Penetration Testing

CrossCountry Consulting

In a penetration test, the CrossCountry team forgoes stealth to find the greatest number of vulnerabilities possible. Typically, a penetration test is announced to the client's Security Operations Center, includes vulnerability scanning, and manual verification of detected vulnerabilities.

OUR OFFERINGS

Internal Penetration Test

Our team starts from the internal network to find as many vulnerabilities as possible, including internal web portals, web application vulnerabilities, and network vulnerabilities.

External Penetration Test

Beginning from outside the network, our team finds as many vulnerabilities as possible in internet-facing systems including web servers, VPNs, chat/ email, DNS, and videoconferencing systems.

Web Application Penetration Test

We test web applications for vulnerabilities including injection, privilege escalation, file inclusion, directory traversal, file upload, and many more. For more complete testing, clients may choose to provide test accounts with different privilege levels to use for the penetration test.

Wireless Penetration Test

We scan for rogue wireless access points and determine if they use strong encryption, and if they provide an attacker access to your internal network.

Physical Entry Test

Our team attempts to bypass physical security controls with techniques such as badge cloning, tailgating, burglary tools, and social engineering.

"Click Rate" Phishing Test

We send phishing emails to a large number of employees to measure click rate and assess vulnerability to phishing attacks. We then measure the effectiveness of security training and identify employees in need of additional training.

Contact Us: ERIC EAMES, *Advanced Cyber Risk Lead* • eeames@crosscountry-consulting.com