CS 440 – Cyber Security

Lecture 01 & 02 – Introduction to Cybersecurity

🔐 What is Cybersecurity?



Cybersecurity is the practice of:

- Protecting **systems**
- Protecting **networks**
- Protecting **data**

From:

- Unauthorized access
- Attacks
- Damage

🌍 Why Cybersecurity is Important ?

- Digital transformation everywhere
- Sensitive data stored electronically
- Increasing Cyber Attacks
- Financial loss
- Legal consequences
- Reputational damage

👉 Cybersecurity is not just hacking or antivirus software.

👉 It is a combination of technology, processes, and people working together to protect digital assets.

⚠️ Examples of Cybersecurity Failures

When security fails, we see:

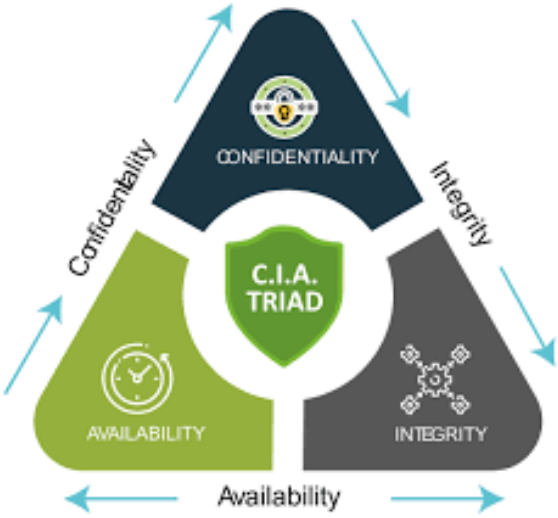
- Data breaches
- Ransomware attacks
- Service outages
- Identity theft
- Hospitals shutting down
- Airports stopping operations
- Companies paying millions in ransom

🛡️ The CIA Triad

👉 All cybersecurity concepts map to **three principles** (CIA).

👉 Every attack we study in this course will violate at least one of these.

1️⃣ Confidentiality



Prevent unauthorized access to information

Examples:

- Passwords
- Encryption
- Access control

If data is stolen → confidentiality is broken

2️⃣ Integrity

Ensure data is accurate and unmodified

Examples:

- Database tampering
- Unauthorized changes (Altered grades/ medical records)

If someone changes a student's grades even without stealing them → integrity is violated.

3️⃣ Availability

Ensure systems work when needed

Examples:

- Denial-of-Service attacks
- System Crashes
- Ransomware

A system that is secure but always down is useless.

🚑 Case Study: The Hospital That Stopped

Scenario

It's **3:17 AM** in a hospital emergency room.

Doctors try to open a patient's medical records, but:

- The system is frozen
- A red warning appears on the screen:

"Your files have been encrypted. Pay 5 Bitcoin within 24 hours."

Suddenly:

- No one can access patient data
- Surgeries are delayed
- Ambulances are redirected
- Doctors switch to pen and paper

🔍 What Actually Happened?

Important point:

- No money was stolen directly
- No secret data was leaked

👉 The attacker only did **ONE thing**:

He attacked one thing **(Availability).** That is ransomware.

🔴 CIA Triad in Real Attacks

Attack Type	Affected Principle
Ransomware	Availability
SQL Injection	Confidentiality + Integrity
DDoS	Availability

👉 Throughout this course, I will ask you one question repeatedly:
“Which part of the CIA triad is being attacked?”

🧠 Threats, Vulnerabilities, and Risks

These three terms are often confused, but they mean very different things in cybersecurity.

1. **Threat:** Anything that can cause harm

Examples:

- Hackers
- Malware
- Insider threats
- Careless employees

👉 A threat = potential danger.

2. **Vulnerability**

A weakness in the system

Examples:

- Weak passwords
- Unpatched software
- Misconfiguration

👉 Without vulnerabilities, threats cannot succeed

3. **Risk:** Likelihood of damage occurring.

Risk = Threat × Vulnerability × Impact

👉 Risk is the probability that a threat will exploit a vulnerability and cause damage.

👉 **Risk management** is what organizations care about."

⚖️ **Ethics in Cybersecurity**

Ethics defines what acceptable behavior is in cybersecurity.

- Authorized access only
- Responsible disclosure
- Professional behavior
- Ethical conduct

Just because you **can do something technically**, doesn't mean you **are allowed to do it.**

🚨 **Legal Boundaries**

- Unauthorized access is illegal
- Laws vary by country
- Severe penalties possible

👉 Accessing systems without permission is illegal, even if no damage is done.

🐧 **Role of Operating Systems (Linux)**

Why Linux?

- Used by attackers
- Used by defenders and incident responders
- Used in servers and SOC environments

👉 Linux is the backbone of cybersecurity tools

Linux in Attacks and Defense

Attacks

- Kali Linux

Defense

- Servers
- Logs
- Monitoring tools
- Incident response

📁 Linux File System Structure

Common directories:

Directory	Purpose
/home	user data
/etc	configuration files
/var/log	logs
/bin	system commands
/usr	applications

👉 “Think of the file system like the map of a city.

If an attacker gains access, where do they go?

If you are defending, where do you check logs?

Understanding structure helps you understand behavior.”

🖥️ Core Linux Commands

Command	Function
ls	list files
cd	change directory
pwd	current path
cat	view file
mkdir	create directory
rm	delete files

👉 Focus on:

- Where you are/ What exists / What you can access/modify

🔑 Linux Permissions

- -rwxr-x---

Owner | Group | Others

Permissions:

- r → read
- w → write
- x → execute

👉 This is a **core security control**

Who can read data? Who can modify it? Who can execute it?

Wrong permissions = security failure

👉 Cybersecurity is not about memorizing Linux commands — it's about knowing how to use Linux practically to investigate and secure compromised systems.