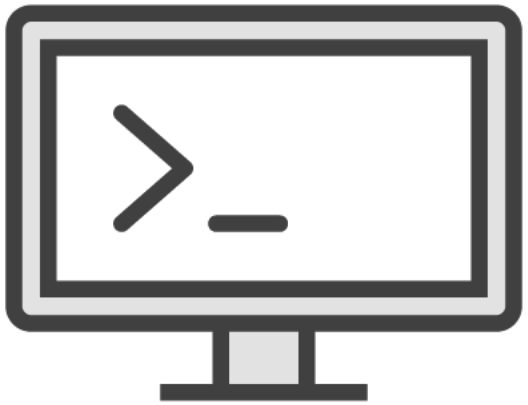
Wireless Network Penetration Testing

INTRODUCTION AND WIRELESS PENETRATION TEST PROCESS OVERVIEW

Ricardo Reimao
CYBER SECURITY CONSULTANT

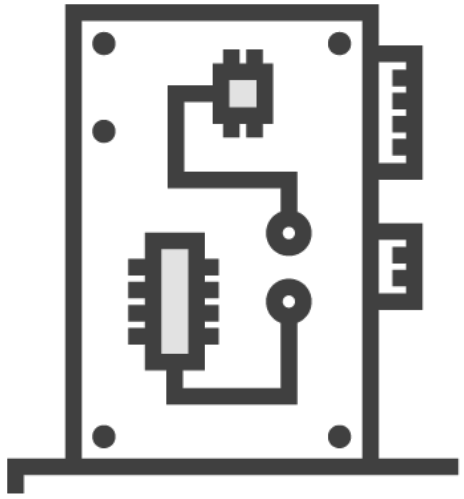
Almost all companies have wireless networks.

What You Will Need



Kali Linux VM

Basic Linux knowledge



Compatible network card

Module Overview

Wireless penetration testing process overview

Pre-engagement tasks

Our course scenario

Wireless Penetration Testing Process

Process Overview

1. Initiation
2. Information gathering
3. Vulnerability identification
4. Exploitation
5. Reporting

Initiation: Pre-engagement

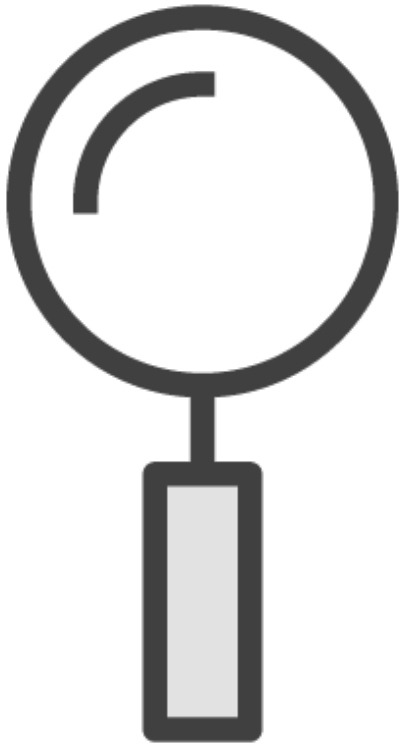
Define scope

Collect environment information

Schedule tests

Communicate to stakeholders

Get client formal sign-off



Information Gathering

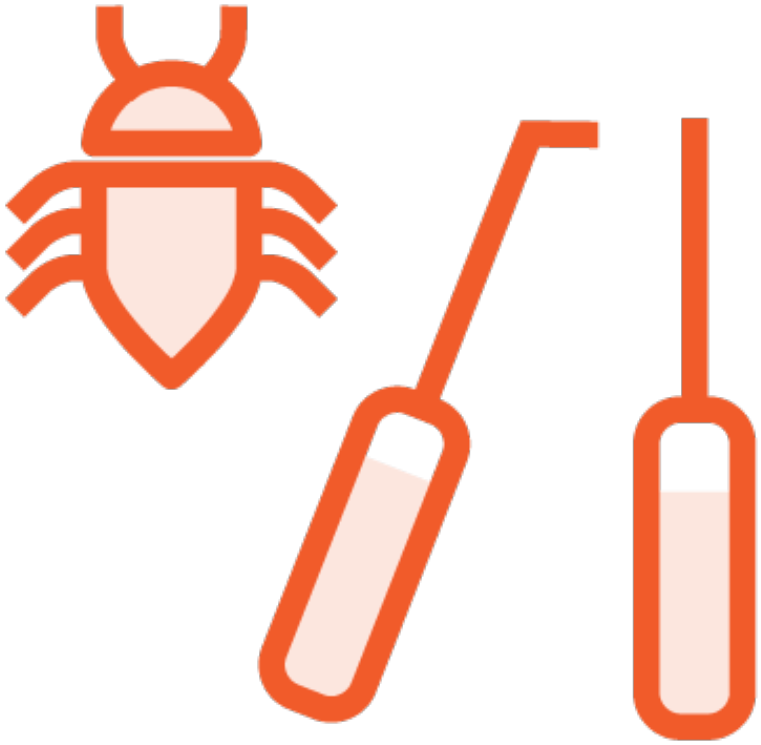
- Identify wireless networks
- Identify network segments
- Identify technologies used
- Identify protocols
- Create a target list

Vulnerability Identification

Identify potential attack vectors

Identify exploitations

Exploitation



Test potential vulnerabilities without breaking anything

Document successful attacks and potential attacks

Reporting

Describe the vulnerabilities found

Describe potential issues

Describe confirmed issues

Define risk

Propose recommendations

Pre-engagement Tasks

Define scope

Collect environment information

Schedule tests

Communicate to stakeholders

Get client formal sign-off

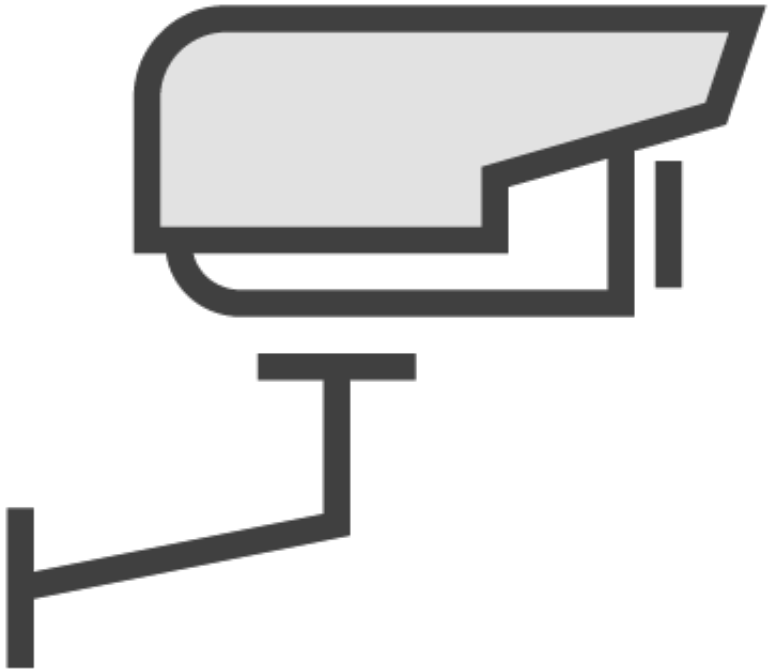
Initiation: Pre-engagement

Globomantics Course Scenario

Scope

Analyze all the wireless networks in the company, determine the risk of the current wireless networks, and propose improvements

Environmental Information



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

Schedule was agreed upon with the client

Communications were sent to IT Managers

Client signed off

Tests are ready to start

Module Summary

It is important to follow a process

The process is composed of 5 stages:

- Initiation
- Information Gathering
- Vulnerability Identification
- Exploitation
- Reporting

Pentests need to be scoped, scheduled and approved by the client

Next up:
Information Gathering