Tools and Methods Used in Cyber line

Phishing:

- Phishing is one type of cyber attack. Phishing got its name from "**phish**" meaning fish. It's a common phenomenon to put bait for the fish to get trapped.
- Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it.
- The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim.

The main motive of the attacker behind phishing is to gain confidential information like

- Password
- Credit card details
- Social security numbers
- Date of birth

The attacker uses this information to further target the user and impersonate the user and cause data theft. The most common type of phishing attack happens through email. Phishing victims are tricked into revealing information that they think should be kept private. The original logo of the email is used to make the user believe that it is indeed the original email. But if we carefully look into the details, we will find that the URL or web address is not authentic.

How Does Phishing Occur?

Below mentioned are the ways through which Phishing generally occurs. Upon using any of the techniques mentioned below, the user can lead to Phishing Attacks.

- **Clicking on an unknown file or attachment:** Here, the attacker deliberately sends a mysterious file to the victim, as the victim opens the file, either malware is injected into his system or it prompts the user to enter confidential data.

- **Using an open or free wifi hotspot:** This is a very simple way to get confidential information from the user by luring him by giving him free **wifi**. The wifi owner can control the user's data without the user knowing it.

- **Responding to social media requests:** This commonly includes social engineering. Accepting unknown friend requests and then, by mistake, leaking secret data are the most common mistake made by naive users.

- **Clicking on unauthenticated links or ads:** Unauthenticated links have been deliberately crafted that lead to a phished website that tricks the user into typing confidential data.

Types of Phishing Attacks:

Email Phishing: The most common type where users are tricked into clicking unverified spam emails and leaking secret data. Hackers impersonate a legitimate identity and send emails to mass victims. Generally, the goal of the attacker is to get personal details like bank details, credit card numbers, user IDs, and passwords of any online shopping website, installing malware, etc. After getting the personal information, they use this information to steal money from the user's account or harm the target system, etc.

Vishing: Vishing is also known as voice phishing. In this method, the attacker calls the victim using modern caller id spoofing to convince the victim that the call is from a trusted source. Attackers also use IVR to make it difficult for legal authorities to trace the attacker. It is generally used to steal credit card numbers or confidential data from the victim.

Clone Phishing: Clone Phishing this type of phishing attack, the attacker copies the email messages that were sent from a trusted source and then alters the information by adding a link that redirects the victim to a malicious or fake website. Now the attacker sends this mail to a larger number of users and then waits to watch who clicks on the attachment that was sent in the email. It spreads through the contacts of the user who has clicked on the attachment.

Pharming: In pharming attacks, hackers buy domain names adjacent to popular websites like www.gogle.com or www.facebuk.com, hoping that a target will type such a URL in a hurry. When they reach the website, they see an identical web page to the original, submitting their login credentials without cross-checking the address.

Smishing: In this type of phishing attack, the medium of phishing attack is SMS. Smishing works similarly to email phishing. SMS texts are sent to victims containing links to phished websites or invite the victims to call a phone number or to contact the sender using the given email. The victim is then invited to enter their personal information like bank details, credit card information, user id/ password, etc.

Working

Phase 1: A malicious hacker sends an email or a message to the target, acting as a reputed source. More often than not, it asks the target to follow a third-party link for a security inspection or a simple feature update.

Phase 2: The target thinks the email came from the mentioned sender, be it a bank or a company, and follows the malicious link to a counterfeit web page designed to look as similar as possible to an authentic website.

Phase 3: On the fake website, the user is asked to submit some private information, like account credentials for a specific website. Once the details are submitted, all the information is sent to the hacker who designed the website and malicious email.

Phase 4: On receiving the account credentials, the hacker is free to use them by logging in or selling consequent information retrieved on the internet to the highest bidder.

🎻 How To Stay Protected Against Phishing?

Until now, we have seen how a user becomes so vulnerable due to phishing. But with proper precautions, one can avoid such scams. Below are the ways listed to protect users against phishing attacks:

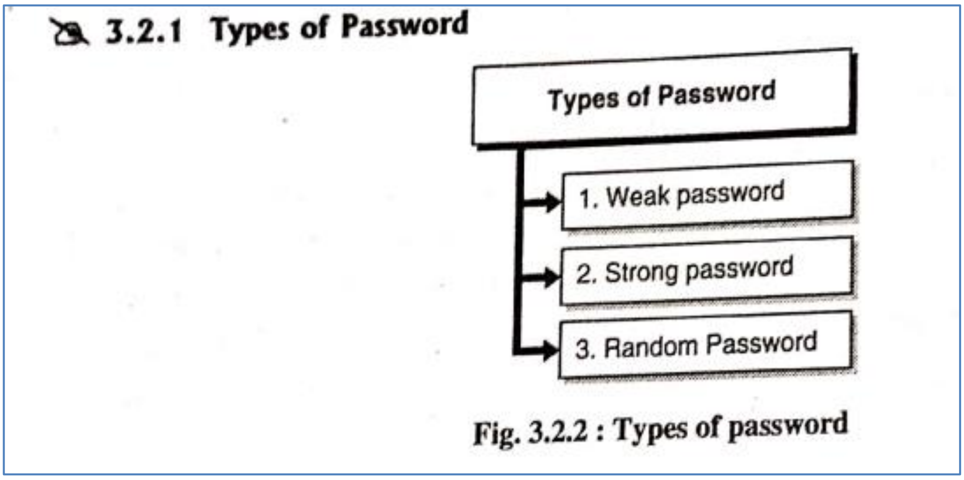
- **Authorized Source:** Download software from authorized sources only where you have trust.
- **Confidentiality:** Never share your private details with unknown links and keep your data safe from hackers.
- **Check URL:** Always check the URL of websites to prevent any such attack. it will help you not get trapped in Phishing Attacks.
- **Avoid replying to suspicious things:** If you receive an email from a known source but that email looks suspicious, then contact the source with a new email rather than using the reply option.
- **Phishing Detection Tool:** Use phishing-detecting tools to monitor the websites that are crafted and contain unauthentic content.
- **Try to avoid free wifi:** Avoid using free Wifi, it will lead to threats and Phishing.
- **Keep your system updated:** It's better to keep your system always updated to protect from different types of Phishing Attacks.

Password Cracking

Password cracking is a process used by attackers to gain unauthorized access to computer systems or user accounts by attempting to decipher passwords.

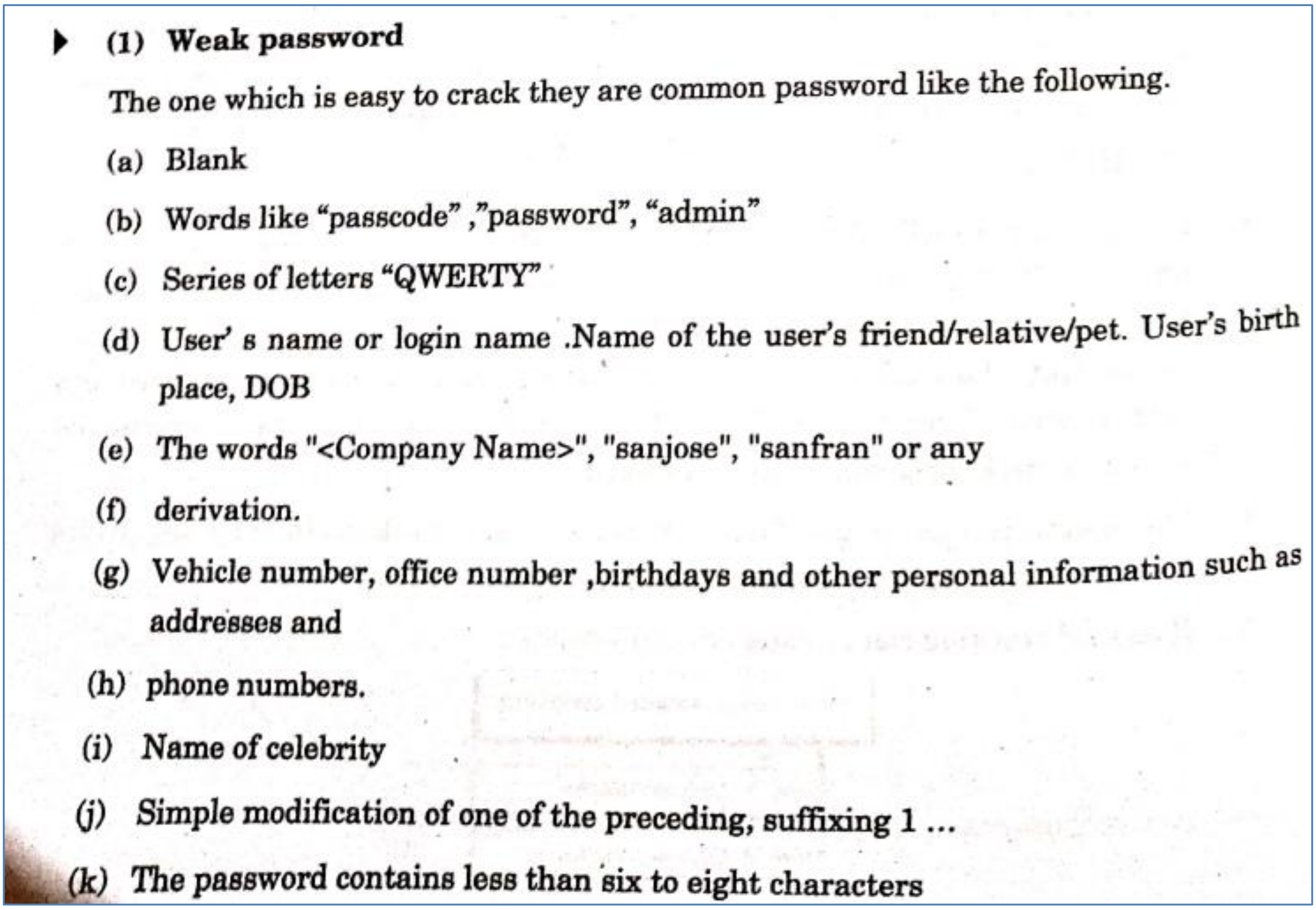
The goal is to discover the correct password through various techniques, allowing the attacker to impersonate a legitimate user.

Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it’s an art of obtaining the correct password that gives access to a system protected by an authentication method.



3.2.1 Types of Password

Fig. 3.2.2 : Types of password



(1) Weak password

The one which is easy to crack they are common password like the following.

(a) Blank

(b) Words like “passcode” ,”password”, “admin”

(c) Series of letters “QWERTY”

(d) User’ s name or login name .Name of the user’s friend/relative/pet. User’s birth place, DOB

(e) The words "<Company Name>", "sanjose", "sanfran" or any

(f) derivation.

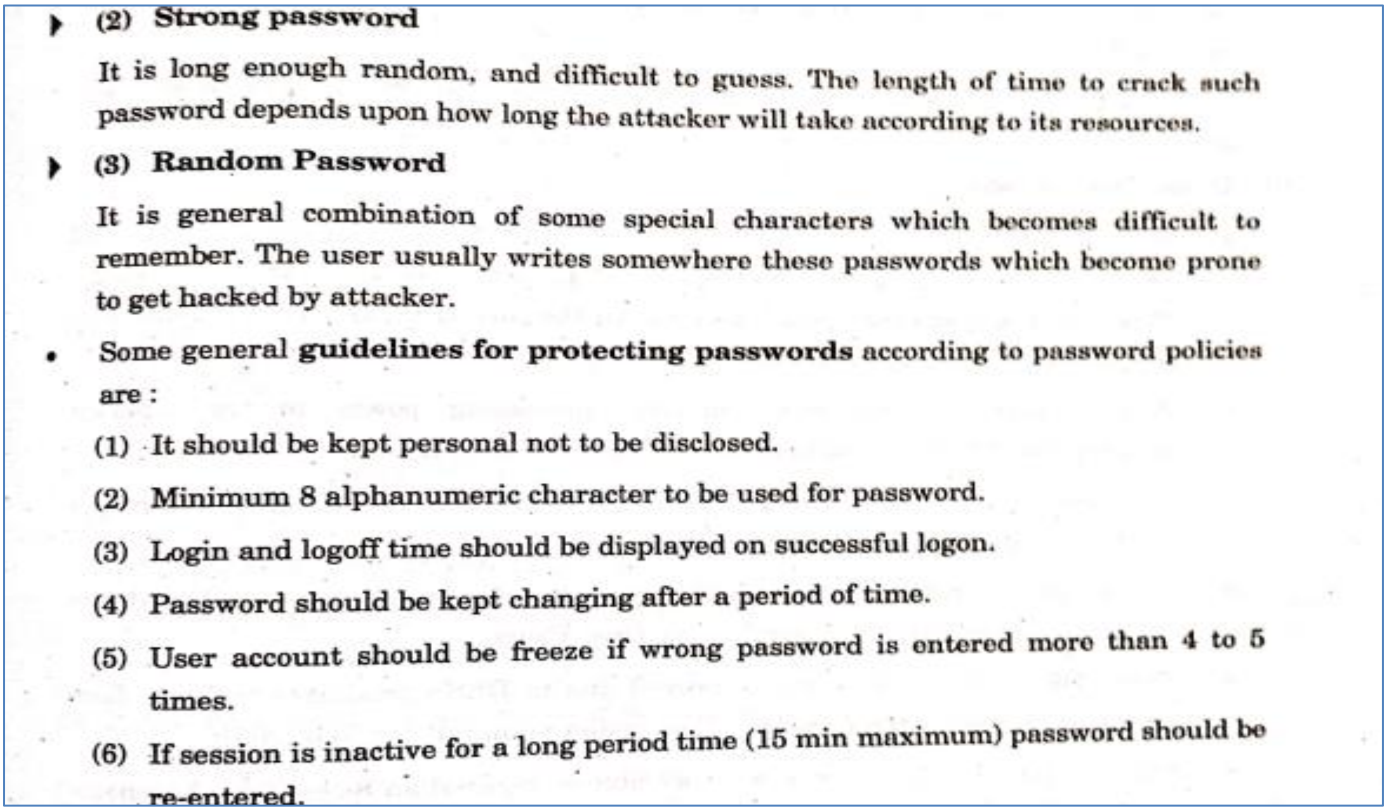
(g) Vehicle number, office number ,birthdays and other personal information such as addresses and

(h) phone numbers.

(i) Name of celebrity

(j) Simple modification of one of the preceding, suffixing 1 ...

(k) The password contains less than six to eight characters



- **(2) Strong password**

  It is long enough random, and difficult to guess. The length of time to crack such password depends upon how long the attacker will take according to its resources.

- **(3) Random Password**

  It is general combination of some special characters which becomes difficult to remember. The user usually writes somewhere these passwords which become prone to get hacked by attacker.

- Some general **guidelines for protecting passwords** according to password policies are :

  (1) It should be kept personal not to be disclosed.

  (2) Minimum 8 alphanumeric character to be used for password.

  (3) Login and logoff time should be displayed on successful logon.

  (4) Password should be kept changing after a period of time.

  (5) User account should be freeze if wrong password is entered more than 4 to 5 times.

  (6) If session is inactive for a long period time (15 min maximum) password should be re-entered.

Password cracking techniques

- **Dictionary attack**– This method involves the use of a wordlist to compare against user passwords.
- **Brute force attack**– This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value “password” can also be tried as p@$$word using the brute force attack.
- **Rainbow table attack**– This method uses pre-computed hashes. Let’s assume that we have a database which stores passwords as md5 hashes. We can create another database that has md5 hashes of commonly used passwords. We can then compare the password hash we have against the stored hashes in the database. If a match is found, then we have the password.
- **Guess**– As the name suggests, this method involves guessing. Passwords such as qwerty, password, admin, etc. are commonly used or set as default passwords. If they have not been changed or if the user is careless when selecting passwords, then they can be easily compromised.
- **Spidering**– Most organizations use passwords that contain company information. This information can be found on company websites, social media such as facebook, twitter, etc. Spidering gathers information from these sources to come up with word lists. The word list is then used to perform dictionary and brute force attacks.

Strong password :

- **Contain both upper and lower case characters (e.g., a-z, A-Z)**
- **Have digits and punctuation characters as well as letters e.g., 0-9, @#$%^&*()_+|~-=\`{}[]:";'<>?,./)**
- **Are at least eight alphanumeric characters long.**
- **Are not a word in any language, slang, dialect, jargon, etc.**
- **Are not based on personal information, names of family, etc.**
- **Passwords should never be written down or stored on-line.**
- **Try to create passwords that can be easily remembered.**
- **One way to do this is create a password based on a song title, affirmation, or other phrase.**
- **For example, the phrase might be: "This May Be One Way To Remember"**
- **and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.**

Password cracker Tools:

John the Ripper

John the Ripper uses the command prompt to crack passwords. This makes it suitable for advanced users who are comfortable working with commands. It uses to wordlist to crack passwords. The program is free, but the word list has to be bought. It has free alternative word lists that you can use. Visit the product website https://www.openwall.com/john/ for more information and how to use it.

Ophcrack

Ophcrack is a cross-platform Windows password cracker that uses rainbow tables to crack passwords. It runs on Windows, Linux and Mac OS. It also has a module for brute force attacks among other features. Visit the product website https://ophcrack.sourceforge.io/ for more information and how to use it.

Cain & Abel

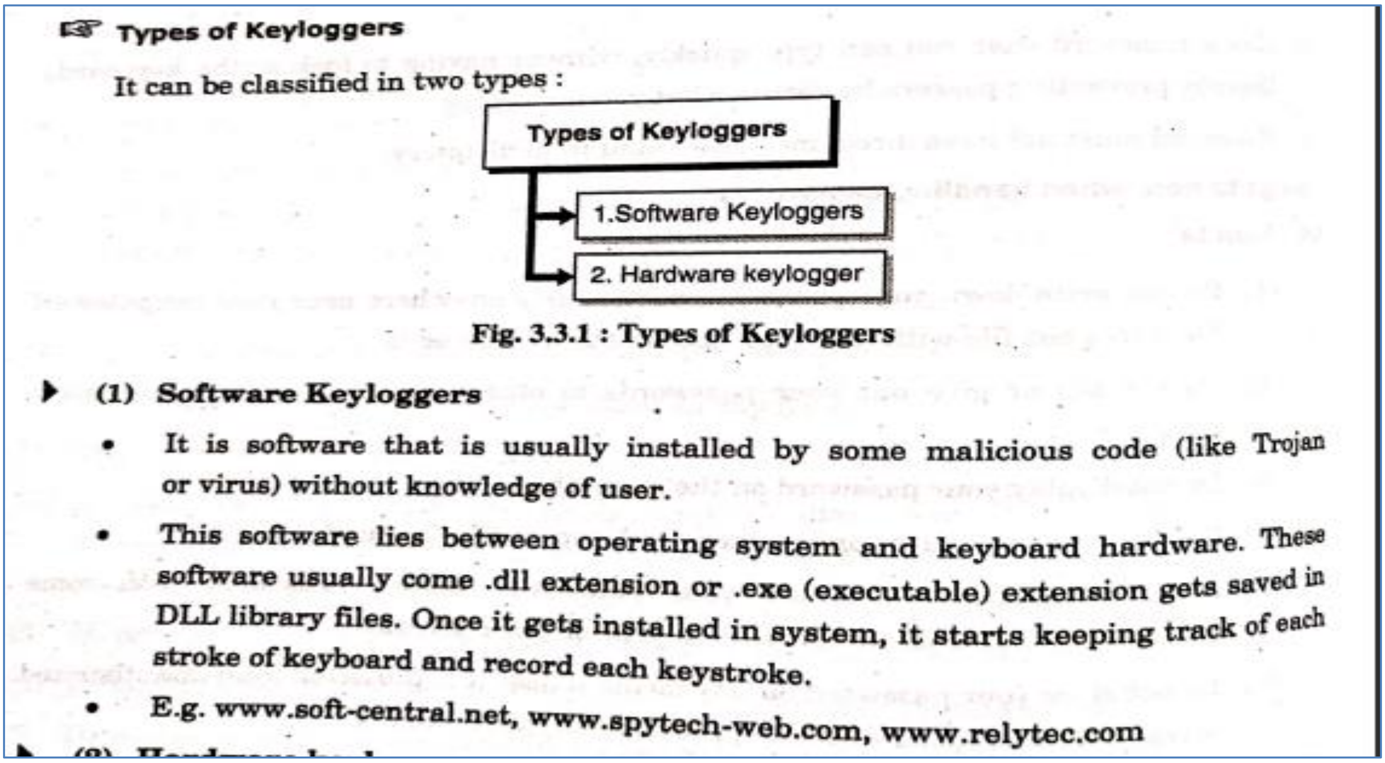
Cain & Abel runs on windows. It is used to recover passwords for user accounts, recovery of Microsoft Access passwords; networking sniffing, etc. Unlike John the Ripper, Cain & Abel uses a graphic user interface. It is very common among newbies and script kiddies because of its simplicity of use. Visit the product website https://sectools.org/tool/cain/ for more information and how to use it.

Key loggers and Spywares:

Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware.

Key logger can be software or can be hardware.

Working: Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.



Types of Keyloggers

It can be classified in two types :

Types of Keyloggers

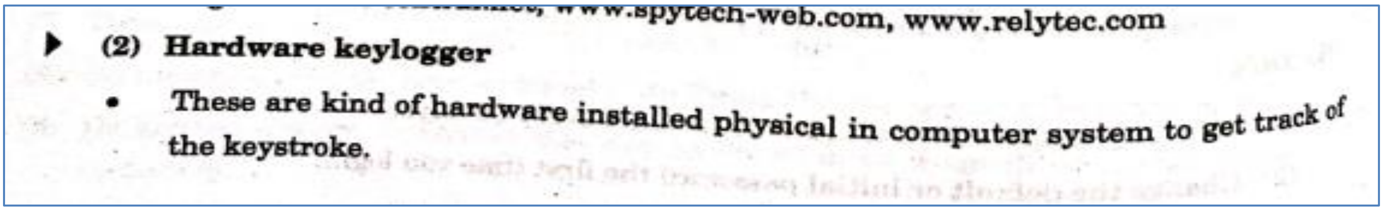
1.Software Keyloggers

2. Hardware keylogger

Fig. 3.3.1 : Types of Keyloggers

▶ **(1) Software Keyloggers**

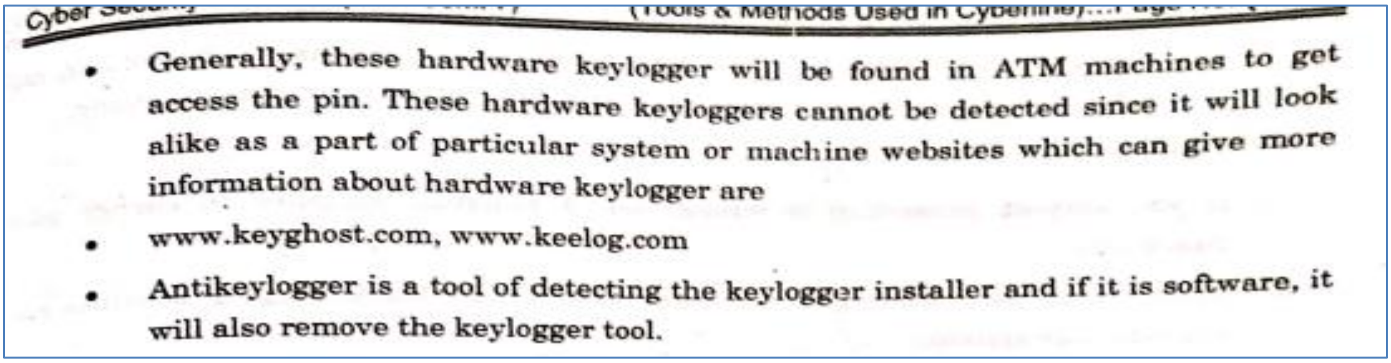
- It is software that is usually installed by some malicious code (like Trojan or virus) without knowledge of user.
- This software lies between operating system and keyboard hardware. These software usually come .dll extension or .exe (executable) extension gets saved in DLL library files. Once it gets installed in system, it starts keeping track of each stroke of keyboard and record each keystroke.
- E.g. www.soft-central.net, www.spytech-web.com, www.relytec.com



www.spytech-web.com, www.relytec.com

▶ **(2) Hardware keylogger**

- These are kind of hardware installed physical in computer system to get track of the keystroke.

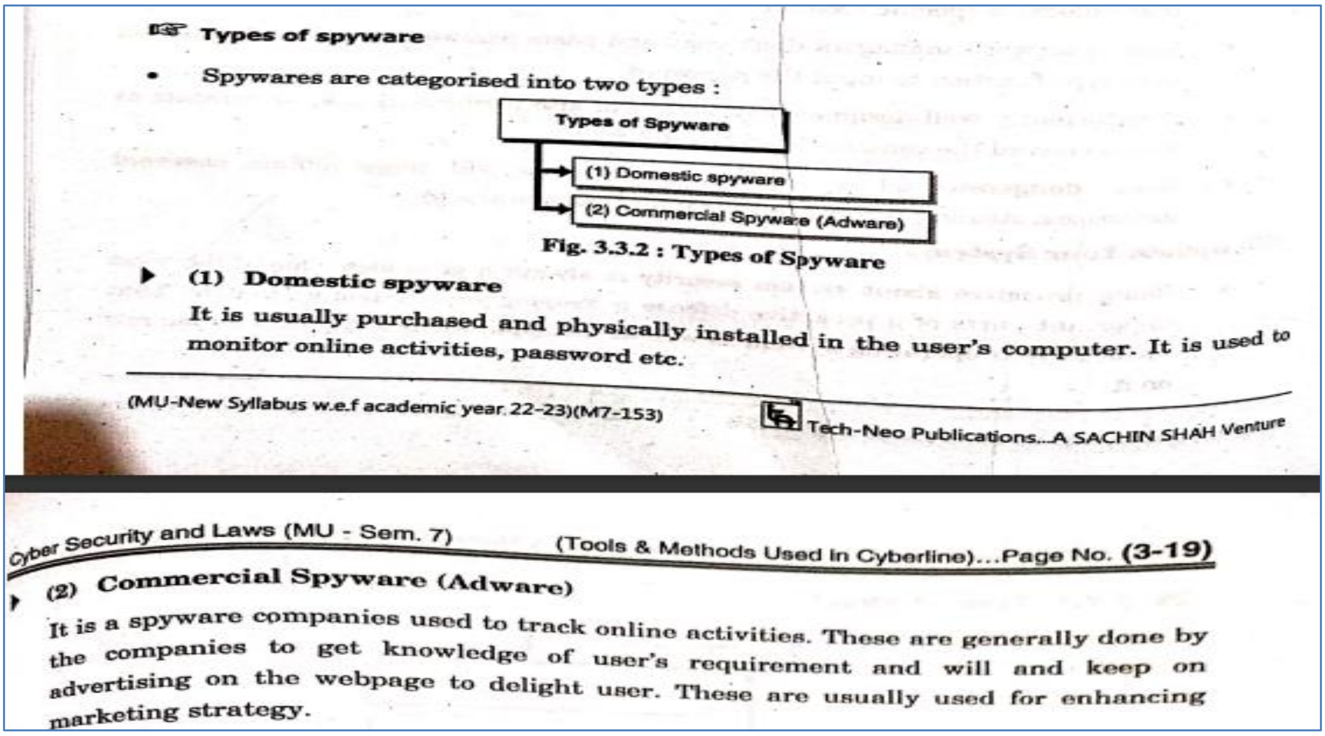


Cyber Secu... (Tools & Methods Used in Cyberline)...

- Generally, these hardware keylogger will be found in ATM machines to get access the pin. These hardware keyloggers cannot be detected since it will look alike as a part of particular system or machine websites which can give more information about hardware keylogger are
- www.keyghost.com, www.keelog.com
- Antikeylogger is a tool of detecting the keylogger installer and if it is software, it will also remove the keylogger tool.

🗝 **Prevention from key-loggers**:

1. **Anti-Key-logger –** As the name suggest these are the software which are anti / against key loggers and main task is to detect key-logger from a computer system.
2. **Anti-Virus –** Many anti-virus software also detect key loggers and delete them from the computer system. These are software anti-software so these can not get rid from the hardware key-loggers.
3. **Automatic form filler –** This technique can be used by the user to not fill forms on regular bases instead use automatic form filler which will give a shield against key-loggers as keys will not be pressed .
4. **One-Time-Passwords –** Using OTP's as password may be safe as every time we login we have to use a new password.
5. **Patterns or mouse-recognition –** On android devices used pattern as a password of applications and on PC use mouse recognition, mouse program uses mouse gestures instead of stylus.



☞ **Types of spyware**

- Spywares are categorised into two types :

Types of Spyware
(1) Domestic spyware
(2) Commercial Spyware (Adware)

Fig. 3.3.2 : Types of Spyware

▶ **(1) Domestic spyware**

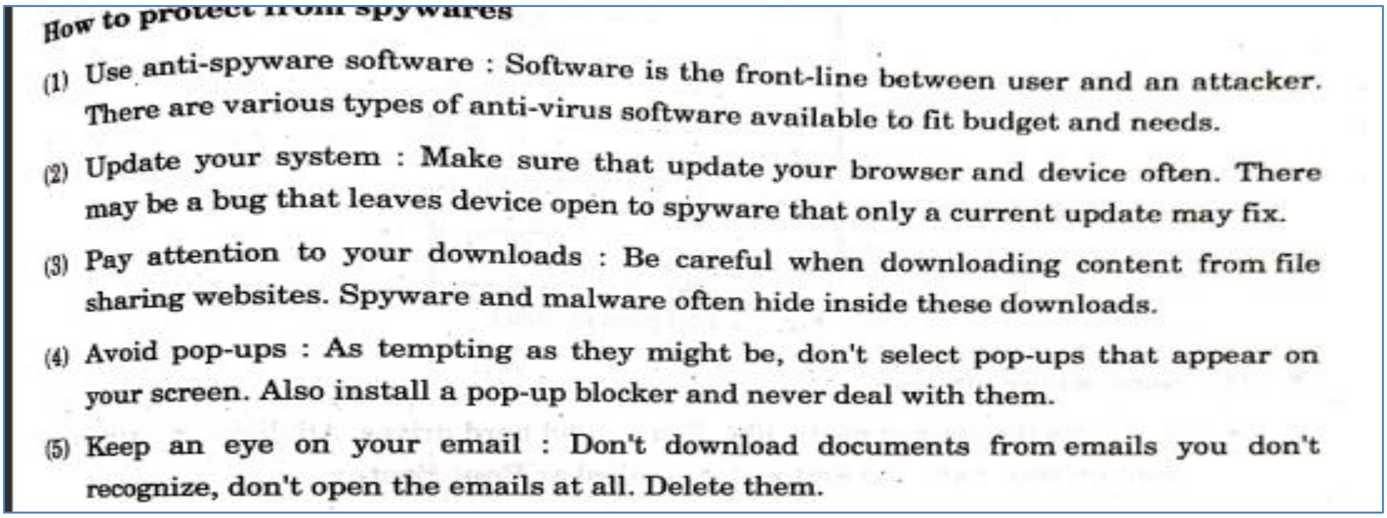
It is usually purchased and physically installed in the user's computer. It is used to monitor online activities, password etc.

(MU-New Syllabus w.e.f academic year 22-23)(M7-153) Tech-Neo Publications...A SACHIN SHAH Venture

Cyber Security and Laws (MU - Sem. 7) (Tools & Methods Used in Cyberline)...Page No. (3-19)

▶ **(2) Commercial Spyware (Adware)**

It is a spyware companies used to track online activities. These are generally done by the companies to get knowledge of user's requirement and will and keep on advertising on the webpage to delight user. These are usually used for enhancing marketing strategy.



How to protect from spywares

(1) Use anti-spyware software : Software is the front-line between user and an attacker. There are various types of anti-virus software available to fit budget and needs.

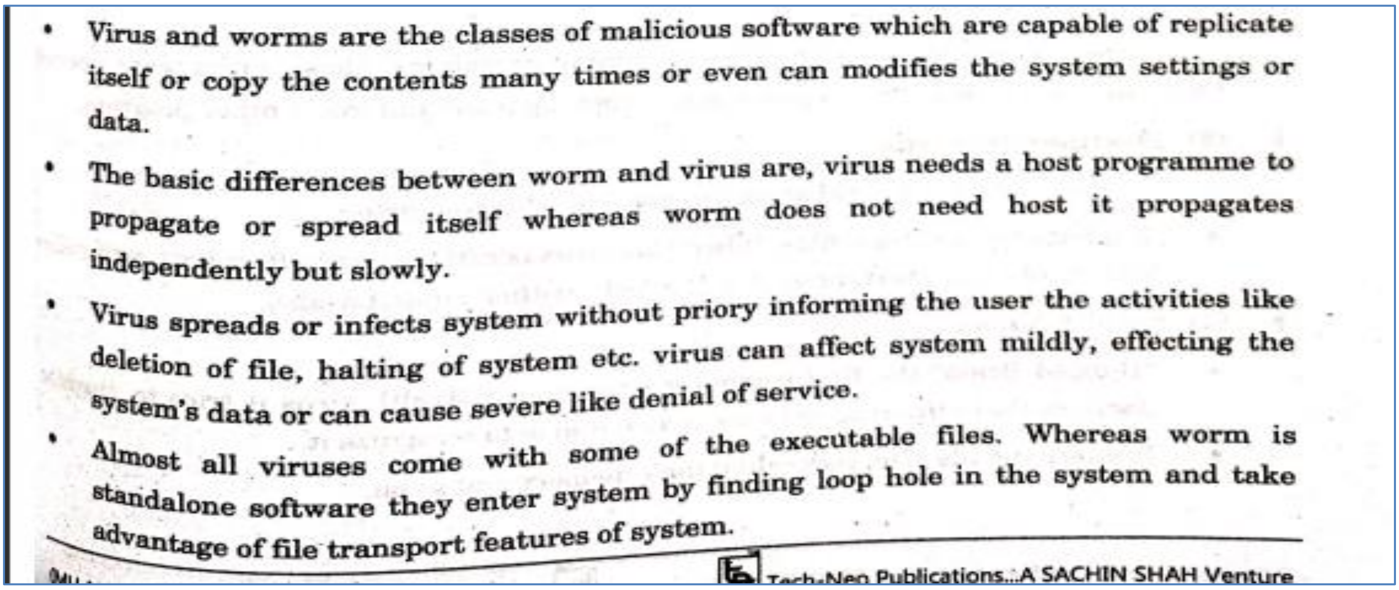
(2) Update your system : Make sure that update your browser and device often. There may be a bug that leaves device open to spyware that only a current update may fix.

(3) Pay attention to your downloads : Be careful when downloading content from file sharing websites. Spyware and malware often hide inside these downloads.

(4) Avoid pop-ups : As tempting as they might be, don't select pop-ups that appear on your screen. Also install a pop-up blocker and never deal with them.

(5) Keep an eye on your email : Don't download documents from emails you don't recognize, don't open the emails at all. Delete them.

😈Virus and Worms:



- Virus and worms are the classes of malicious software which are capable of replicate itself or copy the contents many times or even can modifies the system settings or data.
- The basic differences between worm and virus are, virus needs a host programme to propagate or spread itself whereas worm does not need host it propagates independently but slowly.
- Virus spreads or infects system without priory informing the user the activities like deletion of file, halting of system etc. virus can affect system mildly, effecting the system's data or can cause severe like denial of service.
- Almost all viruses come with some of the executable files. Whereas worm is standalone software they enter system by finding loop hole in the system and take advantage of file transport features of system.

Tech-Neo Publications...A SACHIN SHAH Venture

⚾Various types of viruses:

Boot sector Virus:

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory viruses** as they do not infect the file systems.

Macro Virus:

Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Polymorphic Virus:

A **virus signature** is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus:

In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then execute.

Memory Resident Virus:

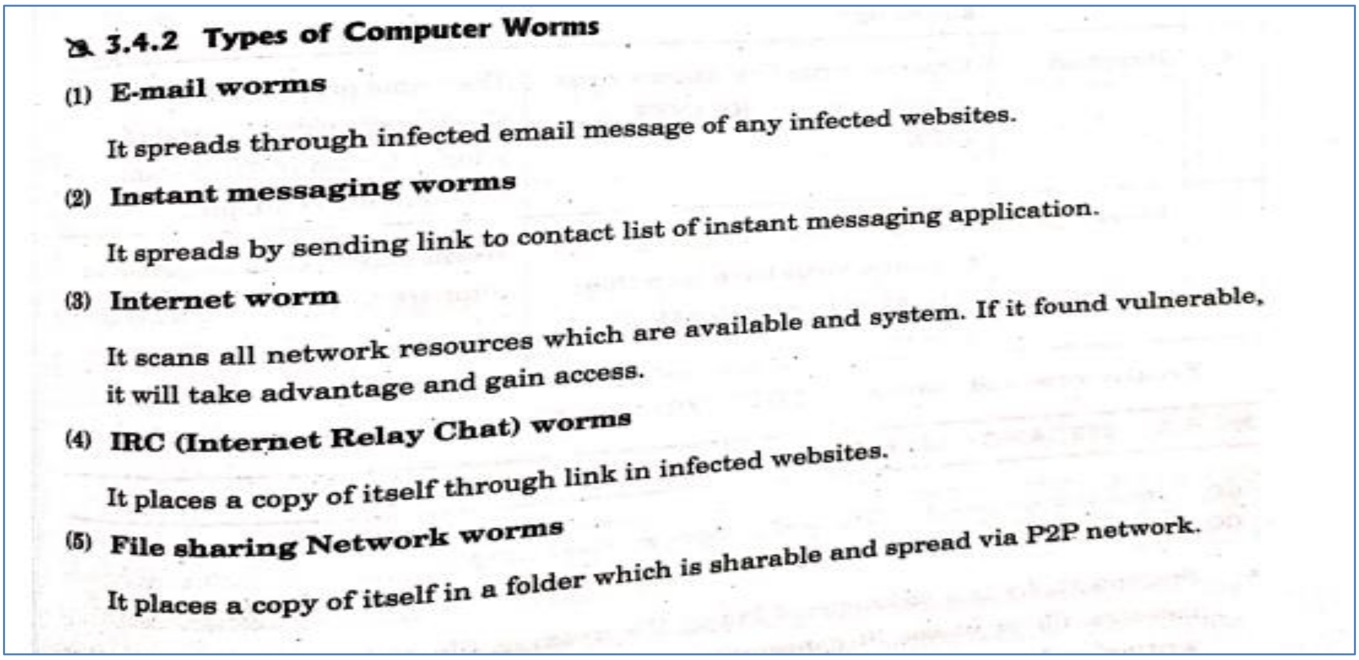
Resident viruses installation store for your RAM and meddle together along with your device operations. They behave in a very secret and dishonest way that they can even connect themselves for the anti-virus software program files.

Multipartite Virus:

This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

Directory Virus:

This virus is also called called File System Virus or Cluster Virus. It infects the directory of the computer by modifying the path that is indicating the location of a file.



3.4.2 Types of Computer Worms

(1) **E-mail worms**

It spreads through infected email message of any infected websites.

(2) **Instant messaging worms**

It spreads by sending link to contact list of instant messaging application.

(3) **Internet worm**

It scans all network resources which are available and system. If it found vulnerable, it will take advantage and gain access.

(4) **IRC (Internet Relay Chat) worms**

It places a copy of itself through link in infected websites.

(5) **File sharing Network worms**

It places a copy of itself in a folder which is sharable and spread via P2P network.

Ex.

The following list of computer viruses are some examples of computer virus:

- Worm

A computer **worm** is a type of trojan horse malware that, unlike traditional viruses, does not require the user's intervention to spread from device to device. After breaching a system, it can spread from one computer to another without human intervention.

- ILOVEYOU

The **ILOVEYOU** virus is an overwrite virus. This virus disguised itself as a love letter from one of its victims' contacts and spread via email.

It was the most damaging malware event of all time when it occurred in 2000. In just about 10 days, it reached an estimated 45 million users and caused $10 billion in damages.

- SQL Slammer

Sr.No.	Basis of Comparison	WORMS	VIRUS
1.	Definition	A Worm is a form of malware that replicates itself and can spread to different computers via Network.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.
2.	Objective	The main objective of worms is to eat the system resources. It consumes system resources such as memory and bandwidth and made the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
3.	Host	It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.
4.	Harmful	It is less harmful as compared.	It is more harmful.
5.	Detection and Protection	Worms can be detected and removed by the Antivirus and firewall.	Antivirus software is used for protection against viruses.
6.	Controlled by	Worms can be controlled by remote.	Viruses can't be controlled by remote.
7.	Execution	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
8.	Comes from	Worms generally comes from the downloaded files or through a network connection.	Viruses generally comes from the shared or downloaded files.
9.	Symptoms	• Hampering computer performance by slowing down it • Automatic opening and running of programs • Sending of emails without your knowledge • Affected the performance of web browser • Error messages concerning to system and operating system	• Pop-up windows linking to malicious websites • Hampering computer performance by slowing down it • After booting, starting of unknown programs. • Passwords get changed without your knowledge

10.	**Prevention**	• **Keep your operating system and system in updated state** • **Avoid clicking on links from untrusted or unknown websites** • **Avoid opening emails from unknown sources** • **Use antivirus software and a firewall**	• **Installation of Antivirus software** • **Never open email attachments** • **Avoid usage of pirated software** • **Keep your operating system updated** • **Keep your browser updated as old versions are vulnerable to linking to malicious websites**
11.	**Types**	**Internet worms, Instant messaging worms, Email worms, File sharing worms, Internet relay chat (IRC) worms are different types of worms.**	**Boot sector virus, Direct Action virus, Polymorphic virus, Macro virus, Overwrite virus, File Infector virus are different types of viruses**
12.	**Examples**	**Examples of worms include Morris worm, storm worm, etc.**	**Examples of viruses include Creeper, Blaster, Slammer, etc.**
13.	**Interface**	**It does not need human action to replicate.**	**It needs human action to replicate.**
14.	**Speed**	**Its spreading speed is faster.**	**Its spreading speed is slower as compared to worms.**

Steganography:

The word Steganography is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’.

Steganography is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

- Steganography can make use of any medium to hide messages
- Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

The various terms used to describe image steganography include:

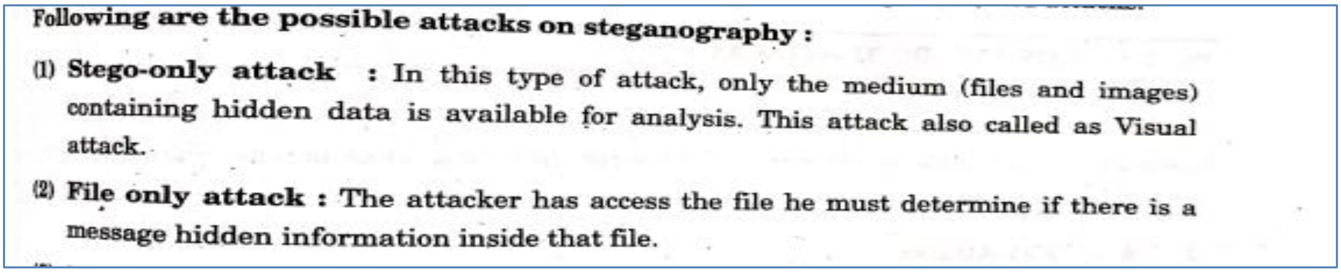
- **Cover-Image** - Unique picture that can conceal data.
- **Message** - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- **Stego-Image** – A stego image is an image with a hidden message.
- **Stego-Key** - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

- **Audio Steganography** – It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.
- **Video Steganography** – Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme.

Steganography Examples

Steganography uses careful techniques to hide the fact that a certain content exists. There are several creative ways to execute it, and it can be used with a variety of latest technologies. Here are a few examples:

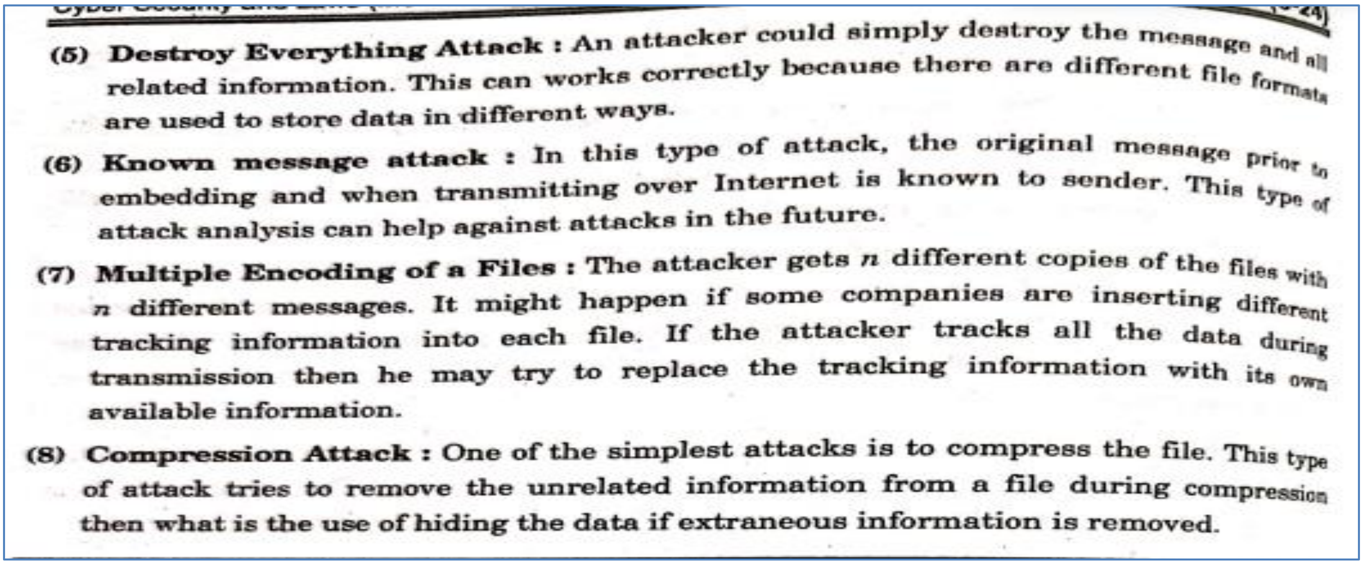
- A hidden message that can be revealed by playing a video at a faster frame rate
- Content that can be unveiled by playing an audio track backward
- Embedding a message into an RGB image by hiding it in the red, green, or blue channel
- Adding noise or sound to encrypt a message within a photo
- Hiding content within the file header or metadata.



Following are the possible attacks on steganography :

(1) **Stego-only attack** : In this type of attack, only the medium (files and images) containing hidden data is available for analysis. This attack also called as Visual attack.

(2) **File only attack** : The attacker has access the file he must determine if there is a message hidden information inside that file.



(5) **Destroy Everything Attack** : An attacker could simply destroy the message and all related information. This can works correctly because there are different file formats are used to store data in different ways.

(6) **Known message attack** : In this type of attack, the original message prior to embedding and when transmitting over Internet is known to sender. This type of attack analysis can help against attacks in the future.

(7) **Multiple Encoding of a Files** : The attacker gets *n* different copies of the files with *n* different messages. It might happen if some companies are inserting different tracking information into each file. If the attacker tracks all the data during transmission then he may try to replace the tracking information with its own available information.

(8) **Compression Attack** : One of the simplest attacks is to compress the file. This type of attack tries to remove the unrelated information from a file during compression then what is the use of hiding the data if extraneous information is removed.

Advantages of Steganography

- Unlike other methods, steganography has the added benefit of hiding communications so well that they receive no attention. However, in countries where encryption is illegal, sending an encrypted message that you can easily decipher will raise suspicion and may be risky.
- Steganography is a form of encryption that protects the information within a message and the connections between sender and receiver.
- The three essential elements of steganography—security, capacity, and robustness—make it worthwhile to covert information transfer via text files and develop covert communication channels.
- You can store an encrypted copy of a file containing sensitive information on the server without fear of unauthorized parties gaining access to the data.

- Government and law enforcement agencies can communicate secretly with the help of steganography corporations.

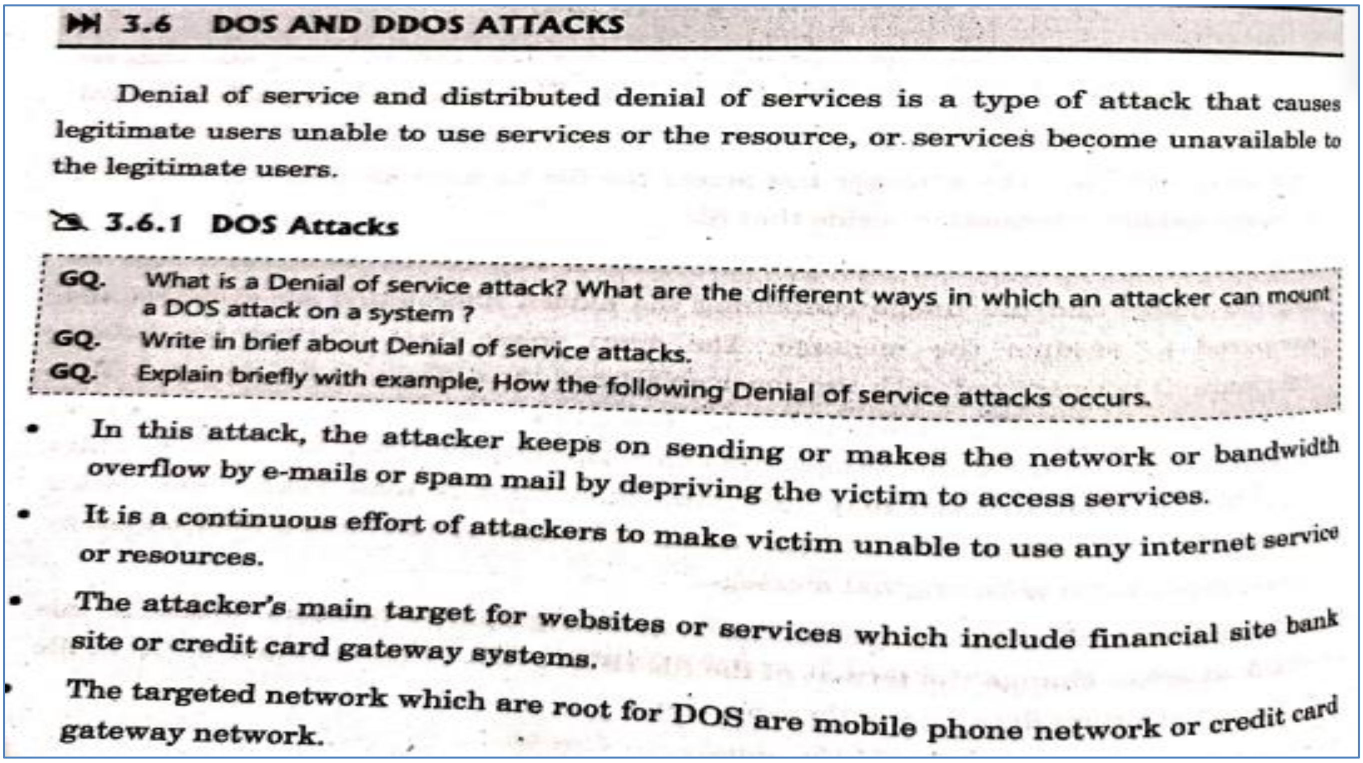
Steganography Tools

Various tools or software that support steganography are now readily accessible. Though most hide information, some provide additional security by encrypting it beforehand. You can find the following free steganography resources online:

- **Steghide**: Steghide is a free tool that uses steganography to conceal information in other files, such as media or text.
- **Stegosuite**: It is a Java-based, free steganography tool. Stegosuite makes it simple to obfuscate data in pictures for covert purposes.
- **OpenPuff**: It is a high-quality steganographic tool that allows you to conceal data in other media types like images, videos, and Flash animations.
- **Xiao Steganography**: To conceal information in BMP images or WAV files, use the free Xiao Steganography tool.
- **SSuite Picsel**: The free portable program SSuite Picsel is yet another option for hiding text within an image file; however, it uses a somewhat different method than other programs.

DoS and DDoS Attacks:

1. DOS Attack is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large number of traffic to it.



3.6 DOS AND DDOS ATTACKS

Denial of service and distributed denial of services is a type of attack that causes legitimate users unable to use services or the resource, or services become unavailable to the legitimate users.

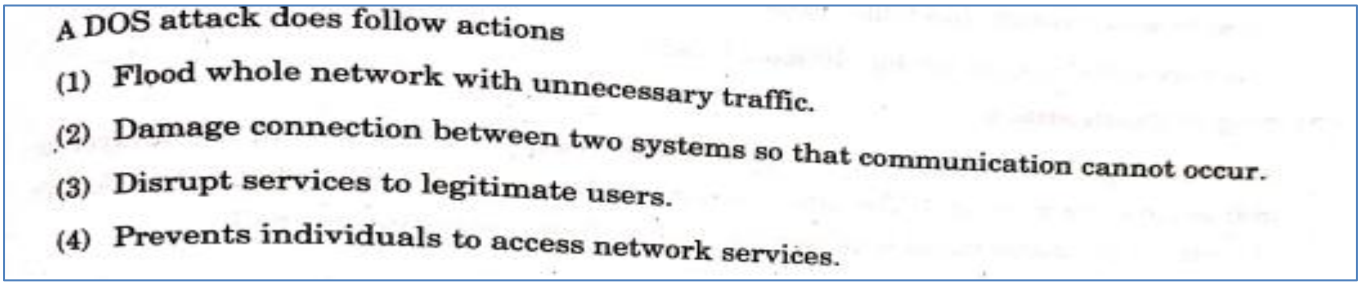
3.6.1 DOS Attacks

GQ. What is a Denial of service attack? What are the different ways in which an attacker can mount a DOS attack on a system ?

GQ. Write in brief about Denial of service attacks.

GQ. Explain briefly with example, How the following Denial of service attacks occurs.

- In this attack, the attacker keeps on sending or makes the network or bandwidth overflow by e-mails or spam mail by depriving the victim to access services.
- It is a continuous effort of attackers to make victim unable to use any internet service or resources.
- The attacker's main target for websites or services which include financial site bank site or credit card gateway systems.
- The targeted network which are root for DOS are mobile phone network or credit card gateway network.



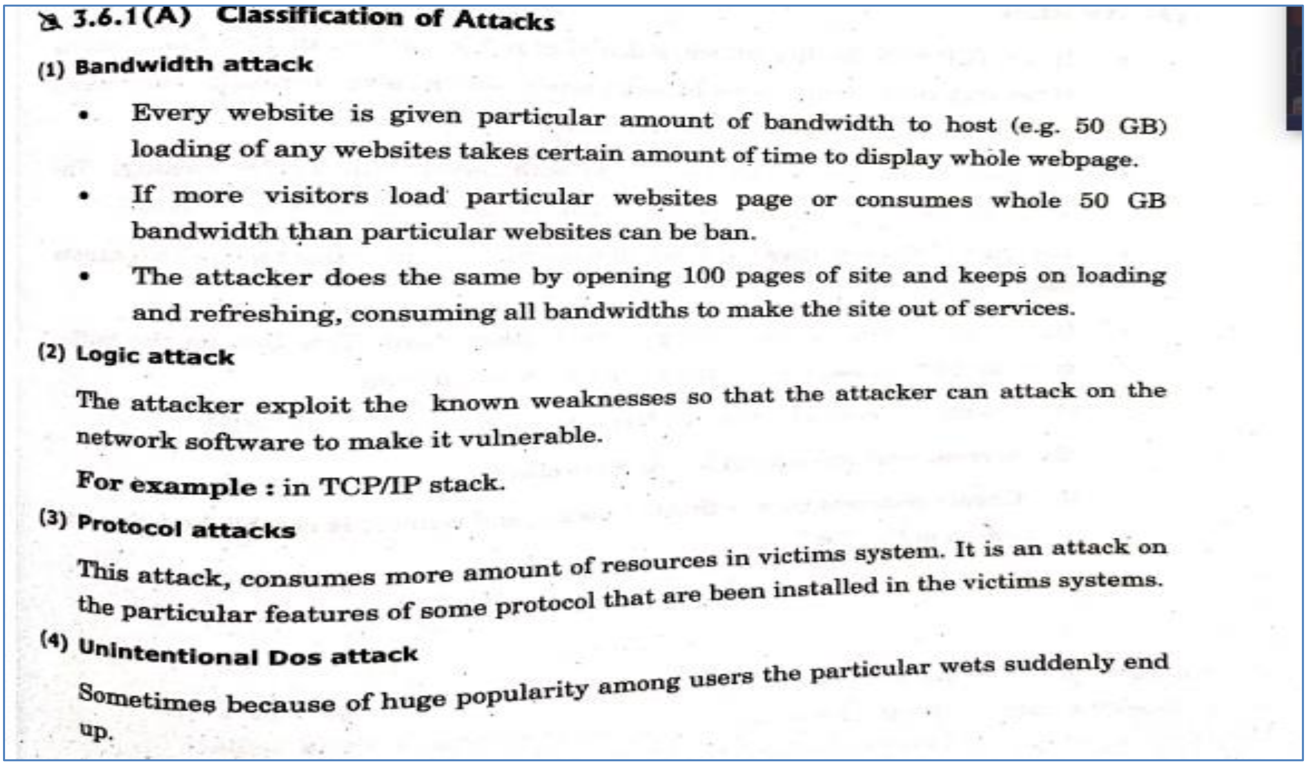
A DOS attack does follow actions

(1) Flood whole network with unnecessary traffic.

(2) Damage connection between two systems so that communication cannot occur.

(3) Disrupt services to legitimate users.

(4) Prevents individuals to access network services.



3.6.1(A) Classification of Attacks

(1) Bandwidth attack

- Every website is given particular amount of bandwidth to host (e.g. 50 GB) loading of any websites takes certain amount of time to display whole webpage.
- If more visitors load particular websites page or consumes whole 50 GB bandwidth than particular websites can be ban.
- The attacker does the same by opening 100 pages of site and keeps on loading and refreshing, consuming all bandwidths to make the site out of services.

(2) Logic attack

The attacker exploit the known weaknesses so that the attacker can attack on the network software to make it vulnerable.

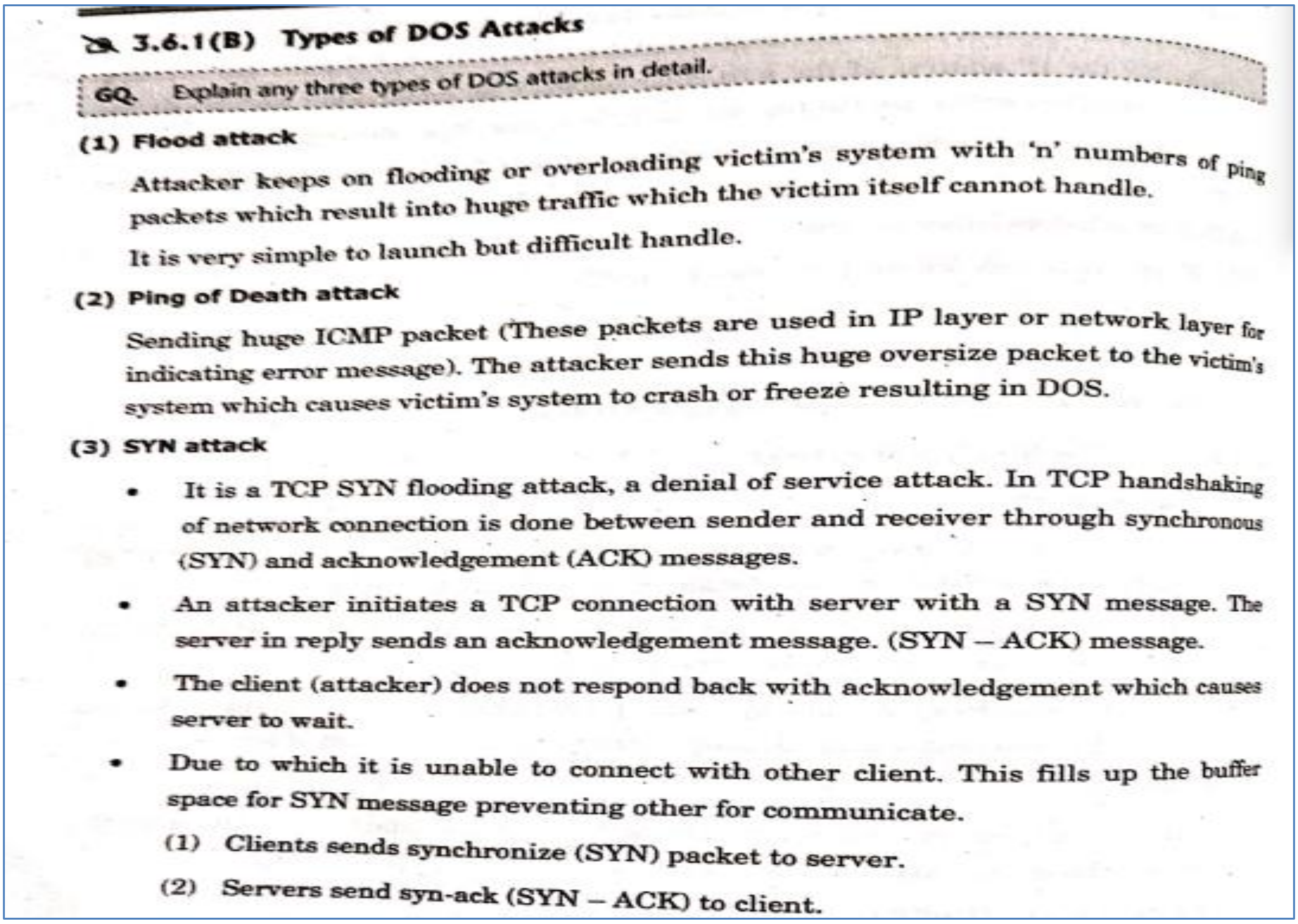
For example : in TCP/IP stack.

(3) Protocol attacks

This attack, consumes more amount of resources in victims system. It is an attack on the particular features of some protocol that are been installed in the victims systems.

(4) Unintentional Dos attack

Sometimes because of huge popularity among users the particular wets suddenly end up.



3.6.1(B) Types of DOS Attacks

GQ. Explain any three types of DOS attacks in detail.

(1) Flood attack

Attacker keeps on flooding or overloading victim's system with 'n' numbers of ping packets which result into huge traffic which the victim itself cannot handle.

It is very simple to launch but difficult handle.

(2) Ping of Death attack

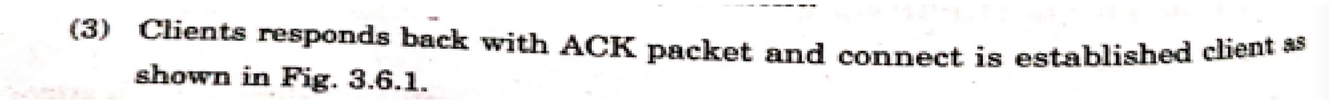
Sending huge ICMP packet (These packets are used in IP layer or network layer for indicating error message). The attacker sends this huge oversize packet to the victim's system which causes victim's system to crash or freeze resulting in DOS.

(3) SYN attack

- It is a TCP SYN flooding attack, a denial of service attack. In TCP handshaking of network connection is done between sender and receiver through synchronous (SYN) and acknowledgement (ACK) messages.
- An attacker initiates a TCP connection with server with a SYN message. The server in reply sends an acknowledgement message. (SYN – ACK) message.
- The client (attacker) does not respond back with acknowledgement which causes server to wait.
- Due to which it is unable to connect with other client. This fills up the buffer space for SYN message preventing other for communicate.

(1) Clients sends synchronize (SYN) packet to server.

(2) Servers send syn-ack (SYN – ACK) to client.



(3) Clients responds back with ACK packet and connect is established client as shown in Fig. 3.6.1.

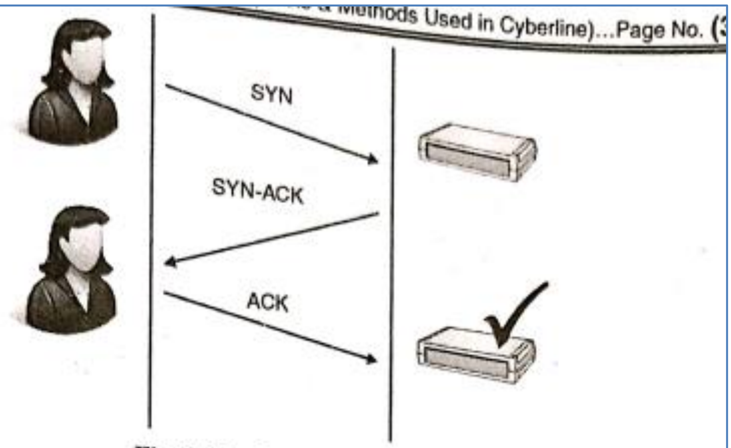
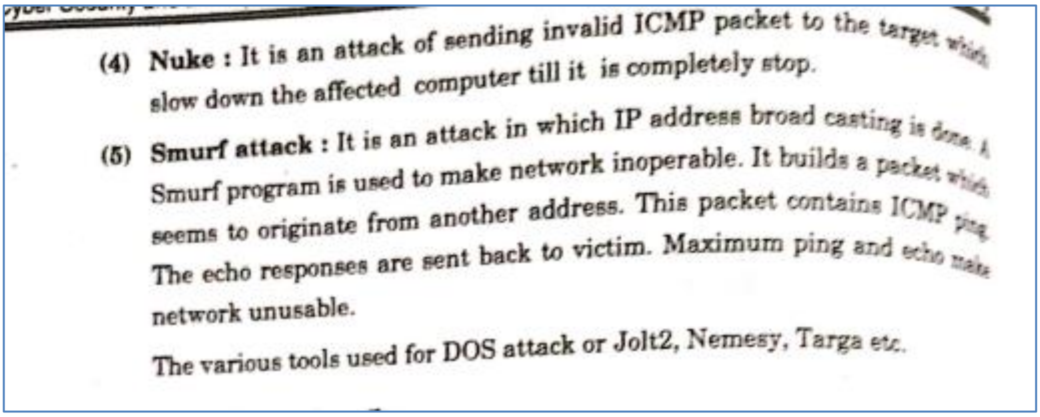


Fig. 3.6.1 : 3 way handshake



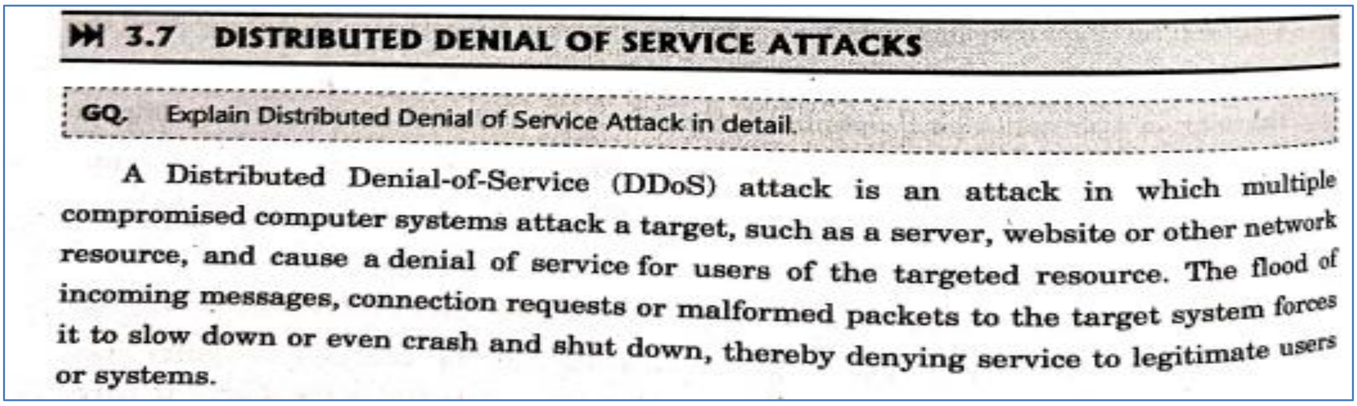
(4) **Nuke :** It is an attack of sending invalid ICMP packet to the target which slow down the affected computer till it is completely stop.

(5) **Smurf attack :** It is an attack in which IP address broad casting is done. A Smurf program is used to make network inoperable. It builds a packet which seems to originate from another address. This packet contains ICMP ping. The echo responses are sent back to victim. Maximum ping and echo make network unusable.

The various tools used for DOS attack or Jolt2, Nemesy, Targa etc.

Features to help mitigate these attacks (prevent):

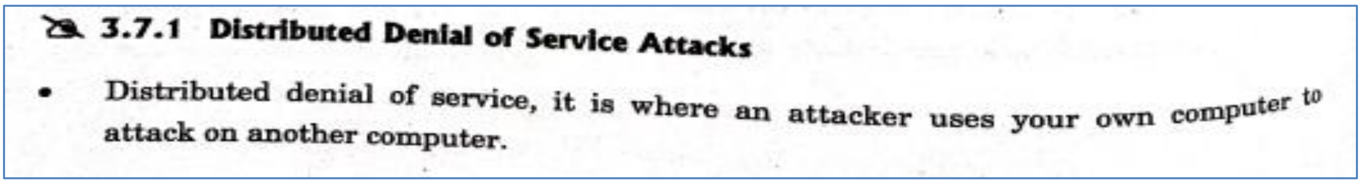
- **Network Segmentation:** Segmenting the network can help prevent a DoS attack from spreading throughout the entire network. This limits the impact of an attack and helps to isolate the affected systems.
- **Implement Firewalls:** Firewalls can help prevent DoS attacks by blocking traffic from known malicious IP addresses or by limiting the amount of traffic allowed from a single source.
- **Use Intrusion Detection and Prevention Systems:** Intrusion Detection and Prevention Systems (IDS/IPS) can help to detect and block DoS attacks by analyzing network traffic and blocking malicious traffic.
- **Use Anti-Malware Software:** Anti-malware software can help to detect and prevent malware from being used in a DoS attack, such as botnets.



3.7 DISTRIBUTED DENIAL OF SERVICE ATTACKS

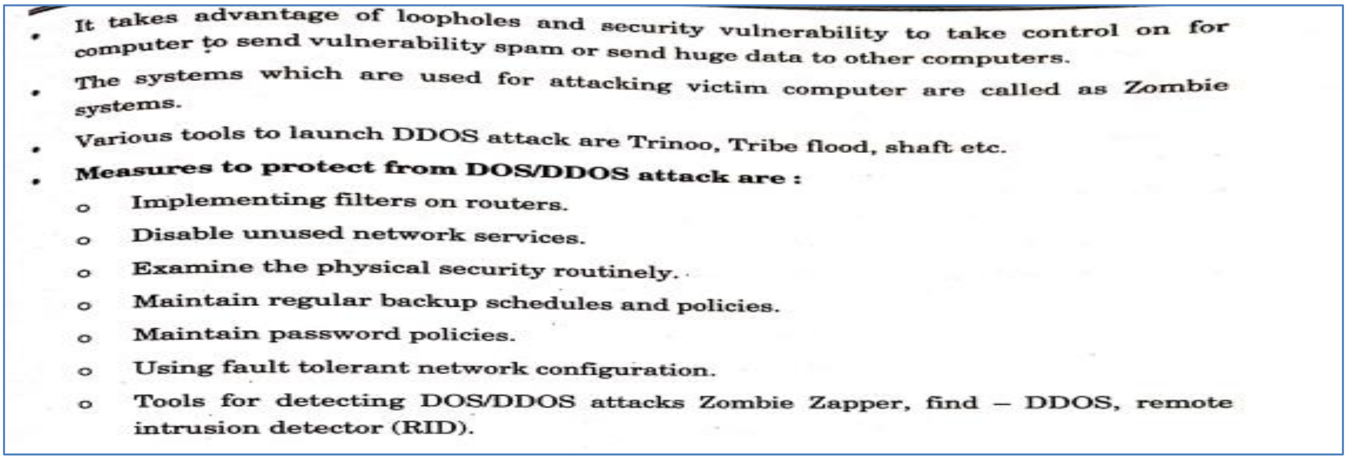
GQ. Explain Distributed Denial of Service Attack in detail.

A Distributed Denial-of-Service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.



3.7.1 Distributed Denial of Service Attacks

- Distributed denial of service, it is where an attacker uses your own computer to attack on another computer.



- It takes advantage of loopholes and security vulnerability to take control on for computer to send vulnerability spam or send huge data to other computers.
- The systems which are used for attacking victim computer are called as Zombie systems.
- Various tools to launch DDOS attack are Trinoo, Tribe flood, shaft etc.
- **Measures to protect from DOS/DDOS attack are :**
  - Implementing filters on routers.
  - Disable unused network services.
  - Examine the physical security routinely.
  - Maintain regular backup schedules and policies.
  - Maintain password policies.
  - Using fault tolerant network configuration.
  - Tools for detecting DOS/DDOS attacks Zombie Zapper, find – DDOS, remote intrusion detector (RID).

Types of DDoS attacks –
DDoS attacks can be divided into three major categories:

1. **Application layer attacks –**
   These attacks focus on attacking layer 7 of the OSI model where the webpages are generated in response to the request initiated by the end-user. For a client, generating a request does not take any heavy load and it can easily generate multiple requests to the server. On the other hand, responding to a request takes the considerable load for the server as it has to build all the pages, compute any queries and load the results from the database according to the request.
   Examples: HTTP Flood attack and attack on DNS Services.

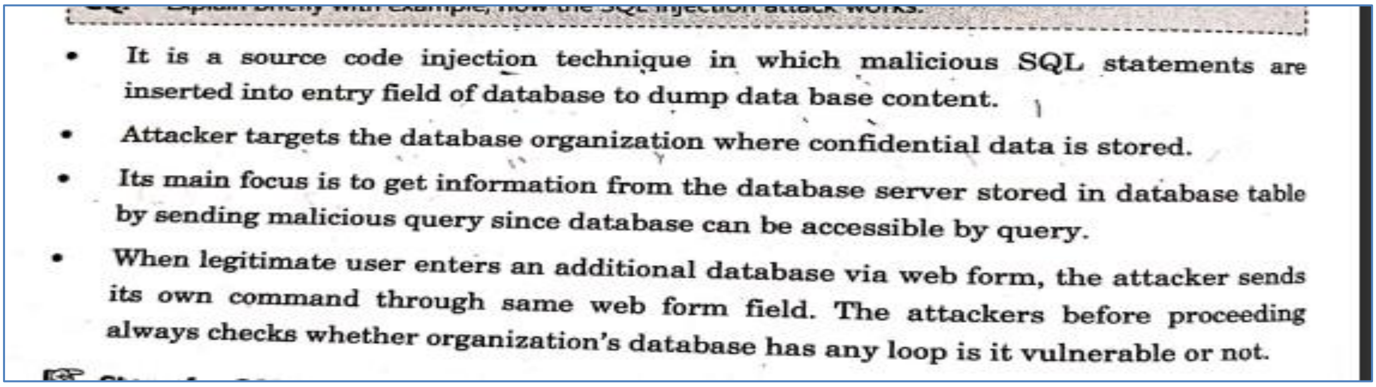
2. **Protocol attacks –**
   They are also known as state-exhaustion attacks. These attacks focus on vulnerabilities in layer 3 and layer 4 of the protocol stack. These types of attacks consume resources like servers, firewalls, and load balancers.
   Examples: SYN Flood attack and Ping of Death.

3. **Volumetric attacks –**
   Volumetric attacks focus on consuming the network bandwidth and saturating it by amplification or botnet to hinder its availability to the users. They are easy to generate by directing a massive amount of traffic to the target server.
   Examples: NTP Amplification, DNS Amplification, UDP Flood attack, and TCP Flood attack.

SQL Injection:

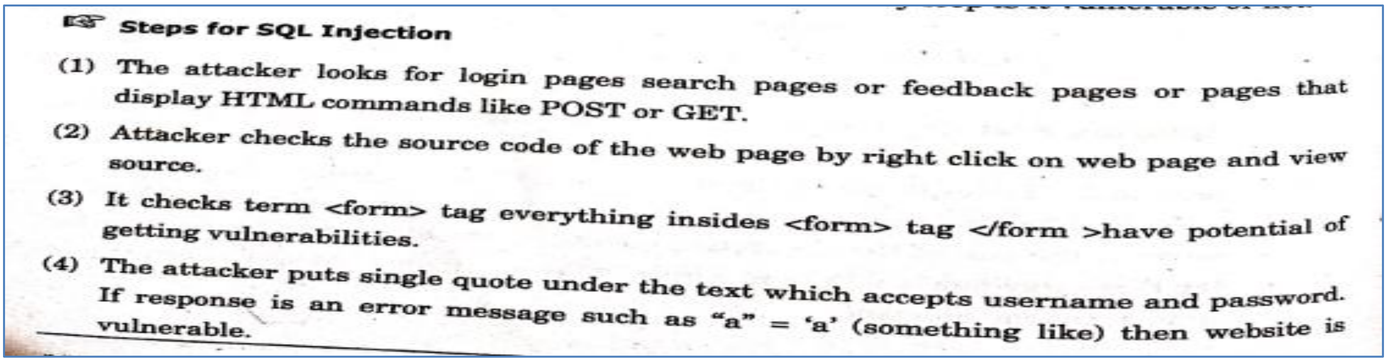
SQL injection is a technique used to extract user data by injecting web page inputs as statements through SQL commands. Basically, malicious users can use these instructions to manipulate the application's web server.

1. SQL injection is a code injection technique that can compromise your database.
2. SQL injection is one of the most common web hacking techniques.
3. SQL injection is the injection of malicious code into SQL statements via web page input.



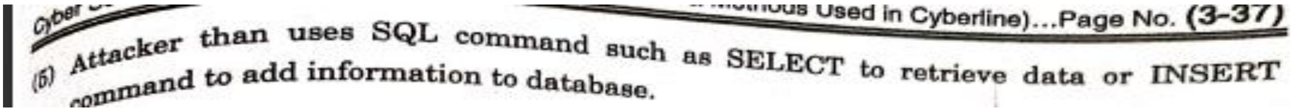
Explain briefly with example, how the SQL injection attack works.

- It is a source code injection technique in which malicious SQL statements are inserted into entry field of database to dump data base content.
- Attacker targets the database organization where confidential data is stored.
- Its main focus is to get information from the database server stored in database table by sending malicious query since database can be accessible by query.
- When legitimate user enters an additional database via web form, the attacker sends its own command through same web form field. The attackers before proceeding always checks whether organization's database has any loop is it vulnerable or not.

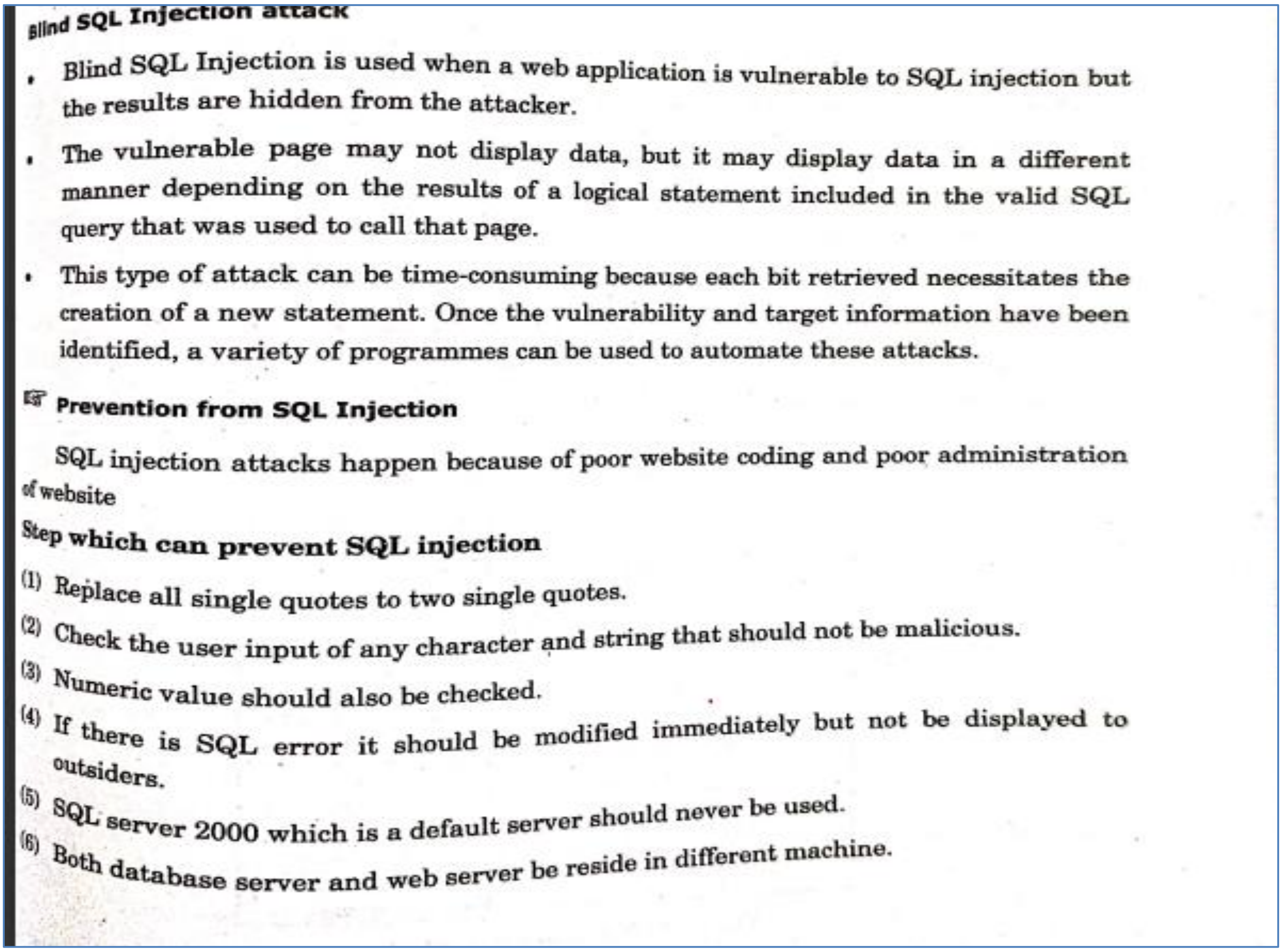


☞ **Steps for SQL Injection**

(1) The attacker looks for login pages search pages or feedback pages or pages that display HTML commands like POST or GET.
(2) Attacker checks the source code of the web page by right click on web page and view source.
(3) It checks term <form> tag everything insides <form> tag </form >have potential of getting vulnerabilities.
(4) The attacker puts single quote under the text which accepts username and password. If response is an error message such as "a" = 'a' (something like) then website is vulnerable.



(5) Attacker than uses SQL command such as SELECT to retrieve data or INSERT command to add information to database.



Blind SQL Injection attack

- Blind SQL Injection is used when a web application is vulnerable to SQL injection but the results are hidden from the attacker.
- The vulnerable page may not display data, but it may display data in a different manner depending on the results of a logical statement included in the valid SQL query that was used to call that page.
- This type of attack can be time-consuming because each bit retrieved necessitates the creation of a new statement. Once the vulnerability and target information have been identified, a variety of programmes can be used to automate these attacks.

☞ **Prevention from SQL Injection**

SQL injection attacks happen because of poor website coding and poor administration of website

Step which can prevent SQL injection

(1) Replace all single quotes to two single quotes.
(2) Check the user input of any character and string that should not be malicious.
(3) Numeric value should also be checked.
(4) If there is SQL error it should be modified immediately but not be displayed to outsiders.
(5) SQL server 2000 which is a default server should never be used.
(6) Both database server and web server be reside in different machine.

Preventing SQL Injection

- User Authentication: Validating input from the user by pre-defining length, type of input, of the input field and authenticating the user.
- Restricting access privileges of users and defining how much amount of data any outsider can access from the database. Basically, users should not be granted permission to access everything in the database.
- Do not use system administrator accounts.

✐Buffer Overflow

When a lot of data is written to a buffer than it can hold, a buffer overflow occurs. The extra data is written to the adjacent memory, overwriting the contents of that location and resulting in unpredictable program results. Buffer overflows occur when the data is written without sufficient validation (no boundaries). It's seen as a flaw or defect in the software.

- A buffer, also known as a data buffer, is a physical memory storage region that is used to hold data temporarily. At the same time, it is being transported from one location to another. These buffers are usually held in RAM.
- Attackers can take advantage of buffer overflows to corrupt software. Buffer overflow attacks, despite being well-understood, remain a serious security issue that plagues cyber-security teams. Because of a buffer

overflow vulnerability in SSL software, a threat known as 'heartbleed' exposed hundreds of millions of people to assault in 2014.

- Buffer is a temporary memory with small size which holds the data. Many software programs use buffer memory to speed up processing.
- Buffer is also used to store changes to data, the information in the buffer is copied to the disk. Buffer overflow occurs when more information is put into the buffer than its capacity to handle.

Types of Buffer Overflow Attacks:

Stack-based Buffer Overflow

It is often known as stack buffer overrun, a type of buffer overflow attack. In a last-in, first-out structure, the stack stores data. It's a continuous memory space used to arrange data connected with function calls, such as function parameters, function local variables, and management information like frame and instruction pointers.

Heap-based Buffer Overflow Attack:

The heap is a much larger chunk of memory used to store more complex data such as images, or text, that relates to the program. The premise here is similar to the previous, but is trickier for the attacker to implement because the heap isn’t directly used to determine where in memory executable code is located.

Arithmetic attacks :

These buffer overflow attacks emerge from the way C handles signed vs. unsigned numbers. Specifically, it’s possible to convert a negative (signed with -) number that requires little memory space to a much larger unsigned number that requires much more memory. A crash subsequently occurs and can be leveraged to yield an attack.

Format attacks:

Text strings, rather like signed numbers, are sometimes converted automatically from a smaller format to a larger (such as by operating systems that require Unicode values). This means attackers can design a buffer overflow attack that exceeds the buffer length if the programmer hasn’t been careful to take into account the larger format.

Buffer Overflows prevention

Complier modifications: A technique to avoid buffer overflow attack is to modify the way the data is stored in the memory. StackGuard is a type of a complier which can be used to add gaps in the memory in between, these gaps are known as Canaries.

Array bounds checking: Each time an operation needs to be performed on an array, we can do the boundary checking. If boundary is reached it won’t allow writing into the array, thus avoiding the buffer overflow.

Non-Executable Stack: marking of the stack as Non-Executable can help stopping Buffer Overflow. But this in turn also stops genuine programs from executing directly from the stack.

Write correct code: To avoid any kind of attack if to write good and correct code. It is a human’s tendency to write and forget the code, but that same code can be checked by someone else as well.

Split stack: Split Stack or Secure Address Return Stack (SAS) is a proposed technique to prevent buffer overflow attack. In this technique two software stacks are used, one for control information and another for data information. Hence even if an attacker gains access to the data stack, he cannot affect the control stack. Although it might need to read and write from 2 stacks it is worth the time.

🕸**Wireless network attacks**

Wireless network attacks are deliberate and malicious actions aimed at exploiting vulnerabilities in wireless communication systems to gain unauthorized access, intercept sensitive data, disrupt network operations, or compromise the security of devices and users connected to the network.

These attacks target weaknesses in the protocols, configurations, or encryption mechanisms of wireless networks, taking advantage of their inherent nature of broadcasting signals over the airwaves.

Types of Wireless Network Attacks:

Rouge access point: When an unauthorized access point (AP) appears on a network, it is referred to as a rouge access point. These can pop up from an employee who doesn’t know better, or a person with ill intent. These APs represent a vulnerability to the network because they leave it open to a variety of attacks. These include vulnerability scans for attack preparation, ARP poisoning, packet captures, and Denial of Service attacks.

Password theft: When communicating over wireless networks, think of how often you log into a website. You send passwords out over the network, and if the site doesn’t use SSL or TLS, that password is sitting in plain text for an attacker to read. There are even ways to get around those encryption methods to steal the password. I’ll talk about this with man in the middle attacks.

War driving: War driving comes from an old term called war dialing, where people would dial random phone numbers in search of modems. War driving is basically people driving around looking for vulnerable APs to attack. People will even use drones to try and hack APs on higher floors of a building. A company that owns multiple floors around ten stories up might assume nobody is even in range to hack their wireless, but there is no end to the creativity of hackers!

Blueooth attacks: There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the a victims Bluetooth enabled device.

WEP/WPA attacks: Attacks on wireless routers can be a huge problem. Older encryption standards are extremely vulnerable, and it’s pretty easy to gain the access code in this case. Once someone’s on your network, you’ve lost a significant layer of security. APs and routers are hiding your IP address from the broader Internet using Network Address Translation (unless you use IPv6 but that’s a topic for another day). This effectively hides your private IP address from those outside your subnet, and helps prevent outsiders from being able to directly attack you. The keyword there is that it helps prevent the attacks, but doesn’t stop it completely.

Man in the middle attack: It’s possible for hackers to trick communicating devices into sending their transmissions to the attacker’s system. Here they can record the traffic to view later (like in packet sniffing) and even change the contents of files. Various types of malware can be inserted into these packets, e-mail content could be changed, or the traffic could be dropped so that communication is blocked.

Jamming: There are a number of ways to jam a wireless network. One method is flooding an AP with de-authentication frames. This effectively overwhelms the network and prevents legitimate transmissions from getting through. This attack is a little unusual because there probably isn’t anything in it for the hacker. One of the few examples of how this could benefit someone is through a business jamming their competitors WiFi signal. This is highly illegal (as are all these attacks), so businesses would tend to shy away from it. If they got caught they would be facing serious charges.

☝**Tool:**

1. **Aircrack** is used as 802.11 WEP and WPA-PSK keys cracking tool around the globe. It first captures packets of the network and then try to recover password of the network by analyzing packets. It also implements standard FMS attacks with some optimizations to recover or crack password of the network. Optimizations include KoreK attacks and PTW attack to make the attack much faster than other WEP password cracking tools.
2. **AirSnort** AirSnort is wireless LAN password cracking tool. It can crack WEP keys of Wi-Fi 802.11b network. This tool basically operates by passively monitoring transmissions and then computing the encryption key when enough packets have been gathered.
3. **Kismet** Kismet Wi-Fi 802.11 a/b/g/n layer 2 wireless network sniffer and intrusion detection system. This tool is basically used in Wi-Fi troubleshooting.
4. **Cain and Able** Cain and Able tool used for cracking wireless network passwords. This tool was developed to intercept the network traffic and then use the brute forcing to discover the passwords.
5. **WireShark** WireShark is the network protocol analyzer tool which lets you check different things in your office or home network. You can live capture packets and analyze packets to find various things related to network by checking the data at the micro-level.