TASK 1

RISK ASSESSEMENT REPORT

Naoufal
GUENDOUZ

15 JUN 2024

Introduction

The purpose of this risk assessment is to evaluate the security of a typical small office network and identify potential weaknesses that could expose the organization to cybersecurity risks. The assessment encompasses various aspects of network security, including:

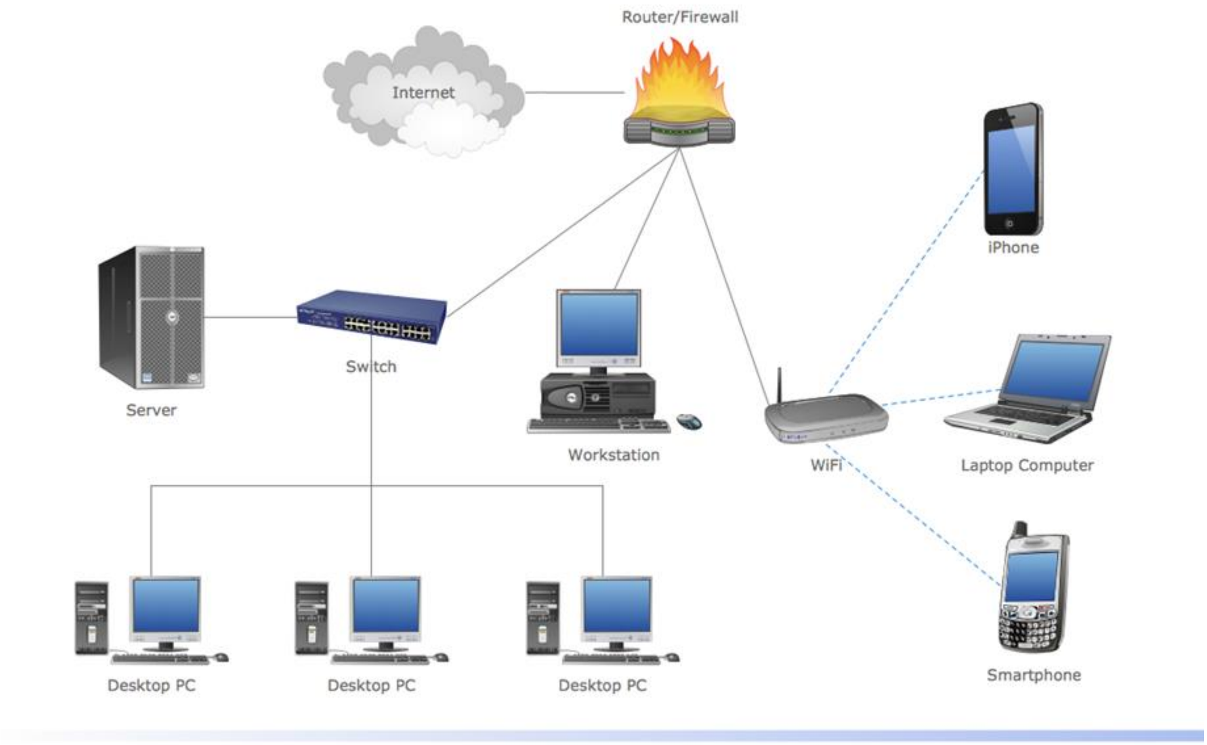
- Physical security
- Authentication mechanisms
- Network segmentation
- Configuration management
- Monitoring and logging
- Patch management
- Social engineering awareness
- Data leakage prevention
- Denial of service protection

by thoroughly examining these areas, we aim to identify vulnerabilities and provide recommendations to enhance the overall security posture of the office network.

Scope

The scope of this risk assessment includes all network devices, systems, and infrastructure components within a typical small office network. This encompasses:

- Routers
- Switches
- Firewalls
- Servers Endpoints (such as desktop PCs, laptops, smartphones, and workstations)
- Wireless access points
- Any other devices connected to the network



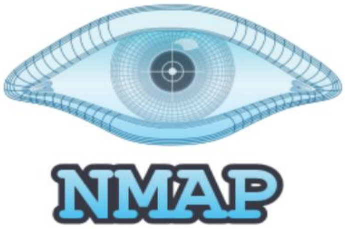
Threats and vulnerabilities Identification

- ## Router:
  - Threats : Someone getting into the router and messing with settings
  - Vulnerabilities : Easy-to-guess passwords or not updating the router's security.
- ## Switch:
  - Threats : Someone sneaking into the network by tricking the switch.
  - Vulnerabilities : Weak passwords or not setting up the switch's security features properly
- ## Employees:
  - Threats : Employees accidentally or purposely causing trouble with the network.
  - Vulnerabilities : Using easy passwords or not updating software, making it easier for attackers to get in.
- ## Firewall:
  - Threats : Employees accidentally or purposely causing trouble with the network.
  - Vulnerabilities : Using easy passwords or not updating software, making it easier for attackers to get in.
- ## File Server:
  - Threats : Someone breaking into the file server and stealing or messing with files.
  - Vulnerabilities : Letting too many people access the files or not protecting them well enough.
- ## Internet Connection:
  - Threats : Cyber attacks from outside, like viruses or hackers trying to break in.
  - Vulnerabilities : Weak spots in the connection could let attackers in, like if the firewall isn't set up right

Vulnerability Scanning

The risk assessment was conducted using a combination of technical assessments, interviews, documentation reviews, and analysis of existing security controls and practices. Vulnerability scanning tools, penetration testing techniques, and manual configuration reviews were employed to identify potential vulnerabilities and weaknesses in the network infrastructure. Inte reviews with key personnel were conducted to gather information on existing security policies, procedures, and practices.

Tools:



Nmap: Essential for network mapping and security auditing.

Nessus: Effective for vulnerability scanning and assessments.

NMAP Scanning

1. Install Nmap:

   Nmap is available for various operating systems, including Windows, Linux, and macOS.

2. Identify Target hosts:

   We determine the IP addresses or hostnames of the devices we want to scan in our network topology. This includes devices such as routers, switches, firewalls, laptops and file server.

3. Run Basic Scan:

   We open a command prompt or terminal window on your computer and use the nmap command with the IP addresses or hostnames of the target devices.

   For example: nmap ’IP Address’.

   This will perform a basic scan on the specified IP address to identify open ports and running services.

4. Scan Specific Ports:

   We can also specify specific ports or port ranges to scan using the -p option. For example, to scan ports 1-100 we can use:

   ```
   nmap -p 1-100 ‘IP Adresse’
   ```

5. Perform OS Detection:

   Nmap can attempt to detect the operating system running on the target devices using the -O option. This can provide additional information about the devices in your network.

   For example, if we want to detect the os of a given machine we can use:

   ```
   nmap -O ‘IP Adresse’
   ```

6. Output Results:

   By default, Nmap will display the scan results in the terminal window. We can also save the results to a file for later analysis using the -oN option followed by the desired filename.

7. Interpret Results:

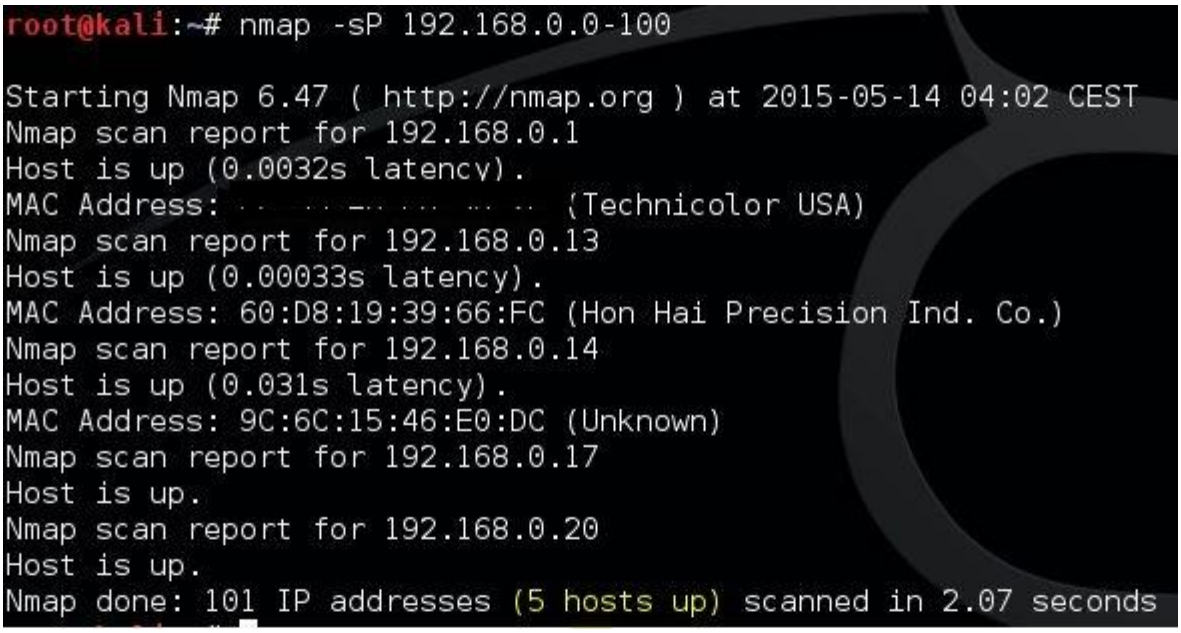
   We can review the scan results to identify open ports, running services, and potentially vulnerable configurations. Pay attention to any unexpected or unauthorized services running on the devices.

8. Repeat for Other Devices:

We repeat the scanning process for other devices in your network topology,

Scanning Output:

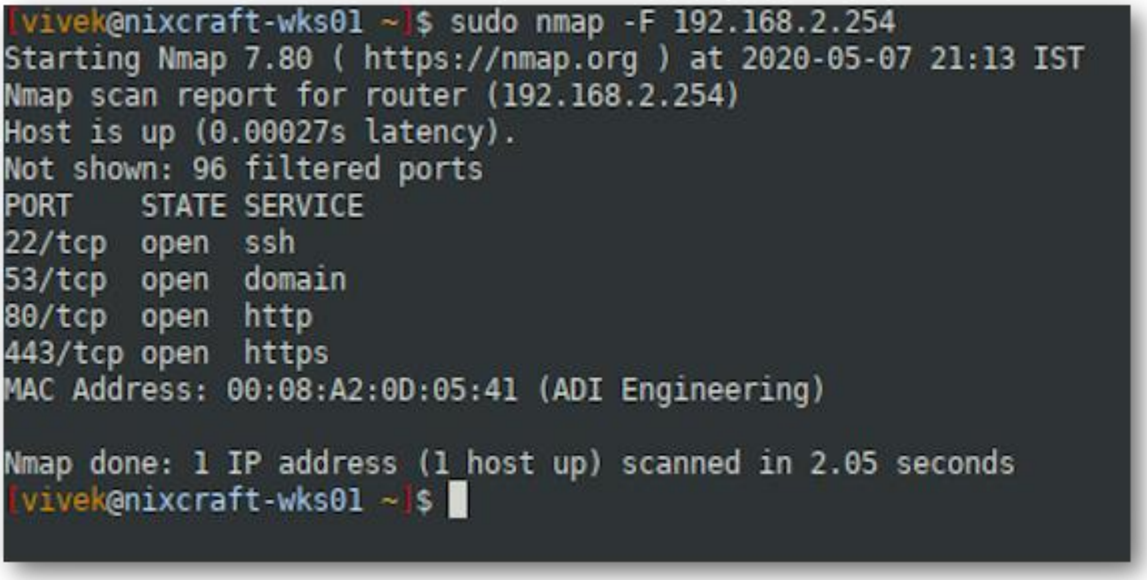
1. Live Hosts Scan Example:



```
root@kali:~# nmap -sP 192.168.0.0-100

Starting Nmap 6.47 ( http://nmap.org ) at 2015-05-14 04:02 CEST
Nmap scan report for 192.168.0.1
Host is up (0.0032s latency).
MAC Address: [redacted] (Technicolor USA)
Nmap scan report for 192.168.0.13
Host is up (0.00033s latency).
MAC Address: 60:D8:19:39:66:FC (Hon Hai Precision Ind. Co.)
Nmap scan report for 192.168.0.14
Host is up (0.031s latency).
MAC Address: 9C:6C:15:46:E0:DC (Unknown)
Nmap scan report for 192.168.0.17
Host is up.
Nmap scan report for 192.168.0.20
Host is up.
Nmap done: 101 IP addresses (5 hosts up) scanned in 2.07 seconds
```

2. Port Scan Example:



```
[vivek@nixcraft-wks01 ~]$ sudo nmap -F 192.168.2.254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 21:13 IST
Nmap scan report for router (192.168.2.254)
Host is up (0.00027s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:08:A2:0D:05:41 (ADI Engineering)

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
[vivek@nixcraft-wks01 ~]$
```

Nessus Scanning

1. **Install Nessus:**
   a. We download and install Nessus on a computer within our network. Nessus is available for various operating systems, including Windows, Linux, and macOS.
   b. We launch Nessus and follow the setup wizard to configure the necessary settings, such as network scanning preferences and credentials for authenticated scans.
2. **Create a New Scan:**
   a. We log in to the Nessus web interface using our credentials.
   b. We click on the "Scans" tab and then on the "New Scan" button.
   c. We provide a name for our scan and select the appropriate scan template based on your requirements. For a basic network scan, we can use the "Basic Network Scan" template.
3. **Configure Scan Targets:**
   a. We specify the IP addresses or hostnames of the devices we want to scan in our network topology.
   b. We can also define scan ranges or import target lists from a file.
4. **Scan Options:**
   a. We customize scan options based on your requirements. For example, we can configure scan intensity, scan speed, and port scanning preferences.
   b. We can enable credential-based scanning if we have credentials for authenticated scans on Windows systems (e.g., Windows 10 laptops and Windows Server 2019 file server).
5. **Schedule and Launch Scan:**

a. Optionally, we can schedule the scan to run at a specific date and time or configure recurring scans for continuous monitoring.
b. We click on the "Launch" button to start the scan.

6. Review Scan Results:

a. Once the scan is complete, we navigate to the "Scans" tab to view the scan results.
b. We click on the completed scan to view detailed findings, including identified vulnerabilities, misconfigurations, and compliance issues.

7. Prioritize Remediation:

a. Review the scan results to prioritize remediation efforts based on the severity and potential impact of identified vulnerabilities.
b. Generate reports with risk scores and recommended actions for addressing high-risk vulnerabilities.

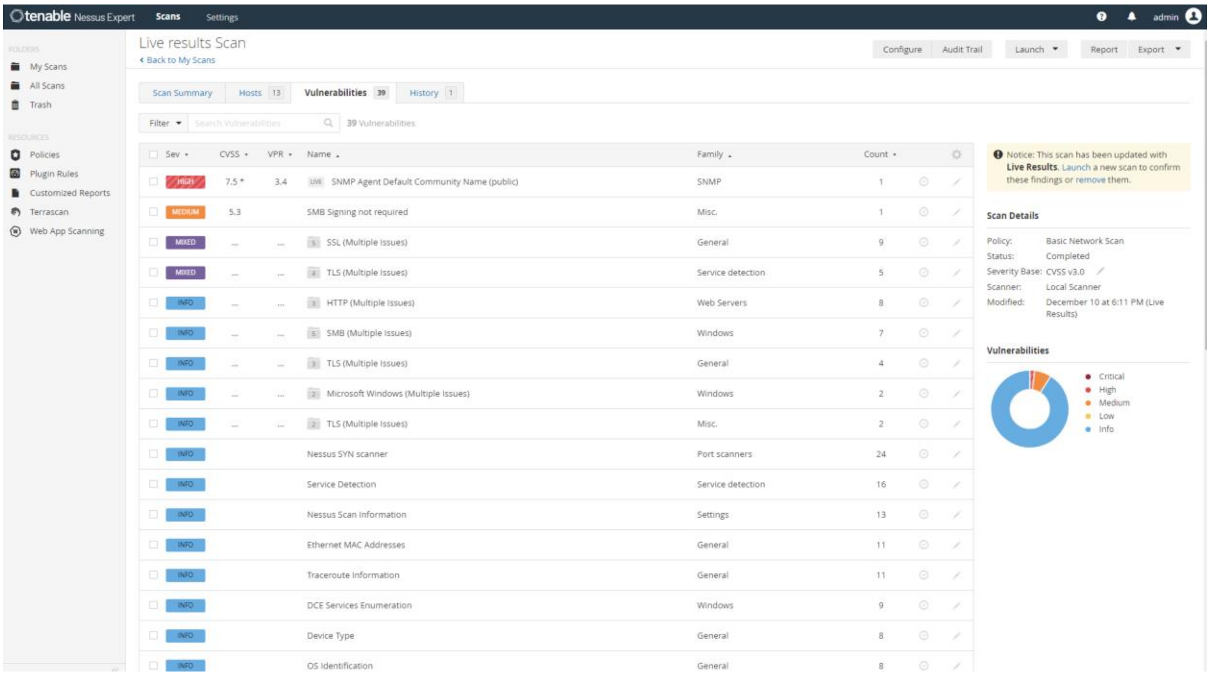
8. Remediate Vulnerabilities:

a. Work with relevant teams to remediate identified vulnerabilities and security weaknesses across your network infrastructure.
b. Follow best practices and security guidelines to apply patches, update configurations, and mitigate security risks.

9. Continuous Monitoring:

a. Schedule regular scans with Nessus to ensure continuous monitoring of your network topology for new vulnerabilities and changes in the security posture
b. Adjust scan frequencies and timing based on the dynamic nature of your environment.

Scanning Output Example:



Live results Scan

‹ Back to My Scans

39 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
HIGH	7.5 *	3.4	LIVE SNMP Agent Default Community Name (public)	SNMP	1
MEDIUM	5.3		SMB Signing not required	Misc.	1
MIXED	...	...	5 SSL (Multiple Issues)	General	9
MIXED	...	...	4 TLS (Multiple Issues)	Service detection	5
INFO	...	...	3 HTTP (Multiple Issues)	Web Servers	8
INFO	...	...	5 SMB (Multiple Issues)	Windows	7
INFO	...	...	3 TLS (Multiple Issues)	General	4
INFO	...	...	2 Microsoft Windows (Multiple Issues)	Windows	2
INFO	...	...	2 TLS (Multiple Issues)	Misc.	2
INFO			Nessus SYN scanner	Port scanners	24
INFO			Service Detection	Service detection	16
INFO			Nessus Scan Information	Settings	13
INFO			Ethernet MAC Addresses	General	11
INFO			Traceroute Information	General	11
INFO			DCE Services Enumeration	Windows	9
INFO			Device Type	General	8
INFO			OS Identification	General	8

Notice: This scan has been updated with **Live Results**. Launch a new scan to confirm these findings or remove them.

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Modified:	December 10 at 6:11 PM (Live Results)

Vulnerabilities

Identifying vulnerabilities

Since we don't have access to real systems, we'll simulate the scan results for some component in the network for most known vulnerabilities :

- ### Desktop PC 1 (192.168.1.10/24):

  Identified Vulnerabilities:

  - **Outdated Operating System:** The operating system is outdated and lacks recent security patches.
    - Severity: High
    - Potential Impact: Increases the risk of compromise through known vulnerabilities.
  - **Weak Password Policies:** User accounts have weak password policies.
    - Severity: Medium

        - Potential Impact: Makes it easier for attackers to gain unauthorized access through brute force attacks.

- ### Desktop PC 2 (192.168.1.11/24):

  Identified Vulnerabilities:

  - **Unpatched Software**: Several installed software applications are not up-to-date.
    - Severity: High
    - Potential Impact: Increases the risk of exploitation through known vulnerabilities.
  - **Lack of Antivirus**: No antivirus software is installed.
    - Severity: High
    - Potential Impact: Leaves the system vulnerable to malware attacks.

- ### Desktop PC 3 (192.168.1.12/24):

  Identified Vulnerabilities:

  - **Default User Accounts**: Default user accounts are enabled and have not been secured.
    - Severity: High
    - Potential Impact: Allows attackers to gain unauthorized access with default credentials.
  - **Insufficient Logging**: System activity is not adequately logged.
    - Severity: Medium
    - Potential Impact: Makes it difficult to detect and investigate security incidents.

- ### Switch (192.168.1.20/24):

  Identified Vulnerabilities:

  - **Default Credentials**: Switch is accessible using default administrative credentials.
    - Severity: High
    - Potential Impact: Allows unauthorized access to network configurations.

    - **Unsegmented Network**: Lack of VLANs for network segmentation.
        - Severity: Medium
        - Potential Impact: Increases the risk of lateral movement within the network.

- **Server (192.168.1.30/24):**

  Identified Vulnerabilities:
    - **Lack of Encryption**: Data on the server is not encrypted at rest.
        - Severity: Medium
        - Potential Impact: Increases the risk of data exposure in the event of unauthorized access.
    - **Excessive User Privileges**: Some users have unnecessary administrative privileges on the server.
        - Severity: High
        - Potential Impact: Increases the risk of unauthorized changes or data breaches.

- **Workstation (192.168.1.40/24):**

  Identified Vulnerabilities:
    - **Outdated Software**: Critical software applications are outdated.
        - Severity: High
        - Potential Impact: Increases the risk of exploitation through known vulnerabilities.
    - **Weak Authentication**: Uses weak passwords for user authentication.
        - Severity: Medium
        - Potential Impact: Easier for attackers to gain unauthorized access.

- **Router (192.168.1.1/24):**

  Identified Vulnerabilities:

    - **Default Credentials**: Router is using default administrative credentials.
        - Severity: High
        - Potential Impact: Allows attackers to change network settings and compromise the network.
    - **Unsecured Remote Management:** Remote management is enabled without proper security controls.
        - Severity: High
        - Potential Impact: Allows remote attackers to access and control the router.
- Firewall (192.168.1.254/24):

  Identified Vulnerabilities:
    - **Misconfigured Rules**: Firewall rules are not properly configured.
        - Severity: High
        - Potential Impact: May allow unauthorized traffic to pass through, compromising network security.
    - **Lack of Logging**: Firewall activity is not adequately logged.
        - Severity: Medium
        - Potential Impact: Makes it difficult to detect and investigate security incidents.
- WiFi (192.168.1.100/24):

  Identified Vulnerabilities:
    - **Weak Encryption**: WiFi is using weak encryption protocols (e.g., WEP).
        - Severity: High
        - Potential Impact: Makes it easier for attackers to intercept and decrypt network traffic.
    - **Default SSID**: WiFi is using a default SSID, which can be easily identified and targeted.
        - Severity: Medium
        - Potential Impact: Increases the likelihood of being targeted by attackers.

Risk Analysis

- This analysis prioritizes the identified vulnerabilities based on their severity and likelihood of exploitation. We'll use a scale of High, Medium, and Low for both factors.
- Prioritization Factors:
  - **Severity**: The potential impact of a vulnerability being exploited. (High, Medium, Low)
  - **Likelihood of Exploitation**: The chance of an attacker successfully exploiting the vulnerability. (High, Medium, Low)

System	Vulnerability	Severity	Likelihood	Priority
Desktop PC 1	Outdated Operating System	High	Medium	High
Desktop PC 1	Weak Password Policies	Medium	Medium	Medium
Desktop PC 2	Unpatched Software	High	Medium	High
Desktop PC 2	Lack of Antivirus	High	Medium	High(Critical)
Desktop PC 3	Default User Accounts	High	Medium	High
Desktop PC 3	Insufficient Logging	Medium	Low	Medium
Switch	Default Credentials	High	Medium	High(Critical)
Switch	Unsegmented Network	Medium	Medium	Medium
Server	Lack of Encryption (at rest)	Medium	Medium	Medium

Server	Excessive User Privileges	High	Medium	High(Critical)
Workstation	Outdated Software	High	Medium	High
Workstation	Weak Authentication	Medium	Medium	Medium
Router	Default Credentials	High	High	High(critical)
Router	Unsecured Remote Management	High	Medium	High
Firewall	Misconfigured Rules	High	Medium	High(Critical)
Firewall	Lack of logging	Medium	Low	Medium
WiFi	Weak Encryption	High	High	High(Critical)
WiFi	Default SSID	Medium	Medium	Medium

Recommendations to Secure the Network

1. Desktop PC 1

Outdated Operating System: Update the operating system to the latest version and ensure that all security patches are applied promptly.
Weak Password Policies: Implement and enforce strong password policies, requiring complex passwords and regular password changes.

2. Desktop PC 2

Unpatched Software: Regularly update all installed software applications to their latest versions to ensure vulnerabilities are patched.
Lack of Antivirus: Install and maintain reputable antivirus software, ensuring that it is regularly updated.

3. Desktop PC 3

Default User Accounts: Disable default user accounts or change their credentials to strong, unique passwords.
Insufficient Logging: Enable and configure logging to monitor system activities and detect potential security incidents.

4. Switch

Default Credentials: Change the default administrative credentials to strong, unique passwords.
Unsegmented Network: Implement VLANs to segment the network and limit the scope of potential attacks.

5. Server

Lack of Encryption (at rest): Implement encryption for data stored on the server to protect against unauthorized access.
Excessive User Privileges: Review and restrict administrative privileges to only those users who absolutely need them.

6. Workstation

Outdated Software: Ensure all software applications on the workstation are updated to the latest versions.
Weak Authentication: Implement multi-factor authentication (MFA) to enhance security.

7. Router

Default Credentials: Change the default administrative credentials to strong, unique passwords.
Unsecured Remote Management: Disable remote management or secure it with strong passwords and, if possible, use VPNs for remote access.

8. Firewall

Misconfigured Rules: Review and properly configure firewall rules to ensure only necessary traffic is allowed.
Lack of Logging: Enable and configure logging to monitor firewall activities and detect potential security incidents.

9. WiFi

Weak Encryption: Upgrade to a stronger encryption protocol such as WPA3.
Default SSID: Change the default SSID to a unique name that does not reveal the network's identity.

General Recommendations:

Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address new vulnerabilities.

Employee Training: Provide regular cybersecurity awareness training to employees to help them recognize and avoid common threats such as phishing and social engineering.

Patch Management: Implement a robust patch management process to ensure all systems and applications are kept up-to-date with the latest security patches.

Backup and Recovery: Establish and maintain a comprehensive backup and recovery plan to ensure data integrity and availability in case of an attack or system failure.

Network Monitoring: Deploy network monitoring tools to continuously monitor network traffic and detect suspicious activities.

Incident Response Plan: Develop and regularly update an incident response plan to quickly and effectively respond to security incidents.