PENETRATION TESTING

DATA SHEET

UNRESTRICTED

1. PENETRATION TESTING

1.1 SERVICE DESCRIPTION

By using all the tools and tricks available to real-world attackers, Coresecurity penetration tests uncover weaknesses in your infrastructure and applications, helping you proactively prevent real-world attacks. They're also a core component of a good risk-management strategy, improving your overall security posture, and keeping you in total control.

At Coresecurity, we tailor our penetration testing methodology to meet your underlying business, security, and compliance objectives, so you get the most from your test. Once the test is complete, our comprehensive report includes a high-level executive summary to give the bigger picture, before drilling down into vital details. Our reports also include clear, easy-to-follow remediation advice for each discovered security threat.

Our skilled penetration testers are independently certified by the likes of CREST and Tigerscheme, and our services are delivered in-line with ISO 27001 and 9001 standards. The types of penetration testing services we offer are detailed in section 2.

1.2 DELIVERABLES

Upon the completion of the penetration testing process, the lead penetration tester will present the results in a clear, comprehensive report. This report will be split into two sections: an executive summary and a technical breakdown, typically delivered within five working days after the completion of the penetration test.

1.2.1 EXECUTIVE SUMMARY

- High-level, non-technical discussion of the overall assessment and findings
- Confirmation of the scope and methodology
- An overview of the business impact of the discovered threats

1.2.2 TECHNICAL BREAKDOWN

- Description of steps taken during the assessment
- Detailed description and evidence of vulnerabilities identified, including their Common Vulnerability Scoring System (CVSS) and priority for remediation
- Evidence and proof-of-concept information for target exploitation
- Detailed steps on how to remediate any vulnerabilities and how to prevent them in the future
- Additional details, such as tools used during the assessment, people involved, checklists etc.

2. TYPES OF PENETRATION TEST

2.1 INFRASTRUCTURE/NETWORK TEST

An infrastructure penetration test is a comprehensive test of your systems, infrastructure, and network, designed to uncover and exploit a wide range of security weaknesses. This is achieved by simulating a real-world hack, with our penetration testers armed with a variety of pre-made and custom-built exploits and techniques.

2.2 WEB AND MOBILE APPLICATION TEST

Coresecurity's application tests use a blend of cutting-edge automated tools and manual expertise to find and exploit security weaknesses in your mobile and web apps. As champions of industry best-practices, our tests are carried out by qualified security professionals and are based on the industry-standard OWASP methodology.

2.3 BUILD REVIEW

Reviewing the configurations of applications, operating systems, servers, firewalls and other components is vital to protect yourself against threats. After all, if a poorly-configured build containing security vulnerabilities is deployed across your entire estate, the impact to your organisation's security could be substantial. We can also help ensure your deployments meet various compliance frameworks, such as PCI DSS.

2.4 SOCIAL ENGINEERING

Humans are often the weakest link in the cyber security chain, with even the tightest technical controls overcome by a compromised employee. By testing and then educating your staff, you can make this link as strong as possible, drastically increasing your organisation's overall security. Coresecurity provide a range of social engineering tests, including phishing, vishing, SMShing, preloading and pretexting. This can even be extended to full Red Team assessments.

2.5 RED TEAM ASSESSMENTS

Red Teaming is a comprehensive security audit that makes use of all the above tactics in an attempt to breach your physical and cyber security defences. Our expert operatives will leverage every technical and social engineering weakness in an attempt to compromise your security, with the goal of gaining access to physical site(s).

3. EXAMPLE TESTS

The following tests are indicative cases of penetration tests on a small, medium, and larger scale. They're included here to give a sample of common types of tests and example vulnerabilities found. For an accurate quote, please contact our sales team.

3.1 EXAMPLE SMALL TEST

Popular with smaller organisations wanting to know their own security posture as well as demonstrate good security practices to their customers.

DESCRIPTION	Penetration testing of a small web application and associated cloud infrastructure, designed to mimic a real-world attack with no details about the app or environment disclosed upfront.
TEST TYPE	Black box, unauthenticated test.
LIMITATIONS	No denial of service (DoS) No social engineering
VULNERABILITIES	Poor error handling Depreciated cryptography Cross-site scripting
TYPICAL PRICE	

3.2 EXAMPLE MEDIUM TEST

Popular with larger SMEs and any business with a strong focus on delivering services via custom-built web apps.

DESCRIPTION	Application test of a medium web-based management portal and associated cloud infrastructure.	
TEST TYPE	Grey box, authenticated and unauthenticated test.	
LIMITATIONS	No denial of service (DoS) No social engineering	
VULNERABILITIES	SQL injection User enumeration Credentials sent in clear text	Weak ciphers Stored XSS
TYPICAL PRICE	£3,000 - £5,000	

3.3 EXAMPLE LARGER TEST

Larger tests vary greatly depending on the business and security objectives of the organisation being tested.

DESCRIPTION	A larger test of internal applications, systems infrastructure and social engineering. A comprehensive security review with limited information disclosed to us up front.		
TEST TYPE	Grey box, unauthenticated test.		
LIMITATIONS	No denial of service (DoS)		
VULNERABILITIES	Poor network segmentation Improper access controls Missing critical OS patches	Directory Traversal Remote code execution	Social engineering awareness
TYPICAL PRICE	£5,000-£20,000		

Email: info@Coresecurity.co.jp Web site: www.coresecurity.co.jp