Internet

It is the global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols (TCP/ IP).

ARPANET was the world's first fully operational packet switching computer network, developed by the Advanced Research Projects Agency of the U.S. Department of Defense in 1969. It connected with only four computers. ARPANET adopted TCP/IP in 1983 and the “network of networks” became the modern Internet.

World Wide Web - WWW is one of the services interconnected over the internet. It is a collection of all information, resources, pictures, sounds, multimedia on the internet which is formatted in HTML and accessed through HTTP.

Web Server – A web server stores, processes and delivers web pages to the users. The intercommunication between users and servers is done using Hypertext Transfer Protocol (HTTP).

Web Page – It is a document was written in HTML that can be accessed through the internet by using the web browser. It is identified by Uniform Resource Locator.

Web Browser - It is a software application that allows users to access the websites. Internet Explorer, Google Chrome, Opera, Mozilla Firefox, UC Browser, Apple Safari are some examples of a web browser.

Home Page – Homepage is the default page of the website.

Hypertext Mark-up Language (HTML) – HTML is used to create web pages that are displayed on the Internet.

Hypertext Transfer Protocol (HTTP) - This protocol is used to transfer data over the web. It runs on top of the TCP/IP set of protocols. It uses a server-client model.

Transmission Control Protocol/Internet Protocol (TCP/IP) – It is a set of communication protocols which is used to access the internet. TCP/IP was developed by Bob Kahn and Vint Cerf in 1978.

Internet Host – Host is a computer or application which is used to transfer the data on the internet. Each host has a unique IP address called Hostname.

Internet Protocol Address (IP Address) – It is a logical numeric address that is used to identify the host over the internet network.

- The stable version of IP – IPv4 (32 bits). It is written in decimal and separated by periods.
- Latest Version of IP – IPv6 (128 bits). It is written in Hexadecimal and separated by colons.

Uniform Resource Locator (URL) - A uniform resource locator (URL) is used to locate the address of a resource and protocol.

Domain Name - A domain name serves as an address which is used to access the website. It can be universally understood by Web servers and online organizations.

Top Level Domains are following.

Domain Name	Description
.com	Commercial
.net	Network-oriented
.org	Non-Profit Organization
.edu	Education
.gov	Government
.mil	Military
.int	International Treaties

Domain Name System (DNS) – DNS translates domain names into IP addresses. It has a large database of domain names and its IP addresses.

Uploading – It refers to the transmission of data or files from the computer to the internet server. Uploaded file can be retrieved by anyone.

Downloading – It is the process of copying files from the internet to the user's computer.

Email - Electronic mail is the transmission of messages over the internet. In an email, the user can attach documents, pictures, videos etc.

Carbon copy (CC) – It is used to share e-mail with one or more recipients. Both the main recipients and other (CC) recipients can see all the mail addresses.

Blind Carbon Copy (BCC) – In this, the recipients of the message and other recipients (BCC) cannot see the persons who all receive the e-mail.

Computer Security

Computer security also known as cyber security is the protection of information systems from theft or damage to the hardware, the software and to the information on them, as well as from disruption of the services they provide.

Security is based on the following issues:

Privacy: The ability to keep things private/confidential.
Trust: we trust data from an individual or a host.
Authenticity: Are security credentials in order.
Integrity: Has the system been compromised /altered already

Computer Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. It is the unauthorized access to or control over computer network security systems for some illicit purpose.
Viruses, Key loggers, Rootkit, Spoofing attack, Packet Sniffer, Trojan horse, and Password cracking are several of techniques for hacking.

Classification of hackers based on their attitude:

White Hat: A "White hat" hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker.

Black Hat: A "Black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers break into secure networks to destroy, modify, or steal data; or to make the network unusable for those who are authorized to use the network. Black hat hackers are also referred to as the "crackers" within the security industry and by modern programmers.

Grey Hat: A grey hat hacker lies between a black hat and a white hat hacker . Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

Blue Hat: A blue hat hacker is someone outside computer security consulting films who is used to bug-test a system prior to its launch, looking for exploits so they can be closed

Threats classified into one of the categories below:

Back doors: A back door in a computer system, a cryptosystem is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration.

Direct-access attacks: An unauthorized user gaining physical access to a computer is most likely able to directly download data from it.

Eavesdropping: It is the act of surreptitiously listening to a private conversation, typically between hosts on a network.

Spoofing: Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.

Tampering: It describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers

Phishing: It is the attempt to acquire sensitive information such as usernames, passwords and credit card details directly from users.

Types of virus

Computer Virus - A computer virus is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions. Stuxnet, Petya, Wanna cry, Code red, Melissa, Sasser, Zeus, Mydoom, Crypto Locker, Flashback are some example of Viruses.

The Elk Cloner virus was the first self-replicating computer program to spread on a large scale. It was created by a 15-year-old Rich Skrenta in 1982. Ryuk, Troldesh are ransomware family of newly discovered viruses.

Computer Worm - A computer worm is a malicious, self-replicating software program (malware) which affects the functions of software and hardware programs. Stuxnet is the most famous computer worm.

Ransomware - Ransomware is a type of malware program that infects and takes control of a system. It infects a computer with the intention of extorting money from its owner.

Botnet – Botnet is a set of networks connected computers/devices that are used for malicious purposes.

Each computer in a botnet is called Bot. It is also known as Zombie.

Trojan horse – It is a type of malware that presents itself as legitimate software. It may perform actions on a computer that is genuine but will install malware actions.

Keylogger - A keylogger is a type of malware that stores all keystrokes of a computer. It can record all sorts of personal information, such as usernames, passwords, credit card numbers, and personal documents such as emails and reports.

Rootkit - A rootkit is a secret computer program designed to provide continued access to a computer while actively hiding its presence. Rootkits are associated with malware such as Trojans, worms, viruses.

Spyware - Spyware is a software that is installed on a computing device without the end user's knowledge. It steals internet usage data and sensitive information such as usernames and passwords, activating the microphone or camera on a computer to record physical activity.

Adware - Adware is unwanted software designed to display advertisements on the computer screen to generate income. This type of ads cannot be removed easily.

Phishing – Phishing is a cyber-attack that used to steal user data, including login credentials and credit card numbers. They use email as a weapon and trick the email recipient into believing that the message is received from real companies such as banks, Amazon etc to harvest the recipient’s details. Email Phishing, Spear Phishing (targets special person/organization) are techniques of Phishing.

Smurfing - It is a type of denial-of-service attack that relies on flooding a network with a large volume of traffic through the manipulation of IP addresses in that network. This type of attack can result in a high volume of excess activity, which can overwhelm a server or IT setup.

The following are some well-known viruses.

1. CodeRed: It is a worm that infects a computer running Microsoft IIS server. This virus launched DOS attack on White House‘s website. It allows the hacker to access the infected computer remotely.

2. Nimba: It is a worm that spreads itself using different methods. IT damages computer in different ways.

It modified files, alters security settings and degrades performance.

3. SirCam: It is distributed as an email attachment. It may delete files, degrade performance and send the files to anyone.

4. Melisa: It is a virus that is distributed as an email attachment. IT disables different safeguards in MS Word. It sends itself to 50 people if Microsoft Outlook is installed..

5. Ripper: It corrupts data from the hard disk.

6. MDMA: It is transferred from one MS Word file to other if both files are in memory.

7. Concept: It is also transferred as an email attachment. It saves the file in template directory instead of its original location.

8. One Half: It encrypts hard disk so only the virus may read the data. It displays One_Half on the screen when the encryption is half completed