

Module 5.2: WLAN Threats

Endpoint Security | Cisco Networking Academy

Prepared by: Kudzaishe Majeza

Agenda

- ▶ Wireless Security Overview
- ▶ DoS Attacks on WLANs
- ▶ Rogue Access Points
- ▶ Man-in-the-Middle Attacks
- ▶ Real-World WLAN Threats
- ▶ Summary

Wireless Security Overview

- ▶ Wireless networks transmit data over radio waves.
- ▶ This makes them easier to intercept than wired networks.
- ▶ Weak encryption and poor configuration increase risk.

DoS Attacks on WLANs

- ▶ Denial of Service attacks disrupt wireless availability.
- ▶ Attackers send deauthentication frames.
- ▶ Clients are forced offline repeatedly.

Rogue Access Points

- ▶ Unauthorized access points connected to a network.
- ▶ Can be malicious or misconfigured.
- ▶ Used to intercept traffic.

Man-in-the-Middle Attacks

- ▶ Attackers position themselves between client and AP.
- ▶ They intercept or modify data traffic.
- ▶ Often combined with rogue APs.

Summary

- ▶ Wireless threats exploit open communication.
- ▶ Monitoring and encryption are essential.
- ▶ User awareness reduces risk.