Purple Team Penetration Test

DATASHEET

Know Your Risks

Penetration Testing, also known as Red Team Testing, is an important part of your information security program. Our team of security experts, the "Red Team" or offense, performs a vulnerability scan of your network(s) and then attempts to manually exploit any found vulnerabilities. While offensive testing gives you essential information about your vulnerabilities, it does not determine if your internal security team, the "Blue Team" or defense, is able to detect these security incidents as they occur.

Beyond your standard penetration test, our Purple Team Test will not only identify steps that an attacker could take during a real-world attack, but also the effectiveness of your organization's response.

Not Just Identification

During the Red Team portion of testing, our analyst documents all scanning and exploited steps, including the date, time, tools used, and more. Using this information, we work with your Blue Team to determine what they were alerted to during testing. The Blue Team review can happen in conjunction with the Red Team testing, or after testing is complete.

At the end of the Purple Team Test, you will receive a comprehensive report that includes all findings identified during testing as well as actionable recommendations for improvement. We will provide recommendations for detection and security configuration improvements.

Frequently Asked Questions

What is the difference between vulnerability scanning and penetration testing?
Vulnerability scanning is an automated method that identifies vulnerabilities that may exist on an organization's network. Penetration testing is by nature more accurate than vulnerability scanning since it actually confirms that a suspected weakness is exploitable.

Will this hurt my network?
This is extremely unlikely. We do not attempt any denial-of-service attacks.

How much time will you need from our internal security team during the Blue Team review?
This very much depends on the size of your network infrastructure, and the size of your team. We typically scale these assessments based on the number of systems to be addressed. The more time available for collaboration with the Blue Team, the better.

How long does a Purple Team Penetration Test typically take?
This depends very much on the number of devices to be tested. A Purple Team Test can range from 8 hours to 24 hours of testing time, or more if requested by the client.

A Purple Team Pen Test Includes:

- Vulnerability scanning of network(s)
- Manual exploit testing of vulnerabilities
- Comparison of Red Team attacks with Blue Team alerts
- Verification of IDS/IPS systems
- Comprehensive report with recommendations for improvement.