Explain various types of cybersecurity threats

- Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
- Common categories of cyber threats include malware, social engineering, man in the middle (MitM) attacks, denial of service (DoS), and injection attacks

Malware attack :

- Malware is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack.
- **Trojan virus** — tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.
- **Ransomware** — prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. Learn more in our guide to ransomware prevention.
- **Wiper malware** — intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.
- **Worms** — this malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS).
- **Spyware** — this malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers.
- **Fileless malware** — this type of malware does not require installing software on the operating system. It makes native files such as PowerShell and WMI editable to enable malicious functions, making them recognized as legitimate and difficult to detect.

Social engineering attacks :

- **Phishing:** Attackers send fraudulent emails or messages impersonating legitimate sources to trick users into revealing sensitive information or downloading malware.

- **Spear Phishing**: Targeted phishing attacks aimed at specific individuals with authority or access to sensitive information.
- **Malvertising:** Malicious advertising containing harmful code that infects users' devices when they interact with the ad.
- **Drive-by Downloads:** Malware is automatically downloaded onto users' devices when they visit compromised websites.
- **Scareware Security Software:** Fake security software that deceives users into paying for unnecessary services or revealing financial information.
- **Baiting:** Placing infected physical devices, like USB drives, in locations where targets are likely to find and use them, leading to malware installation.
- **Vishing:** Voice phishing attacks conducted over the phone to manipulate targets into divulging personal or financial information.
- **Whaling**: Phishing attacks targeting high-profile individuals, such as CEOs or CFOs, to gain access to sensitive company data.

Distributed denial of service (DDoS):

- A DDoS (Distributed Denial of Service) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic.
- Unlike traditional DoS attacks where the attack comes from one source, DDoS attacks involve multiple compromised devices, often distributed across various locations.
- These devices, known as botnets, are controlled remotely by the attacker and coordinated to generate a massive volume of traffic towards the target.

Man-in-the-middle attack (MitM):

- When users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system.
- In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server.
- Once the attacker has intercepted communications, they may be able to compromise a user’s credentials, steal sensitive data, and return different responses to the user.

MitM attacks include:

Session hijacking, Replay attack, IP spoofing, Bluetooth attacks

Password attacks:

A hacker can gain access to the password information of an individual by 'sniffing' the connection to the network, using social engineering, guessing, or gaining access to a password database.

Password attacks include:

- **Brute-force password guessing** — an attacker uses software to try many different passwords, in hopes of guessing the correct one. The software can use some logic to trying passwords related to the name of the individual, their job, their family, etc.
- **Dictionary attack** — a dictionary of common passwords is used to gain access to the computer and network of the victim. One method is to copy an encrypted file that has the passwords, apply the same encryption to a dictionary of regularly used passwords, and contrast the findings.

What is malware? Explain in detail

- Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server.
- Malware is typically delivered in the form of a link or file over email and requires the user to click on the link or open the file to execute the malware.
- Malware may also be created and deployed with the intention of locking the user out of a system or file and drawing a ransom in exchange for the passcode.

Types of malware :

- **Trojan virus** — tricks a user into thinking it is a harmless file. A Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.
- **Ransomware** — prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid. Learn more in our guide to ransomware prevention.
- **Wiper malware** — intends to destroy data or systems, by overwriting targeted files or destroying an entire file system. Wipers are usually intended to send a political message, or hide hacker activities after data exfiltration.
- **Worms** — this malware is designed to exploit backdoors and vulnerabilities to gain unauthorized access to operating systems. After installation, the worm can perform various attacks, including Distributed Denial of Service (DDoS).
- **Spyware** — this malware enables malicious actors to gain unauthorized access to data, including sensitive information like payment details and credentials. Spyware can affect mobile phones, desktop applications, and desktop browsers.
- **Fileless malware** — this type of malware does not require installing software on the operating system. It makes native files such as PowerShell and WMI editable to enable malicious functions, making them recognized as legitimate and difficult to detect.
- **Malvertising:** Malvertising uses legitimate ads to deliver malware to end-user machines.

- **Botnets:** Networks of infected computers (bots) controlled remotely by an attacker, often used to perform distributed denial-of-service (DDoS) attacks.

Preventing and Mitigating Malware :

- **Antivirus Software:** Using up-to-date antivirus software can detect and remove many types of malware.
- **Regular Updates:** Keeping operating systems and software updated helps patch vulnerabilities that malware exploits.
- **Firewalls**: Firewalls can prevent unauthorized access to networks and systems.
- **User Education:** Educating users about safe practices, such as not opening suspicious email attachments or downloading software from untrusted sources, can reduce the risk of infection**.**

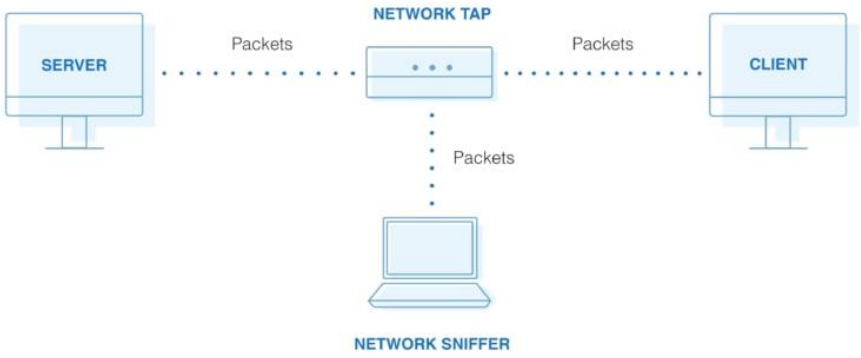
Explain Passive Scanning Technique?

- Passive scanning is a reconnaissance method used by attackers to gather information about a target without directly interacting with the target system.
- This technique minimizes the risk of detection by security systems because it does not involve investigating the target's defenses directly.

Security personnel can use passive vulnerability scanners to:

- Understand what is being sent to and from the various endpoints
- Monitor in-use operating systems
- Monitor various software and their versions
- See which services are available and running
- Identify parts of the network, including open ports that may be vulnerable to threats

- Unlike active scanning, which sends requests or packets to the target and analyzes the responses, passive scanning only gathers information that is readily available, such as information transmitted over the network.
- It is used to gather information about a target system or network for a variety of purposes, including network mapping, vulnerability assessment, and compliance testing.



How Passive scanning can be done –

1. **Websites and Public Information**

- **Company Websites**: Attackers begin by examining the target organization's website. Businesses often publish a wealth of information that can be exploited, such as employee names, job titles, contact information, and organizational structure. For example, if Company XYZ lists John Doe as their IT manager, this information can be a starting point for further research.

- **Social Media and Professional Networks**: Platforms like LinkedIn, Twitter, and Facebook are rich sources of information. Attackers can gather details about employees, their roles, and interactions, which can be used to craft personalized spear-phishing attacks.

2. **Job Advertisements**

- **Technology Stack**: Job ads often specify the technologies and platforms a company uses. If a company frequently advertises for ASP.Net developers, it implies their web applications are built with ASP.Net, running on Windows servers. This information narrows down the potential vulnerabilities an attacker can exploit.
- **Staff Turnover**: Frequent job postings for positions like network administrators in a small company can indicate high turnover. New employees might be less familiar with the company's systems, potentially making it easier for an attacker to exploit their inexperience.

3. **Social Engineering**

- **Pretending to be an Authority Figure: Using** information gathered from public sources, attackers can impersonate someone with authority within the target organization. For example, knowing John Doe's reputation, an attacker might call an employee claiming to be working for John Doe and request login credentials, leveraging the fear of John Doe’s demanding nature to coerce the employee into compliance.
- **Psychological Manipulation:** Attackers exploit emotions like fear, urgency, and helpfulness. By claiming they might get fired if they can't complete a task due to forgotten credentials, attackers increase the likelihood of the target divulging sensitive information.

What is Penetration Testing? Explain step by step process and methods?

- A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities.
- Penetration testing is essentially a controlled form of hacking. The 'attackers' act on your behalf to find and test weaknesses that criminals could exploit.

Penetration testing involves the following five stages:

- **Plan** – start by defining the aim and scope of a test. To better understand the target, you should collect intelligence about how it functions and any possible weaknesses.
- **Scan** – use static or dynamic analysis to scan the network. This informs pentesters how the application responds to various threats.
- **Gain access** – locate vulnerabilities in the target application using pentesting strategies such as cross-site scripting and SQL injection.
- **Maintain access** – check the ability of a cybercriminal to maintain a persistent presence through an exploited vulnerability or to gain deeper access.
- **Analyse** – assess the outcome of the penetration test with a report detailing the exploited vulnerabilities, the sensitive data accessed, and how long it took the system to respond to the pentester's infiltration.

Types of Penetration Testing

Multiple types of penetration tests are available, each with varying objectives, requirements, and scope.

Social Engineering Penetration Testing –

- In a social engineering test, testers attempt to trick employees into giving up sensitive information or allowing the tester access to the organization's systems.

Network Penetration Testing

- Here, the penetration tester audits a network environment for security vulnerabilities. Network penetration tests can be further subdivided into two categories: external tests and internal tests.

Web Application Penetration Testing

- Web application penetration testing is performed to identify vulnerabilities in web applications, websites, and web services. Pen testers assess the security of the code, weaknesses in the application's security protocol, and the design.

Blind testing

- In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

How to detect and eliminate virus, spyware. Explain in detail

- A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works.
- A virus spreads between systems after some type of human intervention.

These are tips for protecting yourself against spyware :

Keep software and operating system updated

- Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- Software updates often include patches or fixes for security vulnerabilities that have been identified since the previous version was released.
- By installing updates promptly, you ensure that your system is equipped with the latest defenses against known security threats.

Use anti-virus software and keep it updated

- Antivirus software is designed to detect and prevent malware infections on your computer. It scans files, programs, and other data for known malware signatures and behavioral patterns associated with malicious activity.
- Many antivirus programs offer real-time protection features that continuously monitor your system for suspicious activity.
- These features can detect and block malware in real-time, preventing it from executing and causing damage to your computer.

Use strong passwords

- Using strong passwords is crucial for protecting your accounts and sensitive information from unauthorized access.
- Strong passwords are harder for attackers to guess or crack using automated tools. By using strong passwords, you greatly reduce the risk of unauthorized access to your accounts and the potential compromise of your personal or sensitive information.
- Brute force attacks involve trying every possible combination of characters until the correct password is found. Strong passwords, especially those with a combination of letters, numbers, symbols, and uppercase and lowercase characters, significantly increase the complexity and difficulty of these attacks.

Never open attachments in spam emails

- Malicious actors often use email attachments as a vector to distribute malware, such as viruses, ransomware, or trojans.
- These attachments may appear harmless at first glance but can contain executable files or scripts designed to infect your computer when opened.
- Email attachments can also be used in phishing attacks, where attackers impersonate legitimate entities to trick recipients into opening malicious attachments.
- In addition to delivering malware, email attachments may also be used to steal sensitive information from unsuspecting victims.

Contact companies directly about suspicious requests

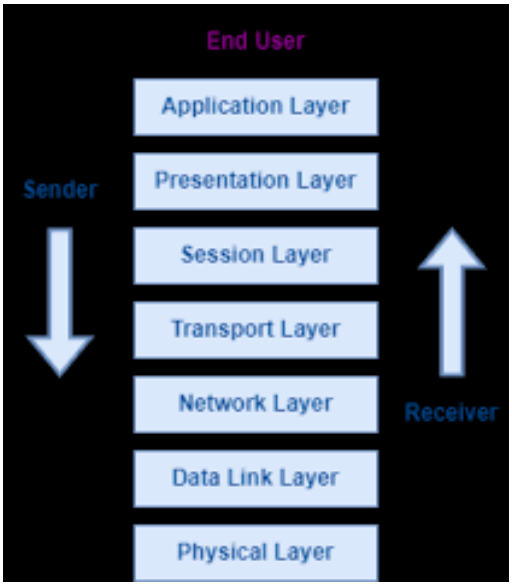
- If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal.
- Ideally, use a different phone to make the call to ensure that the line is not compromised by cybercriminals who could intercept the call.

Manage your social media settings

- Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points.
- For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

Explain OSI Reference model in Detail?

- The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.
- It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.
- It is usually not directly implemented in its entirety in real-world **networking hardware** or **software**. Instead, **specific protocols** and **technologies** are often designed based on the principles outlined in the **OSI model**



Physical Layer – Layer 1

- The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next.

Data Link Layer (DLL) – Layer 2

- The data link layer is responsible for the node-to-node delivery of the message.
- The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
- When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

Network Layer – Layer 3

- The network layer works for the transmission of data from one host to the other located in different networks.
- It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.
- The sender & receiver's IP addresses are placed in the header by the network layer.

Transport Layer – Layer 4

- The transport layer provides services to the application layer and takes services from the network layer.
- The data in the transport layer is referred to as Segments. It is responsible for the end-to-end delivery of the complete message.

Session Layer – Layer 5

- This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Presentation Layer – Layer 6

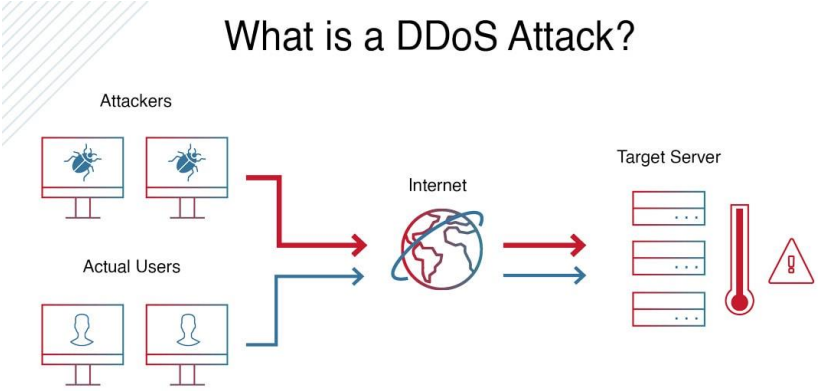
- Also known as the translation layer, the presentation layer translates data so that it can be used by the application layer.
- This layer addresses the syntax and semantics of the information exchanged between the two systems.
- It performs translation, encryption, and compression of data.

Application Layer – Layer 7

- This layer is the closest to the end-user.
- It acts as a window for the application services to access the network and for showing the received information to the user.

Explain DDos with example?

- Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.
- Unlike other kinds of cyberattacks, DDoS assaults don't attempt to breach your security perimeter. Rather, a DDoS attack aims to make your website and servers unavailable to legitimate users.
- A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform.



Types of DDoS Attacks

There are various types of Distributed Denial of Service (DDoS) attacks, each exploiting different vulnerabilities to overwhelm a target's network or services:

1. Volumetric Attacks

Volumetric attacks are the most common type of DDoS attack. They use a botnet to flood the target network or server with excessive traffic, exceeding the network's processing capacity. This overload of junk data consumes all available bandwidth, resulting in a complete denial of service.

2. Protocol Attacks

Protocol attacks, also known as TCP Connection Attacks, exploit vulnerabilities in the TCP handshake process. The attacker sends a request to start a TCP handshake with the target server but never completes the process. This leaves the server's ports in a half-open state, making them unavailable for legitimate requests. Continuous multiple requests overwhelm all the working ports, effectively shutting down the server.

3. Application Attacks

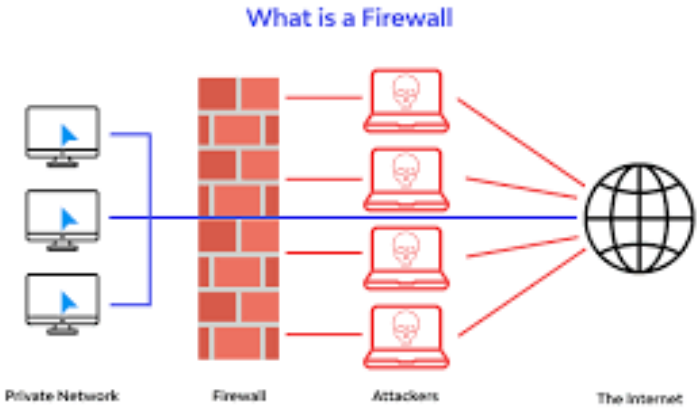
Application layer attacks (Layer 7 attacks) target the applications of the victim, often appearing as legitimate user requests. These attacks focus on the layer where the server generates web pages and responds to HTTP requests. They are combined with other DDoS attacks to target the application, network, and bandwidth simultaneously, making them difficult to detect and mitigate.

4. Fragmentation Attacks

Fragmentation attacks exploit weaknesses in the datagram fragmentation process. IP datagrams are split into smaller packets for transfer across a network and reassembled at the destination. In fragmentation attacks, the attacker sends fake data packets that cannot be properly reassembled, disrupting the network's ability to process legitimate traffic.

What is firewall? Explain types of firewalls

- A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules.
- It acts as a barrier between internal private networks and external sources (such as the public Internet).
- The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks.
- A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.



- **Firewall Types:**
  1. Packet-filtering firewalls
  2. Circuit-level gateways
  3. Stateful inspection firewalls
  4. Application-level gateways (a.k.a. proxy firewalls)
  5. Next-gen firewalls

Packet-Filtering Firewalls

- A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.
- These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.

Circuit-level Gateways

- Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources.
- These types of firewalls typically operate at the session-level of the OSI model by verifying TCP (Transmission Control Protocol) connections and sessions.

Stateful Inspection

- Such a firewall permits or blocks network traffic based on state, port, and protocol.
- Here, it decides filtering based on administrator-defined rules and context.

Application-level Gateways (Proxy Firewalls) :

- Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.

Next-Generation Firewall

- the next-generation firewall is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and information from outside the firewall to go beyond port/protocol inspection and blocking.

Explain the objectives of IT Act?

Objectives of Information Technology Act, 2000

The key objectives of the Information Technology Act, 2000 are:

Provide legal recognition to electronic records and digital signatures: The Act aims to give legal validity and enforceability to electronic records and digital signatures at par with physical documents and handwritten signatures. This enables e-governance and e-commerce.

Facilitate electronic governance and commerce: By recognizing electronic records and signatures, the Act intends to facilitate electronic delivery of government services and transactions between businesses and consumers.

Define and penalize cybercrimes: The Act defines various cybercrimes like hacking, data theft, identity theft, cyberstalking etc. and prescribes penalties for such offences. This aims to create a safe and secure cyber environment.

Regulate cyber activity: The Act empowers the central government to formulate rules and regulations to govern use of electronic medium for online communication and commerce.

Establish institutional mechanisms: The Act establishes mechanisms like adjudicating officers, appellate tribunals and regulatory authorities to enforce the provisions of the Act.

Enable data protection: The Act intends to establish necessary Institutional and legal framework for protecting sensitive electronic data and ensuring data security.

Promote growth of IT sector: By providing a comprehensive legal framework for digital technologies, the Act aims to promote growth of the fledgling but rapidly expanding Indian IT and ITES sector.

Foster innovation: By promoting confidence in digital technologies, the Act seeks to encourage innovation and entrepreneurship in the information technology space.

Features of Information Technology Act, 2000

Here are the key features of the Information Technology Act, 2000:

Gives legal recognition to electronic records and digital signatures: The Act considers electronic records and digital signatures to be at par with physical

documents and handwritten signatures. This is a major feature that enables e-governance and e-commerce.

Defines cybercrimes and prescribes penalties: The Act defines various cybercrimes like hacking, data theft, cyberterrorism, etc. and specifies penalties for such offenses. This helps maintain cyber security.

Provides for establishment of adjudicating officers and tribunals: The Act provides for appointment of adjudicating officers to decide disputes and appellate tribunals to hear appeals against orders of such officers.

Empowers government to make rules and regulations: The Act empowers the central government to frame rules to implement provisions of the Act related to electronic commerce and cybercrime.

Defines roles and responsibilities of intermediaries: The Act clearly specifies conditions under which intermediary liability can be exempted and the due diligence obligations of intermediaries.

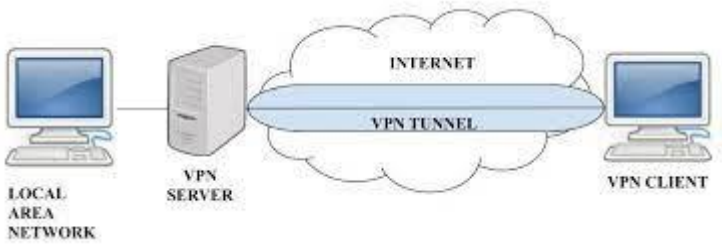
Lays down procedures for use of digital signatures: The Act provides detailed procedures for use of digital signatures along with roles of Certifying Authorities who issue digital signature certificates.

Establishes Indian Computer Emergency Response Team (CERT-In): The Information Technology Act led to creation of CERT-In which is responsible for cybersecurity and cyber incident response.

Amended several times to remain relevant: The Act has been amended in 2008 and 2011 to address technological advancements, implementability concerns and anomalies.

Explain the concept of VPN in detail?

- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network.
- The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.



- There are three different protocols that are used to create VPNs:
    i. Point-to-Point Tunneling Protocol (PPTP)
    ii. Layer 2 Tunneling Protocol (L2TP)
    iii. Internet Protocol Security (IPsec)

Point-to-Point Tunneling Protocol (PPTP)

- PPTP (Point-to-Point Tunneling Protocol) is a type of VPN that uses a simple and fast method for implementing VPNs.
- It creates a secure connection between two computers by encapsulating the data packets being sent between them.
- PPTP is relatively easy to set up and doesn't require any additional software to be installed on the client's device.

L2TP (Layer 2 Tunneling Protocol) VPN

- L2TP (Layer 2 Tunneling Protocol) is a type of VPN that creates a secure connection by encapsulating data packets being sent between two computers.
- L2TP is an extension of PPTP, it adds more security to the VPN connection by using a combination of PPTP and L2F (Layer 2 Forwarding Protocol) and it uses stronger encryption algorithm than PPTP.
- L2TP is relatively easy to set up and doesn't require additional software to be installed on the client's device.

Internet Protocol Security (IPsec) :

- Within the term "IPsec," "IP" stands for "Internet Protocol" and "sec" for "secure."
- The Internet Protocol is the main routing protocol used on the Internet; it designates where data will go using IP addresses.
- IPsec is secure because it adds encryption* and authentication to this process.

There are several types of VPN and these are vary from specific requirement in computer network. Some of the VPN are as follows:

1. Remote Access VPN
2. Site to Site VPN
3. Cloud VPN
4. Mobile VPN
5. SSL VPN

Explain different types of operating system utilities?

- A utility software is one which provides certain tasks that help in proper maintenance of the computer.
- The job of utility programs is to keep the computer system running smoothly. Nowadays many utility softwares are part of the operating system itself.
- Even if there is no utility software on your computer, the computer works but with the right kind of utility software loaded, the computer becomes more reliable and even its processing speed increases.
- Some of the commonly use utility softwares are antivirus, Disk defragmenter, backup, compression etc.

Disk Defragmenter

- The memory is used in small chunks randomly. Sometimes when a memory chunk of appropriate size is not available, the operating system breaks or fragments the files resulting in slower access to files.
- A disk defragmenter scans the hard disk for fragmented files and brings all the fragments together.

Backup Utility

- This utility is used to create the copy of the complete or partial data stored in a disk or CD on any other disk.
- In case the hard disk crashes or some other system failure occurs, the files can be restored using backup software.

Compression Utility

- This utility is used to compress large files. Compression is useful because it helps reduce resources usage and the file transmission on the network becomes easier.

Disk Cleaner

- This utility scans for file that have not been accessed/used since long. Such files might be occupying huge amount of memory space.
- In that case the Disk Cleaner utility prompts the user to delete such files so as to create more space on the disk.

- If the files are important, the user might take a backup before deleting them.

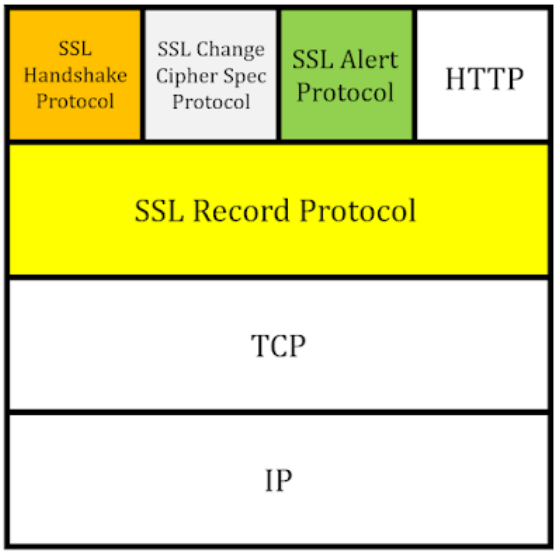
File Management Tools

- This utility helps the user in storing, indexing, searching and sorting files and folders on the system.
- The most commonly used tool is the Windows Explorer and Google Desktop.

Explain concept of SSL

- Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

- SSL is a two layered protocol which was designed to make use of TCP to provide a reliable end-to-end secure service. SSL communicates using the Transport Control Protocol (TCP).
- The term "socket" in SSL refers to the method of sending data via a network between a client and a server.
- A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions.
- SSL is works in between application layer and transport layer the reason SSL is also called TLS (Transport Layer Security).

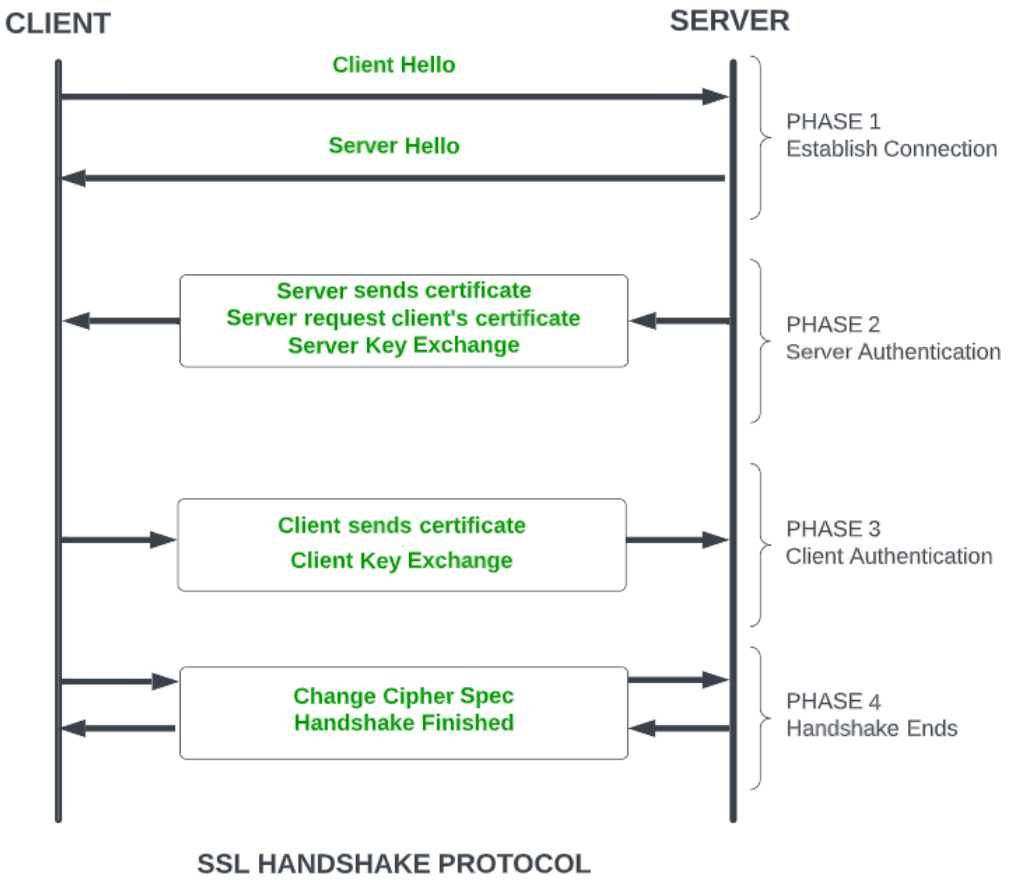


SSL Handshake protocol :

- Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other.

Handshake protocol uses four phases to complete its cycle.

- Phase-1: In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.
- Phase-2: Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.
- Phase-3: In this phase, Client replies to the server by sending his certificate and Client-exchange key.
- Phase-4: In Phase-4 Change-cipher suite occurs and after this the Handshake Protocol ends.



SSL HANDSHAKE PROTOCOL

Explain the Indian cyberspace?

- Cyber Law is the law, which is governing cyber space. Cyber space is a very wide term which includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.
- The law governing all the instruments included in the cyber space is called Cyber law.
- Cyber-crime is the latest and perhaps the most complicated problem in the cyber world.
- Cybercrimes are unlawful acts where computer is used either as a tool; or a target; or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber-crime.
- Thus a simplified definition of cyber law is that it is the “law governing cyber space”.
- Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication.
- It is a large computer network made up of many worldwide computer networks that employ TCP/IP protocol to aid in communication and data exchange activities.
- Cyberspace's core feature is an interactive and virtual environment for a broad range of participants

Threats in cyberspace :

Hacktivism

- Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist.
- Acts of hacktivism may include website defacement, denial-of-service attacks (DoS), website parodies, information theft, virtual sabotage and virtual sit-ins.

Cybercrime

- Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).
- Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes.
- Criminals can also use computers for communication and document or data storage.

Cyber espionage

- Unauthorized spying by computer. The term generally refers to the deployment of viruses that clandestinely observe or destroy data in the computer systems of government agencies and large enterprises.

Cyber terrorism

- Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools.

Describe the methodology for finding evidence on PC

Once you have secured the evidence and made a forensic copy, it is time to start looking for evidence. This evidence can come in many forms:

1**. Finding Evidence in the Browser**

- Direct and Circumstantial Evidence: Browsers can provide both direct and indirect evidence. For example, in cases of child pornography or cyberstalking, browsers might contain direct evidence of the crime. In other cases, such as virus creation, browsers might show indirect evidence, like searches related to virus programming.
- Recovering Deleted History: Even if a user erases their browsing history, it can still be retrieved. Windows stores browsing information in the index.dat file, which contains web addresses, search queries, and recently opened files. Tools available online, such as Eusing's Index.dat Viewer, AceSoft's Index.dat Viewer, and CNET's Index.dat Analyzer, can help retrieve and review this file.

2. Finding Evidence in System Logs

- Windows Logs:
    - Security Log: Contains successful and unsuccessful login events, which are critical for forensic analysis.
    - Application Log: Records events logged by applications, often including errors.
    - System Log: Contains events from Windows system components, such as driver failures, but is usually less relevant to forensics.
    - ForwardedEvents Log: Stores events from remote computers if event forwarding is configured.
    - Applications and Services Logs: Store events specific to applications or components rather than systemwide events.
- Log Manipulation Concerns: Attackers might clear or disable logs using tools like auditpol.exe or WinZapper, which selectively remove log entries.
- Linux Logs:

- /var/log/faillog: Contains failed user login attempts.
- /var/log/kern.log: Logs kernel messages, often less pertinent to computer crimes.
- /var/log/lpr.log: Printer log, useful in corporate espionage cases.
- /var/log/mail.*: Mail server logs, crucial for tracking email-related activities.
- /var/log/mysql.*: Logs MySQL database activities, usually less relevant.
- /var/log/apache2/*: Logs Apache web server activities, useful for tracking web server hacks.
- /var/log/lighttpd/*: Logs Lighttpd web server activities, also useful for tracking web server hacks.
- /var/log/apport.log: Records application crashes, potentially indicating system compromises.
- /var/log/user.log: Logs user activities, important for criminal investigations.

3. Getting Back Deleted Files

- File Recovery Tools: Criminals often attempt to destroy evidence by deleting files. Tools like Disk Digger can be used to recover deleted files on Windows systems. This tool is user-friendly and suitable for learning forensic recovery.

Operation:

- Selecting the Drive: Choose the drive/partition to recover files from.
- Choosing Scan Depth: Select the level of scan, with deeper scans taking longer.
- Viewing Recovered Files: The tool lists recovered files, showing file headers and providing options to recover full files or fragments

This methodology helps forensic investigators systematically gather evidence from various sources on a PC, ensuring a comprehensive analysis of potential digital evidence.

Explain How can you Protect Against Investment Fraud and Identity Theft ?

- Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
- These are tips for protecting yourself against cybercrime. :

Keep software and operating system updated

- Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.
- Software updates often include patches or fixes for security vulnerabilities that have been identified since the previous version was released.
- By installing updates promptly, you ensure that your system is equipped with the latest defenses against known security threats.

Use anti-virus software and keep it updated

- Antivirus software is designed to detect and prevent malware infections on your computer. It scans files, programs, and other data for known malware signatures and behavioral patterns associated with malicious activity.
- Many antivirus programs offer real-time protection features that continuously monitor your system for suspicious activity.
- These features can detect and block malware in real-time, preventing it from executing and causing damage to your computer.

Use strong passwords

- Using strong passwords is crucial for protecting your accounts and sensitive information from unauthorized access.
- Strong passwords are harder for attackers to guess or crack using automated tools. By using strong passwords, you greatly reduce the risk of unauthorized access to your accounts and the potential compromise of your personal or sensitive information.
- Brute force attacks involve trying every possible combination of characters until the correct password is found. Strong passwords, especially those with a combination of letters, numbers, symbols, and uppercase and lowercase characters, significantly increase the complexity and difficulty of these attacks.

Never open attachments in spam emails

- Malicious actors often use email attachments as a vector to distribute malware, such as viruses, ransomware, or trojans.

- These attachments may appear harmless at first glance but can contain executable files or scripts designed to infect your computer when opened.
- Email attachments can also be used in phishing attacks, where attackers impersonate legitimate entities to trick recipients into opening malicious attachments.
- In addition to delivering malware, email attachments may also be used to steal sensitive information from unsuspecting victims.

Contact companies directly about suspicious requests

- If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal.
- Ideally, use a different phone to make the call to ensure that the line is not compromised by cybercriminals who could intercept the call.

Manage your social media settings

- Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points.
- For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

Know what to do if you become a victim:

- If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the **Federal Trade Commission**.
- This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future.