Penetration testing for Wi-Fi networks

AEC

Nowadays, every larger company's infrastructure must include a wireless network allowing employees to connect from notebooks or mobile devices from anywhere in the building. However, wireless networks also provide a potential attacker with new attack vectors to compromise employees or a company's internal network.

Penetration testing helps reveal possible weaknesses or configuration flaws in these networks. These can then be removed as recommended, making it impossible for attackers to exploit these vectors and increasing the security and resilience of the network to a real cyber attack.

Because an attacker does not need to be directly in the company building to access a wireless network, simply within range of the network, this is a crucial matter for security.

Penetration testing for Wi-Fi technologies simulate an attack on access to an organization's internal network via a Wi-Fi signal. After gaining access, there will be a check of the quality of traffic filtering between the Wi-Fi client network segment and the rest of the internal networks.

The tests also include an analysis of the client's configuration of the connection to the wireless network. The test results in an overview and a mapping of the Wi-Fi networks in operation and a list of security findings with their subsequent impact on the organization's internal network.

Penetration testing mainly includes the following categories:

- Mapping and analysis of the Wi-Fi networks available in the company's premises.
- Detecting possible Rogue APs.
- Testing the employee Wi-Fi networks.
- An attempt to gain access.
- An analysis of the filtering between the Wi-Fi and LAN network segments

aec-security.eu

Penetration testing for Wi-Fi networks

Mapping and analysis of the Wi-Fi networks available in the company's premises.

The aim is to map and analyse the Wi-Fi networks available in the company's premises. The analysis focuses on mapping individual Access Points and the use of technological and cryptographic mechanisms used to secure authentication and transmitted data.

Detecting possible Rogue Access Points (AP).

A Rogue Access Point (AP) is an unauthorized Access Point deployed on the premises and in the immediate vicinity of the company. An attacker usually uses a Rogue AP to attack the security of an existing wireless network - here the attacker duplicates the settings of the target network. The second commonly used option is to use an open wireless network with the aim to subsequently attack any connected stations or to intercept access data.

Verification of visitor Wi-Fi networks

This phase aims to analyse the security of visitor Wi-Fi networks. These networks are usually configured with open access and captive portal authentication or with Personal security (WEP, WPA-PSK with TKIP, WPA2-PSK with CCMP).

Testing the employee Wi-Fi networks.

This phase aims to analyse the security of employee Wi-Fi networks. These networks are usually configured as a WPA Enterprise with 802.1X authentication, and sometimes with Personal security (WEP, WPA-PSK with TKIP, WPA2-PSK with CCMP).

An attempt to gain access

The attack procedure to gain unauthorized access varies depending on the network security used. There are various known attacks on WEP, WPA-PSK, WPA2-PSK or WPA-Enterprise security that are tested during this phase. There are many documented attacks for WEP security such as the KoreK chopchop attack, Fragmentation Attack, ARP-request replay attack and others.

For WPA2-PSK, this could be, for instance, cracking a shared password offline or misusing an enabled WPS authentication method. In the case of WPA-Enterprise using standard IEEE 802.1X authentication, the network is checked for weak authentication methods (EAP-MD5, Cisco LEAP). There is a verification of the correct configuration and hardening of the network and client devices. The possibilities of capturing sensitive data such as usernames or passwords are also tested.

An analysis of the filtering between the Wi-Fi and LAN network segments

In this stage, there is an authorized login to all the company's Wi-Fi networks under the provided user accounts. Subsequently, there is a test of how thoroughly the Wi-Fi client network segment is separated from other sensitive network segments (DMZ, production, ...). If different VLANs are present, the above is also checked.

Our strengths

- We are an established Czech security company that has been successfully operating on the market for over 30 years.
- We have more than 10 years of experience in the field of infrastructure and wireless network security.
- A broad team of certified ethical hackers with experience from dozens of penetration tests each year.
- We hold eMAPT, CISSP, OSCP, OSCE, CEH and many other certifications.
- We run our own hackers' lab for research in various types of wireless networks.
- We listen to our clients and adapt our tests to their needs and the time they have available.
- We follow modern trends in wireless network security.
- We emphasize a manual approach whilst testing, which leads to more errors being detected and minimizes false-positive findings.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283