COALFIRE LABS

DATASHEET

Penetration testing

EXPLOIT VULNERABILITIES TO PREVENT ATTACKS

By using sophisticated penetration tests, you can confidently secure your data and your customers' data from evolving threats and continuous attacks. While mandated by compliance requirements, pen tests are also the best way to prove you're prepared for a malicious attack and the most cost-effective method of simulating a real-life attack.

Implement security best practices and meet compliance needs with help from Coalfire Labs. Our certified experts use advanced tradecraft to identify and exploit vulnerabilities – including system and software configuration flaws, operational security lapses, and insufficient countermeasures – so you can understand how successful and unsuccessful breaches occur and strengthen your defenses.

TYPES OF PEN TESTS

- **Red team:** Tests all possible attack vectors – including people, processes, technology, and physical and logical assets – for all possible threats. Includes a dedicated response team.
- **Enterprise:** Tests possible attack vectors, but may exclude the attack surface, hours, or people. Does not include the response team.
- **Technology:** Only focuses on the technology.
- **External only:** Does not include internal testing on applications or the network. Wireless pen testing is optional.
- **Application or mobile:** Only focuses on application or mobile components.
- **Compliance:** Emulates a specific threat with the goal of meeting compliance requirements.

	Response team test	Social engineering	Physical testing	External threat attack	Internal threat attack	Compliance scope	Denial of service	Wireless penetration testing	Application penetration testing	Vulnerability scanning
Red team	●	●	●	●	●	●	○	●	●	●
Enterprise		○	○	●	●	●	○	●	●	●
Technology only				●	●	●	○	●	●	●
External only				●		●	○	○	●	●
Application or mobile only								○	●	●
Compliance only					○	●			○	●

BUSINESS THREATS EMULATED

PROACTIVE THREAT MANAGEMENT

REQUIRED COMPLIANCE

● Included in service ○ Optional in service

THINKING – AND ACTING – LIKE AN ATTACKER

The Coalfire Labs team has a proven record of finding exploitable vulnerabilities in a variety of environments. We design tests around your business and its challenges, and then deliver unbiased advice and actionable recommendations to help you address the gaps we found – before they are exploited.

DIGITAL FORENSICS – HELPING YOU RECOVER

In the unfortunate event your system has already been compromised, we provide digital forensics, litigation support, data recovery, evidence retrieval, and investigative analysis. Our forensic experts use industry-leading methodologies and tools to help you properly extract, preserve, and analyze data. We follow all legal custody procedures for admissible evidence and stand by its authenticity and legitimacy.

> *"Coalfire found vulnerabilities we needed to know about before they became a problem."*
>
> –LEVEL ONE MERCHANT CLIENT

Coalfire's penetration testers are certified.

GIAC CERTIFIED PENETRATION TESTER GPEN

OFFENSIVE security OSCP

OFFENSIVE security OSCE

> *"The Coalfire team kept us informed and up-to-date via status updates. We were never in the dark and were able to keep our potential customer apprised of everything. Not only did they beat the deadline, they advised avenues of improvement and remediation steps we should take to close any concerns... this satisfied customer sleeps well at night because of my partnership with Coalfire."*
>
> GENERAL COUNSEL AND CHIEF COMPLIANCE OFFICER, HEALTHCARE ORGANIZATION

DS_PenTesting_062217

ASSESS THE EFFECTIVENESS OF YOUR SECURITY PROGRAM. CONTACT COALFIRE LABS.

CoalfireLabs.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. **Coalfire.com**

Coalfire is solely responsible for the contents of this document as of the date of publication. The contents of this document are subject to change at any time based on revisions to the applicable regulations and standards (HIPAA, PCI DSS et.al). Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent us from doing so. Consequently, Coalfire is not responsible for any errors or omissions, or for the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. In order to maintain contextual accuracy of this document, all references to this document must explicitly reference the entirety of the document inclusive of the title and publication date; neither party will publish a press release referring to the other party or excerpting highlights from the document without prior written approval of the other party. If you have questions with regard to any legal or compliance matters referenced herein you should consult legal counsel, your security advisor and/or your relevant standard authority.