FRONTLINE
Pen Test™

Leverage Proven Methodologies and Industry Best Practices

While many companies perform vulnerability scans of their networks, web applications and computing platforms, many never know if an attacker could actually exploit the vulnerabilities discovered in the process. Compounding the problem is the fact that most companies do not have staff with the specialized expertise required to adequately test systems without incurring a potential business operations impact.

As a result of these challenges, companies are often left exposed to threats.

Shedding Light on the Issue

Digital Defense Frontline Pen Test™ is a key component to any robust information security program. Performed by trained security analysts and utilizing industry best practice test methodologies, our Pen Test targets systems where weaknesses reside. We efficiently determine if a potential vulnerability is truly exploitable and if it could lead to the compromise of sensitive corporate data.

Frontline Pen Test

Pen Test seeks to compromise systems quickly and efficiently in order to gain the highest level of system access possible.

- External and Internal Penetration Testing
- Robust Executive and Technical Reporting
- Remote Service Delivery
- Industry Standard Testing Methodology
- Quality Control of Reports
- Global Coverage
- Subscription or Project service

Frontline WAPT

Frontline Web Application Penetration Test (Frontline WAPT™) examines internally developed web applications, and those purchased from third parties, to ferret out and expose potential vulnerabilities.

More than a simple software scan for web application vulnerabilities, Frontline WAPT utilizes a variety of sophisticated and automated software tools to detect issues such as:

- SQL insertion
- Improper character filtering
- Cross-site scripting
- Buffer overflows
- and numerous others.

Frontline WAPT is available as a Subscription or Project service.

"Digital Defense can get into the mind of a malicious hacker to determine where weaknesses reside."

A Multi-Phased, In-Depth Process

The penetration test process is actually the culmination of several different activities that ultimately provide client organizations with a clear view of exploitable threats present on its systems or networks.

Planning Phase

The assigned Digital Defense security analyst will work with the client to ensure the engagement is properly scoped and takes key systems and applications into account.

Vulnerability Assessment Phase

The penetration test begins with a comprehensive evaluation conducted via the Digital Defense vulnerability scanning service. The scan evaluates the security posture of the IP addresses or web application included within the penetration test scope in order to fingerprint the device or application and determine the number and severity of the vulnerability associated with them.

Penetration Testing Phase

After the vulnerability assessment has been completed, a certified Digital Defense security analyst utilizes a comprehensive set of tools to exploit and gain access to key systems (core servers, domain controllers, e-mail platforms, ERP, and ERM systems, etc.). The security analyst applies specialized techniques and intensive tactics not necessarily replicable by software-based assessment systems exposing the network asset(s) or web application to attack scenarios common to those experienced in a real world setting.

Documentation Phase

While testing in-scope systems, the analyst documents all test findings within the Frontline.Cloud™ platform, a secure multi-function portal that allows clients to receive centralized and standardized reporting functionality.
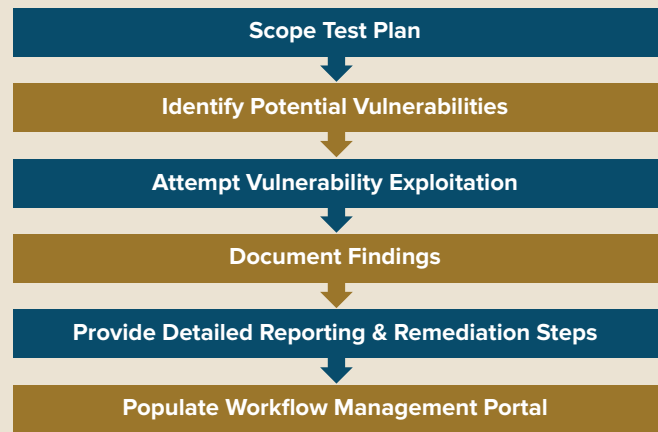
Reporting Phase

At completion of the penetration test, the client is provided full executive and technical reporting via the Frontline.Cloud platform.

Results Management

Clients can take advantage of the integrated results management interface in the Frontline.Cloud platform to quickly and effectively deal with discovered issues.

Figure 1: Penetration Testing Services Diagram

- Scope Test Plan
- Identify Potential Vulnerabilities
- Attempt Vulnerability Exploitation
- Document Findings
- Provide Detailed Reporting & Remediation Steps
- Populate Workflow Management Portal

Results Are Key

Digital Defense Frontline Pen Test and Frontline WAPT allow organizations to:

- Leverage Digital Defense's technical expertise and world-class customer service and support

- Demonstrate your commitment to information security with comprehensive reporting on the security posture of your network and web-enabled applications

- Detect possible security vulnerabilities and respond quickly with actions based on your pre-defined security policies

Let Us Help Identify Your Weaknesses

Emtec.
Business & Technology Empowered

DIGITAL DEFENSE
INCORPORATED

Emtec, Inc.
USA | Canada | India
https://www.emtecinc.com
information@emtecinc.com