M&M 950

Platinum SQUARED

Introduction

Vulnerability assessment and penetration testing are the processes of actively assessing computer networks and applications to determine the likelihood of any malicious attack being successful. Testing will attempt to discover vulnerabilities and weaknesses in the same way an attacker would and, where authorised, actively exploit them. The results of these tests and assessments will give an organisation a snap shot of their technical IT security profile and will provide detailed information on any weaknesses discovered. This information can then be used as an action plan to increase the overall security posture of the system and reduce the likelihood of an unauthorised attack being successful.

Testing can be conducted from various routes (external, internal, physical and user) to simulate a wide range of attack vectors. Assessments can also be conducted with varying levels of system knowledge (black box being no information to white box with maximum system knowledge).

At Platinum Squared, we have a specialist team of penetration testers, each with a minimum of ten years experience, covering a wide range of core skills. To compliment this, our testing team have additional skills including system administration and risk management ensuring we maximise the opportunity for the customer to benefit from the assessment.

We understand that discovering vulnerabilities may lead to delays in systems going live, therefore we ensure the customer is made aware of any major issues upon discovery, allowing, where possible, immediate remediation and re-testing during the assessment.

Platinum Squared offers a wide range of security testing services, which are detailed below:

External Network Testing

An external network assessment will target systems that reside in the company's demilitarised zone (DMZ). Typical systems include web, mail and database servers, firewalls and routers and the testing will be conducted remotely over the Internet.

External Application Testing

This type of testing will concentrate on web-based applications and will aim to discover vulnerabilities at the application layer including Cross Site Scripting (XSS), SQL injection (SQLi) and verbose error leakage.

Internal Network Testing

Internal network assessments will be conducted from within the company network. Typical systems reviewed include core servers, user workstations, printers, routers, firewalls and switches. The purpose of this type of assessment is to simulate an insider threat, be it by an employee or a contractor and will determine how secure, or insecure, a network is from the core out.

Web Application Vulnerability Scan

A web application vulnerability scan (WAVA) is a lighter variant of the traditional web application penetration assessment and is designed give network owners an understanding that their web based applications are secure against the most popular attacks.

Workstation User Testing

This assessment will confirm if a user can bypass network restrictions to gain access to unauthorised data. Examples include restricted storage areas or unmonitored access to the Internet bypassing company security measures.

Laptop / PDA Testing

Laptops & PDAs carry extra risks to a company as they are by their very nature used outside the office and the likelihood of them being lost or stolen is higher. If this were to happen, the consequences could be significant. An assessment of a laptop or PDA device will provide detailed information on the likelihood of data being extracted which could severely damage a company and its reputation.

Citrix / Terminal Services Testing

Many organisations use services such as Citrix and Terminal Services to allow their users secure access to a restricted subset of applications.

At Platinum Squared we are highly skilled in identifying where Citrix hardening, Windows OS hardening, Group Policy and Software Restriction Policy has been ineffective and allow users to gain unauthorized access to files, directories and application.

Server Build / Policy Review

Ensuring servers (Windows, Linux, AIX, Solaris etc) are built, deployed and maintained is key to reducing the likelihood of a security breach. A Platinum Squared server build / policy review will assess core systems against security good practices where we will analyse policy, patching, access rights, auditing, services, antivirus, and third party applications.

ESX and the Virtual Environment

Platinum Squared can offer a security assessment dedicated to the ESX environment that will assess the physical as well as the virtual systems.

Wireless Assessment

Platinum Squared evaluate the security of all the key components making up the wireless solution, in order to assess the security of the wireless architecture.

We will identify the key components within the wireless deployment and will highlight possible security weaknesses that could allow an attacker to gain access to sensitive information such as customer data.

Company Boundary testing

Platinum Squared offer a comprehensive firewall review providing guidance on discovered rules. Controlled external testing can determine if an Intrusion Detection System (IDS) triggers correctly and advise if this can be bypassed or be used to complete a Denial of Service (DoS) attack on internal administrative staff. We also review content filtering systems to determine allowed file types and attempt to bypass these security measures to pass unauthorised file types into the network environment.

Additionally we can review configuration documentation to ensure the rule set and the firewall operating system is as secure as possible.

Physical Security and Social Engineering

Physical and social analysis of corporate offices and data storage facilities has become an even more critical aspect of an organisation's information security and business continuity planning.

At Platinum Squared we can address this requirement using a blend experience and expertise to focus on the critical aspects of physical security and social engineering that impact an organisation's computing and data security environment.

Physical and social analysis of corporate offices and data storage facilities has become an even more critical aspect of an organisation's information security and business continuity planning as a loss of sensitive data through physical or social analysis could ruin an organisation's reputation or financial position.