A Red Team Whitepaper

The Technical Security Assessment

Penetration Testing

A Penetration Test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user. Following the penetration test, the organization will have a much clearer understanding of the weak areas within the IT infrastructure, as well as how to shore up defenses to protect the organization from a costly, potentially devastating security breach. This thorough test provides answers to the questions raised by the vulnerability assessment, and is an invaluable component of a comprehensive technical security assessment.

The Red Team Engineering Technical Security Team is a recognized leader in both external, internal, and web application aspects of information security testing. At Red Team, we offer a range of security services and are able to create a customized solution to meet the unique and specific needs of your business. From periodic vulnerability assessments and full scale penetration tests to mitigation of threats including full data encryption, we can provide solutions that are customized for your organization.

Please visit redteamengineering.com to learn more.

RED TEAM
ENGINEERING INNOVATION

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • www.redteamengineering.com
T: 844.RTE.JV00 F: 844.783.5800 • info@redteamengineering.com

The Comprehensive Technical Security Assessment

The practice of technical security assessment has long been recognized as a standard best practice across all business and industry segments. It is a crucial component in a well-managed information and technology security strategy, and in today's fast-paced e-commerce society, it has become more important than ever.

A qualified technical security firm can provide your business or organization with a comprehensive technical security assessment to identify weaknesses and potential risks that could compromise the enterprise network and systems. This assessment should include the following security components: vulnerability assessment, web application assessment, and penetration testing.

A vulnerability assessment is the process of identifying, quantifying and prioritizing weaknesses and potential risks that could compromise the enterprise network and systems. These vulnerabilities may be caused by unpatched or obsolete software or poorly configured systems. A vulnerability assessment will provide insight into areas that are exploitable by both authorized users and attackers.

Today more than ever, businesses use web-based applications for sales, marketing, accounting and other applications. While these applications have many benefits, including the convenience of online accessibility and enhanced team collaboration; they can also expose an organization to vulnerabilities that could be leveraged to gain unauthorized access to network resources and sensitive data. An effective web application assessment allows for the discovery of vulnerabilities that exist in web-based applications, and provides strategies to protect the organization from breach.

Penetration Testing Demystified

A Penetration Test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user.

During a penetration test, the technical security firm is challenged with taking the position of an attacker to attempt a penetration via previously identified points of weakness. The potential entry points may have been identified either by the organization or through a previously completed vulnerability assessment. The penetration test will confirm the legitimacy of the potential weaknesses. If the attack is successful, the consultant will assess the impact an information security breach could

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • www.redteamengineering.com
T: 844.RTE.JV00 F: 844.783.5800 • info@redteamengineering.com

have on the organization, and will present the findings along with a detailed proposal for mitigation.

Internal vs. External Penetration Testing

When considering a penetration test, an organization must decide whether to conduct internal testing, external testing, or a combination of both.

An external penetration test is commonly referred to as "ethical hacking". The external pen test is performed from "outside" the organization, in a manner similar to the approach that would be used by an actual hacker. Having limited information regarding the network infrastructure, the ethical hacker will garner information from public web pages and attempt to break through any security vulnerabilities that might exist in the infrastructure.

Many threats come from within the organization's firewall - from employees or partners with access to privileged information. These threats, (while often not malicious in their intent,) can have the same damaging results as an external attack from a malevolent hacker. In an internal penetration test, the ethical hacker is given network authorization equivalent to that of an employee or guest user, and will conduct the penetration test from the vantage point of users within the organization's own network.

Results of the Penetration Test

Following the penetration test, the organization will have a much clearer understanding of the weak areas within the IT infrastructure, as well as how to shore up defenses to protect the organization from a costly, potentially devastating security breach. This thorough test provides answers to the questions raised by the vulnerability assessment, and is an invaluable component of a comprehensive technical security assessment.

Benefits of Effective Penetration Testing

Penetration Testing should be performed bi-annually as a part of a comprehensive technical security assessment. The benefits of this act of corporate due diligence include: protection of the organization's reputation; protection of data and assets; third party verification; cost justification; customer/client assurance; and validation of existing security measures. A comprehensive technical security assessment, which includes web application assessment and

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • www.redteamengineering.com
T: 844.RTE.JV00 F: 844.783.5800 • info@redteamengineering.com

vulnerability assessment in addition to penetration testing, will also help ensure legislative and regulatory mandates are met while risk exposure is reduced.

When to Perform Penetration Testing

Penetration Testing should be performed bi-annually as a part of a comprehensive technical security assessment. As changes in the network environment occur, the potential for new weaknesses develops. The testing schedule should be planned with your technology security firm around vulnerability assessments (quarterly) and web application assessments (at least bi-annually, or as new applications are added.)

How Red Team can help:

The Red Team is a recognized leader in both external, internal, and web application aspects of information security testing. At Red Team Engineering, we offer a range of security services and are able to create a customized solution to meet the unique and specific needs of your business. From periodic vulnerability assessments and penetration tests to mitigation practices including full data encryption, Red Team can provide solutions that are customized for your organization. Please visit www.redteamengineering.com to learn more.

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • www.redteamengineering.com
T: 844.RTE.JV00 F: 844.783.5800 • info@redteamengineering.com