

Pen Testing

Uncover vulnerabilities and strengthen business security

Cyber threats evolve rapidly. Traditional security measures alone are not enough to safeguard critical IT systems. Businesses need to go beyond reactive defence. Businesses need to proactively identify vulnerabilities before their attackers do.

Roc's Pen Testing service—also known as Ethical Hacking—simulates real-world cyberattacks to uncover weaknesses across applications, networks, and infrastructure. We help organisations understand their security gaps, prioritise risk mitigation and strengthen overall cyber resilience by replicating the tactics of malicious actors.

Our expert-led service provides the detailed technical assessments and executive-level reporting needed to enhance your cyber security strategy, meet regulatory requirements, and protect business operations from potential breaches. All tests include 12 months' access to a secure online portal, allowing your team to review results in realtime, track remediation progress and schedule follow-up testing when needed. This ongoing visibility helps maintain momentum and supports continuous improvement across your security posture.

Ideal for you if...

- ▶ You've recently implemented or integrated new systems, such as a new website
- ▶ You need to assess security gaps in across your IT infrastructure
- ▶ You are working towards compliance with security frameworks such as ISO 27001 or Cyber Essentials
- ▶ You require clear risk prioritisation to guide cyber-security investment
- ▶ You need to demonstrate your cyber status to third-parties such as customers, insurers and regulators

Why Roc?

24/7/365 In house MSOC	100% UK coverage	70+ highly trained engineers	100% engineers SC or DV cleared
CYBER ESSENTIALS PLUS accredited	ISO9001 accredited	14001 accredited	27001 accredited

Service benefits

- ▶ Identify and fix security gaps before they are exploited
- ▶ Free retest for critical vulnerabilities
- ▶ Gain detailed reporting to inform cyber-security strategy
- ▶ Meet compliance requirements with regulatory-aligned assessments



Service overview

Simulated real-world attacks

Our certified ethical hackers use the same techniques as cyber-criminals to test the resilience of your systems. By simulating real-world attack scenarios, we identify vulnerabilities before they can be exploited. This enables your organisation to strengthen its defences and reduce risk. This proactive approach ensures threats are mitigated before they impact your operations.

Free retest for critical vulnerabilities

As a fully CHECK and CREST-accredited provider, we deliver specialist penetration testing across multiple attack surfaces — giving you a full view of your security posture across your IT estate. We also offer a free retest for any high or critical vulnerabilities to help validate remediation.

Clear, actionable reporting

Each penetration test delivers a detailed technical report and executive summary, providing a risk-prioritised breakdown of discovered vulnerabilities — including simulated attack paths and tailored recommendations based on industry best practices. All results are made available through a secure portal with 12 months' access, enabling your teams to track remediation progress, manage risk over time.

Expert-led remediation planning

Beyond identifying risks, our cybersecurity consultants work with your team to develop a structured mitigation plan. We help address vulnerabilities in order of priority based on business impact, ensuring remediation efforts align with your security strategy and compliance needs. This approach reduces exposure to cyber threats while enabling your IT teams to optimise security resources effectively.

Our service options include:

- ▶ **Web application testing:** identify weaknesses in websites, portals, and online platforms that could allow unauthorised access
- ▶ **WiFi network assessments:** detect security flaws in internal wireless infrastructure that could be exploited
- ▶ **Internal infrastructure testing:** highlight access control gaps and misconfigurations that may provide entry points for attackers
- ▶ **External network testing:** evaluate internet-facing systems to ensure your perimeter security is robust against external threats

