--CYBER SECURITY--

(MINOR PROJECT)

NAME:- ARTI

ROLL NO:-……

BATCH NO:- 9

SUBMITTED TO:-

MR. AMAN GUPTA
(INTERNSELITE)

SUBMITTED BY:-

ARTI GUPTA (MCA-II)
ICFAI UNIVERSITY,DEHRADUN

Describe the introduction and history of Cyber Security.

Introduction:-

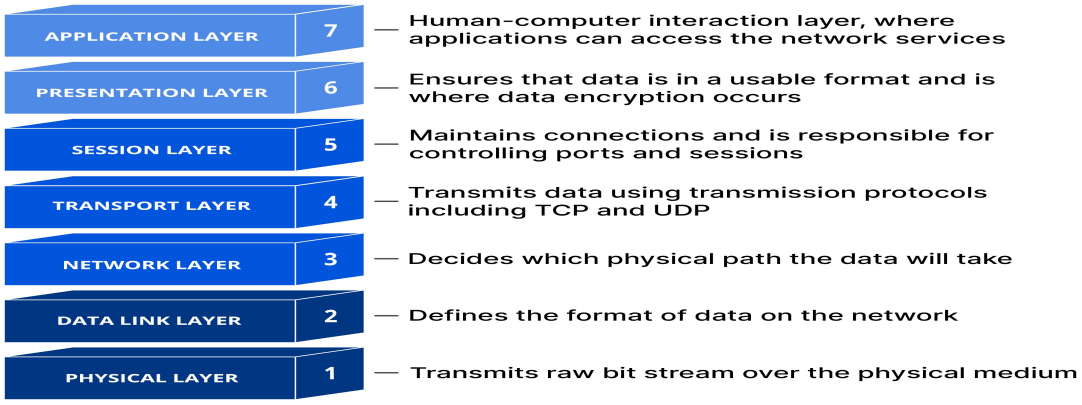
Cyber Security is a process that's designed to protect networks and devices from external threats.It is the protection of internet-connected systems such as hardware, software and data from cyber threats.

History:-

The 1970s saw the actual start or need of cyber security. It was an important decade in the evolution of cyber security. The Advanced Research Projects Agency Network (ARPANET) was the initial endeavor in this. Before the internet was created, this connectivity network was constructed.

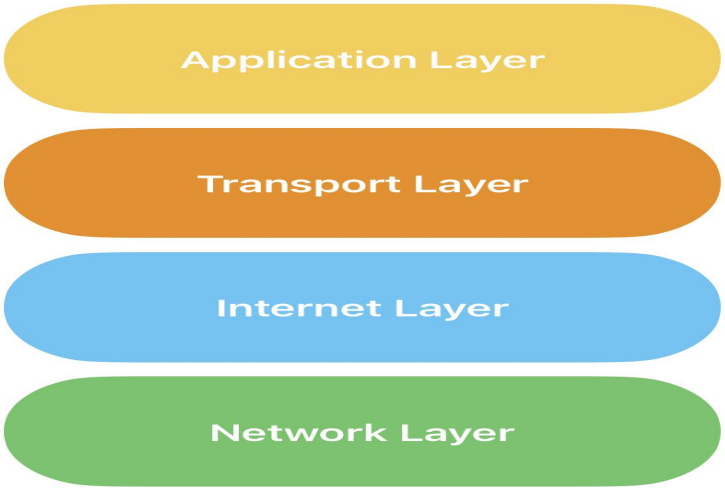
Explain the OSI and TCP/IP model.

This OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers. It is divided into 7 layers that work together to carry out specialised networks functions, allowing for a more systematic approach to networking.



TCP/IP MODEL:-

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model.
The number of layers is sometimes referred to as five or four. Here In this article, we'll study five layers. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.



What is Ethical Hacking? What are its scope and limitations?

Ethical hacking is an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and bypassing system security to identify potential data breaches and threats in a network.
Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They can improve the security footprint to withstand attacks better or divert them.

SCOPE:-

The demand for cybersecurity specialists in India is anticipated to increase by 15% yearly, with a 25% increase in the demand for ethical hackers. This portends a promising future for individuals in India interested in a career in ethical hacking.

Ethical hacking is a fast-expanding industry with many career prospects for qualified people. The necessity to safeguard sensitive data and networks has grown due to our reliance on technology and the internet. As a result, businesses are prepared to spend money on ethical hackers to protect their data.

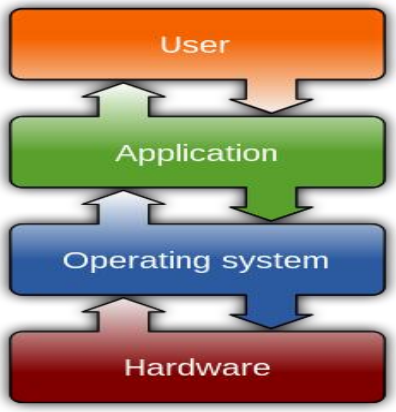
Limitations:-

One key limitation is the defined scope of the testing, which means that ethical hackers cannot go beyond a certain boundary in order to make an attack successful. However, it may be appropriate to discuss potential attacks that fall outside of the defined scope with the organization.

Another limitation is the availability of resources, such as time and budget, which may be more constrained for ethical hackers than for malicious hackers. Additionally, ethical hackers may be required to adhere to certain restrictions on the methods they can use, such as avoiding test cases that could cause servers to crash (e.g., denial of service attacks).

Describe the function and Architecture of OS.

An operating system acts as an intermediary between the user of a computer and computer hardware. The purpose of an operating system is to provide an environment in which a user can execute programs in a convenient and efficient manner. An operating system is a software that manages the computer hardware.



Functions:-

Resource Management: The operating system manages and allocates memory, CPU time, and other hardware resources among the various programs and processes running on the computer.

Process Management: The operating system is responsible for starting, stopping, and managing processes and programs. It also controls the scheduling of processes and allocates resources to them.

Job Accounting: It keeps track of time and resources used by various jobs or users.

File Management: The operating system is responsible for organizing and managing the file system, including the creation, deletion, and manipulation of files and directories.

Device Management: The operating system manages input/output devices such as printers, keyboards, mice, and displays. It provides the necessary drivers and interfaces to enable communication between the devices and the computer.

Backup and Recovery: The operating system provides mechanisms for backing up data and recovering it in case of system failures, errors, or disasters.

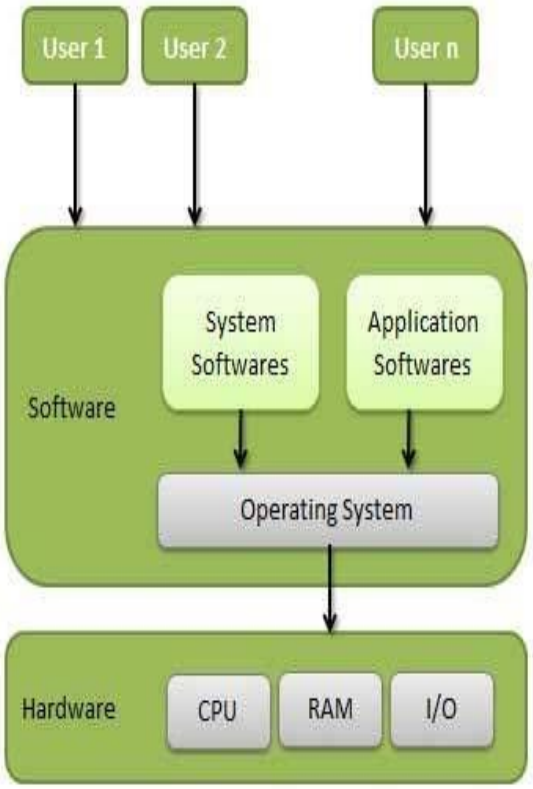
Virtualization: The operating system provides virtualization capabilities that allow multiple operating systems or applications to run on a single physical machine. This can enable efficient use of resources and flexibility in managing workloads.

Architecture:-

Central Processing Unit (CPU): The CPU is the brain of the computer, responsible for executing instructions and performing calculations. The OS interacts closely with the CPU, managing its usage to ensure efficient task execution.

Memory (RAM): Memory is where data and instructions are temporarily stored for fast access by the CPU. The OS manages memory allocation, ensuring that each process gets its fair share while preventing conflicts.

Input/Output Devices: Peripherals like keyboards, mice, displays, and printers connect to the computer via input/output ports. The OS facilitates communication between these devices and user applications.



Describe the commands that used in Reconnaissance.

Nmap -v-O target IP
(The appliances will rocognize and react to active TCP stack OS fingerprinting attempts)

Nmap -v -sS target IP
(The appliances will recognize and react to port scans)

Nmap -v -sN target IP
(The appliances will refuse packets with no flag sets)

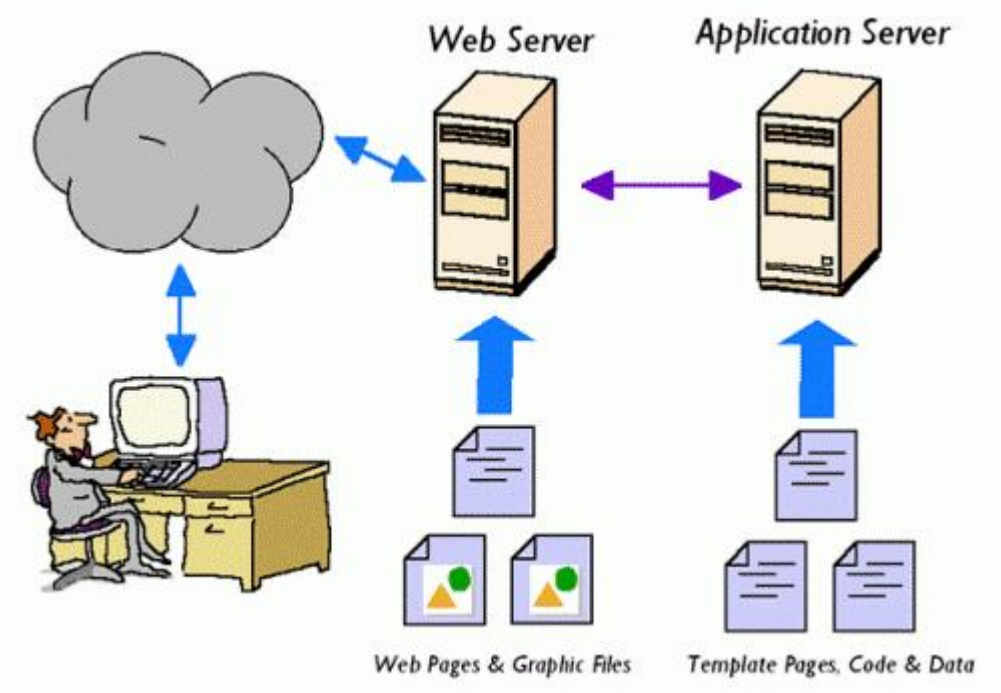
Nmap -v -scanflags SYNFIN target IP
(The appliances will refuse packets with only the SYN and FIN flags set)

ss# Differentiate between Web Server and Application Server.

Web Server:-

It is a computer program that accepts the request for data and sends the specified documents. Web server may be a computer where the online content is kept. Essentially internet server is employed to host sites however there exist different web servers conjointly like recreation, storage, FTP, email, etc.

Example of Web Servers:
*Apache Tomcat
*Resin



Application Server:-

It encompasses Web container as well as EJB container. Application servers organize the run atmosphere for enterprises applications. Application server may be a reasonably server that mean how to put operating system, hosting the applications and services for users, IT services and organizations. In this, user interface similarly as protocol and RPC/RMI protocols are used.

Examples of Application Server:

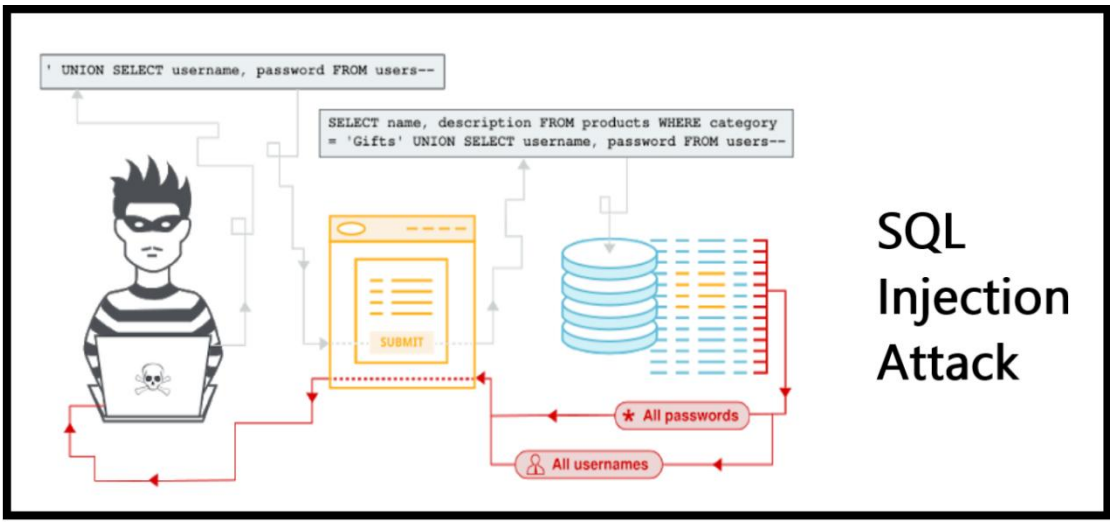
*Weblogic
*JBoss
*Websphere

Factor	Web Server	Application Server
Purpose	A Web Server contains a Web container only.	An Application Server contains a Web Container plus an EJB Container.
Useful	A web server is good in case of static contents like static html pages.	An Application server is relevant in case of dynamic contents like bank websites.
Resource Consumption	A Web server consumes less CPU, Memory resources as compared to an application server.	An Application server utilizes more resources.
Target Environment	A Web Server provides the runtime environment for web applications.	Application servers provide the runtime environment for enterprise applications.
Multithreading support	Multithreading is not supported.	Multithreading is supported.
Protocol(s) supported	Web Servers support HTTP Protocol.	Application Servers support HTTP as well as RPC/RMI protocols.
Example	Apache Web Server.	WebLogic, JBoss.

What is SQL Injection? Write down its effect.

SQL Injection:-

SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database. Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database. A successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server. In recent years, there have been many security breaches that resulted from SQL injection attacks.



EFFECTS:-

Confidentiality: Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.

Authentication: If poor SQL commands are used to check user names and passwords, it may be possible to connect to a system as another user with no previous knowledge of the password.

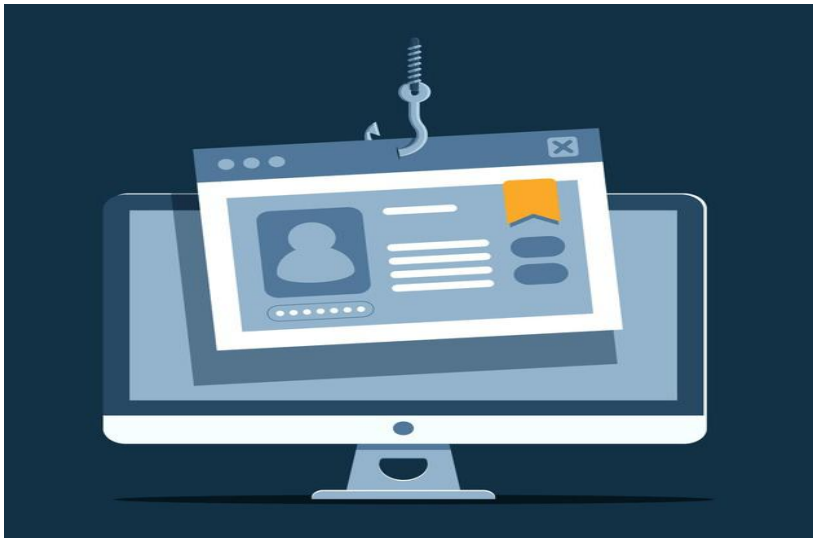
Authorisation: If authorisation information is held in a SQL database, it may be possible to change this information through the successful exploitation of a SQL Injection vulnerability.

Integrity: Just as it may be possible to read sensitive information, it is also possible to make changes or even delete this information with a SQL Injection attack.

What is Phishing websites? How it differ from original websites?

Phishing Website:-

It is a website set up to steal your identity, or at least part of it. It does this by trying to convince you that it is a legitimate website, which needs those details to perform an action from which you will benefit.



It differ from original websites:-

*The link contains any strange characters, then it is probably a phishing link. The strange characters are a sign of URL encoding, in other words, disguising the real address. If the link is embedded or shortened, then it is also probably a phishing link. Use a decoder or expander to check the real address.

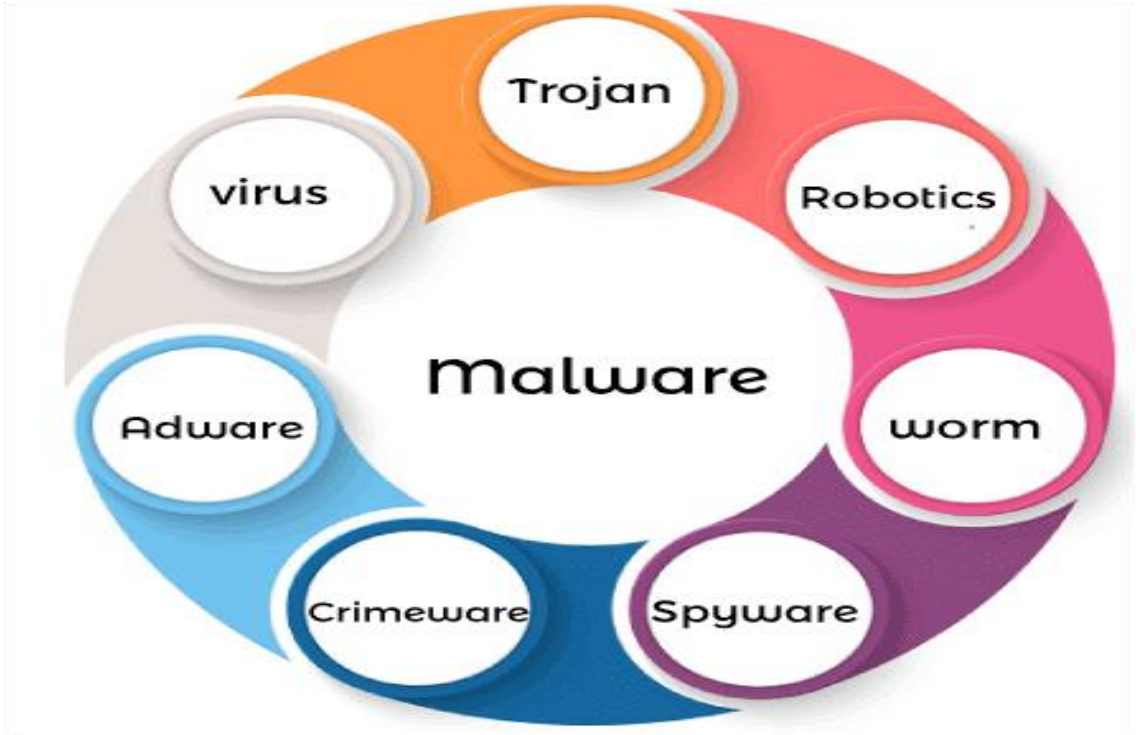
*If a particular webpage we landed on the website seems doubtful, an excellent way to recognize a phishing site is to take a look at the complete website content. Just check the writing style as it might contain spelling mistakes and poor grammar and might be different from that usually used by the sender.
Plus, phishing websites have various red flags, including clickbait headlines, low-resolution photos, empty pages, bad grammar, and excessive advertising.

*If we are using a website and immediately greeted by a pop-up asking you to enter your credentials, additionally, an email is sent to you, asking recipients to verify personal information, such as bank details or a password, these are massive warnings signs

What is Malware? Explain its types.

Malware:-

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.



Types of MALWARE:-

Virus:-
Viruses are a subgroup of malware. A virus is malicious software attached to a document or file that supports macros to execute its code and spread from host to host. Once downloaded, the virus will lie dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

Worms:-
A worm is a type of malicious software that rapidly replicates and spreads to any device within the network. Unlike viruses, worms do not need host programs to disseminate. A worm infects a device through a downloaded file or a network connection before it multiplies and disperses at an exponential rate. Like viruses, worms can severely disrupt the operations of a device and cause data loss.

Trojan virus:-
Trojan viruses are disguised as helpful software programs. But once the user downloads it, the Trojan virus can gain access to sensitive data and then modify, block, or delete the data. This can be extremely harmful to the performance of the device. Unlike normal viruses and worms, Trojan viruses are not designed to self-replicate.

Spyware:-

Spyware is malicious software that runs secretly on a computer and reports back to a remote user. Rather than simply disrupting a device's operations, spyware targets sensitive information and can grant remote access to predators. Spyware is often used to steal financial or personal information. A specific type of spyware is a keylogger, which records your keystrokes to reveal passwords and personal information.

Adware:-

Adware is malicious software used to collect data on your computer usage and provide appropriate advertisements to you. While adware is not always dangerous, in some cases adware can cause issues for your system. Adware can redirect your browser to unsafe sites, and it can even contain Trojan horses and spyware. Additionally, significant levels of adware can slow down your system noticeably. Because not all adware is malicious, it is important to have protection that constantly and intelligently scans these programs.

Ransomware:-

Ransomware is malicious software that gains access to sensitive information within a system, encrypts that information so that the user cannot access it, and then demands a financial payout for the data to be released. Ransomware is commonly part of a phishing scam. By clicking a disguised link, the user downloads the ransomware. The attacker proceeds to encrypt specific information that can only be opened by a mathematical key they know. When the attacker receives payment, the data is unlocked.

Fileless malware:-

Fileless malware is a type of memory-resident malware. As the term suggests, it is malware that operates from a victim's computer's memory, not from files on the hard drive. Because there are no files to scan, it is harder to detect than traditional malware. It also makes forensics more difficult because the malware disappears when the victim computer is rebooted. In late 2017, the Cisco Talos threat intelligence team posted an example of fileless malware that they called DNSMessenger.

Describe the types of WI-FI with its Encryption Method.

WI-FI:-

Wi-Fi security is the protection of devices and networks connected in a wireless environment. Without Wi-Fi security, a networking device such as a wireless access point or a router can be accessed by anyone using a computer or mobile device within range of the router's wireless signal.

Types of wireless security protocols:-

There are four main wireless-security protocols. These protocols were developed by the Wi-Fi Alliance, an organization that promotes wireless technologies and interoperability. The group introduced three of the protocols, described below, in the late 1990s. Since then, the protocols have been improved with stronger encryption. The fourth protocol was released in 2018.

WEP:-

The first wireless security protocol was WEP (Wired Equivalent Privacy). It was the standard method of providing wireless network security from the late 1990s until 2004. WEP was hard to configure, and it used only basic (64-/128-bit) encryption. WEP is no longer considered secure and should be replaced by a newer protocol such as WPA2, described below.

WPA:-

WPA (Wi-Fi Protected Access) was developed in 2003. It delivers stronger (128-/256-bit) encryption than WEP by using a security protocol known as Temporal Key Integrity Protocol (TKIP). Along with WPA2, WPA is the most common protocol in use today. But unlike WPA2, it is compatible with older software.

WPA2:-

WPA2, a later version of WPA, was developed in 2004. It's easier to configure and provides even greater network security than WPA by using a security protocol known as the Advanced Encryption Standard (AES). Versions of the WPA2 protocol are available for individual users and enterprises.

WPA3:-

A new generation of WPA, known as WPA3, is designed to deliver simpler configuration and even stronger (192-/256-/384-bit) encryption and security than any of its predecessors. It is also meant to work across the latest Wi-Fi 6 networks.

Types of Wi-Fi network security devices:-

Active device:-

There are several types of commercially available devices that can provide network security by blocking adversarial attacks and unwanted network traffic. One type is known as an "active" device, which is hardware configured to block surplus network traffic. Examples of these devices for Wi-Fi network security include firewalls, antivirus scanners, and content-filtering devices.

Passive device:-

Passive Wi-Fi network security devices detect and report on unwanted network traffic. Passive devices use less power than other Wi-Fi devices. They also have an extra layer of security because they can communicate with Wi-Fi routers only when the routers are seeking them.
That extra layer makes man-in-the-middle (MITM) attacks more difficult. In an MITM attack, an adversary attempts to intercept communications between two parties to "listen in" on their activity or to modify the traffic traveling between them.

Preventive device:-

A preventive device, such as a wireless intrusion prevention system (WIPS), can scan networks to identify potential security issues. A WIPS can be integrated into networks or overlaid using standalone sensors. Some WIPSs, however, conduct only intermittent monitoring, leaving networks occasionally vulnerable.

Encryption:-

A more common method of protecting Wi-Fi networks and devices is the use of security protocols that utilize encryption. Encryption in digital communications encodes data and then decodes it only for authorized recipients.
There are several types of encryption standards in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). See the section "Types of wireless security protocols" on this page for more details about these and other standards related to Wi-Fi security.
Most newer network devices, such as access points and Wi-Fi routers, feature built-in wireless-security encryption protocols that provide Wi-Fi protection.