Redpoint
Cybersecurity LLC

PENETRATION TESTING ("PenTesting")

Redpoint Cyber delivers a unique human-led, automated penetration testing platform that improves the way organizations assess their cyber security risk. Backed by nation-state experienced professionals, Redpoint is able to deliver one of the most sophisticated and cost-effective PenTests on the market.

Having a continuously updated platform that mimics the hacker's perspective, Redpoint engineers identify, analyze and prioritize remediation of cyber defense vulnerabilities. Our clients can engage Redpoint to perform continuous, machine-based PenTests to improve their organization's immunity against cyber attacks across their networks.

TOOLS & TECHNIQUES

Software PenTest:

- Extremely fast and thorough
- Continuously testing and identifying vulnerabilities and exploits not found by a human ethical hacker

MITRE ATT&CK®:

- The PenTest follows the MITRE ATT&CK® Matrix, exploiting the network to the fullest extent possible to mimic a malicious actor

What is MITRE ATT&CK for Enterprise?

A framework and knowledge base of adversary tactics and techniques based on real world observations. Redpoint engineers use the framework and technology to ethically hack using the same techniques that actual bad actors use regularly.

THE CHALLENGE

As hackers increase their sophistication, corporate security officers and regulators have begun proactively defending their networks by integrating tactics, techniques, and procedures (TTPs) from the very actors they are warding off in a revamped cyber defense strategy.

Professional services-based PenTesting, as we know it today, is time consuming, intrusive and costly. Further, this type of testing represents a point-in-time snapshot, and cannot comply with the need for continuous security validation within a dynamic IT environment.

THE SOLUTION

Redpoint Cyber is able to automate and deploy tests worldwide to ensure its clients receive continuous compliance and immediate visibility into the network enterprise while they maintain full control of their operational environment.

Focused on the inside threat, Redpoint mimics the hacker's attack, automating the discovery of vulnerabilities and performing ethical exploits while ensuring an undisrupted network operation. Curated reports are produced along with proposed remediation presented in a Wiki-format, keeping organizations one step ahead of tomorrow's malicious hacker.

MACHINE-BASED PENTEST VS HUMAN-BASED PENTEST

A global shortage of cyber security professionals, coupled with an increase in cyber threat sophistication, has driven the need for more advanced automated penetration testing software. At Redpoint, we believe the best results come from a **human-led, technology-enabled solution**. In the past (and currently still offered by many other firms), the traditional human-only PenTest was a labor intensive effort that might not have changed from test to test. By using constantly updated software that mimics the most current attack methodologies, we can achieve much **more realistic results** in a **more efficient manner**, in terms of time and cost.

OUR PLATFORM

An **automated PenTesting platform** is locally installed on your network, effectively **securing your vulnerabilities from the internet and the outside world**. The software requires standard hardware and installation takes only a few hours.

Upon completion of the installation, **the entire network functionality** is accessible to Redpoint engineers in any environment. Redpoint ensures **full transparency** during the connecting, testing and disconnecting phases and the client has access to its data from inception to the backend disconnection.

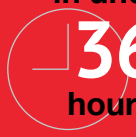
CLIENT SUCCESS

A global organization faced a large-scale ransomware attack. We provided emergency response combined with remediation and rebuild services.

Following the rebuild we performed a PenTest to identify vulnerabilities on the network,

testing
196
endpoints

with over
12,757
exploits leveraged against the network



in under
36
hours.

An in-depth report highlighted vulnerabilities and attack vectors and provided insight to support a holistic cyber security approach. This roadmap for improved cyber hygiene was critical to the organization's forward-looking initiatives to improve security and compliance.

TAB BRADSHAW

tab@redpointcyber.com
Chief Operating Officer
Redpoint Cybersecurity
www.redpointcyber.com