Анатомия вирусов.

Биологические вирусы—это очень маленькие, простые организмы, которые поражают живые клетки, известны как носители, прикрепляясь к ним и используя их для собственной репродукции. Часто это приносит вред клеткам-носителям.

Подобно биологическим вирусам, компьютерные вирусы—это маленькие программы, которые заражают компьютерную и используют ресурсы носителя для воссоздания самих себя. Обычно, это происходит путём корректировки операционной системы компьютера, чтобы она могла определять файлы с расширением COM или EXE. Потом, они дублируют свой код в файлы с такими расширениями. Такие действия часто приводят к нанесению ущерба компьютерным системам.

Когда пользователь запускает заражённую программу, она загружается в память содержа вирус. Вирус использует общие программные техники, что б оставаться в памяти. Вирусы могут использовать операцию репродукции, что б заражать другие программы. Этот процесс продолжается до момента, пока компьютер не выключится.

Вирус также может содержать исполняемую часть, которая бездействует до того момента, пока её не активирует триггерное событие, например: нажатие определённой кнопки. Действие может иметь множество форм. Оно может совершать относительно безобидные вещи такие как: отображение сообщений на монитор или более опасные действия—удаление файлов с жёсткого диска.

Когда вирус заражает файл, вирус замещает первую инструкцию патронной программы, инструкцией, которая меняет порядок нормального запуска программы. Этот тип команд известен как JUMP-команды и ведёт к тому, что инструкции вируса запускаются перед инструкциями носителя. Потом, вирус возвращает управление программе-носителю которая в последствии, продолжает работать в нормальном порядке.

Для того, что б называться вирусом, программа обязана иметь только репродуктивную функцию, которая позволяет заражать другие программы. Тем не менее, вирусы имеют 4 основные части. Задача задания неверного направления, что позволяет вирусу скрываться; репродуктивная задача, которая позволяет вирусу копировать самого себя в другие программы; триггер, который запускает задачу в конкретное время, при нажатии конкретных кнопок ил по достижении определённого события, а также исполняемая часть, которая может быть довольно злой, но шуткой либо же крайне разрушительной. Программа, которая имеет исполняемую часть, но не имеет репродуктивной функции называется трояном.

Ex 5

1. Computer viruses infect computer system and uses its resources to replicate itself just like biological viruses replicate itself using host cells. Always harming the cell or the host.
2. Virus copies itself to programs with COM and EXE files, where inserts instructions before beginning of host-program that viruses code runs first. When user runs infected program, virus loads and then does whatever is programmed for.
3. Computer viruses use the same logic as other programs. It should stay resident in memory, that helps it to reproduce itself and infect more and more programs.
4. The writer provides next examples of payload: displaying a message on the monitor, deleting files from hard drive and changing the normal execution settings.
5. Programs, that have file extension COM or EXE are the main aim of virus
6. misdirection hides the presence of the code
7. reproduction attached a copy of itself to another program
8. trigger decides when and how to activate the payload
9. payload does the damage

7) Trojan doesn’t have a reproduction routine. That’s the only difference.

Ex 8

1) Salami Shaving Manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere. The victims are often unaware of the crime because the amount taken from any individual is so small.

2) DoS attack. Swamping a server with large number of requests.

3) Trojan Horse. Adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. In other words, it appears to do something useful but actually does something destructive in the background.

4) Trapdoors. Leaving, within a completed program, an illicit program that allows unauthorised - and unknown - entry.

5) Mail bombing. Inundating an email address with thousands of messages, thereby slowing or even crashing the server

6) Software piracy. Unauthorised copying of a program for sale or distributing to other users

7) Piggybacking. Using another person's identification code or using that person's files before he or she has logged off.

8) Spoofing. Redirecting anyone trying to visit a certain site elsewhere.

9) Defacing. Changing the information shown on another person's website.

10) Hijacking. Tricking a user into revealing confidential information such as an access code or a credit-card number.