CYBER SECURITY

INTERNSHIP

ASSIGNMENT - 1

WHAT IS CYBER SECURITY?”

is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security comprises cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. “Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity.

Types of Cyber Crime.

- *Hacking*
- *Phishing*
- *Denial of Service*
- *Spam Email*
- *Spyware, Adware*
- *Malware (Trojan, Virus, Worms etc.)*
- *ATM Skimming and Point of Scale*
- *Crimes*
- *Ransomware*

•Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. It is also known as cracking. Government websites are the hot targets of the hackers due to the press coverage, it receives.

.Phishing

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. Phishing is the attempt to obtain sensitive information such as username, password and credit card details, often for malicious reasons through an electronic communication (such as E-mail).A common online phishing scam starts with an email message that appears to come from a trusted source(legitimate site) but actually directs recipients to provide information to a fraudulent web site.

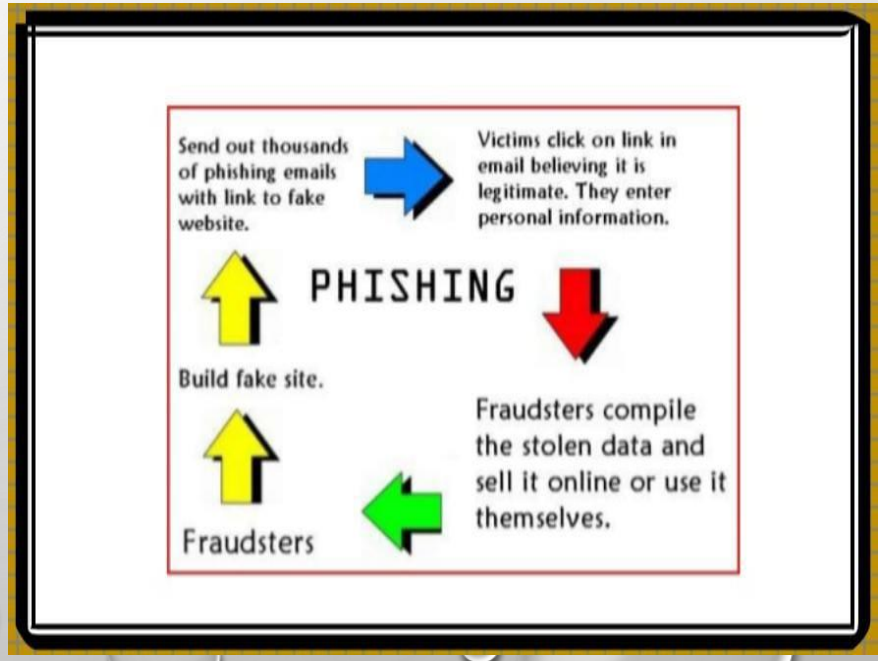
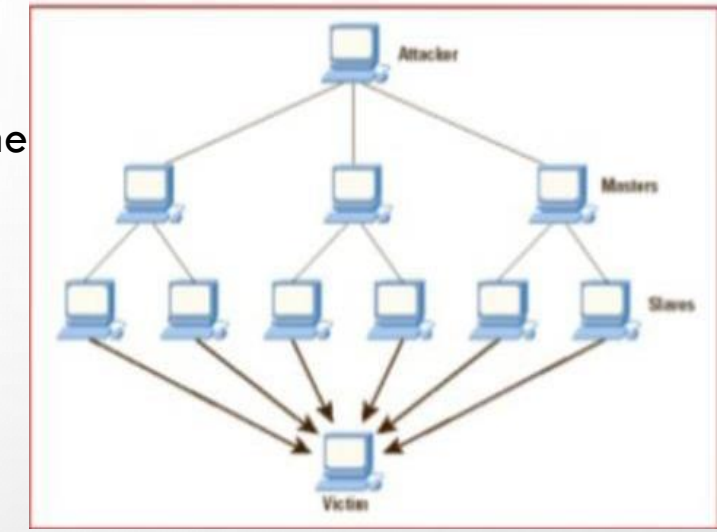
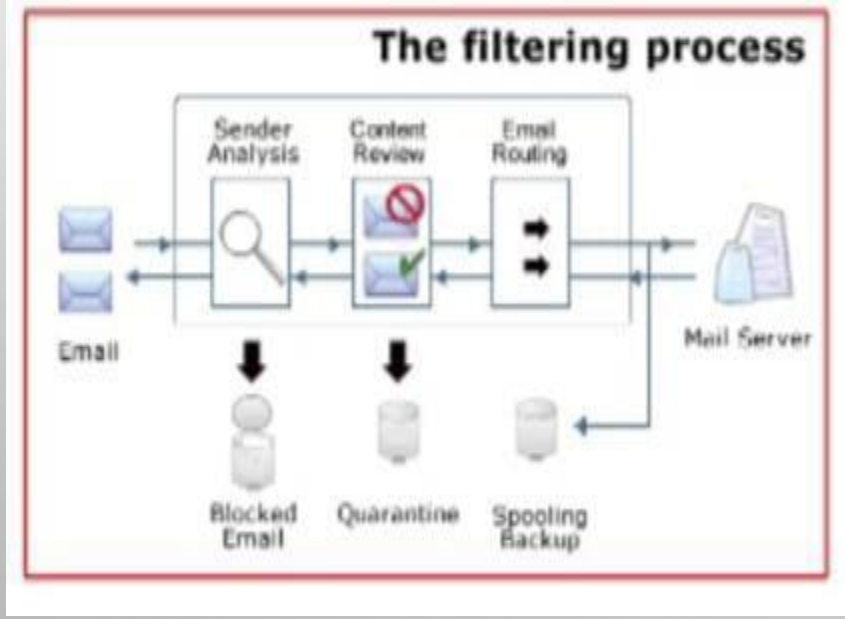


Figure of DDoS attack:



- **Denial of Service**

This is an act by the criminals who floods the Bandwidth of the victims network. In the DoS attack, a hacker uses a single internet connection to either exploit a software vulnerability or flood a target with fake request-usually in an attempt to exhaust server resources. On the other hand, DDoS attacks are launched from multiple connected devices that are distributed across the internet . DoS When a single host attacks. DDoS = when multiple hosts attack simultaneously and continuously.



- **Spam Email**

Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks.

- **Malware**

It's malicious software (such as Virus, Worms & Trojan), which specifically designed to disrupt or damage computer system or mobile device. hackers use malware for any number of reasons such as, extracting personal information or passwords, stealing money, or preventing owners from accessing their device. Viruses are programs that attach themselves to a computer or a file and then. circulate themselves to other files and to other computers on a network. They usually affect the data on a computer and mobile device either by altering or deleting it. Worms unlike viruses do not need the host to attach themselves. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on the computer's memory. Trojan is a type of malware that pretends to be something useful, helpful, or fun while actually causing harm or stealing data. Trojans are often silently downloading other malware (e.g. spyware, adware, ransomware) on an infected device as well.Trojans can infect you in places where you might not expect it, such as emails, downloads and more. It's always better to be safe than sorry when it comes to avoiding this type of malware.

- **Spyware**

Spyware is a type of malware that hackers use to spy on you in order to gain access to your personal information, banking details, or online activity. We should protect ourselves by an anti-spyware tool.

- **Adware**

Adware is a type of malware that bombards you with endless ads and pop-up windows that could potentially be dangerous for your device. The best way to remove adware is to use an adware removal tool.

- **Ransomware**

Ransomware is as scary as it sounds. Hackers use this technique to lock you out of your devices and demand a ransom in return for access. Ransomware puts you in a sticky situation, so it's best to know how to avoid it. Ransomware (a.k.a. rogueware or scareware) restricts access to your computer system and demands that a ransom is paid in order for the restriction to be removed. The most dangerous ransomware attacks are caused by Wannacry , Petya , Cerber and Locky ransomware. The money which suppose to be paid to remove ransomware from your system which is called ransom money.Current affairs: eg. WannaCrypt, Petya Variant

- **ATM Skimming and Point of Scale Crimes**

It is a technique of compromising the ATM machine by installing a skimming device a top the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine . Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number codes that are later replicated to carry out fraudulent transaction.

Layers of TCP/IP Model

Application Layer
Transport Layer(TCP/UDP)
Network/Internet Layer(IP)
Data Link Layer (MAC)
Physical Layer

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

- **What Does TCP/IP Do?**

The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

- **What is the Difference between TCP and IP?**

TCP and IP are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

- **How Does the TCP/IP Model Work?**

Whenever we want to send something over the internet using the TCP/IP Model, the TCP/IP Model divides the data into packets at the sender's end and the same packets have to be recombined at the receiver's end to form the same data, and this thing happens to maintain the accuracy of the data. TCP/IP model divides the data into a 4-layer procedure, where the data first go into this layer in one order and again in reverse order to get organized in the same way at the receiver's end.

1. Physical Layer

it is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

2. Data Link Layer

The packet's network protocol type, in this case, TCP/IP, is identified by the data-link layer. Error prevention and "framing" are also provided by the data-link layer. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of data-link layer protocols.

3. Internet Layer

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows IP: IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions: IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users ICMP: ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems : ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP . The Internet Layer is a layer in the Internet Protocol (IP) suite, which is the set of protocols that define the Internet.

4. Transport Layer

The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. End-to-end communication is referred to as such. Transmission Control Protocol (TCP) and User Datagram Protocol are transport layer protocols at this level (UDP).TCP: Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission UDP: The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

5. Application Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are HTTP and HTTPS: HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and carry out bank transactions . SSH: SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection .NTP: NTP stands for Network Time Protocol.

THE END