Red Teaming

Each organization has its own unique combination of needs, policies and tolerances that impact the way security assessments are conducted. This is especially true of Red Team penetration testing, which often involves some sort of disruptive or intrusive activity. Casaba not only knows how to identify and exploit potential vulnerabilities to gain access, we know how to customize our approach to best suit each client's IT and business environments, and make sure your blue teams are tested.

Are you ready for an attack?

Assess overall security posture

Casaba can employ the full range of tactics in the hacker's toolbox to determine if and how an attacker can break in and compromise a network or access specific assets such as trade secrets or source code.

Evaluate ability to detect an attack

Would anyone notice if someone tried to break in? If so, what would it take to set off the alarm? Companies call us to test the integrity of their detection, monitoring and incident response mechanisms. This is where Casaba's ability to adopt different attack styles provides valuable insight into a client's level of awareness and resilience in various situations.

Simulate a Breach or APT

If an attacker has already gained access and set up shop on a network, he or she can stay there for weeks or months, possibly gathering assets or spying on the company and its people. By emulating this behavior, Casaba conducts the same type of stealthy activities to see whether a client can detect our presence and respond effectively. We can also apply this approach to run a counter-intelligence operation to find out who it is and what they're up to.

Application Penetration Testing

Your applications are also important to understanding your security posture. Web and mobile applications should be considered 'in scope' for attack as they would be fair game for any real-world scenario. Depending on our level of engagement, Casaba can give you a clear picture regarding the integrity of your:

- User Interface
- Authentication
- Authorization
- Session Management
- Input Validation and Sanitation
- Information Disclosure
- Integrity
- Transport and Protocol Security
- Business Logic
- Stability and Availability

The Casaba Approach and Process

Red team operations come in all shapes and sizes. In order to most effectively identify weaknesses we work with each client to adjust the parameters and variables for the best results. For example, we can make a lot of noise or sneak in like ninjas; we can work as a known entity or "go dark" and run a covert operation; we can work in the role of internal or external threat. In any case, the goal of red team should be to test your 'blue team' capabilities to see if our attacks and movements can be detected or at the least can be investigated during a post-mortem.

Whatever the engagement actually looks like, our core process consists of several important aspects:

Reconnaissance

We begin by gathering as much information as possible about the "target," which could be your network, applications, or even personnel, in much the same way that a would-be attacker might "case the joint."

Infrastructure / Application Hacking

We look for vulnerabilities to exploit in the network, via routers and servers, or in the application layer through reverse engineering, fuzzing, Denial of Service (DoS) and other attacks.

Social Engineering

The human factor should not be underestimated. We can explore and exploit vulnerabilities that may exist among personnel, including email, social media and other avenues through which a potential attacker could gather potentially harmful information.

Report & Recommendations

At the conclusion of testing, Casaba provides a custom written report documenting the project's objectives, process and detailed tactical findings. We can also deliver the report as a presentation to the management team. If desired, Casaba can be hired to provide a range of remediation services to definitively resolve any or all of the issues discovered.

About Casaba

Casaba is a strongly integrated team of security pioneers with a reputation for relentlessly researching, developing, and implementing innovative solutions to the most difficult security problems. We are prepared to assist in every phase of security consulting and auditing, and we are fully bonded and insured by Lloyds of London.

Get Started

Contact us today for a free consultation and security review:

- Phone: 1-888-869-6708
- Email: info@casaba.com
- Web: www.casaba.com

casaba