



CLASS - VI - COMPUTER SCIENCE JANUARY MONTH NOTES

CHAPTER - 8 COMPUTER VIRUS

A. Tick (✓) the correct option.

1. In _____ Melissa virus attacked Microsoft.
(c) March 1999
2. The Creeper virus was detected on the _____.
(b) ARPANET
3. Which virus infects program files which have an .exe extension?
(c) Direct Action Virus
4. Virus can infect files that are saved in _____.
(c) All of these
5. Computer viruses spread through:
(c) All of the above

B. Fill in the blanks.

1. Memory Resident Virus is a type of virus that hides and stores itself in the computer memory.
2. Macroviruses target applications and software that contain macros.
3. FAT stands for File Allocation Table.
4. A Script virus usually infects a system when you visit certain webpages.
5. Network virus spreads through Local Area Network and sometimes the Internet.

C. Write 'T' for true and 'F' for false for the following statements.

1. VIRUS stands for Vital Information Under Size. F
2. Computer viruses are computer programs that cause harm to computers. T
3. For using an antivirus software, it is not necessary to install it in the computer. T
4. Creeper virus was detected in the 1970s. T
5. A virus also affects the hardware of the computer. F

D. Differentiate between:

1. Macro Virus and Directory Virus

Macro Virus:

- Macro viruses target applications and software that contain macros.
- These viruses can carry out a series of operations affecting the performance of the program or software.

Directory Virus:

- This virus works by changing the path of the file location by infecting the directory of your computer.
- These viruses infect the entire directory but are usually found in a location in the disk.

2. Virus and Worm

Virus:

- A virus is a computer program that attaches itself to other programs without the consent of the owner.
- The main intention of the virus is to cause harm to the computer.

Worm:

- A worm is a computer program capable of replicating and spreading to other computers through a computer network.
- Worms are particularly destructive because they can spread without a user's help

3. Spyware and Sweeper

Spyware:

- Spyware is unwanted software that infects your computing device and steals your Internet usage data and sensitive information.
- Spyware is a type of malware designed to gain access to, or damage your computer, often without your knowledge.

Sweeper:

- Sweeper is a fake antivirus program. It is also known as a rogue.
- Sweeper usually enters a computer system in one of two possible ways.

E. Short answer questions.

1. What is a computer virus?

- A VIRUS is a computer program that attaches itself to other programs without the consent of the owner.
- The main intention of the virus is to cause harm to the computer.

2. Name the different types of viruses.

The different types of viruses are:

- Web Scripting Virus
- FAT Virus
- Polymorphic Virus
- Directory Virus
- Boot Sector Virus
- Overwrite Virus
- Memory Resident Virus
- Direct Action Virus
- Macro Virus
- Network Virus

3. What do you mean by Trojan Horse?

- Trojan Horse is a computer program which misrepresents itself to appear useful to convince the user to install it.
- In Trojan Horse, the code is hidden in a program like a game or a spreadsheet which looks safe for running but has hidden side effects.

4. Define malware.

- There are some other kinds of software and malicious programs that attack computers.
- They are Worm, Spyware, Trojan Horse and Sweeper.
- These are also known as malware, which is short for malicious software. Viruses are also a type of malware.

5. What is a firewall?

- A software program or a hardware device which filters the traffic flowing into the PC or the network through an Internet connection is called a firewall.
- It is used to protect the machine from viruses. It stops unauthorized persons from accessing the device.

F. Long answer questions.

1. Explain five different types of viruses.

Five different types of viruses are:

FAT Virus:

- FAT stands for File Allocation Table.
- This is the most commonly used process in Microsoft to maintain and access information about all files quickly.
- FAT viruses infect this file allocation table causing widespread damage

Oligotrophic Virus:

- This virus infects a computer as part of an encrypted file.
- These viruses are less or not harmful since they cannot take control of the encrypted source code.

Polymorphic Virus:

- Polymorphic viruses use a special method of encoding or encryption every time they infect a system.
- They can replicate very easily.

Directory Virus:

- This virus works by changing the path of the file location by infecting the directory of your computer.
- These viruses usually found in a location in the disk.

Boot Sector Virus:

- Boot sector viruses affect floppy disks.
- They came into existence when floppy disks were important as they were also used to boot a computer.

2. What are the symptoms of a virus attack?

The symptoms of a virus attack may be all or one of the following:

- Unexpected error messages pop up.
- Unexplained data is lost.
- Certain drives on the computer become inaccessible.
- Dialogue boxes and menus appear distorted.
- The computer may restart repeatedly.
- The size of files may change.
- Applications take longer to load or do not work at all.

3. List some harmful activities performed by viruses.

Some harmful activities performed by a virus are:

- Infect executable files such as word processors, spreadsheets and operating systems.
- Infect disks by attaching themselves to special programs called boot records on hard disks.
- Infect files attached to e-mail messages or infecting disks and pen drives attached to an infected computer.

4. Can you prevent a virus attack on your computer? How?

Yes, a virus attack can be prevented on a computer.

- Install an antivirus program and keep it updated.
- Ignore unknown attachments in e-mails.
- Isolate the drives that have been affected.
- Install a firewall to check incoming and outgoing network traffic.
- Avoid downloading pirated software from the Internet.
- Scan the downloaded files before opening them.
- Take a backup of important files.
- Never use an unknown disk or storage device without scanning it.

5. What is antivirus software?

- Antivirus software usually runs as a background process, scanning computers, servers to detect the spread of malware.
- Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities.
- Antivirus software usually performs the following basic functions:
 - Scanning directories or specific files for known malicious activity indicating the presence of malicious software.
 - Allowing users to schedule scans so that they run automatically.
 - Allowing users to initiate new scans at any time.
 - 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.