INFRASTRUCTURE PENETRATION TESTING

CNS
at Six Degrees

Improve Your Organisation's Cyber Resilience with Expert Infrastructure Penetration Testing Services from our Cyber Security Assurance Team

What is Infrastructure Penetration Testing?

Your organisation is under constant threat of cyber-attack by those who seek to exploit any vulnerabilities they can find. By testing for vulnerabilities, you can identify and address them before they can be exploited. Penetration testing is one way of achieving this.

The National Cyber Security Centre (NCSC) defines penetration testing as an authorised test of a computer network or system designed to look for security weaknesses.

Infrastructure Penetration Testing assesses your infrastructure's cyber resilience and provides insights into how it can be enhanced.

There are a number of types of penetration test that assess different parts of your organisation's infrastructure.

Our Infrastructure Penetration Testing Services

With ransomware and other types of cyber-attacks on the rise, Six Degrees' Infrastructure Penetration Testing services give you the actionable information you need to enhance your protection. Our Infrastructure Penetration Testing services provide an expert view of your infrastructure, enabling you to understand and address your areas of weakness before they can be exploited by hackers.

Full Cyber Security Lifecyle Testing Services

Six Degrees offers three levels of cyber security testing services that encompass the entire cyber security lifecycle, tailored to your organisation's cyber security maturity:

Vulnerability Scanning.

Automated testing that enables your organisation to establish its cyber security baseline and take the first steps towards cyber security maturity.

Infrastructure and Application Penetration Testing.

Expanding the scope of vulnerability scanning with manual testing and detailed reporting delivered by Six Degrees' expert Penetration Testers.

Red Teaming.

Robust manual testing with an unlimited scope of attack vectors and techniques, providing actionable insights that enable your organisation to enhance its ability to detect, respond and recover from cyber-attacks.

Why Carry Out Infrastructure Penetration Testing?

All organisations should carry out Infrastructure Penetration Testing. Here's why:

- Understand and reduce the level of risk your organisation is exposed to.
- Receive clear, easy to understand reports that include remediation advice.
- Work with a cyber security partner who can support you with those mitigating actions.
- Schemes like Cyber Essentials Plus require evidence of penetration testing as part of their certification processes.

Organisations that don't carry out Infrastructure Penetration Testing risk:

- Not having a clear understanding of their cyber security postures.
- Being unable to identify vulnerabilities that can be exploited by hackers.
- Lacking visibility of new and potentially vulnerable devices and servers that are added to their networks.
- Not being covered by cyber insurance companies who require evidence of penetration testing as part of their policies.

Our Infrastructure Penetration Testing Process

Port Scanning. We will scan your target hosts via an automated scanner and will enumerate all available ports and services that are exposed to the internet.

Vulnerability Scanning. We will scan each open port and service via an automated scanner to identify potential vulnerabilities.

Penetration Testing. We will probe each open port and service manually and put together a potential attack tree. We will prioritise any vulnerabilities identified and manually examine ports and services to identify potential vulnerabilities.

Reporting. Results are placed into a report for you to review the results and recommended remediation steps as well as the Penetration Tester's own executive summary.

Our Infrastructure Penetration Tests

Internal Penetration Testing. Six Degrees' Internal Penetration Testing service enables you to understand the level of risk you are exposed to from an attacker placed within your internal network. This attacker could be a rogue employee, guest, or an intruder within the environment. Internal Penetration Testing allows you to identify areas of weakness and implement controls to prevent an attacker moving around inside your infrastructure, escalating privileges and launching damaging attacks.

External Penetration Testing. Six Degrees' External Penetration Testing service enables you to understand and reduce the level of risk you are exposed to over the Internet. External Penetration Testing identifies external points of entry to your environment(s), establishes where areas of weakness lie, and allows you to take action to prevent an attacker breaching your security perimeter.

External Vulnerability Scanning. Six Degrees' External Vulnerability Scanning helps you to achieve a greater level of assurance around your Internet-facing hosts via a regular, repeatable streamlined process. Automated vulnerability scanning is backed up with manual reviews carried out by certified Penetration Testers.

Scenario Testing. Six Degrees' Scenario Testing service allows you to have a greater depth of interaction with our Security Testing Team to build a set of customised attack scenarios that are specific to your organisation. These scenarios are then subjected to malicious activities such as penetration testing, malware creation/deployment and phishing techniques, among others, all with the purpose of identifying and assessing how your organisation performs within the scope of a given scenario.

NCSC ITHC Penetration Testing. Six Degrees' National Cyber Security Centre (NCSC) IT Health Check (ITHC) Penetration Testing service identifies areas of weakness and provides a report that contains recommendations on how you can mitigate the risks raised during the test. The ITHC is recognised by the UK Government, and you can submit the test report generated by Six Degrees as an artefact to assist with the attainment of a recognised security accreditation or standard.

Red Teaming. Six Degrees' Red Teaming services take testing your organisation's cyber resilience to a whole new level. Through a range of techniques including phishing, scenario testing, and physical and social security compromise, Red Teaming allows you to gain total visibility of your organisation's vulnerabilities through the eyes of a hacker.

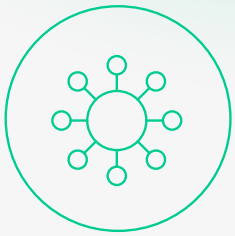
Why Six Degrees?

Over 20 years of cyber security heritage and experience.

SC cleared, UK-based Penetration Testers.

CHECK, CREST and Cyber Scheme certified.

Tailored testing that suits your organisational requirements.



Access to complementary testing, consultancy, and managed security services.

Meet our Experts

Our Infrastructure Penetration Testing services are provided by some of the most highly experienced and accredited Penetration Testers in the industry. We are members of the National Cyber Security Centre (NCSC) CHECK scheme, and our team members and leaders are certified under CREST and the Cyber Scheme.

Andy Swift, Technical Director – Cyber Security Assurance
Andy is Technical Director – Cyber Security Assurance at Six Degrees. He is responsible for spearheading innovation within our Cyber Security Assurance team, ensuring we stay at the forefront of cyber security techniques and technology by carrying out research, building exploits, and delivering cutting edge insights into Six Degrees, its clients, and the wider industry.

Robert Sugrue, Cyber Security Product Director
Robert is Cyber Security Product Director at Six Degrees. He is responsible for providing strategic guidance and planning across Six Degrees' entire cyber security portfolio, ensuring product success by championing cyber security product development while assuring clear understanding of complex products for clients.

Service Credentials

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CREST

THE CYBER SCHEME
OFFICIAL CYBER SCHEME SPONSOR

Six Degrees Credentials

Member of Microsoft Intelligent Security Association
Microsoft

CERTIFICATION BODY
CYBER ESSENTIALS PLUS

ISO 27001

CNS
at Six Degrees

Get in Touch
For more information about our Infrastructure Penetration Testing services, schedule a call here.