Protect • Comply • Thrive

# Internal Infrastructure Penetration Test

## Service description

**Internal Infrastructure Penetration Test**
An Internal Infrastructure Penetration Test assesses your internal infrastructure for vulnerabilities. Advanced manual testing techniques and automated scans will be used to simulate real-world attacks. This testing could include end-user devices, servers and networking equipment. This service will result in a report that identifies business and technical risks, and will provide a prioritised action plan with remediation guidance to help you address any risks that are found.

For more information about this service and a tailored quote, please contact us on **+44 (0)333 800 7000**.

**Benefits**

- Identify and understand the technology-related vulnerabilities affecting your internal infrastructure.
- Find out how an attacker could move through your internal infrastructure, escalating their privileges and compromising key services.
- Get an understanding of the business impacts presented by vulnerabilities in your internal infrastructure.
- Demonstrate your security posture to clients by providing third-party assurances that your internal infrastructure is secure.
- Supports compliance with ISO 27001, the UK Data Protection Act 2018 and the General Data Protection Regulation, the PCI DSS, and other laws, regulations and contractual obligations.
- Protect brand loyalty and corporate image by reducing the likelihood of a security breach.

**Objectives**
This penetration test is designed to help mitigate the threat from both opportunistic and determined attackers. It involves:

- Identifying vulnerabilities in the defined internal infrastructure;
- Attempting to exploit any identified vulnerabilities; and
- Providing a report that contains an ordered list of issues, their associated risk, and remediation advice for identified vulnerabilities.

**Methodology**
The Internal Infrastructure Penetration Test follows IT Governance's proprietary security testing methodology, which is closely aligned with the SANS and Open Source Security Testing Methodology Manual (OSSTMM) methodologies.

This service will assess all internal-facing network devices that you specify. It does not include segmentation testing – for a dedicated segmentation testing service, please get in touch.

IT Governance uses both automated scans and advanced manual testing techniques to assess your security and identify vulnerabilities. The penetration test will assess:

- **Secure configurations**
  The tester will review open ports and their services to ensure that appropriate firewall configurations have been implemented. They will also assess available

services to ensure that they have been suitably hardened and to identify whether default configurations are present.

- **Network traffic**
  The tester will attempt to intercept network traffic to identify misconfigurations that could allow an attacker to collect users' hashes that can later be cracked offline. The tester will also attempt to identify any sensitive network traffic sent in cleartext.

- **Secure passwords**
  The tester will perform limited password attacks against authentication services to check that common or default credentials are not being used. They will also analyse password hashes extracted during testing to identify whether users are operating with weak passwords.

- **Patching**
  The tester will research software versions to ensure they are not affected by any publicly known vulnerabilities and are still supported by the vendor.

- **Secure authentication**
  The tester will ensure there are appropriate mechanisms to confirm a user's identity. To assess this, the tester will investigate how the authentication process works and use that information to attempt to circumvent the authentication mechanism. This may include checking for default credentials and username enumeration.

- **Encryption**
  The tester will assess the implementation of encryption for the transmission of data. This includes checking for common weaknesses in SSL/TLS configurations and verifying that all sensitive data is being securely transferred.

- **Information leakage**
  The tester will review server configurations to ensure information is not being leaked. This is assessed by reviewing configurations and examining how the server communicates to discover any information disclosure that could present a security risk.

**Reporting**

The tester will present their findings in a comprehensive report, which will consist of the following sections:

- Executive summary
  - High-level, non-technical summary of vulnerabilities identified.
  - Business risks if the vulnerabilities are successfully exploited.
  - Overall risk rating, based on the common vulnerability scoring system (CVSS) version 3 scoring scheme.
- Testing details
  - Detailed description of the methodologies followed and objectives of testing.
  - Scope of testing (defined internal infrastructure), along with any testing limitations or restrictions.
- Vulnerability findings
  - Overview of the vulnerability findings.
  - Consultant's commentary, which discusses the issues identified and how the vulnerabilities could be linked within an attack chain.

- Descriptions of each technical vulnerability identified, which will include:
  - A risk score based on the CVSS; scores may be adjusted based on the vulnerability finding or the consultant's expertise;
  - A description of the vulnerability and its impact;
  - Proofs of concept to support the findings and, where possible, vulnerability replication; and
  - Remediation advice and supporting references.

The report will be delivered within ten working days of completing the testing unless agreed otherwise.

A separate executive summary or letter of attestation for sharing with non-technical management and third parties can be provided upon request. If you would like to see a sample report before engaging, please contact us.

**Eligibility**

This service is suitable for most organisations with an internal corporate network that would like to test their security measures should an attacker gain access to the infrastructure. This service may be especially useful to organisations with a high staff turnover.

For further information and a tailored quote, please contact us on **+44 (0)333 800 7000**.

**Why choose IT Governance Ltd?**

- Our CREST-certified penetration testing team will provide you with clarity and technical expertise, as well as peace of mind knowing that your internal infrastructure has been reviewed by experienced testers in line with your business requirements.
- Get one-to-one expert advice at any stage of the engagement, along with an end-of-test debrief and answers to queries following the issue of the report.
- Our detailed reports describe any identified business risks from both technical and non-technical perspectives.
- Our established and experienced penetration testing team has been operational since 2010, amassing extensive testing experience that ensures clients receive a comprehensive testing service.