26/10/23

UNIT - 3

Tools and methods used in cybercrime.

1. Phishing
2. Password cracking.
3. Keyloggers.
4. Spyware
5. Virus & worm
6. Trojen horse
7. Backdoors
8. Steganography
9. DOS & DDOS Attack
10. Buffer overflow
11. SQL injector.

Proxy Server -

"Proxy server is a computer on a network which acts as an intermediary for connection with other computer on that network."

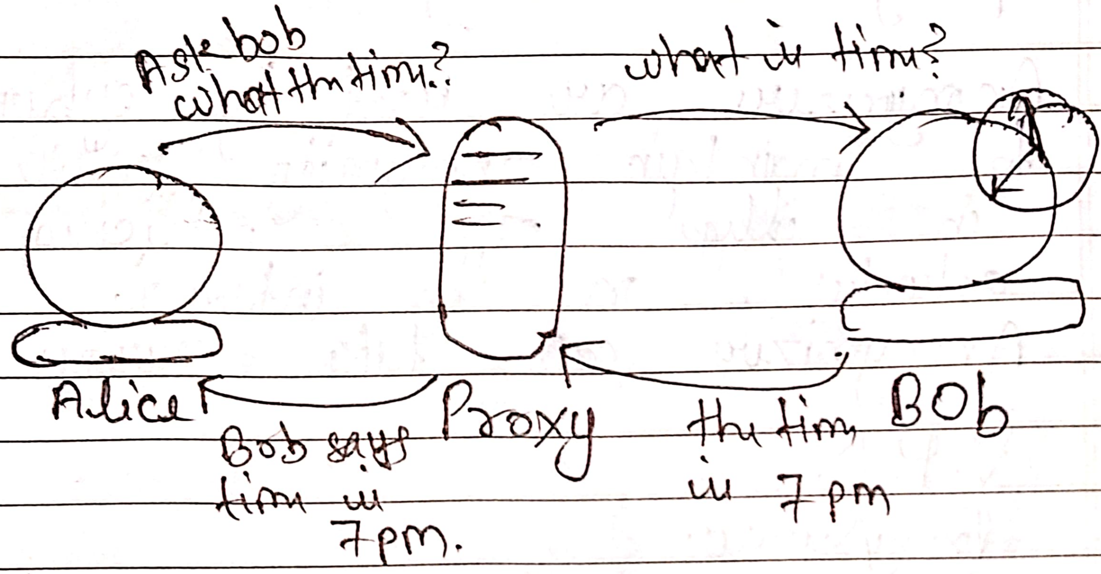
(OR)

A proxy server is like a middleman for your internet connection. when you use the internet, your device sends requests for information (like opening a website) to the server that host that information.

A proxy server

stands between your device and the internet and forward your request to the website or online service you want to use.

Ex- Think of it like having a friend who goes to the store for you because you don't want the store to know you're the one buying something. the friend brings you what you need. but the store does not know its for you that's like a proxy server does for your internet requests.



Q. why use a proxy server?

A. Privacy- It can hide you real IP address making it harder for website to track your online activity.

Security- It can act as a barrier, protect from harmful website or content.

Access- It can help you access website that might be restricted in ourlocation.

Anonymizers -

* An anonymizer or an anonymous proxy is a tool that attempts to make activity on the internet untracable.

It access the internet on the user's behalf, protecting personal information by hiding the source computer's identifying information

* Anonymizers are services used to make web surfing anonymous by utilizing a website that acts as a proxy server for the web client.

* Anonymizers are used by cybercriminals to maintain anonymity while engaging in illegal or malicious activities on the internet.

Anonymizers can take various forms -

1. V.P.N
2. Proxy Server
3. Anonymous mail Service
4. The onion router.

How phishing works -

एक mail बहुत लोगों को भेजना

[1.] Planning - Use mass mailing and address collection ~~ti~~ techniques - spammers

[2.] Setup - Email/webpage to collect data about the target.

[3.] Attack - Send a authentic(phony) msg to the target.

[4.] Collection - Record the info. obtained.

[5.] Identity theft & Fraud - Use info. to commit fraud or illegal purchase.

Password Cracking -

* Password is like a key to get an entry into computerised system like a lock.

* Password cracking is a process of recovering passwords from data that have been stored in or transmitted by a computer system.

* Usually, in password cracking, attacker follows a common approach repeatedly making guess for the password.

The purpose of password cracking is as follows -

1.) To recover a forgotten password.
2.) To gain unauthorised access to system.

There are different methods which are used for password cracking -

[1.] **Brute force Attacks** - This is like trying every possible combination untill they find the right one. ~~its like going~~

[2.] **Dictionary Attack** - Instead of trying every possible combination, attacker uses a "dictionary" of common words, phrases or passwords.

[3.] **Rainbow table Attacks** - Imagine if every possible password and its corresponding hash (a unique code generated from the password) were pre-computed and stored in massive table! Attackers can then compare the hash of your password against this table to find a match.

To protect against password cracking, it's important to use strong and unique passwords, avoid easily passwords and enable additional security like a two-factor authentication.

Keyloggers - (Keystroke logging)

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims.

A keylogger is a form of Spyware that capture every moment.

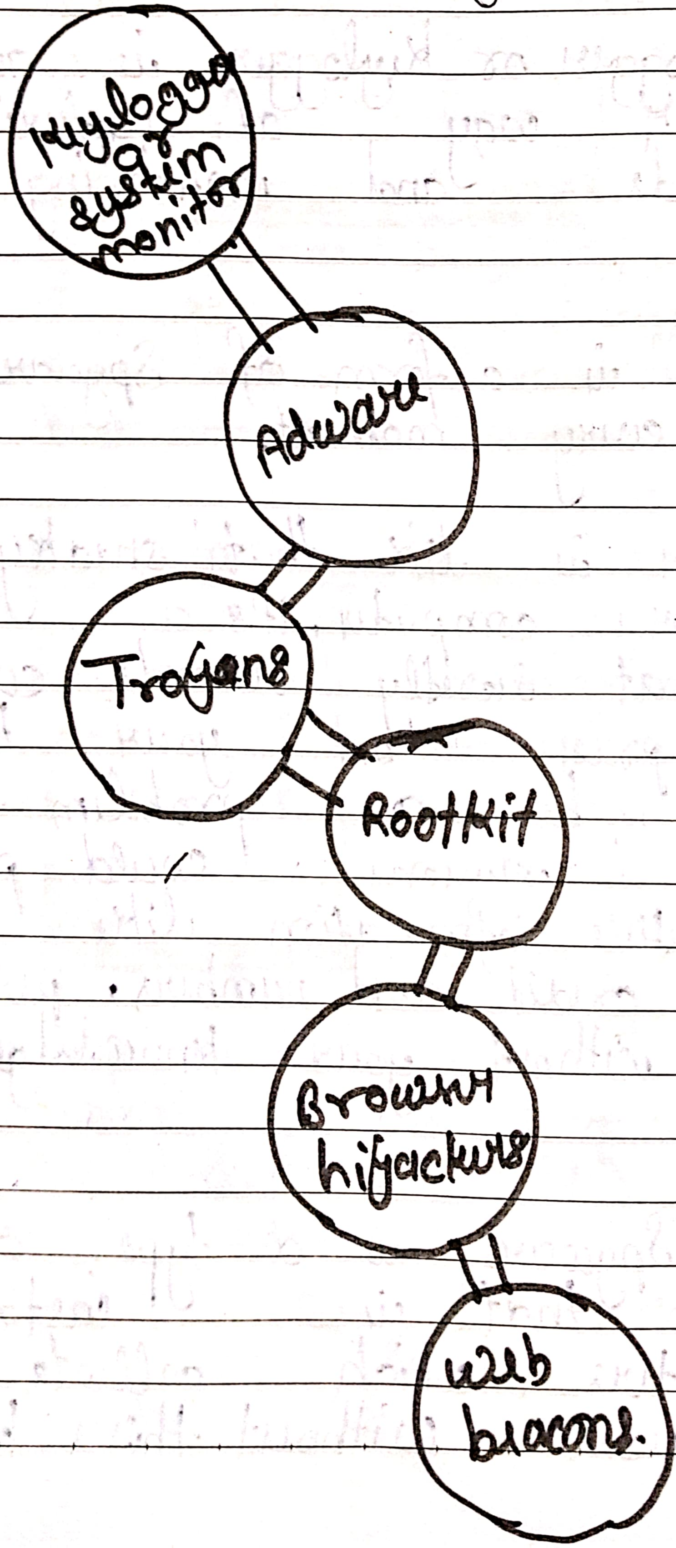
A keylogger is like that sneaky observer for your computer. it's a type of S/W that secretly records every key you press on your keyboard this can be a problem because it means someone could potentially see sensitive information like your passwords, credit card numbers, personal messages without your knowledge.

Spyware -

* Spyware is a type of malware that is installed on computers which collects informati about users without their knowledge.

The presence of Spyware is typically hidden from the user. it is secretly installed on the user personal computer.

Types of Spyware



Parameter	Spyware	Keylogger.
Meaning.	S/W that collects info. about user without their knowledge	S/W that record every keystroke a person on computer
Records	User activity and internet browsing	User keystroke
Prevention S/W	Antispyware	Anti keylogger
Type.	Keylogger, adware, trojans etc.	winspy, Spyware

Viruses -

* Virus is type of malware it is created by malicious code or program.

* A computer viruses passes from computer to computer in a similar manner as a biological virus passes from person to person.

* Viruses may also contain malicious instruction that may cause damage the combination of possibly malicious code with the ability to spread is what makes viruses a considerable concern.

Worms -	Viruses.
① Worms like spreading germs, worms is a type of malware it copy itself and travel through n/w causing a lot of trouble for many devices.	Viruses is also type of malware it is created by malicious code it is spread from computer to computer.
② Replicate from one computer to another	It requires a host for spreading
③ It is less harmful as compared.	It is more harmful
④ Worms can be control by remote	Viruses can't be control by remote
⑤ To prevent from worms avoid opening email from unknown sources.	keep your browser & operating system updated.
⑥ Worms can be detected and removed by anti virus and firewall	Antivirus s/w is used for protection against viruses.

Trojan horse -

Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and cause harm, for example running the file allocation table on the hard disk.

Trojan pretend to be nice apps or files, but they secretly cause damage once you open them. Unlike viruses or worms, trojans do not replicate themselves but they can be equally destructive

For example. waterfalls.scr is a waterfall screen saver as originally claimed by the author however, it can be associated with malware and become a trojan to unload hidden programs and allow unauthorised access to the user's P.C.

Backdoors -

A backdoors is a mean of access to a computer program that bypass security mechanism A programmer may sometimes install a backdoor so that the program can be accessed for troubleshooting or other purpose.

[OR]

A backdoor in computing refers to a hidden or documented method of gaining access to a computer system, S/W application or N/W. It provides an alternative way to enter a system without going through standard authentication process.

Backdoors can be intentionally created by S/W developer for debugging and maintenance purpose, but they can also be exploited or inserted by attackers for malicious activities and with the help of backdoors an individuals to manipulate or control a system without proper authorization.

Regular security measures, monitoring and detection mechanism are essential to identify and

bulling (criminal activity) 1-2 - Unit-4 & Unit-5
Unit-3

prevent the misuse of backdoors.

(cryptography) Secret covert msg in cover media (hidd

Steganography

A steganography attack is the art and science of embedding hidden messages or malware in a carrier medium such as an image or video file in a way the recipient does not realize the file is malicious.

* Steganalysis is the art and science of detecting messages that are hidden in images, audio/video file using steganography.

* Steganography is like hiding a msg within a picture. Imagine you have a photo, and instead of just sing the image, certain pixels subtly encode a secret message. Similarly, in Steganography, data is concealed within other data to avoid detection, making it a covert way to transmit information without arousing suspicion.

Can be correct by n/w event

* Denial of Service (DOS) -

Denial of Service means to make inaccessable of the website or n/w. and the purpose of the attacker to ~~to~~ do for this to demand money for realising the website.

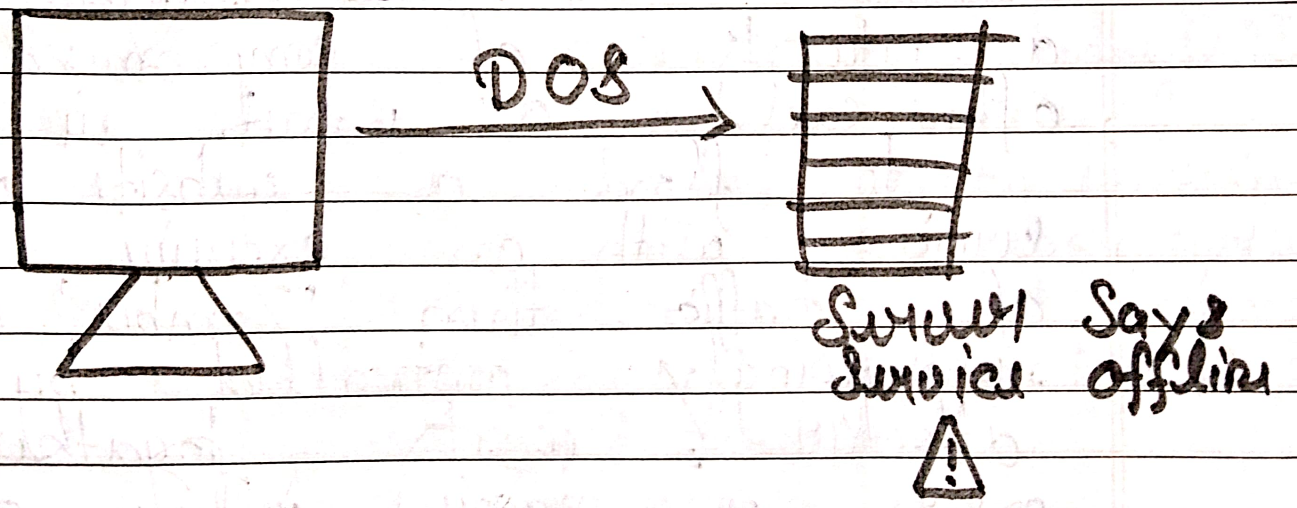
[OR]

A DOS Attack is an attack mean to shut down a machine or network, making it inaccessible to its intended users. DOS attacks accomplish this by flooding the target with traffic, or sending it information that trigger a crash.

Imagine you're at popular ICE Cream shop. and there's long line of people waiting to order their favorite ICE Cream flavors. the shop has a limited Capacity to serve a certain no. of customer at a time,

Now, Suppose someone maliciously decide to block the entrance of the shop, preventing new customer from entering. this person might not be interested in buying ice cream. their intention is to create chaos and make it difficult for others to enjoy the ice cream they want.

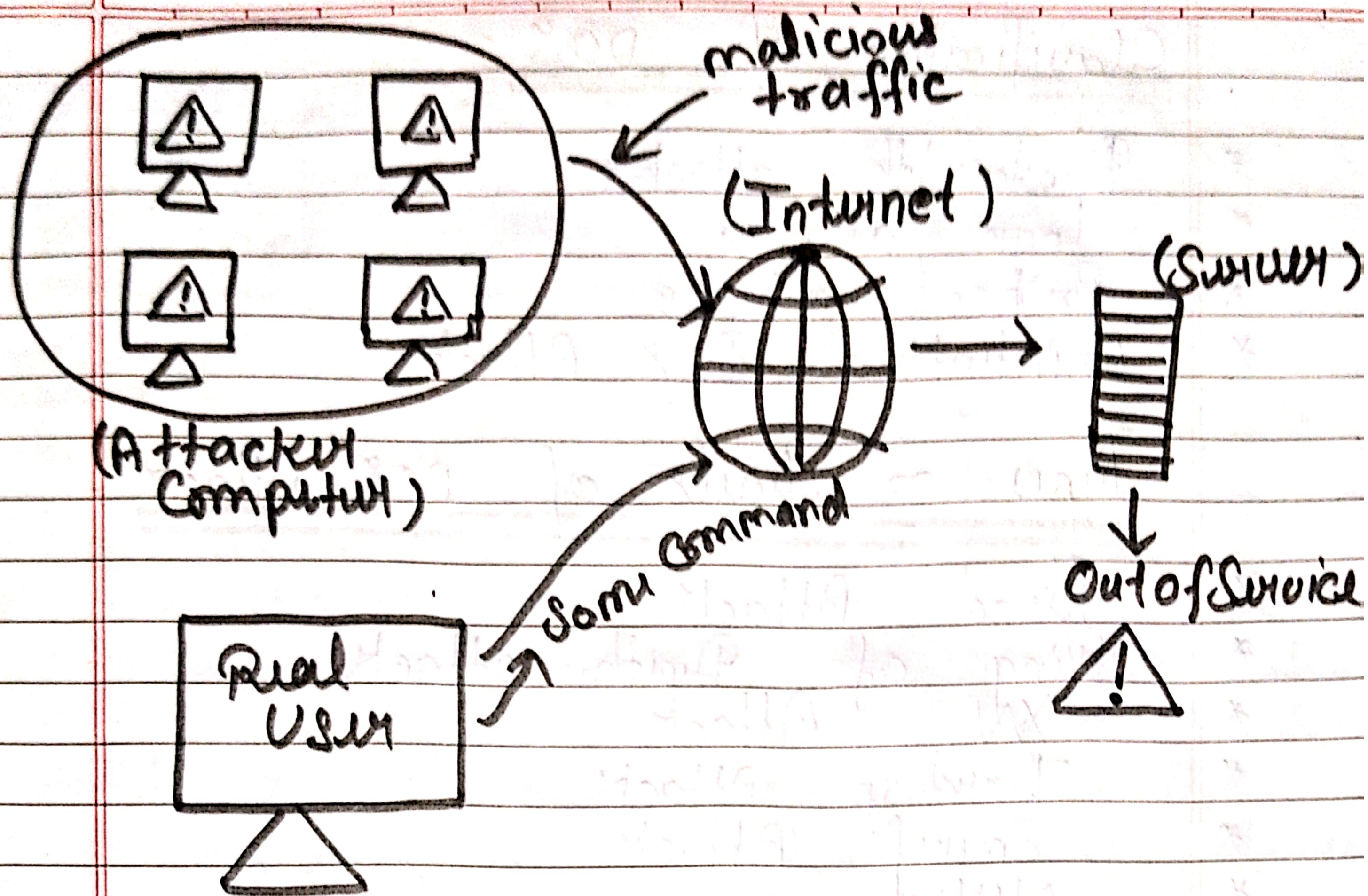
→ In the world of Computer network, a Denial of Service (DOS) Attack is similar. instead of blocking ~~or~~ a physical entrance attackers flood (बाढ़) a website or an online service with an overwhelming (भारी पड़ना) amount of traffic, making it difficult for legitimate users to access the website or service. the goal is to overwhelm the system resources and cause a disruption in its normal functioning, denying access to genuine users.



* Distributed Denial of Service (DDOS).

Imagine the same popular ICE Cream shop, but now there's a twist. instead of one person blocking the entrance shop. A large group of trouble makers spread out and block multiple entrances to the shop simultaneously. each troublemaker doesn't individually cause a significant problem, but collectively they create chaos by overwhelming the shop's capacity to handle customers

→ In the world of Computer n/w, a DDOS attack is similar. instead of a single attacker, a network of compromised computers, often called a Botnet, is used to flood a website or online service with an excessive amount of traffic. these 'Zombie' computers, unknowingly controlled by the attacker, work together to create a massive influx of requests, making it extremely challenging for the targeted system to function properly.



* DOS Vs DDOS

	DOS	DDOS
Acronym	Denial of Service	Distributed DOS
Description	A single system targetting a single system.	A n/w of system targetting a single system
Method	Flood just enough traffic from a single loc. to disable the victim n/w.	Floods massive amount of traff
Impact	Moderately effective	Very effective
Traceability	Easily traceable	Difficult to trac
Speed.	slow attack	Quick attack

Classification of DOS -

- * Bandwidth attacks
- * Logic attacks
- * Protocol attacks
- * Unintentional DOS Attack.

Types or levels of DOS Attack -

- * Flood Attack
- * Ping of Death attack
- * SYN Attack
- * Teardrop Attack
- * Smurf Attack
- * NUKE.

SQL Injection -

Structured Query language (SQL) is a database computer language design for managing data in relational database management systems (RDBMS).

* SQL injection is a code injection technique that might destroy your database.

* SQL injection is one of most common web hacking techniques.

* SQL injection is the placement of malicious code in SQL statement via web page Input.

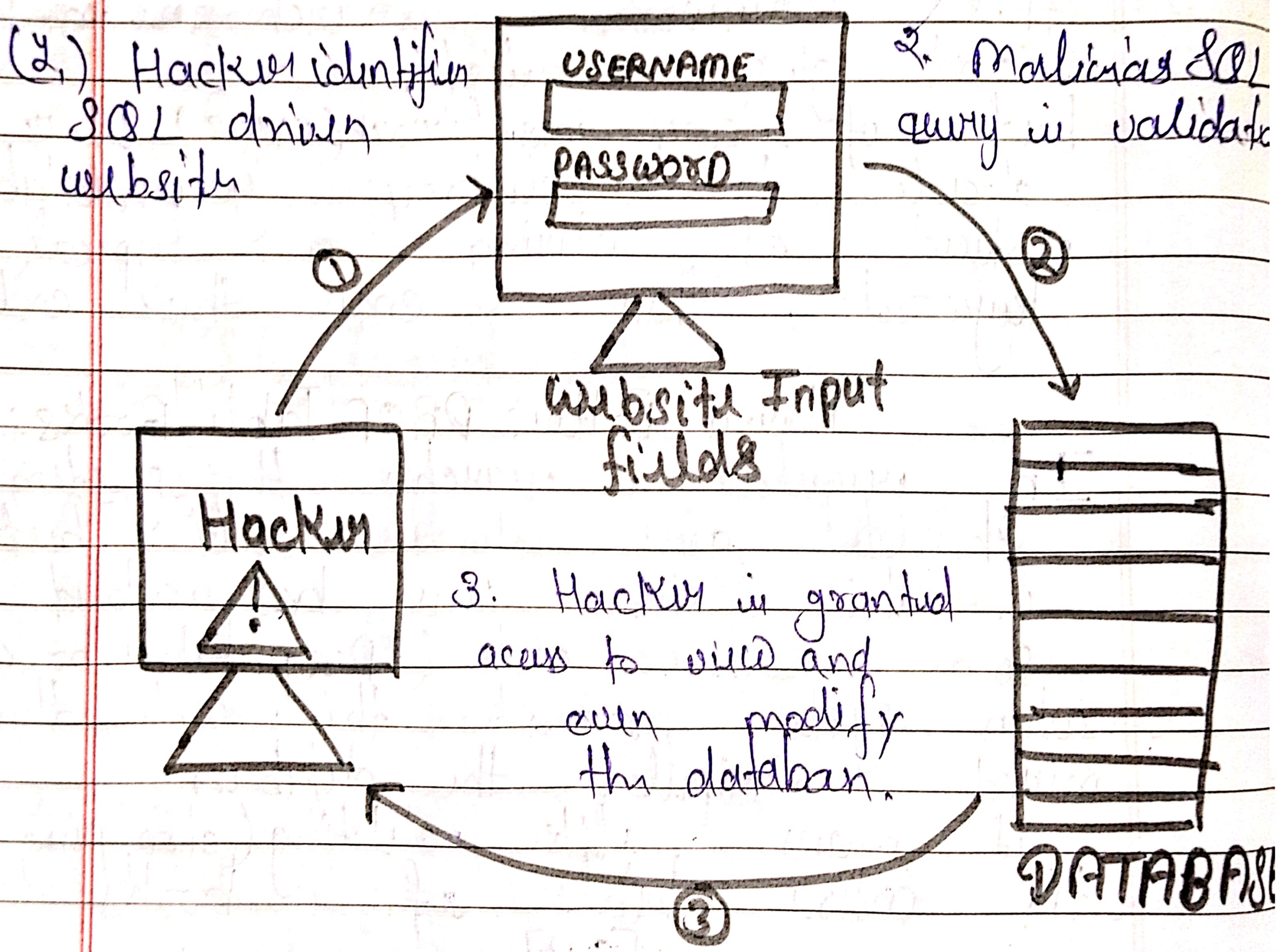
Example: Imagine a library user wants to find a book by typing a keyword into ~~a~~ the searchbar. normally the system would take this keyword, search the catalog and give a list. but if any mischivous (शरारती) user decide to destroy your database instead of entering a typical keyword, they enter this code

Harry Potter; DROP Table Books;--

In regular searches the system should give the result but in this case user has added some extra code ("Drop table books;") when system processed this code then might manipulate the database it means like deleting (dropping) the entire table of books

[OR]

→ In real world term's, SQL injection is a technique where attackers input malicius SQL code into forms or i/p fields on a website, exploiting vulnerabilies to manipulate the underlying database and potentially gain unauthorized access or perform unintended actions. its important for developers to impliment proper security measures to prevent SQL injection attacks.


(1.) Hacker identifies SQL driven website
USERNAME
PASSWORD
Website Input fields
2. Malicious SQL query is validated
1
2
Hacker
3. Hacker is granted access to view and even modify the database.
3
DATABASE

Q. what is Blind SQL injection?
(User did not know ---)

An Blind SQL injection is used when a web application is vulnerable to an SQL injection, but the result of the injection are not visible to the attacker.

* Buffer overflow -

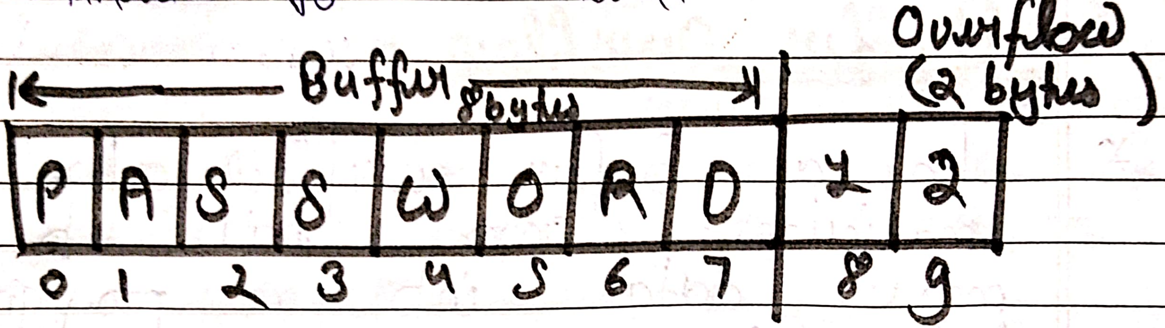
* In a Buffer overflow attack, a malicious actor tries to input more data into a program memory buffer than it can accommodate if the program doesn't properly handle this excess input, it can lead to unintended consequences such as overwriting or executing malicious code.

* The Buffer over flow Attack result unreliable program behaviour, including memory access error, incorrect result, crash systems.

* Programming language commonly associated with buffer overflow include C and C++ which provide no built in protection against overwriting data in any part of memory and do not automatically check that data written to an Array.

* Buffer Overflow occurs when a program or process tries to store

more data in a buffer (temporary data storage area) than it was intended to hold.



For exp-

```
{ int main
      int buffer[10];
      buffer[20] = 5;
  }
                 ↑
           Buffer Overflow
```

How to minimize buffer overflow -

* Assessment of secure code manually
* Disable stack execution
* Compiler tools
* Various tools are used to detect -

→ StackGuard
→ Propolice
→ Libsafe.

·;- Attacks On wireless network -

*** Different Component of wireless network**

there are different component of wireless network as fallows –

① **802.11 networking standards.** The 802.11 standards refer to a set of rules and specification for wireless localarea networking (WLAN). these standards define how devices communicate with each other over Wi-Fi.

② **Wireless Devices.** These are gadget like our phone, laptop or tablet that can connect to the internet without any physical cable.

③ **Wireless Router –** Think of this as the traffic cop for your internet. it helps direct data between your device and the internet.

④ **Acess points-** Imagine these a Wi-Fi" signal boosters. they help spread the wireless network coverage, making sure all your devices can connect smoothly.

⑤ **Wifi Hotspot** -

Wi-Fi Hotspot are location where wireless access to the internet is availble, often provided by public establishments such as cafes, airports and Hotels.

⑥ **Service set identifier (SSID)**

Imagine your wifi networks is like a club and the SSID is the name of that club. it helping you know which Wi-Fi n/w you want to join.

When you see a list of wi-fi names those are SSIDs Each n/w has its own name. and you can select the one you want to connect.

⑦ **Wi-Fi protected access (WPA or WPA2)** -

WPA and WPA2 are improved and more secure encryption and security protocols for Wi-Fi n/ws.

⑧ **Media acess Control (MAC) -**

Think of a mac address as a special id card for your device, like your phone or laptop. just like you have a unique name. each device has a unique MAC address. it's like a way for your device to introduce itself on a n/w.
When device communicate on a n/w, they use their MAC address to identify the MAC address helps make sure data goes to the right device, like your message etc.

* Techniques of attacks on wireless network -

① **Eavesdropping:** Imagine you and your friend are passing notes, but someone nearby is secretly reading what you're writing. it in the digital world, eavesdropping is like someone snooping on the messages being sent over a wireless n/w. trying to steal information

~~Unit - 5~~

(2) Denial of Service (DOS) Attack.

DOS attack floods a wireless n/w with more traffic, making it hard to connect.

(3) Man-in the middle attacks (MitM) :-

पहुँचा रहे हैं

Imagine someone interupting your notes to your friend changing the messages, and passing them along without you knowing. ~~in~~ + A man in the middle attack involves an attacker secretly interupting and possibly altering the Communication between two parties.

(4) WPA Cracking.

Attackers may use special tools to ~~chect~~ crack the encryption and gain unauthorised access to the n/w

(5) SSID Spoofing:-

Attackers may create a fake Wi-Fi n/w with the same name (SSID) as a legitmate one fooling users into connecting to the wrong n/w.