REDSCAN

ASSESS

Penetration testing

Test the effectiveness of your cyber security to safeguard against evolving threats

With threats continuing to grow in both volume and sophistication, understanding how an attacker might breach your business' defences and the appropriate action needed to address the risk is an important part of effective cyber security.

Insecure network configurations, authentication problems, as well as flaws in application source code and logic, are just three in a long line of underlying vulnerabilities that could be exploited by criminal hackers. With your organisation's attack surface continuing to grow, keeping out the bad guys is an uphill task.

2017 Computing Security Awards
WINNER
Pen Testing Solution of the Year

As a CREST accredited provider of penetration testing services, Redscan can help your business to improve its resistance to threats by identifying, ethically exploiting and helping to remediate vulnerabilities that could lead to infrastructure, systems, applications and personnel being compromised.

Our range of penetration tests includes:

- Internal & external infrastructure
- Wireless network
- Web services/ API
- Application
- Mobile application
- Build & configuration review

"Should I need any security testing again in the future, Redscan would be my first port of call"

Stuart Barea, Project Analyst
STM Life Assurance

"Redscan's hands-on approach identified security flaws that had previously been overlooked by other vendors"

Andrew Jobson
Technical Operations Manager
Sporting Index

Business benefits

- ✓ Widely assess the capability of technology, people and processes to defend against the latest attacks
- ✓ Reveal gaps in security architecture so that new investments deliver the greatest improvements
- ✓ Understand the effectiveness of cyber defences and prioritise remediation of weaknesses
- ✓ Uncover lesser-known vulnerabilities that automated tools alone are unable to detect
- ✓ Significantly reduce information security risk to improve boardroom and investor confidence
- ✓ Receive help and support addressing complex security vulnerabilities

Key features

- + Cutting-edge hacking tools and assessment techniques ensure latest exploits are tested
- + Internal and external network assessments pinpoint weaknesses across your business' attack surface
- + Experienced ethical hackers: CREST CRT, CCT APP, CCT INF, CCSAM, CCSAS, OSCP, TIGER CTM, CEH
- + Utilises up-to-the-minute internal research and intelligence from leading exchanges like CiSP
- + Confidential engagements with no damage or disruption to network services
- + Clear, concise and detailed reports suitable for technical and management review

CREST

SC 2018 awards EUROPE
Winner
Best Customer Service

2017 Computing Security Awards
WINNER
Pen Testing Solution of the Year

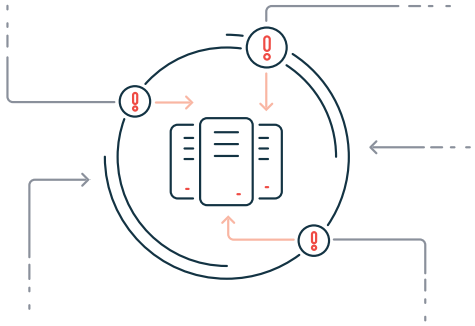
REDSCAN

ASSESS

The value of penetration testing

Hidden vulnerabilities detected by our ethical hackers include:

- Insecure setup or configuration of networks, hosts and devices
- Flaws in authentication and session management
- Input validation errors
- Information leakage
- Out-of-date software and applications



Our 9-step methodology

Redscan's assessment services are based on a systematic approach to vulnerability detection and reporting

1 **Scoping** of test to identify areas to attack
2 **Reconnaissance & intelligence** gathering
3 **Active scanning** of whole attack surface
4 **Identification & mapping** of key assets
5 **Analysis** of applications on target hosts
6 **Exploitation** of identified vulnerabilities
7 **Targeting** of high privilege accounts
8 **Pivot attacks** on other network systems
9 **Detailed reporting** and activity debrief

Reasons to choose Redscan

- ✓ One of the highest accredited ethical hacking companies in the UK
- ✓ A deep understanding of how hackers operate
- ✓ Complete post-test care for effective risk remediation
- ✓ In-depth threat analysis and advice you can trust

2017 Computing Security Awards
WINNER
Pen Testing Solution of the Year

Safeguard your business today

Talk to our experts about a custom security assessment

EMAIL US
info@redscan.com

CALL US
0800 107 6098

ONLINE
redscan.com

Frequently asked questions

What is a pen test?

A penetration test, or pen test for short, is a form of ethical cyber security assessment designed to identify and safely exploit vulnerabilities affecting computer systems, networks, applications and websites so that any weaknesses discovered can be addressed in order to mitigate the risk of suffering a malicious attack.

How does a pen test differ from a vulnerability scan?

While a vulnerability scan uses only automated tools to search for known vulnerabilities, a penetration test is a more in-depth assessment that utilises a combination of machine and human-driven approaches to identify hidden weaknesses.

How is a pen test conducted?

Penetration testing utilises the tools, techniques and procedures used by genuine criminal hackers. Common black hat methods include phishing, SQL injection, brute force and deployment of custom malware.

How long does a pen test take?

The time it takes an ethical hacker to complete a penetration test is dependent upon the scope of the test. Factors affecting duration include network size, if the test is internal or external facing, and whether network information and user credentials are shared with Redscan prior to the engagement.

How often should testing be carried out?

All businesses are advised to conduct a penetration test at least once a year, as well as after any significant upgrades or modifications to infrastructure or applications. Given the rapid rate at which new exploits are discovered, Redscan recommends that quarterly tests are performed. Regular penetration tests are often required for compliance with regulations such as PCI DSS.

What happens after the pen testing is completed?

After each engagement, the ethical hacker(s) assigned to the test will produce a custom written report, detailing and assessing the risks of any weaknesses identified plus outlining recommended remedial actions. A comprehensive telephone debrief is conducted following submission of the report.