Penetration testing datasheet

Understand your cyber attack surface strengths and vulnerabilities with penetration testing.

By simulating real-world attacks, organisations can identify vulnerabilities and weaknesses in their systems before malicious actors exploit them. This proactive approach not only helps to safeguard sensitive data and intellectual property, but also helps prevent potential financial and reputational damages.

Critically, penetration testing is essential for meeting regulatory and compliance standards as it provides a tangible demonstration of an organisation's commitment to maintaining a secure environment. Through regular penetration testing, organisations can continually assess their security posture, refine their defence strategies and maintain a resilient stance against evolving cyber threats.

Our approach

Orro is an Australian-owned business specialising in cyber security, enterprise networking, cloud and collaboration solutions. With extensive experience in penetration testing for businesses of all sizes, we adopt a holistic approach.

Our testing can cover every aspect of your network and systems, including security and assurance testing for customised applications. We identify and report vulnerabilities and risks in a clear, prioritised format with recommendations.

Orro's penetration testing approach is closely aligned to the Open Web Application Security Project (OWASP) guidelines. To provide a consistent, repeatable and high quality result, we use a number of methodologies depending on the organisation and the targets. These include well-defined standards such as:

- OWASP Top 10 (Web, Mobile and API - latest versions as released)
- OWASP Testing Guide
- SANS 25 (based on the CWE framework) & SANS CSC (version 6)
- OSSTMM
- MITRE ATT&CK

We are experts at running large scale ongoing penetration testing for organisations and can integrate our reporting into a range of task tracking systems, as required.

Key benefits

Validate your cyber security across your entire attack surface and align vulnerability management with key business objectives.

Prioritised and actionable reports to guide remediation of vulnerabilities and manage risk.

Gain an understanding of your systems management and application development strengths and weaknesses to guide continuous security process improvement.

Revalidation of testing within three months to ensure patches are applied, firmware is updated and security gaps are closed.

Comply with regulations including data privacy and security, to build customer trust and protect your organisation from penalties.

orro®
Cyber Security

Services overview

Web application assessment

Web testing is based on the Open Web Application Security Project (OWASP) industry guidelines as well as the Common Weakness Enumeration (CWE) Top 25.

Inclusions

Orro can test all your web applications, whether they are:

- Small brochureware sites
- Medium sized web applications, or
- Large and complex web applications

Orro maintains test cases based on industry best practice, such as the OWASP testing guide(s) and other industry-developed techniques.

With every tester utilising the same workflow and practices and with every test including an extensive QA process by a senior tester, you can be assured of thorough and consistent outcomes.

Application test outcomes are valuable indicators of internal application development skills and gaps, providing opportunities for training and tooling improvements to future issues.

Wireless security assessment

Wireless networks can provide an attack surface that extends well beyond the physical boundary of an organisation's premises. This makes them an attractive target for a determined attacker.

Inclusions

Wireless security methodology focuses on the following components:

- Wireless environment – scanning and discovery
- Wireless Infrastructure – device configuration review
- Wireless infrastructure – deployment and operations assessment
- Validation of network segregation between wireless networks such as guest and corporate networks
- After initial review is completed and any issues addressed, this will form a security baseline

API security assessment

Our approach is based on the Open Web Application Security Project (OWASP) industry guidelines for API testing.

Inclusions

Testing can be performed as standalone (using a Postman or Open API specification) or as part of a broader test including the web application or other API client.

All testing is performed against industry best practice, and findings are mapped to the latest OWASP API Top 10.

Services overview

Host configuration assessment

Host configuration assessment considers the device configuration of particular servers (and supporting applications) or other devices.

Inclusions

Areas of focus and review during this activity may include:

- Operating system (or equivalent) updates and patches
- Default configurations
- File system permissions
- Misconfiguration of, and any known vulnerabilities with, installed services
- Security controls used in the provision of services on file servers
- Configurations of supporting applications
- Minimised attack surface (no extraneous services are running)
- Comparison against provided baseline / documented configurations
- Access to sensitive data, such as configuration files containing credentials

Mobile security assessment

Our approach is based on the Open Web Application Security Project (OWASP) industry guidelines for mobile testing.

Inclusions

With so many applications being delivered these days via mobile, we meet your native, web or hybrid security testing requirements.

All testing is performed against industry best practice and findings are mapped to the latest OWASP Mobile Top 10.

Internal network penetration test

Internal network penetration testing assesses the hosts and services within internal networks for vulnerabilities and weaknesses that could be exploited by an insider threat, or compromised internal machine.

Inclusions

This is typically undertaken as one of three approaches:

- Objective based testing, where a tester is provided a standard user account within the network, and has an objective to gain access to an agreed target (such as Active Directory, Financial or Customer Data)
- Living off the land (LoL) where a tester is provided access to the internal network, and then uses standard tools and techniques to gain access to systems, exploring identified vulnerabilities and lateral movement opportunities
- Vulnerability assessment, where all in-scope targets are scanned using industry leading tools, and all findings are manually reviewed and categorised to help assess overall risk

Services overview

External network penetration test

External network penetration testing assesses the security posture of the infrastructure exposed to the broader internet.

Inclusions

This is undertaken in two broad categories:

- Automated scanning - scans all exposed services for known misconfigurations or vulnerabilities
- Manual testing - applies manual testing techniques and expertise to review exposed hosts and services

Identified devices are interrogated using a variety of tools to identify open ports, services and vulnerabilities.

Areas of focus and review include:

- Infrastructure misconfigurations
- Known vulnerabilities related to exposed services
- SSL Certificate configurations
- Analysis of results from network security assessment tools such as Nessus and Nmap
- Manual analysis of reported vulnerabilities to assess exploitability and criticality

Red team

Planning, coordination, execution, assessment, analysis and reporting on a simulated real-world attack using Red team techniques. We utilise attack and penetration tools intended to covertly test the organisation's technology and process controls against attack, including phishing, malware, application or infrastructure attacks.

Inclusions

In performing a Red teaming engagement, we will target specific objectives which are core to the current and future operations of your organisation.

The goal throughout this exercise is to improve your overall security posture by demonstrating the impact of a targeted attack and providing recommendations and learning opportunities to improve security incident response.

This engagement is expected to follow a phased approach:

- Planning and preparation
- Gaining an initial foothold (external attack activities)
- Identifying internal paths to target objectives
- Obtaining objectives (internal attack activities)
- Increasing 'noise' to attempt to validate Blue team response
- Reporting
- Purple teaming (optional)
- Employee security awareness training (optional)

Services overview

Application code review

Orro can perform security-focused reviews of applications developed using a wide variety of languages and platforms.

Inclusions

- Manual high-level review where the code is searched for common security issues and weaknesses
- Deeper code scanning assessments can be implemented using SAST or DAST tools
- Identifying security weaknesses and vulnerabilities at the source code level and show how these result in security defects
- Additional code review for applications running on older codebases and frameworks to identify new and emerging classes of coding vulnerabilities

Cloud services security review

Security assessment of cloud-based services (SaaS/PaaS/IaaS) such as AWS, Azure and O365 based on a configuration and implementation review.

Inclusions

- Review configuration settings and options against vendor and industry best practices
- Examine user and group administration practices and effectiveness
- Analyse data protection measures
- Evaluate retention policies, eDiscovery and audit logs as part of the compliance and audit controls
- Documentation and reporting of results with actionable recommendations

Reporting & analytics

The Orro security portal provides both automated and manual reporting for penetration testing. Our standard report includes a high-level executive summary of findings, along with a detailed description of all findings, associated risk ratings and recommendations.

We can also provide:

- Static reports which can be used for compliance reporting
- Advanced analytics platform that clients can use to explore, manage and organise any issues and recommendations
- Integration to ITSM tools for issue reporting
- Integration with any Defect Tracking Systems (e.g. Jira or Service Now) for large or repeat programs of work, to automatically push new findings and reports into your systems for easy tracking.

Our penetration testing credentials

Orro is an ISO/IEC 27001 certified testing organisation which maintains a global team of security specialists. We operate a SOC2.0 model internally with 3 divisions allowing for cross-divisional support for our clients. As part of the Orro team, all members of the Orro Cyber Security Assurance team obtain (at a minimum) the following qualifications:

CREST | PEN TEST

CREST Registered Penetration Tester

OffSec OSCP

Offensive Security Certified Professional (OSCP)

Our staff are experienced in aspects of information technology management and governance, enterprise security architecture and service management frameworks, including ISO 27000, NIST, COBIT and SABSA.

The future feels like this.®

We're Australia's leading platform-enabled, secure network and digital infrastructure provider. We're trusted by our clients to deliver the future now, transforming business and bringing people closer together.

CONTACT US

1300 900 000 sales.enquiries@orro.group

Sydney | Melbourne | Brisbane | Perth | UK | Philippines

orro.group

Securely Connected Everything™