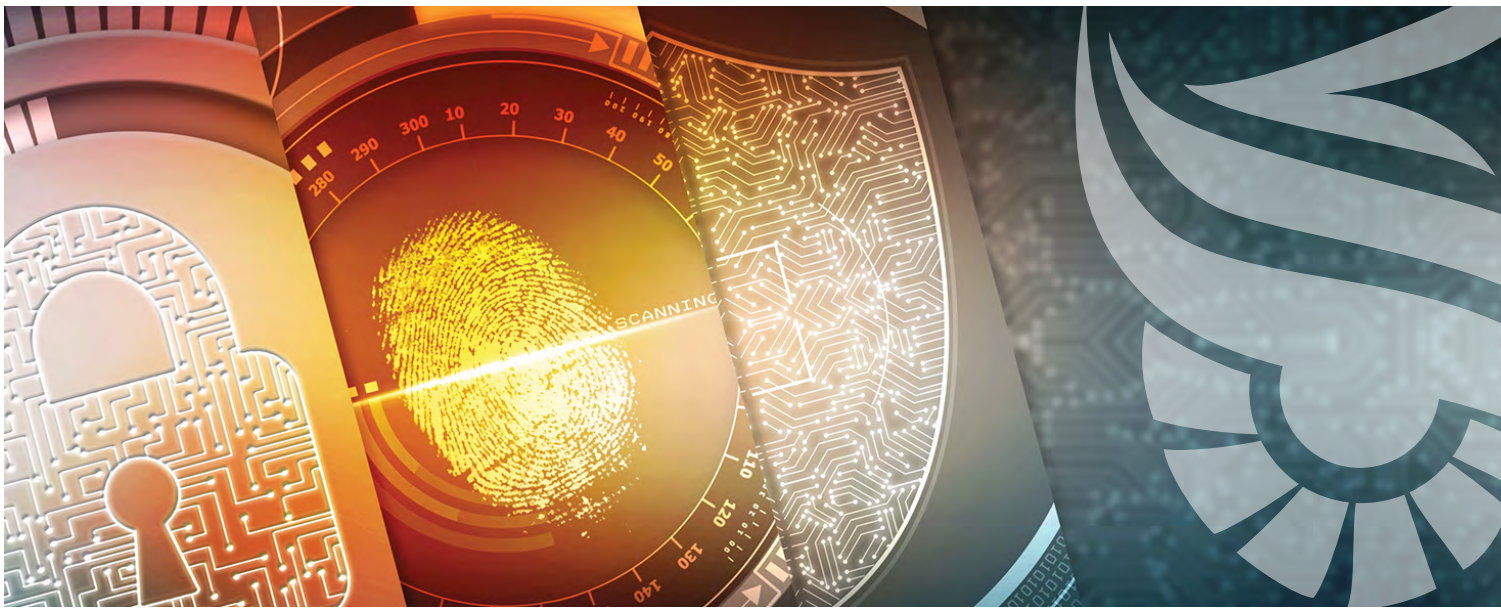
COGNISYS
Smarter Cyber Security



Internal Penetration Testing

Internal Penetration Testing is conducted on premise, targeting systems specified by the client.

Regular testing of IT systems 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 a key system (or systems), our consultants attempt to compromise specified hosts using multiple, non-destructive, attack methods.

This escalates to data exfiltration if security weaknesses permit and includes a vulnerability assessment of all exposed hosts and their services.

Continued overleaf....

COGNISYS
Smarter Cyber Security

The testing aims to highlight vulnerabilities and mis-configurations of systems, privilege escalation, 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 specialist techniques to help your organisation resolve issues as quickly as possible.

This helps to reduce the risk posed to you and your people, reducing the likelihood of reputational or financial damage.

Our service can be fully tailored 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 can be included within the assessment:

- Host discovery & port scanning.
- Vulnerability assessment.
- Manual identification and fingerprinting of services.
- Privilege escalation attempts.
- Password evaluation.
- VLAN assessments.
- Analysis of VOIP services.
- Network mapping.
- Exfiltration of data.

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

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