CYBERSECURITY

PENETRATION TESTING

UNCOVER VULNERABILITIES BEFORE HACKERS DO!

Good security practice involves regular testing of your IT infrastructure for vulnerabilities and exploitable weaknesses. Penetration Testing, also referred to as Pen Testing or ethical hacking, is an authorised attack on a computer system, such as a network, web/mobile application, or a Wi-Fi network to find security vulnerabilities that an attacker could exploit.

Why is Penetration Testing important?

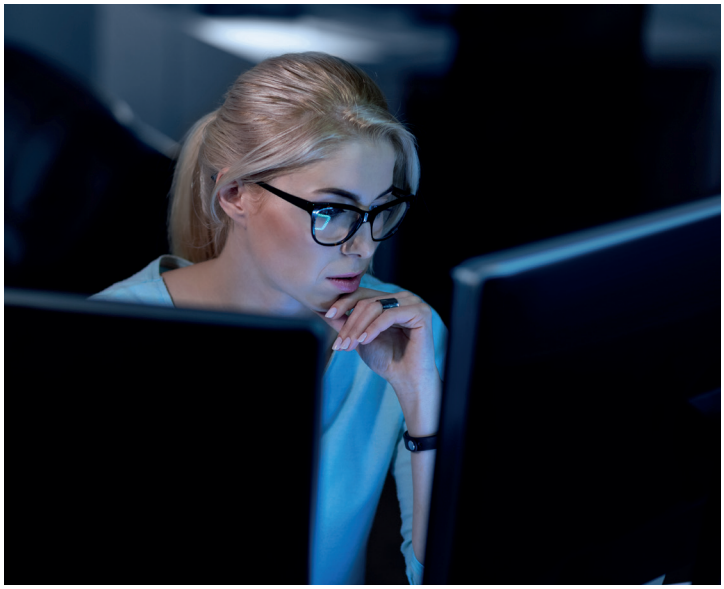
It identifies weaknesses in your cyber defences before they can be taken advantage of by real cyber criminals. Forewarned is forearmed.

WHAT ARE THE KEY BENEFITS OF PENETRATION TESTING?

- Finds weaknesses and vulnerabilities that can be fixed before exploitation.
- Validates effectiveness of existing security measures.
- Demonstrates due diligence and compliance with regulations.
- Raises security awareness for IT teams.
- Provides reports, data and recommendations to strengthen defences.

WHY DOES IT MATTER?

- **Proactive Defence:** Pen Testing helps organisations find weak spots before real attackers do. It's like a security health checkup for your systems.
- **Risk Mitigation:** By identifying vulnerabilities, you can patch them up before they lead to data breaches, financial loss or downtime.
- **Compliance:** Many regulations, such as Cyber Essentials, Cyber Essentials Plus and ISO Certifications require regular penetration testing to ensure data protection and compliance. For PCI DSS (Payment Card Industry Data Security Standard) organisations that process, store or transmit payment card data must complete external and internal penetration testing at least annually and after any significant infrastructure changes.



TYPES OF PENETRATION TESTS

OPEN-BOX
Some info provided ahead of time.

CLOSED-BOX
No background info – just the target company name.

COVERT
Almost no one in the company knows the test is happening.

EXTERNAL
Tests external-facing technology (websites, network servers).

WHY STONE?

When it comes to Penetration Testing for your organisation, it pays to work with qualified professionals.

- **Compliance Matters:** Trust our CREST and Cyber Scheme certified testers.
- **Qualified Professionals:** NCSC recommends CHECK scheme certified testers for government entities and CREST/Cyber Scheme certified testers for non-governmental organizations.
- **Peace of Mind:** Our team complies with industry standards, ensuring legal, ethical, and high-quality penetration tests.

Contact us today to discuss Penetration Testing services for your organisation. Our ethical hackers can conduct network, web application, mobile app, wireless and social engineering tests tailored to your unique environment.

We offer flexible payment plans, including bespoke subscription models to suit your budgetary needs and one-off payments for cybersecurity services.

Strong defences start with knowing your weaknesses. Get ahead of hackers with penetration testing from Stone.

For more information email
sales@stonegroup.co.uk
or call today on **08448 22 11 22**