PENETRATION TESTING

Siege Cyber offers comprehensive **penetration testing** services designed to identify and address vulnerabilities in your organisation's systems, networks and applications. Our penetration testing services help businesses understand their security posture, comply with regulatory requirements and protect their critical assets.

We are proud to be an official Network Partner of the Australian Cyber Security Centre (ACSC).

INITIAL CONSULTATION

Understand your business environment and specific cybersecurity needs:

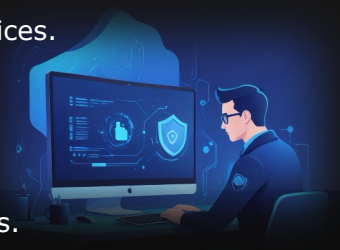
- ✓ Discuss the current cybersecurity posture and challenges.
- ✓ Identify critical assets, data and business goals.
- ✓ Understand regulatory and compliance requirements.
- ✓ Define the scope and objectives of the penetration testing engagement.

TYPES OF PENETRATION TESTING

We provide a comprehensive suite of penetration testing services to address various aspects of cybersecurity:

External Network Testing:

- ✓ Assess the security of external-facing assets.
- ✓ Identify vulnerabilities in firewalls, routers and other perimeter devices.
- ✓ Test for misconfigurations, open ports and unpatched systems.



Internal Network Testing:

- ✓ Evaluate the security within the internal network.
- ✓ Simulate an attacker's access after breaching the perimeter.
- ✓ Identify vulnerabilities in internal systems, workstations and servers.

Web Application Penetration Testing:

- ✓ Identify and exploit vulnerabilities in web applications.
- ✓ Test for common vulnerabilities such as SQL injection, XSS, CSRF and more.
- ✓ Assess authentication, authorisation and session management.
- ✓ Evaluate the security of APIs and web services.

Mobile Application Penetration Testing:

- ✓ Assess the security of mobile applications on iOS and Android platforms.
- ✓ Test for vulnerabilities specific to mobile environments.

Wireless Network Penetration Testing:

- ✓ Identify vulnerabilities in wireless networks.
- ✓ Assess the security of Wi-Fi access points and configurations.

Social Engineering Testing (Phishing and Vishing):

- ✓ Assess the human element of security.
- ✓ Conduct phishing campaigns to test employee awareness.
- ✓ Perform vishing (voice phishing) and impersonation attempts.

siegecyber.com.au contact@siegecyber.com.au

PENETRATION TESTING

PENETRATION TESTING PROCESS

Our structured approach for conducting penetration tests.

Planning and Scoping:
✓ Define the scope, objectives, and rules of engagement.

Reconnaissance:
✓ Gather information about the target environment.

Exploitation:
✓ Simulate real-world attack scenarios.

Post-Exploitation:
✓ Assess the potential impact of successful attacks.

Reporting:
✓ Provide a detailed report of findings and recommendations.

RECOMMENDATIONS AND ROADMAP

We provide a detailed roadmap for improving your security posture:

Remediation Plan:
✓ Specific actions to address identified vulnerabilities.
✓ Prioritised list of remediation steps.

Implementation Roadmap:
✓ Detailed plan for implementing security controls.

CONTINUOUS MONITORING AND IMPROVEMENT

Ensure ongoing cybersecurity resilience and continuous improvement:

Security Monitoring:
✓ Implement and oversee continuous security monitoring.

Metrics and Reporting:
✓ Track and report on key performance indicators.
✓ Regular reports to senior management.

Continuous Improvement:
✓ Identify and implement improvements.
✓ Regular reviews and updates of cybersecurity strategies and controls.

CONCLUSION

By partnering with Siege Cyber for **penetration testing services**, your business can proactively identify and address vulnerabilities, ensuring robust protection of its critical assets. Our comprehensive approach includes a range of testing services, tailored recommendations and ongoing support to maintain a strong security posture.

siegecyber.com.au contact@siegecyber.com.au