Network Security

Network Security Concepts

Network security is the process of physical and software preventative measures to **protect** the networking infrastructure **from unauthorized access, malfunction, destruction, misuse, modification, or improper disclosure**, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.

Network Security Concepts

Network security threats types:

- Passive Network Threats: Passive cyber attacks employ non-disruptive methods so that the hacker does not draw attention to the attack. Passive attacks are usually data gathering operations, which means they usually employ some sort of malware or hack that eavesdrops on system communications Activities such as wiretapping and idle scans that are designed to intercept traffic traveling through the network.

  •Active Network Threats: Active cyber attacks are often aggressive, blatant attacks that victims immediately become aware of when they occur. Activities such as Denial of Service (DoS) attacks and SQL injection attacks where the attacker is attempting to execute commands to disrupt the network's normal operation. Viruses, worms,Trojan horse,spam,malware, Denial of Service attacks, and password crackers are all examples of active cyber attacks.

Network Security Concepts

Computer virus - is a malicious software program loaded onto a user's computer without the user's knowledge and performs malicious actions.

COMMON TYPES OF COMPUTER VIRUSES

1.RESIDENT VIRUS-Resident viruses set up in RAM and meddle with system operations. They're so sneaky that they can even attach themselves to anti-virus software files.

2.MULTIPARTITE VIRUS-This virus infects the entire system. Multipartite viruses spread by performing unauthorized actions on operating system, folders, and programs.

3.DIRECT ACTION-This virus targets a specific file type, most commonly executable files (.exe), by replicating and infecting files. Due to its targeted nature, this virus type is one of the easier ones to detect and remove.

4.BROWSER HIJACKER-Easily detected, this virus type infects browser and redirects you to malicious websites.

5.OVERWRITE VIRUS-Like the name implies, overwrite viruses overwrite file content to infect entire folders, files, and programs.

6.WEB SCRIPTING VIRUS-This sneaky virus disguises itself in the coding of links, ads, images, videos, and site code. It can infect systems when users download malicious files or visit malicious websites.

7.FILE INFECTOR-By targeting executable files (.exe), file infector viruses slow down programs and damage system files when a user runs them.

8.NETWORK VIRUS-Network viruses travel through network connections and replicate themselves through shared resources.

9.BOOT SECTOR VIRUS-One of the easier viruses to avoid, this virus hides out in a file on a USB drive or email attachment. When activated, it can infect the system's master boot record to damage the system.

Network Security Concepts

Ways to prevent from computer virus –

- Open Emails, Even Coming From Friends, Carefully.
- Install Anti-virus Software and Keep it up to Date
- Scan System Regularly
- Browse Safely
- Download Files Carefully

Network Security Concepts

A computer worm - is a malicious, self-replicating software program (popularly termed as 'malware') which affects the functions of software and hardware programs.

Different types of Computer Worms are:

- Email Worms: Email Worms spread through infected email messages as an attachment or a link of an infected website.

- Instant Messaging Worms: Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

- Internet Worms: Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.

- IRC Worms: IRC Worms spread through IRC chat channels, sending infected files or links to infected websites.

- File-sharing Networks Worms: File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

Network Security Concepts

Ways to prevent from computer worms

- Since software vulnerabilities are major infection vectors for computer worms, be sure that computer's operating system and applications are up to date with the latest versions.

- Install these updates as soon as they're available because updates often include patches for security flaws.

- Phishing is another popular way for hackers to spread worms Always be extra cautious when opening unsolicited emails, especially those from unknown senders that contain attachments or dubious links.
- Be sure to invest in a strong internet security software solution that can help block computer worms.

Network Security Concepts

A Trojan horse - or Trojan, is a type of malicious code or software that looks legitimate but can take control of computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on data or network.

Types of Trojan viruses

- Backdoor Trojans - This type of Trojan allows hackers to remotely access and control a computer, often for the purpose of uploading, downloading, or executing files at will.
- Exploit Trojans -These Trojans inject a machine with code deliberately designed to take advantage of a weakness inherent to a specific piece of software.
- Rootkit Trojans -These Trojans are intended to prevent the discovery of malware already infecting a system so that it can affect maximum damage.
- Banker Trojans -This type of Trojan specifically targets personal information used for banking and other online transactions.
- Distributed Denial of Service (DDoS) Trojans - These are programmed to execute DDoS attacks, where a network or machine is disabled by a flood of requests originating from many different sources.
- Downloader Trojans -These are files written to download additional malware, often including more Trojans, onto a device.

Network Security Concepts

- Ways to prevent from Trojan Horse
- Never download or install software from a source you don't trust completely
- Never open an attachmentor run a program sent in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on computer

Network Security Concepts

Spam - is any kind of unwanted, unsolicited digital communication that gets sent out in bulk through email

Ways to prevent from spam

- Never give out or post your email address publicly
- Think before to click
- Do not reply to spam messages software
- Download spam filtering tools (SpamTitan,**Mailwasher**,ZEROSPA etc) and use anti-virus

Network Security Concepts

- Cookies - are files that contain small pieces of data — like a username and password — that are exchanged between a user's computer and a web server to identify specific users and improve their browsing experience.
- Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like .
- Cookies can’t infect computers with viruses or other malware, although some cyber attacks can hijack cookies and, therefore, browsing sessions.
- Beware Third-Party Cookies-Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads. Cookies
- themselves aren't harmful.

Network Security Concepts

Protection using firewall-

Firewalls are software programs or hardware devices that filter and examine the information coming through your Internet connection.

All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

You need a firewall to protect your confidential information from those not authorised to access it and to protect against malicious users and accidents that originate outside your network.

One of the most important elements of a firewall is its access control features, which distinguish between good and bad traffic.

There are various types of firewall. In ascending order, they are

- Packet layer : This analyses network traffic at the transport protocol layer.
- Circuit level : This validates that packets are either connection or data packets.
- Application layer : This ensures valid data at the application level before connecting.
- Proxy server : This intercepts all messages entering or leaving the network.

Network Security Concepts

- What Kind of Attacks Do Firewalls Protect Against?

• Firewalls prevent cybercriminals from gaining access to your personal information. The issues include, but are not limited to:

• Backdoor Access: A backdoor refers to any security holes or bugs that, when exploited, allow unauthorized control over the program. Even entire operating systems like Windows can have backdoors, and an experienced hacker knows how to take advantage of them.

• Remote Login Hijacking: A remote desktop allows you to connect and control your computer from another location over the internet. However, hackers can hijack the login, access your machine, and steal your files.

• Email Abuse: This type of attack targets an individual in which the perpetrator sends thousands of emails to clog the victim's inbox. Spam email is also popular and while most is merely annoying, some may contain viruses and malware.

• Source Routing: When data packets are traveling through an online network, they are typically "passed along" by multiple routers before reaching its destination. Some hackers take advantage of this system by making malicious data packs look like they're coming from a trusted source. Many firewalls disable source routing for this reason.

Network Security Concepts

HTTPS(Hyper text transfer protocol secure) - helps prevent intruders from tampering with the communications between your websites and your users' browsers. It scramble the messages using that "code" so that no one in between can read the message. It keeps our information safe from hackers.

Https uses the "code" on a Secure Sockets Layer (SSL), sometimes called Transport Layer Security (TLS) to send the information back and forth.

Essentially, we need three things to encrypt data:

- The data to be sent/encrypted
- A unique encryption key
- An encryption algorithm (a math function that garbles the data)

asymmetric encryption is used in https. Asymmetric means we are using two different keys, one to encrypt and one to decrypt.
This encryption is now done at TLS rather than SSL.

Network Security Concepts

Cyber Crime - Any crime that involves a computer and a network is called a “Computer Crime” or “Cyber Crime.

Or in other term ,it is 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).

STEPS TO PROTECT YOURSELF AGAINST CYBER CRIME

1. Make sure your security software is current – and update it regularly.
2. Lock or log off your computer when you step away.
3. Go offline when you don’t need an internet connection.
4. Consider sharing less online.
5. Think twice about using public Wi-Fi.
6. When in doubt, don’t click.

Network Security Concepts

Phishing is a cyber attack that uses disguised email as a weapon.The attackers masquerade as a trusted entity of some kind, The goal is to trick the email recipient into believing that the message is something they want or need — recipient fills/send sensitive information like account no, username ,password etc.

,then attacker use these.

How to prevent phishing

- Always check the spelling of the URLs before click
- Watch out for URL redirects, that sent to a different website with identical design
- If receive an email from that seems suspicious, contact that source with a new email, rather than just hitting reply or phone number, publicly on social media
- Don't post personal data, like your birthday, vacation plans, or your address

Network Security Concepts

Illegal downloading is obtaining files or computer resources that w do not have the right to use from the Internet. Copyright laws prohibit Internet users from obtaining copies of media that we do not legally purchase. These laws exist to prevent digital piracy, much of which is generally conducted through Internet file sharing.

How to prevent illegal downloading

movie piracy has actually decreased significantly through BitTorrent and other traceable methods, as the adoption curve of Netflix (and other) streaming options has increased. The answer there is simple

- make it cheaper and easier to access media in a "legal" manner, and more people will utilize those paths than the "illegal" paths

Network Security Concepts

Child pornography is considered to be any depiction of a minor or an individual who appears to be a minor who is engaged in sexual or sexually related conduct. This includes pictures, videos, and computer-generated content. Even altering an image or video so that it appears to be a minor can be considered child pornography.

Child pornography is a crime in India. IT Act, 2000 & Indian Penal Code, 1860 provides protection from child pornography.The newly passed Information Technology Bill is set to make it illegal to not only create and transmit child pornography in any electronic form, but even to browse it.

Network Security Concepts

With the growth in online services and internet use, there are many opportunities for criminals to commit scams and fraud. These are dishonest schemes that seek to take advantage of unsuspecting people to gain a benefit (such as money, or access to personal details). These are often contained in spam and phishing messages.

Common types of online scams include:

- Unexpected prize scams,
- Unexpected money scams,
- Dating or romance scams,
- Threats and extortion scams,
- Jobs and investment scams, and
- Identity theft.

Do not respond to online scams or fraud. If you receive an email or SMS which looks like a scam, the best thing to do is delete it.It is the best solution for online scam.

Identity Theft

Identity theft or **identity** fraud -in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

- Examples of Identity Theft
- Stolen Checks. If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. ...
- ATM Cards. ...
- Fraudulent Change of Address. ...
- Social Security Number Misuse. ...
- Passports. ...
- Phone Service. ...
- Driver License Number Misuse. ...

Network Security Concepts

Cyber forensics is a way or an electronic discovery technique which is used to determine and reveal technical criminal evidence.

Various capabilities of cyber forensics are.

- Computer forensics
- Computer exams.
- Data analysis.
- Database study.
- Malware analysis.
- Mobile devices.
- Network analysis.
- Photography.
- Video analysis.

Network Security Concepts

Intellectual Property (IP) – is a property created by a person or group of persons using their own intellect for ultimate use in commerce and which is already not available in the public domain.

Examples of IP Property which are, an invention relating to a product or any process, a new design, a literary or artistic work and a trademark (a word, a symbol and / or a logo, etc.),

Intellectual Property Right (IPR) is the statutory right granted by the Government, to the owner(s) of the intellectual property or applicant(s) of an intellectual property (IP) to exclude others from exploiting the IP commercially for a given period of time, in lieu of the discloser of his/her IP in an IPR application.

Network Security Concepts

Why should an IP be protected?

- IP is an assets and can be exploited by the owner for commercial gains any manner
- IP owner may intend to stop others from manufacturing and selling products and services which are dully protected by him
- IP owner can sell and/or license the IP for commercial gains
- IP can be used to establish the goodwill and brand value in the market.
- IP can be mention in resumes of it's creator and thus show competence of it's creator
- IPR certificate establishes legal and valid ownership about an intellectual property

Network Security Concepts

Kinds of IPRs

- **Patent** (to protect technologies - The Patent Act)

- **Trade Mark** (to protect words, signs, logos, labels –The Trade Mark Act)

- **Design** (to protect outer ornamental configuration –The Designs Act)

- **Geographical Indications** (GI) (to protect region specific product –The Geographical Indications of Goods Act)

- **Copyright** (to protect literary and artistic work –The Copyright Act)

Network Security Concepts

IPRs are protected in accordance with the provisions of legislations of a country specific. In India, IPRs can be protected and monopolized as per the act. Some of them are

1The Patent Act, 1970,
2The Designs Act, 2000,
3The Trade Mark Act, 1999,
4The Geographical Indications of Goods Act, 1999,
5The Copyright Act, 1957,
6Protection of Integrated Circuits Layout and Designs Act, 2000,
7- Protection of Plant Varieties and Farmers Rights Act, 2001, and also Trade Secret

Network Security Concepts

Hacking is identifying weakness in computer systems or networks to exploit its weaknesses to gain access. Example:Using password cracking algo. to gain access to a system.

Types of hackers -

- Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
- Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- Script kiddies: A non-skilled person who gains access to computer systems using already made tools.
- Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Network Security Concepts

Cyber law **is any law that applies to the internet and internet-related technologies. Cyber law provides legal protections to people using the internet. This includes both businesses and everyday citizens.** Understanding cyber law is of the utmost importance to anyone who uses the internet.

Cyber law is important because it touches almost **all aspects of transactions and activities and on involving the internet**, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal angles.

Cyber Laws in India prevent any crime done using technology, where a computer is a tool for cybercrime. IT Act 2000 was enacted and amended in 2008 covering different types of crimes under cyber law in India.

Network Security Concepts

The Information Technology Act, 2000 provides legal recognition to the transaction done via an electronic exchange of data and other electronic means of communication or electronic commerce transactions.Some of sections under it act 2000 are given below.

SECTION	OFFENCE	PENALTY
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to Rs. 1,000,000
67B	Publishing child porn or predating children online	Imprisonment up to five years, or/and with fine up to Rs.1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to Rs.1,000,000 on second conviction.
67C	Failure to maintain records	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to three years, or/and with fine up to Rs.200,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to three years, or/and with fine up to Rs.100,000