Ethical Hacking

Module-4

- **Define Types of Viruses.**

Boot Sector Virus

Boot sector viruses infect either the master boot record of the hard disk or the floppy drive. The boot record program responsible for the booting of operating system is replaced by the virus. The virus either copies the master boot program to another part of the hard disk or overwrites it. They infect a computer when it boots up or when it accesses the infected floppy disk in the floppy drive. i.e. Once a system is infected with a boot-sector virus, any non-write-protected disk accessed by this system will become infected.

Examples of boot- sector viruses are Michelangelo and Stoned.

File or Program Viruses

Some files/programs, when executed, load the virus in the memory and perform predefined functions to infect the system. They infect program files with extensions like .EXE, .COM, .BIN, .DRV and .SYS.

Some common file viruses are Sunday, Cascade.

Multipartite Viruses

A multipartite virus is a computer virus that infects multiple different target platforms, and remains recursively infective in each target. It attempts to attack both the boot sector and the executable, or programs, files at the same time. When the virus attaches to the boot sector, it will in turn affect the system's files, and when the virus attaches to the files, it will in turn infect the boot sector.

This type of virus can re-infect a system over and over again if all parts of the virus are not eradicated.

Ghostball was the first multipartite virus, discovered by Fridrik Skulason in October 1989.

Other examples are Invader, Flip, etc.

Stealth Viruses

These viruses are stealthy in nature means it uses various methods for hiding themselves to avoid detection. They sometimes remove themselves from the memory temporarily to avoid detection by antivirus. They are somewhat difficult to detect. When an antivirus program tries to detect the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector.

Polymorphic Viruses

Polymorphic viruses have the ability to mutate implying that they change the viral code known as the signature each time they spread or infect. Thus an antivirus program which is scanning for specific virus codes unable to detect it's presense.

Macro Viruses

A macro virus is a computer virus that “infects” a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless.A macro virus is often spread as an e-mail virus. Well-known examples are Concept Virus and Melissa Worm.

Malware

Malware – Malware is programming or files that are developed for the purpose of doing harm. Thus, malware includes computer viruses, worms, Trojan horses, spyware, hijackers, and certain type of adware.

Backdoor

A program that allows a remote user to execute commands and tasks on your computer without your permission. These types of programs are typically used to launch attacks on other computers, distribute copyrighted software or media, or hack other computers.

Hijackers

A program that attempts to hijack certain Internet functions like redirecting your start page to the hijacker’s own start page, redirecting search queries to a undesired search engine, or replace search results from popular search engines with their own information.

Spyware

A program that monitors your activity or information on your computer and sends that information to a remote computer without your Knowledge.

Adware

A program that generates popups on your computer or displays advertisements. It is important to note that not all adware programs are necessarily considered malware.

There are many legitimate programs that are given for free that display ads in their programs in order to generate revenue. As long as this information is provided up front then they are generally not considered malware.

Dialler

A program that typically dials a premium rate number that has per minute charges over and above the typical call charge. These calls are with the intent of gaining access to pornographic material.

Trojan

A program that has been designed to appear innocent but has been intentionally designed to cause some malicious activity or to provide a backdoor to your system.

Worm

A program that when run, has the ability to spread to other computers on its own using either mass-mailing techniques to email addresses found on your computer or by using the Internet to infect a remote computer using known security holes.

- **Explain any one Antivirus with example.**

Antivirus software is a security program designed to prevent, detect, search and remove viruses and other types of malwares from computers, networks and other devices. Often included as part of a security package, antivirus software can also be purchased as a standalone option.

Typically installed on a computer as a proactive approach to cybersecurity, an antivirus program can help mitigate a variety of cyber threats, including keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, phishing attempts and ransomware attacks.

Due to the constantly evolving nature of cybercrimes and new versions of malware being released daily, including zero-day attacks, no antivirus program can offer detection and protection against all threat vectors.

A virus is just one of the many types of malwares that antivirus software is designed to prevent, detect, search and remove.

How antivirus software works.

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities and perform system scans that monitor device and system files, looking for possible risks.

Antivirus software usually performs the following basic functions: -

- ✓ Scans directories or specific files against a library of known malicious signatures to detect abnormal patterns indicating the presence of malicious software.
- ✓ Enables users to schedule scans so they run automatically.
- ✓ Lets users initiate new scans at any time.
- ✓ Removes any malicious software it detects either automatically in the background or notifies users of infections and prompts them to clean the files.

To scan systems comprehensively, antivirus software must generally be given privileged access to the entire system. This makes antivirus software itself a common target for attackers, and researchers have discovered remote code execution and other serious vulnerabilities in antivirus software products in recent years.