opentext™

Penetration Testing and Methodologies

Bring in the experts to find defense weak points before attackers do

Introduction

With decades of intelligence and cyber expertise, OpenText offers unmatched, full-spectrum end-to-end cyber solutions that help organizations secure their space and confidently navigate the cyber domain. We help clients solve their biggest and most complex cyber challenges, from providing computer network defense and addressing advanced persistent threats to cyber hardening of sophisticated military systems and critical infrastructure protection.

OpenText has successful long and traceable history in performing services as required by our clients. Below paragraphs highlights our detailed approach and how we plan to support your organization with Internal and External Information Technology Security Penetration Assessments and Vulnerability Scan.

Penetration testing, commonly known as pen testing, is a simulated cyber attack against a computer system, network, or web application to identify vulnerabilities that could be exploited by malicious actors. The goal is to assess the security posture of the target and provide actionable insights for strengthening defenses.

Penetration Testing and Methodologies

Bring in the experts to find defense weak points before attackers do

Customer and OpenText team roles and responsibilities

Role	Key Responsibilities
Customer Program Sponsor	▪ Serves as the highest point of escalation for strategic and tactical direction of the project
Customer Trusted Agent	▪ Receives the assessment briefings and milestone reports from OpenText and disseminates that information internally within Customer ▪ Approves Rules of Engagement for the assessment to keep the engagement aligned with customers internal objectives. ▪ Works with the OpenText's team to confirm that customers technical personnel and resources are available for the assessment (i.e., network assistance, helpdesk, etc.) ▪ Attends status meetings and assists in issue resolution
OpenText Team	▪ Executes and delivers agreed-upon services, including all identified deliverables ▪ Monitors assessment status and provides feedback ▪ Provides quality assurance and assists in risk management ▪ Makes recommendations and resolves issues in a timely manner

Penetration Testing and Methodologies

Bring in the experts to find defense weak points before attackers do

Penetration Testing Methods

Type of Penetration Testing	Description	Purpose
Network Penetration Testing	Tests both internal and external network security by simulating attacks on network infrastructure.	Identifies vulnerabilities in network configurations, firewalls, and routers.
Web Application Penetration Testing	Simulates attacks on web applications to find security weaknesses.	Detects vulnerabilities like SQL injection, XSS, and CSRF.
Wireless Penetration Testing	Evaluates the security of wireless networks.	Identifies vulnerabilities in wireless protocols and configurations
Social Engineering Penetration Testing	Uses techniques like phishing to test human vulnerabilities.	Assesses the effectiveness of security awareness training and policies.
Cloud Security Penetration Testing	Assesses the security of cloud environments and services.	Identifies misconfigurations and vulnerabilities in cloud infrastructure.
Red Team vs.Blue TeamExercises	Red team simulates attackers, while blue team defends.	Tests the organization's detection and response capabilities.

Penetration Testing Approaches

Approach	Description
Black Box Testing	Testers have no prior knowledge of the system. Simulates an external attack.
White Box Testing	Testers have full knowledge of the system, including source code and architecture. Simulates an internal attack.
Gray Box Testing	Testers have partial knowledge of the system. Combines elements of both black and white box testing.

Penetration Testing and Methodologies

Bring in the experts to find defense weak points before attackers do

Key Benefits of Penetration Testing

- Early Detection of Vulnerabilities: Identifies security flaws before they can be exploited.
- Enhanced Security Posture: Provides actionable insights for improving security measures.
- Compliance Support: Helps meet regulatory requirements for security assessments.