

“Rule the world with elite.”

CYBER SECURITY

MINOR PROJECT

**Submitted by’**

**Name :-** Yeola Puja Bhagirath

**University :-** MET BHUJBAL KNOWLEDGE CITY, NASHIK

**Year :-** 2023

**Batch :-** July batch

**Submitted to ,**

**Amit Gupta**

**( InternsElite )**

**INDEX**

| **Serial no.** | **Project Name** | **Page no.** |
| --- | --- | --- |
| **1.** | DESCRIBE THE INTRODUCTION AND HISTORY OF CYBER SECURITY. | 4-7 |
| **2.** | EXPLAIN THE OSI AND TCP/IP MODEL. | 8-11 |
| **3.** | WHAT IS ETHICAL HACKING. WHAT ARE IT’S SCOPE AND LIMITATIONS. | 12-14 |
| **4.** | DESCRIBE THE FUNCTIONS AND ARCHITECTURE OF OPERATING  SYSTEM. | 15-18 |
| **5.** | DESCRIBE THE COMMANDS THAT USED IN RECONNAISANCE. | 19-22 |
| **6.** | DIFFERENCE BETWEEN WEB-SERVER AND APPLICATION SERVER. | 23-25 |
| **7.** | WHAT IS SQL INJECTIONS. WRITE DOWN IT’S EFFECTS. | 26-27 |
| **8.** | WHAT IS PHISHING WEBSITES. HOW IS DIFFER FROM ORIGINAL WEBSITES. | 28-30 |
| **9.** | WHAT IS MALWARE. EXPLAIN ITS TYPES. | 31-33 |
| **10.** | DESCRIBE THE TYPES OF WI-FI WITH IT’S ENSCRIPTION METHODS. | 33-36 |

# 1] DESCRIBE THE INTRODUCTION AND HISTORY OF CYBER SECURITY?

* Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."
* Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.
* A successful cyber security approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.
* Cyber security is becoming increasingly significant due to the increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of smart devices and the various devices that constitute the ‘Internet of things’.

**Cyber Security Goals :-**

* Cyber Security's main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.
* We can break the CIA model into three parts: Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security.



**Confidentiality :-**

Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. Data encryption is an excellent example of ensuring confidentiality.

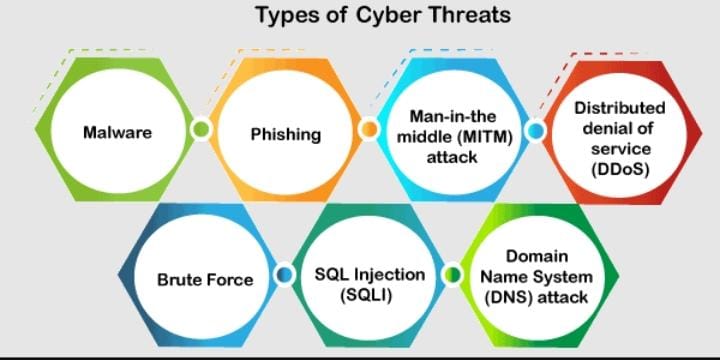
**Integrity :-**

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

**Availability :-**

This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

# Types of Cyber Security Threats :-



# History of Cyber Security :

* **1970s**: ARAPNET and the Creeper : Cybersecurity began in the 1970s when researcher Bob Thomas created a computer programme called Creeper that could move across ARPANET’s network, leaving a breadcrumb trail wherever it went.
* **1980s:** Birth of the commercial antivirus :1987 was the birth year of commercial antivirus although there were competing claims for the innovator of the first antivirus product.
* **1990s:** The world goes online : With the internet becoming available to the public, more people began putting their personal information online.
* **2000s:** Threats diversify and multiply : In the early 2000s crime organisations started to heavily fund professional cyberattacks and governments began to clamp down on the criminality of hacking, giving much more serious sentences to those culpable.
* **2021:** The next generation : The cybersecurity industry is continuing to grow at the speed of light. The global cybersecurity market size is forecast to grow to $345.4bn by 2026 according to Statista. Ransomware is one of the most common threats to any organisation's data security and is forecast to continue to increase.
* **Present day:** Cyber threats continue to evolve and become more complex, including attacks on critical infrastructure and the use of artificial intelligence in cyber attacks. The field of cybersecurity is constantly evolving to keep up with these threats, with a focus on developing advanced technologies and building a skilled workforce to protect against cyber attacks.

**2] EXPLAIN THE OSI AND TCP/IP MODEL?**

OSI and TCP/IP are the networking models.

* OSI Model :- (Open System Interconnection Model)

The Open Systems Interconnection (OSI) model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to its underlying internal structure and technology. OSI Model is developed by ISO in 1974. This model is categorized into 7 different layers.

**1. Physical Layer :**

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

**2. Data Link Layer:**

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

**3. Network Layer:**

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

**4. Transport Layer:**

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connecti**o**n speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

**5. Session Layer:**

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from thelast checkpoint.

**6. Presentation Layer:**

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

# TCP/IP Model :-

It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. It contains four layers. The layers are :-

**Layer 1: Network Access Layer**

The network access layer, also known as the data link layer, handles the physical infrastructure that lets computers communicate with one another over the internet. This covers ethernet cables, wireless networks, network interface cards, device drivers in your computer, and so on.

The network access layer also includes the technical infrastructure — such as the code that converts digital data into transmittable signals — that makes network connection possible.

**Layer 2: Internet Layer**

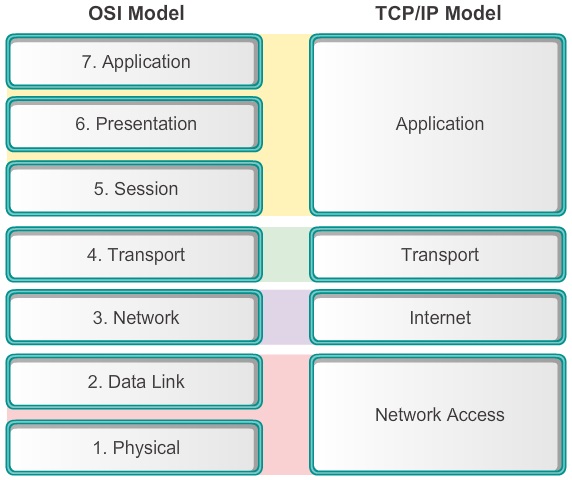
The internet layer, also known as the network layer, controls the flow and routing of traffic to ensure data is sent speedily and accurately. This layer is also responsible for reassembling the data packet at its destination. If there’s lots of internet traffic, the internet layer may take a little longer to send a file, but there will be a smaller chance of an error corrupting that file.

**Layer 3: Transport Layer**

The transport layer provides a reliable data connection between two communicating devices. It’s like sending an insured package: The transport layer divides the data in packets, acknowledges the packets it has received from the sender, and ensures that the recipient acknowledges the packets it receives.

**Layer 4: Application Layer**

The application layer is the group of applications that let the user access the network. For most of us that means email, messaging apps, and cloud storage programs. This is what the end-user sees and interacts with when sending and receiving data.



# 3] WHAT IS ETHICAL HACKING. WHAT ARE IT’S 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.

# Ethical Hacking is important because of the following :-

1. In the age of digitalization, every organization needs to be assertive while ensuring the security and privacy of the data and information they deal with.
2. Ethical hacking is extensively used to test security systems. Ethical hacking is also used during executing, managing and designing stages of test security systems. It finds the security vulnerabilities and corrects them.
3. Ethical hacking is also used to secure crucial data from adversaries. It prevents malicious users from exploiting the organizational or an individual. It reduces the risk of getting blackmailed by a person or organization with ill intentions.
4. Ethical hacking has a crucial role to play in the safety and security of any nation. Many national and state-funded organizations hire hackers to prevent cyber terrorism and terrorist attacks. Many government-employed personnel hire ethical hackers to protect their privacy.
5. In the age of digitalization, every organization needs to be assertive while ensuring the security and privacy of the data and information they deal with.
6. Ethical hacking is extensively used to test security systems. Ethical hacking is also used during executing, managing and designing stages of test security systems. It finds the security vulnerabilities and corrects them.
7. Ethical hacking is also used to secure crucial data from adversaries. It prevents malicious users from exploiting the organizational or an individual. It reduces the risk of getting blackmailed by a person or organization with ill intentions.
8. Ethical hacking has a crucial role to play in the safety and security of any nation. Many national and state-funded organizations hire hackers to prevent cyber terrorism and terrorist attacks. Many government-employed personnel hire ethical hackers to protect their privacy.

# Scope of Ethical Hacking :-

Ethical hacking has an infinite future. Many areas, including government, corporate enterprises, health care, entertainment, banking, and others, are quickly expanding in this arena.

Even though only 32% of people work in the ethical hacking industry. As a result, the demand for new staff is on the rise. Compared to last year, the number of ethical hackers is predicted to rise by 20% by the end of 2023. As a result, this number will continue to grow in the future.

# Limitations of Ethical Hacking :-

Limited scope : Ethical hackers cannot progress beyond a defined scope to make an attack successful. However, it’s not unreasonable to discuss out of scope attack potential with the organization.

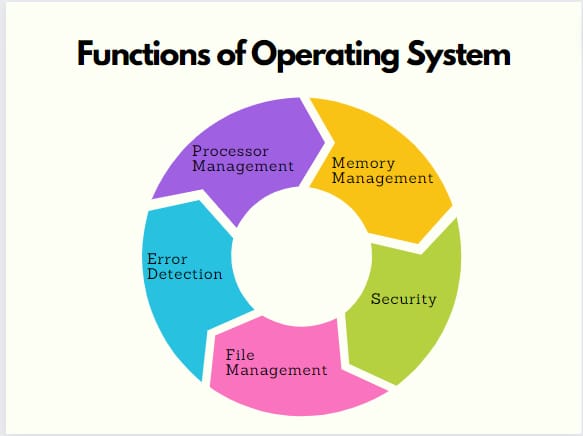
Resource constraints : Malicious hackers don’t have time constraints that ethical hackers often face. Computing power and budget are additional constraints of ethical hackers.

Restricted methods : Some organizations ask experts to avoid test cases that lead the servers to crash (e.g., Denial of Service (DoS) attacks).

# 4] DESCRIBE THE FUNCTIONS AND ARCHITECTURE OF OPERATING SYSTEM?

An Operating System (OS) is a software that acts as an interface between computer hardware components and the user. Every computer system must have at least one operating system to run other programs. Applications like Browsers, MS Office, Notepad Games, etc., need some environment to run and perform its tasks.

The OS helps you to communicate with the computer without knowing how to speak the computer’s language. It is not possible for the user to use any computer or mobile device without having an operating system.



# Functions of Operating System :-

**1.File Management**

An operating system’s (OS) primary function is to manage files and folders.Operating systems are responsible for managing the files on a computer. This includes creating, opening, closing, and deleting files. The operating system is also responsible for organizing the files on the disk.

# 2.Device management

Operating systems provide essential functions for managing devices connected to a computer. These functions include allocating memory, processing input and output requests, and managing storage devices. This device could be a keyboard, mouse, printer, or any other devices you may have connected. An operating system will provide you with options to manage how each device behaves. For example, you can set up your keyboard to type in a specific language or make it so that the mouse only moves one screen at a time.

# 3.Process management

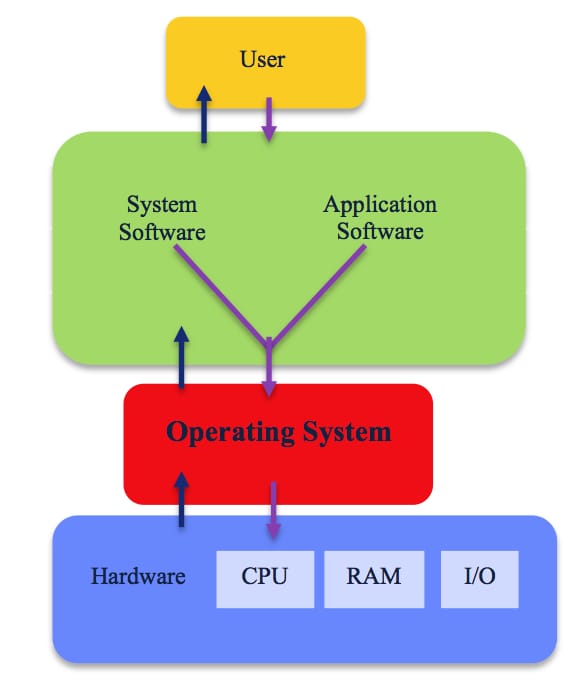
The operating system’s responsibility is to manage the processes running on your computer. This includes starting and stopping programs, allocating resources, and managing memory usage. The operating system ensures that the programs running on your computer should be compatible. It’s also responsible for enforcing program security, which helps to keep your computer safe from potential attacks.

# 4.Memory management

One of the most critical functions of an operating system is memory management. This is the process of keeping track of all different applications and processes running on your computer and all the data they’re using.

# Architecture of OS :-

The Operating system architecture holds a crucial and indispensable role within every computer system. It creates an abstraction layer, serving as an intermediatory connecting the user to the underlying hardware. Numerous operating systems are employed by indivisuals including windows, IOS, Android among others. This article will delve into an exploration of the four primary OS architectures, accompanied by their respective merits and drawbacks.



**Below are the important terms related to OS Architecture :-**

**Kernal** :- Kernel is central component of an operating system that manages operations of computer and hardware. It basically manages operations of memory and CPU time. It is core component of an operating system. Kernel acts as a bridge between applications and data processing performed at hardware level using inter-process communication and system calls. Kernel loads first into memory when an operating system is loaded and remains into memory until operating system is shut down again. It is responsible for various tasks such as disk management, task management, and memory management.

**Shell** :- The shell is an operating system acts as an interface for the users to interact with the computer system. The shell can be a command line interface or a graphical interface.

**BIOS** :- BIOS is a program, stands for basic input/output system, which is stored in nonvolatile memory like ROM (Read Only Memory) or flash memory that allows you to set up and access your computer system at the greatest basic level. Although there is no need for most people to mess with the BIOS on a computer, it can be better to know about BIOS. It is found on motherboards that are a pre-installed program on Windows- based computers that executes when a computer is powered up. Before an OS is loaded, the CPU accesses the basic input/output system (BIOS). Then, the next function of BIOS is to examine all the hardware connections and detects all your devices.

The main function of BIOS is to set up hardware and start an OS, and it contains generic code that is needed to control display screens, the keyboard, and other functions.

**5] DESCRIBE THE COMMANDS THAT USED IN RECONNAISSANCE:-**

Like the windows command prompt, the Linux shell is your interface to the operating system. Some commands are the same, Some are very similar and some are very different.

Like all penetration testing, an Social Engineering Attack begins with foot-printing activity and reconnaissance. The more information you collect about the target organization, the more options become available to you.

**1.Passive reconnaissance** always involves gathering information regarding a potential target without the targeted individual’s or company’s knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave.

However, it’s usually done using Internet searches or by Googling an individual or company to gain information. This process is generally called information gathering. Social engineering and dumpster diving are also considered passive information-gathering methods.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building monitoring: A hacker watches the flow of data to see what time certain transactions take place and where the traffic is going.

**2.Active reconnaissance** involves probing the network to discover individual hosts, IP addresses, and services on the network. This usually involves more risk of detection than passive reconnaissance and is sometime called rattling the doorknobs.

Active reconnaissance can give a hacker an indication of security measures in place (is the front door locked?), but the process also increases the chance of being caught or at least raising suspicion.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it’s usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.

# commands which used in reconnaissance :-

1. Use **traceroute** to determine all the routers between you and your target.

Enter the following command in the terminal :- traceroute -n [www.redhat.net](http://www.redhat.net/)

1. Use **ping** to verify that [www.redhat.net](http://www.redhat.net/) is alive (which we know it is since it is hosting this web page). This is very important verification used to determine the ACL rules of the firewall, if present. If you receive the reply from the target, then you know now ping requests and replies are not filtered by the firewall.

Enter the following command in the terminal :- ping [www.redhat.net](http://www.redhat.net/)

1. **uname -a** command gives you information related to kernel name, network node, release version, hardware name/platform, processor type and operating system name.
2. **uname -a** command gives you information related to kernel name, network node, release version, hardware name/platform, processor type and operating system name.
3. **cat/etc/\* -release** command gives you the information about the version of Linux distro you are running.
4. **cat/proc/version** command is used to set the system wide environmental variables on user shells.
5. **cat.profile** command is used to print users shell on linux system.
6. **cat ps-aux** command basically lists the process id number (PID), CPU usage, Memory usage, total CPU time for each process on the system.
7. **ls -al /usr/bin** command lists the content of /usr/bin directory.
8. **mysql -v** command is used to display the MySQL terminal in verbose mode whereas -V will gives you the version of MySQL server.
9. **apache2 -v** command gives the information about the apache2 server.
10. **cronttab -I** command is used for displaying the crontab file if available which is used for executing commands at specific date and time.
11. **python -version** command gives the installed version of python on the system.
12. **gcc -v** command is used for obtaining the information of gcc compiler.

The GNU compiler collection is a compiler system produced by the GNU project supporting various programming languages. GCC is a keyword component of the GNU tool chain and the standard compiler for most Unix-like operating system.

1. **route** command is used for displaying current contents of the routing tables.
2. **hostname** command is used for displaying the current hostname or domain name of computer i.e. uniquely identifiable by a network.

# 6] DIFFERENCE BETWEEN WEB-SERVER AND APPLICATION SERVER.

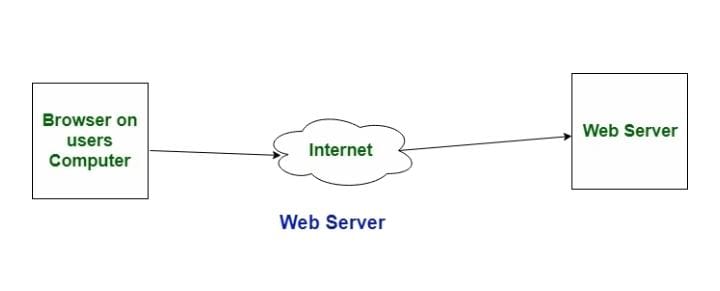
A server is a central repository where information and computer programs are held and accessed by the programmer within the network. Web server and Application server are kinds of the server which employed to deliver sites and therefore the latter deals with application operations performed between users and back-end business applications of the organization.

**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:

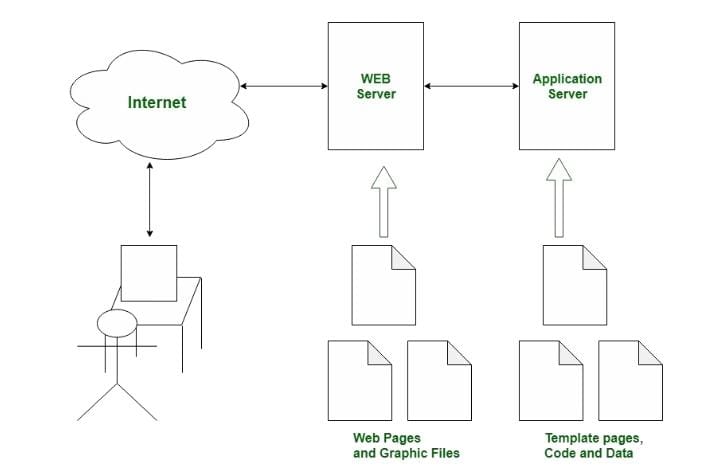
# It encompasses Web container as well as EJB container. Application servers organize the run atmosphere for enterprises applications. Application server may be a reasonably server that mean how to put operating system, hosting the applications and services for users, IT services and organizations. In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

# Examples of Application Server:

# Weblogic

# JBoss

# Websphere



|  |  |  |
| --- | --- | --- |
| S.NO. | WEB SERVER | APPLICATION SERVER |
| 1 | Web server encompasses web container only. | While application server encompasses Web container as well as EJB container. |
| 2 | Web server is useful or fitted for static content | Whereas application server is fitted for dynamic content. |
| 3 | Web server consumes or utilizes less resourses. | While application server utilize more resources. |
| 4 | Web servers arrange the run environment for web applications. | While application servers arrange the run environment for enterprises applications |
| 5 | In web servers, multithreading is supported. | While in application server, multithreading is not supported. |
| 6 | Web servers capacity is lower than application. | While application server’s capacity is higher than web server. |
| 7 | Examples; Apache HTTP server,Nginx. | Example; JBoss, glassfish. |

# 7] WHAT IS SQL INJECTIONS. WRITE DOWN IT’S EFFECTS?

* SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.
* The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.
* The Confidentiality, Integrity and Availability of your data. A SQL Injection has the following consequences:

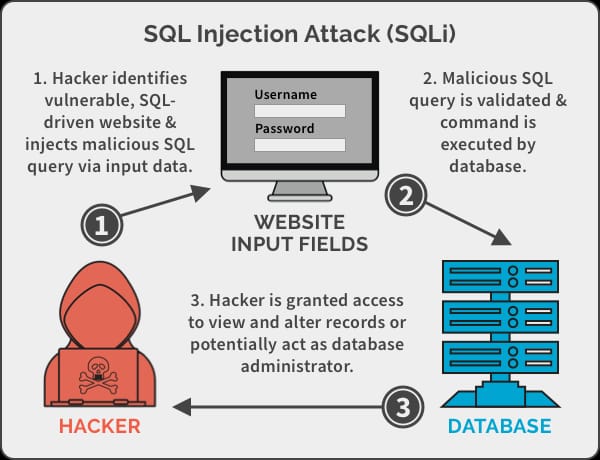
**Confidentiality:** Since SQL databases generally hold sensitive data, loss of confidentiality is a frequent problem with SQL Injection vulnerabilities.

**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.

* SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.



# 8] WHAT IS PHISHING WEBSITES. HOW IS DIFFER FROM ORIGINAL WEBSITES?

* Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other forms of communication. Attackers will commonly use phishing emails to distribute malicious links or attachments that can perform a variety of functions. Some will extract login credentials or account information from victims.
* Deceptive phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate phishing email than it is to break through a computer's defenses. Learning more about phishing is important to learn how to detect and prevent it.
* **Phishing websites** :- Fake website are set to trick victims into divulging personal and financial information, such as passwords, account ID’s or credit card details. Phishing e-mails often appear to come from credible sources and contain link to click on an urgent request for the user to respond quickly.

**Difference between phishing website and original website :-**

# The Domain Name

First of all, the domain name is the one thing that you need to look at. All the legitimate websites will have at least an https domain name, which means that the protocol that it uses should begin with https. This is especially true for sites that require you to log into your account. On the other hand, the phishing site will only provide you with the http domain name. Their name might also be similar, but with very slight alteration to the letters. For instance, the real site might have an address like http[s://ww](http://www.google.com/)w.go[ogle.com/](http://www.google.com/) while the fake site will have an address like [http://www.go0gle.com/.](http://www.go0gle.com/) So, take a look carefully at the domain name in the address bar.

# The Website Security

A good, legitimate, and secure website will usually have a strong security protocol that protects it from various online threats. The SSL security will always exist in any legitimate website that requires your login information. Remember that unless the company is legitimate, the SSL certificate will not be handed to the company since it requires rigorous tests before their application is accepted. Meanwhile, the fake site will not have any security protocol installed on it, thus confirming that the website is not trustworthy. Take a look at the address bar of your browser. If there is a green lock at the left side of the address bar, and you can see that the site is verified by a legitimate security provider, then it means that it is a real website.

# The Link Sender

Most of phishing websites are “promoted” via spam emails to their victims. They might also be promoted via direct messages in various social media platforms. If you get a link that asks you to log into your account, make sure that the one giving you link is a trustworthy person or company. This is because many people that fall into this trap gave their private information via a suspicious link. Instead of verifying its trustworthiness, they decided to ignore it. So, make sure that you really trust the person or company that gives you the link to the website. If you are asked to log into your account in any website, make sure that the one giving you the login link is the company itself.

# Available Website Pages

A fake site will never be able to copy the entire web pages of the real one. So, when you visit a suspicious website that resembles a real one, you have to click on various links available in that website. If they cannot display any other pages other than the login page, then it is certainly a fake site. But, if you can browse the website as usual without any problem, then you are dealing with the real one. So, take some time to browse the website and see if you can access the web pages as usual. Otherwise, stay away from that site.

# The Site Design

Another thing that you have to take a look to differentiate between a real website and a phishing website is the overall site design. Of course, a fake website will try to imitate the real one as much as possible, but it will always be imperfect. Even though they can imitate the site design at first glance, they can’t fool the people if they really compare the design of the real and fake website. So, take a look carefully at the site design. If you see something off, then it might be the sign that this is not the real site that you usually use.

# 9] WHAT IS MALWARE . EXPLAIN ITS TYPES?

The word ‘malware’ is a contraction of ‘malicious software’. Malware is intrusive software that is intentionally designed to cause damage to computers and computer systems. By contrast, software that causes unintentional damage is usually referred to as a software bug.

Malware may be introduced to a network through phishing, malicious attachments, malicious downloads, social engineering, or flash drives. In this overview, we look at common malware types.

# 1.Adware

Adware, a contraction of ‘advertising-supported software’, displays unwanted and sometimes malicious advertising on a computer screen or mobile device, redirects search results to advertising websites, and captures user data that can be sold to advertisers without the user's consent. Not all adware is malware, some is legitimate and safe to use.

Users can often affect the frequency of adware or what kinds of downloads they allow by managing the pop-up controls and preferences within their internet browsers or using an ad blocker.

# 2.Spyware

Spyware is a form of malware that hides on your device, monitors activity, and steals sensitive information like financial data, account information, logins, and more. Spyware can spread by exploiting software vulnerabilities or else be bundled with legitimate software or in Trojans.

# 3.Ransomware and crypto-malware

Ransomware is malware designed to lock users out of their system or deny access to data until a ransom is paid. Crypto-malware is a type of ransomware that encrypts user files and requires payment by a specific deadline and often through a digital currency such as Bitcoin. Ransomware has been a persistent threat for organizations across industries for many years now. As more businesses embrace digital transformation, the likelihood of being targeted in a ransomware attack has grown considerably.

# 4.Trojans

A Trojan (or Trojan Horse) disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, inadvertently allowing malware onto their device. Trojans themselves are a doorway. Unlike a worm, they need a host to work. Once a Trojan is installed on a device, hackers can use it to delete, modify or capture data, harvest your device as part of a botnet, spy on your device, or gain access to your network.

# 5.Viruses

A virus is a piece of code that inserts itself into an application and executes when the app is run. Once inside a network, a virus may be used to steal sensitive data, launch DDoS attacks, or conduct ransomware attacks. Usually spread via infected websites, file sharing, or email attachment downloads, a virus will lie dormant until the infected host file or program is activated. Once that happens, the virus can replicate itself and spread through your systems.

# 6.Worms

One of the most common types of malware, worms, spread over computer networks by exploiting operating system vulnerabilities. A worm is a standalone program that replicates itself to infect other computers without requiring action from anyone. Since they can spread fast, worms are often used to execute a payload—a piece of code created to damage a system. Payloads can delete files on a host system, encrypt data for a ransomware attack, steal information, delete files, and create botnets.

# 7.Keyloggers

A keylogger is a type of spyware that monitors user activity. Keyloggers can be used for legitimate purposes – for example, families who use them to keep track of their children's online activity or organizations which use them to monitor employee activity. However, when installed for malicious purposes, keyloggers can be used to steal password data, banking information, and other sensitive information. Keyloggers can be inserted into a system through phishing, social engineering, or malicious downloads.

# 8.Bots and botnets

A bot is a computer that has been infected with malware so it can be controlled remotely by a hacker. The bot – sometimes called a zombie computer – can then be used to launch more attacks or become part of a collection of bots called a botnet. Botnets can include millions of devices as they spread undetected. Botnets help hackers with numerous malicious activities, including DDoS attacks, sending spam and phishing messages, and spreading other types of malware.

# 10] DESCRIBE THE TYPES OF WI-FI WITH IT’S ENSCRIPTION METHODS?

Computer networks that are not connected by cables are called wireless networks. They generally use radio waves for communication between the network nodes. They allow devices to be connected to the network while roaming around within the network coverage.

# There four main types of wireless networks are :-

**Wireless Personal Area Networks (WPAN)** are short-range networks that connect devices within a relatively small area. A WPAN generally connects devices within a person's reach, though the range can extend up to about 30 feet. Using Bluetooth technology, a WPAN can interconnect compatible devices near a central location, such interconnecting a headset to a laptop on your desk.

**Wireless Local Area Networks (WLAN)** are wireless networks that use radio waves, not Bluetooth technology like WPANs. There is usually at least one cable that is the access point for internet access, such as a wired internet connection going into a router, which then broadcasts the wireless signal to other devices. WLANs are used for connecting to local resources and to the internet. The range can be confined to a single room or home or spread across an entire building or campus with the use of spread- spectrum or OFDM technologies.

**Wireless Wide Area Networks (WWAN)** can be maintained over large areas, such as cities or countries, via multiple satellite systems, antenna sites or mobile phone signals. With a wide coverage area, WWANs provide a way to stay connected when other forms of network access are unavailable.

**Wireless Metropolitan Area Networks (WMAN)** connect several different WLANs in a metropolitan area, such as different buildings in a city.

# Types of encryption network (WEP/WPA/WPA2) :-

Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients. Wireless networks are often less secure than wired ones, so wireless security protocols are crucial for keeping you safe online. The most common Wi-Fi security protocols today are WEP, WPA, and WPA2.

**WEP (Wired Equivalent Privacy)** is the oldest and most common Wi-Fi security protocol. It was the privacy component established in the IEEE 802.11, a set of technical standards that aimed to provide a wireless local area network (WLAN) with a comparable level of security to a wired local area network (LAN).

The Wi-Fi Alliance ratified WEP as a security standard in 1999. Once touted to offer the same security benefits as a wired connection, WEP has been plagued over the years by many security flaws. And as computing power has increased, these vulnerabilities have worsened. Despite efforts to improve WEP, it’s still vulnerable to security breaches. The Wi-Fi Alliance officially retired WEP in 2004.

**WPA (Wi-Fi Protected Access)** is a wireless security protocol released in 2003 to address the growing vulnerabilities of its predecessor, WEP. The WPA Wi-Fi protocol is more secure than WEP, because it uses a 256- bit key for encryption, which is a major upgrade from the 64-bit and 128- bit keys used by the WEP system.

WPA also uses the Temporal Key Integrity Protocol (TKIP), which dynamically generates a new key for each packet, or unit of data. TKIP is much more secure than the fixed-key system used by WEP.

Still, WPA is not without flaws. TKIP, the core component of WPA, was designed to be implemented onto WEP-enabled systems via firmware updates. This resulted in WPA still relying on easily exploitable elements.

**WPA2 (Wi-Fi Protected Access 2)** is the second generation of the Wi-Fi Protected Access wireless security protocol. Like its predecessor, WPA2 was designed to secure and protect Wi-Fi networks. WPA2 ensures that data sent or received over your wireless network is encrypted, and only people with your network password have access to it.

A benefit of the WPA2 system was that it introduced the Advanced Encryption System (AES) to replace the more vulnerable TKIP system used in the original WPA protocol. Used by the US government to protect classified data, AES provides strong encryption.

Unfortunately, like it’s predecessor, WPA2-enabled access points (usually routers) are vulnerable to attacks through WEP. To eliminate this attack vector, disable WEP and, if possible, make sure your router’s firmware doesn’t rely on WEP.