Rogue_APs Documentation

Introduction

Rogue Access Points (Rogue APs) are unauthorized wireless access points used in penetration testing to mimic legitimate networks and capture user credentials.

Features

- Fake captive portals.
- DNS spoofing and redirection.
- Credential harvesting.
- Integration with tools like Hostapd, Dnsmasq, and Apache.

Installation

Requires hostapd, dnsmasq, apache2, and custom scripts.

Example on Kali:

```
sudo apt install hostapd dnsmasq apache2
```

Usage

Configure hostapd.conf and dnsmasq.conf

Start services:

```
sudo hostapd hostapd.conf
sudo dnsmasq -C dnsmasq.conf
```

Use phishing page hosted via Apache to capture credentials.

Disclaimer

Rogue APs are highly intrusive and must only be used in controlled, authorized environments.

Conclusion

Rogue APs are effective for testing user susceptibility to fake networks, especially in social engineering scenarios.