CS 440 – Cyber Security

Lecture 03 – Common Hacking Techniques & Attack Surface

🧠 Attacker Mindset

Attackers look for the **easiest way in**, not the most complex exploit.

They focus on:

1. Weaknesses



- Old software
- Default passwords
- Unused features left enabled

2. Misconfigurations

- Public cloud storage
- Exposed databases
- Incorrect permissions

3. Human mistakes

- Password reuse
- Clicking suspicious links
- Sharing credentials

4. Easy entry points

- Open services
- Simple targets
- Careless users and weak passwords

👉 Key idea:
Attackers choose the easiest victim first

🔓 What is a Hacking Technique?

A method used to exploit an existing weakness

Important:

- It does NOT create the weakness
- It only takes advantage of it



Analogy:

- Weakness = unlocked door
- Technique = opening the door

Used to:

- Gain unauthorized access
- Disrupt, steal or manipulate data

🗂️ Categories of Hacking Techniques

Attacks are grouped into:

1. Network-based
2. System-based
3. Web application
4. Human-based

👉 Real attacks often combine multiple categories

🌐 Network-Based Attacks

Target: Communication paths

Examples:

- Network scanning
- Exploiting open ports
- Man-in-the-Middle (MITM)

More exposed services → higher risk | Attackers usually **scan first, attack later**

💻 System-Based Attacks

Target: The system itself

Examples:

1. **Weak passwords**
   - Short
   - Reused
   - Default credentials
2. **Unpatched software**
   - Known vulnerabilities not fixed
3. **Misconfigured services**
   - Unnecessary services running
   - Wrong permissions
   - Default settings unchanged

👉 Most compromises happen due to **poor maintenance**, not advanced hacking

🌍 Web Application Attacks

Target: Websites & web apps

Examples:

1. **SQL Injection**
   - Manipulate database via input
2. **XSS (Cross-Site Scripting)**
   - Send malicious content to users
3. **Authentication bypass**
   - Access without proper login

👉 Web Applications are one of the **most common attack targets** because they are **publicly accessible.**

👤 Human-Based Attacks

Target: People (weakest link)

Examples:

1. **Phishing**
   - Fake emails or websites
2. **Social engineering**
   - Phone calls or messages
3. **Impersonation**
   - Pretending to be staff/admin/professor

👉 No firewall can stop someone from giving away their password

Defense:

- Awareness
- Verification

🔍 Introduction to OSINT

Open-Source Intelligence

Information that is:

- Publicly available
- Legal to collect
- Used for reconnaissance

OSINT Examples:

- Company websites
- Social media
- Public documents
- Domain records

👉 Attackers gather information BEFORE attacking

🚪 What is an Attack Surface?

Definition:

All possible entry points into a system

Examples:

- Open ports
- Login pages
- APIs
- User accounts

Key idea:

Bigger attack surface = easier to attack

👉 Security is often **not about building stronger walls**, but about **having fewer doors.**

🛠 Reducing the Attack Surface

Best practices:

- Disable unnecessary services
- Apply updates/patches
- Enforce strong authentication

👉 One of the most effective defenses

🔐 Mapping Attacks to the CIA Triad

Attack Goal	CIA Principle
Data theft	Confidentiality
Data manipulation	Integrity
Service disruption	Availability

👉 Every attack violates at least one CIA property