Service Brief

Penetration Testing Services

Proven to work for you

The best way to know how intruders will actually approach your network is to simulate a real-world attack under controlled conditions. This allows you to pinpoint actual risks posed to your company from the perspective of a motivated attacker. Rapid7's Penetration Testing Services team delivers network, application, wireless, social engineering, and boutique engagements to demonstrate the security level of your organization's key systems and infrastructure. Powered by the #1 penetration testing framework, Metasploit, our pen testing team conducts almost 1,000 tests per year.

1,000

Rapid7 penetration testers are renowned experts who conduct almost 1,000 penetration tests per year and are frequently asked to present at leading industry conferences including Black Hat and Defcon.

We're more than security experts

Many security firms hire recent college grads or people with more IT than security experience to do their penetration tests, especially the early phases. Rapid7's penetration testers, on the other hand, aren't just security experts – they're bonafied hackers. All of our penetration testers are also security researchers, devoting 25% of their time to conducting research in such topics as ATM hacking, multi-function printer exploitation, automobile keyless entry attacks, endpoint protection bypass techniques, RFID cloning, security alarm system bypass, and more. Their research has been featured in dozens of news articles and has been presented at over 30 conferences a year.

In addition, Rapid7's penetration testers are active in the community, developing and releasing open source testing tools and writing popular Metasploit modules. Because we own Metasploit, we give our pen testers unparalleled access to the most widely used penetration testing tool in the world.

In the past year, our pen testing team has:

- **Released over six advisories for 0-days**
- **Created open source testing tools:** Serpico, apt2, myBFF, backHack, praedasploit, Boscloner RFID cloning
- **Presented at industry conferences:** Blackhat, Defcon, Bsides Las Vegas, Bsides Boston, HOPE, TakeDownCon, SANS Baltimore, Bsides Baltimore, Bsides Knoxville, Bsides Columbus, BruCon, ISSA Las Vegas, ISSA Phoenix, Toorcon, DerbyCon, Hack in Paris, United Summit, Sector Toronto, Ohio Information Security Forum, The Hackers Conference, 8dot8
- **Conducted and provided insight into newsworthy research:**

  The Washington Times: "Researchers reveal flaw affecting Comcast's Xfinity Home Security system"

  Network World: "Rapid7 disclosed 6 XSS and SQLi flaws in 4 Network Management Systems, 2 unpatched"

072616

> “Rapid7 had great expertise. When you hire a person – or a group of individuals – to do a job like this, you want someone who has done extensive penetration testing, who eats, sleeps, and breathes security, who can think like a hacker.”
>
> *-Jaya Ayyagari*
> *VP of Software Development, EyeLock Corporation*

Methodology and reporting: prioritized and actionable

Many penetration tests will give you a big list of problems with little context on how to fix things or what to prioritize. Rapid7 presents you with a prioritized list by using the DREAD methodology, looking at the damage potential, reproducibility, exploitability, number of affected users, and discoverability of each finding. You will get a detailed description and proof of concept for each finding, as well as actionable remediation guidance and reference. Because Rapid7 understands that the risk severity is only one factor in prioritizing remediation efforts, you will also gain insight into the level of effort needed to remediate the findings. In addition, you will also receive:

- An attack storyboard that walks you through sophisticated chained attacks
- Scorecards that compare your environment with best practices from an attacker’s perspective
- Positive findings that call out what security controls you have that are effective

Compliance is a by-product of good security

Rapid7’s philosophy is that meeting compliance is a by-product of good security. From our investment and commitment in Metasploit to our new attacker analytics products, we focus on helping you understand attackers and how to defend against them. This extends to our penetration testing services; every company’s network and challenges are unique, so our penetration testers tailor their methods and attack vectors for each engagement. We also conduct penetration tests on our own network and products regularly, to ensure they’re always up-to-date in detecting real world attacks. The whole point of a penetration test is to simulate what a real world attacker would be able to do to your environment – and to do that you need the most experienced team using the world’s number one solution.

MENU OF SERVICES:

Rapid7 offers a range of penetration testing services to meet your needs. We also offer custom solutions, so be sure to contact us to learn how we can help your organization.

- **Network Penetration Testing – External or Internal**
  We simulate real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to your network infrastructure.
- **Wireless Network Penetration Testing**
  We leverage the Open Source Security Testing Methodology Manual (OSSTMM) and the Penetration Testing Execution Standard (PTES) as a foundation for our wireless assessment methodology, which simulates real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to your wireless network infrastructure.
- **Web Application Penetration Testing**
  In addition to the Open Source Security Testing Methodology Manual (OSSTMM) and the Penetration Testing Execution Standard (PTES) Rapid7’s application penetration testing service leverages the Open Web Application Security Project (OWASP), a comprehensive framework for assessing the security of web-based applications, as a foundation for our web application assessment methodology.
- **Mobile Application Penetration Testing**
  We leverage the Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM), and Penetration Testing Execution Standard (PTES) methodologies to thoroughly assess the security of mobile applications. As the widespread use of mobile applications continues to grow, consumers and corporations find themselves facing the new threats around privacy, insecure application integration, and device theft. We go beyond looking at API and web vulnerabilities to examine the risk of the application on a mobile platform.
- **Physical Device Penetration Testing**
  Physical devices span the range from the ubiquitous Internet of Things (IoT) to mission critical Industrial Control Systems (ICS). Our physical device testing will assess communication channels, user interfaces, power consumption, and firmware for vulnerabilities that may pose a threat to the consumer or vendor. Our deep dive manual testing not only looks for known vulnerabilities, but will often reveal previously undiscovered findings.
- **Social Engineering Penetration Testing**
  Malicious users are often more successful at breaching a network infrastructure through social engineering than through traditional network/application exploitation. To help you prepare for this type of strike, we use a combination human and electronic methodologies to simulate attacks. Human-based attacks consist of impersonating a trusted individual in an attempt to gain information and/or access to information or the client infrastructure. Electronic-based attacks consists of using complex phishing attacks crafted with specific organizational goals and rigor in mind. Rapid7 will customize a methodology and attack plan for your organization.

Learn more or request a proposal:
www.rapid7.com/penetration-testing