ADVERSARY SIMULATION & PENETRATION TESTING

Risk Advisory Services

Protection of your organization's data is vital, and failure to do so can be costly and potentially disastrous. At CDW, we want to help you understand your risk of exposure more clearly so that you are better equipped to make informed business decisions. Through our adversary simulation and penetration testing services, we are able to uncover security vulnerabilities in your environment, understand your company's security posture and test its readiness to withstand and respond to a real-world cyberattack.

WHAT WE OFFER

ADVERSARY SIMULATION / RED TEAM

Through this service we assess a company's readiness to withstand and respond to a simulated real-world cyberattack.

NETWORK

The network service tests for network weaknesses, misconfigurations and mismanagement of devices. We offer both internal and external network tests:

- Advanced Active Directory attacks
- Scenario-Based Penetration Test
- Wireless
- Vulnerability Assessments

WEB APPLICATION

This service includes testing for application weaknesses, technical flaws or vulnerabilities, and web API testing.

MOBILE APPLICATION

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

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:

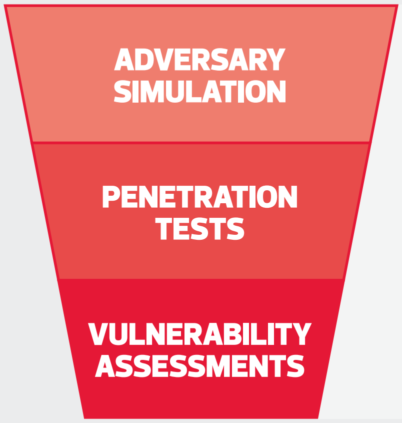
- System Compromise via Social Engineering
- Email Phishing (General & Targeted) Campaigns
- Telephone Campaigns
- Physical including USB Drops

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

Our services come in three tiers, dependent upon your requirements:



ADVERSARY SIMULATION

Assess your organization's detection and response capabilities to real-world cyberattacks.

PENETRATION TESTS

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

VULNERABILITY ASSESSMENTS

Assessments are performed both manually and automated to evaluate a vulnerability. This includes discovery, research and testing.

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.
- **MITRE ATT&CK FRAMEWORK:** Used as a foundation for the development of specific threat models and methodologies.

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