Cyber Security Penetration Vulnerability Testing Datasheet

About Cyber Security Penetration Testing:

Penetration Testing is a target driven service. Whereas vulnerability assessments examine a particular application or service for vulnerabilities, penetration testing is a crafted set of tests conducted specifically to penetrate customer cyber defences with the goal to access a customer specified target application or service.

This type of testing seeks to uncover a set of vulnerabilities that could be exploited to reach a particular target. The goal of this test is to assess the adequacy of a customer's various cyber defences and associated configurations to protect an identified information asset.

Customers may nominate which threat surface is to be used to launch the attack and tests can be conducted on or off-site according to the customer's requirements. The extent of the penetration that is to be conducted may also be set by the customer.

Tests can be conducted on a white, grey or black box approach depending on the level of disclosure the customer wishes to make in regard to their security infrastructure architecture. White box testing works on a full disclosure basis and saves time and money that would normally be spent on discovery and reconnaissance that an attacker would normally have to carry out prior to conducting a cyber-Attack.

Target Audience:

Chief Information / Chief Risk / Chief Security Officers, IT management.

Key Benefits:

The penetration testing service will provide customers with:

- ✓ A thorough test of cyber defences protecting a given information asset or service;
- ✓ Tests the effectiveness of security event instrumentation, monitoring, alerting and monitoring personel responsiveness

- ✓ A detailed report on how the penetration was achieved;
- ✓ A set of priority steps to take in order to mitigate the identified vulnerabilities;
- ✓ Guidance on how to address the identified issues.

Tests Covered Include:

- ✓ Tests of the chosen infrastructure defence infrastructure and security configurations;
- ✓ Tests the effectiveness of IPS/IDS, firewall configurations and router, switch and server hardening as is relevant;
- ✓ Tests the effectiveness of security event instrumentation, monitoring, alerting and monitoring personel responsiveness
- ✓ Uncover possible system and code vulnerabilities and identify exploitable access control issues.

Customer Benefits:

- ✓ Comprehensive test report including a management summary, a detailed risk register, prioritised remediation process and technical details and evidence for the outcomes of each test;
- ✓ A technical and managerial results review with the team conducting the test to provide clarity on the identified vulnerabilities and advice on the best practice remediation steps that can be implemented;
- ✓ Tests can be conducted by certified professionals to meet annual PCI-DSS and ISO27001 compliance requirements.

Contact information:

For further information about this course please contact Dr Graham Wright at-

Mobile: +27 83 252 5727

Email: Grahamw@gnlcyber.com