Simulated Network Security Audit Report

Network Type: Home Network
Prepared by: ALI KAZUNGU
Date: 04/08/2025

1. Introduction

This report presents the findings of a simulated security audit conducted on a small-scale network, typically found in home offices. The network comprises a router, three personal computers (PCs), a wireless access point and a network printer. The audit aims to identify potential vulnerabilities and recommend effective mitigation strategies to enhance the overall security posture of the network.

2. Network Overview

The network setup includes the following devices:

- **Router** (wired to PCs and printer)
- **Three Desktop PCs**
- **Wi-Fi Access Point**
- **Network Printer**

This topology supports both wired and wireless connectivity and enables shared access to printing and internet resources.

3. Identified Security Vulnerabilities

Five critical vulnerabilities were discovered:

1. **Default Router Credentials**
   The router still uses factory-set login credentials, making it a prime target for unauthorized access.
2. **Unsecured Wi-Fi Access**
   The wireless network either lacks encryption or uses outdated security protocols (e.g., WEP), exposing it to eavesdropping and unauthorized connections.
3. **Outdated Firmware and Software**
   The PCs and network printer have not been updated regularly, leaving them vulnerable to known exploits.
4. **Lack of Endpoint Security**
   The PCs operate without antivirus software or active firewalls, increasing the risk of malware infection and internal spread.
5. **Unrestricted Printer Access**
   The printer is accessible over the network without authentication, allowing potential misuse or exploitation.

4. Recommended Mitigations

1. **Secure Router Access**
   - Change the default admin username and password.
   - Disable remote administration unless absolutely necessary.
2. **Strengthen Wi-Fi Security**
   - Enable WPA3 encryption (or WPA2 as a minimum).
   - Implement MAC address filtering and consider hiding the SSID.
3. **Implement Patch Management**
   - Regularly update operating systems, drivers, and firmware for all devices.
   - Enable automatic updates where possible.
4. **Deploy Endpoint Protection**
   - Install antivirus and anti-malware software on all PCs.
   - Enable software and hardware firewalls; train users on cyber hygiene.
5. **Harden Printer Security**
   - Restrict access via administrative credentials.
   - Disable unnecessary network services (e.g., Telnet, FTP).
   - Enable logging and monitor access regularly.

5. Conclusion

While this network is functional for basic home operations, its current configuration exposes it to significant security risks. The implementation of the above mitigation strategies will substantially reduce the network’s attack surface and enhance the confidentiality, integrity, and availability of its resources.