MARATHON PROFESSIONAL SERVICES

Penetration Testing Service

Introduction

The goals of a penetration test vary, but the typical focus is to find vulnerabilities that could be exploited by cyber attacks and informing the client of those vulnerabilities, along with recommended mitigation strategies. Penetration tests are one component of a full security review* and audit.

The Marathon Security Test Methodology

Marathon believe that security testing is only beneficial when analysed within the context of each organisation's policies, controls and network structure. Marathon also understand that the security skills and resourcing required to determine the underlying cause of reported vulnerabilities are not always available inside of the organisations that are being tested. Based on this assumption, Marathon include concise remediation advice for each vulnerability uncovered and are happy to discuss each of our findings to ensure that each client receives best value from the Penetration Testing service.

Management Reporting

The report provided that follows the testing includes; details of all security vulnerabilities discovered and how these vulnerabilities could be combined to achieve a compromise of the system, within the context of business. This debrief is primarily given in a management context, however, where required the consultant will provide a detailed technical insight of the vulnerabilities

Why Marathon?

Marathon's Information Security Group have vast experience of helping organisations assess the business risks associated with cyber threats and security breaches through the use of best practice information security policies, procedures and expert services

Our consultants include:

- Cyber Essentials Certified Assessors
- ISO 27001 Auditors (information security standard)
- ISO 22301 Auditors (business continuity standard)
- Certified Ethical Hackers (CEH)

For more information speak with our Professional Services Team on 0208 329 1000
sales@marathon-ps.com

MARATHON PROFESSIONAL SERVICES

Penetration Testing Deliverables

The default deliverables from Marathon Penetration testing are detailed below. Additional requirements can be catered for on request.

Scope of Penetration Testing Service

The scope of each test will depend on the client's objectives for carrying out the test and in the context of each organisation. The typical scope for the penetration testing service is shown below:

Network Vulnerability Assessment

A network vulnerability assessment is a test to identify vulnerabilities, which includes vulnerability scanning, but stops short of attempts to penetrate target systems by exploiting any discovered weaknesses.

Infrastructure Penetration Testing (Key Threats)

- External internet infrastructure penetration testing
- External third-party WAN infrastructure penetration testing
- Internal infrastructure penetration testing
  - Device identification and network mapping phase
  - Service identification phase
  - Service enumeration
  - Vulnerability and misconfiguration identification phase
  - Exploitation phase
  - Post-exploitation information gathering
  - Post-exploitation privilege escalation
  - Post-exploitation further information gathering
  - Firewall and network device configuration assessment

Timescales

There is typically a two week lead time from the initial enquiry, through to delivering the Penetration Testing Service. The report is normally delivered within 5 working days of the tests being completed

Other Services

Marathon's Information Security practice offer a number of valuable certification and enablement services including:

- Cyber Essentials Enablement
- ISO 27001 Auditing
- ISO 22301 Auditing
- Information Security Reviews *