DigitalXRAID

CYBER SECURITY EXPERTS

Penetration Testing

Strengthening your security by identifying potential cyber risks

IASME Consortium

CREST

CYBER ESSENTIALS

Crown Commercial Service Supplier

DigitalXRAID

...is a trusted and recommended provider of Cyber Security Services. Our Certified security consultants will deliver an intelligent penetration test, tailored to the specific needs of your organisation.

Certified Security Experts

- We provide assurance that your security and defence is robust.
- Arm you with the confidence you need to mitigate and respond effectively to cyber threats.
- Our Penetration Testing is real world and human-led.
- Receive clear post-testing results.
- Priority driven mitigation steps, allowing prompt hardening of your security posture.

Penetration Testing Services

What is Penetration Testing?

Penetration Testing ('pen testing') is an industry recognised simulation for identifying cyber risks within an organisation. The goal for DigitalXRAID is to highlight infrastructure vulnerabilities before a hacker does. This allows the client to implement countermeasures to prevent any unauthorised access. The penetration tests also provide your organisation with an appreciation for the consequences of a potential attack. This often highlights risks that may have not been previously considered.

Our Approach

DigitalXRAID deliver a bespoke service for each organisation. Prior to undertaking any tests, our Security Experts will work with you to conduct scoping. Scoping of your systems, network and applications allows us to fully understand your individual needs. From this information DigitalXRAID will build an accurate approach which fits the profile of your operation. Our consultants can then test for potential threats throughout your organisation.

Post-assessment, we work with you, clearly presenting recommendations in your report on how to mitigate or implement countermeasures for any issues discovered.

Why DigitalXRAID?

- ✓ Certified testers to a minimum of CHECK team member or equivalent.
- ✓ Clear report, management summary and in-depth technical details.
- ✓ Post-test session with our consultant to walk you through the findings.
- ✓ Robust testing methodology.
- ✓ We work to both ISO9001 and ISO27001 Standards.
- ✓ We are IASME Gold Certfiied and auditors for the standard.
- ✓ Cyber Essential Plus Certified.
- ✓ Cyber Essentials Certification Body.
- ✓ CREST member company.
- ✓ CREST registered testers.

Types of Penetration Testing

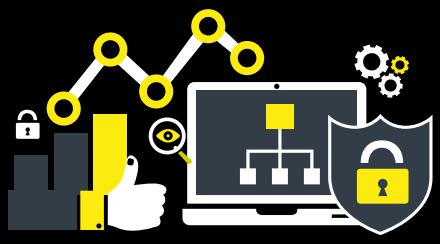
If you need to conduct a penetration test on specific technologies or run a full audit, DIGITALXRAID always provide a focused and comprehensive approach to address your individual requirements.

Internal Assessment Testing

Internal tests will provide your organisation with a review of its security from the point of view of a staff member or someone with access to your internal network. The tests will analyse if it is possible to gain access and exploit privileges to protected company data. It will also look at whether it's possible to then remove this data from the corporate workplace without triggering alarms or leaving a trail.

An internal test will include, but is not limited to:

- ✓ Both wireless and wired infrastructure (inc. WIFI)
- ✓ Network Switches
- ✓ Network Routers
- ✓ Firewalls
- ✓ IPS and IDS
- ✓ Proxy Servers
- ✓ Windows Server
- ✓ Unix Server
- ✓ Novell Server
- ✓ IP Telephony
- ✓ File and Print Services
- ✓ Application Services
- ✓ Shared Storage
- ✓ Native Internet Connectivity
- ✓ Ability to steal and manipulate data
- ✓ Extranet Servers
- ✓ Remote Access



External Assessment Testing

DigitalXRAID use a range of methodologies to uncover and exploit your external facing infrastructure. This provides an in-depth security profile of your external facing networks, along with highlighting how they could potentially be accessed by individuals or systems outside of your organisation.

An external test will include, but is not limited to:

- ✓ DNS servers
- ✓ Firewalls
- ✓ Routers
- ✓ IPS and IDS
- ✓ VPN Servers
- ✓ FTP Servers
- ✓ HTTP Servers
- ✓ Mail Severs
- ✓ Web Services
- ✓ Extranet Servers
- ✓ Cloud Services

Web Application Testing

Web server tests are designed to assess all types of web server, from static websites to e-commerce. At DigitalXRAID we focus on the logic built into the website, with particular focus on an environment which requires an end-user to input data.

A web application test will assess the environment for both server side and client side attacks which could allow an attacker to manipulate the users who access the current infrastructure. DigitalXRAID will assess if your website, website CMS and application software are susceptible to a number of vulnerabilities. This includes assessing the use of cookies, data forms, the way content presents itself and error 404 pages.

Our web application testing is aligned with the Open Web Application Security Project (OWASP Top 10)

A web application test will include, but is not limited to:

- ✓ Cross-site scripting
- ✓ SQL Injection
- ✓ Database Access
- ✓ Privilege Escalation

Mobile Device Testing

With the use of mobile devices increasing every day, and an estimated 7 billion people in circulation across the world, it's never been more important to test both web and mobile.

Whether its phone, tablet, Apple or Android, DigitalXRAID security consultants have a comprehensive knowledge base to expose vulnerability in both devices and applications.

Many mobile applications use web-based functionality, opening them up to session hijack attacks. These allow hackers to capture user displays, perform tap jacking and screen smudge attacks. iOS devices in particular can be vulnerable to buffer overflow attacks, allowing hijackers to find security weaknesses. The idea of mobile device testing is to highlight these risks within your own mobile applications and provide countermeasures for these risks.

Network Device Review

The network device review consists of a thorough audit of all your organisation's network devices and their configurations. This could be switches, routers, balancers etc.

A network device review will include, but is not limited to:

- ✓ Device operating system
- ✓ Base configuration, accessible services and administrative control
- ✓ Logging
- ✓ Security best practices
- ✓ Port security
- ✓ Spanning tree protection
- ✓ VLAN distribution

Server & Workstation Build Review

The server and workstation configuration review consists of a thorough audit of your organisation's server and workstation builds.

The server and workstation build test generally consists of:

- ✓ Operating System Levels
- ✓ Appropriate patching
- ✓ Core Security Configuration
- ✓ Password policies and management
- ✓ User Rights and Permissions
- ✓ Logging and Auditing
- ✓ Base configuration, accessible services, administrative control
- ✓ OS and security best practices
- ✓ CIS Baselining

Firewall and Rule Assessment

DigitalXRAID will examine your firewall rule base line by line, identifying any ineffective or potentially harmful rules.

Further to this, we can also perform an assessment against the firewall itself, to check for potential exploits or vulnerabilities. After completing the assessment, we will produce a report containing recommendations around rule removal, update and general firewall build.

What happens after the tests?

At DigitalXRAID, we produce a high-level management report and in-depth technical review for every organisation we test. The documents highlight security vulnerabilities and identify areas for exploitation. In addition, they provide guidance on how to improve and put countermeasures in place.

Whilst our penetration tests are complex, the reports are tailored to the audience, be it managerial or technical. DigitalXRAID ensure all tests have a full, clear debrief at the end of each engagement which is presented in a way every client can understand and act upon.

DigitalXRAID

CYBER ESSENTIALS • SOCIAL ENGINEERING

GDPR CONSULTANCY • PENETRATION TESTING

COMPLIANCE PCI/ISO/CE • SECURITY CONSULTANCY

DigitalXRAID

Contact HM Network
Tel 03333 444 190
info@hm-network.com