Test Your Network Before Hackers Test It For You

Continuous Validation Reduces Risk and Delivers the Confidence You Need

Numerous studies about network breaches over the last 10 years have proven one thing for sure — your network will be tested for weakness by a hacker at some point in time. According to Statista, in 2018 there were 31,107 cyber security incidents launched against federal United States agencies. Therefore, either you test your network first or they will test it for you. It's your choice, but the legal, political, and financial consequences should be far less devastating if you test your own defenses.

Breach and attack simulation (BAS) solutions solve the testing problem by giving you metrics and instrumentation that enable you to objectively measure the effectiveness of your security tools and assess the real value of your security solution spending. However, the right BAS solution choice will dictate how easy, or how hard, it is to test your agency's production network.

Breach and Attack Simulation Solutions That Work

There are two fundamental categories of network testing solutions. The first is pre-deployment testing. Pre-deployment testing is primarily responsible for informing you about how to dimension components and predict a realistic hardware and programming cost. This activity allows you to significantly reduce the risk and expense of deployment for new security architecture components in the vendor selection phase. The solution is to use a special purpose tester in a lab environment to accurately categorize the performance of all components in a real-world scenario. These testers generate different types of application data (voice, video, data) to load down a device under test so you can thoroughly understand how the device performs in real-world situations.

Here are some example use cases for this type of activity:

1. Audit critical network security equipment in a lab against current attacks (DDoS, testing exploits, and malware) to accurately understand how your proposed security architecture components will perform and dimension the amount of equipment needed.
2. Remove risk and expense of deployment for new security architecture components in the vendor selection phase by validating performance.
3. Perform an independent analysis of security equipment performance that can be used to ask for purchase discounts during the purchasing process, assuming that the real-world performance is far less than the manufacturer's stated throughput.

4. Perform SLA verification of vendor-provided equipment and networks.
5. Conduct encryption efficacy testing and cloud security posture testing to predict live performance.

The second useful type of network testing focuses on the production network. In order to measure security effectiveness, security operations center (SOC) engineers and administrators need operational insights into the effectiveness of their security posture and actionable intelligence to improve it. This type of testing ensures base level control system security using regular, comprehensive, and safe BAS assessments of the production network that provide innovative security solutions to enhance threat identification activities.

Here are some example use cases for this type of activity:

1. Perform continuous security monitoring and testing of live networks to check for security threats using a BAS solution.
2. Routinely test the network after new configuration changes for configuration-created vulnerabilities.
3. Model the way an aggressor nation state hacks networks and exploits vulnerabilities to learn how to defeat them.
4. Reduce latency and risk by using computer analysis to formulate correct conclusions and recommendations to fix problems, display that information on a dashboard, and then transmit that information to a SIEM.

How to Test The Security of Your Network

To implement use cases relevant to government agencies, Keysight Technologies offers an easy to use, yet powerful set of security testing solutions that include:

- Keysight's BreakingPoint is a lab-based solution that enables security engineers to test the security posture of their networks with real applications and a complete range of threat vectors. For instance, BreakingPoint simulates real-world legitimate traffic, distributed denial of service (DDoS) attacks, exploits, malware, and fuzzing to validate an organization's security infrastructure, reduce the risk of network degradation by almost 80%, and increase attack readiness by nearly 70%.
- Keysight's Threat Simulator is a BAS solution that performs continuous tests of your live network cyber security defenses, WAF, and web policy engines to identify any vulnerabilities. Once identified, a patented Recommendation Engine provides detailed easy-to-follow instructions on how to optimally configure your security products to close those gaps and improving your security. These recommendations can also be integrated directly to your SIEM.

Reach out to Keysight Technologies and they will show you how to test your network against multiple threat vectors.

Learn more at: https://getnetworkvisibility.com/industry/government/

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/