
WEEK 1 – DAY 1

CYBERSECURITY FUNDAMENTALS

(Ultra-Detailed, Easy-to-Explain Notes)

---

1. First, Understand What Cybersecurity REALLY Means

Cybersecurity is **not only hacking or hacking tools**.

Cybersecurity means:

Protecting computers, networks, applications, and data from people or programs that should **not** have access to them.

Security work includes:

1. **Prevention** – stopping attacks
2. **Detection** – finding attacks quickly
3. **Response** – reacting correctly
4. **Recovery** – restoring systems

Good security engineers **assume attackers exist** and design systems accordingly.

---

2. CIA Triad – The Heart of Cybersecurity

Every security decision is based on **three goals**:

Confidentiality
Integrity
Availability

If even **one** of these fails, security fails.

2.1 Confidentiality (Keeping Data Secret)

Simple Meaning:

Only the **right people** should see the data.

If someone unauthorized sees the data → **confidentiality is broken**.

Why Confidentiality Is Important

- Protects passwords
- Protects personal details (Aadhaar, phone number, email)

- Protects company secrets

How Confidentiality Is Achieved (Step-by-Step)

1. Authentication – "Who are you?"

This checks **identity**.

Examples:

- Username + password
- OTP
- Fingerprint / face ID

If authentication fails → access denied.

---

2. Authorization – "What are you allowed to do?"

Even after login, users should **not see everything**.

Example:

- Admin can delete users
- Normal user cannot

This is called **least privilege**.

---

3. Encryption – "Make data unreadable"

Even if attackers capture data, they **cannot understand it**.

Examples:

- HTTPS encryption
- Encrypted databases
- Encrypted backups

Real-Life Example

When you log in to Instagram:

- Password is encrypted
- Only Instagram servers can read it
- Others cannot

2.2 Integrity (Keeping Data Correct)

Simple Meaning:

Data should **not change without permission**.

Integrity is about **accuracy**.

Why Integrity Is Important

- Prevents fake transactions
- Prevents data tampering
- Ensures trust

How Integrity Is Protected

1. Hashing

A hash is like a **digital fingerprint** of data.

If data changes → hash changes.

---

2. Input Validation

User input must be checked.

Without validation:

- SQL injection happens
- Commands are altered

---

3. Database Rules

- Primary keys
- Foreign keys
- Constraints

These prevent invalid data.

Example

If an attacker changes a bank balance from ₹5,000 to ₹5,00,000:

- Data wasn't stolen
- But integrity is broken

2.3 Availability (Keeping Systems Online)

Simple Meaning:

Systems should work **when users need them**.

Why Availability Is Important

- Business stops if systems go down
- Customers lose trust

How Availability Is Maintained

1. Backup Systems

If one server fails → another works.

---

2. Load Balancing

Traffic is shared across servers.

---

3. Protection Against Attacks

- DDoS protection
- Rate limiting

Example

If a website crashes due to heavy traffic:

- Availability is lost
- Even if data is safe

---

3. Threat vs Vulnerability vs Risk (VERY IMPORTANT)

This is **commonly asked in interviews**.

3.1 Vulnerability – "The Weak Point"

A vulnerability is a **weakness** in a system.

Examples:

- Weak password
- Old software
- Open port
- No input validation

A vulnerability **by itself does nothing**.

3.2 Threat – "The Attacker or Danger"

A threat is **who or what** can exploit the vulnerability.

Examples:

- Hacker
- Malware
- Insider employee
- Bot

3.3 Risk – "The Actual Danger"

Risk is the **chance that a threat will exploit a vulnerability and cause damage**.

Easy Formula

Risk = Threat × Vulnerability × Impact

Simple Example

- Vulnerability: Open admin page
- Threat: Internet attacker
- Risk: High data breach

Real-Life Analogy

- Vulnerability: Door unlocked
- Threat: Thief
- Risk: Theft

---

4. Attack Surface – "All Possible Entry Points"

Simple Meaning:

Every place an attacker can try to enter.

Examples:

- Login pages
- APIs
- Forms
- File uploads
- Open ports
- Cloud dashboards

Why Attack Surface Is Dangerous

More entry points = more chances to attack.

How to Reduce Attack Surface

- Remove unused features
- Close unused ports
- Restrict APIs
- Enforce authentication

---

5. Defense in Depth – "Multiple Locks"

Simple Meaning:

Do not depend on **one security layer**.

Example

Even if:

- Firewall fails
- Application validation stops attack
- Database permissions limit damage
- Logs detect the attack

Security Layers

1. Network
2. Application
3. OS
4. Data
5. Monitoring

---

6. Security Mindset – How Security People Think

Attacker Thinking

- What if I skip login?
- What if I change input?
- What if this API is public?

Defender Thinking

- Validate everything
- Log everything
- Limit permissions

Important Interview Line

“A good security engineer thinks like an attacker but builds like a defender.”

---

7. Kali Linux, Burp Suite, OWASP ZAP (Easy Explanation)

Kali Linux

- A Linux OS for security testing
- Contains hacking and testing tools

Burp Suite

- Intercepts web traffic
- Finds web vulnerabilities

OWASP ZAP

- Automated vulnerability scanner
- Beginner-friendly
