DATA SHEET

Penetration Testing

Can A Determined Attacker Gain Access to the Critical Assets You Cannot Afford to Have Compromised?

BENEFITS

- Know whether your critical assets are at risk
- Identify and mitigate complex security vulnerabilities before an attacker exploits them
- Understand how the most sophisticated attackers operate based on intelligence gained from our years performing incident response
- Attain realistic findings and comprehensive recommendations

Why Mandiant

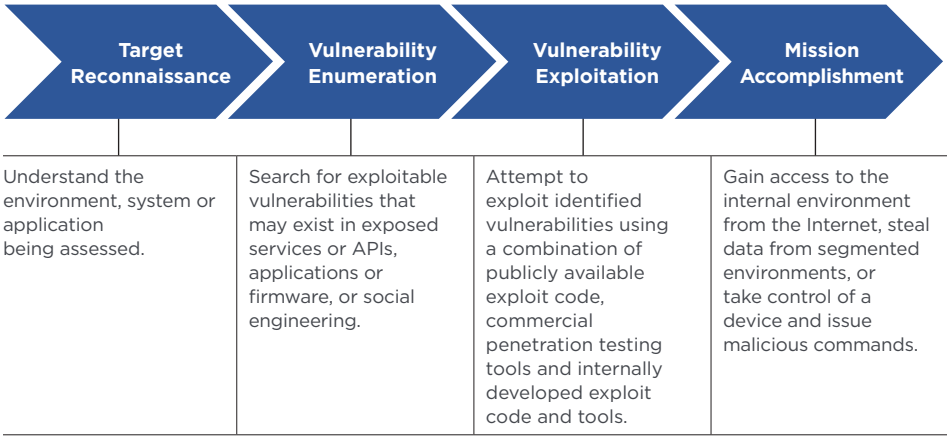
Mandiant, a FireEye company, has over 14 years of experience at the forefront of cyber security and cyber threat intelligence. Our incident responders have been on the frontlines of the world's most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tactics, techniques and procedures.

Our penetration tests leverage deep knowledge of advanced persistent threats (APTs) and attacker behavior, using the same tools, tactics and procedures (TTPs) we see every day during our incident response engagements.

Service Overview

Mandiant's penetration tests are custom-tailored to an organization's environment and needs, assessing specific aspects of the security program and the state of security of an organization's critical systems, networks and applications. We take advantage of the intelligence gained from our years of experience responding to the most sophisticated threat actors worldwide.

Approach



Assessments can be performed black box (starting the assessment with zero knowledge of the environment) or white box (starting with knowledge of the environment).

Table 1. Range of customizable penetration testing services

Penetration Test	Objective	Benefit
External Penetration Tests	Identify and exploit vulnerabilities on systems, services and applications exposed to the Internet	Understand risk to assets exposed to the Internet
Internal Penetration Tests	Simulate a malicious insider or an attacker that has gained access to an end-user system, including escalating privileges, installing custom-crafted malware or exfiltrating faux critical data	Understand risk to business from a breach
Web Application Assessments	Comprehensively assess web or mobile applications for vulnerabilities that can lead to unauthorized access or data exposure	Understand the security of applications that broker access to critical data
Mobile Device Assessments	Comprehensively assess the security of mobile devices and installed applications	Understand risk introduced to an organization through newly developed mobile applications or company-issued cell phones
Social Engineering	Assess the security awareness and general security controls with respect to human manipulation, including email, phone calls, media drops and physical access	Understand how an organization reacts to exploitation of human beings
Wireless Technology Assessments	Assess the security of your deployed wireless solution (e.g., 802.x, Bluetooth, Zigbee, etc.)	Understand how secure data in transit and systems communicating via wireless technology actually are
Embedded Device\ Internet of Things (IoT) Assessments	Assess the security of your device by attempting to exploit the embedded firmware, control the device by passing or injecting unsolicited malicious commands, or modify data sent from the device	Understand the security of devices and the ability to guarantee that the commands issued to and information received from the device are legitimate
ICS Penetration Tests	Combine penetration testing and exploitation experience with ICS expert knowledge to prove the extent an attacker can access, exploit or otherwise manipulate critical ICS/SCADA systems	Understand the vulnerabilities in an ICS environment before an attacker exploits them

WHAT YOU GET

- Summary for executive- and senior-level management
- Technical details that include enough information to recreate our findings
- Fact-based risk analysis sto confirm a critical finding is relevant to the targeted environment
- Tactical recommendations for immediate improvement
- Strategic recommendations for longer-term improvement

Suspect an incident? Email us at **investigations@mandiant.com** or visit **https://www.fireeye.com/company/incident-response.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™