RedTeam
SECURITY CONSULTING

RedTeam Security Testing Guide

AN OVERVIEW OF OUR OFFENSIVE SECURITY SERVICES
AND BEST PRACTICES FOR YOUR ORGANIZATION

Re:

RedTeam Security
redteamsecure.com
sales@redteamsecure.com
twitter.com/redteamsecure

214 4th Street E., #140
St. Paul, MN 55101

Table of Contents

© Copyright 2018 RedTeam Security Corporation. All rights reserved.

Who We Are

We educate. We identify. We inform. We help reduce your attack surface.

The statement above has become a bit of a motto here at RedTeam, and it's one we live by in every engagement. We serve our clients with an 'education first' mentality. After all, what good is an in-depth vulnerability report if you have no idea what anything inside it means? We take the fright factor out of information security, helping you first to understand, then helping you to reduce your threat level.

We're experts in offensive security; it's the only thing we do, not one of 100 other services like some larger firms. With RedTeam Security you can expect a boutique experience with individualized attention and near-constant communication during our engagement.

What Are Red Team Operations?

A red team operation is a multi-faceted attack simulation that identifies vulnerabilities in your technology, people and infrastructure. It's as close as you can get to a real-world attack and tests how well your organization would fare if challenged by a malicious party.

A thorough red team operation will test and expose vulnerabilities in a multitude of areas. Here are just a few:

- Technology. Your networks, applications, routers, switches, appliances, etc.
- People. Your staff, independent contractors, vendors, departments, business partners, etc.
- Physical. Your offices, buildings, warehouses, substations, data centers, etc.

A well-executed red team operation is never a cookie-cutter approach. It's customized based on your organization's size, scope, industry, regulatory requirements and other unique security challenges. This is why any organization can benefit from red teaming.

The cost of the average security breach is a whopping $7.35 million. The best defense is a good offense!

© Copyright 2018 RedTeam Security Corporation. All rights reserved.

Our Services

At RedTeam, we focus solely on offensive security. Our services include:

- Red Team Operations
- Network Penetration Testing
- Application Penetration Testing
- Physical Penetration Testing
- Social Engineering

We also offer our exclusive RedTeam Training sessions several times per year, giving small groups of students hands-on training that's not available anywhere else.

Network Penetration Testing

A network penetration test identifies an organization's network security weaknesses the same way an attacker would: by hacking it. The goal is to help you better understand and ultimately minimize the risk associated with your IT assets.

Network penetration testing can take two forms: internal and external. As its name suggests, internal network penetration testing focuses on internal systems while external network penetration testing focuses on public-facing systems.

Our network penetration testing is conducted using globally accepted, industry standard frameworks which cover the following:

- Passwords
- Switches
- Routers
- Firewalls
- Servers
- VPN
- AV
- IDS/IPS

These frameworks are based on the Penetration Testing Execution Standard (PTES) and the Information Systems Security Assessment Framework (ISSAF) and ensure a sound, comprehensive network penetration test.

Application Penetration Testing

Web applications are particularly vulnerable to external attacks because they're inherently designed to be accessible to the Internet. Application penetration testing combines manual testing with the results from industry-leading scanning tools to enumerate and validate vulnerabilities, configuration errors, and business logic flaws.

Manual testing is key here because it enables us to find what scanners cannot find. Application penetration testing helps you lower your risk of a data breach, improve productivity, protect your brand, and maximize the ROI from your web applications.

RedTeam's comprehensive approach to application penetration testing covers the classes of vulnerabilities outlined in the Open Web Application Security Project (OWASP):

- Injection (i.e.: SQL injection)
- Broken Authentication and Session Management
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring
- And More

A well-executed application penetration test will reveal real-world opportunities for hackers to compromise applications in such a way that allows for unauthorized access to sensitive data or even takeover of systems for malicious/non-business purposes.

© Copyright 2018 RedTeam Security Corporation. All rights reserved.

Physical Penetration Testing

The primary goal for a physical security operation is to measure the strength of existing physical security controls and uncover their weaknesses before bad actors are able to discover and exploit them.

Physical penetration testing, or physical intrusion testing, will reveal real-world opportunities for bad actors to compromise physical barriers in such a way that allows for unauthorized physical access to sensitive areas, which could result in data breaches and system/network compromise.

Physical penetration testing covers:

- Doors and locks
- Sensors and cameras
- Security guards
- Physical barriers
- Biometrics
- Situational awareness
- And more

RedTeam's physical penetration testers have experience infiltrating some of the most secure environments the same way bad guys would. They leverage this experience to zero in on critical issues and provide actionable remediation guidance.

© Copyright 2018 RedTeam Security Corporation. All rights reserved.

Social Engineering Testing

Your people are your greatest asset, but they can also be one of the most dangerous when it comes to your security. Social engineering testing from RedTeam Security allows organizations to simulate real-world attack scenarios in an effort to identify security awareness and personnel gaps without the devastating consequences of an actual social engineering attack.

Social engineering testing covers employees, executives, vendors, stakeholders and more and may consist of the following:

- Email phishing
- Spearphishing
- Telephone vishing
- Onsite pretexting
- Spoofing
- Identity impersonation
- And more

Social engineering testing provides companies highly valuable information about the security posture and security awareness levels of your employees. It's a crucial component to measuring your overall security posture and helps pinpoint where security gaps need to be filled and where budgetary dollars should be directed.

© Copyright 2018 RedTeam Security Corporation. All rights reserved.

Elements Of A Red Team Strategy

An effective red team strategy isn't a one-size-fits-all approach. It should be customized to your organization and take into consideration several factors, including your industry, size, and organization-specific risks.

The work doesn't end with a single red team operation. Offensive security is an ongoing battle, so regular testing is key to maintaining a strong security posture.

Best Practices

For the best possible chance of preventing an attack, follow these security best practices:

- Have written security policies and procedures
- Train your workforce on security procedures and best practices
- Require multi-factor authentication
- Never use default passwords
- Mandate security patch updates
- Perform regular backups
- Use reputable services and vendors
- Encrypt sensitive data
- Stay up-to-date with compliance standards like HIPAA, NERC, PCI, NIST and FDIC
- Conduct regular penetration testing

We've said it before and we'll say it again: the best defense is good offense.

Take The Next Step

Ready to improve your security posture with the help of RedTeam Security?

- **Schedule a consultation** to chat one-on-one about your unique security needs and get your questions answered.
- If you're ready for us to prepare a proposal, **fill out our scoping questionnaire** and give us a bit of background information to get started.
- Browse the many resources available on **the RedTeam blog**.

© Copyright 2018 RedTeam Security Corporation. All rights reserved.