ACRONYM

SECURE IT
PENETRATION TESTING SERVICES

SECURITY

Real-World Attack Emulation to Validate Your Security Defences

PRODUCT OVERVIEW

We understand your systems and applications to identify and address gaps and security weaknesses vulnerable to cyber-attacks. Penetration testing is about finding the path of least resistance before threat actors exploit it. This testing can involve the attempted breaching of application systems (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities that are susceptible to modern threats and attacks. Our range of penetration testing engagements helps organizations effectively manage cyber security risk by identifying, safely exploiting, and helping to remediate vulnerabilities that could otherwise lead to data and assets being compromised by malicious attackers.

IDENTIFY WEAK ATTACK VECTORS

Make informed decisions on where to focus your budget and attention to close the gap on attackers.

REPORT & REMEDIATION PLANNING

Receive an actionable report with prioritized remediation action items.

COMPLIANCE & BEST PRACTICES

Comply with industry, government or corporate standards that require this form of security testing.

WORLD-CLASS SECURITY EXPERTS

Certified and highly experienced global team of security engineers utilizing modern and advanced ethical hacking techniques to help keep your organization safe.

HOW IT WORKS

The Penetration Testing process begins well before simulated attacks occur. The discovery will allow our ethical hackers to study the systems and infrastructure, explore its strengths and weaknesses, and identify the right strategies and tools to breach the system. The penetration testing process involves four phases: Discovery and reconnaissance, assessment and analysis, exploitation and gaining system access and your final analysis/report.

DISCOVERY

- Open source intelligence
- Understanding the platform
- Client side vs Server side scenarios

ASSESSMENT/ ANALYSIS

- Static analysis
- Archive analysis
- Local file analysis
- Network and web traffic
- Reverse engineering
- Inter process communication

EXPLOITATION

- Attempt to exploit the vulnerability
- Privilege escalation

REPORTING

- Risk assessment for the findings
- Final report

WEB APPLICATION PENETRATION TESTING

Web applications are often exposed to the world and not always protected very well. Standard Web application penetration testing can involve the attempted breaching of application systems (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks. A web application penetration test aims to identify security vulnerabilities resulting from insecure development practices in the design, coding and publishing of software or a website. The vulnerabilities are presented in a format that allows an organization to assess its relative business risk and remediation cost.

INTERNAL PENETRATION TESTING

Internal threats are among the most difficult for enterprises to detect and stop. The sheer scope of attacks that can happen inside your network is one of the main reasons why they're so difficult to prevent. They include everything from staff accidentally losing or damaging data to malicious actors stealing information or compromising systems. Because staff has easier access to systems and assets, the internal network is where organizations are most vulnerable. Our internal network test will assess specified internal-facing network devices, using both automated scans and advanced manual testing techniques to assess your security and identify vulnerabilities.

EXTERNAL PENETRATION TESTING

External penetration testing (also known as external network penetration testing) is a security assessment of an organization's perimeter systems. Your perimeter comprises all those systems which are directly reachable from the internet. Inherently, these are the most exposed systems as they are out in the open and are therefore the most easily and regularly attacked. External penetration testing is a method of evaluating a computer system or network protection using a simulation of a directed attack from the generally accessible networks that simulate the Internet intruder's behaviour.

FEATURES

EXTERNAL PENETRATION TESTING

INTERNAL PENETRATION TESTING

WEB APPLICATION PENETRATION TESTING

TESTING PERFORMED BY CERTIFIED ETHICAL HACKERS

DETAILED REPORTING AND REMEDIATION STRATEGIES

BENEFITS

- Fix security gaps and vulnerabilities before they are exploited by threat actors.
- Provide awareness and understanding of your cyber security gaps and risks to your network and applications.
- Measure the effectiveness of your security controls and manage your risk, especially when it comes to protecting high-value systems and data. By carrying out a penetration test, you will be able to gauge how secure you really are from a cyber-attack.
- Avoid costly data breaches and loss of business operability – recovering from a data breach can be expensive!