# Trustsec Penetration Test

## Identify Your Vulnerabilities

Stay ahead of criminal hackers with professional penetration testing. Identify the weak spots in your organization's security, and save your organization from cyber-attacks.

let our experts put your defences to the test. We use different pen testing strategies to help pen-testing teams focus on the desired systems and gain insight into the types of attacks that are most threatening.

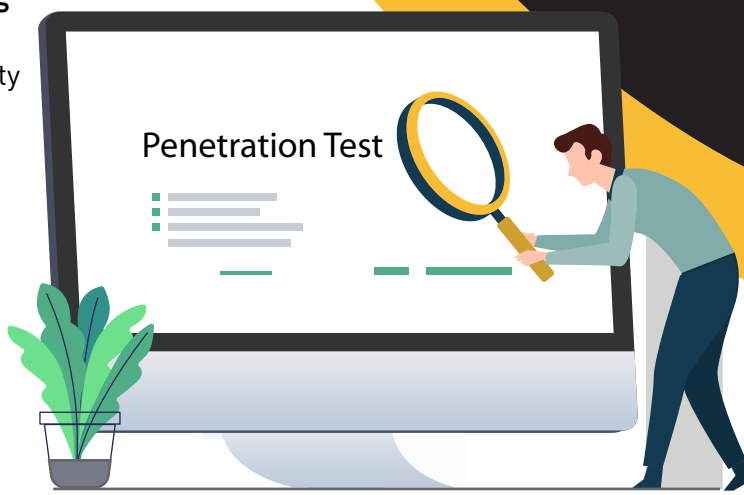
## Why Penetration Testing?

**Identify business risks**
Penetration test helps you proactively identify vulnerabilities in your IT systems that can be exploited by hackers, and could expose the business to critical risks.

**Evaluate the effectiveness of IT defenses**
Ethical hacking through penetration testing can be used to check whether your IT security defenses would function effectively against real attacks.

**Improve your IT security posture**
Penetration testing allows you to proactively close the security gaps in your system and prevent future cyber-attacks.

**Save business reputation**
With penetration testing, you can proactively identify vulnerabilities and fix them before getting exposed to attacks that could ruin the business reputation or data stealing.




+48784784 504
info@trustsec.net
www.trustsec.net

# Trustsec Penetration Testing Services

Trustsec provides penetration testing and vulnerability assessment services for the following:


## Web Applications Penetration testing:

Trustsec team examines web application components using manual and automated methods to identify any weak points, misconfigurations or vulnerable components which can be exploited by malicious authenticated users as well as unauthorized cyber criminals.

## Mobile applications penetration testing:

Examining mobile applications by simulating numerous attacks on the mobile client side and the server side to identify weak areas and exploitable vulnerabilities.

## SSDLC:

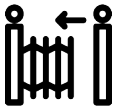
Software companies and application vendors create, release, and maintain functional software applications. However, the increasing cyber security concerns and business risks associated with insecure software have brought increased attention to the need to integrate security into the development process.

Trustsec Team integrates security in the Software Development Life Cycle (SDLC) by embedding security activities with each phase in building the software, starting from the functional requirement gathering to application deployment.

## Internal penetration testing:

Trustsec team examines internal IT systems behind the network perimeter defenses for weaknesses that could be exploited by an attacker. This is typically performed on client premises, but can be performed remotely with VPN access as well.

This test's aim is to assess the effectiveness of internal security controls in fending off attacks initiated by attackers who have initial foothold in the client infrastructure or unauthorized visitors or employees who may have malicious intents.



## External penetration testing:

In this service, Trustsec team emulates remote attackers who target client assets. Executed without any privileges and only with basic knowledge of the target environment, the service can include all external and publicly accessible assets as well as any published services.

+48784784 504
info@trustsec.net
www.trustsec.net

# Trustsec Penetration Testing Services

Trustsec provides penetration testing and vulnerability assessment services for the following:

## Wireless penetration testing:

Exposed WiFi networks introduce new attack vectors that could allow malicious unauthorized attackers to compromise the client infrastructure.

Trustsec team examines the information security measures taken in WiFi Networks and analyses weaknesses, technical flaws, and critical wireless vulnerabilities.

## Adversary data collection simulation:

Trustsec team simulates external adversary actions taken to collect information about the client before gaining initial foothold on the client infrastructure.

This service focuses on public assets related to the client. It involves the analysis of the collected sensitive data which may be misused by attackers to gain an initial foothold in the client infrastructure.

## Red teaming:

Based on the "Assume Breach" security strategy, the service is executed between two groups:

1) - Trustsec Red Team
2) - Client Blue Team

This service's goal is to test the client infrastructure using tactics, techniques and procedures that emulate those of real adversaries against live production infrastructure. It also validates the security detection and response capabilities, identifies production vulnerabilities, configuration errors and enhances the blue team skills for data recovery and threat detection.

Every red team attack path is followed by a full disclosure to the client blue team to identify gaps and improve the network defending and breach response skills.

+48784784 504
info@trustsec.net
www.trustsec.net