VULNERABILITY & PENETRATION TESTING

Security - Risk Advisory Services

CDW provides vulnerability assessment and penetration testing services which will help you to better understand your security posture, which weaknesses hackers could leverage, and whether your organization could withstand a malicious attack.

Protection of your organization's data is vital, and failure to do so can be costly, and potentially disastrous. We want to help you understand your risk of exposure more clearly, so that you are equipped to make informed decisions regarding your business.

WHAT WE OFFER

NETWORK

Network tests involve testing for network weaknesses, misconfigurations, and mismanagement of devices. We offer both internal and external network tests.

WEB APPLICATION

Web application tests involve testing for application weaknesses, technical flaws or vulnerabilities. Our services also include web API testing.

MOBILE APPLICATION

Mobile application tests involve testing for mobile application weaknesses, technical flaws or vulnerabilities. Our services include testing the entire multi-tier mobile application architecture.

WIRELESS

Wireless testing involves identifying vulnerabilities in a wireless network, at the access point or on hosts. This test requires physical proximity to an access point.

SOCIAL ENGINEERING

Social engineering is a manipulation strategy designed to trick employees into performing an action that is not in their best interest. It is often used by attackers to target a user's credentials or to compromise machines. We prepare and educate our clients by offering:

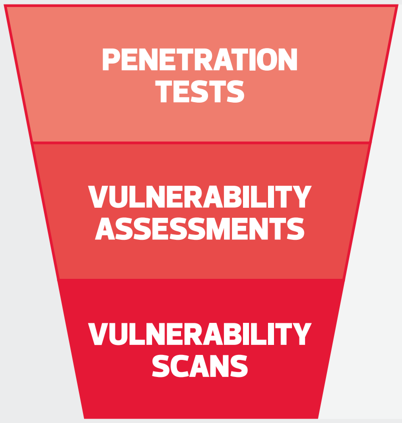
- Email phishing campaigns
- System compromise via social engineering
- Telephone campaigns
- USB drops

INTELLIGENCE GATHERING

Open source intelligence gathering (OSINT) involves finding, selecting and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. OSINT is used to determine what information an organization has that could be leveraged by an attacker.

WHAT WE DO

We offer three tiers of service to match your requirements.



PENETRATION TESTS

Discovered vulnerabilities are used to perform a goal (e.g. take over an active directory, leak information, disable services, etc.).

VULNERABILITY ASSESSMENTS

Manual and automated means to evaluate a vulnerability, which includes discovery, research and testing.

VULNERABILITY SCANS

Use of automated tools and report generation.

OUR TESTING APPROACH

Depending on the specific objectives of your business, we offer several methods of testing:

- Black-box testing: Testing with no prior information about the target, network or application.
- Grey-box testing: Testing with some information about the target, network or application.
- White-box testing: Testing with full information about the target, network or application.

OUR METHODOLOGY

We use industry best standards for performing penetration tests. The following methodologies are used:

- **OPEN WEB APPLICATION SECURITY PROJECT (OWASP) TESTING GUIDE:** Standard utilized for web application vulnerability assessments and penetration tests.
- **OWASP MOBILE TOP 10:** Standard utilized for mobile vulnerability assessments and penetration tests.
- **PENETRATION TESTING STANDARD (PTES):** Standard utilized for intelligence gathering, social engineering, wireless and network penetration tests.
- **NIST TECHNICAL GUIDE TO INFORMATION SECURITY TESTING & ASSESSMENT (SP800-115):** Used as a general approach for conducting security testing and assessments.

For more information, contact your CDW account manager at 800.972.3922 or visit CDW.ca/security

The terms and conditions of product sales are limited to those contained on CDW's website at CDW.ca. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. CDW®, CDW·G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners.