**Cyber Security Risk Management Project.**

**Introduction:**

I welcome you all to my cyber security project where we will dive into the world of computer networks/systems and its components how they are connected and why it’s crucial to keep them protected at all times.

The security landscape is very complex and therefore proper measures need to be taken to ensure that the networks ,physical security as well as systems are safe ,we will be identifying potential issues that arise within computer architectures like misconfiguration of systems/software, unauthorized access, unpatched programs, misconfigured firewalls or unpatched, ransomware, social engineering (phishing, vishing),DDOS/DOS with the being so many attacks we can’t go through all of them at once we will glance through the above mentioned ones.

**Scanning and its importance in Cybersecurity**

**Scanning**

Vulnerability scanning is a crucial process in cybersecurity that involves identifying, classifying, and prioritizing security vulnerabilities in computer systems, networks, and applications. It is an essential proactive measure to protect organizations from potential cyber threats and attacks. Vulnerability scanning tools are used to automate the process of identifying weaknesses within a system, allowing organizations to take necessary steps to mitigate these vulnerabilities before they can be exploited by malicious actors.

For our scan we are going to use Splunk and TCP dump and we are going to document our findings in our playbook which will lead us on what necessary steps we should take to solve these incidents.



I initially created this network for a company where they had multiple computers to connect for employees, wireless connections, and remote connections for remote work.

Thereafter I conducted a vulnerability scan for the network so that we can ensure the network is safe for use .And below I documented my findings.

**Tools utilized.**

Nmap scan 10.0.2.6

A screenshot of a computer

Description automatically generated

**Risk Analysis and Findings**

**Insecure remote access:**

* Vulnerability: weak or insecure remote connections
* Severity: medium
* Potential: Unauthorized access, compromised remote network ,compromised data and information.

**Misconfigured firewalls:**

* Vulnerability: misconfigured firewalls
* Severity: high
* Potential impact: network intrusion, unauthorized access, leaked information

**Unpatched system:**

* Vulnerability: exploits from missed upgrades
* Severity: medium
* Potential Impact: multiple exploits, compromised system, system instability and degradation, increased risk of malware infections.

**Phishing and social engineering**

* Vulnerability: No user training or awareness
* Severity: High
* Potential impact: System breaches, unauthorized access ,ransomware, compromised network or system.

**DOS attacks :**

* Vulnerability: unsatisfactory measures to protect against DOS attacks
* Severity: high
* Potential impact: Network downtime, affected operating systems, restricted access to employees.

**Mitigation strategies:**

To ensure safe access of or systems from the identified vulnerabilities .We can follow these guidelines.

**Dos attacks:**

* Blocking IP address spoofing and inbound traffic.
* Monitor network traffic and block traffic that is not of company utilization

**Insecure Remote connections:**

**Secure remote Connections:**

* Utilize VPNS as the is variety to choose from.
* Implement multi-factor authentication
* Limit access

**Phishing and social engineering:**

* Report suspicious activity
* Verify requests of any sorts
* Educate users
* Use security tools to enable email filters, spam blockers etc.

**Firewall configuration:**

* Regularly update firewall software
* Configure firewall settings properly
* Monitor firewall logs

We conclude our research and have come to agreement of how important security is for systems and its organizations’ understand that security is the backbone of any successful network. People need to importance of patching and being knowledgeable about current threats and vulnerabilities< Through teaching and upskilling employees or just ordinary people can stay safe online.