Name – Subham Maity
Roll – 14400119043
Subject Code - PEC-CS702E
Subject Name – Cyber Security
Academic Session: 2022-23 (Odd Semester)
Department: CSE(7)
College Name: NITMAS (144)

Topic

Viruses

Explanation

Dos , Worm ,
Trojan Horse

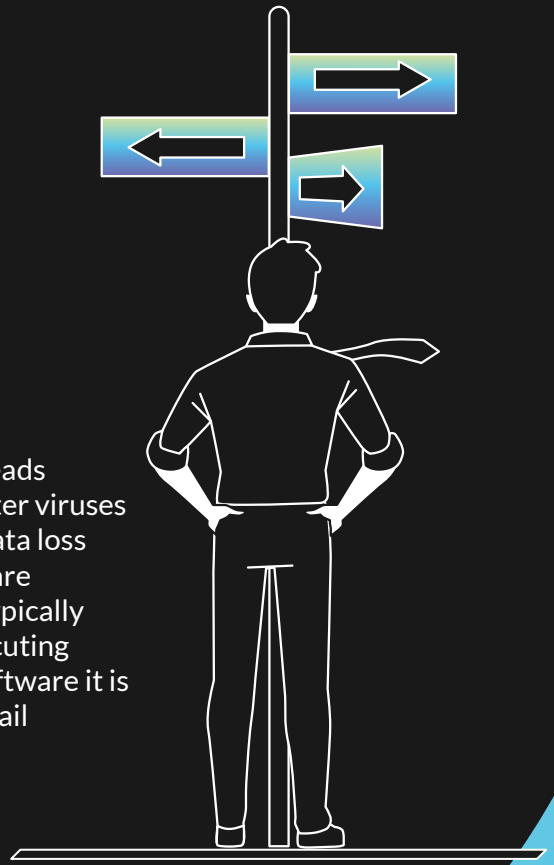
Explanation

Sniffing
Spoofing

Explanation

INTRODUCTION
Virus

A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software. Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage. A key thing to know about computer viruses is that they are designed to spread across programs and systems. Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file-sharing programs, or infected email attachments.



Common Signs of Computer Viruses

Speed of System A computer system running slower than usual is one of the most common signs that the device has a virus. This includes the system itself running slowly, as well as applications and internet speed suffering. If a computer does not have powerful applications or programs installed and is running slowly, then it may be a sign it is infected with a virus.

Pop-up Windows Unwanted pop-up windows appearing on a computer or in a web browser are a telltale sign of a computer virus. Unwanted pop-ups are a sign of malware, viruses, or spyware affecting a device.

Programs Self-executing If computer programs unexpectedly close by themselves, then it is highly likely that the software has been infected with some form of virus or malware. Another indicator of a virus is when applications fail to load when selected from the Start menu or their desktop icon.

Accounts Being Logged Out Some viruses are designed to affect specific applications, which will either cause them to crash or force the user to automatically log out of the service.

Common Signs of Computer Viruses

Crashing of the Device System crashes and the computer itself unexpectedly closing down are common indicators of a virus. Computer viruses cause computers to act in a variety of strange ways, which may include opening files by themselves, displaying unusual error messages, or clicking keys at random.

Mass Emails Being Sent from Your Email Account Computer viruses are commonly spread via email. Hackers can use other people's email accounts to spread malware and carry out wider cyberattacks. Therefore, if an email account has sent emails in the outbox that a user did not send, then this could be a sign of a computer virus.

Changes to Your Homepage Any unexpected changes to a computer—such as your system's homepage being amended or any browser settings being updated—are signs that a computer virus may be present on the device.

Types of Computer Viruses

Resident Virus, Multipartite Virus, Direct Action, Browser Hijacker, Overwrite Virus, Web Scripting Virus, File Infector, Network Virus, Boot Sector Virus

Dos

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users. A DoS attack is characterized by using a single computer to launch the attack.

How does a DoS attack work?

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in a denial of service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall into 2 categories:

Buffer overflow attacks An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in a denial of service.

Flood attacks By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service. In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

Computer worm

A worm virus refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm virus exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.

Email-Worm An email worm refers to a worm that is able to copy itself and spread through files attached to email messages.

IM-Worm An Instant Messenger (IM) worm is a kind of worm that can spread through IM networks. When an IM-worm is operating, it typically finds the address book belonging to the user and tries to transmit a copy of itself to all of the person's contacts.

IRC-Worm An IRC-worm makes use of Internet Relay Chat (IRC) networks to send itself over to other host machines. An IRC worm drops a script into the IRC's client directory within the machine it infects.

Net-Worm A net-worm refers to a kind of worm that can find new hosts by using shares made over a network. This is done using a server or hard drive that multiple computers access via a local-area network (LAN).

P2P-Worm A P2P worm is spread through peer-to-peer (P2P) networks. It uses P2P connections to send copies of itself to users.

Trojan Horse

A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social Engineering to hide malicious code within legitimate software to try and gain users' system access with their software. The simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data.

Sniffing

Sniffing is a process of monitoring and capturing all data packets passing through a given network. Sniffers are used by network/system administrators to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as passwords, account information, etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic.

There are two types:

Active Sniffing:
Sniffing in the switch is active sniffing. A switch is a point-to-point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

Passive Sniffing:
This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network. Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and captured.

Spoofing

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server. Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an advanced persistent threat or a man-in-the-middle attack.

Types of spoofing

Caller ID Spoofing With caller ID spoofing, attackers can make it appear as if their phone calls are coming from a specific number
Website Spoofing Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users.

IP Spoofing Attackers may use IP (Internet Protocol) spoofing to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address spoofing is to gain access to networks that authenticate users based on IP addresses.

ARP Spoofing Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data

DNS Server Spoofing DNS (Domain Name System) servers resolve URLs and email addresses to corresponding IP addresses. DNS spoofing allows attackers to divert traffic to a different IP address, leading victims to sites that spread malware.