



ARE YOUR COMPUTERS VULNERABLE TO HACKERS?

Companies routinely protect their networks with security devices, but how do you know if they are effective? Similarly, how well do these devices protect against the latest threats on the internet?

A penetration test is the process of actively evaluating security measures by attempting to compromise systems. It conducts this with the same methodologies as those utilised by a hacker, but in a more controlled manner.

Vialtus Solutions have partnered with Integralis to provide 4 different Pen Testing services:

- External penetration Test
- Internal Penetration Test
- Vulnerability Assessment
- Web Application Audits.



Whilst IT security solution best practice is frequently being followed, it represents ever increasing costs and still does not provide the necessary overview of the security of the network. Penetration testing is a unique approach to solving these missing elements. Without assessments such as these it is difficult to quantify the effectiveness of existing security components or identify missing elements. Remote and on-site penetration testing helps to complete the picture on the effectiveness of existing security solutions such as firewalls and IDS and ensures that the devices that they are trying to protect are also as secure as possible.

EXTERNAL PENETRATION TEST

A consultant will try to penetrate (externally) the specified areas of your clients network and will compile a report which will include any recommendations.

Essentially this is a manual scan across the internet, of specified hosts. This can be run as two options:

- A vulnerability assessment designed to identify – but not exploit potential vulnerabilities.
- A full Penetration test to identify exploits and leverage them to determine further issues.

INTERNAL PENETRATION TEST:

This is essentially the same as an external penetration test – but is performed locally, on specified hosts to provide an assessment of the effectiveness of deployed internal network security. It is designed to identify, but not exploit, potential vulnerabilities. The internal scan can include a Denial of Service testing however this will only be performed with prior express approval due to the potential of increased risk. Examples of areas that would be tested during an Internal Penetration Test include:

- Unexpected or overly permissive visibility of hosts, such as back end servers within an organization's internal network
- In depth testing of internally visible services, to ensure that appropriate versions and patches are utilised.
- Identification of non-essential services, which could potentially be used to compromise hosts.

FEATURES

- Proactive risk and vulnerability assessment
- Manual Analysis of all results by experienced consultants
- Comprehensive report, suitable for both technical and management levels
- Tests can be tailored to fall in line with planned changes to IT systems security infrastructure.

BENEFITS

- Provides proactive assessments before any incidents occur
- Manual analysis provides thorough, accurate reports and reduced false positives
- No permanent harm or modification occurs
- Recommended remedial work is clearly identified.

VULNERABILITY ASSESSMENT

This is an intelligent, comprehensive, automated scan, across the internet of your hosts. It provides a vulnerability assessment designed to identify, but not exploit, potential vulnerabilities.

This service is recommended for scanning all Internet Facing IP addresses it identifies:

- Vulnerabilities that exist through misconfiguration
- Vulnerabilities present in commercially released operating systems or applications, which may be exploited to gain unauthorised access to the internal network or key servers.

This service is an automated service and therefore is complimentary to the full Interrogate External Penetration Test. Utilising both of these services would allow detailed, targeted manual scanning of key systems, such as web systems and web hosts, as well as the hosts identified by the vulnerability assessment as having significant security issues.

WEB APPLICATION AUDIT:

Simple coding and implementation errors can often leave an e-commerce infrastructure open to abuse. From high profile disclosures such as credit card compromises to subtle shopping cart manipulation, the need to ensure the security of web sites and applications is vital.

Where web applications are involved security reviews need to extend beyond traditional penetration testing.

Increasingly, the primary method of illicit ingress into a network is via a web application. The Integralis Web Application Audit provides detailed analysis and testing of web application interfaces including traditional client browser traffic as well as Web Service configurations. The service aims to ensure that all web sites are adequately secured, promoting a defence in depth strategy.

The Web Application Audit service is carried out by experienced Consultants. Highly recommended for all critical web servers, the service seeks to identify any vulnerabilities that exist in the web site being tested. The Web Application Audit is designed to conduct detailed testing of the website including the OWASP Top Ten security issues.

The service is capable of testing a variety of web application servers and languages: ASP and ASP.NET, Tomcat, PHP, JSP and Websphere are all supported along with client side Java Script.

Examples of the areas covered during a Web Application Audit include:

- HTTP request/responses
- HTTP supported methods
- HTTP authentication methods
- HTTP session management: Cookies, Session ID's, Viewstate decoding
- Manipulation and analysis of data stored in Cookies
- URL encoding to bypass IDS/IPS logic
- Input via forms, field validation
- FORM content, query strings, field buffer overflow issues
- Information leakage
- Exception condition handling
- Data handling
- robots.txt content analysis
- SQL injection
- HTTP login brute-forcing
- User spoofing or manipulation of user credentials*
- Cross-Site Scripting vulnerabilities

* This requires two 'TEST' users to be set up for the purpose of testing privilege escalation and session hijacking. In a web application with users having multiple levels of privilege, a test user pair at each level to be tested is desirable.

FEATURES

- Provides comprehensive Web Application Testing
- Identifies security issues including those found in the OWASP Top Ten
- A combination of manual and automated processing is utilised

BENEFITS

- Builds on network level penetration testing to encompass web applications
- Manual testing allows thorough understanding and analysis of web applications
- Provides a level of assurance for complex web applications against data theft and manipulation



VIALTUS
SOLUTIONS



Vialtus Solutions

connections@vialtus.com | 08000 317 317 | www.vialtus.com