Cybersecurity Interns  
 Intern Career

Task One: Cybersecurity Risk Assessment

Network or system setup  
A small business network that is composed of switches, router, servers, modems, computers and network cables.

Potential Threats and Vulnerabilities  
Phishing attacks can be a threat towards the network because of the lack of education and self-awareness by employees, regarding phishing techniques.  
Weak Authentication can be a threat towards the network due to the lack of strong passwords, absence of Multi-Factor Authentication and an absence of lockout mechanism if user has many login attempts.  
Due to no firewall configured, the network is exposed to malicious software being installed or downloaded in the system, intended to exploit the system and data.

Vulnerability Scanning  
Identified vulnerabilities using these tools:

* *Nmap:* open ports which can be exploited were found and outdated software were identified.
* *Nessus:* softwares that need updates and patching were identified, default credentials which are risky were also identified and weak security settings were discovered. All of these are risky because there are high chances of having cyber attacks due to the vulnerabilities.
* *Wireshark:* a pattern of Denial of Service (DoS) was identified which could result to response delays, data breaches and impacting the availability of services, unencrypted traffic and unauthorized access has been identified which is putting the network at risk by making it easy for hackers to access the network and steal or exploit data.

Potential Risks

* 1. The risk of having **outdated software** could result in high sensitivity to malware, compromise of the networks integrity and unauthorized access.
  2. **Unpatched systems** are prone to performance issues, unexpected downtime and crashes.
  3. Having **default credentials** in the system could result to unauthorized access and sensitive data being compromised.