**Basic Security Audit Report**

**Prepared by: Muhammad Talah Khan**

**Date: [04/03/2025]**

**System Audited:** [Acer Predator]

# Comprehensive Security Audit Report

## Overview of Current Security Settings and Configurations

The current security settings and configurations have been thoroughly reviewed across several critical areas to identify potential vulnerabilities and areas for improvement.

### 1.1 System Settings:

User Accounts: While most user accounts possess strong passwords, a notable deficiency exists in the lack of two-factor authentication for some accounts, which significantly enhances security by requiring an additional form of verification beyond just a password.

Automatic Updates: The system is configured to automatically update, ensuring that timely security patches are applied to protect against newly discovered vulnerabilities.

Firewall Configurations: Although the firewall is enabled, it lacks specific rules to block known malicious IP addresses, which could allow unauthorized traffic to reach the system.

### 1.2 Antivirus and Malware Scan:

Malware Scan: A recent scan did not detect any malware, but the antivirus software is not updated to the latest version, which could leave it ineffective against newer threats.

Antivirus Software: Windows Defender is installed and running, providing baseline protection against malware.

### 1.3 Browser Security Settings:

Privacy Settings: Browser privacy settings are not fully optimized, allowing some tracking cookies to compromise user privacy.

Cookie Policies: Cookies are not automatically cleared upon browser closure, potentially leaving sensitive data exposed.

Security Configurations: While HTTPS is enforced for secure connections, some security extensions are outdated, which could expose users to known vulnerabilities.

### 1.4 Password Management:

Password Manager: A password manager is not installed, leading to weak and non-unique passwords across accounts.

Password Strength and Uniqueness: Many stored passwords lack the complexity and uniqueness required to prevent unauthorized access.

### 1.5 Network Security:

Encryption Protocols: The network uses WPA2 encryption, which is outdated and vulnerable to certain attacks.

Password Strength: The network password is weak and has not been changed recently, increasing the risk of unauthorized access.

Unauthorized Access Prevention: MAC address filtering is not enabled, allowing any device to connect to the network.

## Identified Vulnerabilities or Areas of Concern

Weak Passwords: Inadequate password strength combined with the lack of two-factor authentication for user accounts significantly increases the risk of unauthorized access.

Outdated Antivirus Software: The failure to update antivirus software to the latest version may result in ineffective protection against new malware threats.

Inadequate Browser Privacy: Allowing tracking cookies and using outdated security extensions compromise user privacy and security.

Lack of Password Manager: The absence of a password manager leads to weak and non-unique passwords, increasing the risk of password compromise.

Network Encryption: The use of outdated WPA2 encryption and weak network passwords makes the network vulnerable to hacking.

Firewall Configuration: The lack of specific rules to block malicious traffic leaves the system open to potential attacks.

## Potential Risks Associated with the Findings

Unauthorized Access: Weak passwords and outdated encryption protocols increase the risk of unauthorized access to user accounts and the network, potentially leading to data theft or system compromise.

Malware Infections: Outdated antivirus software may fail to detect and remove new malware threats, resulting in system compromise or data loss.

Data Breaches: Inadequate browser privacy settings and the lack of a password manager increase the risk of data breaches through tracking and password compromise.

Network Compromise: Weak network passwords and outdated encryption protocols make the network vulnerable to hacking, which could lead to unauthorized access and data theft.

## Recommendations for Improving Security

### 4.1 System Settings Improvements:

Implement Two-Factor Authentication: Enable two-factor authentication for all user accounts to significantly enhance security.

Update Firewall Rules: Add specific rules to block known malicious IP addresses and prevent unauthorized traffic.

### 4.2 Antivirus and Malware Scan Improvements:

Update Antivirus Software: Ensure the antivirus software is updated to the latest version to protect against new threats.

Regular Scans: Schedule regular malware scans to detect and remove any malware promptly.

### 4.3 Browser Security Settings Improvements:

Optimize Privacy Settings: Block all tracking cookies and configure the browser to clear cookies upon closure to enhance user privacy.

Update Security Extensions: Ensure all security extensions are updated to protect against known vulnerabilities.

### 4.4 Password Management Improvements:

Install a Password Manager: Install a reputable password manager like LastPass or 1Password to generate and store strong, unique passwords.

Password Strengthening: Use the password manager to generate strong, unique passwords for all accounts.

### 4.5 Network Security Improvements:

Upgrade Encryption Protocol: Update the network encryption to WPA3 to ensure robust protection against hacking attempts.

Strengthen Network Password: Change the network password to a strong, unique one and ensure it is changed regularly.

Enable MAC Address Filtering: Configure MAC address filtering to prevent unauthorized devices from connecting to the network.

## Step-by-Step Instructions

### 5.1 Installing a Password Manager:

Download and install a reputable password manager (e.g., LastPass).

Create a strong master password.

Import existing passwords and generate new strong passwords for each account using the password manager.

### 5.2 Updating Network Encryption:

Access the router settings via its IP address.

Navigate to the wireless settings section.

Select WPA3 as the encryption protocol.

Save changes and restart the router.

### 5.3 Enabling Two-Factor Authentication:

Go to account settings for each user account.

Look for two-factor authentication options (e.g., SMS, authenticator app).

Enable two-factor authentication for each account.

## Conclusion

Implementing these recommendations will significantly enhance the security posture of the system, reducing vulnerabilities and potential risks. Regular audits and updates are crucial to maintaining robust security configurations and ensuring ongoing protection against evolving threats. By addressing these areas of concern, organizations can protect sensitive data and maintain the trust of their users.