A Red Team Whitepaper

Choosing the Right Security Assessment

Navigating the various types of Security Assessments and selecting an IT security service provider can be a daunting task; however, it does not have to be. Understanding the available services and defining your organization's needs at the beginning can help you get started on the right foot, which will ultimately save both time and money.

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

Choosing the Right Security Assessment

I. Know what types of services are available.

In order to choose the best security service for your needs, you should first be aware of some common industry terms surrounding security assessments.

Vulnerability Assessment

A periodic vulnerability assessment will help to ensure your system's integrity, and is a crucial component of a well-managed information and technology security strategy. The vulnerability assessment allows a technical security consultant to identify risks within your system in a manner that is non-intrusive. It is the simplest security assessment available, and in today's fast-paced e-commerce marketplace it has become more important than ever.

How does it work?

Vulnerability Assessment identifies, quantifies and prioritizes weaknesses and potential risks that could compromise your enterprise network and systems. The primary vulnerabilities uncovered in a vulnerability assessment can be categorized as unpatched or obsolete software, poorly configured systems, and missing or poorly configured security protocols.

Summary:

A Vulnerability Assessment is an unobtrusive way to obtain insight into areas that are potentially exploitable by both authorized users and attackers.

Penetration Test

During a penetration test, (commonly referred to as a pen test), organizations identify a domain or range of assets to be tested. A technical security consultant takes the position of a possible attacker, performing an actual attack or attempted penetration via the points of weakness identified by your organization or within in the vulnerability assessment (see above). If an attack is successful, the technical security consultant will examine the effects of the attack and assess the impact an information security breach could have on your organization.

How does it work?

Differing from the Vulnerability Assessment, a penetration test actually infiltrates the system. Identified vulnerabilities are penetrated, and then evaluated based on potential business impact if exploited. Findings are presented along with a detailed approach for mitigation.

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

Choosing the Right Security Assessment

Summary:
Taking the vulnerability assessment one step further, a penetration test is an invaluable component of a comprehensive technical security assessment. A Penetration Test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user. It confirms the legitimacy of potential weaknesses identified in the vulnerability assessment and quantifies potential business impact if exploited.

Web Application Test

Most businesses today employ web-based applications for sales, marketing, accounting and othervarious business functions. 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 or sensitive data. A Web Application Assessment allows for the discovery of vulnerabilities that exist in web-based applications and provides strategies to protect the organization against identified points of weakness.

How does it work?
There are two types of application testing designed to identify potential weaknesses in specific web applications. Web application vulnerability assessments and penetration tests are performed similarly to their non-application specific counterparts while they focus on discrete applications in order to analyze their security.

Summary:
Web application testing will allow an organization to determine the security level of its web-based applications. Upon completion of the assessment, the technical security consultant will recommend mitigation strategies to maximize your system integrity and security.

II. Consider your testing options.

When considering a Vulnerability Assessment, Penetration Test or Web Application Testing you will also want to determine whether to conduct internal testing, external testing, or a combination of both.

An external test is performed from outside, similar to the approach that would be taken by a hacker. Armed with minimal information such as targeted IP addresses or ranges, the "ethical hacker" will then obtain information from public web pages and hacker" will then obtain information from public web pages and attempt to break through any security vulnerabilities that might exist in your IT infrastructure.

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

Choosing the Right Security Assessment

An internal test is performed from the point of view of a possible inside threat. The tester will imitate someone inside the company, such as an employee or partner, and will be allowed to utilize privileged information that a specific employee/partner should be able to access under normal circumstances. From there the tester will determine whether an employee/partner can access priviledged information that they should typically not be allowed to see.

Many threats come from within the organization's firewall - from employees 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 test, the ethical hacker is given network authorization equivalent to that of an employee or guest user, and conducts the penetration or vulnerability test from the vantage point of users within your own network.

III. Determine testing type and frequency.

A comprehensive technical security assessment will include internal and external vulnerability assessments, penetration testing and web application testing. It will afford the organization the opportunity to:

- Protect its reputation
- Protect data & assets
- Protect against data breach
- Demonstrate third-party verification
- Execute corporate due diligence
- Ensure customer privacy
- Guarantee regulatory compliance
- Comply with legislative mandates
- Reduce risk exposure
- Validate existing security measures

It is up to your organization to determine what an acceptable level of risk may be, and what areas you want to ensure are safeguarded.

Internal or External?
If your most common threats are believed to be from the outside (as in most organizations), then an external test is going to be the most effective solution to meet your needs. Once a penetration is achieved, the tester can work from inside the network to find more weaknesses. If your greatest potential threat is from those who are inside your company, then the internal test may be the best place to begin.

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

Choosing the Right Security Assessment

When and how often?
Industry standards suggest that vulnerability assessments be performed quarterly, while network penetration tests should be performed at least bi-annually. Web application assessments should be performed at least annually and whenever new applications are added. Remember, each time you upgrade your system or your software, you open new portals for possible exploitation. To protect against new threats, you should consider running security assessments before and after any new software is introduced into your infrastructure.

Another important element to consider is timing.
Penetration Tests have the potential to cause interruptions for the daily work routine of your employees. Because of this, you must balance security with convenience. An important factor to consider is whether or not the assessment will hinder your employees, your network, or your infrastructure. Testing has the potential to disrupt normal network operations if the tester is successful. Therefore, it is important to know what protocol the security firm has in place in case the network is compromised. Every information security firm should provide your organization with "rules of engagement" to mitigate the possibility of network interruptions and eliminate any surprises. If you require a less obtrusive method, then a vulnerability assessment may be the best solution for you. However, if your company requires that you actually test these threats and you need a higher level of confidence in your security posture, then a penetration test is the best approach for your company.

IV. Overview

The following service comparison chart can serve as a good starting point for most organizations in understanding the various types of security assessments and the recommended frequency with which each should be performed:

Service Comparison | Red Team Engineering Technical Security Offerings

	Technical Security Assessment	Web Application Assessment	Vulnerability Assessment	Network Penetration Test
Protect Corporate Reputation	●	●	●	●
Third Party Verification	●	●	●	●
Protect Data & Assets	●	●	●	●
Data Breach Protection	●	●	●	●
Corporate Due Diligence	●	◑	●	●
Cost Justification	●	◑	●	●
Customer Assurance	●	●	◑	●
Compliance	●	●	●	◑
Legislative Mandates	●	●	●	
Reduce Risk Exposure	●	●	●	
Validate Existing Security Measures	●		●	●
Regulatory	●	●		
Recommended Frequency		at least annually *and as new applications added*	quarterly	bi-annually

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