

Uncover hidden vulnerabilities within your internal network and fortify your defences with our comprehensive internal infrastructure penetration testing.

Why conduct internal infrastructure penetration testing?

Internal infrastructure penetration testing is essential for identifying and addressing vulnerabilities within your network before attackers can exploit them. It uncovers weaknesses that are not visible through external assessments, including misconfigured systems and outdated software. Simulating real-world attack scenarios reveals how attackers might move laterally, escalate privileges, and access sensitive data.

This proactive approach enhances incident response and strengthens security. Regular testing also helps ensure compliance with industry standards and reduces the risk of costly breaches and reputational damage. Ultimately, it provides a clear understanding of your network's security, enabling effective implementation of controls and safeguards.

Scoping and planning

Define objectives

We collaborate with your team to establish the specific goals of the internal infrastructure penetration testing. Whether you need to evaluate network segmentation, identify potential insider threats, or ensure compliance with internal security policies, we tailor our approach to address your key concerns and objectives.

Requirements

We prepare for the assessment by gathering information about your network infrastructure. This includes IP ranges, NUC device setup, and any specific configurations or devices that need to be tested. We ensure we have the necessary access to perform a thorough evaluation, including setting up any required testing environments.

Rules of engagement

Next, we establish clear rules of engagement to guide the testing process. This includes the testing methods, tools, and techniques used. Additionally, we agree on operational guidelines, such as testing windows, communication protocols, and how sensitive findings will be handled to minimise disruption.

Methodology

Network scanning

We perform comprehensive network scanning to identify active devices, open ports, and potential vulnerabilities within your internal network. This process helps us map your network infrastructure and pinpoint areas susceptible to attacks or misconfigurations.

Vulnerability assessment

Our team conducts a detailed vulnerability assessment to uncover security weaknesses in your network components, such as servers, routers, and switches. We utilise advanced tools and techniques to identify vulnerabilities and assess their potential impact on your network's security.

Penetration testing

We simulate real-world attack scenarios to test the robustness of your network defences. By exploiting identified vulnerabilities and testing network defences, we provide a practical evaluation of how well your network can withstand potential threats.

SmartView takes care of your reporting

Cognisys' SmartView Portal provides a centralised platform for clients to manage their projects and vulnerabilities efficiently. The portal allows the clients can track the status of each identified issue, assign tasks to team members, and monitor the progress of remediation efforts.

A detailed report is prepared once the internal infrastructure penetration testing is complete, prioritising findings and providing strategic, actionable recommendations to strengthen the external security posture through our SmartView portal.

Why Cognisys?

Enhance your network security with our internal network assessment services. Our certified and highly skilled team has a proven track record of delivering exceptional results, ensuring a thorough evaluation of your network infrastructure. We offer actionable insights through comprehensive analysis and detailed reporting, providing practical recommendations to strengthen defences.

Our approach helps you proactively address emerging threats and improve your network's resilience. We tailor our assessments to align with your specific security objectives, offering strategic guidance to maintain a robust and secure network.

[BACK TO CONTENTS](#)

