

|  |
| --- |
| Cyber Security  Task # 1 Solution |
|  |
| september 11  Digital Empowerment Pakistan Foundation  Authored by: Muhammad Hassan Yaseen |

Security Audit Report

Date: March 12, 2023

Network Overview:

The network in question comprises 20 Windows 10 work stations, 2 Windows Server 2019 servers, 1 Cisco 2811 router, 1 pfSense firewall and 1 wireless access point, namely a Cisco Aironet 1815i. The network is for a small business that employs round about fifty people.

Risk Assessment:

During the security audit I had to perform a threat analysis in order to determine vulnerabilities to the system. The following threats were identified: The following threats were identified:

Other risks include unpatched vulnerabilities in either the software being used with the firm’s operating system or in the operating system itself.

Some of the employees’ passwords are very insecure and easily guessable.

Unsecured Wi-Fi network

Configuration of routers and getting rid on firewalls.

Infections originating from user activities of the employees

These threats are the ones which have been analyzed based on the network topology and device configurations. It can also be manual or by use of automated tools as was the case when conducting the risk assessment.

Vulnerability Scanning:

In order to find out some weaknesses in the network, I ran a vulnerability scan in the network with a view of determining the ports in the network, the services being offered in the network and maybe some of the vulnerabilities that the network might contain. The scan revealed the following vulnerabilities: The scan revealed the following vulnerabilities:

CVE 2020 1472: A vulnerability that is yet to be patched existing in Windows 10 workstations

CVE-ID: CVE-2019-19781 – Untouched vulnerability in Windows Server 2019

This is normally brought about by a poor configuration of the SSL/TLS on the router and firewall.

These vulnerabilities were extraordinary and discovered from the combination of automated and manual testing.

Security Policies and Procedures Review: Security Policies and Procedures Review:

During the network security assessment, I began familiarizing myself with its security policies and practices to note some of the potential deficiencies. The following issues were identified: The following issues were identified:

Failure to install updates for work stations and servers from time to time

Lack of stringent password policy where things such as password expiry and use of strong passwords or passwords with additional authentication measures.

Lack of network segmentation, this is there are no VLANs or subnets separating secured information.

These problems were discovered with reference to the network’s security policies and procedures and by consulting with the network administrators.

Recommendations:

Recommendations: After the risk assessment, vulnerability scanning and security policy review, following were the recommendations made.

Establish a patch management program: Keep up to date on workstations and servers with the newest security patches.

Enforce a strong password policy: Establish best practices and policies that include things such as multi-factor authentication, regular password changes requirements, and complex passwords.

Use a string Wi-Fi network: Set up the WAP with WPA2 encryption and an unequivocally secure password.

Establish network segmentation: Deploy VLANs or subnets to isolate important information in addition to minimizing the impact of an attack.

Firewall Configuration: Block all un necessary incoming and Outgoing traffic from the Router and Firewall.

Conclusion:

Numerous security lapses such as vulnerabilities and weaknesses on the network were noted during the assessment. Adhering to their security recommendations can further mitigate these risks and overall improve the network's security posture.