RED TEAM ENGAGEMENT

Assessments for Mature Security Teams

While penetration testing aims to identify and exploit vulnerabilities in a defined scope such as a web application – a Red Team engagement focuses on compromising predetermined assets or 'flags'. By remaining agnostic to a explicitly fixed target scope and focusing on potential impact, our Red Team Cybersecurity Engagement can demonstrate the risk posed by an APT (Advanced Persistent Threat). These comprehensive, complex security assessments are best used by companies looking to improve a maturing security organization.

A leader in these sophisticated campaigns, Rhino Security Labs has developed a world-class team of offensive security engineers and researchers. Including some of the foremost experts in the field, our team is comprised of specialists in a wide range of technologies and backed with the research to prove it. From building hardware implants to developing dozens of zeroday vulnerabilities, we have the experience and expertise to exercise the most hardened organization.

By harnessing this unique combination of attack capabilities, we can determine:

- Attack process to compromising your critical business assets
- Where vulnerabilities exist in your network, applications, IoT devices, and personnel
- Effectiveness of your security monitoring and alerting capabilities
- Weaknesses in your incident response policy and procedures
- Priorities and demonstrated impact for your future security initiatives

From building hardware implants to developing dozens of zeroday vulnerabilities, we have the experience and expertise to exercise the most hardened organization.

GOAL FOCUSED. IMPACT PROVEN

Each Red Team engagement targets a series of specific ‘Flags’ – critical business assets such as domain controllers, proprietary data, or credit card data. These Flags are determined on a per client basis to create a customized engagement and distinctively defined scope for the duration of the project. We understand that your security concerns are distinct to your organizational processes and industry. A red team engagement – or any security assessment for that matter – should always take that into consideration.

Flag Example – SaaS Company

One such example is a Software as a Service (SaaS) company. Some of the flags were common across enterprises - email servers, executive devices, and domain controllers. However through our process, we were able to identify unique flags to their business.

Application availability was central to this company’s success, so gaining control over the main web application became a worthwhile target. Sensitive user data was another, so access to the user database (or other stores) became an additional flag. By targeting these unique data points, Rhino Security Labs demonstrated tangible business risks – and how to mitigate them.

CUSTOM SCENARIOS FOR UNIQUE THREATS

Red Team engagements include custom scenarios that simulate real-world tactics an external attacker might use to gain a foothold within a network. These scenarios identify risks unique to a single scenario or environment, such as a malicious insider, a compromised mobile device, malicious hardware installation, or other unique threats.

Custom Scenario Example – Compromised Vendor

One popular scenario model is a compromised third-party vendor, where the attacker has obtained VPN or other privileged access to the corporate network. By starting the engagement with similar permissions, clients receive realistic insights into how escalation would occur – and where monitoring and response capabilities should be improved.

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.