Day 1 of the #100DaysHackingChallenge

I always believed hacking meant shortcuts and illegal tricks shown in movies—hoodies, scrolling green text, and guessing passwords in three tries.

On Day 1, my perspective completely changed. I understood that real hackers don't start with tools; they start with **white-hat fundamentals**.

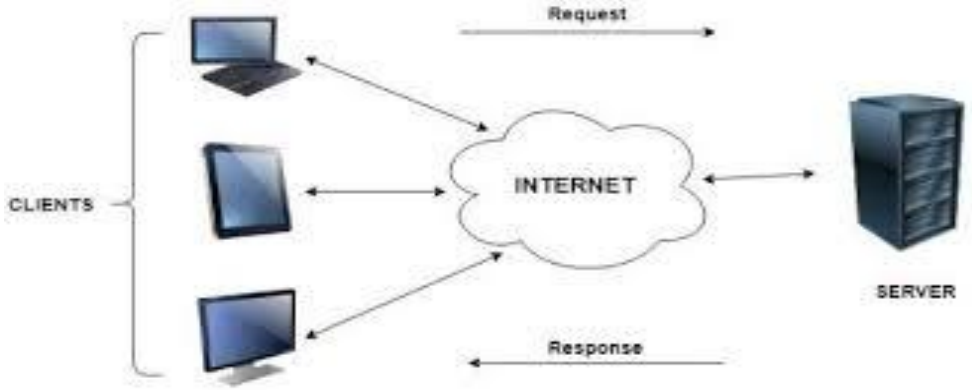
Here is what my first day of deep-diving into the real world of cybersecurity looked like:

1. The Foundation: Computer Networking

Before you can break into a system, you have to know how it connects. It’s about knowing the "pipes" of the internet.

We started with the role of **Client-Server Architecture**. This is the fundamental handshake of the web.

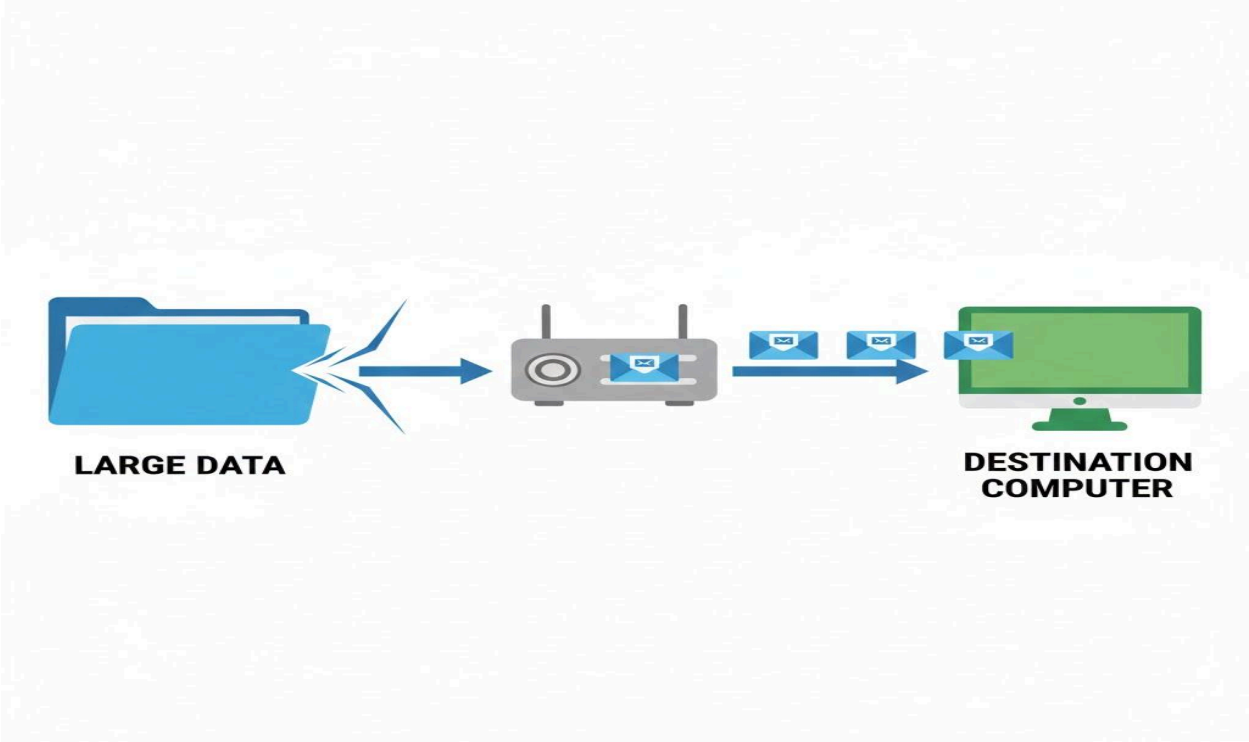
- **The Client:** This is you (your laptop or phone browser) making a "request" for information.
- **The Server:** A powerful, remote computer that receives that request and "serves" the data back to you.



2. How Data Packets Travels

I learned that when I send a photo or an email, it doesn't magically teleport in one piece.

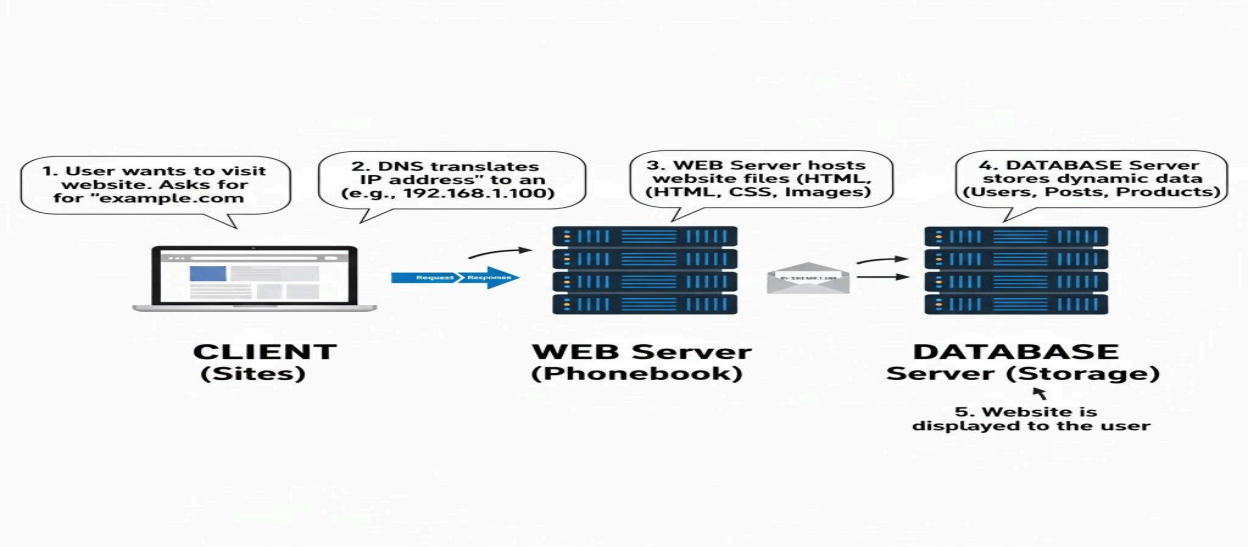
We covered how **data packets travel**. Your data gets chopped up into tiny digital envelopes called "packets." These packets speed along cables, get directed by routers (acting like digital traffic cops), and get reassembled in the right order at the destination.



3. Not All Servers Are Equal

Just like buildings have different purposes (banks, libraries, post offices), I learned how **different types of servers function**.

- A **Web Server** holds the website files you look at.
- A **DNS Server** is the internet's phonebook, turning "https://www.google.com/search?q=google.com" into an IP address like 142.250.190.46
- A **Database Server** is an organized filing cabinet for storing massive amounts of user data.

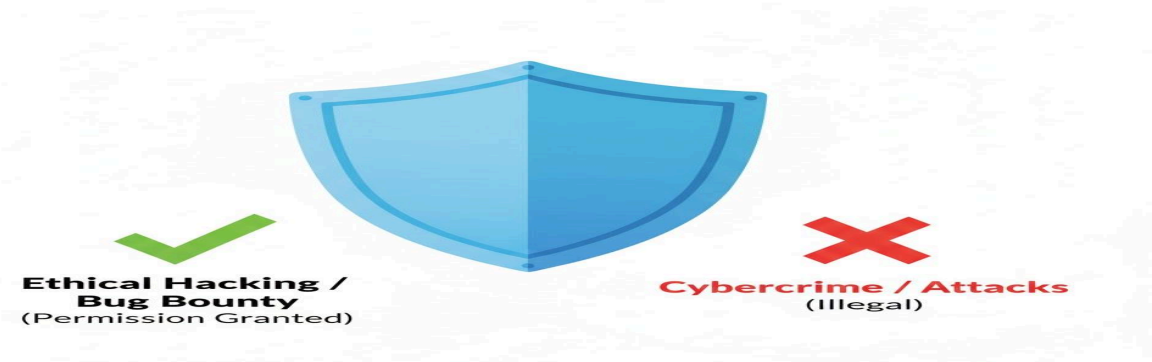


4. The Rules of Engagement : (Ethical Boundaries)

This foundational networking knowledge is what real cybercrime investigators and security professionals rely on before touching any tool.

But the biggest differentiator between a "hacker" and a "cybercriminal" is understanding **Legal & ethical boundaries**.

- I learned what **Bug Bounty Hunting** really is: legally getting paid by companies to find flaws in their systems so they can fix them.
- I learned how **Penetration Testing** (a structured, authorized security drill) differs entirely from random, illegal attacks.



5. The North Star of Security: The CIA Triad

Finally, the day concluded with the most critical concept in InfoSec. Every security measure we take is designed to protect one of three things in the **CIA Triad**:

- **C - Confidentiality:** Keeping secrets safe from people who shouldn't see them.
- **I - Integrity:** Ensuring data hasn't been untruthfully changed or tampered with.
- **A - Availability:** Ensuring systems are actually up and running when users need them.