• Define Types of Viruses.

Common types of computer viruses include boot sector viruses, file infectors, macro viruses, polymorphic viruses, and resident viruses. These viruses can spread through various means, such as email attachments, infected files, or network vulnerabilities. Understanding these different types of viruses is crucial for implementing effective cybersecurity measures.

Here's a breakdown of some common types of computer viruses:

* **Boot Sector Viruses:**

These viruses infect the boot sector of a storage device, which is crucial for loading the operating system.

* **File Infector Viruses:**

These viruses attach themselves to executable files, and when the infected file is run, the virus executes as well.

* **Macro Viruses:**

These viruses are written in the same macro language used by applications like Microsoft Word or Excel and can be embedded in documents.

* **Polymorphic Viruses:**

These viruses change their code each time they infect a system, making them harder to detect with traditional antivirus methods.

* **Resident Viruses:**

These viruses install themselves in the computer's memory and can infect other files even after the original infected program is closed.

* **Direct Action Viruses:**

These viruses are designed to carry out specific actions, such as modifying files or causing system instability.

* **Multipartite Viruses:**

These viruses can infect both the boot sector and files, making them more versatile and dangerous.

* **Browser Hijackers:**

These viruses alter browser settings without permission, potentially redirecting users to malicious websites.

* **Web Scripting Viruses:**

These viruses exploit vulnerabilities in web scripting languages like JavaScript to execute malicious code on websites.

• Create virus using Http Rat Trojan tool.

A RAT or remote administration tool, is software that gives a person full control a tech device, remotely. The RAT gives the user access to your system, just as if they had physical access to your device. With this access, the person can access your files, use your camera, and even turn on/off your device. RAT is used to remotely connect and manage single or multiple computers. RAT is one of the most dangerous Trojan because it compromises features of all types of Trojans. It provides an attacker with nearly unlimited access to host computer along with Screen Capture, File management, shell control and device drivers control. RATs uses reverse connections to connect remote system and hence are more likely to remain undetected. They can hide themselves in process space of legitimate program and hence never appear in task manager or system monitors. A Trojan generally has two parts Client and Server or Master and Slave. We can say Server is Slave and Client is Master. So a server side is installed on a remote host and the attacker manipulates it with client software.

• Explain any one Antivirus with example.

Antivirus software is a crucial component of cybersecurity that protects devices from malware, including viruses, worms, and trojans. One example of a widely used antivirus is Norton AntiVirus Plus. It actively monitors for threats, scans incoming files and programs, and eliminates or quarantines identified malware. Norton also offers features like real-time protection, phishing and ransomware shields, and a firewall to enhance overall security.

Here's a more detailed explanation:

How Antivirus Software Works:

* **Real-time scanning:**

Antivirus software continuously monitors your computer for suspicious activity, scanning files and programs as they are accessed or executed.

* **Signature-based detection:**

Antivirus programs maintain a database of known malware signatures. When a file matches a signature, it's identified as malicious.

* **Heuristic analysis:**

This method analyzes the behavior of programs to detect suspicious activities that might indicate malware, even if the specific malware isn't in the database.

* **Quarantine and removal:**

If malware is detected, antivirus software can isolate it in a quarantine area or remove it from the system.

* **Regular updates:**

Antivirus software needs to be regularly updated with the latest malware definitions and security protocols to stay effective against new threats.

Example: Norton AntiVirus Plus:

* **Comprehensive Protection:**

Norton AntiVirus Plus provides protection against various types of malware, including viruses, spyware, ransomware, and phishing attacks.

* **Real-time threat protection:**

It constantly monitors your computer for suspicious activity, blocking threats as they emerge.

* **Firewall:**

A built-in firewall helps prevent unauthorized access to your computer by blocking malicious network traffic.

* **Password Manager:**

Norton AntiVirus Plus also includes a password manager to help you create and manage strong, unique passwords for your online accounts.

* **Performance Optimization:**

Some antivirus software, like Norton, also includes tools to optimize your computer's performance and remove unnecessary files