Rogue Access Point Simulation Report

Project Overview

This project demonstrates the creation and analysis of a rogue access point (AP) using the WiFi Pineapple and Kali Linux. The purpose was to simulate a real-world attack scenario where an attacker creates a fake network to intercept user data. The project also includes recommendations to mitigate such risks.

Objectives

Purpose:

- Simulate a rogue access point to analyze the risks posed by malicious APs.
- Understand how attackers capture sensitive data and exploit network vulnerabilities.

Scope:

- Focused on demonstrating how users might connect to a rogue AP and analyzing intercepted traffic.
- Includes recommendations for detecting and preventing rogue access points.

Methodology

Environment Setup

Hardware: WiFi Pineapple connected via USB to a Kali Linux VM running on VMware.

Network: All devices (WiFi Pineapple, Kali Linux VM, and testing devices) connected to the same Wi-Fi network.

Tools Used:

- WiFi Pineapple for rogue AP creation.
- Kali Linux tools such as Wireshark for traffic capture and analysis.

Simulation Procedure

1. Configured the WiFi Pineapple to act as a rogue AP broadcasting a fake SSID, *"Free Public WiFi."*
2. Enabled PineAP features:
    - Beacon Response.
    - SSID Pool broadcasting.

3.Set up traffic forwarding from the Pineapple to simulate internet access for connected clients.

4.Monitored traffic using Wireshark on Kali Linux to analyze captured data and identify potential vulnerabilities.

Category	Details
SSID Broadcasted	"Free Public Wifi"
Connected Clients	2 devices connected during simulation.
Traffic Captured	HTTP requests, DNS lookups, and unencrypted traffic packets.
Vulnerabilities Observed	Users connected to an untrusted network without verification.

Traffic Analysis

- Observed unencrypted HTTP traffic, including potential sensitive data.
- DNS queries exposed the browsing behavior of connected clients.

Recommendations

For Users:

1. Avoid connecting to unknown or untrusted Wi-Fi networks.
2. Verify the legitimacy of public networks before connecting.
3. Use a VPN to encrypt data traffic when using public Wi-Fi.

For Organizations:

1. Implement Wireless Intrusion Detection Systems (WIDS) to identify rogue APs.
2. Educate users on the risks of rogue access points.
3. Encourage the use of HTTPS and VPNs to secure communications.

Conclusion

The rogue access point simulation demonstrated the ease with which attackers can intercept unencrypted traffic and exploit user trust in public Wi-Fi networks. By implementing the recommended countermeasures, individuals and organizations can significantly reduce the risk posed by rogue access points and enhance overall network security.