Is your Wi-fi under attack?

Employing a wireless solution can offer greater flexibility, but it comes with greater potential for attack. From rogue access points to weak encryption algorithms, threats to wireless networks are unique and the risks can be significant.

Common types of Wi-Fi attack

Packet sniffing

Packet sniffing: The act of capturing packets of data flowing through a computer network. Traffic is often sent in the clear, meaning that there is no encryption and files are in plaintext for anyone to read. This can lead to stolen passwords or leaks of sensitive information.

Rogue access points

Rogue access points: Are unauthorized access points on a network. These represent a vulnerability to the network because they leave it open to a variety of attacks. These include vulnerability scans for attack preparation, ARP poisoning, packet captures and Distributed Denial Of Service attacks.

Password theft

Password theft: If you send passwords over the network, and if the site doesn't use SSL or TLS, that password is sitting in plain text for an attacker to read. Hackers even have methods to get around encryption methods to steal passwords.

Man-in-the-middle

Man in the middle attack: Hackers trick communicating devices into sending their transmissions to the attacker's system. This allows traffic to be captured and even manipulated. Various types of malware can be inserted, email content can be changed, or the traffic can be dropped.

Evil twins

Evil twins: Designed to look and act exactly like a legitimate access point. Hackers can clone an access point you know and trust, and create one that is identical. When you connect via this access point, you're actually connecting to the evil twin, which then sends info to the hacker.

Ad hocs

Peer-to-peer ad hoc connections: These circumvent network security policies. This type of access point can provide easy, automated direct connections to other users, bypassing network security and routing traffic onto the enterprise network.

Endpoint attacks

Endpoint: hackers can access your laptop by setting up fake websites that then grant them access to the entire network. If the entry point is not your own computer, you might not even be aware that a hacker has gained access to the network.

Worms

Worms: Can propagate by themselves. When you are connected to a public Wi-Fi network, if you do not have proper security in place, a worm can jump onto your computer from another device that's connected to the network you are using.

Misconfigured access points

Misconfigured access points: your IT department could misconfigure or accidentally duplicate a wireless network. It's not uncommon for employees to just leave the default user and password on a Wi-Fi router, which makes the network incredibly easy to access.

Examples of breaches

The 'secure' Wi-Fi standard has a huge, dangerous flaw [1]

In October 2017, researchers identified a serious vulnerability in Wi-Fi Protected Access 2 (WPA2) - the current industry standard that encrypts traffic on Wi-Fi networks to thwart eavesdroppers. A flaw in WPA2's cryptographic protocols could be exploited to read and steal data that would otherwise be protected. In some situations, the vulnerability even leaves room for an attacker to manipulate data on a Wi-Fi network, or inject new data in.

Hacker shows how easy it is to take over a city's public Wi-Fi network [2]

In 2016, an Israeli hacker successfully took over the free Wi-Fi network of an entire city. By connecting to the city-wide free Wi-Fi network set up by the local administration of Tel Aviv, the attacker found a buffer overflow vulnerability that could be exploited to take full control of the device.

TalkTalk customers urged to change Wi-Fi passwords [3]

In 2016 it was found that passwords for as many as 55,000 wireless routers provided by Talk Talk in the UK were easily available to hackers. Having stolen the default passwords for routers, hackers were then able to attack customers' networks, although the hackers had to be within signal range to do so.

Hackers used luxury hotel Wi-Fi to steal business executives' data [4]

Business executives visiting luxury hotels have been infected with malware delivered over a public Wi-Fi network. As soon as they logged on to the hotel Wi-Fi, they were greeted with a pop-up asking them to download updates. But giving permission for the download only led to infection and subsequent theft of data from their devices.

Wireless penetration testing

Wireless capabilities can provide opportunities for attackers to infiltrate an organization's secured environment - irrespective of security controls. Penetration testing can help validate weaknesses in the wireless infrastructure.

Identification

Wi-Fi network identification, including wireless fingerprinting, information leakage and signal leakage.

Encryption

Determine encryption weaknesses, such as encryption cracking, wireless sniffing and session hijacking.

Access controls

Attempt to penetrate a network by using wireless or evading WLAN access control measures.

Authentication

Identify legitimate user identities and credentials to access otherwise private networks and services.

Choose which test you need

At IT Governance we offer two levels of penetration test to meet your budget and technical requirements.

Level 1

Identifies the vulnerabilities that leave your IT exposed. Combining a series of manual assessments with automated scans, our team will assess the extent of your system or network's vulnerabilities, allowing you to evaluate your security posture and make more accurate budgetary decisions.

Purchase our quick and fixed-price penetration tests online.

Buy online

Level 2

Involves attempting to exploit the identified vulnerabilities to see whether it is possible to access your assets and resources. This more thorough assessment of your security posture enables you to make more accurate decisions about investing in securing your business critical systems.

Please contact us for further information.

Contact us

For more penetration testing information or to request a quote, visit our website by clicking here.

References

1. Serious KRACK Exploit Affects All Wi-Fi Devices Using WPA2 Protocol, SC Media (October 2017).
2. Hackers Used Luxury Hotel Wi-Fi To Steal Business Executive's Data, The Guardian (2014).
3. Hacker shows how easy it is to take over a city's public Wi-Fi network, CSO (November 2016).
4. TalkTalk customers urged to change Wi-Fi passwords, The Telegraph (December 2016).