FOTHION

PENETRATION TESTING DEMYSTIFIED

How Businesses Can Stay Ahead of Hackers

https://fothion.com

Why Penetration Testing Matters

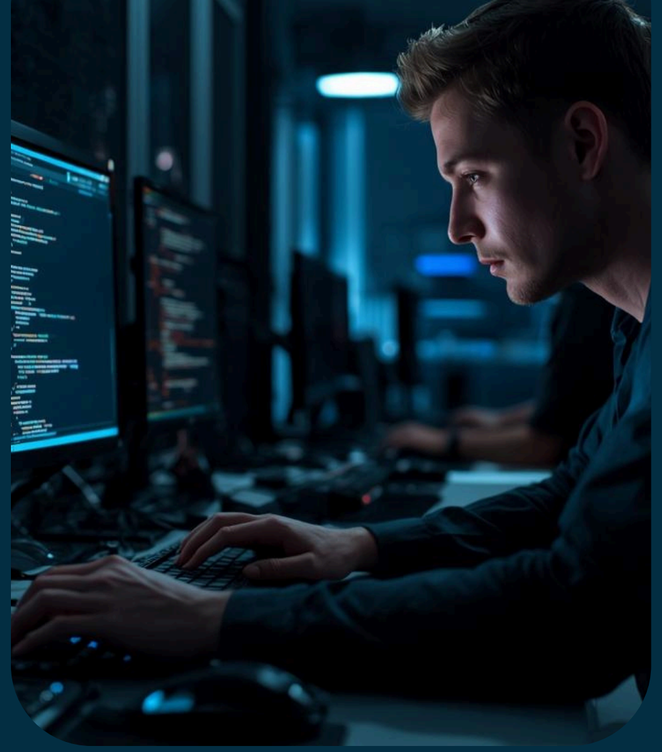
Understanding the necessity of proactive security measures

Cyberattacks are rising, and one unpatched vulnerability can cost millions. ploit them.

In the 2023 **MOVEit breach**[1], attackers exploited a zero-day flaw to compromise 2,500+ organizations and leak data from 77 million individuals—a stark reminder of the cost of inaction. Penetration testing helps uncover these risks before they're exploited, making it a cornerstone of any resilient cybersecurity strategy.

✅ Compliance requires proactive defense.
✅ Testing exposes risks before hackers exploit them.

[1] *Schaefer, M. (2025, March 14). The MOVEit Data Breach: Understanding the Risks and Mitigation Strategies. University of Hawai'i-West O'ahu. https://tinyurl.com/The-MOVEit-Data-Breach*



Understanding Penetration Testing

Exploring the necessity and process of pen testing

A penetration test is a simulated cyberattack led by security experts to uncover vulnerabilities within a network or system before real attackers do.

Think of it as a fire drill for your cybersecurity—a proactive strategy that strengthens defenses, ensures compliance, and builds resilience where it counts most.

✅ Goal: Identify weaknesses before they're exploited
✅ Outcome: Actionable insights, stronger security posture

FOTHION

Types of Penetration Testing[2]

Network

Simulate Insider Threat
Mimic the actions of a malicious insider with authorized access.

Test Access Controls
Evaluate the effectiveness of internal access controls like firewalls and user permissions.

Compromised Credentials
Use compromised employee credentials to gain access to internal systems.

Supply Chain Attack
Explore vulnerabilities in third-party software or services used within the network.

Pivot Through Internal Network
Leverage compromised internal systems to move laterally and access sensitive resources.

Web App

Identify Entry Points
Find all user-accessible areas like logins, search bars, and comment sections.

Parameter Tampering
Manipulate user input parameters to identify vulnerabilities like SQL injection and XSS.

Session Hijacking
Exploit weaknesses in session handling to steal user sessions and gain unauthorized access.

Broken Authentication
Test for vulnerabilities in authentication mechanisms like weak password policies and MFA bypasses.

Authorization Bypass
Attempt to access unauthorized resources or functionalities within the application.

Wireless

War Driving
Search for open Wi-Fi networks and assess their security posture.

Eavesdropping
Capture wireless traffic to steal sensitive information transmitted without encryption.

Road Access Point (Evil Twin)
Set up a fake access point to trick users into connecting and steal their credentials.

Wireless Intrusion Prevention System (WIPS) Bypass
Evaluate the effectiveness of WIPS deployed to detect and prevent unauthorized access

Denial-of-Service (DoS) Attacks
Disrupt legitimate users' access to the wireless network.

Mobile App

Reverse Engineering
Analyze the application's code to identify vulnerabilities and hidden functionality.

Insecure Data Storage
Test how the application stores sensitive data on the device and during transmission.

Insecure APIs
Evaluate the security of APIs used by the application to communicate with backend servers.

Inter-App Communication
Explore vulnerabilities arising from interaction with other apps on the device.

Man-in-the-Middle (MitM) Attacks
Intercept communication between the mobile app and the server to steal data.

Others

Client-Side Penetration Testing
Focus on vulnerabilities in user software (browsers, media players) for network access.

Social Engineering Penetration Testing
Evaluate susceptibility to phishing, pretexting, and other social engineering techniques

Physical Penetration Testing
Assess physical security measures and simulate physical attacks like tailgating and device theft.

[2] *TYPES OF PENETRATION TESTING: EXPLAINED IN DETAIL. SafeAeon Inc.* https://www.safeaeon.com/resources/infographics/types-of-penetration-testing/

Benefits of Pen Testing

REAL-WORLD SIMULATION
Simulates a cyberattack to assess your security measures.

COMPLIANCE WITH REGULATIONS
Maintains compliance to avoid legal and financial consequences

RISK MITIGATION
Enables effective prioritization and mitigation of potential cyber-risks.

CUSTOMER DATA PROTECTION
Addresses vulnerabilities that lead to breaches, identity theft or unauthorized access.

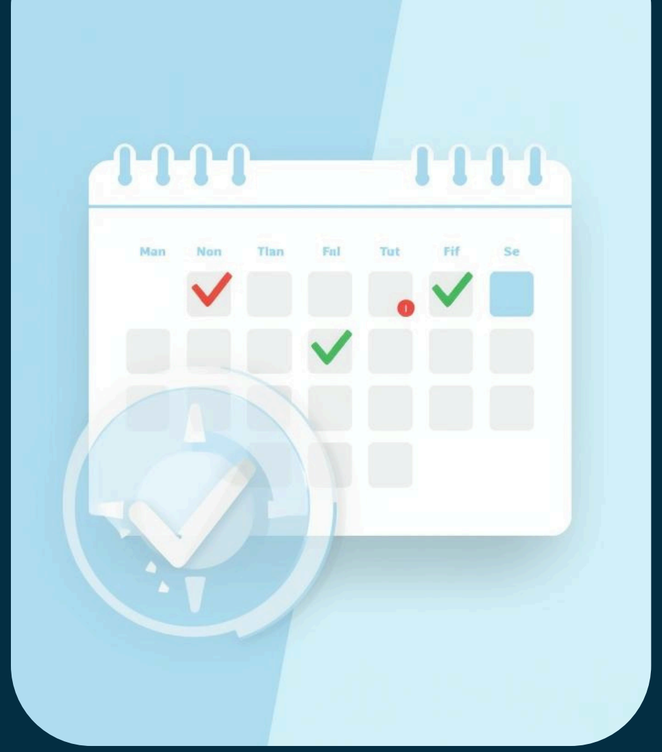
RISK PRIORITIZATION
Prioritizes vulnerabilities by degree of risk, addressing critical issues first.

VULNERABILITY IDENTIFICATION
Exposes security vulnerabilities to reveal potential entry points.

PROACTIVE OFFENSE
Proactively reduces attack surfaces through threat assessments.

THREAT DEFENSE
Identifies vulnerabilities missed by traditional security measures

COMPREHENSIVE SECURITY ASSESSMENT
Evaluates current security controls to ensure systems can withstand cyberthreats.



When to Conduct Pen Testing

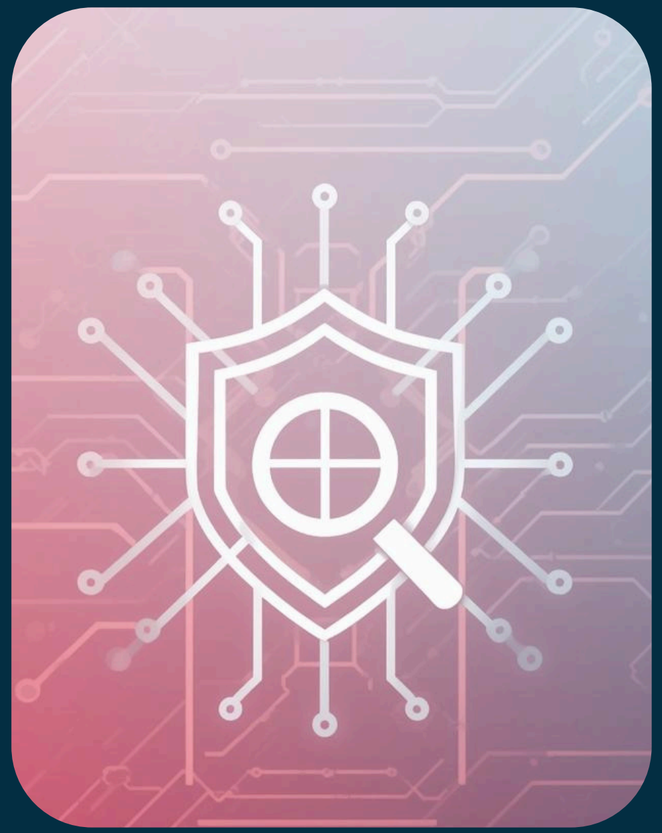
Right timing for penetration tests

Regularly conducting penetration tests is crucial for maintaining security. This proactive approach helps safeguard your systems and data from potential threats.

Penetration testing should be scheduled:

- 📅 Regularly (quarterly or annually)
- 📅 After major IT changes
- 📅 To meet compliance requirements and certifications
- 📅 Before launching new systems

FOTHION



Get Started with Pen Testing!

Unlock the potential of your cybersecurity strategy

Is Your Network Truly Secure?

🚀 Put it to the test with a professional Penetration Test

🗓️ Book a free consultation with Fothion today

👉 https://fothion.com/schedule-a-phone-call/

https://fothion.com

salesteam@fothion.com

(310) 598-7585

FOTHION