Secure Wireless Networks Documentation

Overview

This document outlines the implementation of security measures for a wireless network, including the configuration of WPA3 for encryption and the deployment of a Wireless Intrusion Prevention System (WIPS) to safeguard against unauthorized access.

Network Configuration Details

1. Wireless Network Encryption: WPA3

Network Name (SSID): SecureNet-Home
Frequency Bands: 2.4 GHz and 5 GHz
Encryption Protocol: WPA3-Personal

Configuration Steps:

1. **Access Router Settings:**
    - Login to the router's admin interface via its IP address (e.g., `192.168.1.1`).
    - Use administrator credentials.
2. **Enable WPA3 Encryption:**
    - Navigate to **Wireless Settings** or **Security Settings**.
    - Select WPA3-Personal from the available security protocols.
3. **Set a Strong Password:**
    - Password requirements: Minimum 12 characters, including uppercase, lowercase, numbers, and special symbols.
    - Example Password: `5ecur3N3tw0rk!`
4. **Save and Apply Changes:**
    - Reboot the router if necessary.
    - Verify all connected devices support WPA3.

2. Wireless Intrusion Prevention System (WIPS)

Purpose:

To monitor the wireless network for potential threats and prevent unauthorized access by rogue devices or access points.

Components of WIPS:

- **Sensor Devices:**
  - Deployed strategically to detect and analyze network traffic.
  - Positioned in areas prone to unauthorized access.
- **WIPS Software:**
  - Runs on a dedicated server or cloud platform.
  - Provides real-time alerts and mitigation options.

Configuration Steps:

1. **Install WIPS Software:**
   - Use a trusted WIPS solution (e.g., Cisco Meraki Air Marshal, Aruba WIPS).
   - Follow vendor-specific installation guidelines.
2. **Define Security Policies:**
   - Configure rules to identify unauthorized devices.
   - Enable automatic prevention measures, such as:
     - Blocking rogue access points.
     - Disconnecting unauthorized users.
3. **Enable Alerts:**
   - Set up email or SMS notifications for detected threats.
   - Integrate with an IT ticketing system for efficient response.
4. **Perform Regular Audits:**
   - Review logs weekly for any irregular activities.
   - Update WIPS rules to adapt to emerging threats.

Testing and Verification

1. WPA3 Connectivity Test

- **Devices Used:** Laptop (Windows 11), Smartphone (Android 13), Tablet (iOS 17).
- **Process:**
  - Connect devices to the network using the WPA3-secured SSID.
  - Verify successful connection and internet access.
- **Result:**
  - All tested devices connected securely without issues.

2. WIPS Functionality Test

- **Simulated Threats:**
  - Attempted connection from a rogue access point.
  - Connection attempts from unauthorized devices.

- **Process:**
    - Monitor WIPS dashboard for detected threats.
    - Confirm automated blocking actions.
- **Result:**
    - WIPS successfully identified and mitigated all simulated threats.

Conclusion

The implementation of WPA3 encryption and a Wireless Intrusion Prevention System has significantly enhanced the security of the wireless network. These measures ensure robust protection against unauthorized access and cyber threats, safeguarding both sensitive data and network integrity.

Next Steps: Continue monitoring network performance and updating security configurations to address new vulnerabilities.