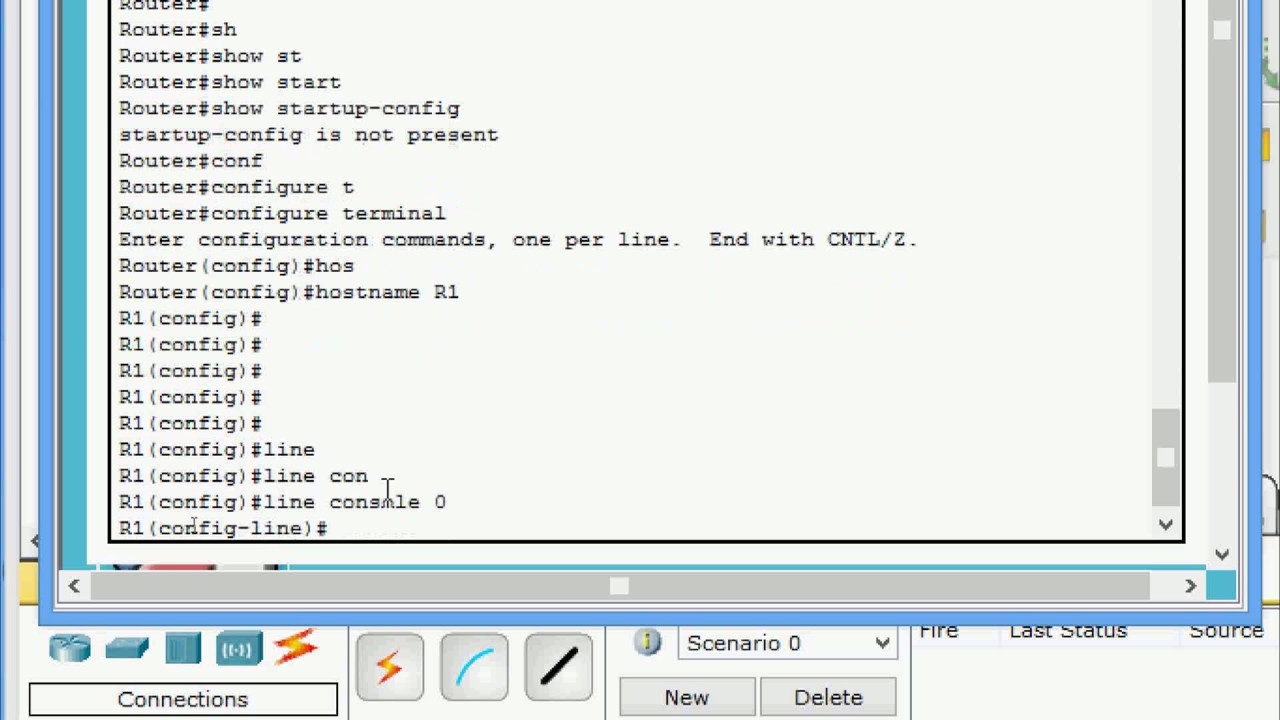
**Default Router Configuration**



Class: Cyber Security

Prepared by: Rickardo Brown, St Patrick Currey

# Date: 30/05/2023

# **Situation:** A small office sets up a new router without modifying its default configuration. The network contains sensitive information, and there is a concern about unauthorized access and potential attacks.

**Task:** Research the default settings of commonly used routers and analyze the security implications. Propose recommendations to secure the router configuration.

**Research and Recommendations:**

Research has shown that many commonly used routers come with default settings that may pose security risks if left unmodified. Here are the typical default settings and their security implications, along with recommendations to secure the router configuration:

1. Default Administrator Credentials:

Most routers have default usernames and passwords for the administrator account, such as

"admin/admin" or "admin/password." These default credentials are well-known and easily exploitable by attackers.

Recommendation: Change the default administrator username and password immediately after setting up the router. Choose a strong, unique password that combines letters, numbers, and special characters. Additionally, consider using a password manager to securely store and manage your router password.

2. Default Wi-Fi Network Name (SSID):

Manufacturers often assign a default Service Set Identifier (SSID) to Wi-Fi networks. These default SSIDs can reveal the router's brand and model, making it easier for attackers to identify potential targets.

Recommendation: Change the default SSID to a unique and nondescript name that does not disclose information about the router or the network. Avoid using personal or identifiable information in the SSID.

3. Default Wi-Fi Security Settings:

Many routers come with insecure default security settings, such as using outdated encryption protocols (e.g., WEP) or weak encryption keys.

Recommendation: Use the latest Wi-Fi Protected Access (WPA2 or WPA3) encryption protocol with a strong password. Implement AES encryption, which is more secure than older encryption algorithms like TKIP. Regularly update the Wi-Fi password and consider implementing a password rotation policy.

4. Firewall and Port Forwarding:

Routers typically have built-in firewalls, but they may be disabled by default. Additionally, some routers have pre-configured port forwarding rules that can expose internal network services to the internet, potentially allowing unauthorized access.

Recommendation: Enable the router's firewall to protect against external threats. Configure port forwarding rules only when necessary and review them regularly to ensure they are essential and properly secured. Disable port forwarding for any unnecessary services.

5. Remote Management:

Some routers have remote management features enabled by default, allowing administrators to manage the router from outside the local network. This can pose a security risk if left enabled, as it provides an additional entry point for attackers.

Recommendation: Disable remote management unless it is absolutely necessary. If remote management is required, limit access to specific IP addresses and use secure protocols like HTTPS for remote administration.

6. Firmware Updates:

Router manufacturers release firmware updates to address security vulnerabilities and improve performance. However, routers often do not automatically install these updates, leaving them exposed to known security flaws.

Recommendation: Regularly check for firmware updates from the router manufacturer's website and apply them promptly. Enable automatic firmware updates if available. Routinely review security bulletins and announcements from the manufacturer to stay informed about potential vulnerabilities.

7. Disable Unused Services:

Routers may have various additional services enabled by default, such as UPnP (Universal Plug and Play) or remote access protocols like Telnet or SSH. These services can introduce unnecessary security risks.

Recommendation: Disable any services that are not needed or used. Only enable essential services and protocols required for network functionality.

8. Guest Network Isolation:

Many routers support guest networks, which provide separate Wi-Fi access for visitors. However, if not properly configured, guest networks can potentially provide a bridge for attackers to access the internal network.

Recommendation: Enable guest network isolation to ensure that devices connected to the guest network cannot communicate with devices on the main network. This helps protect sensitive information from potential unauthorized access.

By implementing these recommendations, the small office can significantly enhance the security of their router configuration, reducing the risk of unauthorized access and potential attacks.