COGNISYS
Smarter Cyber Security

Internal Penetration Testing

It takes the average company 280 days to realise an attacker is in their network.

Do you know how far an attacker could get within your environment in that time?

Internal Infrastructure Testing is an integral part of any organisation's security strategy, assessing how misconfigurations or vulnerabilities within your internal network, both on premise and in the cloud, could be exploited by an attacker who has insider access to your environment.

Working to an agreed scope, our consultants attempt to compromise hosts, including Active Directory, Windows & Linux servers, and database servers, using non-destructive attack methods. Where possible, this may lead to the exfiltration of data.

The outcome of an internal infrastructure test is a list of confirmed vulnerabilities within the specified hosts and a solid remediation plan for mitigating the risks.

Continued overleaf...

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

The testing aims to highlight vulnerabilities and misconfigurations of systems, which can lead to privilege escalation, theft of data, and even the ability to gain a persistent foothold within the network.

Although methods used will vary for each engagement, dependent on the services in use and the client's appetite for risk, we follow a similar methodology in each project. Initially, our consultants run vulnerability scans to quickly highlight potential risks. They then manually investigate issues, which leads to the exploitation of vulnerabilities and the eventual compromise of the host or system where possible.

As part of the engagement, our consultants provide risk ratings for each vulnerability based on the ease of exploitation and the potential impact should the exploit be used. This helps you to prioritise your remediation efforts, and manage your risks accordingly.

Given that every environment is constructed slightly differently, all of our internal infrastructure penetration tests are tailored to your specific requirements.

Following the delivery of the report, we recommend a follow-up call to run through the findings and ensure that remediation advice is clear. This also allows your team to ask any further questions and clarify any areas of uncertainty.

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.

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