Course Name : O Level(B4-Ist sem.)	Subject : ITT&NB

Topic : About Antivirus	Date : 15-06-20

Antivirus in Windows Operating System

Virus, Worm, and Malware

Virus

A computer virus is a piece of software that can 'infect' a computer, install itself and copy itself to other computers, without the users knowledge or permission**.** Virus is designed to spread from host to host and has the ability to replicate itself. A computer virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. It also known as Threat.

Once a virus has successfully attached to a program, file, or document, it will lie dormant until circumstances cause the computer or device to execute its code. A virus can do stealing passwords or data, logging keystrokes, corrupting files, spamming email contacts etc.

Worm

Unlike a virus, a worm is a standalone piece of malicious software that replicates itself in order to spread to other computers. Often, it simply clones itself over and over again and spreads via a network (say, the Internet, a local area network at home, or a company's intranet) to other systems where it continues to replicate itself.

One of the most common ways for worms to spread is via email spam. Worms could hide in the main text of an email, but as modern email clients caught on and began blocking.

Malware

Malware is short for "malicious software" and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a standalone computer or a networked computer. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission**.**

Trojan horse

A type of malware that uses malicious code to install software that seems ok, but is hidden to create back doors into a system. This typically causes loss or theft of data from an external source.

Spyware

Spyware is software that aids in gathering information about a person or organization without their knowledge. Spyware can monitor and log the activity that is performed on a target system, like log key strokes, or gather credit card and other information.

Introduction to Antivirus software

Antivirus software was originally developed to detect and remove computer viruses. If a virus is detected, the computer displays a warning asking what action should be done. In particular, modern antivirus software can protect from: malicious browser helper objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, trojan horses, worms, fraud tools, adware and spyware. Some software also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, etc.

Working of Antivirus Software

Antivirus software will scans the file on computer programs and comparing specific bits of code against information in its database and if it finds a pattern duplicating one in the database, it is considered a virus, and it will quarantine or delete that particular file It will also scan computer for behaviors that may signal the presence of a new, unknown malware**.**

Different Types of Antivirus Software:

Different Types of Antivirus Software are Avira, Awast, Macfee, AVG, BITDefender, kaspersky, Trendmicro etc.

Exercise:

1. **Write short notes on Antivirus.**