

# PENETRATION TESTING

## Advanced Professional Services



Interconnected corporate networks of partners, clients, remote offices, wireless LANs, vendors and the Internet have created multiple avenues for an attacker to target companies. Organisations face greater risks to customer data, intellectual property and financial records. CIOs and CFOs must have a clear understanding of risks and vulnerabilities to protect their organizations from external attacks. Our Penetration Testing services address these issues.

### SERVICES HIGHLIGHTS

- Identify existing and potential vulnerabilities and risks from external attacks
- Utilise experienced security analysts with the specialized skills and tools needed to mitigate client risk
- Conduct testing in a safe and controlled environment without compromising routine business activities
- Reduce investment associated with employing full time security analysts, tools and technologies
- Integrate with an overall risk management solution to address the audit requirements of policy and compliance framework such as ISO 27001, SOX, HIPPA, PCI etc

### TESTED ENVIRONMENTS

- Internal Servers Security Assessment
- Network Security Assessment
- External Penetration Testing
- Web Application Security Assessment
- Mobile Application Security Assessment (Android, Apple and Windows)
- Wireless Network Security Assessment
- Security Device Configuration Audit

### THREATS WE TEST FOR

◦ Remote Access & VPN	◦ Broken Authentication and Session Management	◦ Non-validated Redirects and Forwards
◦ Privacy Issues	◦ Insecure Direct object References	◦ Buffer Overflows
◦ Data Injection and Mining	◦ Cross-Site Request Forgery	◦ Improper error handling and trapping
◦ Web Application Vulnerabilities	◦ Security Misconfiguration	◦ Commented code
◦ Wireless Network Vulnerabilities	◦ Insecure Cryptographic Storage	◦ Insecure implementation of embedded Flash. XML. AMF. Java. ect.
◦ Cross-Site Scripting	◦ Failure to Restrict URL Access	◦ Unnecessary services running
◦ Denial of Service	◦ Insufficient Transport Layer Protection	◦ Failure to properly segregate functions or data
◦ Session Hijacking	◦ Social Engineering	

## PENETRATION TESTING METHODOLOGY

### STEP 1: INITIATION & SCOPING

Success criteria definition



### STEP 2: INFORMATION GATHERING

◦ Web server fingerprinting ◦ Spidering ◦ Error code analysis ◦ Default web server configuration



### STEP 3: VULNERABILITY DETECTION & ANALYSIS

◦ Configuration management      ◦ Session management      ◦ Web services/ Ajax testing  
◦ Authentication & authorization      ◦ Data validation      ◦ Denial of service testing



### STEP 4: EXPLOITATION

◦ Verify existence of well known vulnerabilities ◦ Elimination of false positives & false negative



### STEP 5: ANALYSIS & REPORTING

Analyze & consolidate findings to report vulnerabilities



## DELIVERABLES



#### EXECUTIVE SUMMARY REPORT

A high-level overview of your pentest report, highlighting critical vulnerabilities.



#### FULL TECHNICAL REPORT

An in-depth look into how your information security controls held up during testing.



#### AN ACTION PLAN FOR REMEDIATION

An actionable guide to help secure your organization's vulnerabilities.



#### A VALIDATION OF REMEDIATION EFFORTS (EXTERNAL PENTESTS ONLY)

In external penetration tests, integrity provides free validation of remediation efforts within a designated timeframe from the delivery of your report. These validations ensure that your organization has performed the necessary tasks to protect and secure your confidential data. This is the difference between finding real value in the test and simply searching for issues.