Wireless Network Security

Exercise 1: Configuring Security on a Wireless Router

A wireless router is a device that performs the functions of a router and includes the functions of a wireless access point.

Lab Scenario

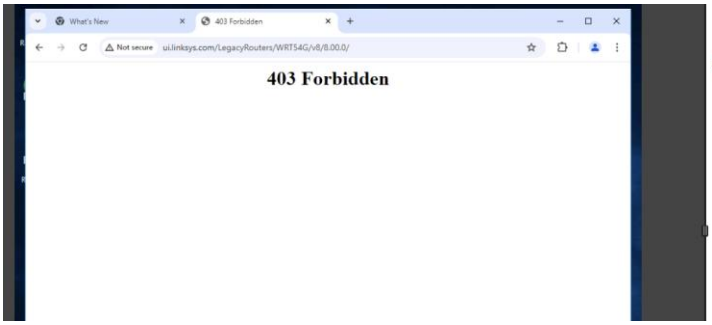
Organizations allow wireless devices to connect to their network in today's environment (Bring Your Own Device or BYOD). However, the security of the network infrastructure is a major challenge for organizations while adopting wireless devices. A wireless router/access point is the main entry for attackers. Attackers compromise wireless access points to gain access to the organization's network. Organizations should ensure that their wireless access points are configured securely. As a network defender, you should be able to configure the wireless router securely by applying all possible hardening techniques.

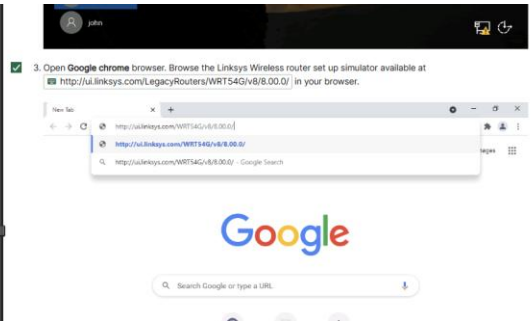
Lab Objectives

This lab will demonstrate the various hardening techniques on a wireless router.

Overview of Wireless Router Security

A wireless router is the first line of defense against attackers trying to access the organization's network. To prevent attackers from compromising the security of wireless routers, appropriate configuration changes need to be made in order to make a router more secure.





Lab Summary: Configuring Security on a Wireless Router

Scenario

This lab focused on securing a wireless router, which acts as both a router and an access point. Because wireless routers are often the first line of defense in BYOD environments, misconfigurations can expose the entire network to attacks.

Objectives
The lab demonstrated how to:

- Configure WPA2 encryption for wireless security
- Change default administrator credentials
- Disable remote management when unnecessary
- Enable the router's firewall and filtering features
- Adjust SSID broadcast settings for better security

Outcome
When the lab was originally completed in May, the router hardening steps were performed successfully using the online Linksys simulator. On review, however, the simulator link now returns a **403 Forbidden** error, preventing the configuration from being repeated in the current environment. Because of this, the May completion is treated as the successful execution, while the recent run-through relied on reviewing the provided instructions and screenshots.

Reflection
This exercise highlighted how essential it is to apply strong encryption, change default credentials, and disable unnecessary services to harden wireless routers. The current unavailability of the online simulator also shows the importance of documenting results promptly, since external lab resources may not remain accessible long-term.