secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Wireless Penetration Testing

Wireless networks are a potential weak point in the corporate perimeter and an enticing entry point for attackers.

If an attacker can gain access to one of your wireless networks (which may include legacy networks you don't know about), they can begin to target internal systems. This can range from the compromise of wireless access points, to accessing production applications or data repositories.

Who Is It For?

With fewer companies operating on a purely local scale, remote working and flexible office hours remove the geographical barrier to business. To enable such flexible working for your staff, your clients and external partners, the typical solution is a combination of hot desking and wireless networking.

WiFi networks are not generally afforded the same level of physical network access controls as they are with traditional Ethernet implementations. Furthermore, it is commonplace to provide 'guest' or Bring Your Own Device 'BYOD' access to wireless networks, which create an increased risk of rogue devices being introduced.

Whilst this provides opportunities for growth, you may also be opening new avenues for compromise by attackers.

How Can We Help?

We are able to conduct a full review of your wireless network either as a standalone assessment or as part of a larger scale investigation into your infrastructure security posture.

We will often deliver a standalone wireless assessment from a black-box perspective, but we may also combine with an architecture review (thereby utilising a white-box approach), enabling a more thorough analysis.

What We Test

We check the configuration of your wireless technologies, test for rogue access points that may have been installed, and determine whether less secure Wi-Fi networks can provide an avenue to the corporate network. We will also check that wireless security standards around SSIDs, encryption and authentication are all in place. We most commonly find flaws relating to:

- **Encryption protocols**

  The first line of defence for a wireless network. If an attacker can crack the encryption then they can gain access to the network.

- **Authentication**

  As an example the PSK acts as a password to authenticate a user to the network. Passwords that are weak, or not stored securely, offer an easy avenue onto the network for an attacker.

- **Segmentation**

  Weak or absent network segregation can lead to the disclosure of sensitive data, access to (or compromise of) internal systems, and the targeting of internal users.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

This assessment will review the implementation of 802.11 wireless networks (WiFi) in order to understand the security risk that they present. The following provides a high-level overview of the Secarma wireless network testing methodology:

PROTOCOL CONFIGURATION

802.11 can be implemented using several different protocol versions, that establish everything from the radio frequency used, to the way in which client negotiations are handled. To review this, a wireless network packet capture will be taken.

By reviewing the packet capture, and protocol implementation, attack vectors will be established. Furthermore, this packet capture will enable a range of client-focused and offline attacks.

AUTHENTICATION CONFIGURATION

Authentication over a wireless network can be handled in several ways, including:

Captive portal
Password
Certificate
RADIUS
WPS
NAC

The specific implementation of each mechanism will have a security implementation, and so will be reviewed to ensure that it has been implemented in line with best-practice guidance.

SIGN LEAKAGE

Wireless signals can operate on 2.4GHz and 5GHz frequencies, which have an effective range of up to 150 feet. This can often lead to signals extending beyond the perimeter of an office environment. The risk of this is that an attacker may be able to interact with the wireless network from a public location, without the need to physically breach the premises.

The extent of signal leakage will be reviewed through a process known as 'War-driving', where the wireless signals will be mapped geographically to determine their operational range.

ROUTER CONFIGURATION

Wireless access points often offer administrative interfaces, through which various security configurations can be managed. These interfaces often present weaknesses in their implementation which may lead to a compromise of the device, and subsequently the network or client.

The following configurations will be reviewed:

Transport layer security
Authentication credentials
Administrative security configurations
Use of known vulnerable components

NETWORK FIREWALLING AND ISOLATION

Wireless access points provide routing for clients in much the same way as conventional ethernet-based switches. As such, firewalling and isolation between clients should be implemented to reduce the impact if a foothold on the network is achieved.

This will be reviewed by attempting to move laterally and communicate with assets that should not be accessible through the wireless network, for instance by accessing a network file share through a guest network.