COGNISYS
Smarter Cyber Security

External Infrastructure Penetration Testing

External Infrastructure Penetration Testing is conducted remotely, to assess web-facing systems specified by the client.

Regular testing of IT infrastructure to highlight vulnerabilities and weaknesses that can be exploited is an essential security measure.

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

The client specifies a key system (or systems) and our consultants attempt to compromise specified hosts using multiple, non-destructive, attack methods, escalating to data exfiltration if security weaknesses permit.

Continued overleaf....

COGNISYS
Smarter Cyber Security

This testing aims to highlight vulnerabilities and mis-configurations of systems, potential data theft or the ability to gain a foothold in the supporting network.

The method may vary for each test, depending on the network, organisation and environment. This will also take into account client concerns and risk appetite.

Whilst establishing the technical risk, our consultants use analysis techniques to help your organisation resolve issues as quickly as possible.

This will help reduce the risk posed to you and your people, reducing the likelihood of reputational damage.

Our service can be fully tailored to your specific needs and environment, with reporting delivered in your preferred format where possible.

After reporting the issues discovered during the assessment, Cognisys consultants are also available for further follow-up calls to clarify certain issues or help your organisation understand the risks posed.

ANALYSIS AND POTENTIAL EXPLOITATION

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

This may involve escalating privileges if possible, accessing key systems and ultimately exfiltrating confidential data if practical.

OVERVIEW

The following is typically included within the assessment:

- Host discovery & port scanning.
- Vulnerability assessment.
- Fingerprinting of services.
- Exploitation and privilege escalation.
- Password evaluation.
- TLS/SSL analysis.
- Identify security mis-configuration.
- Exfiltration of data (if possible).

The hosts are scanned, with exposed services assessed using a combination of manual and automated techniques. This includes a vulnerability assessment of all exposed hosts and their services.

The assessment commences, analysing the findings and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered.

If access is gained to the internal network, attempts will be made to access key systems on the internal network.

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.

BE SMART. BE SAFE. BE SECURE.

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