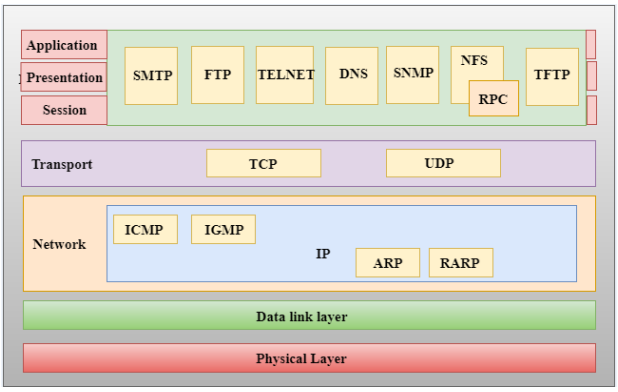
UNIT 1- Cyber Forensics

TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
    - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
    - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

ICMP Protocol

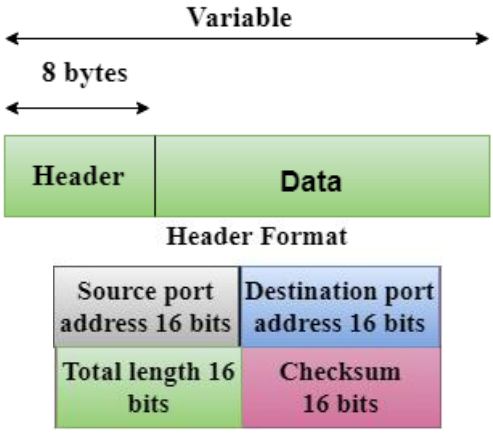
- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
    - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
    - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

Transport Layer

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**
    Source port address: The source port address is the address of the application program that has created the message.
    Destination port address: The destination port address is the address of the application program that receives the message.
    Total length: It defines the total number of bytes of the user datagram in bytes.
    Checksum: The checksum is a 16-bit field used in error detection.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.

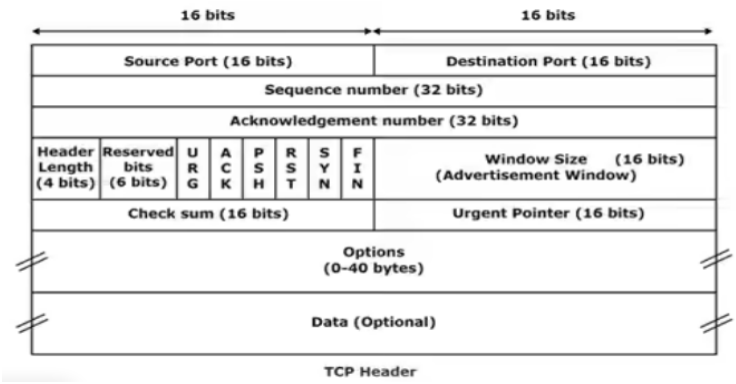
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Conclusion:

Layer Number	Layer Name	Protocol	Protocol Data-unit	Addressing
5(innermost)	Application	HTTP, SMTP	Messages	n/a
4	Transport	TCP/UDP	Segments	Ports
3	Network	IP	Packets	IP Address
2	Data-link	Ethernet/Wifi	Frames	MAC Address
1(outermost)	Physical	10 Base	Bits	n/a



- Source port: this field contains the source port address, which is 16 bits.
- Destination port: So, this field contains the destination port address, which is 16 bits.
- Sequence number: This field contains the sequence number of data bytes in a particular session.
- Acknowledgment number: When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received.
- HLEN: It specifies the length of the header indicated by the 4-byte words in the header.
- Reserved: It is a 4-bit field reserved for future use, and by default, all are set to zero.

There are six control bits or flags:

❖ URG: It represents an urgent pointer. If it is set, then the data is processed urgently.

❖ ACK: If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.

❖ PSH: If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.

❖ RST: If it is set, then it requests to restart a connection.

❖ SYN: It is used to establish a connection between the hosts.

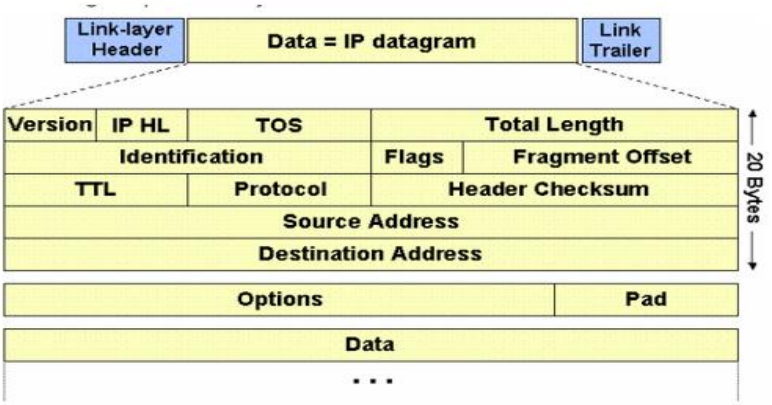
❖ FIN: It is used to release a connection, and no further data exchange will happen.

• Window size: It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment.

• Checksum: It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.

• Urgent pointer: It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.

• Options: It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.



What is a cyber attack?

A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

Any individual or group can launch a cyber attack from anywhere by using one or more various attack strategies.

People who carry out cyber attacks are generally regarded as cybercriminals. Often referred to as *bad actors*, *threat actors* and *hackers*, they include individuals who act alone, drawing on their computer skills to design and execute malicious attacks. They can also belong to a criminal syndicate, working with other threat actors to find weaknesses or problems in the computer systems -- called *vulnerabilities* -- that they can exploit for criminal gain.

Government-sponsored groups of computer experts also launch cyber attacks. They're identified as *nation-state attackers*, and they have been accused of attacking the information technology (IT) infrastructure of other governments, as well as nongovernment entities, such as businesses, nonprofits and utilities.

Why do cyber attacks happen?

Cyber attacks are designed to cause damage. They can have various objectives, including the following:

Financial gain. Cybercriminals launch most cyber attacks, especially those against commercial entities, for financial gain. These attacks often aim to steal sensitive data, such as customer credit card numbers or employee personal information, which the cybercriminals then use to access money or goods using the victims' identities.

Other financially motivated attacks are designed to disable computer systems, with cybercriminals locking computers so owners and authorized users cannot access the applications or data they need; attackers then demand that the targeted organizations pay them ransoms to unlock the computer systems.

Still, other attacks aim to gain valuable corporate data, such as propriety information; these types of cyber attacks are a modern, computerized form of corporate espionage.

Disruption and revenge. Bad actors also launch attacks specifically to sow chaos, confusion, discontent, frustration or mistrust. They could be taking such action as a way to get revenge for acts taken against them. They could be aiming to publicly embarrass the attacked entities or to damage the organizations' reputations. These attacks are often directed at government entities but can also hit commercial entities or nonprofit organizations.

Nation-state attackers are behind some of these types of attacks. Others, called *hacktivists*, might launch these types of attacks as a form of protest against the targeted entity; a secretive decentralized group of internationalist activists known as Anonymous is the most well known of such groups.

Insider threats are attacks that come from employees with malicious intent.

Cyberwarfare. Governments around the world are also involved in cyber attacks, with many national governments acknowledging or suspected of designing and executing attacks against other countries as part of ongoing political, economic and social disputes. These types of attacks are classified as cyberwarfare.

How do cyber attacks work?

Threat actors use various techniques to launch cyber attacks, depending in large part on whether they're attacking a **targeted** or an **untargeted** entity.

In an **untargeted attack**, where the bad actors are trying to break into as many devices or systems as possible, they generally look for vulnerabilities in software code that will enable them to gain access without being detected or blocked. Or, they might employ a phishing attack, emailing large numbers of people with socially engineered messages crafted to entice recipients to click a link that will download malicious code.

In a **targeted attack**, the threat actors are going after a specific organization, and the methods used vary depending on the attack's objectives. The hacktivist group Anonymous, for example, was suspected in a 2020 distributed denial-of-service (DDoS) attack on the Minneapolis Police Department website after a Black man died while being arrested by Minneapolis officers. Hackers also use spear-phishing campaigns in a targeted attack, crafting emails to specific individuals who, if they click included links, would download malicious software designed to subvert the organization's technology or the sensitive data it holds.

Cyber criminals often create the software tools to use in their attacks, and they frequently share those on the so-called dark web.

Cyber attacks often happen in stages, starting with hackers surveying or scanning for vulnerabilities or access points, initiating the initial compromise and then executing the full attack -- whether it's stealing valuable data, disabling the computer systems or both.

In fact, most organizations take months to identify an attack underway and then contain it. According to the "2022 Cost of a Data Breach" report from IBM, organizations with fully deployed artificial intelligence and automation security tools took an average of 181 days to identify a data breach and another 68 days to contain it, for a total of 249 days. Organizations with partially deployed AI and automation took a total of 299 days to identify and contain a breach, while those without AI and automation took an average of 235 days to identify a breach and another 88 days to contain it, for a total of 323 days.

How can you prevent a cyber attack?

There is no guaranteed way for any organization to prevent a cyber attack, but there are numerous cybersecurity best practices that organizations can follow to reduce the risk.

Reducing the risk of a cyber attack relies on using a combination of skilled security professionals, processes and technology.

Reducing risk also involves three broad categories of defensive action:

1. preventing attempted attacks from actually entering the organization's IT systems;
2. detecting intrusions; and
3. disrupting attacks already in motion -- ideally, at the earliest possible time.

Best practices include the following:

- **implementing perimeter defenses**, such as firewalls, to help block attack attempts and to block access to known malicious domains;
- adopting a **zero trust framework**, which requires every attempt to access an organization's network or systems -- whether it comes from an internal user or from another system -- to verify it can be trusted.
- using software to protect against malware, namely **antivirus software**, thereby adding another layer of protection against cyber attacks;

- having a **patch management program** to address known software vulnerabilities that could be exploited by hackers;
- setting appropriate **security configurations, password policies and user access controls**;
- maintaining a **monitoring and detection program** to identify and alert to suspicious activity;
- instituting a **threat hunting program**, where security teams using automation, intelligent tools and advanced analyses actively look for suspicious activity and the presence of hackers before they strike.
- creating **incident response plans** to guide reaction to a breach; and
- **training and educating individual users** about attack scenarios and how they as individuals have a role to play in protecting the organization.

What is Cyber Security?

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

The world of Cyber Security revolves around the industry standard of confidentiality, integrity, and availability, or CIA. Privacy means data can be accessed only by authorized parties; integrity means information can be added, altered, or removed only by authorized users; and availability means systems, functions, and data must be available on-demand according to agreed-upon parameters.

The main element of Cyber Security is the use of authentication mechanisms. For example, a user name identifies an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be.

Types of Cyber Crimes

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it.

Cybercriminals usually try to profit off of their crimes using a variety of tactics, including:

- Denial of Service, or DOS

  Where a hacker consumes all of a server's resources, so there's nothing for legitimate users to access
- Malware

  Where victims are hit with a worm or virus that renders their devices useless
- Man in the Middle

  Where a hacker puts himself between a victim's machine and a router to sniff data packets
- Phishing

  Where a hacker sends a seemingly legitimate-looking email asking users to disclose personal information

Other types of cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (which can also be physical), SQL-injection attacks, and birthday attacks based on algorithm functions.

What Motivates Cyber Criminals?

The main motive behind the cybercrime is to disrupt regular business activity and critical infrastructure. Cybercriminals also commonly manipulate stolen data to benefit financially, cause financial loss, damage a reputation, achieve military objectives, and propagate religious or political beliefs. Some don't even need a motive and might hack for fun or simply to showcase their skills.

So who are these cybercriminals? Here's a breakdown of the most common types:

- Black-Hat Hackers

  Black-hat hackers use fake identities to conduct malicious activities for a profit

- Gray-Hat Hackers

  They work both with malicious intent and as legitimate security analysts

- White-Hat Hackers

  White-hat hackers work as security analysts to detect and fix flaws and protect against malicious hackers

- Suicide Hackers

  They aim to openly bring down the critical infrastructure for a social cause

- Script Kiddies

  They are unskilled hackers who run scripts and software created by more experienced hackers

- Cyber Terrorists

  They create fear by disrupting large-scale computer networks; motivated by religious or political beliefs

- State-Sponsored Hackers

  They penetrate government networks, gain top-secret information, and damage information systems; paid by a hostile government

- Hacktivists

  Promote political agendas by secretly defacing and disabling websites

Cyber-Terrorism

Terrorism: (FBI Definition)

"the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives".

Terrorist:

"one who causes intense fear; one who controls, dominates, or coerces through the use of terror in futherance of political or social objectives".

Cyber-Terrorist:

An individual that uses computer\network technology (i.e., networks, computers, Internet) to cause intense fear; one who uses computer\network technology to control, dominate, or coerce through the use of terror in futherance of political or social objectives.

While some authorities claim that there hasn't been any true cyber terrorism attack yet, others assert that terrorists already take advantage of the Internet. The source of this disagreement is inability to exactly define both "terrorism" and "cyber terrorism".

However some authors were able to produce quite general definitions. In terms of its etymology, the word "terror" comes from the Latin word "terrere", meaning "to frighten, to terrorize, to intimidate". Usually, a series of terror incidents that are interconnected and directed at a certain political target is required in order to arrive a definition of terrorism. According to Bozdemir "Terrorism is a strategic approach which, for political purposes, identifies itself with a method which includes the use of organized, systematic and continuous terror".

Denning defines terrorism as "The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for ideological or political reasons".

Denning also defines cyber terrorism as; the convergence of terrorism and cyberspace. “It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear”.

The term cyber terrorism may be mixed up with “information warfare” and “cyber crime”. But there is a major difference between cyber terrorism and information warfare. Cyber terrorism means premeditated, politically motivated attacks by sub national groups or clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against noncombatant targets. But older term known as information warfare is defined as “a planned attack by nations or their agents against information and computer systems, computer programs, and data that result in enemy losses.”.

National Information Infrastructure (NII)

- Weak overall security
- Documented attacks on 911, air traffic control, stock exchanges, military sites, banks

Global Information Infrastructure (GII)

- Weak overall security
- No borders
- Few if any international agreements

Information Warfare

In the fall of 2006, the U.S. Air Force announced a new mission statement in which it pledges to “fight in Air, Space and Cyberspace.”The new mission statement recognizes what has been apparent for some time : warfare can and will migrate into cyberspace. “Cyberwarfare” constitutes the conduct of military operations by virtual means. It consists of nation-states’ using cyberspace to achieve the same general ends they pursue through the use of conventional military force, i.e., to achieve certain advantages over a competing nation-state or to prevent a competing nation-state from achieving advantages over them.

This is already happening, according to some accounts. There are reports that the People’s Republic of China (“PRC”) is launching cyberattacks that are intended to cripple Taiwan’s infrastructure and “paralyze” the island’s government and economy. The attacks allegedly target Taiwan’s public utility, communications, transportation and “operational security” networks.

As noted above, the distinguishing characteristic of war is that it is a struggle between nation-states; it, like all human activity, is carried out by individuals, but those individuals are acting for a particular nation-state. Like terrorism, warfare tends to result in the destruction of property (often on a massive scale) and in the injury and deaths of individuals (also often on a massive scale). Unlike terrorism, war is supposed to be limited to clashes between the aggregations of individuals (armies) who respectively act for the warring nation-states -- their armies. Injuring and killing civilians (those who are not serving in one of the combatant nation-states' armies) occurs, but like most property damage/destruction, it is supposed to be a collateral event. The primary focus of war in general and of particular wars in specific is to "triumph" over the adversarial nation-state(s), whatever that means in a given context. Inflicting injury/death on civilians and destroying civilian property is not the primary focus of warfare.

Since warfare is conducted between nation-states in an effort to maintain or restore external order, it is essentially outside the scope of this analysis. Our primary concern here is with how those who are charged with adopting and enforcing domestic laws – laws designed to maintain internal order – should address the related phenomena of cybercrime and cyberterrorism.

Definition:

“actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems”

Three General Categories:

Offensive

- To deny, corrupt, destroy, or exploit adversary's information

Defensive

- To safeguard ourselves and allies from similar actions

Exploitation

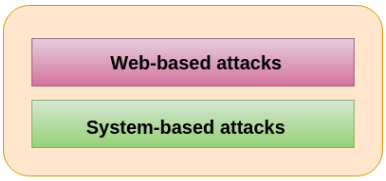
- To exploit information in a timely fashion, to enhance our decision/action cycle and disrupt the adversary's cycle

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Now a day, most of the people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks: It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing: DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker?s computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking: It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing: Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force: It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service: It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks: This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation: It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks: It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks: It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Types of Digital Fraud

The main types of digital fraud impacting online retailers and customers are:

- Account takeover
- Fraudulent payments
- Identity theft

- Phishing
- Ransomware attacks.

Computer Forensics

Computer forensics is a branch of digital forensic science concerned with evidence found in computers and digital storage media, it is defined as the discipline that combines elements of law and computer science to collect and analyze data from wireless communications, computer systems, networks, and storage devices in a way that is permissible as evidence by the court. Because computer forensics is a new discipline, there are not many standard rules or practices for it, there is little standardization and consistency across the industry and courts.

Types of Computer Forensics:

There are multiple types of computer forensics depending on the field in which digital investigation is needed. The fields are:

- Network forensics

  https://www.vskills.in/certification/tutorial/network-forensics/

- Email forensics

  https://www.vskills.in/certification/tutorial/forensics-analysis-of-e-mail/

- Media forensics

  https://www.geeksforgeeks.org/multimedia-forensics/

- Machine forensics

  https://www.slideshare.net/primeteacher32/virtual-machine-forensics