Department of
Software Engineering
BAHRIA UNIVERSITY
Discovering Knowledge

Threats & Vulnerabilities

Information Security (CSC-407)

Fall 2024 (BSE-7A & 7B)

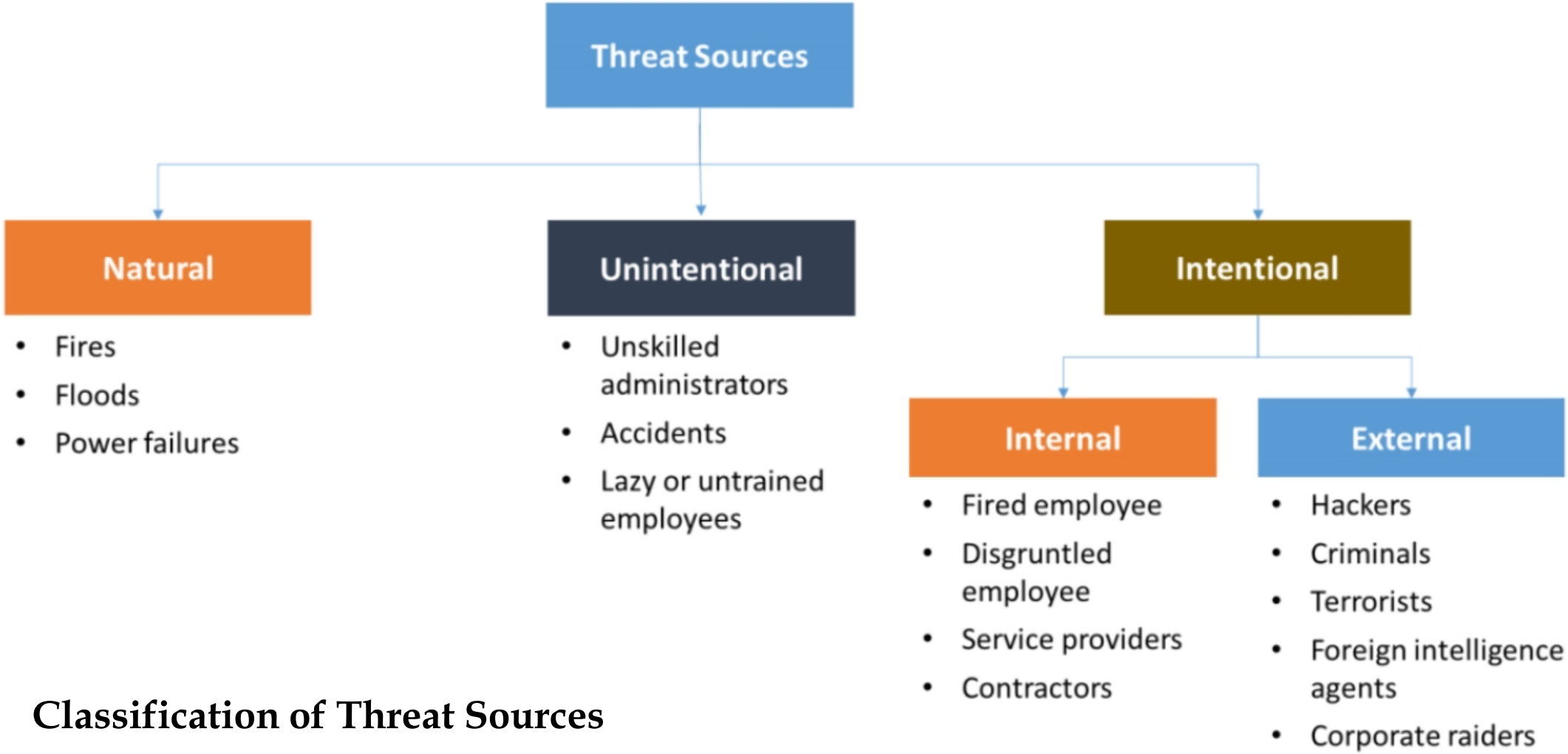
Information Security Threat

- Attackers break into systems for various reasons.
- It is important to know **how** malicious hackers exploit and attack systems and possible reasons **(why)** behind the attacks.
- An information security threat has a:
  a. Threat **sources**
  b. Threat **actors / agents**
  c. Threat **vectors**

Information Security Threat (Cont.)

- **Threat:** the potential occurrence of an **undesirable event** that can damage / disrupt the operational activities of an organization.
- **Examples** of possible threats:
  - *Stealing sensitive data*
  - *Causing server shut down*
  - *Tricking an employee into revealing sensitive information*
  - *Performing URL redirection / forwarding*
  - *Eavesdropping on a communication channel*
  - *Executing DDoS attacks*

Threat Sources



Classification of Threat Sources

Threat Sources (Cont.)

- **Natural Threats;** factors such as ***fires, floods, power failures, lightning*** and ***earthquakes*** are potential threats that these may cause severe **physical damage** to computer systems.
- **Unintentional Threats;** the potential for unintentional errors occurring **"within the organization"**, such as ***negligence, operator errors, unskilled administrators, untrained employees*** and ***accidents***.
- **Intentional Threats;**
  a. Internal Threats
  b. External Threats

Internal Threats

Internal Threats:

I. Most cyber crimes nowadays are **internal attacks**, where such attacks are performed by insiders within the organization. Most attacks are performed by **privileged users**.

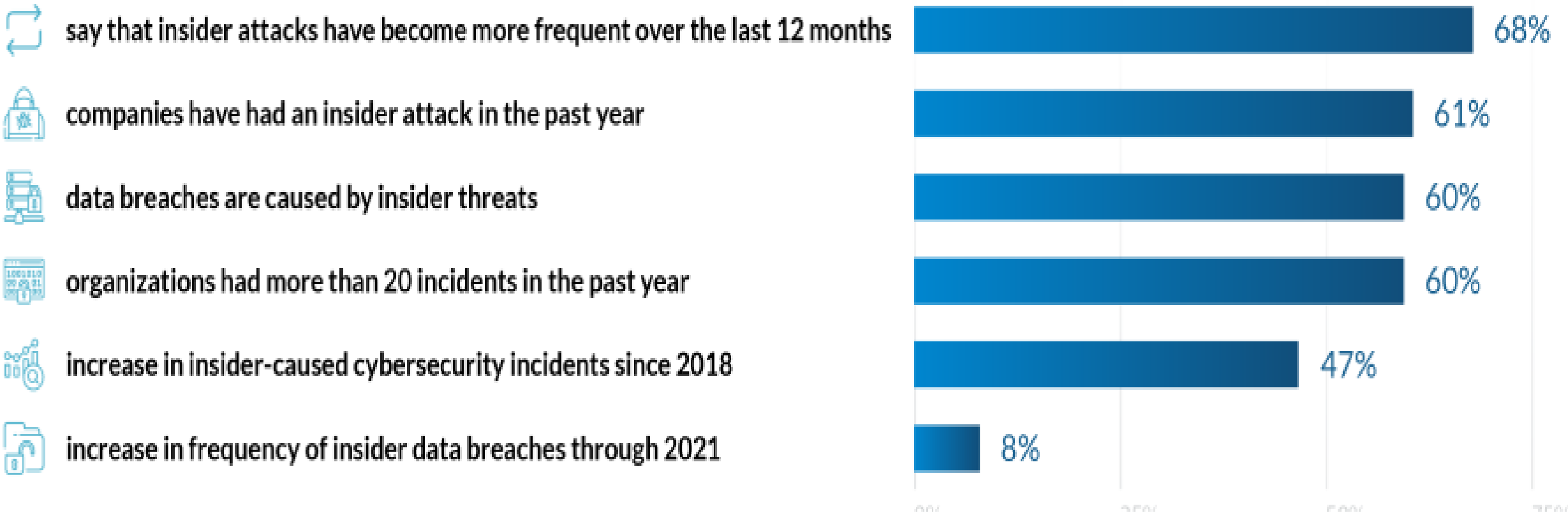
II. Internal attacks are more dangerous than external attacks because ***insiders are familiar with the network architecture, security policies, and regulations of the organization***.

III. Existing security solutions focus more on **external attacks**, hence leading an organization to be underequipped to identify and counter **internal attacks**.

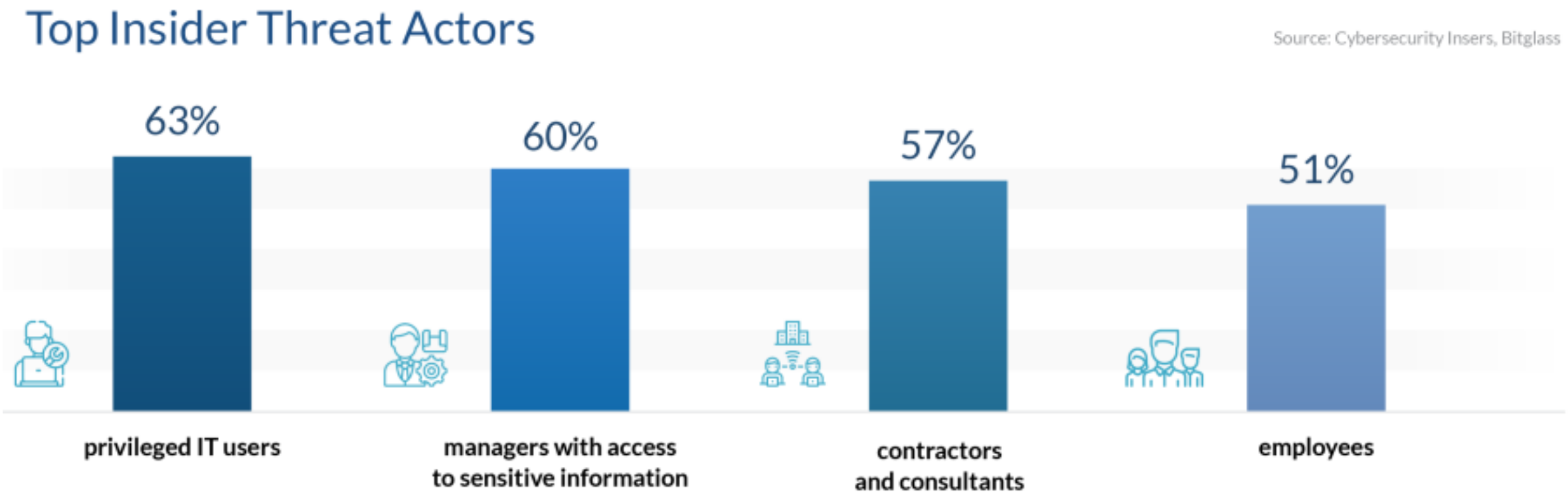
Internal Threats (Cont.)

Insider Threat Frequency of Attacks

Sources: Goldstein, CyberSecurity, ObserveIT, Shey, Bitglass, IBM



Internal Threats (Cont.)



https://financesonline.com/insider-threat-statistics/

External Threats

External Threats:

I. Usually performed by exploiting **vulnerabilities**.

II. Attackers have a **predefined plan** and use **specialized tools** and **techniques** to penetrate networks.

III. External threats can be further classified into two types:

   a. **Structured external threats:** implemented by technically skilled attackers.

   b. **Unstructured external threats:** implemented by unskilled attackers ***(known as script kiddies)***.

Threat Actors / Agents

1. **Black Hats;** individuals who use their computing skills for illegal purposes, also known as **crackers**. Such hackers are often involved in **criminal activities**.

2. **White Hats;** individuals who use their hacking skills for **defensive purposes**, also known as **penetration testers / security analysts**. Organizations have such people who are knowledgeable about hacking countermeasures to secure their networks and information systems. Such individuals **have permission** from the system owners.

Threat Actors / Agents (Cont.)

3. **Gray Hats;** individuals who work both **offensively** and **defensively**. Gray hats might **help hackers** to find various vulnerabilities, and at the same time **help vendors** to improve products (software or hardware) by checking limitations and making them more secure.

4. **Script Kiddies;** unskilled hackers who compromise systems by **running scripts, tools** and **software** developed by real hackers.

Threat Actors / Agents (Cont.)

In-terms of other **motivations**, threat actors / agents can also be classified as:

- **Cyber Terrorists;** individuals who are motivated by religious or political beliefs.
- **State-Sponsored Hackers;** skilled individuals having expertise in hacking and are **employed by the government** to exploit a nation's infrastructure, penetrate, gather intelligence ***(i.e. espionage)***, damage information systems of other government or military organizations ***(i.e. sabotage activities)***, also known as **Advanced Persistent Threats (APTs)**.

Threat Actors / Agents (Cont.)

- **Hacktivist;** hackers break into government or corporate systems as an act of protest. Hacktivists use hacking to increase awareness of their **social or political agendas**. Common hacktivist targets include government agencies and multinational corporations. Hacktivists typically promote and publicize their cause through:
  - Website defacement
  - Theft and distribution of data for negative publicity or to compromise their targets

Threat Actors / Agents (Cont.)

- **Industrial Spies;** individuals who perform **corporate espionage** by illegally spying on competitor organizations. They focus on stealing critical information such as **blueprints *(i.e. development plans)*, formulas, product designs, trade secrets, and marketing strategies.**

Threat Vectors

- **Threat vector:** the **means** by which an attacker gains access to a system by **exploiting vulnerabilities** within that system.
- Some of the threat vectors used by malicious actors include:
  a. Removable media
  b. Wireless
  c. Email
  d. Cloud
  e. Third-party vendor

Risk in Information Security

- **Risk:** the **potential loss or damage** that can occur when a threat to an asset exists in presence of a vulnerability.
- A risk can be thought of as the **intersection** of an asset, threat, and vulnerability:

Risk = Asset + Threat + Vulnerability

- ***If threats exist, but vulnerabilities do not exist in a system, then there is little or no risk.***

Information Security Vulnerabilities

- There are several **main causes** for systems being vulnerable:
  a. **Poor design** of networks / applications
  b. **Poor programming** practices
  c. Software / Hardware **misconfiguration** → ***Studied as Example***
  d. Inherent **technology weaknesses**
  e. Careless approach of **end users**

Misconfigurations / Weak Configurations

- Mainly caused by **human error**.
- Attackers can detect misconfigurations through various **scanning techniques** and then exploit the **backend systems**.
- Administrators **MUST** change the **default configuration** of devices and optimize their security.
- Generally addressed in two areas:
  - ***Network Misconfigurations***
  - ***Host Misconfigurations***

Network Misconfigurations

- Examples of weak network configurations:

  I. Open Ports and Services;

  a. **Servers** often operate with some **open ports**, but all open ports are not dangerous, ***unless misconfigured, unpatched, or implemented with poor security rules***.

  b. However, open ports must be **limited** and used only for important services.

Network Misconfigurations (Cont.)

- Examples of weak network configurations (Cont.):

III. **Weak Encryption; improper encryption** can lead towards compromising of the data being **transmitted** over a network or **stored** in a device.

Some causes of weak encryption are:

a. Usage of ***weak encryption algorithms***

b. Key generation with ***guessable credentials***

c. Insecure ***key distribution***

Host Misconfigurations

- Attackers can exploit **configuration flaws** in host server to gain **administrator level access**.
- Examples of weak host configuration:

I. Open Permissions;

a. Granting **unnecessary permissions** to user in accessing applications / files can lead to security issues.

b. Attackers can perform privilege escalation by using **unnecessarily created accounts** (***e.g. access unprotected files or run commands on OS***).

Host Misconfigurations (Cont.)

- Examples of weak host configuration (Cont.):

II. Unsecured Root Accounts;

a. **Manufacturer-allotted** default account credentials ***(e.g. for database or applications)*** can lead to security issues.

b. Failing to implement a secure password policy can allow attackers to **guess credentials** using **brute-force** techniques.

Common Areas of Vulnerabilities

- **Common areas** where attackers search for vulnerabilities:
  1. Human errors; e.g. ***(using default passwords)***
  2. Operating System; e.g. ***(unpatched OS, default services and open ports at OS installation)***
  3. Applications; e.g. ***(new applications / old applications with new features)***
  4. Network devices; e.g. ***(Access points, Routers, Switches)***
  5. Configuration Files; e.g. ***(system configuration files)***

Thank You!