Penetration Testing Services

Contents

1.0 The What and Why of Penetration Testing 3

2.0 Certified Engineers 3

3.0 Our Penetration Testing Service 4

4.0 Deeper Dive into Selected Penetration Testing Services 5

4.1 Web Application Security 5

4.2 Network Security Audit 6

4.3 Mobile Application Security 7

4.4 External Penetration Test 8

4.5 Internal Penetration Testing 8

4.6 Application Pentest 9

4.7 IoT Pentest 10

4.8 Stress Testing & DoS Simulation 10

4.9 Secure Software Development Partner and Secure Code Review 10

5.0 Free with every service 11

6.0 Your XCELIT Representative 11

1.0 The What and Why of Penetration Testing

An ethical penetration test (or "Pentest") is an authorized attack against your IT systems to identify and exploit their security weaknesses / vulnerabilities, in order to evaluate the real-world risks, they pose to your business.

The goal of a Penetration Testing is to proactively uncover your weakest links and identify the extent of damage a real malicious attacker could cause your business.

Penetration Testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as un-sanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF (web-application firewall) security policies and patch detected vulnerabilities.

Penetration Testing also satisfies some of the compliance requirements for security auditing procedures, including ISO27001, PCI DSS and SOC 2.

XCELIT's Penetration Testers are deliberately independent of all other services to ensure little-to-no prior knowledge of how client's systems are secured.

XCELIT is a CREST Certified Penetration Testing provider.

If you have a need not mentioned in this explainer, please ask.

2.0 Certified Engineers

Crest Certified Penetration Testing by Certified Penetration Testers

3.0 Our Penetration Testing Service

- Web Application Penetration Testing
- Closed-Box Penetration Testing
- Open-Box Penetration Testing
- White Box Penetration Testing
- Black Box Penetration Testing
- Grey Box Penetration Testing
- Active Directory Penetration Testing
- Android App Penetration Testing
- API Services Audit
- Application Penetration Test
- Cloud Security Penetration Testing
- Compromise Audit
- Covert Penetration Testing
- Dynamic Application Security Test (DAST)
- External Penetration Testing
- Firewall Penetration Testing
- GPDR Penetration Testing / Audit
- Internal Network Penetration Testing
- IoT Pentest / IoT Device Pentest
- Load / Stress Testing & DoS Simulation
- MPLS Security Audit
- Network Resiliency Audit
- PCI DSS Security Audit
- Purple Teaming
- Red Teaming
- Secure Code Review
- Security Controls Audit
- Social Engineering & Phishing Penetration Testing
- SS7 Telco Penetration Testing
- Threat Intelligence Service

We have not dived into every service within this document.

Should you require specifics, please reach out.

4.0 Deeper Dive into Selected Penetration Testing Services

4.1 Web Application Security

The primary objective of a web application penetration test, is to identify exploitable vulnerabilities in applications before hackers are able to discover and exploit them.

Web application penetration testing reveals real-world opportunities for hackers to compromise applications in ways that allow unauthorized access to sensitive data or even system take-overs for malicious purposes.

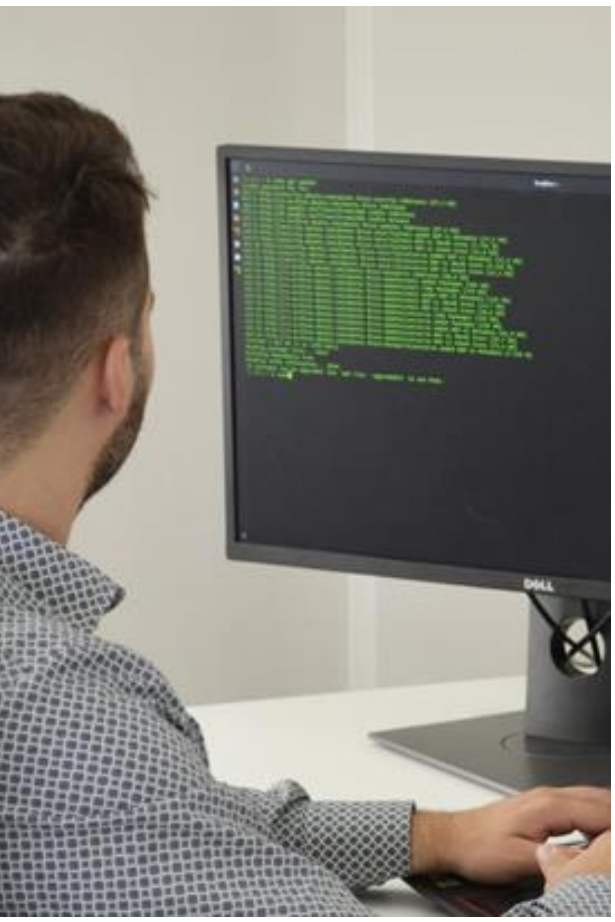
In our testing we include everything:

- Injections: SQL, XSS, CSRF
- Authentication tests and Session Management
- Sensitive Data Exposure checks
- Broken Access Control
- Security Misconfigurations and Security Misconfigurations

We understand applications

Our Penetration testers:

- Have experience developing software, not just trying to break it.
- Use this experience to zero in on critical issues and provide actionable remediation guidance.
- Identify application security flaws in the environment.
- Understand the level of risk for your organisation.
- Can help address and fix identified application flaws.



4.2 Network Security Audit

A Network Security Audit is an audit of all your network systems to make sure that potential security risks are eliminated or minimized.

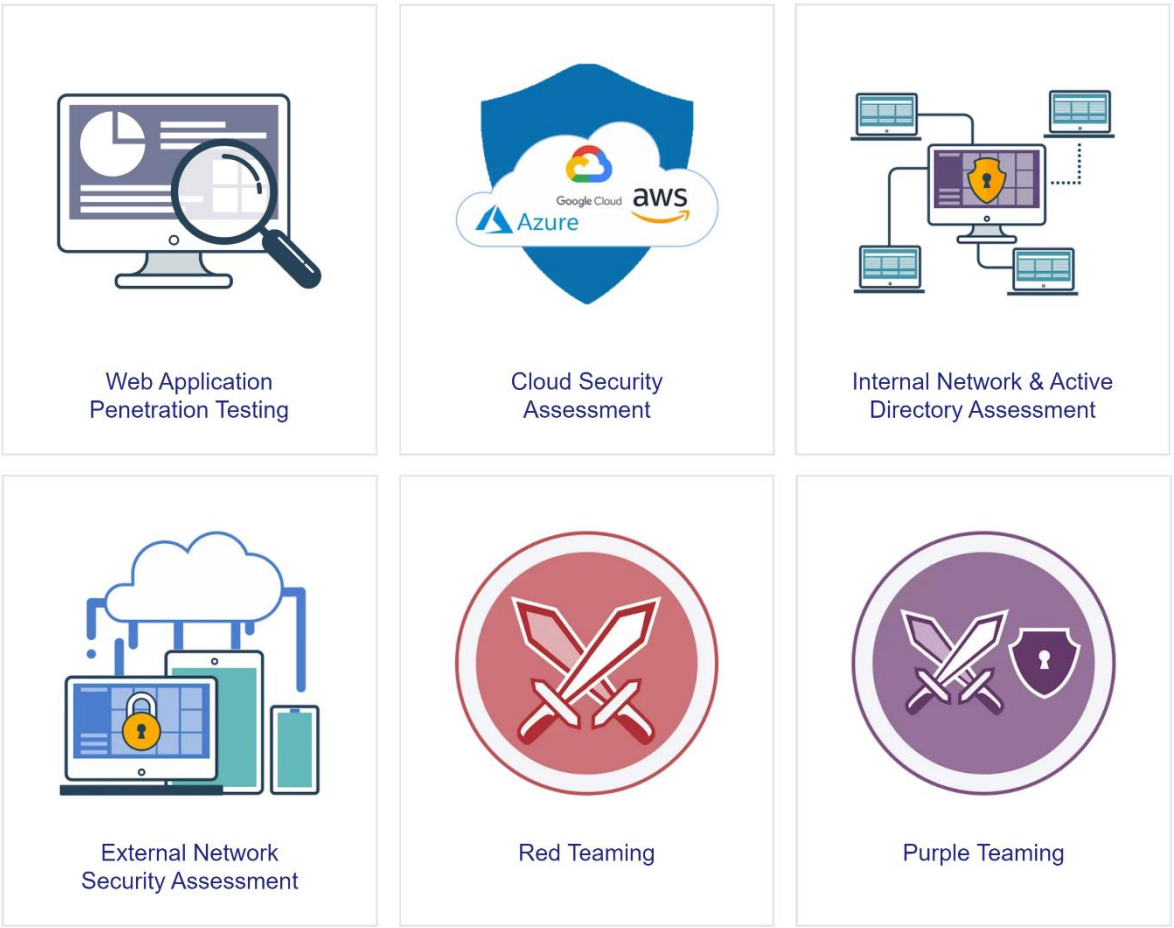
Cloud, servers, routers, workstations, gateways, must all be checked to make sure they are secure and safe and aren't sharing any sensitive information.

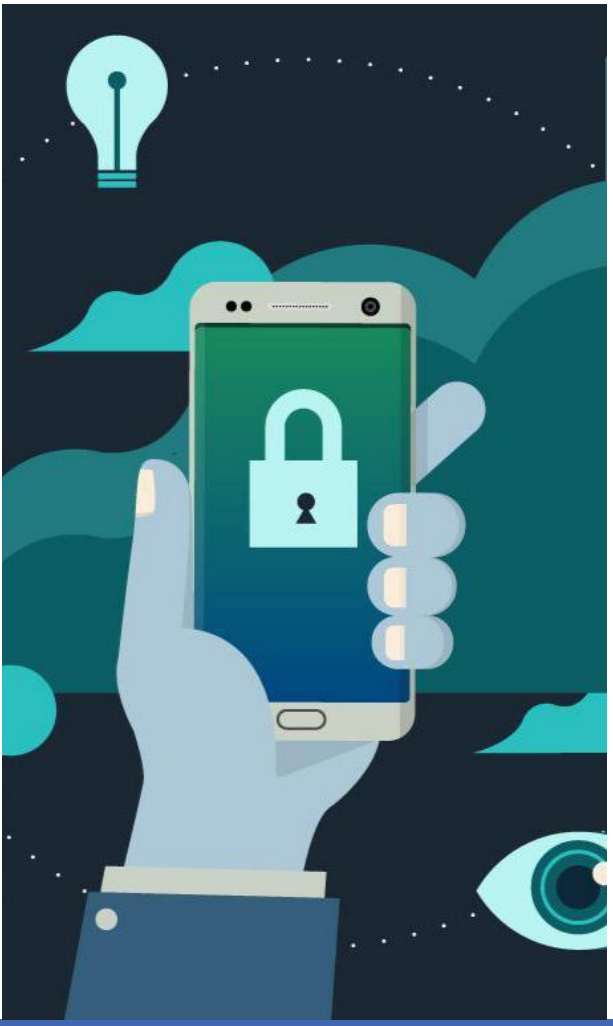
XCELIT's Network security audit methodology is based on extensive professional experience and information system security assessment best practices gathered from:

- the Open-Source Security Testing Methodology Manual ("OSSTMM")

- the National Institute of Standards and Technology ("NIST") Special publication 800-115: Technical Guide to Information Security Testing and Assessment

- the Penetration Testing Execution Standard ("PTES"), and the Open Web Application Security Project ("OWASP") Testing Guide v4.0.





4.3 Mobile Application Security

As application security experts, it is our mission to define and promote mobile application security.

XCELIT performs penetration testing and code review on all platforms for mobile applications and has created a dedicated testing environment fully equipped for testing Android and iOS applications.

During testing, we simulate a multitude of attacks, both general application attacks and mobile dedicated attacks.

The testing simulates a real hacker and what he can do to penetrate the application and retrieve confidential or sensitive data.

Based on OWASP Mobile security

When testing the security of mobile applications our security team uses the framework from OWASP mobile project, regarded as the leading framework by Penetration Testing experts.

Part of the security checks can be seen bellow:

M1: Improper Platform Usage

M2: Insecure Data Storage

M3: Insecure Communication

M4: Insecure Authentication

M5: Insufficient Cryptography

M6: Insecure Authorization

M7: Client Code Quality

M8: Code Tampering

M9: Reverse Engineering

M10: Extraneous Functionality

4.4 External Penetration Test

The best method to simulate an actual external attack is to undertake an External Penetration test. In an external Penetration Test the Penetration Testers are not provided with any real information about the target environment (other than IP address), and they must covertly collect information before the attack.

External Penetration Testing includes everything from web application security, web servers, services, physical security, phishing attacks, Denial of Service and many others

Our Penetration Testers are armed with the objective of trying to find any and all ways that will allow an attacker inside the company network.

Use XCELIT for:

- Realistic attack scenarios which portray actual results and methods of an attacker, covering all public areas from the network from services, applications, servers and IPs
- Clearly explained step-by-step definitions of each and every vulnerability.
- Remediation support

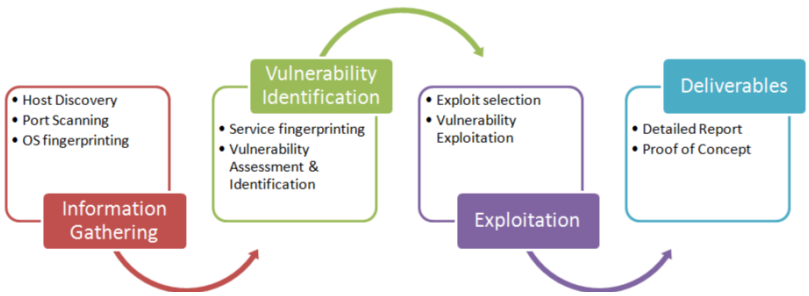
4.5 Internal Penetration Testing

Internal Penetration Tests simulate the scenario where the an attacker has already gained access by infecting an employees PC or server.

Internal Penetration Tests can be used to identify the biggest risk in case of an already breached network and what exactly a Threat Actor may be able to obtain. In an Internal Penetration Test the XCELIT Team will have access to the company network without any knowledge about network configuration or architecture.

Our Penetration testers will then try to detect all weaknesses and vulnerabilities from inside the network and will try to escalate their privilege until they will have complete access.

General Internal Penetration Testing Approach



4.6 Application Pentest

The objective of the assessment is to identify vulnerabilities in the application and use manual testing techniques to verify their existence. These assessments are most successful when clients share all known information with the consultant; however, the client can elect to share less information.

XCELIT follows a highly-structured methodology to ensure a thorough test of the application and its environment is conducted.

Our methodology uses a phased approach, consisting of information gathering, testing, verification, and notification.

XCELIT follows industry best practice methodologies when performing application security testing activities.

Such methodologies include:

- Open-Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP) Testing Guide
- The National Institute of Standards and Technology (NIST) SP 800-115

4.7 IoT Pentest

Complete security assessment and penetration testing of IoT and Smart devices by our subject matter experts to reveal any possible security flaws that might lead to a security breach of your device.

4.8 Stress Testing & DoS Simulation

Verify the stability & reliability of the system under extremely heavy load conditions.

4.9 Secure Software Development Partner and Secure Code Review

Integrate Cyber Security into Your Product Development or use XCELIT for Secure Code Review before releasing new software.

We are cybersecurity engineers with expertise in software product development and we can help you build your secure product.

Social Engineering & Phising

Network Resiliency Assessment

Security Controls Audit

MPLS Security Audit

Firewall Assessment

PCI DSS Security Audit

5.0 Free with every service

The followings are included in every service: - Scoping & technical meeting with the client - Management & Technical report containing the description of the vulnerabilities - Public-facing report that can be shared with clients & third-parties - A public "TRUSTED system" certificate that proves the security was assessed - **The retesting of the remediated vulnerabilities** - Technical support to remediate vulnerabilities	**Free**

6.0 A little about XCELIT

At XCELIT, our mission is crystal clear: Delivering Excellent IT Services that drive cost reduction and fortify against cyber threats, all while enabling businesses to reach their full potential. We're dedicated to your success!

We accomplish this by providing comprehensive end-to-end fully managed IT solutions customized to align perfectly with each organization's unique requirements.

Our XCELIT services include:

- Managed Cyber Security
- Managed IT
- Pentesting
- Consulting
- Outsourcing

XCELIT is fundamentally rooted in a cybersecurity-first ethos, having emerged from HackNo - Managed Cyber Security and Pentesting. Over time, we evolved with customer demand to encompass Managed IT Services, IT Consulting, and Outsourcing, all while keeping cybersecurity at the forefront of our mission.

7.0 Your XCELIT Representative

Richard Webb – Managing Director
Excellent IT, XCELIT

- **Managed Cyber Security**
- **Managed IT**
- **Pentesting**
- **Consulting**
- **Outsourcing**

Phone +61 450 322 128
Click Here to Set a Meeting
https://xcelit.io/

contents of this information is prohibited and this message should be deleted. Should the contents of this email be discussing commercial matters, no binding agreement is made until a formal contract is executed.