CYFLARE
The threat stops here.

Penetration Testing Services Overview

A common misconception by enterprises is that their existing security tools can cater to their penetration test needs and just training their vendors and employees will ensure reduced risks. However, they miss the value a dedicated penetration tester brings in. As ethical hackers, they create ways to hack the system to show you the risk and create a remediation plan to avoid actual vulnerability.

The primary goal of Penetrating Testing (or pentesting) is to identify weak spots in an organization's security posture, as well as to measure the compliance of its security policy and test the staff's awareness of security issues. Ideally, Penetration Testing determines if a hacker were to target your network, application, or users -- how successful would they be?

Why Implement a PenTest?

Reduce Threat Surface

Our assessments help you reduce the attack surfaces exposed to adversaries.

Improve Compliance

Our services are designed to ensure that you meet compliance requirements like PCI DSS, HIPAA, GDPR, ISO, etc.

Validate Your Existing Defense

Test your resilience against a real-life cyber attack and obtain advisory on how to protect your business better.

Our Penetration Testing Services

Network PenTest

Identify weaknesses within network infrastructures, systems and devices.

Web Application PenTest

Test both the application and the environment around the application to provide a comprehensive risk analysis.

Mobile Application PenTest

Designed to identify and address vulnerabilities in mobile apps that could be exploited by hackers.

CYFLARE
The threat stops here.

Our Approach and Methodology

CyFlare's experienced penetration testers work as an independent team and identify any vulnerabilities and data security risks that enterprises may have. A complete report of risks, as well as plans for the fixing of these weak defenses and related validations, are created for the specific enterprise to follow.

We enable you to enhance your security posture, reduce risk, facilitate compliance and improve operational efficiency.

1

Scoping and Enumeration

Prior to a test, our network pen-testing team will discuss the requirements for your network or infrastructure assessment to define the scope of the test. This is followed by service enumeration, network mapping, banner reconnaissance, and prepared threat identification.

2

Reconnaissance

CyFlare will enumerate the network assets and compile a list of all accessible systems, identify vulnerabilities within systems, and find where malicious actors could break in.

3

Active Scanning and Vulnerability Analysis

Using a combination of manual and automated tools, the testing team discovers potential vulnerabilities and prepares plans to exploit them. In essence, the ideation of attack is developed here.

4

Exploitation

CyFlare's experienced security testers ethically exploit all identified vulnerabilities by employing heavy manual testing tactics that are often quite time-sensitive.

5

Identification and Remediation

A comprehensive report detailing vulnerabilities, classified according to business risk along with a remediation procedure, is provided after each assessment.

6

Re-Test

As a final step in the process, we recommend a re-test to ensure the remediation has closed on all loopholes.

CYFLARE
The threat stops here.

DREAD Scoring Overview

Upon completion of penetration testing, CyFlare will provide analysis and reporting of each identified risk with documented attack chains and proofs-of-concept (POC). This invaluable report describes risks and technical findings related to our assessment, with outlined results that are easy-to-understand and actionable.

When calculating risk scores, CyFlare uses the DREAD threat model.

Using DREAD, a numeric score between 1 and 10 can be calculated by measuring five risk categories. The DREAD name is an acronym of the five risk categories that include:

Damage Criteria		Damage Description	Critical 9.0 - 10.0	High 7.0 - 8.9	Medium 4.0 - 6.9	Low 1.0 - 3.9
D	Damage Potential	The level of damage and exposure that could be caused if a vulnerability were exploited	A malicious actor has gained full access to the system; execute commands as admin	A malicious actor can gain non-priveleged user access, leaking extremely sensitive information	Sensitive information leak; Denial of Service	Leaving trivial information
R	Reproducibility	The level of difficulty in reproducing an attack	The attack can be reproduced every time and does not require a timing window	The attack can be reproduced most of the time	The attack can be reproduced, but only within a window of time	The attack is very difficult to reproduce, even with the knowledge of the security hole
E	Exploitability	The ease to which the attack could be launched	No programming skills are needed; automated exploit tools exist	A novice hacker/ programmer could execute the attack in a short time	A skilled programmer could create the attack, and a novice could repeat the steps	The attack required a skilled person and in-depth knowledge every time to exploit
A	Affected Users	The volume of users and assets that are affected in a successful attack scenario	All users; default configuration, key customers	Most users; common configuration	Some users; non-standard configuration	Very small percentage of users; obscure features; affects anonymous users
D	Discoverability	The level of difficulty involved in enumerating the vulnerability	Vulnerability can be found using automated scanning tools	Published information explains the attack. The vulnerability is found in the most commonly used feature	The vulnerability is in a seldom-used part of the product, and few users would come across it	The vulnerability is obscure and it is unlikely that it would be discovered

877.729.3527

www.cyflare.com

sales@cyflare.com