website to trick the users into believing them. For example, see this image below. A seemingly harmless and authentic email from PayPal asking to provide details.

3. Spamming

Some bad players can send infected links via email or social media inboxes. They can also leave these links in their comments or messages on blog posts and contact forms. Once you click on such links, they will direct you to their spam websites, where you may end up being a victim.

4. DoS & DDoS Attacks

Many e-commerce websites have incurred losses due to disruptions in their website and overall sales because of DDoS (Distributed Denial of Service) attacks. What happens is that your servers receive a deluge of requests from many untraceable IP addresses causing it to crash and making unavailable to your store visitors.

5. Malware

Hackers may design a malicious software and install on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, trojan, and ransomware.

The systems of your customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect your website.

6.SQL Injection

It is a malicious technique where a hacker attacks your query submission forms to be able to access your backend database. They corrupt your database with an infectious code, collect data, and later wipe out the trail.

7. Cross-Site Scripting (XSS)

The attackers can plant a malicious JavaScript snippet on your e-commerce store to target your online visitors and customers. Such codes can access your customers' cookies and compute. You can implement the Content Security Policy (CSP) to prevent such attacks.

8.Bots

Some attackers develop special bots that can scrape your website to get information about inventory and prices. Such hackers, usually your competitors, can then use the data to lower or modify the prices in their websites in an attempt to lower your sales and revenue.

NETWORK SECURITY

Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.
The most basic example of Network Security is password protection which the user of the network oneself chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as:

1. Users
2. Locations
3. Data
4. Devices

5. Applications

Types of Network Security

The few types of network securities are discussed below:

1. Access Control
2. Antivirus and Anti-Malware Software
3. Cloud Security
4. Email Security
5. Firewalls
6. Application Security
7. Intrusion Prevention System(IPS)

1. Access Control: Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

2. Antivirus and Anti-malware Software: This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. Malicious software like Viruses, Trojans, and Worms is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well-equipped to fight once it has entered.

3. Cloud Security: Now a day, a lot of many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

4. Email Security: Email Security depicts the services, and products designed to protect the Email Account and its contents safe from external threats. For Example, you generally see, fraud emails are automatically sent to the Spam folder. because most email service providers have built-in features to protect the content.

5. Firewalls: A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules

accepts, rejects, or drops that specific traffic. Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.

6. Application Security: Application security denotes the security precautionary measures utilized at the application level to prevent the stealing or capturing of data or code inside the application. It also includes the security measurements made during the advancement and design of applications, as well as techniques and methods for protecting the applications whenever.

7. Intrusion Prevention System(IPS): An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

Firewall Design

A **Firewall** is a hardware or software to prevent a private computer or a network of computers from unauthorized access, it acts as a filter to avoid unauthorized users from accessing private computers and networks. It is a vital component of network security. It is the first line of defense for network security. It filters network packets and stops malware from entering the user's computer or network by blocking access and preventing the user from being infected.

Characteristics of Firewall

1. **Physical Barrier:** A firewall does not allow any external traffic to enter a system or a network without its allowance. A firewall creates a choke point for all the external data trying to enter the system or network and hence can easily block access if needed.
2. **Multi-Purpose:** A firewall has many functions other than security purposes. It configures domain names and Internet Protocol (IP) addresses. It also acts as a network address translator. It can act as a meter for internet usage.
3. **Flexible Security Policies:** Different local systems or networks need different security policies. A firewall can be modified according to the requirement of the user by changing its security policies.

4. **Security Platform:** It provides a platform from which any alert to the issue related to security or fixing issues can be accessed. All the queries related to security can be kept under check from one place in a system or network.
5. **Access Handler:** Determines which traffic needs to flow first according to priority or can change for a particular network or system. specific action requests may be initiated and allowed to flow through the firewall.

Need and Importance of Firewall Design Principles

1. **Different Requirements:** Every local network or system has its threats and requirements which needs different structure and devices. All this can only be identified while designing a firewall. Accessing the current security outline of a company can help to create a better firewall design.
2. **Outlining Policies:** Once a firewall is being designed, a system or network doesn't need to be secure. Some new threats can arise and if we have proper paperwork of policies then the security system can be modified again and the network will become more secure.
3. **Identifying Requirements:** While designing a firewall data related to threats, devices needed to be integrated, Missing resources, and updating security devices. All the information collected is combined to get the best results. Even if one of these things is misidentified leads to security issues.
4. **Setting Restrictions:** Every user has limitations to access different level of data or modify it and it needed to be identified and taken action accordingly. After retrieving and processing data, priority is set to people, devices, and applications.
5. **Identify Deployment Location:** Every firewall has its strengths and to get the most use out of it, we need to deploy each of them at the right place in a system or network. In the case of a packet filter firewall, it needs to be deployed at the edge of your network in between the internal network and web server to get the most out of it.

FIREWALL DESIGN PRINCIPLES

1. Developing Security Policy

Security policy is a very essential part of firewall design. Security policy is designed according to the requirement of the company or client to know which kind of traffic is allowed to pass. Without a proper security policy, it is impossible to restrict or allow a specific user or worker in a company network or anywhere else. A properly developed security policy also knows what to do in case of a security breach. Without it, there is an increase in risk as there will not be a proper implementation of security solutions.

2. Simple Solution Design

If the design of the solution is complex. then it will be difficult to implement it. If the solution is easy. then it will be easier to implement it. A simple design is easier to maintain. we can make upgrades in the simple design according to the new possible threats leaving it with an efficient but more simple structure. The problem that comes with complex designs is a configuration error that opens a path for external attacks.

3. Choosing the Right Device

Every network security device has its purpose and its way of implementation. if we use the wrong device for the wrong problem, the network becomes vulnerable. if the outdated device is used for a designing firewall, it exposes the network to risk and is almost useless. Firstly the designing part must be done then the product requirements must be found out, if the product is already available then it is tried to fit in a design that makes security weak.

4. Layered Defense

A network defense must be multiple-layered in the modern world because if the security is broken, the network will be exposed to external attacks. Multilayer security design can be set to deal with different levels of threat. It gives an edge to the security design and finally neutralizes the attack on the system.

5. Consider Internal Threats

While giving a lot of attention to safeguarding the network or device from external attacks. The security becomes weak in case of internal attacks and most of the attacks are done internally as it is easy to access and designed weakly. Filtering can be added to keep track of the traffic moving from lower-level security to higher level.

Advantages of Firewall:

Blocks infected files: While surfing the internet we encounter many unknown threats. Any friendly-looking file might have malware in it. The firewall neutralizes this kind of threat by blocking file access to the system.

Stop unwanted visitors: A firewall does not allow a cracker to break into the system through a network. A strong firewall detects the threat and then stops the possible loophole that can be used to penetrate through security into the system.

Safeguard the IP address: A network-based firewall like an internet connection firewall(ICF). Keeps track of the internet activities done on a network or a system and keeps the IP address hidden so that it cannot be used to access sensitive information against the user.

Prevents Email spamming: In this too many emails are sent to the same address leading to the server crashing. A good firewall blocks the spammer source and prevents the server from crashing.

The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN

may support a modem pool that provides dial-in capability for traveling employees and telecommuter

Limitations of firewall

- The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuter.

- The firewall does not protect against internal threats. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attackers.

- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses