

Name :- Rugvedi Jamgaonkar

Roll No - 15

Subject :- Cyber Security - I

Class :- Msc computer science - I

Enrollment Number :- 2002242

### Assignment - 1

#### \* Introduction to computer contaminant

##### 1. Concept of computer contaminant :-

① Computer contaminant means set of computer instructions that are designed -

a) to modify, destroy, record, transmit data or program residing within a computer or computer network.

b) by any means to USURP the normal operation of the computer, computer system or computer network.

④ Computer contaminants are also called as malicious codes

⑤ and there are three broad categories of computer contaminants are :-

① Computer virus ② Worm ③ Trojan

##### 2. Concept of computer viruses :-

① A virus is one of the popular form of a computer contaminant which creates negative impact on the computer system

② A virus is a small piece of code that attaches itself to another program and enters into the computer system

③ There are two phases of computer virus :-

① Insertion phase and ② Execution phase.

④ There are three basic functions of computer virus :-

1. It deletes data

2. It destroys data

3. It modifies data



3. Two types of computer virus :-

- ① Boot sector virus :- It infects the boot sector of the system, executing every time system is booted and before operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory virus as they do not infect file system.
- ② Direct Action Virus :- When a virus attaches itself directly to a .exe or .com file and enters the device while its execution is called a Direct action virus. If it gets installed in the memory, it keeps itself hidden. It is also known as Non-Resident virus.

4. Concept of Worm :-

- ① A computer worm is the another form of computer contaminant which creates negative impact on the computer system
- ② A worm is a standalone program which creates replicas of itself and occupies a space of hard disk. A worm
- ③ hampers speed of the computer system significantly but if it remains in a computer for a longer period of time it crashes the entire computer system
- ④ A worm infects the vulnerable computers and travels through the computer networks.

5. Concept of Trojan - Rootkit, keylogger :-  
Trojan :-

- ① A trojan is one of the most dangerous form of computer contaminant which has some known and unknown effects.
- ② A trojan enters into the the computer with the permission of the user by hiding itself with the utility programs.
- ③ Trojans are generally use by the cyber criminals for the purpose of hacking the computer system
- ④ Following are two



Page: \_\_\_\_\_

broad categories of a trojan:

1. Root kit program :-

Also known as RAT (Remote Access Trojan).<sup>①</sup> A root kit is a specific form of trojan which enters into the computer system by attaching itself to the utility program.<sup>②</sup> A root kit program is one of the popular tool used for the purpose of hacking the computer system.

- ③ The root kit provides the access of victims computer to the criminal even from the remote location as long as the victim remains online.<sup>④</sup> If the rootkit is installed properly, the hacker can use victims computer as if he is using his own computer where he can delete, destroy, modify, copy, rename the files and information without victims knowledge.<sup>⑤</sup> The rootkit program is also called as remote access trojan.

2. Keylogger :-

- ① A keylogger is one of the specific form of a trojan which is used to obtain the personal and sensitive information from the victims computer without his knowledge. A key
- ② logger is a kind of program that records all the key strokes type by the user using the keyboard or keypad.
- ③ i.e. the reason the keylogger is considered as one of the successful tool of password cracking because with the help of keylogger, Any form of password can be created. Irrespective of length and type of password.
- ④ Following are some of the methods which can be used to counter the keylogging attacks these are -
- ① Use of virtual keypad
  - ② Use of OTP



6.

Preventive measures against computer contaminants. (any 5)

- ① Do not visit the unsecure sites.
- ② Do not download pirated softwares or audio/video files.
- ③ Do not use open wifi connections unless you trust them.
- ④ Do not download the unknown attachment.
- ⑤ Do not click all the unknown and suspicious link.
- ⑥ Always scan your computer system frequently & regularly.