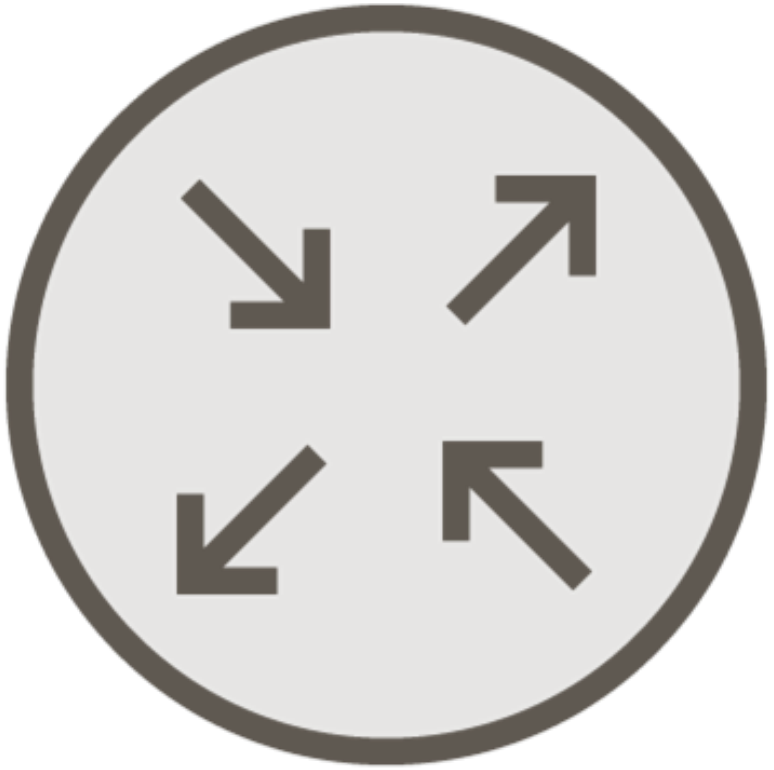
Identifying and Exploiting Vulnerabilities

Ricardo Reimao
CYBER SECURITY CONSULTANT

Wireless Vulnerabilities

Analytic attacks	Packet injection	Weak credentials
Eavesdropping	Brute-forcing	Authentication bypass

Open Networks



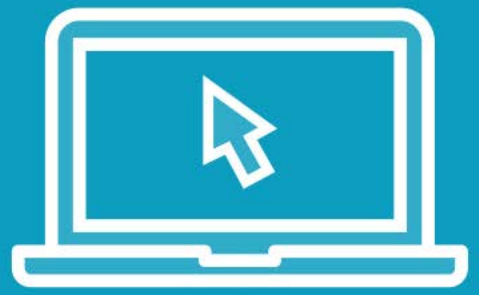
Open Networks

Usually implemented for guests

Unencrypted traffic, easy to eavesdrop

Can lead to internal networks

Demo



Listening traffic with Wireshark

Testing for misconfigured routes

WEP Networks

WEP Security Risks

Easy to recover the password

No protection against traffic injection

WEP Vulnerabilities

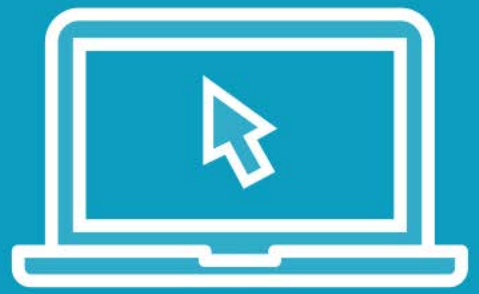
Initialization Vector (IV)

Vulnerable to analytic attacks

Lack of cryptographic integrity protection

Allows packet injection

Demo



Cracking a WEP network

WPA/WPA2 Networks

WPA/WPA2 PSK

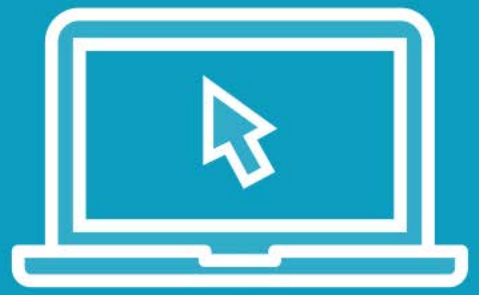
Improved security

Fixes most of the WEP vulnerabilities

Vulnerable to offline brute-force attacks

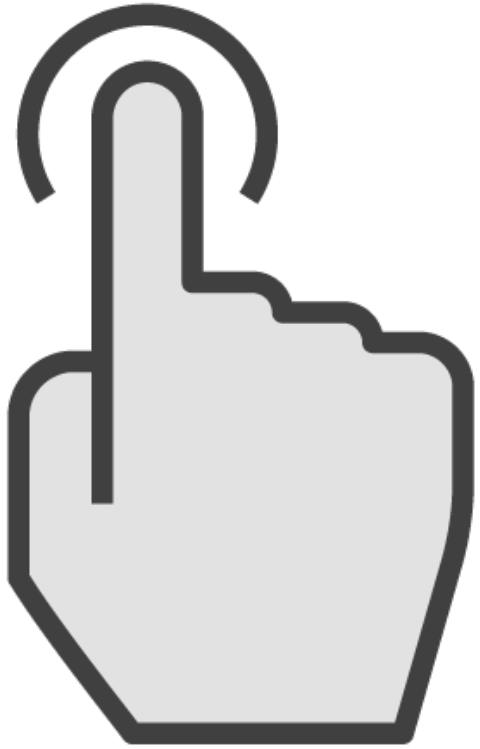
Risk depends on the strength of the key

Demo



Dictionary attack on a WPA/WPA2 network

WPS Enabled Network



Initial authentication: 8 digit pin

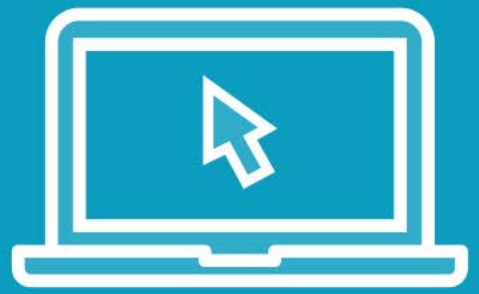
- Divided in two stages of 4 digits

Brute-force made easy:

- Guess the first 4 digits= 10k possibilities
- Guess the last 4 digits= 10k possibilities

Important to implement lock-outs

Demo

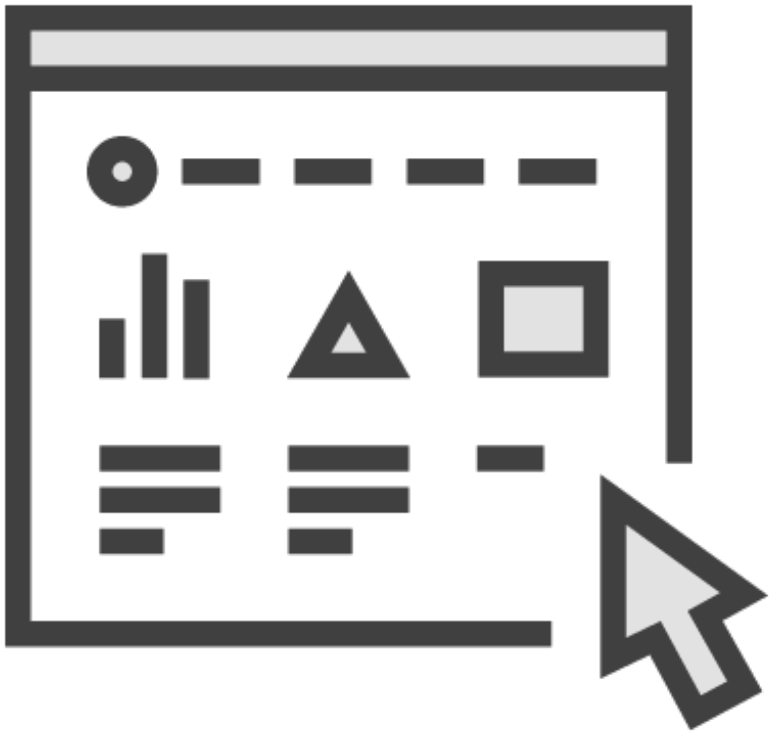


WPS cracking

- Wash
- Reaver

Router Misconfigurations

Vulnerable Captive Portals



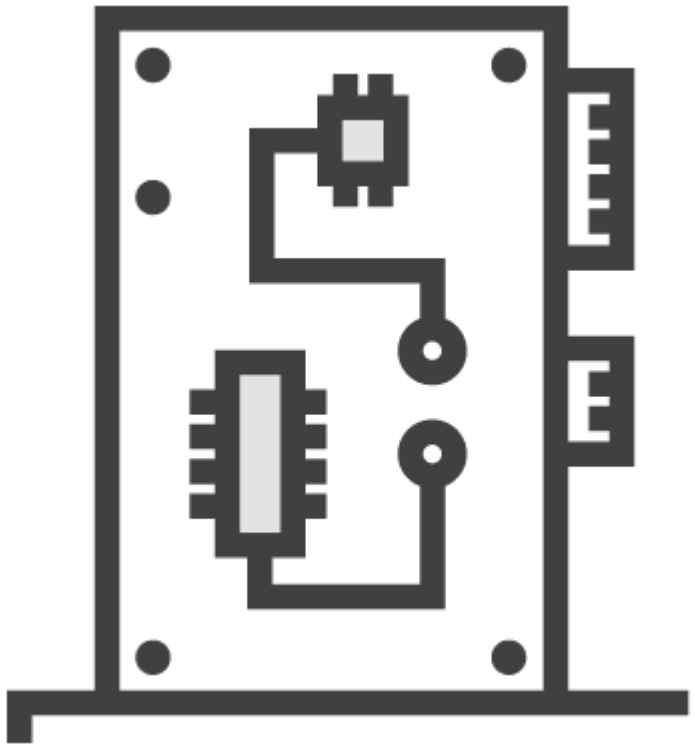
Guest networks

Captive portals are web applications

Web applications can be vulnerable

- SQL Injection
- Authentication bypass
- HTTP eavesdropping

MAC Restriction Bypass

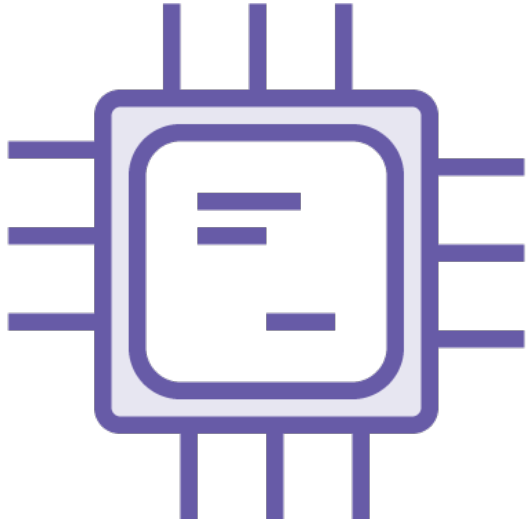


Implemented to restrict access to devices

Used in whitelists of guest networks

Insecure Management Interface

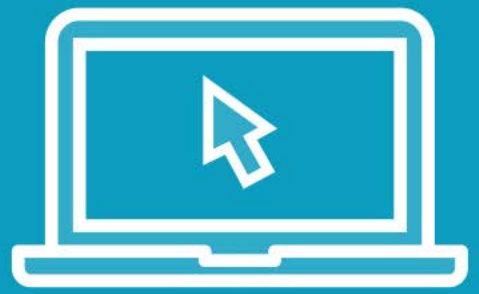
Telnet/HTTP eavesdropping



Lack of patching

Weak/default credentials

Demo



Finding Router Vulnerabilities

- Vulnerable captive portal
- MAC restriction bypass
- Default credentials

Post Exploitation

Capturing the Treasure

Authentication passwords

Network design

Known vulnerabilities

Traffic eavesdropping

Reachable services

Summary

Using outdated protocols can introduce a high risk

It is important not only using latest protocols but also having proper configuration and strong keys

No wireless network is 100% secure

Next up:
Developing Recommendations and Reports