COGNISYS
Smarter Cyber Security

External Penetration Testing

In an increasingly connected world, our internet-facing systems are critical to the running of our businesses, and they're often the first port of call for a malicious actor.

Regular testing of your external infrastructure, to highlight vulnerabilities that can be exploited, is an essential security measure.

Testing attempts to discover and expose system weaknesses within a specific brief, focused on web-facing technology such as firewalls, remote access gateways, and web servers.

Working with a strict scope, our consultants attempt to compromise specified hosts using non-destructive attack methods to gain entry to the network, escalate privileges and exfiltrate data where security weaknesses permit.

Continued overleaf...

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

External infrastructure testing aims to highlight vulnerabilities and misconfigurations of systems which could allow for access into the supporting network.

Although the method for each test may vary, the goal is ultimately the same- to assess the organisation's security posture and understand how a threat actor could gain unauthorised access via exposed services.

Our consultants report on the technical vulnerabilities and provide guidance on activities to remediate, helping you to reduce the risk posed to your business and limit the likelihood of an attack.

Following the delivery of the report, the team are on hand for a follow-up call to clarify any areas of uncertainty.

Analysis and Potential Exploitation

This testing is designed to assess security posture against best practices. Where permitted, attempts are made to safely exploit any vulnerabilities discovered.

Overview

The following is typically included within the assessment:

- Host discovery & port scanning.
- Open-Source Intelligence (OSINT) gathering.
- Fingerprinting of services.
- TLS/SSL analysis.
- Identify security misconfiguration.
- Exfiltration of vulnerabilities.

Following a vulnerability scan, the exposed services are further assessed for issues. Manual exploitation of weaknesses occurs where it is safe and practical to do so, and the consultant documents their findings.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk