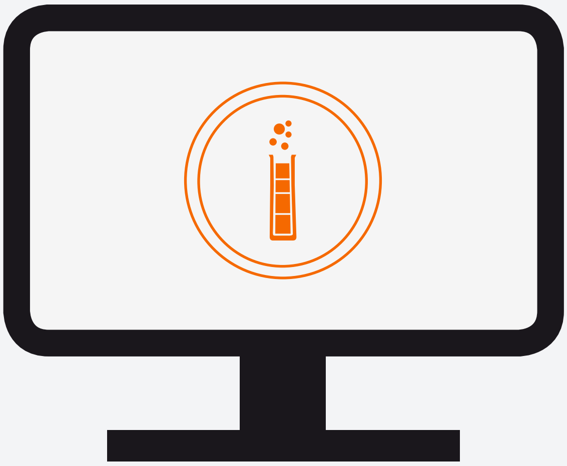
CIPHER SECURITY

CIPHER SECURITY:
INFRASTRUCTURE SECURITY TESTING

www.cipher-security.com

INFRASTRUCTURE TESTING IN A NUTSHELL



An infrastructure penetration test is a method of evaluating the organization’s cybersecurity posture by simulating an attack that could be carried out by malicious source. The test is regarded as a Black Box test, where the tester has no prior knowledge of the organization’s infrastructure and serves to demonstrate a real-life scenario; It is, however, conducted within a predefined scope - as agreed by the client. Infrastructure Security Testing is typically categorized as either ‘external’ or ‘internal’. An external test is conducted remotely, simulating an attack on the organization’s perimeter. By contrast, an internal test is conducted within the organization’s network and simulates a scenario where an attacker has gained physical access to the organization’s infrastructure.

THE NECESSITY OF AN INFRASTRUCTURE TEST

The organization’s successful operation and it business continuity largely depend on the health of it IT infrastructure - which comprises both hardware and software systems. It is imperative to ensure that misconfigurations and vulnerabilities are identified, prioritized and the appropriate solutions are addressed to solved these issues. It has become necessary to periodically carry out such Infrastructure Security Tests - in order to substantially reduce the risk of security breaches that may adversely impact the organization.

METHOD OF OPERATION

Our Infrastructure Security Tests follow a systematic approach that is founded on best practice methodologies and frameworks, such as SANS, NIST, ISO 27001, OWASP, and OSSTMM.

Whilst taking the client's needs, requirements, development processes, and technologies into consideration,the infrastructure testing can be performed - either remotely (external test) or on-premises (internal test).

Within the predefined scope, a variety of different systems such as: Web servers, Application servers, Database servers, and Mail servers, VPNs, RAS (Remote Access) Gateways, Network devices, Domain controllers are being tested for the following:

Missing Operating System security patches

Missing security patches for Third Party products or plugins

Outdated Software

Server and host misconfigurations

Network and infrastructure misconfigurations

Enterprise password policy

ABOUT US

Based in Tel-Aviv, Israel, Cipher Security is a unique Information Security provider that operates in respect with its main values - integrity, accountability, reliability, and partnership.

A trusted partner, we are ready to fulfill requirements and surpass expectations, delivering outstanding value in any given challenge. The Cipher Security specialized services portfolio includes cutting-edge Distributed Denial of Service Tests (DDoS) Consulting, Cyber Workshops, Infrastructure and SCADA Penetration Tests, and tailor-made Exploit Development.

We address our innovative services to a vast scope of industries; from Banking and Investments sector, through the Industrial domain and Critical Infrastructure, to vendors and service providers from around the world.

www.cipher-security.com