Q. What is a virus?

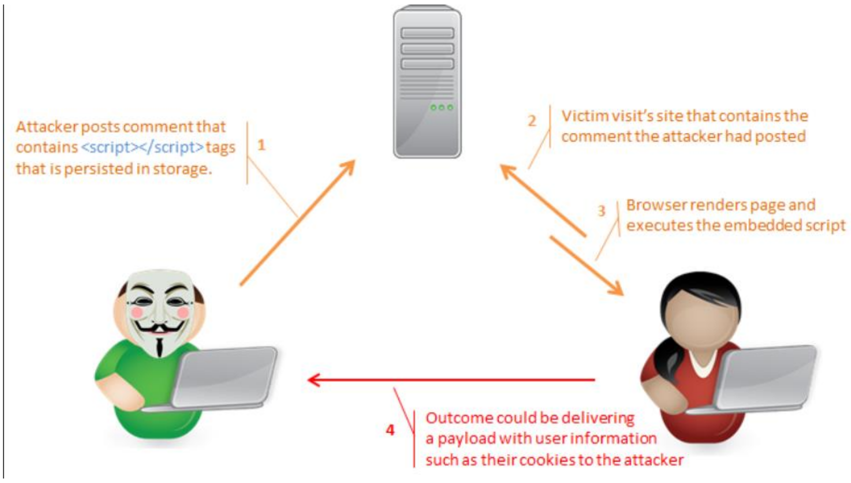
A computer virus is a malicious software program that can be loaded onto a user's computing device without the user's knowledge and performs malicious actions based on its payload. It can self-replicate, inserting itself onto other programs or files, infecting them in the process.

Q. With the aid of a diagram give a detailed account of Cross-Site Scripting.

Cross Site Scripting

• XSS is an attack technique that forces a website to echo attacker-supplied executable code, which then loads in a user's Web browser.

• The user is the intended victim, with the hacker using the vulnerable website as a means of attack.


Attacker posts comment that contains <script></script> tags that is persisted in storage.
1
2
Victim visit's site that contains the comment the attacker had posted
3
Browser renders page and executes the embedded script
4
Outcome could be delivering a payload with user information such as their cookies to the attacker

• XSS exploit code is typically (but not always) written in HTML/JavaScript and does not execute on the server.

• The server is merely the host, while the attack executes within the Web browser.

XSS enables the theft of Web browser cookies, which can then be reused to hijack online user accounts.

➢ Online accounts include Web banks, Web mail, blogs, and any other website feature accessible with a username and password. XSS attacks can take complete control over browser. There are two ways for users to become infected by XSS attacks.

➢ Users are either tricked into clicking on a specially crafted link (Non-Persistent Attack)

➢ Unknowingly attacked by simply visiting a Web page embedded with malicious code (Persistent Attack).

Q. What is obfuscation technique? Give an account of the four virus obfuscation techniques: Encryption, Polymorphism, Metamorphism, Stealth

Obfuscation techniques are those techniques that are used by virus writers to avoid detection and analysis of their specimens (programs).

Examples of different obfuscation techniques ➢ No Obfuscation ➢ Encryption ➢ Polymorphism ➢ Metamorphism ➢ Stealth

No obfuscation ➢ Some of the viruses don’t use any type of obfuscation technology. It is easier to build a virus of this type.

Encryption ➢ This type of viruses use cryptography to hide their functionality. They place a decrypter along with the encrypted body that decrypts the virus on-the-fly.

Polymorphism ➢ These viruses change the look of the virus code every time it infects a new file. The code still has the same functionality but it uses different instructions so it is harder to detect and reverse engineer.

Metamorphism ➢ These viruses change the virus body instead of appearance. This way every specimen looks different and generation of a signature is harder. These techniques are mostly used by macro and script viruses.

Stealth ➢ A stealth virus is a type of virus that tries to remain undiscovered by hiding the infection events from everyone, instead of trying to obfuscate its code. It achieves this by restoring certain original properties of the host file for example, timestamps. It also intercepts system calls to hide any other resulting changes like the increase in the size of the host file.

Q. Name and describe four types of virus payloads (non, non-destructive, destructive, Droppers)

Virus Payloads

Normally when you have been infected by a virus, it leaves a payload behind. There are four different types:

➢ No Payload ➢ Non-Destructive Payload ➢ Destructive Payload ➢ Droppers

No Payload ➢ Some of the viruses present don’t do anything than just infecting the files

Non-destructive ➢ These viruses generally carry a message or a graphic. Some of them just tease the user by controlling hardware like the CD-ROM or speakers. They can be designed to disable certain features like caps lock, special keys. For these viruses, damage is only caused by the non-productivity of the user.

Destructive

➢ Destruction is one of the main motives of attackers.

➢ Viruses with this kind of payloads are decreasing as there is no financial gain except in few situations that involve rival groups or businesses.

➢ In areas where there is a financial gain, more advancement in the virus creation is happening.

➢ The destruction varies according to the virus.

Droppers

➢ Some viruses help the attackers in gathering the resources required for conducting malicious activities like identity theft, DDOS, software license theft and phishing.

➢ Most of the viruses today belong to this category as there is a huge financial gain.

➢ These viruses drop various bots and keyloggers that are used to carry out these malicious activities.

Q.Give an account of any four of the following types of virus (Note that you should be able to explain all) - Boot, File Infector, Macro, Resident, Direct Action, Overwrite,

1. Boot Sector Virus

• A boot infector attacks the critical section of a floppy disk or hard drive that helps to start your computer.

• When the computer starts up, the malicious code is launched by the system and your machine becomes wide open to virus coders.

2. File Infector Virus

• The role of a file infector is to infect the files of a computer.

• This is one of the most frequently deployed viruses and has been known to inflict considerable damage.

3. Macro Virus

• A wide variety of programs provide support for Macros – special actions programmed into the document using a specific macro programming language.

• Some viruses use macros to infect and spread to other systems.

• If the user can be tricked into running the macro(s), the virus can push its macro to the application global macro pool.

3. Resident

• These are permanent viruses dwelling in RAM memory.

• In this case, they would be in a position to overcome, as well as interrupt, all operations that the system executes.

• Their effects include corrupting programs and files that are opened, closed, renamed or copied.

• They get activated every time the OS runs

4. **Direct Action**

• These viruses replicate or take action once they are executed.

• When a certain condition is met, the viruses will act by infecting the files in the directory or the folder specified in the AUTOEXEC.BAT file.

• These viruses are usually found in the hard disk’s root directory, but they keep on changing location.

5. **Overwrite**

• This kind of virus deletes the information contained in the files that it infects, rendering them partially or totally useless once they have been infected.

• The only way to remove an overwrite virus is to delete the file completely.

6. **Directory**

• These are also known as cluster virus or file system virus.

• Directory viruses infect the computer’s directory by changing the path indicating file location.

• Once the program is executed that has been infected it is in fact the virus that is being executed while the original has been moved.

• They are usually located in the disk but affect the entire directory.

7. **Email Virus**

• Due to the increase in use of email, the email virus was developed.

• This is a virus spread via an email.

• Such a virus will hide in an email and when the recipient opens the mail it does it’s work.

8. **Companion**

• Companion viruses are file infector viruses as are resident and direct-action types.

• Companion viruses are so named because once they get into the system they travel with the other files that already exist.

• Companion viruses wait in memory until a program is run or act immediately by making copies of themselves.

9. **FAT**

• These viruses attack the File Allocation Table or FAT, which is a part of a disk used to connect information and is vital for the normal functioning of the computer.

• This type of virus attack prevents access to certain sections of the disk. This virus can result in information loss from individual files or even loss of access to entire directories.

10. Polymorphic Virus

• These viruses change the look of the virus code every time it infects a new file. The code still has the same functionality but it uses different instructions so it is harder to detect and reverse engineer.

• The polymorphic virus is one of the more complex computer threats.

• This is primarily done to elude the detection of a virus scanner as some are not able to identify different instances of an infection.

• One method it commonly uses to bypass a scanner involves self-encryption performed with a variable key.

11. Browser Hijacking

• This type of virus, which can spread itself in numerous ways including voluntary download, effectively hijacks certain browser functions, usually in the form of re-directing the user automatically to particular sites.

• It’s usually assumed that this tactic is designed to increase revenue from web advertisements.

• There are a lot of such viruses, and they usually have “search” included somewhere in their description.

• CoolWebSearch may be the most well known example, but others are nearly as common.

Examples of Virus Types

Virus Type	**Examples**
Boot	Polyboot.B, AntiEXE, pakastani brain
File Infector	W32.Xpaj.B
Macro	Relax, Melissa.A, Bablas, O97M/Y2K
Resident	Randex, CMJ, Meve, and MrKlunky
Direct Action	Vienna
Overwrite	Way, Trj.Reboot, Trivial.88.D
Directory	dir-2
Email	Melissa
Companion	Asimov.1539, stator and terrax.1069
FAT	the link
Multipartite	Flip, invader, tequila
XSS	JS.Fortnight
Browser Hijacker	the cool web search

============end lecture 3 notes==========================