Common Cyber Threats and Potential Attacks

Threat Category: Malware
Threat Name: Malware
Possible Attacks:

- Virus: Self-replicating code that infects files and programs.
- Worm: Self-propagating malware that spreads through networks.
- Trojan: Malicious program disguised as legitimate software.
- Ransomware: Encrypts files and demands payment for decryption.
- Spyware: Collects user data without consent.
- Adware: Displays unwanted advertisements.

Threat Category: Social Engineering Threat Name: Social Engineering
Possible Attacks:

- Phishing: Deceiving users into revealing personal information.
- Pretexting: Creating a believable scenario to gain trust.
- Baiting: Offering something enticing to lure victims.
- Tailgating: Physically following someone into a secure area.

Threat Category: Network Attacks

Threat Name: Denial of Service (DoS)
Possible Attacks: Overwhelming a system with traffic to prevent legitimate access.

Threat Name: Man-in-the-Middle (MitM)
Possible Attacks: Intercepting communication between two parties.

Threat Name: SQL Injection
Possible Attacks: Exploiting vulnerabilities in web applications to access databases.

Threat Category: Web Application Attacks

Threat Name: Cross-Site Scripting (XSS)
Possible Attacks: Injecting malicious scripts into web pages.

Threat Name: Cross-Site Request Forgery (CSRF)
Possible Attacks: Forcing users to execute unwanted actions on a web application.

Threat Category : Exploit

Threat Name: Insider Threat
Possible Attacks: Malicious actions by employees or contractors.

Threat Name: Zero-Day Exploit
Possible Attacks: Exploiting vulnerabilities unknown to software vendors.

Threat Name: Supply Chain Attack
Possible Attacks: Targeting software or hardware suppliers to compromise downstream users.