Cyber Security - fundamentals

Ethical Hacking:

The ethical hacking means testing computers, networks & applications by legally trying to break into them in order to find security weakness before malicious hackers do.

→ Hacking with permission and responsibility is called as "ethical hacking"

→ Why it is called "Ethical"

↳ The permission is taken from the system owner.

* It follows legal rules and constraints permissions.
* When found vulnerabilities are reported not misused.
* It respected the user privacy and data.

→ Ethical Hackers also called as

↳ White Hat Hacker
↳ Security Analyst
↳ Pentration Tester

Importance of ethical Hacking

* It prevents cyber Attacks
* It protects personal data
* It gives secures banking and online transactions.
* It helps companies follow security laws.
* The saves money by avoiding data breaches.

Eg: The banks uses ethical hackers to check if hackers can steal money & customer details.

What Do ethical Hacker

* They can test websites and apps for security holes.
* It check networks for weak password.
* The identification of malware and vulnerabilities.
* It performes penetration testing
* They suggest security fixes.

Types of Hackers:

The hackers are categorized by intent and methods ranging from ethical to malicious. Each has distinct motivations and impacts on system

Core Types

→ **White Hat:**
The ethical hackers authorized to test and fix security vulnerabilities.

→ **Black Hat:**
The malicious actors who exploit system illegally to profit & damage.

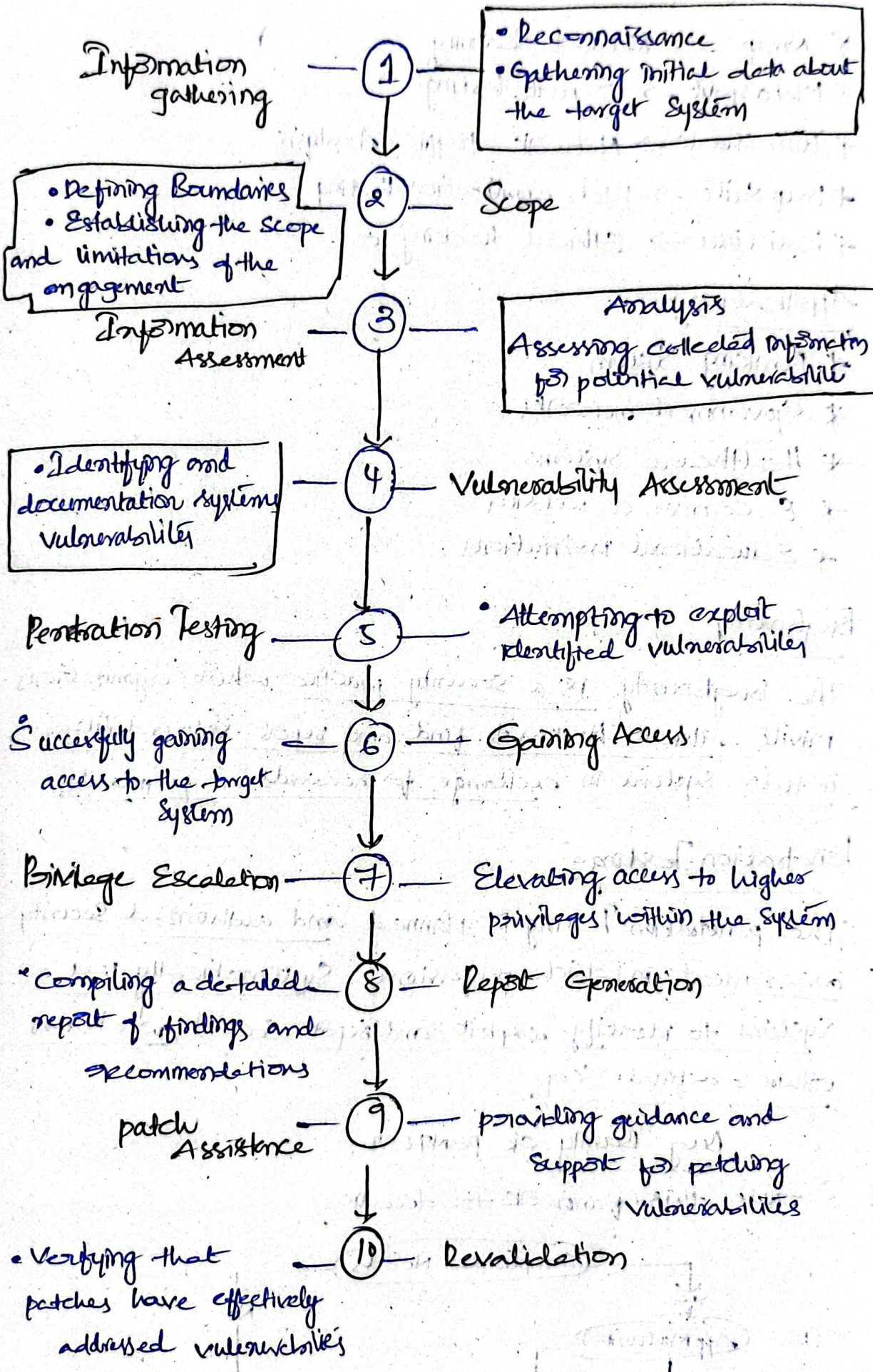
→ **Gray Hat:**
The Hack without permission but discloses flaws, often seeking recognition & reward.

Other Types

* Red Hat
* Green Hat
* Script kiddie
* Hacktivisit

Steps followed by Ethical Hackers

1. Information gathering
2. Scope
3. Information Assessment
4. Vulnerability Assessment
5. penetration testing
6. Gaining Acces
7. Repot Generation
8. privilege Escalation
9. patch Assistance
10. Revalidation.


Information gathering
1
• Reconnaissance
• Gathering initial data about the target System
• Defining Boundaries
• Establishing the scope and limitations of the engagement
2
Scope
Information Assessment
3
Analysis
Assessing collected information for potential vulnerabilities
• Identifying and documentation systems vulnerabilities
4
Vulnerability Assessment
Penetration Testing
5
• Attempting to exploit identified vulnerabilities
• Succesfully gaining access to the target System
6
Gaining Access
Privilege Escalation
7
Elevating access to higher privileges within the System
• Compiling a detailed report of findings and recommendations
8
Report Generation
patch Assistance
9
providing guidance and support for patching vulnerabilities
• Verifying that patches have effectively addressed vulnerabilities
10
Revalidation

Tools:

* Nmap → Network Scanning
* Metasploit → Exploit testing
* Wireshark → Network traffic Analysis
* Burp Suite → Web application testing
* Kali Linux → Ethical hacking os.

Application:

* Banking System
* Government networks
* Healthcare Systems
* E-commerce websites
* Educational institutions.

BugBounty

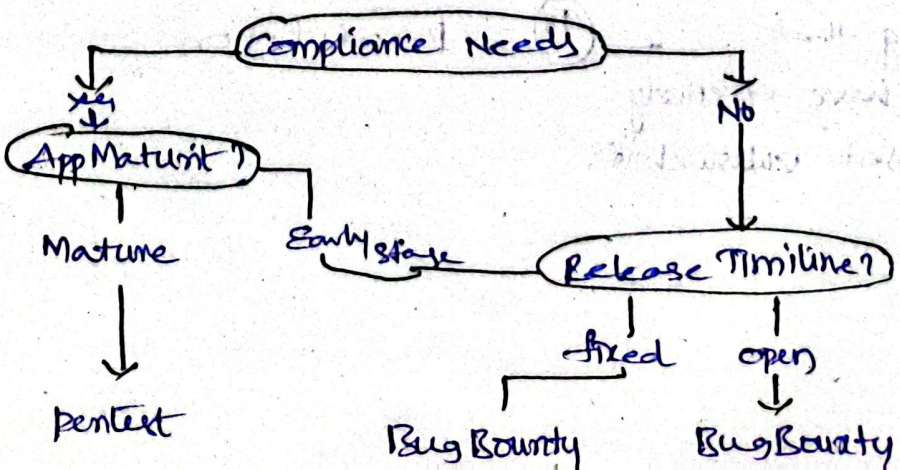
The BugBounty is a security practice where organizations invite ethical hackers to find and report vulnerabilities in their systems in exchange for rewards or payments.

Penetration Testing:

The penetration Testing is planned and authorized security assessment in which professional systematically test a system to identify, exploit, and report security weaknesses within a defined scope.

Bug Bounty OR PENTEST

→ use this framework to decide.



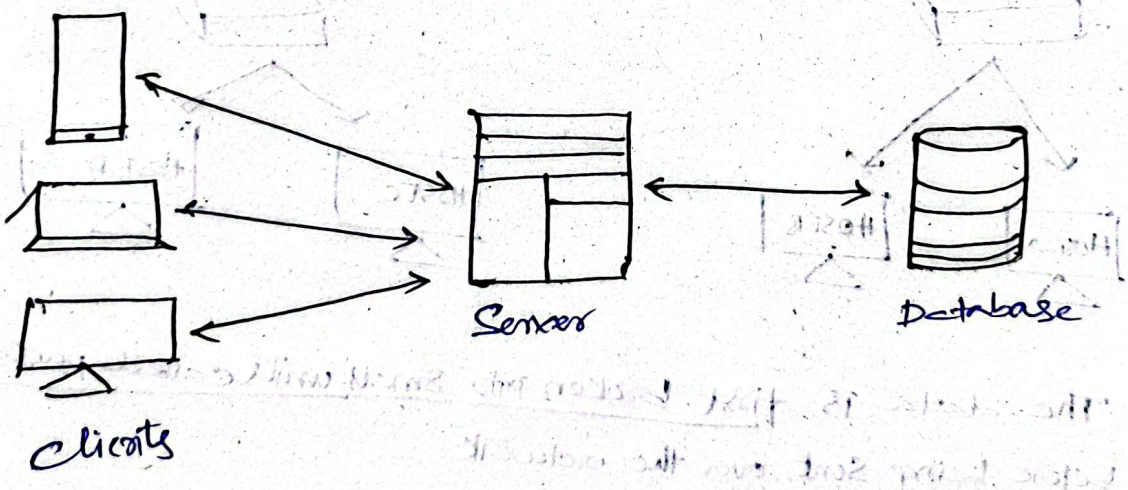
Bug Bounty

* The finding security bugs to earn rewards
* It given through public bounty programs
* It has independent ethical hackers
* They paid only if a valid bug is found
* It limited to program rules
* They continuous or ongoing
* It depends on the hacker
* The purpose is discover individual vulnerabilities

Penetration Testing

* The professional testing to evalute system security.
* It given through a legal content.
* It has hired security professionals.
* They fixed payment regardless of bugs.
* It has predefined and detailed scope.
* It has fixed testing duration.
* It deep and systematic testing
* It purpose the evalute overall security strength.

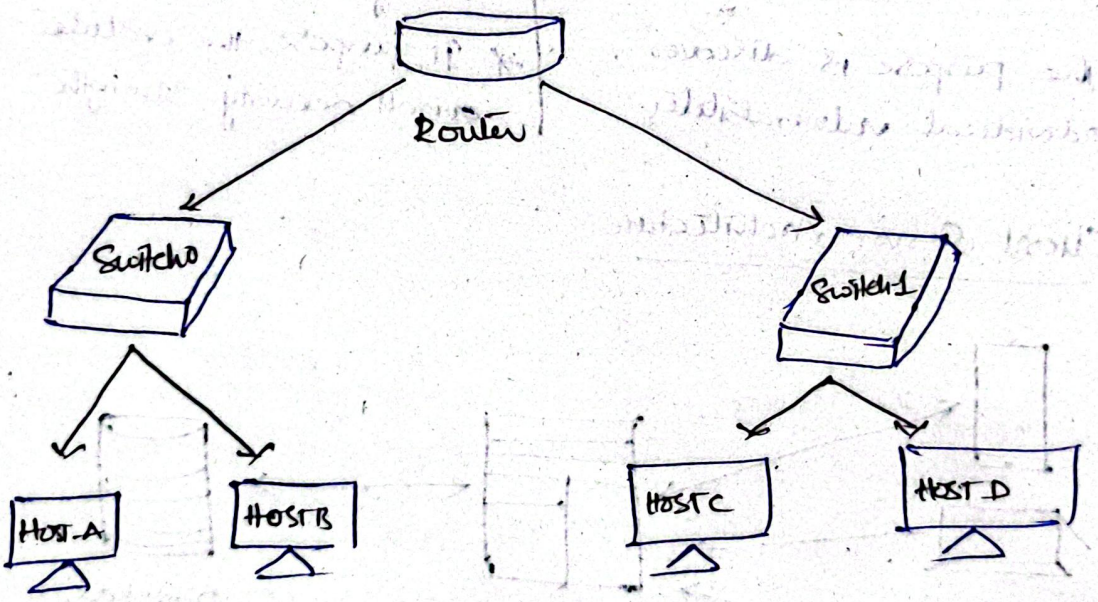
Client Server Architecture



* The client server architecture helps in dividing work between the user side (client) and the system side (Server)
* The client sends a request and the server processes the request and sends a response which makes communication organized
* It allows central storage of data, so users donot need to store everything on their own devices.

* The Security is better because important data and access control are managed by the Server.
* The many users can access the same services at the same time without affecting each other.
* It maintence becomes easier since updates are done on the Server not on every client devices.
* It supports scalability meaning more users can be added by improving the Server
* This architecture is widely used in websites, mobile apps online banking and cloud systems.

How Data Packets Travel Across Networks:



* The data is first broken into small units called packets before being sent over the network
* In each packet carries source and destination address information.
* The packets can travel through routers and switches which decide the best path.
* The different packets may take different routes depending on network traffic

* At the destination packets are reassembled in the correct order to form the original data.

Eg:

When you open a website the page data is split into packets sent through different network routes and then rejoined in your browser to display the page.

Server Software:

The Server software is a program that runs on a computer and provides services or resources to other computers (clients) over a network

→ The Server software listens to client requests and sends responses.

XAMPP:

The XAMPP is a cross platform server packages used to run the web applications on personal computer.

X → Cross platform
A → Apache
M → MySQL
P → PHP
P → Perl

* It works on windows, linux and mac os.
* It is mostly used to learnings, testing and develop -ment side.
* It is Easy to install and use.
* It contains phpMyadmin for database
* The projects can runs offline without internet.

Eg:

→ It is used to run DVWA, PHP projects for colleges.
→ It commonly used in cybersecurity lab and practise setups.

WAmp

Windows-based local server environment

W → Windows
A → Apache
M → MySQL
P → PHP

* It works only on windows
* It similar works like XAmpp but limited to windows
* It is mainly used for windows developers.
* It has simple system tray control panel
* They have good integration windows system files.

Eg:
→ It is used to php website on windows.
→ It is suitable for small scale local web projects.

LAMP:

The Lamp is a server stack used mainly on linux systems especially for production servers.

L → Linux
A → Apache
M → MySQL
P → PHP / Python / perl

* It is used on real hosting servers.
* It has more secure and stable
* It requires command line knowledge.
* It has widely used in cloud and enterprise servers.

Eg: It used to host live websites and web applications.
→ They common stack for professional web hosting