Information Gathering

Ricardo Reimao
CYBER SECURITY CONSULTANT

The main weaknesses are on the unknown

Module Overview

Packet capture

- Monitor mode (promiscuous mode)
- Network cards
- Antennas
- Aircrack-ng suite

Identifying target networks

Demo: Capturing packets and hidden networks

Packet Capture

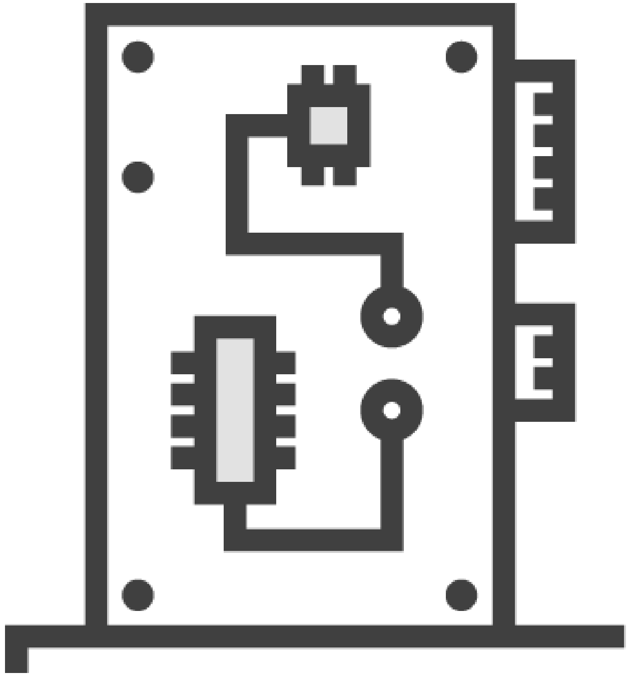
Promiscuous Mode

Default network interface

- Only listen to packets addressed to them or broadcast

Promiscuous (or monitor)

- Listen to any traffic, independent of the mac address



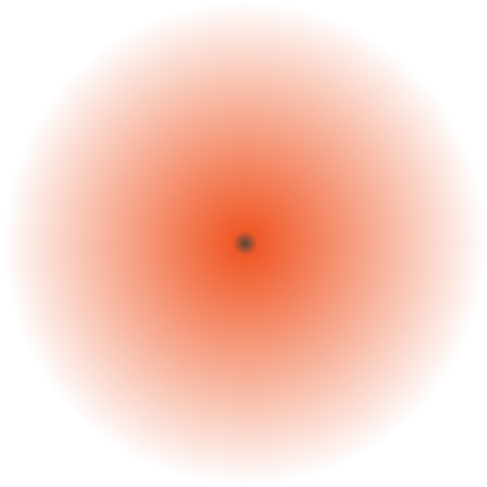
Network Cards

Packet injection and monitoring support

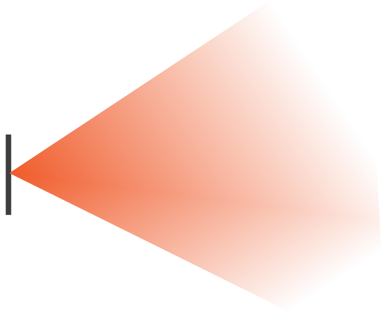
Compatible models

- TP-LINK TP-WN722N
- Alfa AWUS036NHA
- Alfa AWUS036NH
- D-Link DWL-G132

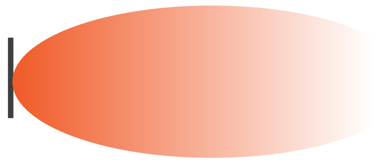
Antennas



Omni-directional



Directional



Highly directional (Yagi)

Airmon-NG Suite

Airmon-ng

Airodump-ng

Aireplay-ng

Aircrack-ng

Identifying Target Networks

Wireless Mapping

Simple solution

- Walking around the building with your laptop and a airmon-g

Fancy solution

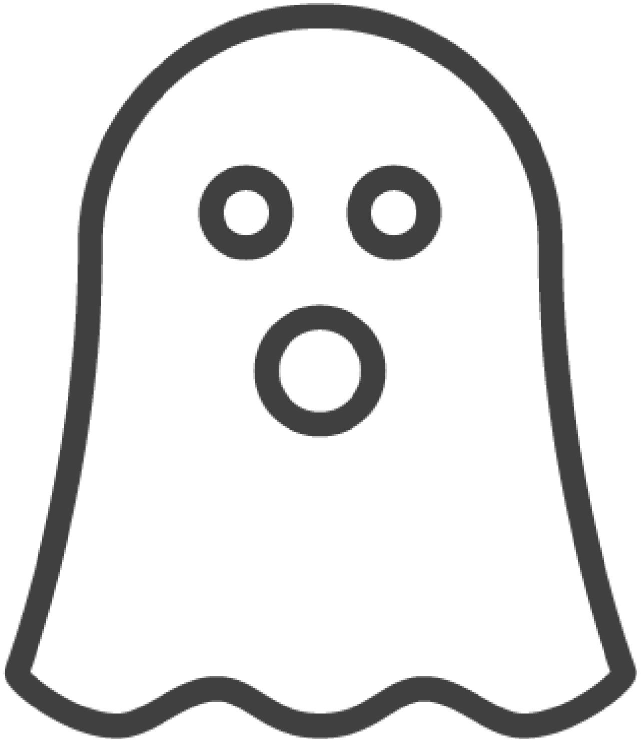
- Use of specific tools
  - Heatmapper

Rogue Access Points

Unintentional

Malicious

Hidden Wireless Networks



Networks that do not broadcast SSID

Perceived as a secure network

Any attacker would detect

Information Gathering

Demo

Enabling monitor mode

```
airmon-ng start <wlan0>
```

Analyzing the wireless traffic

```
airodump-ng <wlan0mon>
```

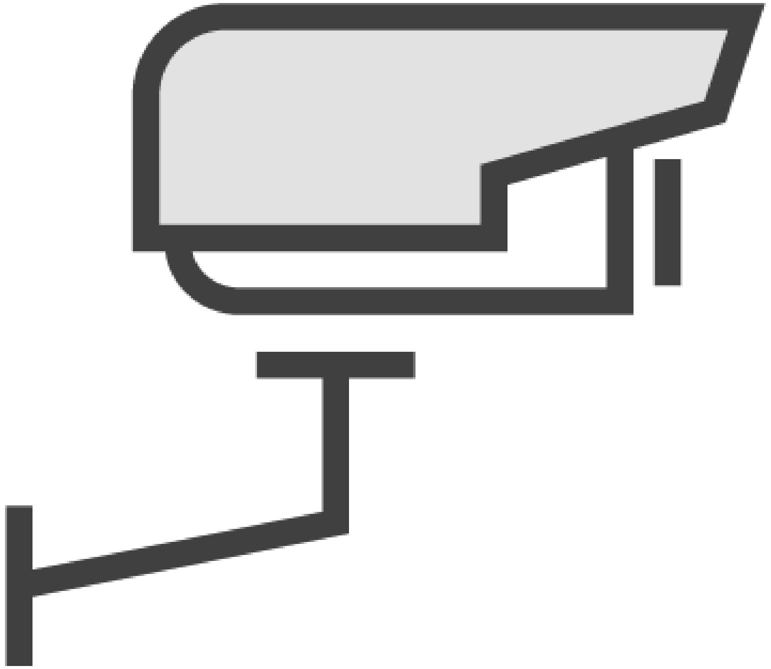
Identifying Hidden Networks

Demo

Identifying a hidden network

Creating a target list

Environment Information



GBM laptops (WPA2/WPS)
GBM cameras (WPE)
GBM guest Wi-Fi (open/portal authentication)
GBM cafeteria (open)

GBM Hidden (open)

Summary

Identifying all attack vectors is key!

Usually the vulnerabilities are on the non-documented parts of the system

Hidden networks provide a false sense of security

Next up:
Identifying and Exploiting Vulnerabilities