NEW AND EXPANDED
SECURITY PORTFOLIO

PENETRATION TESTS

Did you know that 90 percent of all IT systems have weak points? Learn how to effectively protect yourself against criminal attacks and how to close potential security gaps in your systems!

In many cases, conducting penetration testing is mandatory or recommended for compliance. These include regulations from GDPR, PCI-DSS, or ISO guidelines.

In close cooperation with you we analyze the security of your systems from the perspective of highly specialized attackers and look for security gaps and vulnerabilities.

Our penetration tests are based on the comprehensive know-how of experienced penetration testers.

When conducting such tests, we use best practices and methods, and consider industry standards such as OWASP Top 10 or PCI-DSS.

FAST LANE
Central Eastern Europe

T +386 1 320 78 80
E info-cee@fastlane.net
W fastlane-cee.net/security

Why Penetration Testing?

- Prevent criminal attacks on your IT systems.
- Protect your digital assets.
- Reduce the risk for your company.
- Identify and fix vulnerabilities.
- Comply with regulations that apply to your company.
- Protect your IT security investments.
- Maintain your good reputation.
- Protect customers, partners and third parties.

Modules

We offer a variety of different tests, which can also be combined.

Web Applications

Testing your web applications, where 70% of all attacks take place (e.g., programming and implementation, SQL injection, cross-site scripting).

Social Engineering

Checking the behavior of users on your IT systems (social hacking, phishing attacks, voice phishing, USB devices with simulated malware).

Cloud

Analysis of your cloud infrastructure, services, and applications.

Mobile Applications

Detailed security test of your mobile applications and devices (traffic and encryption, runtime analysis, code signing and memory protection, fuzzing).

Internet of Things (IoT)

We perform a thorough security assessment that considers all the layers of IoT including embedded devices, wireless communication, IoT specific architectures, operating systems, applications and communication protocols.

Wireless

This includes your WLAN infrastructure (wireless encryption and authentication mechanisms, man-in-the-middle (MITM) attacks, denial of service tests, Bluetooth security tests, and similar).

Network and Infrastructure

Testing of your networks, infrastructure, and overall architecture (server services, operating systems, firewalls, and others network components).

Methods

Depending on your requirements, we carry out different penetration tests.

White Box Test

In this scenario our testers receive extensive information about the customer (e.g., network maps, source codes or internal information that is available to every employee) in order to focus on certain areas to identify specific weak points and design protection measures.

Grey Box Test

In this scenario, our testers have access to partial information (e.g., user information of a conventional user, and we are checking what can be done with this piece of information. For example, circumvent security measures and gain higher rights to steal valuable information.

Black Box Test

A complete assault testing where the client does not provide any information about their infrastructure. The client may provide no more than a URL or even just the company name. Our testers behave like real hackers and, depending on your needs, will test your IT systems, the behavior of your employees (social engineering) and physical security (building security, data center security, an similar).

Frequency

If it's just a snapshot in time, security tests still have value but will not protect you for long.

With every software update and / or the addition or removal of functionalities your attack surface is changing. Also, new attack methods and tools are being developed constantly and vulnerabilities are being published on a daily basis. For example, just in 2021 Google paid the amount of $ 8.7 million in rewards to third party bug hunters for detecting thousands of vulnerabilities in Android, Chrome, and Google Play. It's obvious that in order to achieve ongoing protection, security tests should be fully integrated into the security process and be carried out at regular intervals.

Focus Areas

Internal Focus

In this scenario we review and analyze your internal IT infrastructure from the point of view of an internal hacker. Our specialists simulate an attacker with access to the internal network and try to identify vulnerabilities caused by outdated software versions, weak access controls or misconfiguration.

Our tests include an automatic vulnerability scan and manual analysis of all active network services. With your consent, the vulnerabilities found will be actively exploited to illustrate the attack potential.

Internal networks offer hackers many interesting and lucrative targets for attack, which are often less secure than the publicly accessible systems of a company. The tests we offer can be performed either on-site or remotely (via VPN).

External Focus

In this scenario we focus on publicly accessible IT infrastructure, mimicking an external hacker. This includes the analysis of all systems accessible from the Internet. Here, after consultation, a real attack is simulated, and an attempt is made to compromise externally available systems without prior knowledge (black box) or with the addition of information provided by you (grey box).

In the first part of the scenario, our experts perform a passive analysis of publicly available information (OSINT) about your infrastructure. The focus here is on identifying and comparing the identified systems with your asset lists.
In the second phase, active tests are carried out, consisting of a vulnerability scan and manual attacks on all identified systems and services.

Internal Focus Services

- Analysis of the remote access infrastructure providing a secure and encrypted connection
- Analysis of IaaS and PaaS infrastructures in AWS and Azure
- Assessment of IT systems in the cloud, e.g., Container, Docker or S3
- Assessment of external file services e.g., SFTP, FTP or WebDAV
- Assessing email server systems

External Focus Services

- Review and analysis of the Windows-based infrastructure
- Review and analysis of the Linux / Unix based infrastructure
- Analysis of used network protocols and services
- Checking peripheral devices such as printers, fax machines, etc. in the internal structure

Procedure of Penetration Tests

Before we conduct any test we will discuss the goal, the modules, the method, and the focus of our engagement. Then, all identified IT systems are extensively examined for security weaknesses and attacked according to the jointly agreed specifications. After completing the tests, we will present our results and you will receive a detailed documentation. In addition, a prioritization, and a catalogue of measures with concrete suggestions are included for each attack scenario. Depending on the outcome of the penetration tests, we are also happy to conduct special workshops for your IT experts.

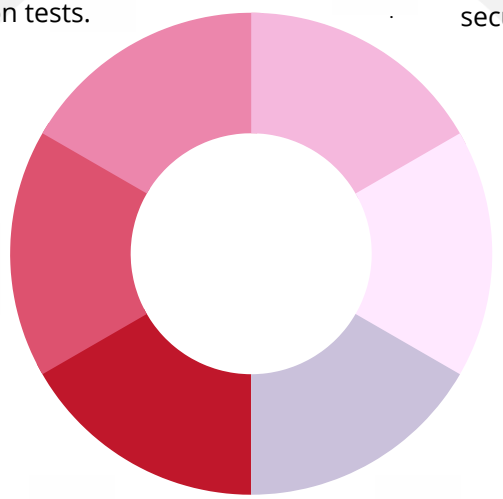
1 | Kick Off

Define goals and procedure of the penetration tests.

2 | Modules

Analysis of weaknesses and security gaps:

- Network
- Web Applications,
- Wireless
- Internet of Things (IoT)
- Cloud
- Mobile Applications
- Social Engineering



6 | Subsequent Test

Verification of fixed vulnerabilities, need to be commissioned separately as we don't know at the beginning of our engagement how much effort will be involved.

3 | Documentation

Management summary and technical report on vulnerabilities and threats.

5 | Fixing Vulnerabilities

Fix the vulnerabilities of the systems.

4 | Presentation

Results, risk assessment, prioritization, recommendations for action, if necessary, workshop for measures.

No time to start like now.

We are here to help.
Contact us for further information and customized cyber security services.

FAST LANE Central Eastern Europe

T +386 1 320 78 80
E info-cee@fastlane.net
W fastlane-cee.net/security