Day 1: Cyber Security Fundamentals

Welcome to Day 1! Today, we lay the foundation. Before learning tools or code, you must learn how to *think* like a security professional. We will cover the security mindset, risk analysis frameworks, and analyze historical breaches to understand what went wrong.

1. The Security Mindset

Security is not a product; it is a process. It requires shifting your perspective from "How does this work?" to "How can this be broken?"

The CIA Triad

The industry standard model for information security. All security controls aim to protect one of these three:

1. **Confidentiality:** Only authorized people can see the data (e.g., Encryption, Permissions).
2. **Integrity:** The data has not been altered or tampered with (e.g., Hashing, Digital Signatures).
3. **Availability:** The data is accessible when needed (e.g., Backups, Redundancy).

Defense in Depth

Never rely on a single defensive mechanism. Think of it like a castle: you have a moat, then a wall, then a gate, then guards. If one fails, the others stand.

- **Layer 1:** Physical Security (Locks, Cameras)
- **Layer 2:** Network Security (Firewalls)
- **Layer 3:** Endpoint Security (Antivirus)
- **Layer 4:** Application Security (Input Validation)
- **Layer 5:** Data Security (Encryption)

2. Risk Analysis Basics

You cannot protect everything equally. You must identify what is most important.

The Risk Formula:

$$Risk = Threat \times Vulnerability \times Asset \ Value$$

- **Asset:** What are you protecting? (Customer data, servers, intellectual property).
- **Threat:** Who/what is trying to attack? (Hackers, malware, natural disasters).
- **Vulnerability:** What is the weakness? (Unpatched software, weak passwords).

Risk Management Strategies

Once risk is identified, you have four choices:

1. **Mitigate:** Reduce the risk (e.g., install a patch).
2. **Accept:** The cost of fixing is higher than the loss (e.g., ignoring a low-risk bug).
3. **Transfer:** Move the risk to someone else (e.g., Cyber Insurance).
4. **Avoid:** Stop the activity causing the risk (e.g., deleting the risky feature).

---

3. Real-World Case Studies

Learning from history is crucial. Here are two major breaches and the lessons learned.

Case Study A: Equifax (2017)

- **What happened:** Attackers stole the personal data of 147 million people.
- **The Cause:** A known vulnerability in the Apache Struts web framework. A patch was available, but Equifax failed to update their systems for months.
- **Lesson: Patch Management is critical.** Known vulnerabilities are the easiest way for attackers to get in.

Case Study B: Target (2013)

- **What happened:** 40 million credit card numbers were stolen.
- **The Cause:** Attackers did not hack Target directly; they hacked an HVAC (air conditioning) vendor that had access to Target's network.
- **Lesson: Supply Chain Security.** Your security is only as strong as your weakest third-party vendor.

Day 1 Assignment

- **Identify Assets:** Look at your own computer. What is the most valuable "asset" on it? (Photos? Tax documents?).
- **Assess Threats:** What is the biggest threat to that asset? (Ransomware? Hard drive failure?).

- **Apply Controls:** How are you protecting it? Does it satisfy the CIA triad?