# Threats, Vulnerabilities and Risks

**Threat, vulnerability and risk are terms that are commonly mixed up. However, their understanding is crucial for building effective cybersecurity policies and keeping your company safe from various cyber attacks.**

## Threat:

**A threat is any type of danger, which can damage or steal data, create a disruption or cause harm in general.**

**Common examples of threats include malware, phishing, data breaches and even rogue employees. Threats are manifested by threat actors, who are either individuals or groups with various backgrounds and motivations.**

## Vulnerability

**A vulnerability is a weakness in hardware, software, personnel or procedures, which may be exploited by threat actors in order to achieve their goals.**

**Vulnerabilities can be physical, such as a publicly exposed networking device, software-based, like a buffer overflow vulnerability in a browser, or even human, which includes an employee susceptible to phishing attacks.**

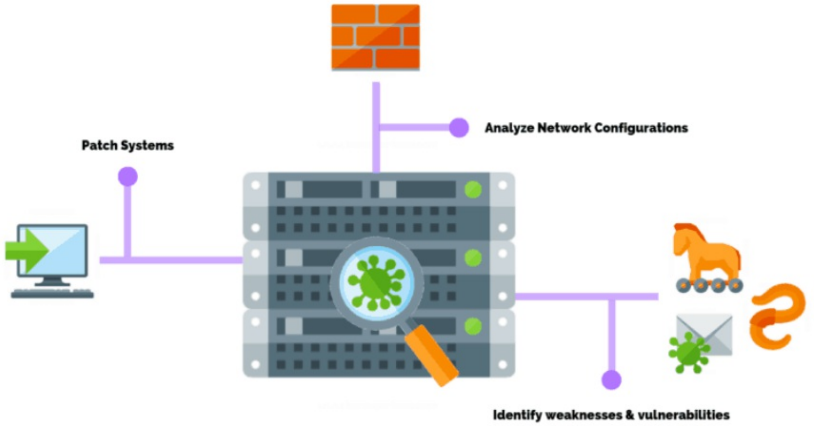
## Risk

**Risk is a combination of the threat probability and the impact of a vulnerability. In other words, risk is the probability of a threat agent successfully exploiting a vulnerability, which can also be defined by the following formula:**

**Risk = Threat Probability * Vulnerability Impact.**

# What Is A Network Vulnerability?

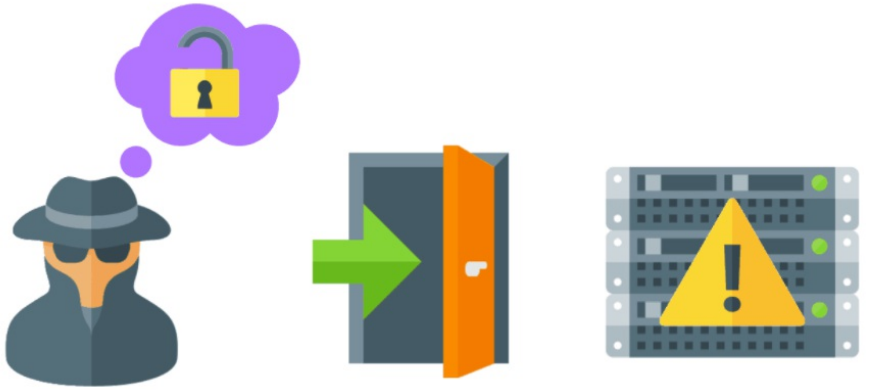
**A network vulnerability is a weakness or flaw in software, hardware, or organizational processes, which when compromised by a threat, can result in a security breach.**




**Nonphysical network vulnerabilities typically involve software or data. For example, an operating system (OS) might be vulnerable to network attacks if it's not updated with the latest security patches. If left unpatched a virus could infect the OS, the host that it's located on, and potentially the entire network.**

# Physical network vulnerabilities

**involve the physical protection of an asset such as locking a server in a rack closet**



**Servers have some of the strongest physical security controls in place as they contain valuable data and trade secrets or perform a revenue-generating function like a web server hosting an eCommerce site. Often stored in off-site data centers or in secure rooms, servers should be protected with personalized access cards and biometric scanners.**

# The 8 Types of Security Vulnerabilities:

**1. Unpatched Software – Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.**

# The 8 Types of Security Vulnerabilities:

**1. Unpatched Software – Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.**

**2. Misconfiguration – System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.**

# The 8 Types of Security Vulnerabilities:

**1. Unpatched Software** – Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.

**2. Misconfiguration** – System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.

**3. Weak Credentials** – An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.

# The 8 Types of Security Vulnerabilities:

**1. Unpatched Software** – Unpatched vulnerabilities allow attackers to run a malicious code by leveraging a known security bug that has not been patched. The adversary will try to probe your environment looking for unpatched systems, and then attack them directly or indirectly.

**2. Misconfiguration** – System misconfigurations (e.g. assets running unnecessary services, or with vulnerable settings such as unchanged defaults) can be exploited by attackers to breach your network. The adversary will try to probe your environment looking for systems that can be compromised due to some misconfiguration, and then attack them directly or indirectly.

**3. Weak Credentials** – An attacker may use dictionary or brute force attacks to attempt to guess weak passwords, which can then be used to gain access to systems in your network.

**4. Phishing, Web & Ransomware –** Phishing is used by attackers to get users to inadvertently execute some malicious code, and thereby compromise a system, account or session. The adversary will send your users a link or malicious attachment over email (or other messaging system), often alongside some text/ image that entices them to click.

# The 8 Types of Security Vulnerabilities:

**5.Trust Relationship – Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.**

# The 8 Types of Security Vulnerabilities:

**5.Trust Relationship –** Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.

**6.Compromised Credentials –** An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.

# The 8 Types of Security Vulnerabilities:

**5.Trust Relationship –** Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.

**6.Compromised Credentials –** An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.

**7. Malicious Insider –** An employee or a vendor who might have access to your critical systems can decide to exploit their access to steal or destroy information or impair them. This is particularly important for privileged users and critical systems.

# The 8 Types of Security Vulnerabilities:

**5.Trust Relationship –** Attackers can exploit trust configurations that have been set up to permit or simplify access between systems (e.g. mounted drives, remote services) to propagate across your network. The adversary, after gaining access to a system, can then proceed to breach other systems that implicitly trust the originally compromised system.

**6.Compromised Credentials –** An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.

**7. Malicious Insider –** An employee or a vendor who might have access to your critical systems can decide to exploit their access to steal or destroy information or impair them. This is particularly important for privileged users and critical systems.

**8. Zero-days & Unknown Methods** – Zero days are specific software vulnerabilities known to the adversary but for which no fix is available, often because the bug has not been reported to the vendor of the vulnerable system. The adversary will try to probe your environment looking for systems that can be compromised by the zero day exploit they have, and then attack them directly or indirectly.