7-Day Ethical Hacking Starter Kit

by Sanjay Singh (@icybersanjay)

Helping beginners take their very first confident step into cybersecurity — without confusion, fear, or overwhelm.

👋 Welcome

I'm Sanjay Singh — cybersecurity practitioner, trainer, and content creator.
I created this guide for students and beginners who want to get into cybersecurity but don't know where to start. Maybe you've watched YouTube videos, heard about hacking tools, or seen posts about high-paying cyber jobs…

…but you still feel:

• "Where do I actually begin?"
• "What should I study first?"
• "Do I need coding?"
• "How do I practice legally?"
• "How do I become job-ready?"

If that sounds like you — this guide is for you.

My goal is simple:

- Make cybersecurity learning clear, friendly, ethical, and beginner-friendly
- Help you build confidence & fundamentals
- Show you how to become job-ready — step-by-step

No jargon.
No shortcuts.
No illegal nonsense.

Just honest guidance — written like a mentor speaking to you.

You'll go through 7 structured days of learning, followed by powerful bonus sections like labs, roadmaps, resume help, role guides, and study planners.

By the end, you'll feel:
✓ clearer
✓ more confident
✓ more prepared
✓ more "industry-aware"

And that's a BIG win for a beginner

Welcome to your cybersecurity journey
— Cyber Sanjay

Disclaimer — Legal & Ethical Responsibility

Cybersecurity exists to **protect people, data, and systems.**

This guide teaches:
✓ concepts
✓ awareness
✓ legal practice
✓ security mindset

It does **NOT** encourage or support illegal activity.

Illegal actions include:
• hacking systems without permission
• accessing private data
• bypassing security controls
• testing real websites without approval

Doing so can lead to:
⚠️ legal trouble
⚠️ academic consequences
⚠️ loss of career opportunities

You agree to:
✓ practice only in legal labs
✓ follow responsible disclosure
✓ respect privacy
✓ stay ethical always

Everything in this guide is for **education & career development only.**

Your ethics define your future.

And I want your future to be bright 🙂

— **Cyber Sanjay**

How To Use This Guide?

This is not a "*read once and forget*" PDF → This is your **learning companion**.

Here's the best way to use it:

Step 1 — Read One Chapter a Day
Each day builds on the previous one.
Spend **30–60 minutes daily** — that's enough.

Step 2 — Keep a Learning Journal
Write:
• new concepts
• tools
• doubts
• reflections

- Professionals document everything — and now, so will you.

Step 3 — Practice Only in Legal Labs
Such as:
✓ TryHackMe
✓ OverTheWire
✓ PortSwigger Academy

- Never test random websites.

Step 4 — Use the Bonus Resources
At the end, you also get:
• Beginner Lab Roadmap
• 30-Day Study Plan
• Responsible Disclosure Templates
• Career Role Roadmaps
• Linux + Web Cheat Sheets
• Glossary
• Learning Roadmap

- This turn learning into **real-world preparation.**

Step 5 — Go Slow. Stay Consistent.
You don't need to become an "expert hacker".
Just focus on:
✓ understanding
✓ curiosity
✓ ethics
✓ discipline

- That's what employers value.

Who This Guide Is For?

This guide is designed especially for:

Students

who want to explore cybersecurity properly

Beginners

with little or zero experience

Curious Learners

who like technology and problem-solving

Job-Seekers

who want structure & clarity instead of random tutorials

Indian Students

who want realistic guidance for the Indian market

- Let's Learn Together Let's Grow Together

This guide is NOT for

❌ People looking for illegal hacking

❌ Shortcut seekers

❌ Those wanting instant high-salary magic

❌ People unwilling to learn step-by-step

Real cybersecurity = patience + ethics + curiosity.

And if you have those —

you're exactly where you need to be.

A Personal Note From Cyber Sanjay

I started exactly where you are now — curious, confused, and searching for direction.

So, I built this guide to be the **starting point I wish I had**.

My promise to you:

I will keep things:

✓ simple

✓ practical

✓ ethical

✓ honest

If you stay consistent and learn with heart,

you **WILL** grow.

And one day —

you'll look back and say:

"This guide was my first real step into cybersecurity."

That will make me happier than anything 😊

Let's begin your journey.

One day at a time.

One concept at a time.

Ethically. Confidently. Proudly.

— ***Cyber Sanjay***

Chapter 1 — Introduction & Safe Lab Setup

Learning Objectives

By the end of this chapter, you will:

✓ Understand what ethical hacking truly means

✓ Know the difference between legal & illegal hacking

✓ Learn why cybersecurity matters

✓ Set up a safe beginner-friendly learning environment

✓ Start your learning journal

No technical background required.

What Is Ethical Hacking?

Ethical hacking simply means:

“Learning how hacking works so you can protect systems — with permission and legal approval.**”**

Cybercriminals break systems to harm people.
Ethical hackers test systems to protect people.
Same skills.
Different purpose.

Example

A locksmith studies how locks can be broken…
so they can design better locks.

Ethical hackers do the same for computers and networks.

⚠️ Very Important: Permission Matters

Hacking **without permission** is illegal—even if your intention is good.

Ethical hacking always follows:

✓ Permission

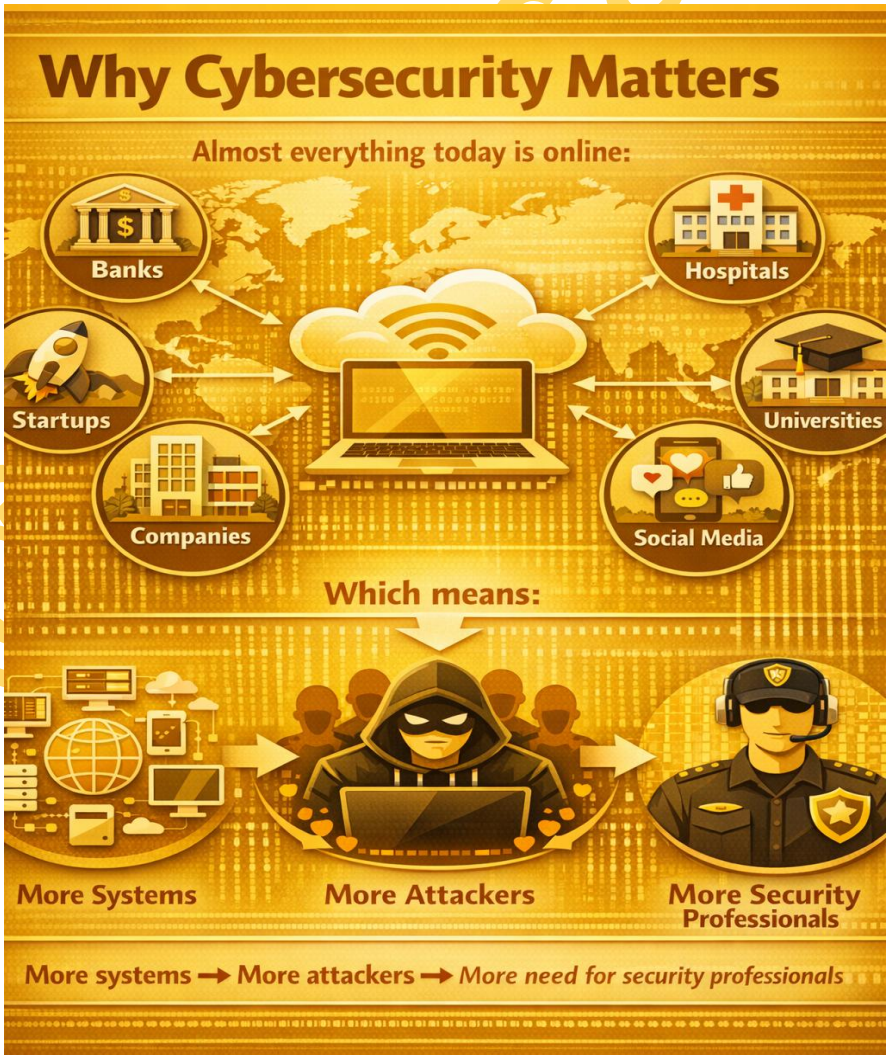
✓ Rules

✓ Legal Scope

✓ Responsible behaviour

This is the foundation of your career.

Why Cybersecurity Matters



Almost everything today is online: banks, hospitals, universities, social media, companies, startups, etc.

Which means: **More systems → more attackers → more need for security professionals**

Cybersecurity protects:

✓ data
✓ people
✓ businesses
✓ trust

And skilled beginners are in high demand.

Myth-Busting for Beginners

❌ **"I need to be a coding expert"**

Not at all. Coding helps, but it's not step one.

❌ **"Cybersecurity is only for toppers"**

No. It's for curious learners.

❌ **"Hacking means breaking into banks"**

No. Real work is more about testing & securing.

But the Fact ⋙ If you stay ethical and consistent, you can build a real career here.

Your Safe Learning Environment

We NEVER test random websites. So, we use **legal practice platforms**.

Option 1 — Online Labs (Recommended for Students)

✓ TryHackMe

✓ PortSwigger Academy

✓ OverTheWire

No setup needed. Works on most laptops.

Option 2 — Virtual Machine (Later Stage)

Tools like:

• VirtualBox
• Kali Linux

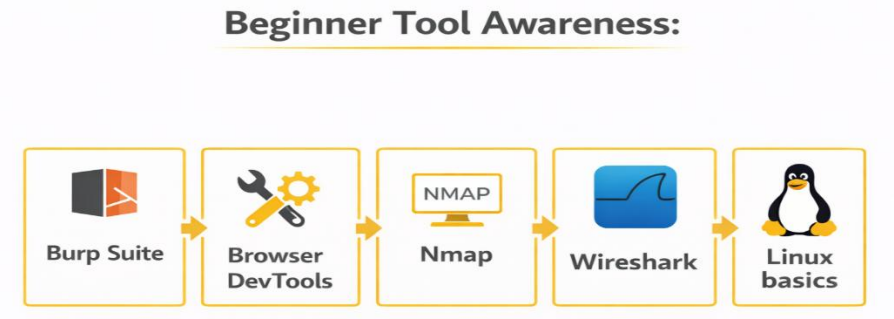
This is useful — but optional for now.

We'll introduce it slowly later.

Beginner Tool Awareness (No Setup Required Yet)

You will slowly learn about tools like: Burp Suite, Browser DevTools, Nmap, Wireshark, Linux basics.

But not today.
Today is about clarity.



Create Your Cybersecurity Learning Journal

This is your first real task.

You can use: Notebook or Google Docs

Add sections:

• New terms I learn
• Tools I discover
• My questions
• My reflections

Professionals document everything.

Start today 😊

Chapter 1 Checklist

Tick what you understand:

- I know what ethical hacking means
- I understand permission is essential
- I know why cybersecurity matters
- I understand I don't need to be a genius to start
- I created my learning journal

If you ticked 3+

➢ You're on track…

Well Done!!! Keep Going…and Remember Consistency is the Key ✌️

Know yourself

Write short answers:

1. Why am I interested in cybersecurity?
2. What scares me about it?
3. What excites me the most?

This helps you stay motivated…

End of Chapter 1 — Key Takeaways

✓ Ethical hacking = legal security testing

✓ Permission & ethics are the foundation

✓ Cybersecurity protects real people

✓ You don't need to be perfect to start

✓ Small daily progress matters

You've officially begun your journey -

Warm-Up Questions

Q1. What is ethical hacking?

Q2. Why do companies need cybersecurity?

Q3. Why is permission important in hacking?

Practice short, clear answers

Chapter 2 — OSINT & Recon: How Hackers Collect Information (Legally & Safely)

Learning Objectives

By the end of this chapter, you will:

✓ Understand what **reconnaissance (recon)** means
✓ Learn what **OSINT** is and how it's used legally
✓ See how information is gathered from public sources
✓ Build your security awareness mindset
✓ Practice passive research safely

What Is Reconnaissance?

Before attacking, criminals **collect information first**.

Ethical hackers also collect information…

…but only to **help protect systems**.

That information-gathering step is called:

Reconnaissance (Recon)

- Collecting information about a system, organization, or target to understand it better — before any testing.

Think of recon like **research before an exam**.

You learn:

- What exists
- How things are structured
- What technologies are used

No breaking in.
No illegal actions.
Just **smart observation.**

What Is OSINT?

OSINT stands for: **Open-Source Intelligence**

Meaning:

📌 Collecting information from publicly available sources.

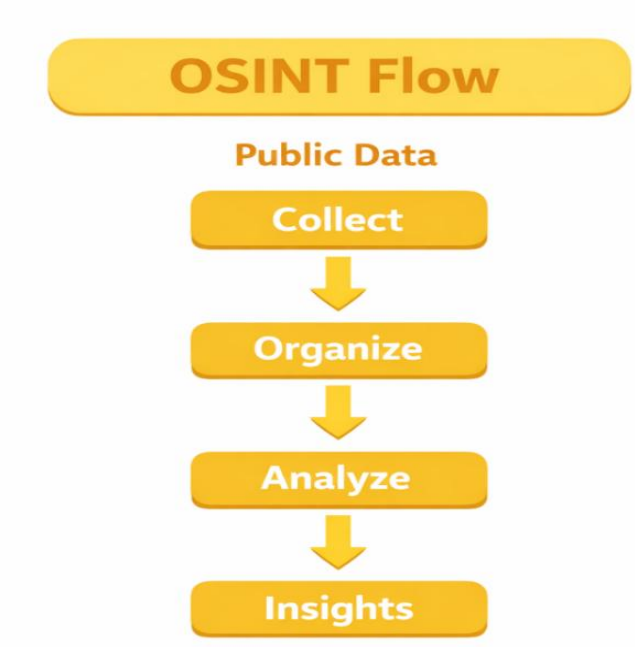
These include:

✓ search engines
✓ websites
✓ blogs
✓ job postings
✓ social media
✓ public reports
✓ forums
✓ GitHub
✓ PDFs
✓ news

Everything is already public.

Nothing is hacked.

Simple Diagram — OSINT Flow



Ethical hackers use insights to improve security.

Criminal hackers use insights to attack.

Same information.
Different intention.

Legal vs Illegal

✓ Legal

- Reading public websites
- Using Google
- Viewing company profiles
- Checking job listings
- Researching technologies used

❌ Illegal

- Logging into accounts
- Bypassing security
- Accessing private data
- Testing real websites without permission

When confused:

🚨 Stay on the safe side.

Ethics first

Career matters.

Types of Recon

1. Passive Recon

You only **observe public information.**

Examples:

✓ reading job descriptions
✓ checking company tech blogs
✓ scanning public documents

This is SAFE and LEGAL.

2. Active Recon (Advanced — Later)

You interact with the system.

Examples:

✓ port scanning
✓ packet inspection

This requires permission and should NOT be done on random websites.

For now, we focus ONLY on:

📌 **Passive Recon**

Real-World Job Use

Recon is used in:

✓ Pentesting
✓ Threat Intelligence
✓ SOC monitoring
✓ Incident response

Interviewers expect at least:

What is OSINT?

- If you can answer confidently, you stand out…But Don't forget to Give a Try

Some Simple & Real OSINT Examples

Example 1 — Job Listing

A company lists: "We are hiring Linux admins with AWS & Nginx experience."

From this you learn:

✓ They use Linux
✓ AWS cloud
✓ Nginx web server

This helps security teams prepare better defenses.

Example 2 — Tech Blog

A company blog mentions: “We migrated to React frontend & Node backend.”

Security teams learn what tech stack is in use.

Awareness = better protection.

Chapter Checklist

Let’s have Revision…Write in your journal:

- I understand what recon means
- I know OSINT = public info research
- I can explain passive recon
- I understand legal limits
- I see why recon matters in jobs

If you answer 4+

- ➢ You’re learning the right way… Keep Going 👍

Practical Exercise

Exercise 1 — Google Like a Researcher

Pick any **well-known company** in India: Tata | Infosys | Wipro | HCL | Zomato | Paytm

Search: Company Name + Careers

Now observe:

✓ Technologies listed
✓ Security roles mentioned
✓ Skills required

Write in your journal:

- What skills are common?
- Do they mention cybersecurity?
- Do they mention Linux/cloud/web?

📌 ***You’re building awareness.***
That’s step one to becoming employable.

Exercise 2 — OSINT on Yourself (Safe & Fun)

Google your name.

Ask yourself:

✓ What information is public?
✓ Do I want this visible?
✓ Is my LinkedIn professional?

- This builds **privacy awareness.**

Know Yourself

Write short answers:

1. What surprised me about OSINT?
2. Did I notice how much is public online?
3. Do I now see why companies need security teams?

- *Always Remember, Self-awareness = Growth.*

Key Takeaways — Chapter 2

✓ Recon = information gathering
✓ OSINT = public data intelligence
✓ Passive recon is legal
✓ Hackers & defenders both use OSINT
✓ Awareness improves security

And you are **slowly learning to think like a security professional.**

- *Be Calm. Structured. Ethical.*

Warm-Up Questions

Q1. What is OSINT?
Q2. What is the difference between passive & active recon?
Q3. Why is recon important in cybersecurity?

Practice answering with clarity — not jargon.

Chapter 3 — Networking Basics: How the Internet Actually Works

Learning Objectives

By the end of this chapter, you will:

✓ Understand what a network is
✓ Learn what IP addresses, DNS, servers, and ports are
✓ Visualise what happens when you open a website
✓ Connect networking basics to real cybersecurity jobs

- *No formulas. No complex theory.* ***Just clarity.***

What Is a Network?

A **network** simply means:

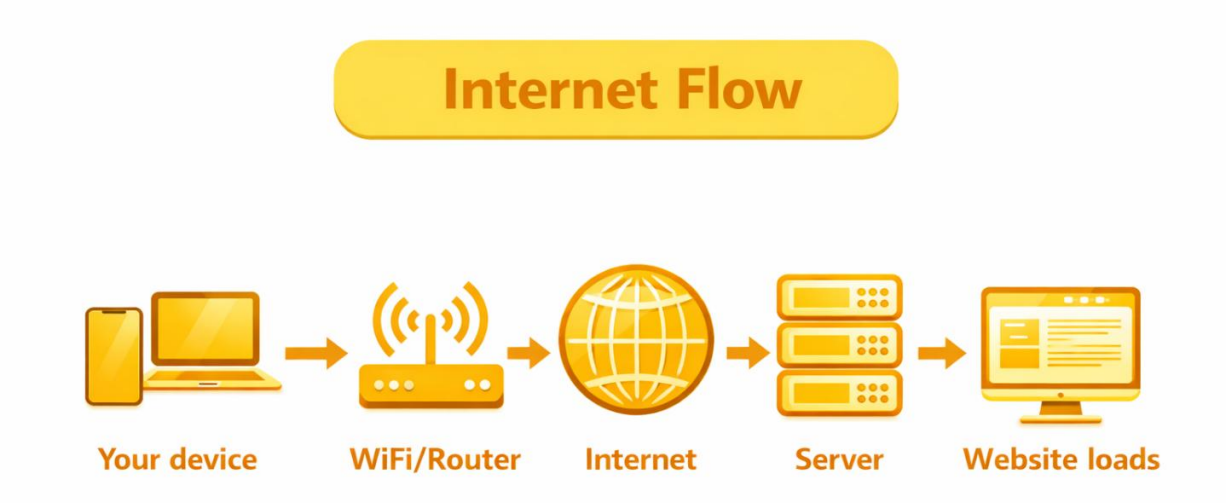
> *Two or more devices connected so they can share information.*

Examples:

✓ Your phone connected to Wi-Fi
✓ College computers connected to a lab network
✓ The internet — the largest network on Earth

That's it.
Networking = communication between devices.

Simple Internet Flow



Your device sends a request.
A server responds with the webpage.

Done.

IP Address — The Home Address of Devices

Every device on a network has an **IP address**.

Just like your home has an address so deliveries reach you…

Your device needs an IP address so data reaches it.

Example of an IP: 192.168.1.10

So, remember:

- **IP Address = Identity of a device on a network**

Private vs Public IP

Private IP

Used **inside homes or offices**

Examples:

192.168.x.x
10.x.x.x

Public IP

Visible on the internet.
Assigned by your Internet Provider.

So:

✓ Private IP → internal network
✓ Public IP → global internet

What Is a Server?

A **server** is just a powerful computer that:

✓ stores websites
✓ processes requests
✓ sends information to users

Examples:

- Google servers
- Netflix servers
- Banking servers

Servers usually sit in data centres — not in bedrooms 😉

DNS — The Contacts App of the Internet

You don't type: 142.251.33.206

You type: google.com

DNS converts website names → into IP addresses.

Just like:

You tap "Mum" in your phone
but the phone dials the number in the background.

DNS = name-to-number converter.

Ports — The Doors to a Computer

Imagine a house with multiple doors.
Each door has a purpose… Right?

*Computers have **ports**, which work like doors for different services.*

Examples:

Port	Use
80	Normal websites (HTTP)
443	Secure websites (HTTPS)

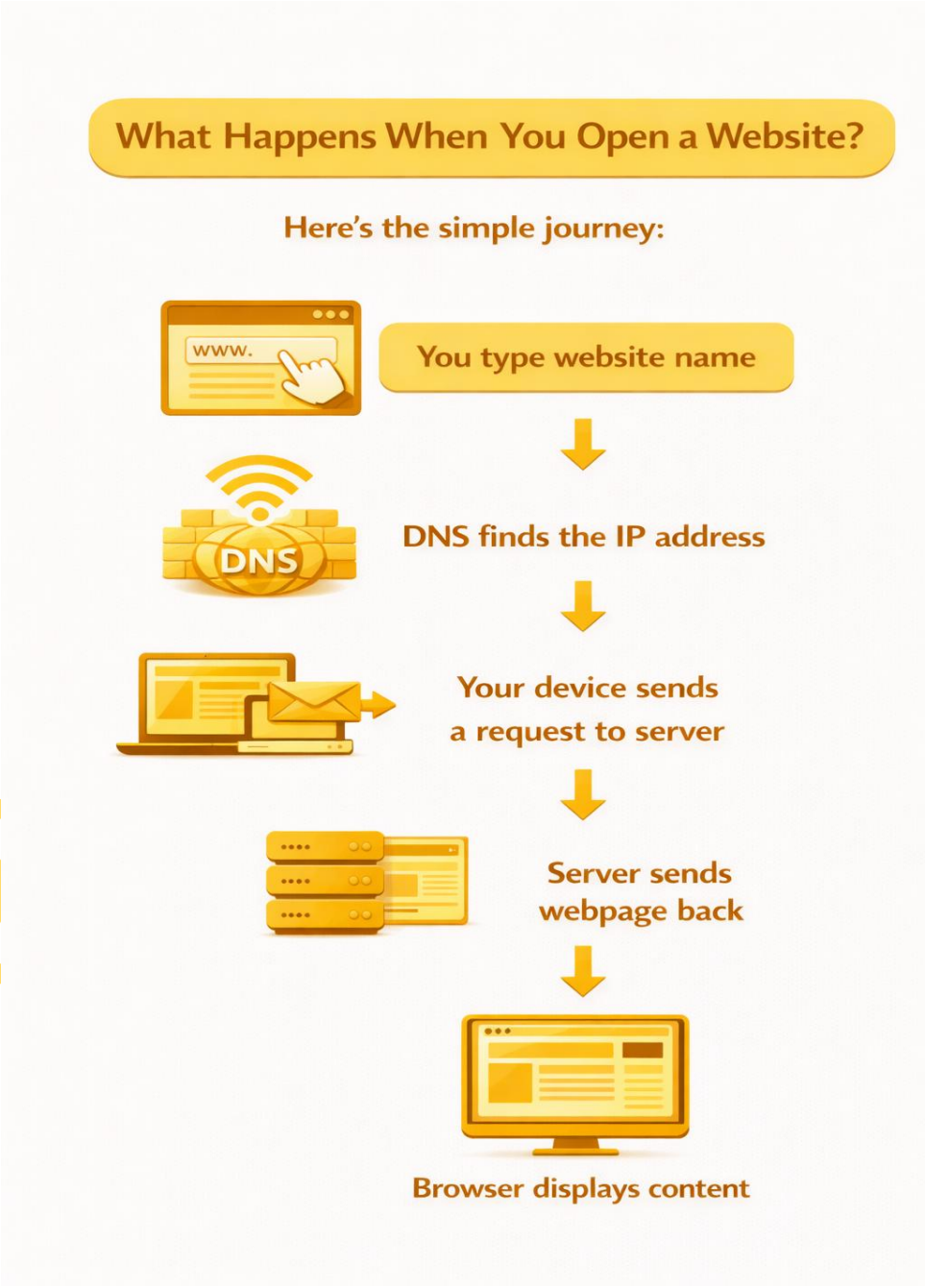
22	Remote login (SSH)

So, when you open a website:

You enter through Port 80 or 443

- Ethical hackers often test whether these “doors” are secure.

What Happens When You Open a Website?



- Millions of these tiny conversations happen every second.

Why Networking Matters in Cybersecurity

Almost every cyber-attack travel through a network.

So basic networking is expected in roles like:

✓ SOC Analyst
✓ Security Analyst
✓ Pentester
✓ Threat Hunter
✓ Incident Responder

Interviewers commonly ask:

Q. What is an IP address?
Q. What is DNS?
Q. What happens when you type a URL?

Today's chapter prepares you for that.

Networking Basics — Quick Checklist

Check out yourself and write in your journal:

- I understand what a network is
- I know what an IP address means
- I know the difference between public & private IP
- I understand what a server is
- I know DNS converts names to IPs
- I know ports work like doors

If you answer more than 4

➢ your foundation is getting stronger.

Practical Exercises

Exercise 1 — Find Your Public IP

Search on Google: What is my IP

Note it in your journal.

This makes networking real — not theory.

Exercise 2 — Look Up a Website IP

Search: DNS lookup tool

Enter a website like: google.com

See its IP.

- That's DNS in action.

Exercise 3 — Explain Networking in One Line

Write in your journal:

- *Networking is devices communicating using IP addresses.*

Short. Clear. Professional.

Know yourself

1. Do I now feel less scared of networking?
2. Can I explain DNS in simple words?
3. Do I understand why security jobs care about networks?

- Clarity builds confidence.

Key Takeaways — Chapter 3

✓ Networks allow devices to communicate
✓ IP = device address
✓ DNS = converts name → IP
✓ Server = powerful computer storing websites
✓ Ports = service doors
✓ Networking is the base of cybersecurity

- Solid fundamentals = stronger career.

Warm-Up Questions

Q1. What is an IP address?
Q2. What is DNS and why do we need it?
Q3. What happens when you open a website?
Q4. What is a server?
Q5. What are ports?
Practice giving short, clear answers.

Chapter 4 — Web Security Basics: How Websites Really Work

Learning Objectives

By the end of this chapter, you will:

✓ Understand how websites work behind the scenes
✓ Learn what a vulnerability is
✓ Get introduced to common web security risks
✓ See why companies hire ethical hackers
✓ Connect concepts to real-world security jobs

This chapter builds the foundation for web security.

What Is a Website — In Simple Words

When you visit a website like: amazon.in

you're actually connecting to a **server** — a powerful computer that:

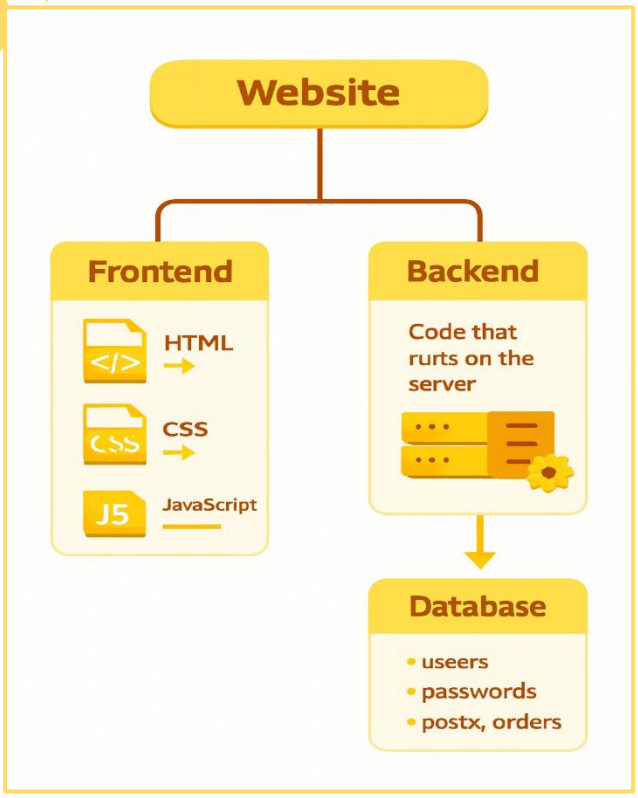
✓ stores the website
✓ processes your request
✓ sends information back to your browser

A typical website has these parts:

Frontend (what you see):
HTML → structure
CSS → design
JavaScript → interaction

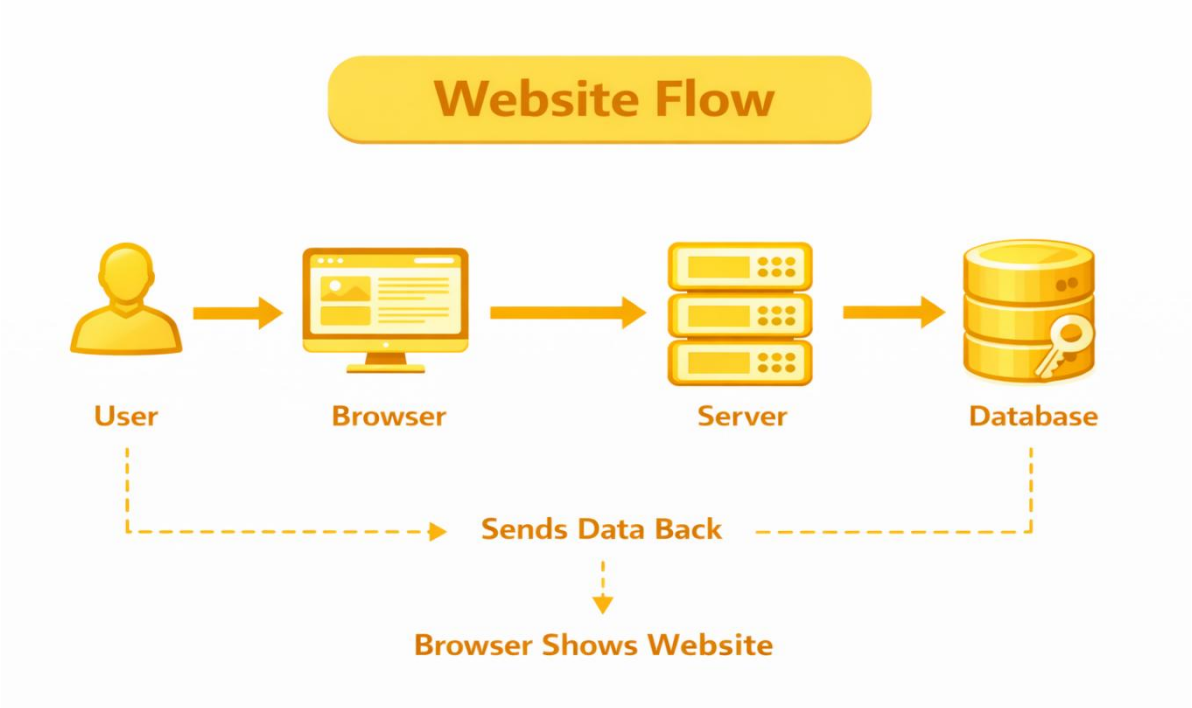
Backend (behind the scenes):
Code that runs on the server
Business logic

Database:
Stores information like:
users, passwords, posts, orders



- Everything together = web application.

Simple Website Flow



- Every click is just a request and response.

What Is a Vulnerability?

A **vulnerability** means:

> *A weakness in a system that can be exploited if not fixed.*

Examples:

✓ bad coding
✓ weak passwords
✓ misconfigured servers
✓ exposed data

Ethical hackers find these weaknesses
→ report them
→ help companies secure systems.

- That's the job.

Why Do Vulnerabilities Exist?

Because:

✓ humans write code
✓ systems are complex
✓ deadlines create mistakes
✓ configurations break

So even big companies like Google or Meta sometimes have security issues.

📌 That's why **bug bounty programs and pentesters exist.**

Common Web Vulnerabilities

Let's understand a few at a simple level — no technical depth yet.

SQL Injection (SQLi)

Websites store data in databases. If user input is not properly checked, an attacker can send **malicious queries** instead of normal data.

This may allow:

⚠️ viewing data
⚠️ modifying data

Ethical hackers test for such issues to protect users.

Cross-Site Scripting (XSS)

If a website allows user input and does **not properly sanitize it**, scripts can run inside the page.

This may allow:

⚠️ stealing cookies
⚠️ redirecting users
⚠️ injecting malicious code

Again — ethical hackers help identify and fix this.

Broken Authentication

If login systems are weak:

⚠️ accounts can be accessed
⚠️ sessions can be hijacked

This is a major real-world risk.

Security Misconfigurations

Sometimes the problem isn't code.

It's configuration like:

⚠️ default passwords
⚠️ unsecured admin portals
⚠️ debug info visible
⚠️ open storage buckets

*This is one of the **most common real-world issues**.*

OWASP Top 10 — Industry Standard

You will/might have hear this everywhere in cybersecurity.

OWASP Top 10 = A list of the 10 most critical web application security risks.

Companies use it as a **guideline for security.**

📌 *You don't need to memorize it yet — just recognize the term.*
This is very useful for interviews.

Job Relevance — Why This Matters

Web security knowledge is used in:

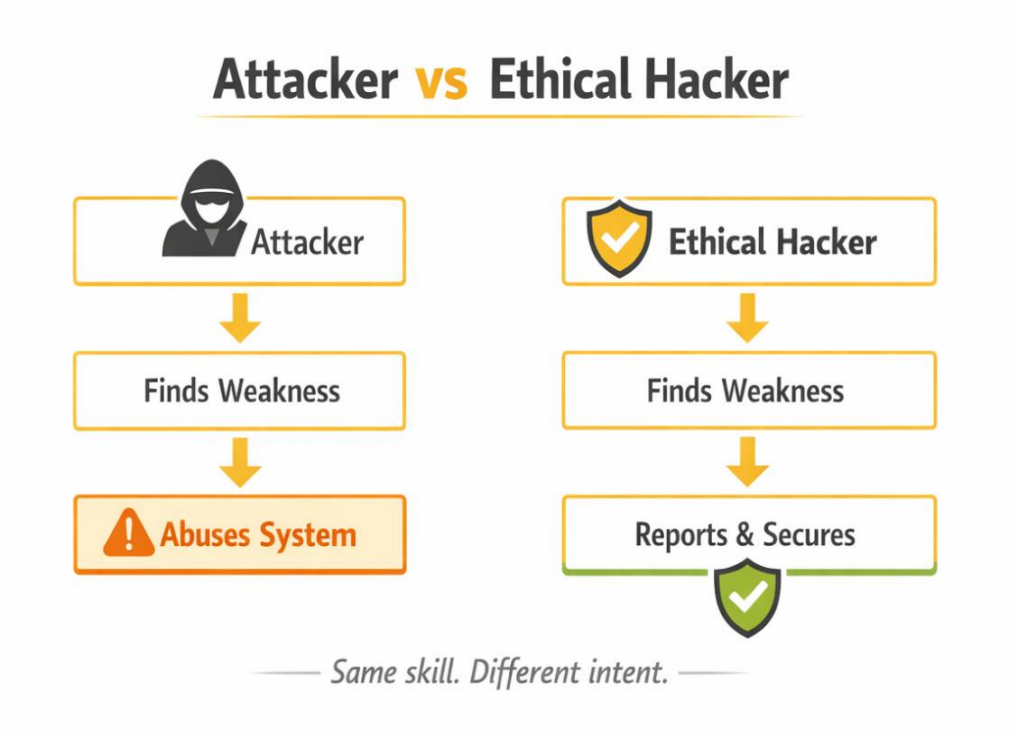
✓ Pentesting
✓ Bug bounty
✓ SOC monitoring
✓ Application security
✓ Security auditing

Interviewers often ask:

Q. What is SQL Injection?
Q. What is OWASP Top 10?
Q. What is a vulnerability?

This chapter prepares you to answers confidently.

Simple Diagram — Attacker vs Ethical Hacker



Same skillset.
Different intention.
Different outcome.
- Be Ethical

Web Security Basics — Checklist

Analysis yourself:

- I understand what a web application is
- I know what a vulnerability means
- I've heard of SQL Injection
- I've heard of XSS
- I know OWASP Top 10 exists
- I understand why security testing is needed

If you answer most of these
- ➢ you're building real industry awareness.

Keep Going…

Practical Exercises

Exercise 1 — Observe a Login Page

Open any well-known login page:

✓ Gmail
✓ LinkedIn
✓ Instagram

Ask yourself:

- What happens if login fails?
- Is there multi-factor authentication?
- Why must this be secure?

This builds awareness.

Exercise 2 — Explain Vulnerability in One Line

Note: "*A vulnerability is a weakness in a system that can be exploited*."

- Simple. Clear. Professional.

Exercise 3 — Google OWASP Top 10

Just read the headings.

No pressure to understand details yet.

Know Yourself

1. Does web security feel less mysterious now?
2. Can I explain what a vulnerability is?
3. Do I understand that ethical hacking helps companies stay safe?

- *Honest reflection builds clarity.*

Key Takeaways — Chapter 4

✓ Websites = frontend + backend + database
✓ Vulnerability = weakness in a system
✓ SQL Injection & XSS are common risks
✓ OWASP Top 10 is an industry framework
✓ Ethical hackers protect systems
✓ Web security is a core cybersecurity skill

This knowledge makes you more job-ready.

Warm-Up Questions

Q1. What is a vulnerability?
Q2. What is SQL Injection?
Q3. What is XSS?
Q4. Why do companies need web security testing?
Q5. What is OWASP Top 10?

Try answering briefly and clearly.

Chapter 5 — Vulnerabilities & CVEs: How the Industry Tracks Security Risks

Learning Objectives

By the end of this chapter, you will:

✓ Understand what a vulnerability means in industry terms
✓ Learn what a **CVE** is and why it exists
✓ Understand severity levels and **CVSS scoring**
✓ See how real security teams track and fix risks
✓ Prepare for common beginner interview questions

This chapter connects you directly to how cybersecurity works in real companies.

What Is a Vulnerability?

You already learned the basic idea:

> *A vulnerability is a weakness in a system that can be exploited.*

In the real world:

✓ software has bugs
✓ systems are misconfigured
✓ code has mistakes
✓ humans make errors

These weaknesses — if discovered — are reported, tracked, and fixed.

But here's the question…

How does the world track thousands of vulnerabilities every year?

*That's where **CVE** comes in.*

What Is CVE?

CVE stands for: **Common Vulnerabilities and Exposures**

Meaning:

> CVE is a public identification number assigned to a known security vulnerability.

Think of it like:

- A roll number for each vulnerability
- A unique ID everyone in the world can refer to

Example: CVE-2021-44228

This one is related to the well-known Log4j vulnerability.

- Google it

Simple Breakdown of a CVE ID

Example: CVE-2023-12345

Part	Meaning
CVE	It belongs to the CVE system
2023	Year published
12345	Unique ID number

So, when security teams say: *"Patch CVE-2021-44228"* everyone knows exactly which vulnerability they mean.

- No confusion.

Why CVEs Exist

Cybersecurity is global.

So, CVEs help:

✓ companies
✓ researchers
✓ governments
✓ security vendors

talk about the **same issue using the same reference ID.**

This standardization is critical.

Severity Levels — How Dangerous Is It?

Not all vulnerabilities are equal.

So, we use: **CVSS — Common Vulnerability Scoring System**

Scores range from **0 to 10**

Score	Level
0–3.9	Low
4.0–6.9	Medium
7.0–8.9	High
9.0–10	Critical

Meaning in simple words

Low
Minor risk. Not urgent.

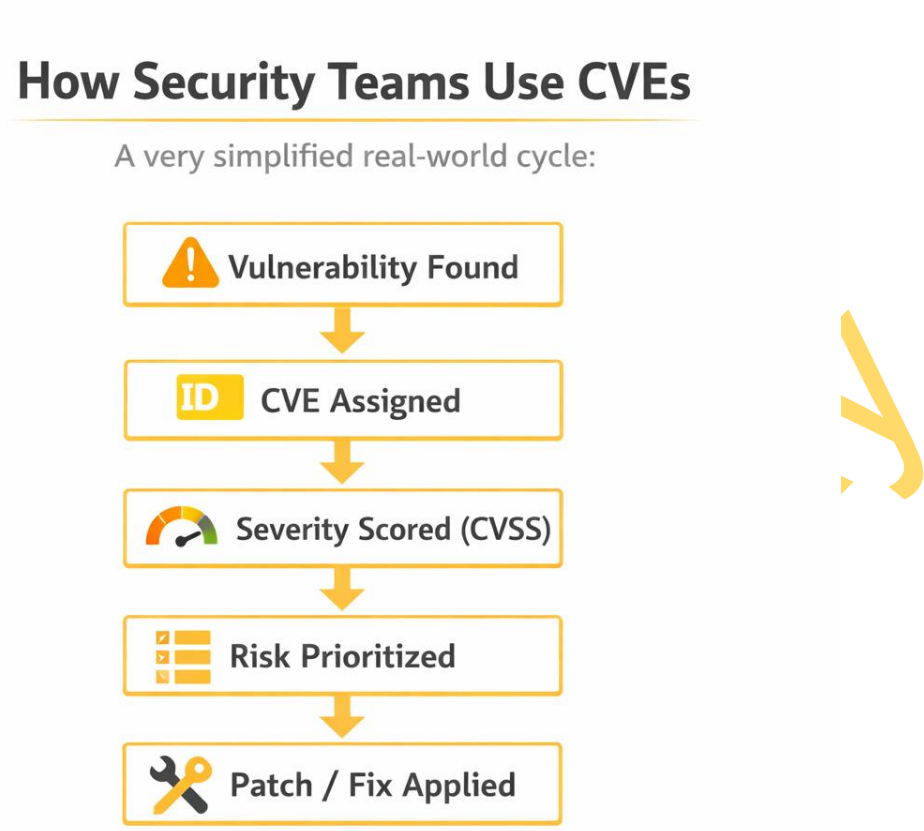
Medium
Needs fixing, but not emergency.

High
Serious risk. Needs priority attention.

Critical
Extremely dangerous. Fix immediately.

This helps companies decide: What should we fix first?

How Security Teams Use CVEs



This process runs daily inside cybersecurity teams.

Real Example — React2Shell (2025)

CVE ID: CVE-2025-55182

Severity:

🟥 Critical (10/10)

Impact:

✓ Millions of application affected worldwide
✓ Companies rushed to patch
✓ Security teams worked nonstop

This event proved:

Cybersecurity is not optional → It protects businesses and people.

Industry-Ready Checklist

Check yourself:

- I know what a vulnerability means
- I understand what CVE stands for
- I know why CVEs exist
- I understand severity levels
- I know CVSS measures risk

If you answer most of these

- ➢ you're developing real-world awareness.

Well Done!!!

Job Relevance — Where This Knowledge Is Used

You'll see CVEs everywhere in roles like:

✓ SOC Analyst
✓ Threat Intelligence
✓ Pentesting
✓ Security Analyst
✓ Vulnerability Management

Interviewers love asking:

Q. What is CVE?
Q. What does CVSS measure?
Q. What is a critical vulnerability?

You're now prepared to answer these clearly.

Practical Exercises

Exercise 1 — Search a Real CVE

Go to Google and type: CVE-2025-55182

Observe:

✓ description
✓ severity
✓ impacted systems

You don't need to understand everything — just recognize the structure.

Exercise 2 — Learn These One-Line Definitions

Write in your journal:

CVE = Public ID for security vulnerabilities
CVSS = System that scores severity

Short. Clear. Professional.

Exercise 3 — Severity Awareness

Write:

Low → small risk
Medium → moderate
High → serious
Critical → severe and urgent

This builds instinct.

Know Yourself

1. Do CVEs now feel less confusing?
2. Can I explain what severity means?
3. Do I understand why companies track vulnerabilities?

Clarity = confidence.

Key Takeaways — Chapter 5

✓ CVE = identification number for vulnerabilities
✓ CVSS = severity scoring system
✓ Critical issues need urgent fixes
✓ Security teams track & patch vulnerabilities daily
✓ This knowledge is highly relevant for jobs
✓ You are now speaking the language of the industry

This is a big milestone in your learning journey.

Warm-Up Questions

Q1. What is a vulnerability?
Q2. What is a CVE?
Q3. What does CVSS measure?
Q4. What is a critical vulnerability?
Q5. Why do companies track CVEs?

Practice answering in simple English.

Clear communication matters more than fancy terms.

Chapter 6 — Ethics, Law & Bug Bounties: Becoming a Responsible Security Professional

Learning Objectives

By the end of this chapter, you will:

✓ Clearly understand what is legal vs illegal in cybersecurity
✓ Learn what **Responsible Disclosure** means
✓ Understand **Bug Bounty** programs and how they work
✓ Build the ethical mindset expected in the industry
✓ Avoid mistakes that can destroy a career

This chapter protects you — not just technically, but professionally.

The Golden Rule of Cybersecurity

> **Testing or accessing any system without permission is illegal.**

Even if:

❌ you don't steal anything
❌ you're "just checking"
❌ you think you're helping

It is still unauthorized access — and it can be a crime.

Ethical hacking = ***permission + scope + responsibility.***

This mindset is non-negotiable.

Legal vs Illegal

Action	Legal ?	Why
Learning concepts	Yes	Education
Practicing in labs	Yes	Safe + authorized
Testing systems you own	Yes	You control it
Testing random websites	No	No permission
Accessing private data	No	Unauthorized
Breaking into accounts	No	Illegal

When you are unsure → Don't do it.

- *Your future career is more important than curiosity.*

What Is Responsible Disclosure?

Sometimes researchers find vulnerabilities in real systems.

The **professional way** to handle it is:

Identify issue
↓
Privately report to the company
↓
Give them time to fix it
↓
Share publicly only after approval (optional)

This is called: **Responsible Disclosure**

It protects:

✓ users
✓ companies
✓ reputations

Acting responsibly builds trust.

Why Companies Trust Ethical Hackers

Because professionals:

✓ respect privacy
✓ follow rules
✓ report clearly
✓ never exploit weaknesses

Trust is your biggest asset. If, Lose it once → career damage is permanent.

What Is Bug Bounty?

Bug Bounty programs allow ethical hackers to:

✓ legally test approved systems
✓ find vulnerabilities
✓ submit reports
✓ earn rewards, swag, or recognition

Platforms include:

- HackerOne
- Bugcrowd
- Intigriti

But ONLY within **approved scope.**

You must read:

✓ rules
✓ exclusions
✓ legal terms

before testing anything.

Bug bounty = permission-based testing.

Safe Path vs Risky Path

Always choose the safe path.

Real-World Workplace Ethics

In cybersecurity roles, you will often:

✓ sign NDAs
✓ follow security policies
✓ protect sensitive information
✓ behave professionally
✓ never disclose internal data

Ethics is part of your job description.

Professional Ethics Checklist

Analysis yourself:

- I understand that permission is essential
- I will only practice in legal environments
- I know what Responsible Disclosure means
- I understand Bug Bounty scope rules
- I value trust & professionalism

If you answer these

- ➢ you already think like a security professional.

Practical, Safe Learning Activities

Exercise 1 — Write Your Ethical Commitment

In your journal: “I will only practice cybersecurity in legal and authorized environments.”

Keeping this promise protects your future.

Exercise 2 — Read One Bug Bounty Policy

Search online: “HackerOne program directory”

Open any program and read:

✓ scope
✓ allowed testing
✓ not allowed testing

This gives real-world understanding.

Exercise 3 — Learn This Key Term

Write: **Responsible Disclosure = reporting vulnerabilities safely and privately to the owner.**

Short. Clear. Job-ready.

Know Yourself

1. Do I fully understand what NOT to do now?
2. Do I realize why ethics matter in cybersecurity?
3. Do I feel more confident acting professionally?

- *Awareness protects you.*

Key Takeaways — Chapter 6

✓ Permission is the foundation of ethical hacking
✓ Unauthorized testing is illegal
✓ Responsible Disclosure protects users & businesses
✓ Bug Bounty programs are legal, rule-based systems
✓ Ethics and trust matter more than tools
✓ Professional mindset = job-ready mindset

This isn't just technical learning.

- It's character building — and it will define your career.

Warm-Up Questions

Q1. What is Responsible Disclosure?
Q2. Is testing a random website without permission legal?
Q3. What is a Bug Bounty program?
Q4. Why is ethics important in cybersecurity?
Q5. What should you do if you find a vulnerability in a real system?

Practice answering calmly and clearly.

Chapter 7 — Your First Mini-Project & Career Roadmap (From Learner to Job-Ready Beginner)

Learning Objectives

By the end of this chapter, you will:

✓ Complete a simple, legal beginner cybersecurity project
✓ Learn how to document your work professionally
✓ Understand realistic beginner career paths
✓ Know what to learn next after this kit
✓ Convert learning into resume-worthy experience

*This chapter turns your knowledge into something you can **show**.*

Your First Mini-Project

- Its Beginner-Friendly & 100% Legal

Project Title

Beginner Cybersecurity Recon & Awareness Report

This project demonstrates:

✓ understanding of recon & OSINT
✓ awareness of web security basics
✓ knowledge of CVEs
✓ ethical mindset
✓ documentation skill

These are all valued in internships & entry-level roles.

Project Format

Create a Google Doc / Word file with the following sections:

1 Introduction (Short & Honest)

Write about:

- who you are (student / beginner)
- why you're learning cybersecurity

- your interest area (SOC / web security / general learning)
- your goal: ethical, responsible learning

Tone: simple, not bragging.

2️⃣ Passive Recon & OSINT (Legal Only)

Pick **one well-known company** (Example: Tata, Infosys, Wipro, Google, Zomato, Paytm etc.)

Collect only **public information**, such as:

✓ careers page
✓ tech blogs
✓ public documentation
✓ news articles

Now write:

- Technologies mentioned
- Any security-related keywords
- Skills employers look for
- Tools repeatedly listed

This shows industry awareness.

⚠️ No scanning
⚠️ No login attempts
⚠️ No testing
Only observation.

3️⃣ Networking Awareness

Add a section titled: **"How the Internet Works — Beginner Understanding"**

Explain briefly:

- What is an IP
- What is DNS
- What is a server
- What are ports

Use clear, simple language → This gives conceptual clarity.

4️⃣ Web Security Fundamentals

Write short explanations:

- What is a vulnerability
- What SQL Injection means
- What XSS means
- What OWASP Top 10 is

No technical depth needed — just understanding.

5️⃣ CVE Awareness

Choose one CVE such as **Log4j** and write:

- CVE ID
- Severity
- One-line description

Example: CVE-2021-44228 is a critical Log4j vulnerability that allowed remote code execution.

This shows you understand industry language.

6️⃣ Ethics & Legal Awareness

Add a short statement:

“I only practice cybersecurity in legal environments and with permission. My goal is to learn ethically and responsibly.”

This builds trust and professionalism.

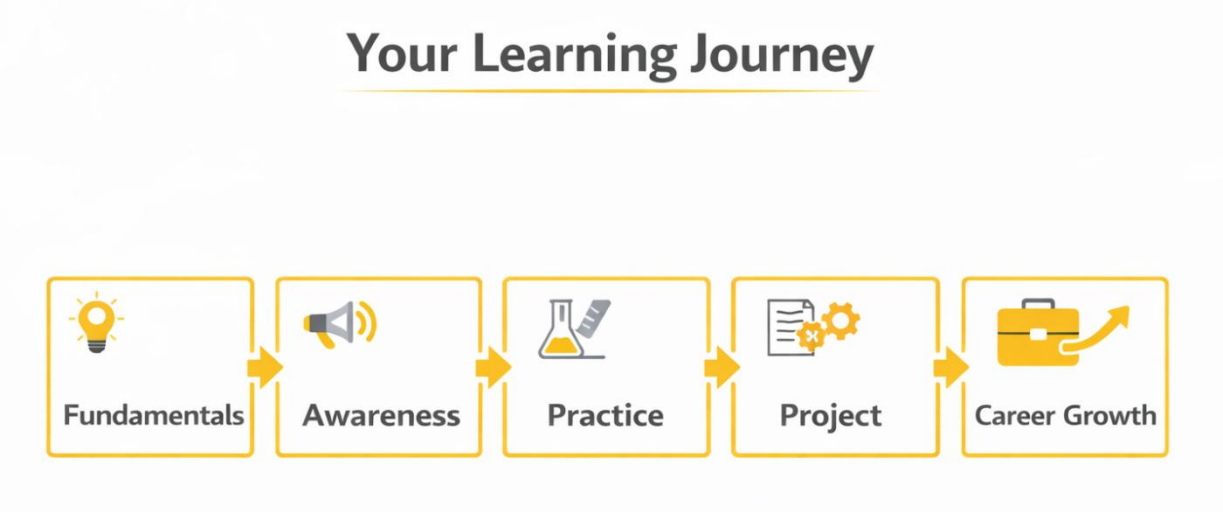
7️⃣ Reflection

Answer honestly:

- What did I learn?
- What confused me?
- What do I want to study next?

Reflection demonstrates maturity.

Simple Visual For Your Learning Journey



Congrats…You've completed the first stage 😈

Well Done!!!

Job-Readiness & Career Direction

Cybersecurity has many entry-level paths.

Here are realistic beginner-friendly options:

SOC Analyst

Can be First Great role to step in cybersecurity

You will:

✓ monitor security alerts
✓ analyse suspicious activity
✓ create reports
✓ escalate incidents

Skills that help:

- networking basics
- security fundamentals
- log analysis mindset

Security Analyst Intern

You may:

✓ assist security teams
✓ learn tools
✓ help with documentation
✓ research security topics

Companies value:

- curiosity
- discipline
- clear writing
- basic concepts

Junior Pentesting Trainee (with more practice)

You:

✓ support pentesting
✓ learn web security
✓ follow guidance from seniors

All you Required is patience & structured learning.

What To Learn Next

#Roadmap to advance your skills and knowledge.

Phase 1 — Strengthen Core Skills

✓ Networking
✓ Linux basics
✓ Web technologies
✓ Security fundamentals

Phase 2 — Hands-On Practice

✓ TryHackMe
✓ PortSwigger labs
✓ CTFs (beginner-level)

Phase 3 — Professional Growth

✓ Resume
✓ LinkedIn
✓ Internships
✓ Projects

*This is where the **Resume Booster Pack** will help you.*

Resume-Ready Bullet Points

You can honestly write:

✓ Completed a structured 7-day cybersecurity fundamentals program
✓ Learned networking, OSINT, web security, and vulnerability concepts
✓ Studied OWASP Top 10 & CVE severity scoring
✓ Created a beginner cybersecurity recon & awareness report
✓ Follow strict ethical & legal cybersecurity practices

Short. Strong. Professional.

Final Self-Check

- I understand core cybersecurity basics
- I completed the mini-project
- I feel more confident
- I know learning must stay ethical
- I have direction for my next steps

If yes — you're on the right track ✌️

Reflection — End of the 7-Day Journey

Ask yourself:

1. What was my biggest learning?
2. Do I feel less confused than before?
3. Am I motivated to continue?

Just honest with yourself.

Growth starts here.

Interview-Style Practice Questions

Q1. What is ethical hacking?
Q2. What is OSINT?
Q3. What is a CVE?
Q4. Why is ethics critical in cybersecurity?
Q5. What happens when you open a website?

Practice speaking your answers aloud.

Confidence matters.

Final Note ✨

You've completed the **7-Day Ethical Hacking Starter Kit.**

You now have:

✓ clear fundamentals
✓ ethical mindset
✓ project experience
✓ industry awareness
✓ direction for growth

Most students never take this first structured step.
You did.
And that's something to be proud of.

All the best!!!

Extra's Section

…which add some extra value. It's going to cover these two things:

i. Beginner Cybersecurity Glossary
ii. Cybersecurity Learning Roadmap

1. Beginner Cybersecurity Glossary

Authentication
Verifying who a user is (like logging in).

Authorization
What a user is allowed to do after login.

Attack Surface
All the ways an attacker could target a system.

Bug Bounty
Rewards given to ethical hackers for legally finding security issues.

CVE (Common Vulnerabilities and Exposures)
Unique ID given to known security vulnerabilities.

CVSS (Common Vulnerability Scoring System)
A system to score how serious a vulnerability is.

Cyber Attack
Any attempt to damage, steal or misuse data or systems.

Cybersecurity
Protecting systems, networks, and data from attacks.

Data Breach
When sensitive data is exposed or stolen.

DNS (Domain Name System)
Converts website names into IP addresses.

Encryption
Converting data into unreadable form to protect it.

Ethical Hacking
Testing systems legally to improve security.

Exploit
A method or code used to take advantage of a vulnerability.

Firewall
A security barrier that controls network traffic.

Incident Response
Handling and managing cybersecurity incidents.

IP Address
Unique address that identifies a device on a network.

Linux
A popular operating system used in cybersecurity.

Malware
Malicious software like viruses, ransomware, trojans, etc.

MITM (Man-In-The-Middle)
When an attacker intercepts communication between two parties.

Network
Devices connected to share information.

OSINT (Open Source Intelligence)
Collecting information from public sources.

Patch
A software update that fixes bugs or vulnerabilities.

Pentesting (Penetration Testing)
Legal hacking to test security.

Phishing
Tricking users into revealing information.

Port
A communication doorway for services on a device.

Reconnaissance (Recon)
Gathering information before testing a system.

Server
A computer that stores and delivers data/services.

SOC (Security Operations Center)
Team that monitors security threats.

SQL Injection (SQLi)
Attack targeting databases through user input.

Threat
Anything that can cause harm to systems or data.

Vulnerability
A weakness that attackers may exploit.

XSS (Cross-Site Scripting)
Running malicious scripts inside web pages.

More at https://www.sans.org/security-resources/glossary-of-terms

2. Cybersecurity Learning Roadmap

(Beginner → Job-Ready Path)

Phase 1 — Foundations (1–3 months)

Focus on:

✓ Basic IT concepts

✓ Networking fundamentals

✓ Linux basics

✓ Security awareness

Suggested learning topics:

- What is IP / DNS / Ports
- Linux terminal basics
- Web application basics
- Security terminology

Goal:

To Understand concepts clearly.

Phase 2 — Hands-On Exploration (3–6 months)

Start using beginner platforms:

✓ TryHackMe

✓ PortSwigger Academy

✓ Basic CTFs

Practice:

- OSINT
- Web fundamentals
- Simple labs
- Cyber tools overview

Goal:

Gain practical exposure — slowly & ethically.

Phase 3 — Build Experience (6–12 months)

Create:

✓ small projects

✓ lab write-ups

✓ documentation

✓ GitHub or Notion notes

Apply for:

- internships
- SOC trainee roles
- junior analyst positions

Goal:
Show learning + curiosity + discipline.

Phase 4 — Grow Professionally

Later, you may choose paths like:

- SOC Analyst
- Pentester
- Threat Intel
- Cloud Security
- AppSec

Growth pillars:

✓ continuous learning
✓ strong fundamentals
✓ ethical behaviour
✓ clear communication

Recommended Tools & Platforms

Learning Platforms

- TryHackMe — beginner-friendly labs
- PortSwigger Web Academy — web security learning
- OverTheWire — Linux & security games

Basic Tools to Be Aware Of

(learn slowly — not all at once)

- Browser DevTools
- Burp Suite
- Nma
- Wireshark
- Linux terminal

Goal: *awareness → not overwhelm.*

Communities & Resources

- Security YouTube channels

- Cybersecurity blogs
- Reddit security forums
- Local tech communities

📌 *Networking matters.*

Soft Skills & Mindset Tips

Technical skills help you get in.
Mindset keeps you growing.

Be Curious — But Ethical

Always ask: “Is this legal?”, “Do I have permission?”
If unsure → don’t do it.

Learn to Document Clearly

Write:
✓ what you learned
✓ what worked
✓ what failed
✓ what confused you
Always Remember: Clear writing is a superpower.

Communication Matters

Be:
✓ respectful
✓ humble
✓ clear
✓ honest
Companies value this highly.

Progress Slowly — But Consistently

Cybersecurity is a marathon.
Small steps daily **>** random bursts.

Protect People, Not Hurt Them

Real security work is about:
✓ safety
✓ trust
✓ responsibility

Never forget that.

Templates & Notes Pages

Use these as printable or digital pages.

Learning Journal Template

Date:
Topic Studied:
Key Concepts I Learned:
1.
2.
3.

Tools / Terms I Discovered:

What I Found Difficult:
What I Want to Explore Next:

Project Log Template

Project Name:
Objective:
Scope (Legal Only):
Steps Taken:
1.
2.
3.

Outcome / Learning:
Notes & Reflections:

Interview Prep Notes

Concept: Explanation in simple words:
Example / Use Case:

Daily Study Checklist

- Studied at least 30–60 mins
- Practiced / revised concepts
- Wrote notes
- Reflected on learning

- Stayed ethical & legal

Consistency **>** *intensity.*

Reflection Page

- **What motivates me to learn cybersecurity?**
- **What progress have I made recently?**
- **What scares me — and how will I face it?**
- **What am I proud of learning so far?**

Self-awareness builds confidence.

Some More Useful Resources

1️⃣ Beginner Lab & Practice Guide Roadmap
2️⃣ Responsible Disclosure Email Templates
3️⃣ Career Role Roadmaps
4️⃣ Linux + Web Cheat Sheets
5️⃣ 30-Day Study Plan

1. Beginner Lab & Practice Guide

A Safe, Simple Way for You To Start Hands-On Cybersecurity

Follow it step-by-step, and you'll start practicing cybersecurity safely, confidently, and legally — without confusion or overwhelm.

What You Will Get from This Guide

By the end, you will:

✓ Know exactly where to practice
✓ Understand how to begin — step-by-step
✓ Avoid unsafe or illegal activities
✓ Build real-world confidence
✓ Learn in a structured way

Level 1 — Absolute Beginner (Weeks 1–4)

Goal

Your first goal is to understand the basics and get comfortable — without stress.

Where You Will Practice

You will use these two learning platforms:

- **TryHackMe** — beginner-friendly labs
- **OverTheWire (Bandit)** — Linux basics

Both are safe, legal, and perfect for students.

Step 1 — Create Your TryHackMe Account

1. Open TryHackMe
2. Sign up for a free account
3. Start learning

Start With These Rooms (in order)

✓ Introduction to Cyber Security
✓ Pre-Security
✓ Web Fundamentals
✓ Linux Fundamentals (Parts 1–3)

These are written for beginners and give hints when you're stuck — so don't worry 😊

Step 2 — Learn Basic Linux With OverTheWire

Search online for:
OverTheWire Bandit

- Start from **Level 0** and move upward slowly.

You will learn:
✓ how to use the terminal
✓ how files work
✓ basic problem-solving
✓ simple security-style thinking

This becomes your technical foundation.

How Much Should You Study Daily?

Aim for:

30–60 minutes per day

Recommended rhythm:
✓ Study 5 days
✓ Review notes 2 days

Small daily progress beats random long sessions.

Build Your Learning Journal

After every session, write:
• Lab name
• What you learned
• New commands or terms
• Where you got stuck
• How you solved it

This is what real professionals do — and it will help you in interviews later.

Avoid These Common Beginner Mistakes

❌ jumping straight to hacking tools
❌ copying commands blindly
❌ skipping fundamentals

❌ testing real websites
❌ comparing your speed with others

You are learning — not racing 🚶
🧘 ***Patience wins.***

Level 2 — Confident Beginner (Weeks 5–10)

Goal

Now you'll start understanding **how attacks work** — still safely and legally.

Continue Learning on TryHackMe

Move into topics like:

✓ Introduction to Web Hacking
✓ Basic OWASP concepts
✓ Simple network security labs

You will begin to understand:

• how logins work
• how data travels
• how websites handle input
• why mistakes become vulnerabilities

Go slowly. Read everything.

Understanding **>** *speed.*

Tools You Will Start Noticing

You don't need to "master" these yet — just understand what they are:

- Browser Developer Tools
- Burp Suite (basic idea only)
- Linux terminal

Your awareness is the goal.
Depth will come later.

The Way You Will Learn

Use this simple method:

Pause → Think → Try → Learn

1️⃣ Read the task
2️⃣ Think what it means
3️⃣ Try solving

4️⃣ Check hints if stuck
5️⃣ Write what you learned

This trains your brain to think like a security professional.

Level 3 — Structured Skill Building (Weeks 11–16)

Goal

You will now start thinking like a junior analyst or trainee tester.

Add PortSwigger Web Security Academy

Start with:

✓ HTTP Basics
✓ Beginner Labs
✓ Introductory vulnerabilities

This platform is used by professionals worldwide — learning here builds strong credibility.

Start Writing Mini-Reports

For every lab you complete, document:

Problem: what was the goal?
Understanding: how did the vulnerability work?
Fix: how can it be prevented?

This:

✓ improves clarity
✓ strengthens your resume
✓ prepares you for interviews
✓ builds discipline

Keep your language simple and honest.

Practice Safety Rules

Always Do:

✓ Practice only on learning platforms
✓ Follow legal boundaries
✓ Respect privacy
✓ Ask permission when required
✓ Keep ethics first

Never Do:

❌ Hack random websites
❌ Test college / office networks
❌ Access private data
❌ Share sensitive information
❌ Brag about illegal activity

One wrong step can permanently damage your career.

Stay safe. Stay ethical.

Your Weekly Study Structure

Here is a simple routine you can follow:

Day 1–3: Learn new topics
Day 4–5: Practice labs
Day 6: Review notes
Day 7: Rest + reflect

Consistency creates confidence.

Progress Tracker (Ready-To-Use)

Week	Platform	Topic	Status	Notes
1	TryHackMe	Intro to Cyber Security		
2	Bandit	Linux Basics		
3	TryHackMe	Web Fundamentals		
4	TryHackMe	Linux Fundamentals		

Tick as you go ✓

Seeing progress keeps you motivated.

Growth Mindset Reminders (For You)

• You don't need to know everything
• Struggle = learning
• Curiosity is your strength
• Ethics matter more than speed
• Progress takes time

Cybersecurity is a journey — not a race.

When Are You Ready To Move Forward?

You are ready when you:

✓ understand the basics
✓ feel comfortable using labs
✓ write your own notes
✓ respect legal limits
✓ learn consistently

You do NOT need to be perfect.
Nobody is 🙂

Know Yourself

Write your answers honestly:

1. What part of labs do I enjoy the most?
2. Where do I usually get stuck — and why?
3. Do I rush, or do I stay patient?
4. Am I staying ethical and legal always?
5. What small win am I proud of this week?

Reflection = growth.

Words From Me To You

Hands-on cybersecurity feels scary at first.
Then it becomes interesting.
Then it becomes your strength.

If you:

✓ stay ethical
✓ stay curious
✓ practice daily

you WILL improve.

This guide is your **safe starting point**.
And I'm glad you chose to learn the right way 🙂

2. Responsible Disclosure & Professional Communication Templates

How To Report Security Issues Safely, Legally & Professionally

If you ever discover a possible security issue, the way you communicate matters a LOT.

This section gives you **ready-to-use templates** so you sound:
✓ professional
✓ respectful
✓ non-threatening
✓ ethical
✓ clear

Your goal is always to **help — not accuse, threaten, or demand.**

Use these ONLY when:
✓ you tested within allowed scope
✓ you followed rules
✓ you acted ethically

Never report results from illegal testing.

Very Important Reminder

If a site does NOT allow testing and you test it anyway — that is **illegal**.

Only report responsibly discovered issues such as:
✓ accidental discovery
✓ allowed bug bounty scope
✓ university or corporate permission
✓ legal lab environments

When in doubt — don't test.

Your career comes first.

Template 1 — Initial Responsible Disclosure Email

Subject: Security Vulnerability Disclosure — Responsible Reporting

Hello Team,

I hope you are doing well.

I would like to responsibly report a potential security issue that I observed in your system. I want to clarify that I do not intend any harm and I am sharing this information so that your team can review and secure the application.

If possible, please let me know the correct process or security contact to report the details privately.

Thank you for your time and for keeping users safe.

Kind regards,
[Your Name]
Cybersecurity Student / Learner

Template 2 — Detailed Report (When They Ask For More Info)

Subject: Responsible Disclosure Report — Potential Security Issue

Hello Team,

As requested, here are the details of the potential security issue I observed:

Summary:
Brief description of the issue in simple language.

Location:
Affected page / feature (do NOT share sensitive data).

Steps to Reproduce (Simple & Clear):
1.
2.
3.

Impact (Possible Risk):
Explain how it *could* affect users or data.

Important Notes:

- I did not attempt to exploit or misuse the issue
- I stayed within ethical boundaries
- No data was accessed or damaged

My intention is to help improve security.

Please let me know if you need any clarification.

Thank you,
[Your Name]

Template 3 — If They Don’t Reply

Subject: Friendly Follow-Up — Responsible Disclosure Report

Hello Team,

Just checking in regarding the responsible disclosure report I shared earlier.
I completely understand you may be busy.

If possible, please let me know if the report has been received and is under review.

Thank you again for your time.
Best regards,
[Your Name]

Template 4 — If They Resolve the Issue

Subject: Thank You — Security Issue Resolved

Hello Team,

Thank you for reviewing and resolving the security issue.
I appreciate your quick response and your commitment to protecting users.

If you need any further information, I am happy to help.
Warm regards,
[Your Name]

What You Should NEVER Write

Avoid messages like:

❌ “Your site is vulnerable, reply fast”
❌ “Pay me or I’ll make it public”
❌ “I hacked your system and found xyz”
❌ rude or threatening tone
❌ sharing sensitive data publicly
❌ flexing or bragging

Professionalism builds trust.
Aggression destroys it.

Your Ethical Responsibility Statement (Optional Signature Line)

You may add this line at the end of emails:

> I am a cybersecurity learner committed to legal and ethical security practices.
> My intention is to support user safety and responsible disclosure.

This helps organizations feel safe communicating with you.

Private Notes Template (For Your Records Only)

Keep your own copy of:

Date Observed:
Website / System:
Type of Issue:
Actions Taken:
Did You Stay Within Legal Scope? Yes / No
Disclosure Date:
Response Received:

Do NOT store sensitive data.

This builds your habit of **professional documentation**.

Your Goal As an Ethical Learner

Always remember:
✓ protect users
✓ protect companies
✓ protect your career
✓ stay humble
✓ stay legal

Responsible disclosure is about: **helping quietly — not showing off loudly.**
That's what professionals do.

Note From Me To You ✨

If you ever feel unsure about legality or scope:

Pause.
Don't continue.
Seek guidance.

Your ethics are your biggest strength in cybersecurity.
Guard them carefully — they will take you far 🙂

3. Career Role Roadmaps

This section is written honestly for you — based on what actually works in the job market. *No hype. No fake promises. Just clarity*.

Cybersecurity has many roles.
You don't need to master everything.
You only need to choose **one starting direction** — then grow step-by-step.

Below are the **three most realistic beginner-friendly roles**.

Roadmap 1 — SOC Analyst (Best Entry-Level Role)

What This Role Means

You monitor and analyse security alerts in tools like SIEM to detect suspicious activity.

Think of it like being the **security guard of IT systems — but smarter.**

Who This Role Is Good For

✓ Students with basic IT + networking knowledge
✓ Freshers
✓ Non-coding background
✓ People who like monitoring, analysis, patterns

Skills You Actually Need (Beginner Level)

- Networking basics
- Windows / Linux basics
- Security fundamentals
- SIEM awareness (like Splunk / QRadar / Azure Sentinel)
- Log analysis basics
- Understanding threats & alerts

Soft skills:

- written communication
- problem-solving
- attention to detail

What You Should Learn — Step-by-Step

Phase 1 — Foundations

- IP / DNS / Ports
- HTTP basics
- What is a firewall?
- What is malware?

Phase 2 — Practical Exposure

- TryHackMe defensive labs
- Basic Linux practice
- Understanding SOC workflows

Phase 3 — Tools Awareness

(Not mastery — just awareness)

- SIEM
- EDR
- Antivirus dashboards
- Ticketing systems

Certifications (Optional — Not Mandatory)

- Google Cybersecurity Certificate
- Security+ (if affordable)

Do NOT chase 4c unless truly needed.

Salary Expectation (Realistic)

Type	Range
Fresher / Trainee	₹2.5–4.5 LPA
1–3 yrs	₹4–8 LPA

Varies by city, company & skills.

How You Can Get This Role Faster

✓ Build a foundation
✓ Practice labs
✓ Create mini-writeups
✓ Make a simple resume
✓ Apply widely
✓ Improve English & communication

This is the **most accessible starting path** for freshers.

Roadmap 2 — Junior / Trainee Pentester

What This Role Means

You test websites or systems to find vulnerabilities — ethically and legally.
This role needs **more technical depth** than SOC.

Who This Role Is Good For

✓ Students who enjoy problem-solving
✓ Curious minds
✓ People okay with coding basics
✓ Those willing to learn deeply

Core Skills Needed

- Networking
- HTTP & web basics
- Linux
- Burp Suite
- OWASP Top 10
- Basic scripting (Python / JS helpful)

Soft skills:

- documentation
- patience
- analytical mindset

Learning Path — Step-by-Step

Phase 1 — Web Basics

- HTML / JS basics
- HTTP requests
- Cookies / sessions

Phase 2 — Security Concepts

- OWASP Top 10
- Common vulnerabilities
- Basic manual testing

Phase 3 — Tools

- Burp Suite
- Wordlists
- Recon tools

Phase 4 — Practice

- PortSwigger Academy
- TryHackMe
- Legal bug bounty programs (optional)

Certifications (Optional)

- eJPT (good starting cert)
- PNPT (later stage)

CEH is not enough for pure pentesting.

Salary Expectation (Realistic)

Type	Range
Fresher / Intern	₹2–4 LPA
Junior Pentester	₹4–9 LPA

Top companies may pay higher — but skills matter more.

⚠ Important Reality Check

Pentesting is competitive.

Companies look for:
✓ labs
✓ projects
✓ writeups
✓ clarity

So, take time to build depth.

Roadmap 3 — Cybersecurity Generalist / Analyst Intern

What This Role Means

You assist the security team in different activities:

- documentation
- vulnerability tracking
- compliance support
- research
- basic analysis

This is a **great starting point** if you're unsure which path to choose.

Who This Role Is Right For

✓ Students
✓ Freshers
✓ College beginners
✓ Non-technical backgrounds

Skills Needed

- Basic IT concepts
- Basic networking
- Security awareness
- Excel / Docs
- Communication

Over time you can specialise in:

- cloud security
- governance / risk / compliance (GRC)
- SOC
- pentesting

Salary Expectation (India)

Type	Range
Intern / Trainee	₹8k–25k per month
Analyst	₹2.5–5 LPA

Good stepping stone into the industry.

How To Choose Your Path (Simple Guide)

Ask yourself:

Do I enjoy monitoring & analysis?
👉 SOC Analyst

Do I enjoy breaking & testing systems?
👉 Pentester

Do I like organising, documentation & research?
👉 Security Analyst / GRC / Generalist

There is **no right or wrong.**

Choose what fits your personality.

Common Myths — Busted

❌ “I need to be a hacker genius to start.”
→ No. Basics + patience = progress.

❌ “Cybersecurity pays lakhs from day one.”
→ Entry salaries can be modest. Growth happens with skills.

❌ “Certifications guarantee jobs.”
→ They help — but real understanding matters more.

❌ “Only coders can do cybersecurity.”
→ Many roles need logic & analysis — not hardcore coding.

What Employers Actually Look For

✓ basics clear
✓ strong ethics
✓ willingness to learn
✓ communication
✓ discipline
✓ curiosity

If you work on these daily —you become employable.

Your First Practical Steps (Start Now)

1️⃣ Finish this 7-Day Kit
2️⃣ Practice beginner labs
3️⃣ Create a small project report
4️⃣ Build a simple resume
5️⃣ Apply for internships
6️⃣ Keep improving communication

Small actions → real results.

4. 30-Day Cybersecurity Study Plan

A Simple, Realistic Plan for Beginners & Students in India

This plan is written directly for you.
Follow it day-by-day. Stay consistent. Don't rush.
30–60 minutes daily is enough — steady progress beats burnout.

You'll learn:
✓ fundamentals
✓ hands-on labs
✓ documentation habits
✓ ethics & professionalism

Everything here is **legal, beginner-friendly, and structured**.

How This Plan Works

• **Week 1–2:** Basics & foundations
• **Week 3:** Web security & vulnerabilities
• **Week 4:** Practice, revision & mini-project

You'll use:

- TryHackMe
- OverTheWire Bandit
- PortSwigger Academy

(Free or low-cost options)

*Keep a notebook or Google Doc as your **Learning Journal**.*

Week 1 — Strong Foundations (Days 1–7)

Goal of the Week

Understand the basics of cybersecurity, networking, and Linux — without pressure.

Day 1 — Introduction to Cybersecurity

Learn:

- What cybersecurity is
- Roles in cybersecurity
- Why security matters

Write in your journal:

- Why am I interested in cybersecurity?

Day 2 — Networking Basics (Simple)

Read about:

- What is IP?
- What is DNS?
- What is a server?

Write 3 lines each in your own words.

Day 3 — HTTP & The Internet

Understand:

- What happens when you open a website
- HTTP vs HTTPS

Watch 1 short video or article.

Day 4 — Linux Basics (Concepts)

Learn:

- what Linux is
- why security uses it

Write:

- 3 places Linux is used

Day 5 — Start OverTheWire Bandit (Level 0–2)

Take it slow.

Write:

- Commands you used
- What each did

Day 6 — Bandit (Level 3–4)

Try solving on your own first.

If stuck → read hints → learn.

Day 7 — Review & Reflection

No pressure day.

Write:

- What was easy
- What was difficult
- How you felt learning

Rest. Recharge 🙂

Week 2 — Hands-On Comfort (Days 8–14)

Goal of the Week

Get comfortable with tools & safe labs.

Day 8 — TryHackMe Setup

Create your account.

Start:

Introduction to Cyber Security (part 1)

Take your time.

Day 9 — TryHackMe (Continue)

Complete a few sections.

Write:

- New terms you learned

Day 10 — Linux Fundamentals (Part 1 — Start)

Learn:

- navigation
- files
- permissions

Practice. Note commands.

Day 11 — Linux Fundamentals (Continue)

Re-do exercises you found difficult.

Repetition builds confidence.

Day 12 — Web Fundamentals (Start)

Understand:

- requests
- responses
- parameters

Think like a learner — not a hacker.

Day 13 — Bandit (Next 1–2 levels)

Solve calmly.

Write how you solved it.

Day 14 — Review Day

Summarise:

✓ Networking
✓ Linux
✓ Web basics

Rest your mind.
You're doing great.

Week 3 — Web Security & Vulnerabilities (Days 15–21)

Goal of the Week

Understand **how websites break — and how to protect them.**

Day 15 — OWASP Top 10 (Overview)

Read headings only.

Write:

- What each one roughly means

Day 16 — PortSwigger Academy (Start)

Do:

- HTTP basics lab(s)

Take your time.

Day 17 — Input & Forms

Understand:

- validation
- what can go wrong
- why security matters

Relate learning to real life.

Day 18 — Common Vulnerabilities (Simple Level)

Learn:

- SQL Injection
- XSS

In plain English.

Write:

- One-line definition each

Day 19 — CVE & CVSS Basics

Search:

CVE-2021-44228 (Log4j)

Write:

- severity
- simple explanation

Day 20 — Ethics & Legal Awareness

Revisit:

- Responsible Disclosure
- Permission rules

Write your ethical commitment.

Day 21 — Reflection Day

Answer honestly:

1. What do I enjoy most so far?
2. What confuses me?
3. What do I want to learn next?

This builds self-awareness.

Week 4 — Practice, Project & Job Readiness (Days 22–30)

Goal of the Week

Turn your learning into **real beginner-level experience.**

Day 22 — TryHackMe Review

Redo labs you didn't fully understand.

Understanding **>** *speed*

Day 23 — PortSwigger Practice

Do 1–2 beginner labs.

Document clearly.

Day 24 — Learn Basic Documentation

Create a simple template:

Problem → Understanding → Fix

This is how professionals write.

Day 25 — Start Mini-Project

Project name:

Beginner Cybersecurity Recon & Awareness Report

Add:

- intro
- recon awareness
- networking basics

Day 26 — Continue Project

Add:

- web security basics
- OWASP awareness
- CVE summary

Day 27 — Ethics Section

Write:
"I practice cybersecurity legally and respectfully."

This matters.

Day 28 — Finalise Project

Check:

✓ grammar
✓ clarity
✓ honesty

Keep it simple.

Day 29 — Interview Warm-Up

Practice questions:

- What is IP?
- What is DNS?
- What is CVE?
- What is ethical hacking?
- Why do you want cybersecurity?

Answer in plain English.

Day 30 — Reflection & Next Step Plan

Write:

- how much you've grown
- what you want to learn next
- what excites you

Reward yourself.

You completed a structured program 🎉

Study Rules To Follow

✓ 30–60 mins per day
✓ Quality > quantity
✓ Stay ethical
✓ Take notes
✓ Ask questions
✓ Be patient

❌ Don't rush
❌ Don't compare
❌ Don't test illegal targets

This journey is **yours**.

Ready-To-Use Daily Tracker

Day	Topic	Done ✓	Notes
1	Intro to Cybersecurity		
2	Networking Basics		
3	HTTP & Internet		
4	Linux Basics		
5	Bandit 0–2		
6	Bandit 3–4		
7	Review		
8–30	Continue as planned		

Fill daily. Stay accountable.

Message To You 💔

If you complete this 30-day plan — honestly —
you will be far ahead of most beginners.

You'll have:
✓ clarity
✓ fundamentals
✓ lab practice
✓ a mini-project
✓ documentation habit
✓ ethical mindset

And that is exactly what companies like to see in freshers.

Keep going.
Stay ethical.
Stay curious.

Your cybersecurity journey has officially begun 😊

5. Linux + Web Security Cheat Sheets

Simple, Practical & Ready-to-Use for Beginners

These cheat sheets are written directly for you — short, clear, and beginner-friendly.
Use them while studying, doing labs, or revising concepts.

Linux Basics Cheat Sheet

The Most Important Commands You'll Use as a Beginner

Linux is the backbone of cybersecurity.
These commands help you navigate and work confidently.

Navigation & Files

Command	What It Does
pwd	Show current location (folder path)
ls	List files in current folder
ls -la	List files including hidden ones
cd foldername	Move into folder
cd ..	Go back one level
cd /	Go to root directory
cd ~	Go to home directory
cat file.txt	Display file content
head file.txt	Show first lines
tail file.txt	Show last lines

Creating & Managing Files

Command	What It Does
touch file.txt	Create empty file
mkdir folder	Create folder
rm file.txt	Delete file
rm -r folder	Delete folder & contents
cp file1 file2	Copy file
mv file1 file2	Move / rename file

⚠️ Be careful with delete commands.

Permissions (Simple View)

Symbol	Meaning
r	read
w	write
x	execute/run

Command	What It Does
ls -l	View permissions
chmod 755 file	Change permissions
sudo command	Run as admin (be careful!)

Searching & Finding

Command	Meaning
grep text file.txt	Search inside file
grep -r text folder	Search inside folder
find / -name file.txt	Find file by name

Networking Basics in Linux

Command	Meaning
ifconfig / ip a	View IP info
ping website.com	Test connection
curl website.com	Fetch webpage
netstat -tulnp	Show network connections

Useful System Commands

Command	Meaning
whoami	Show current user
history	Show past commands
clear	Clean terminal screen
top	Show running processes
uname -a	System info

Remember These Tips

✓ Linux is case-sensitive
✓ Read errors — they help you
✓ Use Tab for auto-complete
✓ Use Up Arrow to repeat commands

Web Security Cheat Sheet

The Essentials You Should Know as a Beginner

Web security starts with understanding **how websites work**.

HTTP Basics

When you open a website:

- Browser → sends request
- Server → sends response

Common Request Methods

Method	Meaning
GET	Retrieve data
POST	Send data (forms)

HTTP vs HTTPS

HTTP	HTTPS
Not encrypted	Encrypted
Data readable	Data protected
Risky for logins	Safer

HTTPS = security layer added

Cookies

Cookies = small files websites store to:

✓ keep you logged in

✓ remember preferences

Protecting cookies = protecting accounts

Sessions

A **session** keeps you logged in after authentication.
If session is stolen → account risk.

That's why security matters.

Common Web Vulnerabilities (One-Line)

Term	Simple Meaning
SQL Injection	Attacker manipulates database queries
XSS	Attacker injects malicious script
CSRF	User unknowingly triggers an unwanted action
Broken Auth	Login / session flaws
Insecure Direct Object Reference	Accessing data not meant for you

*These are part of **OWASP Top 10**.*

OWASP Top 10 — What You Should Know

OWASP Top 10 = The most important web security risk categories.

You don't need mastery yet — just awareness.

Basic Web Testing Flow

Understand → Observe → Test → Document

Never jump to tools first.
Think → analyse → then test.

Useful Web Headers

Header	Purpose
Content-Security-Policy	Prevents script injection
X-Frame-Options	Stops click-jacking
Strict-Transport-Security	Forces HTTPS

Companies use them to secure users.

Request & Response Basics

Request Example
GET /login HTTP/1.1
Host: example.com
Cookie: session_id=123

Response Example
HTTP/1.1 200 OK
Content-Type: text/html

Understanding this = understanding web security.

Security Golden Rules

✓ Validate user input
✓ Protect authentication
✓ Encrypt sensitive data
✓ Handle sessions securely
✓ Log & monitor threats

Your Legal Practice Rule

Only test inside:
✓ TryHackMe
✓ PortSwigger Labs
✓ authorised environments

Never test random websites.

Quick Reference Table

Topic	Key Idea
Linux	Core OS for security
HTTP	Web communication
HTTPS	Secure communication
Cookies	Store user state
Session	Authenticated identity
CVE	Vulnerability ID
OWASP	Web security standard

Ready-To-Use Notes Section

New Linux Command I Learned Today:

New Web Concept I Learned Today:

Where I Struggled:

How I Solved It:

Final Reminder For You ✨

You don't need to remember everything.
Cheat sheets exist so you can **refer back anytime.**

Use them daily.
Learn slowly.
Stay ethical.
Stay curious.

You're building real-world skills — one small step at a time 😊

Connect & Join Me for more… ✌️

Dedicated Handles -
WhatsApp: https://whatsapp.com/channel/0029Vb7dfiDD38CXfUkLz00b

Telegram: https://t.me/icybersanjay

Instagram: https://www.instagram.com/icybersanjay

LinkedIn: https://www.linkedin.com/in/sanjay70023/

Website: https://www.cybersanjay.com/

Interview Bible:
https://drive.google.com/file/d/1N79KTkQyd7ckU8O6gnu9cu2JAnGcfRjb/view?usp=drive_link