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 attachment or 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.