Penetration testing the external infrastructure

AEC

Prevent unauthorized access

During penetration testing of the external infrastructure the focus is on revealing all available network services and components and enumerating them in detail. Collecting as much public information as possible about a company‘s network infrastructure is crucial for an attacker - this information is used to uncover vulnerabilities, carry out cyber attacks and gain access to the company‘s internal network or steal client data.

This test simulates the actions of an attacker who chooses a company as an interesting target and attacks the company‘s external perimeter anonymously and remotely via the Internet.

aec-security.eu

Penetration testing the external infrastructure

An external penetration test simulates an attacker attacking the components of an information system from outside. The tests aim to determine how easily identifiable a target an organization‘s ICT infrastructure is, what technical information can be obtained on publicly available services, to detect vulnerabilities that can be exploited to gain unauthorized access to sensitive system resources and to propose recommendations for removing them.

The comprehensive security assessment of the external components tested during penetration testing includes the following steps

- identifying targets,
- finding active services,
- uncovering vulnerabilities,
- exploiting vulnerabilities / gaining access,
- escalating privileges and controlling the target

Penetration testing the external infrastructure

When carrying out penetration tests, we rely primarily on the current OSSTMM methodology, with an emphasis on using the techniques listed below:

Identifying targets

- Collecting as much information as possible (DNS names, IP addresses, publicly available information, registration databases, traces, response times, etc.).

Finding active services

- Scanning open ports and running services,
- detecting the type of operating system and individual software versions,
- an emphasis on using system tools and automated scanners.

Uncovering vulnerabilities

- Based on the results of the previous phases and further scanning, we find out where the vulnerabilities occur,
- an attempt to exploit vulnerabilities and compromise services/systems,
- we use powerful, commercial vulnerability scanners as well as our own proprietary tools.

Gaining access

- An attempt to penetrate systems/services using the vulnerabilities found in previous phases,
- the aim is primarily unauthorized acquisition of sensitive information, access to systems, etc.

Escalating privileges and controlling the target

- The goal is to gain full control over the given asset,
- or the possible use of the target for „pivoting“ - attacking other systems through ones already compromised.

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 20 years of experience in the field of external infrastructure security.
- We have the largest team of ethical hackers in the Czech Republic, one that is made up of more than 15 of our own employees.
- We hold CEH, eMAPT, CISSP, OSCP, OSCE and many other certifications.
- Our team is composed of specialists with experience from hundreds of projects.
- We listen to our clients and adapt our tests to their needs and the time they have available.
- We follow modern trends in security and technology.
- During testing, we put an emphasis on a thorough enumeration of the specified targets. This leads to the uncovering a larger number of vulnerabilities.

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