Introduction to Cybersecurity

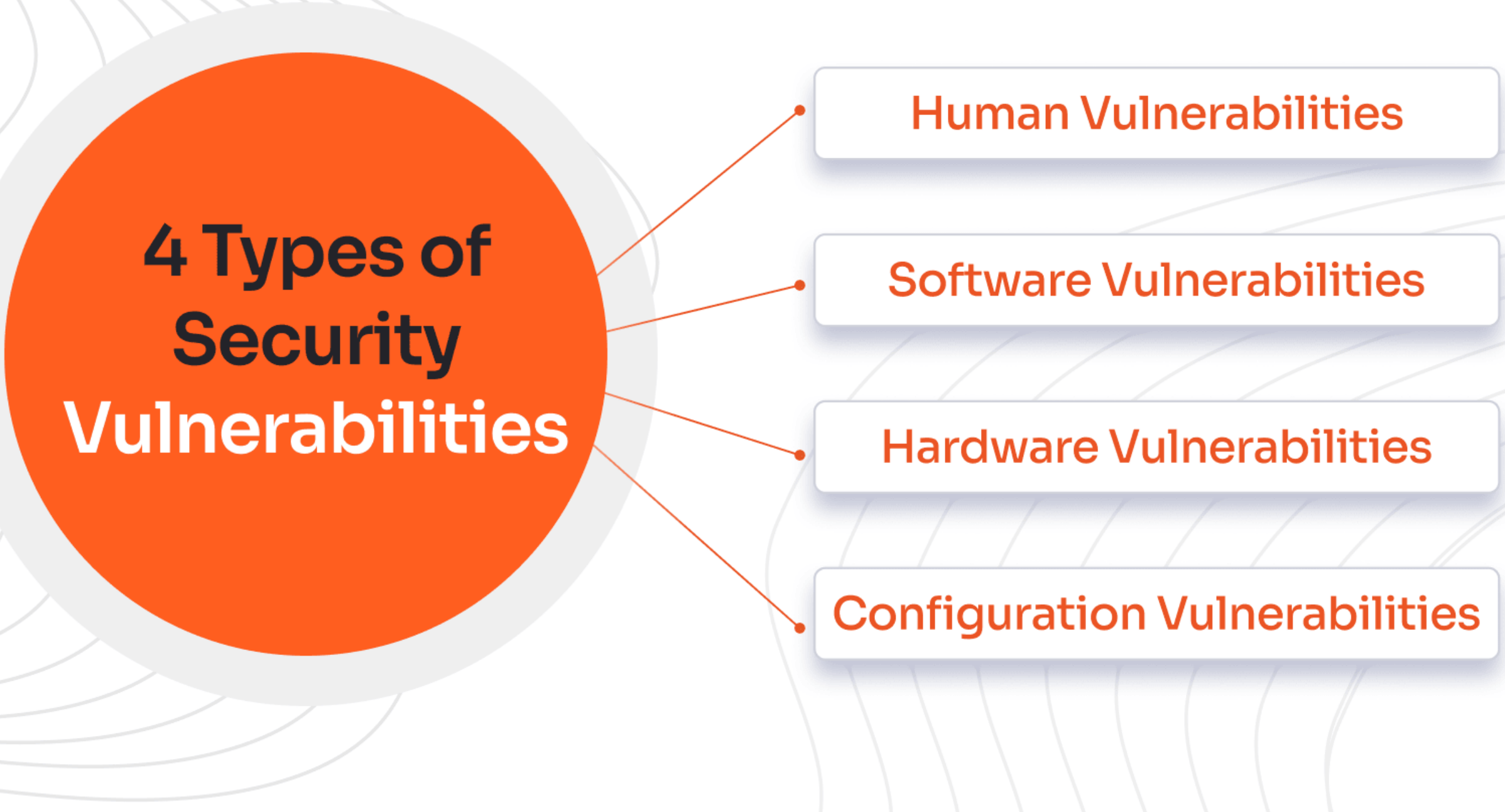
CSC3104

Dr. Sondos Fadl
Faculty of Computers &Information System
ECU

Fall 2025

Agenda

- Why Vulnerabilities Matter in Cybersecurity Frameworks
- 4 Vulnerabilities types
  - **Human Vulnerabilities**
  - **Software Vulnerabilities**
  - **Hardware Vulnerabilities**
  - **Configurations Vulnerabilities**
- Impacts from vulnerabilities


4 Types of Security Vulnerabilities
Human Vulnerabilities
Software Vulnerabilities
Hardware Vulnerabilities
Configuration Vulnerabilities

Why Vulnerabilities Matter in Cybersecurity Frameworks

- Cybersecurity frameworks (ISO 27001) emphasize vulnerability management as a **cornerstone** of **proactive defense**. Here's why:
- **Early Detection**: Identifying vulnerabilities helps prevent breaches before they occur.
- **Compliance** : Addressing known weaknesses is often a regulatory requirement (e.g., HIPAA).
- **Risk Reduction**: Fixing vulnerabilities lowers the chance and impact of an exploit.
- **Strategic Planning**: Vulnerability data informs threat models, access policies, and investment in controls.
- **Incident Response Preparedness**: Knowing where your weak points are helps teams respond faster if breached

Human Vulnerabilities

- Stem from **user behavior**, clicking phishing links, using weak or shared passwords, mishandling sensitive data, or failing to follow security protocols. Human error remains one of the most exploited and difficult-to-patch vulnerabilities.

Software Vulnerabilities

- **Software exploitation** means an attack that targets a vulnerability in software code.
- It is also important to realize that software vulnerabilities affect all types of code, not just applications:
  - ✓ Operating system (OS)— A vulnerability in an OS kernel file or shared library is more likely to **allow privilege escalation**, where the malware code runs with higher access rights (system or root).
  - ✓ Firmware—vulnerabilities can exist in the BIOS/UEFI firmware that controls the boot process for PCs.

Software Vulnerabilities

- An **application vulnerability** is a design flaw that can cause the security system to be circumvented or that will cause the application to crash.

- Vulnerability management is one of the most important aspects of securing an application because **vulnerabilities can lead to malicious activities** such as stealing confidential information, defacing websites, or launching denial-of-service attacks.

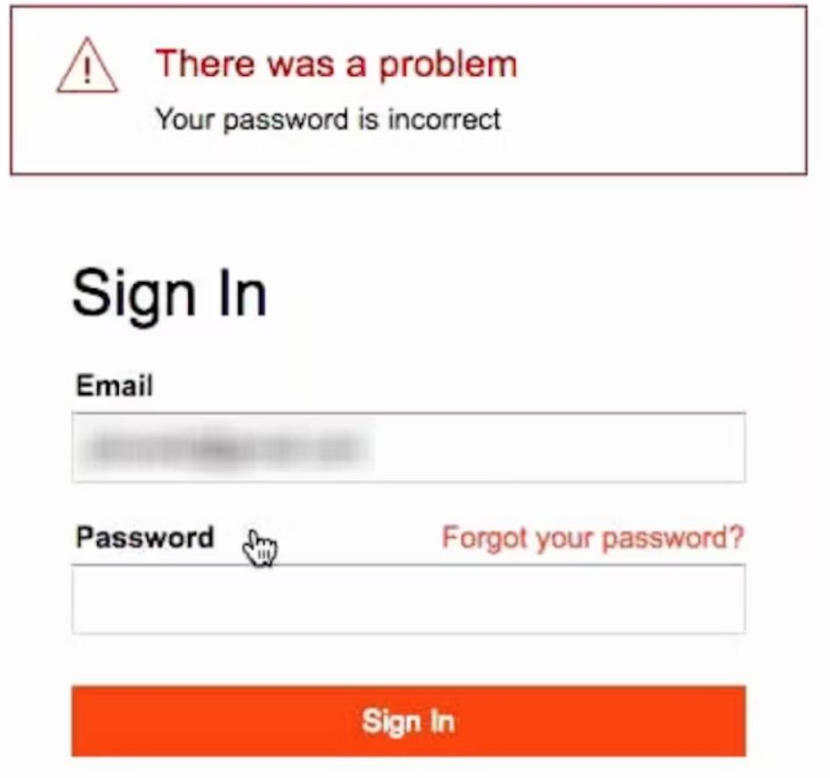
Software Vulnerabilities

Errors

✓Weakly configured applications may display unformatted **error messages under certain conditions**.

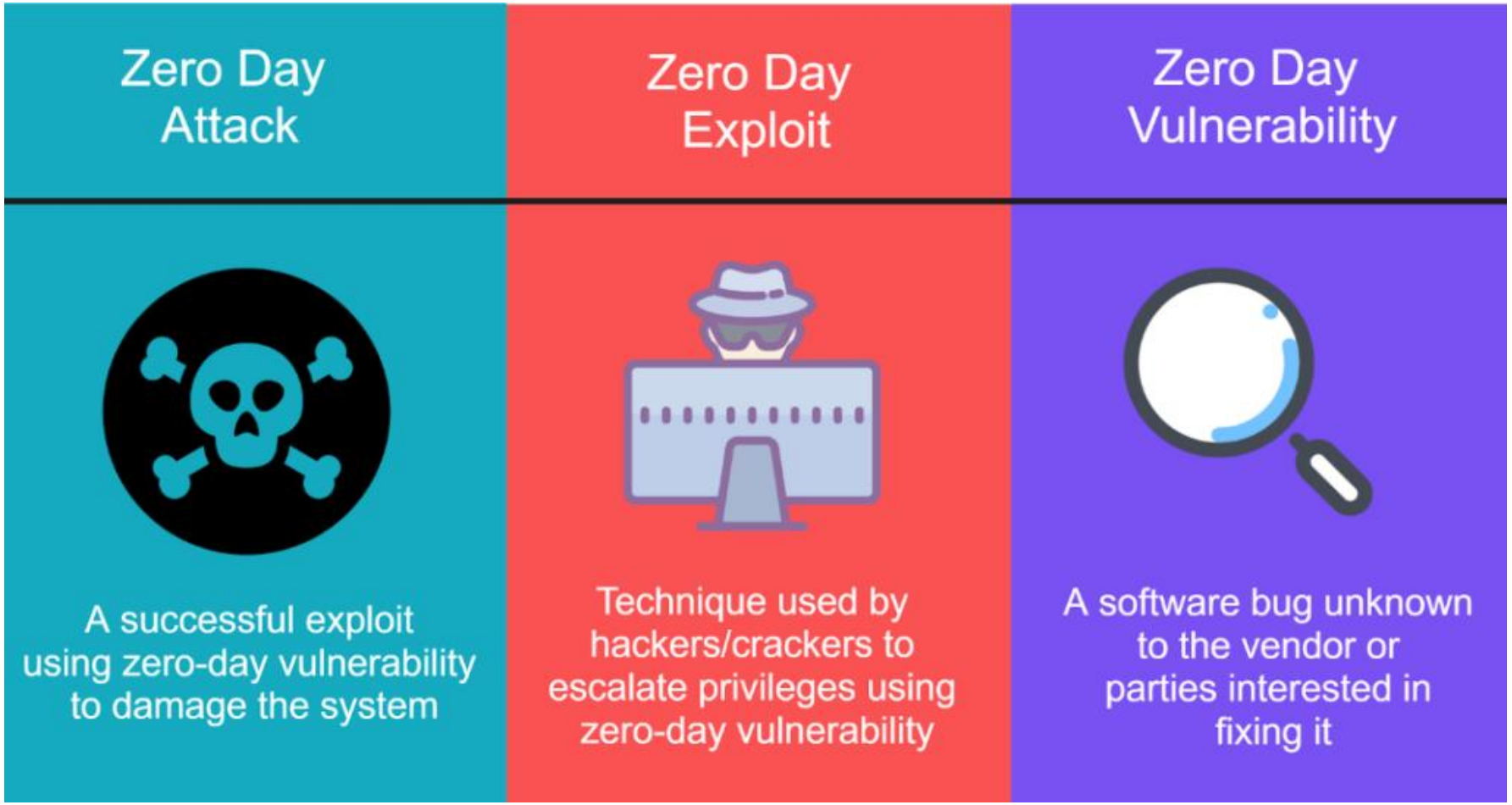
✓These error messages can be revealing to threat actors probing for vulnerabilities and coding mistakes.

✓Secure coding practices should ensure that if an application fails, it does so gracefully without revealing information that could assist the development of an exploit.



Zero-day Vulnerabilities

- **Zero-Day** is a vulnerability that is exploited before the developer knows about it or can release a patch.



Legacy Platform Vulnerabilities

- A **legacy platform** is one that is **no longer supported** with security patches by its developer or vendor.
- By definition, legacy platforms are **unpatchable**.
  - Such systems are highly likely to be vulnerable to exploits and **must be protected by security controls** other than patching, such as isolating them to networks that an attacker cannot physically connect to.

Hardware Vulnerabilities

- Involve flaws in physical devices, like **unpatched device.** IoT devices, outdated network gear are frequent targets for exploitation.

Configurations Vulnerabilities (weak Host)

Default Settings

- ✓Relying on the manufacturer default settings when deploying an appliance or software applications is one example of **weak configuration**.
- ✓It is not sufficient to rely on the vendor to ship products in a default-secure configuration, though many now do.
- ✓Default settings may **leave unsecure interfaces** enabled that allow an attacker to compromise the device.
- ✓Network appliances with weak settings can allow attackers to move through the network unhindered and snoop on traffic.

Configurations Vulnerabilities (weak Host)

Unsecured Root Accounts

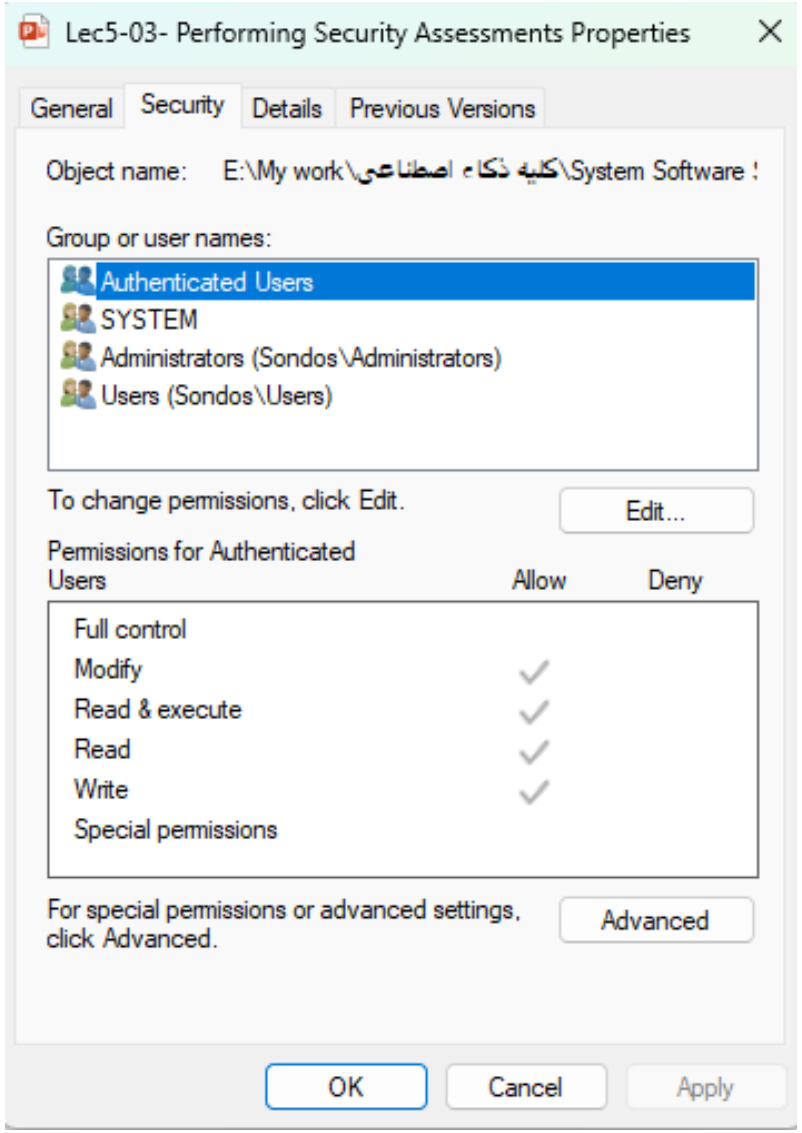
- ✓The root account, referred to as the default **Administrator account** in Windows or generically as the superuser, has no restrictions set over system access.
- ✓A superuser account is used to install the OS.
- ✓An unsecured root account is one that an adversary is able to gain control of, either by guessing a weak password or by using some local boot attack to set or change the password.

Configurations Vulnerabilities (weak Host)

Open Permissions

✓Open permissions refers to provisioning data files or applications **without differentiating access rights for user groups**.

✓Permissions systems can be complex and it is easy to make mistakes, such as permitting **unauthenticated guests to view confidential data files**, or **allowing write access when only read access is appropriate.**



Configurations Vulnerabilities (weak Network)

Open Ports and Services

✓Network applications and services allow client connections via Transport Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers.

✓Servers must operate with at least some open ports, but security best practice dictates that these should be restricted to only necessary services.

✓Running unnecessary open ports and services increases the attack surface.

✓Some generic steps to harden services to meet a given role include:

- ➢ Restrict endpoints that are allowed to access the service by IP address or address range.
- ➢ Disable services that are installed by default but that are not needed.

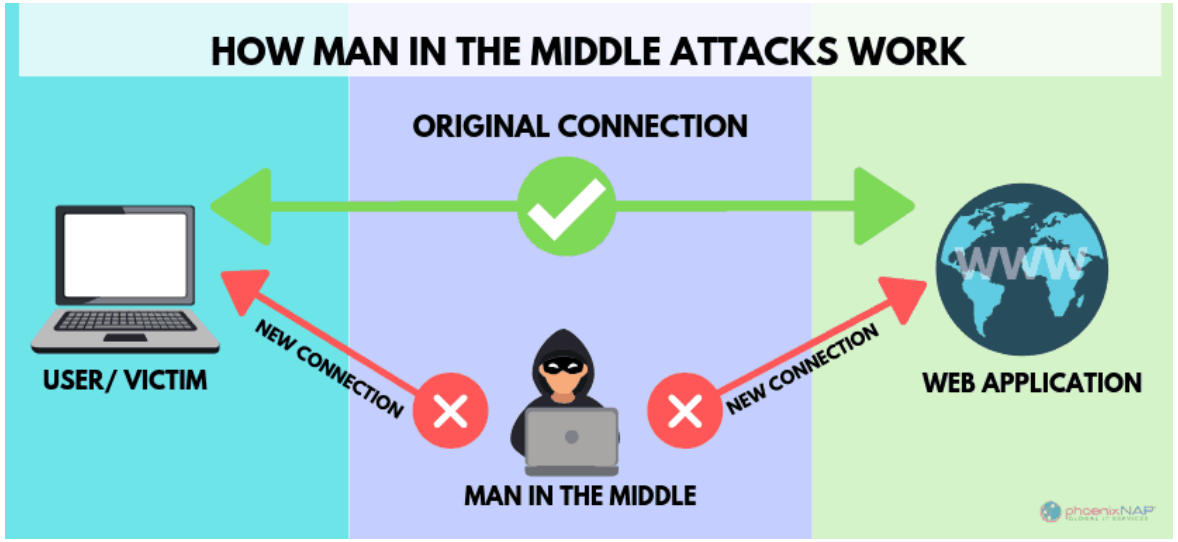
Configurations Vulnerabilities (weak Network)

Unsecure Protocols

✓An unsecure protocol is one that **transfers data as cleartext**; that is, the protocol does not use encryption for data protection.

✓**Lack of encryption** also means that there is no secure way to authenticate the endpoints.

✓This allows an attacker to intercept and modify communications, acting as **man-in-the-middle** (MITM).



Configurations Vulnerabilities (weak Network)

Weak Encryption

✓Encryption algorithms protect data **when it is stored on disk** or **transferred** over a network.

✓Encrypted data should only be accessible to someone with the correct decryption key.

✓Weak encryption vulnerabilities allow unauthorized access to data.

IMPACTS FROM VULNERABILITIES

1. Data Breaches and Data Exfiltration Impacts

✓All information should be collected, stored, and processed by authenticated users and hosts subject to the permissions (authorization) allocated to them by the data owner.

✓Data breach and data exfiltration describe **two types** of event where **unauthorized information use** occurs:

- A **data breach** event is where confidential data is read, transferred, modified, or deleted without authorization.

IMPACTS FROM VULNERABILITIES

1. Data Breaches and Data Exfiltration Impacts

✓All information should be collected, stored, and processed by authenticated users and hosts subject to the permissions (authorization) allocated to them by the data owner.

✓Data breach and data exfiltration describe **two types** of event where **unauthorized information use** occurs:

- **Data exfiltration** is the methods and tools by which an attacker transfers data without authorization from the victim's systems to an external network or media.

IMPACTS FROM VULNERABILITIES (cont.)

2. Identity Theft Impacts

✓A **privacy breach** may allow the threat actor to perform **identity theft** or to sell the data to other malicious actors.

✓The threat actor may obtain account credentials or might be able to **use personal details** and **financial information** to make fraudulent credit applications and purchases.

IMPACTS FROM VULNERABILITIES (cont.)

3. Financial and Reputation Impacts

✓All these impacts can have **direct financial impacts** due to damages, fines, and loss of business.

✓Data/privacy breach and availability loss events will also cause a company's **reputation to drop** with direct customers.