# Cybersecurity threats and vulnerabilities

Edin Esquivel

# 01

# Threats

# Threats

Cybersecurity is the practice of protecting computers, networks, and data from hackers, viruses, and other online threats. It involves tools and strategies to keep sensitive information safe and prevent unauthorized access.

# Threats

**What does it do?**

It identifies and prevents threats such as:

- **Phishing**: Fake emails or messages designed to steal information.
- **Malware**: Harmful software like viruses or ransomware.
- **Hacking**: Attempts to break into systems to steal or damage data.v

# Threats

## Why is it important in the development of the track

Understanding cyber threats is essential because our world is increasingly dependent on digital systems for communication, finance, healthcare, and daily tasks. Awareness helps individuals protect their personal data, prevent financial losses, and avoid falling victim to scams. For students studying cyber threats, it’s even more critical—they are preparing to become the future experts who will defend organizations, governments, and individuals from sophisticated cyber attacks, ensuring privacy, security, and trust in our digital infrastructure

# Threats

**What is a good resource that students can use**

Some good resources students can use are:

- **CISA** (cisa.gov) – Beginner-friendly guides on cybersecurity.
- **Stay Safe Online** (staysafeonline.org) – Tips and educational materials.
- **Cybrary** (cybrary.it) – Free cybersecurity courses.
- **Khan Academy** (khanacademy.org) – Lessons on internet safety.
- **SANS Cyber Aces** (cyberaces.org) – Free beginner courses.
- **Interactive Platforms:** tryhackme.com, academy.hackthebox.com.

# Threats

What is the technology

What does it do

Why is it important in the development of the track

What is a good resource that students can use

# Threats

What is the technology

What does it do

Why is it important in the development of the track

What is a good resource that students can use q

# Threats

What is the technology

What does it do

Why is it important in the development of the track

What is a good resource that students can use q

# 02

# Vulnerabilities

# Software Vulnerabilities

- **Definition:**
  - Flaws or weaknesses in software that attackers exploit.
- **Examples:**
  - **Outdated Software:** Unsupported operating systems or applications (e.g., Windows XP).
  - **Unpatched Bugs:** Vulnerabilities like the Log4Shell exploit targeting Java-based systems.
  - **Zero-Day Exploits:** Newly discovered bugs without patches available.
- **Impact:**
  - System downtime, data breaches, and financial losses.
  - Exploits are often automated, allowing large-scale attacks.

# Weak Passwords

- **Definition:**
  - Easily guessable or insecure user credentials.
- **Examples:**
  - Common passwords: "123456," "password," "qwerty."
  - Credential stuffing: Attackers use stolen passwords from other breaches.
  - Single-factor authentication (no MFA).
- **Impact:**
  - Unauthorized access to sensitive systems and data.
  - Brute-force and dictionary attacks succeed more often.
- **Best Practices:**
  - Use strong passwords (12+ characters, mixed case, symbols).
  - Enforce MFA and regular password updates.

# Unsecured Networks

- **Definition:**
  - Networks with weak or no protections against intrusion.
- **Examples:**
  - Open Wi-Fi without passwords or encryption.
  - Use of outdated encryption standards like WEP instead of WPA3.
  - Rogue Access Points (APs): Fake networks set up to steal data.
- **Impact:**
  - Exposure of sensitive information like login credentials or financial data.
  - Man-in-the-middle (MITM) attacks intercept communications.
- **Solutions:**
  - Use Virtual Private Networks (VPNs) on public Wi-Fi.
  - Implement strong encryption and secure network configurations.

# Misconfigured Systems

- **Definition:**
  - Systems with improper settings, creating security gaps.
- **Examples:**
  - Publicly exposed APIs without authentication mechanisms.
  - Excessive permissions (e.g., granting admin rights unnecessarily).
  - Default passwords not updated after installation.
- **Impact:**
  - Data exposure or unauthorized system access.
  - Systems vulnerable to automated attacks or insider threats.
- **Solutions:**
  - Regularly audit system configurations and access controls.
  - Use tools to scan for misconfigurations (e.g., cloud security posture management).

# Lack of Employee Training

- **Definition:**
  - Human errors stemming from limited knowledge of security best practices.
- **Examples:**
  - Falling victim to phishing attacks by clicking malicious links.
  - Mishandling sensitive data (e.g., emailing unencrypted files).
  - Sharing passwords or using personal devices for work without protection.
- **Impact:**
  - Entry point for attackers through social engineering.
  - High cost of recovery from preventable incidents.
- **Solutions:**
  - Conduct ongoing cybersecurity awareness programs.
  - Simulate phishing attacks to assess and improve employee response.
  - Create clear policies for data protection and device usage.

# 03

# Protections

# How to keep your system protected?

**Protections**

- **Definition:**
- **Examples:**
  - strong access controls
  - vulnerability management
  - keeping software updated
  - Firewalls
- **Impact:**
  - financial losses from breaches, preserving its reputation, Customer trust
-