Information Technology
Lect. Harish Gupta
Department of Architecture
Govt. Polytechnic Panchkula

Lecture
Anti virus

1.0 Antivirus

Antivirus software is a class of program designed to prevent, detect and remove malware infections on individual computing devices, networks and IT systems. Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety of threats, including other types of malicious software, suchas keyloggers, browser hijackers, Trojan, horses, worms, rootkits, spyware, adware, botnets and ransomware.

2.0 Functioning of antivirus software

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 as they happen, as well as system scans that monitor device and system files looking for possible risks.

Antivirus software usually performs these basic functions:

- Scanning directories or specific files for known malicious patterns indicating the presence of malicious software;
- Allowing users to schedule scans so they run automatically;
- Allowing users to initiate new scans at any time; and
- Removing any malicious software it detects. Some antivirus software programs do this automatically in the background, while others notify users of infections and ask them if they want to clean the files.

In order 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.

3.0 Features of an Effective Antivirus

The following features of any antivirus are to be looked for when you decide on installing one

Proactive scanning for malwares, and deleting once detected

Default-Deny Protection – Default-Deny protection that is implemented to prevent the entry of suspicious files by default.

Auto Sandbox Technology – A virtual environment where suspicious and unknown files are secluded and run to check for any malicious activity without interfering with the normal operations.

Containment Technology – Validates and authorizes the programs that are executable and ensures that the processes are run without effecting the regular operations of the system.

Host Intrusion Protection System (HIPS) – This feature works on a protocol-based intrusion prevention system, that oversees all the application and program activities that aare processed in the system. The HIPS terminates any malicious activities once found. This prevents the malware from infecting the operating system, registry keys or personal data or system memory.

4.0 Types of Antivirus

Antiviruses are also of different types based on the OS compatibility

Antivirus for Windows OS

Antivirus for Linux OS

Antivirus for Android OS

Antivirus for MAC OS Types of antivirus programs

Antivirus software is distributed in a number of forms, including stand-alone antivirus scanners and internet security suites that offer antivirus protection, along with firewalls, privacy controls and other security protections.

Some antivirus software vendors offer basic versions of their products at no charge. These free versions generally offer basic antivirus and spyware protection, but more advanced features and protections are usually available only to paying customers. While some operating systems are targeted more frequently by virus developers, antivirus software is available for most Operating Systems are :

- **Windows antivirus software**. Most antivirus software vendors offer several levels of Windows products at different price points, starting with free versions offering only basic protection. Users must start scans and updates manually and typically free versions of antivirus software won't protect against links to malicious websites or malicious attachments in emails. Premium versions of antivirus software often include suites of endpoint security tools that may provide secure online storage, ad blockers and file encryption. Since 2004, Microsoft has been offering some kind of free antivirus software as part of the Windows operating system itself, generally under the name Windows Defender, though the software was mostly limited to detecting spyware prior to 2006.
- **Mac OS antivirus software**. Although mac OS viruses exist, they're less common than Windows viruses, so antivirus products for mac OS are less standardized than those for Windows. There are a number of free and paid products available, providing on-demand tools to protect against potential malware threats through full-system malware scans and the ability to sift through specific email threads, attachments and various web activities.
- **Android antivirus software**. Android is the world's most popular mobile operating system and is installed on more mobile devices than any other OS. Because most mobile malware targets Android, experts recommend all Android device users install antivirus software on their devices. Vendors offer a variety of basic free and paid premium versions of their Android antivirus software including anti-theft and remote-locating features. Some run automatic scans and actively try to stop malicious web pages and files from being opened or downloaded.

5.0 Virus detection techniques

Antivirus software uses a variety of virus detection techniques. Originally, antivirus software depended on signature-based detection to flag malicious software. Antivirus programs depend on stored virus signatures -- unique strings of data that are characteristic of known malware. The antivirus software uses these signatures to identify when it encounters viruses that have already been identified and analysed by security experts.

Signature-based malware cannot detect new malware, including variants of existing malware. Signature-based detection can only detect new viruses when the definition file is updated with information about the new virus. With the number of new malware signatures increasing at around 10 million per year as long ago as 2011, modern signature databases may contain hundreds of millions, or even billions, of entries, making antivirus software based solely on signatures impractical. However, signature-based detection does not usually produce false positive matches.

Heuristic-based detection uses an algorithm to compare the signatures of known viruses against potential threats. With heuristic-based detection, antivirus software can detect viruses that haven't been discovered yet, as well as already existing viruses that have been disguised or modified and released as new viruses. However, this method can also generate false-positive matches when antivirus software detects a program behaving similarly to a malicious program and incorrectly identifies it as a virus.

Antivirus software may also use behaviour-based detection to analyse an object's behaviour or potential behaviour for suspicious activities and infers malicious intent based on those observations. For example, code that attempts to perform unauthorized or abnormal actions would indicate the object is malicious, or at least suspicious. Some examples of behaviours that potentially signal danger include modifying or deleting large numbers of files, monitoring keystrokes, changing settings of other programs and remotely connecting to computers.