Interested in learning more about security?

SANS Institute InfoSec Reading Room

Security Testing and Vendor Selection with BreakingPoint

In this product review conducted by SANS instructor Serge Borso, we learned that BreakingPoint is more than just a network testing tool. BreakingPoint provides a unique solution that enables security assessment, vendor selection and change management. It integrates well and is easy to use. We believe the tool has great value to the security community and specifically larger enterprises in the midst of infrastructure updates and those optimizing information security programs.

SANS

A SANS Product Review

Security Testing and Vendor Selection with BreakingPoint

Written by **Serge Borso**

May 2018

Sponsored by:
Ixia, a Keysight Business

Introduction

In this product review, we explored a unique enterprise traffic simulation tool that helps networking teams ensure their equipment is prime-time ready, helps security teams simulate adversarial attacks, complements a mature change management process and provides leadership teams with the information they need to make informed decisions.

Ixia's BreakingPoint is a multifaceted tool that provides actionable data for network security testing and infrastructure validation. BreakingPoint works by simulating traffic aimed at your network appliances and applications. This traffic ranges from legitimate to malware to DDoS attacks. Because BreakingPoint initiates the flow of traffic, security teams can measure network saturation and endpoint responsiveness under extreme load.

Having the ability to thoroughly test equipment during a proof-of-concept (PoC) phase or understanding how an environment handles DoS attacks is a boon to enterprise decision makers. This review will delve into how Ixia BreakingPoint works and look at some solid use cases, as well as some unique and complementary scenarios in which the tool could offer unexpected wins for your enterprise.

Setting Up BreakingPoint

BreakingPoint is available as both a physical and virtual appliance, with the virtual solution supported on both public and private clouds. In our testing, we used the virtual and physical appliances in an on-prem business environment.

The Physical Appliance

BreakingPoint is an enterprise solution, and we quickly learned that a home lab was not sufficient to test this tool mainly due to the fiber requirements of the appliance coupled with 40G throughput. Specifically, Ixia's PerfectStorm 40GE2NG BreakingPoint appliance has one Ethernet management port and two QSFP (fiber optic) ports for traffic flows. We rectified this situation with the acquisition of several new hardware devices—including a 20Gbps throughput Next-Generation Firewall (NGFW), an enterprise switch and a small business switch with built-in IPS capabilities—and started testing in a business environment with fiber cabling. In addition to the newly acquired hardware, we used networking devices supporting SFP and QSFP connections. (BreakingPoint also has 1Gbps and 10Gbps copper/fiber options, as well as 100Gbps QSFP28.)

To administer and interact with the physical or virtual BreakingPoint appliance, we used the web interface, which allows users to access, manage and configure the tool. Integration with a DevOps Continuous Integration (CI)/ Continuous Deployment (CD) pipeline can be handled via the REST API and tweaked via the scripting options built into the device. We will share a bit more on this later.

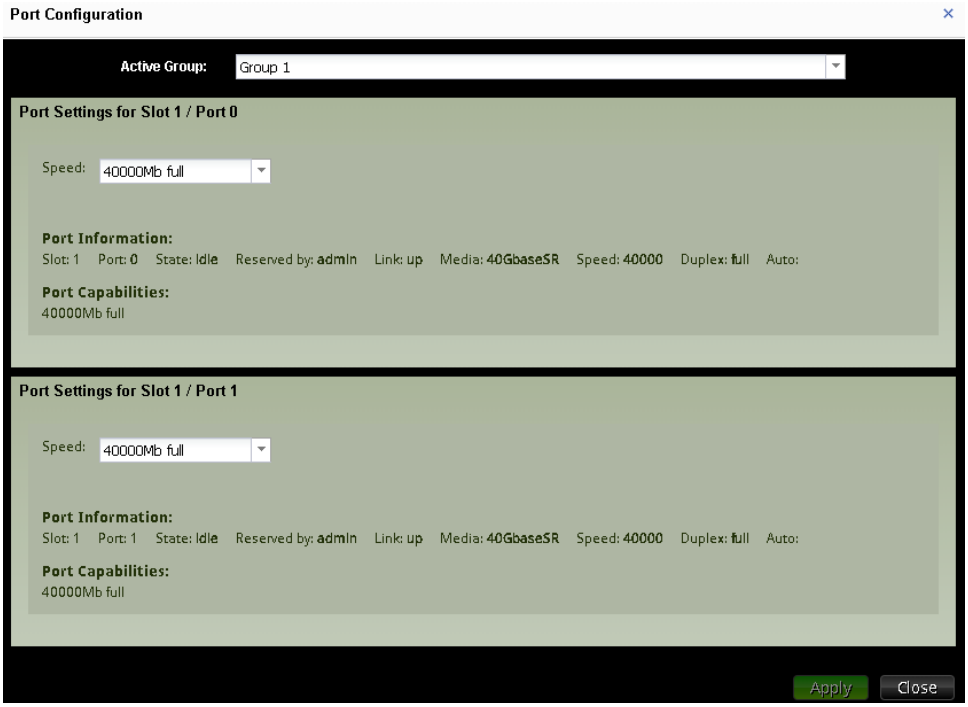


Figure 1. Attending to Port Configuration

Our initial setup took a fair amount of effort to ensure proper port mapping, active group configuration and logical positioning so the device under test (DUT) could talk to the BreakingPoint tool and our subsequent tests were successful. We needed to use care in configuring the networking architecture when applying new groups or target devices/ networks to test. This is relevant not only for configuring applicable throughput (given your target devices), but also for ensuring proper traffic routing. See Figure 1.

The Virtual Appliance

BreakingPoint is available as either a physical hardware appliance or a VM/cloud offering. The capabilities of each seemed comparable, and the main difference was the administration of the chassis.

The virtual appliance consists of two OVA files: a virtual blade and a virtual controller. We deployed the virtual appliance using VMware ESXi and proceeded to configure the virtual blades. This was a critical part of the setup process because testing could not continue without this basic connectivity and configuration of the networking interfaces.

We had questions about using the tool in a cloud hosting environment, as even a virtual private cloud (VPC) has restrictions on acceptable use and 40G of traffic is on par with some of the more aggressive DDoS attacks recently seen. Different cloud hosting providers require customers to complete specific authorization forms to perform penetration testing, but DoS is not typically encouraged. With this in mind, we knew that specific considerations would be required to tune the tool and traffic sent.

Fortunately, BreakingPoint provides an interface for tuning the throughput based on the type of test being performed and, even when using a prebuilt template, various tweaks to how the tests run are managed by the administrator. The virtual appliance can generate traffic from 1Gbps up to the limits of the underlying server.

Setup and Integration

Setting up the device, either the hardware or virtual appliance, requires deciding where the appliance will reside and how it will talk to the devices it needs to test. This is largely configured via the GUI in the "Network Neighborhood" configuration screen shown in Figure 2.

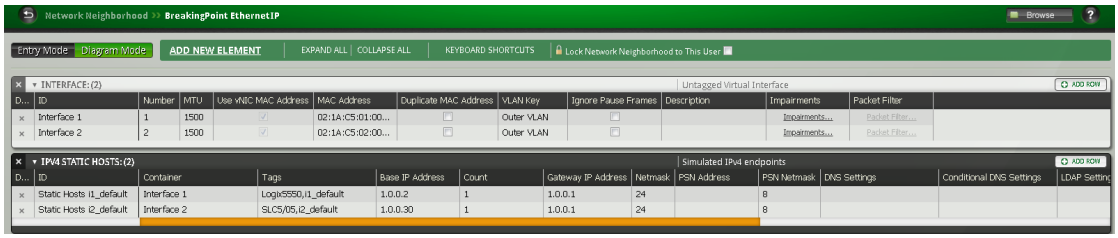


Figure 2. The "Network Neighborhood" Configuration Screen

This component of the GUI allows the user to specify which networks/hosts BreakingPoint will interact with and essentially how that will work with gateway subnetting, container and tag settings. There are, by default, a multitude of choices to select from based on the type of network architecture and port mapping required. We found it useful to select a template and customize it to meet our needs but leveraged the API as well. The API supports selecting, modifying and saving Network Neighborhoods, which was useful for integrating with Python/Bash scripts aimed at automating the setup of new test criteria.

Getting the Most Out of the Tool

Analysts can use BreakingPoint to test the networking capabilities and capacity of other enterprise appliances by simulating malware, DDoS, application fuzzing and legitimate packets. To ensure success of the testing protocol, be sure to identify test criteria, use cases and clear descriptions of what constitutes success vs. failure. For example, some

of our testing consisted of trying to understand how much throughput an IPS can handle before packet loss becomes too great.

Other testing was more involved than simply defining a target device and initiating a test. We wanted to identify metrics: How are we expecting the target application to respond, and what can we learn from the results of the test?

For example, businesses do not typically test for DoS during penetration testing, but maybe they should because all but the most robust systems can be brought down via DDoS. The objective of using BreakingPoint then becomes to tune your testing criteria to ensure you are able to measure performance—resistance to attack, throughput, etc. We found this to be helpful for security scanning in a continuous deployment environment and in the lab environment for PoC research and testing of new networking devices. We spent more than a month with BreakingPoint, and as our familiarity with the tool increased, we identified three business objectives that use of the tool contributed to: security assessments, technology/vendor selection and as an agent of change.

BreakingPoint simulates malware, DoS, application fuzzing and legitimate packets to enable use as a security assessment or vendor selection tool, as well as enabling change management.

BreakingPoint as a Security Assessment Tool

Organizations all run their vulnerability management programs a bit differently, with varying degrees of maturity and success. Organizations new to vulnerability management are typically looking for a point solution that does one thing reliably, such as vulnerability scanning. The natural progression is to add more tools for more purposes, including patch management, threat identification and hunting, risk assessments and acceptance of risk components. The need for this type of testing is evident with more than 14,000 security vulnerabilities published in 2017 alone. We found that BreakingPoint fits into the vulnerability management and penetration testing area as a complementary assessment tool.

Going Further with Vulnerability Assessments

After executing various vulnerability tests, we focused on "Quick Test" options to explore fuzzing capabilities to test applications and the web application firewall's (WAF) ability to detect and block malicious traffic. We wanted to use the tool to send malicious payloads and verify that the target device/application successfully blocked the attacks. To do this, we defined a new test criteria with prebuilt templates and then modified the test with customized components (see Figure 3).

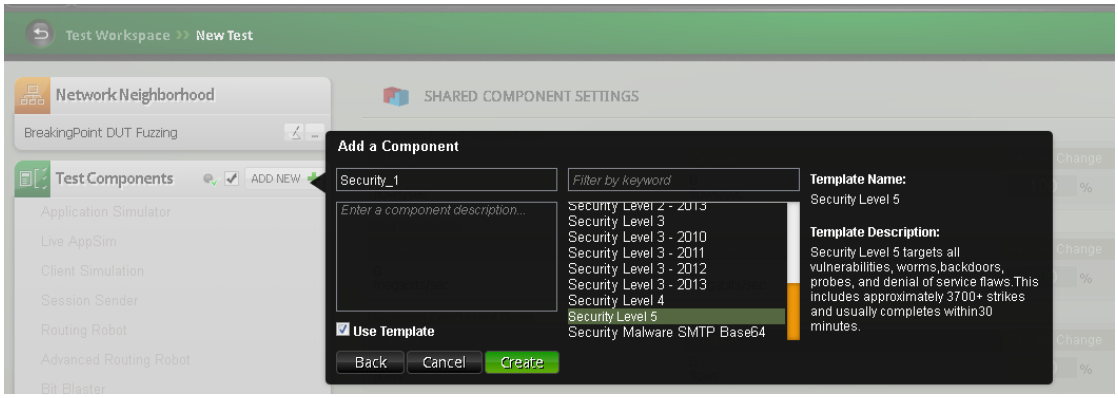


Figure 3. Setting up a New Test

It took some effort to configure the Network Neighborhood to ensure the target applications/devices would receive the traffic destined to them. We needed to define which interface on BreakingPoint

would talk to which hosts, as well as define "containers" and associating "tags" alongside IP addresses, subnets and gateways to ensure proper routing of traffic.

It took some trial and error, reading the help documentation and even watching some YouTube tutorials to understand how components work with one another and how to successfully set up a test against a target system. We needed to do some additional tweaking of the test criteria to select applicable "strikes," similar to vulnerability checks. With more than 38,000 strikes to choose from, the list was extensive and proved to be useful when selecting a specific test, as shown in Figure 4.

splaying 125 of 38540 | Get more results

StrikeId	Name	Prot...	Directi...	Re...	Sev...	Vari...
E09-8...	Mozilla Firefox Top-Level Script Memory C...	http	s2c	CV...	CRI...	2
E13-3...	Oracle Java sun.awt.image.ImagingLib.loo...	http	s2c	CV...	CRI...	1
D02-...	Cisco IOS Malformed SNMP Message-Han...	snmp	c2s	CV...	CRI...	1
E09-5...	Mozilla Firefox nsPropertyTable Propertyli...	http	s2c	CV...	CRI...	1
E11-k...	KingView 6.5.3 SCADA ActiveX Control Buf...	http	s2c	CV...	CRI...	1
E13-y...	Oracle Java Font Processing Memory Corr...	http	s2c	CV...	CRI...	6
D07-...	Apple OS X QuickDraw GetSrcBits32ARGB ...	pop3	s2c	CV...	CRI...	1
D09-...	Microsoft Windows Vista/7 SMBv2 Negotia...	tcp	c2s	CV...	CRI...	1
E08-z...	CA ARCserve Backup for Laptops and Des...	tcp	c2s	CV...	CRI...	1
E09-4...	Microsoft Active Template Library Object ...	http	s2c	CV...	CRI...	4
E10-4...	Google Chrome Google URL Cross Origin B...	http	s2c	CV...	CRI...	3
E10-5...	Mozilla Firefox plugin Array Pointer Heap ...	http	s2c	CV...	CRI...	1
E11-5...	Oracle Java Rhino Javascript Error Parsing...	http	s2c	CV...	CRI...	1

Figure 4. Setting up a Strike List Against a Target System

From a security assessment perspective, another use case we wanted to test was leveraging BreakingPoint to test device patch level or otherwise identify vulnerable systems. At first blush, it didn't seem that BreakingPoint was the right tool for the job in terms of running vulnerability scans. Interestingly, however, we used BreakingPoint to do exactly that, and this is how it works.

Initially setting up BreakingPoint to identify whether a system is vulnerable to Heartbleed, for example, is similar to configuring the tool to tackle any other type of test: Define the criteria to test for and the targets to test and save them to easily run future tests. The results of testing provided in Figure 5 quickly showed that the target systems did not, in fact, "pass the test."

Figure 5. Test Criteria Failure

Augmenting Web Application Penetration Testing

At this point, we had done enough testing to develop a level of confidence that BreakingPoint can help identify how well a WAF is tuned and even identify vulnerable assets not protected by the WAF. In addition, we wanted to use this tool to perform application simulation for token randomization, brute force attacks, dynamic file generation and other such attacks to assist with some components of web app pen testing.

In most environments, we test web applications that are mature and in scope for the likes of PCI or are otherwise required to be tested and, conversely, applications that are pre-production or in various stages of the software development life cycle.

For mature applications, we could set up BreakingPoint to define containers, networks and IP addresses, save those details and automate testing. But for new applications, or at least applications that are not on well-defined networks, we needed to manually define targets on a case-by-case basis. This is relevant because it takes tuning the DevOps process to ensure a group of static networks and IPs for consistent testing with BreakingPoint as applications moved through the pipeline. Once we overcame that hurdle, we needed to tune the test criteria on a per-application basis.

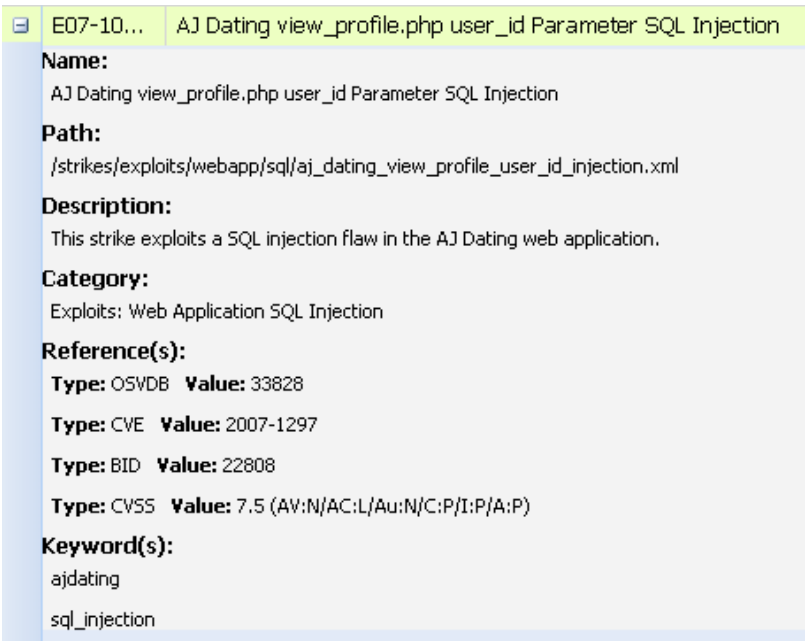


Figure 6. SQL Injection Attacks on the Strike List

The "Strike List" was a good starting point, but with no matches for Open Web Application Security Project (OWASP) and a multitude of vulnerability-specific exploit codes, the list was not ideal for session fuzzing, account brute forcing or logic attacks. For example, when searching strikes for SQL injection, there are several dozen to choose from. Each is built to identify a specific vulnerability in a specific implementation or version of an application. Simply using such a strike with a different implementation or version would result in false positives or unneeded overhead. See Figure 6.

Regardless of OWASP not specifically being called out by name in the various strikes, several OWASP Top 10 vulnerability categories are present and custom strike lists can be crafted or uploaded. We found this useful for testing unique flaws on a target system where a canned strike would not suffice. See Figure 7.

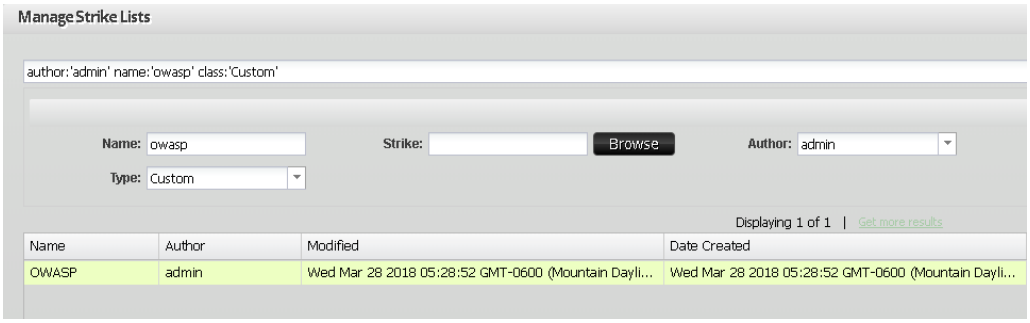
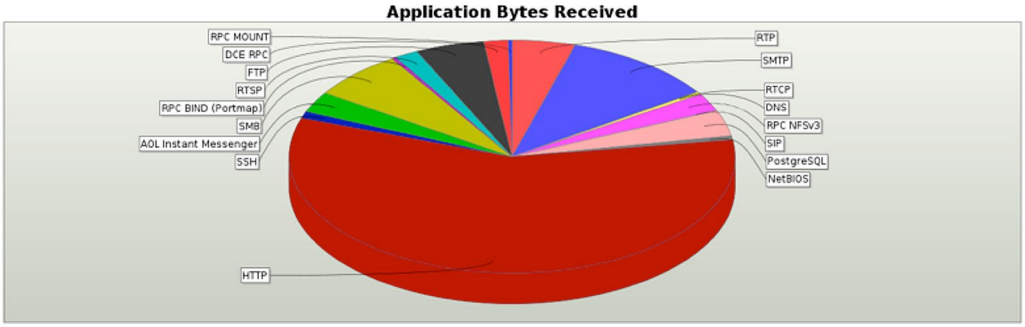


Figure 7. OWASP Vulnerabilities on the Customized Strike List

The reporting capabilities of the tool were thorough if not overly robust, although admittedly configurable. Viewing the results of a test in the web UI allowed us to drill into each specific test component, like "Application Simulation," to home in on information specific to that component. This was useful for information at a glance. However, the more powerful reporting options are available when downloading a report: Out of the hundreds of components available for reporting, you can choose just the select portions you want to report on, like frame bytes on interface two coupled with DNS application throughput (see Figure 8).



Protocol	Data Transmitted (Bytes)	Data Transmitted (%)	Data Received (Bytes)	Data Received (%)
RTP	172,219,002	4.572%	172,219,002	4.572%
SMTP	415,267,506	11.026%	415,267,506	11.026%
RTCP	1,590,558	0.042%	1,590,558	0.042%
DNS	12,708,744	0.337%	12,708,744	0.337%
RPC NFSv3	94,406,136	2.507%	94,406,136	2.507%
SIP	1,411,080	0.037%	1,411,080	0.037%
PostgreSQL	136,481,746	3.624%	136,481,746	3.624%
NetBIOS	19,649,784	0.522%	19,649,784	0.522%
HTTP	2,174,754,123	57.741%	2,174,754,123	57.741%
SSH	34,084,810	0.905%	34,084,810	0.905%
AOL Instant Messenger	108,582,288	2.883%	108,582,288	2.883%
SMP	255,651,454	6.788%	255,651,454	6.788%
RPC BIND (Portmap)	10,537,164	0.280%	10,537,164	0.280%
RTSP	64,814,576	1.721%	64,814,576	1.721%
FTP	187,802,691	4.986%	187,802,691	4.986%
DCE RPC	66,426,400	1.764%	66,426,400	1.764%

Figure 8. BreakingPoint Test Report

BreakingPoint as a Vendor Selection Technology

Whether it's IPS, IDS, NGFW, DDoS mitigation, DLP, SSL/TLS decryption, full packet capture or log collection, sizing up a product is a critical element to an enterprise strategy focused on staying on budget, right-sizing for a given environment and future-proofing the product choice. One of the strong points of BreakingPoint is that it allows the tester to synthesize real-world traffic and real-world conditions customized to the environment in which the devices will be operating.

This concept is relevant in situations where a business has identified the need to purchase hardware and has one or more solutions in the PoC phase actively deployed on the network. We used BreakingPoint in this way to test an NGFW appliance with a datasheet touting 20Gbps throughput with the ability to handle more than 100,000 sessions per second.

The objective of testing was to validate those numbers and, more important, identify whether the firewall would be a good candidate for the environment based on its performance. Most enterprises in a PoC phase don't have the ability to failover a production load to an untested device. This is really where BreakingPoint hits its niche.

BreakingPoint allows you to synthesize real-world traffic and real-world conditions that you can tailor to mimic your own network.

From within the BreakingPoint interface, we configured a test applicable to what the firewall would encounter in the live environment and simply turned up the data rate and configured the "Target Minimum Simultaneous Super Flows" to serve as the criteria to define pass/fail. There are numerous other options that we configured later to tune the test and get the most useful results. See Figure 9.

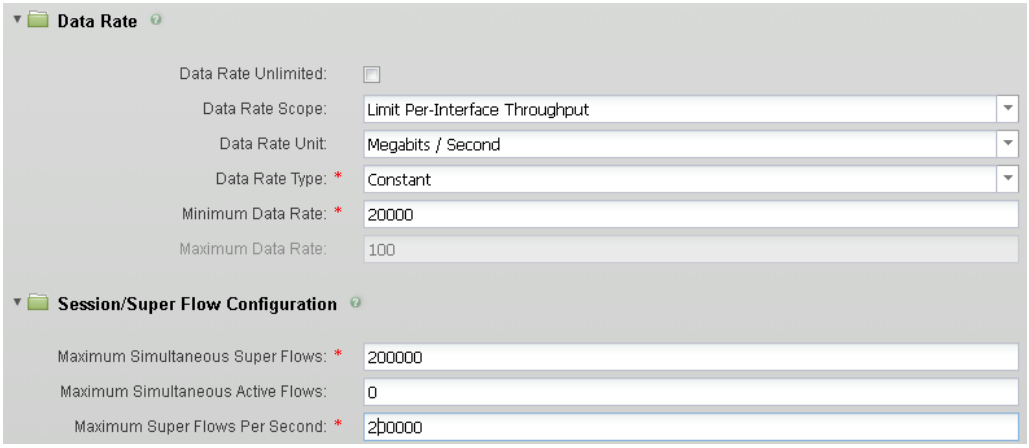


Figure 9. Cranking up the Data Rate

Choosing the Right Solution

Choosing the right solution is hard when you don't have the data to back up your decision. It is not uncommon for organizations to make a purchase decision only to find out months later that their decision was wrong. Simulating traffic can help to determine the correct hardware purchase and uncover gaps in the planning process. With BreakingPoint, we configured specific criteria to test on, defined the target appliances (log collection agents, indexers, etc.) and collectively sent traffic to this group of devices.

Rule of thumb: In testing, set the data rate at one and half times the desired production throughput.

Instead of TCP sessions or application traffic to be filtered by a firewall, we tailored this traffic to the type of testing we wanted to conduct. Specifically, we wanted to make sure that these database activity monitoring devices are capable of handling the amount of throughput currently being gathered in production. As a rule of thumb, users should determine how much capacity is needed and then test for at least one and half times that amount.

At this point, we knew by looking at NetFlow data and local packet capture information that we could expect a baseline of 300Mbps of raw SQL logs. Thus, we wanted to configure BreakingPoint to test for this. There are cases in which traffic is unique, such as proprietary protocols, and you can account for this by using BreakingPoint's "re-create" feature, which essentially allows you to upload a pcap with the exact traffic you want to simulate, as illustrated in Figure 10.

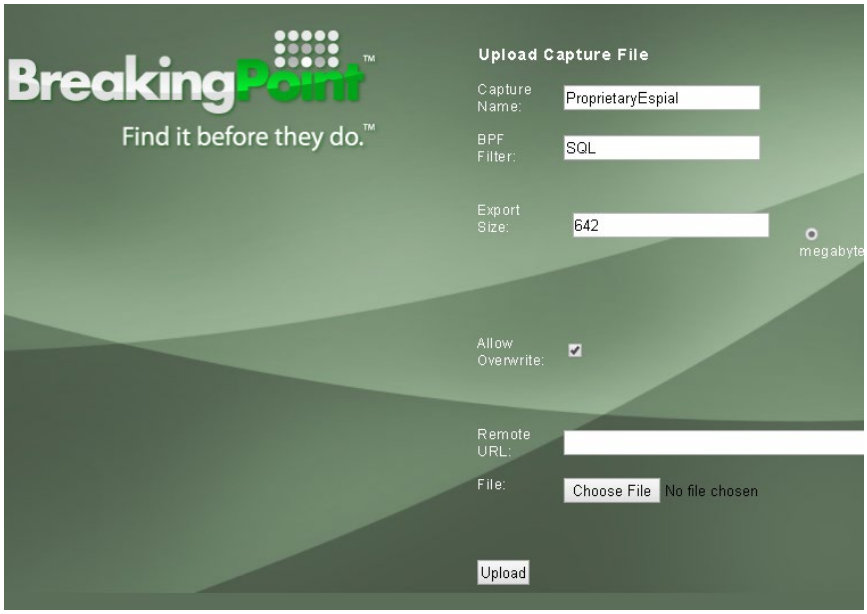


Figure 10. Built-in Options for Sending Traffic

This complements the built-in options for sending application- and protocol-specific traffic. BreakingPoint also supports Ixia NetFlow metadata imported using **`TrafficREWIND`** and **`LiveAppSim`**.

A product sheet can help establish a frame of reference, but it can be invaluable to have live data as it pertains to how a device performs under load that is representative of your network. We learned that the documented sustained throughput on our firewall was generally as advertised until IPS functionality was enabled. In any environment, this is useful information, and for our testing, this actually helped guide a purchase decision. We could certainly imagine a decision leveraging verifiable information to ultimately help negotiations or make a choice on a vendor product when it lives up to its reputation.

BreakingPoint as a Change Agent

We all know change is a constant in the universe, but do you know how the contractual obligation to inspect SSL traffic for your boundary is going to impact your current hardware? This change can be put in front of the change advisory board (CAB), discussed and then put into the PoC, with BreakingPoint providing the hard data to ensure seamless integration.

BreakingPoint Helps Identify Bottlenecks

Let's shift the discussion to measuring the performance impact of turning on SSL "HTTPS Everywhere" or only allowing TLS 1.2 for PCI standards on devices responsible for the encryption overhead. From a security engineer perspective, we found BreakingPoint to be close to ideal as a solution to help us understand the performance impact of enforcing TLS 1.2 across the network.

This shift to allow only the latest TLS protocol in more sensitive environments and in actuality allowing only encrypted connections for most all application layer traffic is becoming a norm. What we wanted to understand was how BreakingPoint can help identify bottlenecks. Once again, planning is an important step when determining how best to establish a test scenario:

- What devices should be included in the test?
- What is the traffic baseline?
- What metrics will guide the pass/fail of the testing?

Planning is essential to testing. Determine devices to be included, baselines and metrics for success or failure before you start.

We needed to know which devices to include in the test because they needed to be configured in BreakingPoint as targets. And we wanted to understand some general baseline throughputs so we could configure applicable tests to gather statistics and determine what would constitute a passing result.

Once we gathered this information, we set up and ran the tests. Results showed what we could expect for throughput when enabling TLS 1.2, as well as which hosts could handle this protocol. More interesting than the reporting was the setup. BreakingPoint allows for detailed configuration of everything from the transaction flag on the client

hello to the certificate exchange, key size and cipher suites to use. We found this particularly useful and convenient because it was granular and allowed us to configure the test to match exactly how the systems in our environment are configured. See Figure 11.

Actions

#	Action	Value	Flow #	Flow	Source
1	Client Hello		1	DTLS	client
	Transaction Flag	Start			
	DTLS Version	1.2			
	Sequence Number	0			
	DTLS Handshake Version	1.0			
	Cookie	HW81HfF1EB492N381MA814LQP93			
	Cipher Suites	2,3,4,6,7			
	Compression Methods				
2	Hello Verify Request		1	DTLS	server
3	Client Hello		1	DTLS	client
4	Server Hello		1	DTLS	server
5	Certificate		1	DTLS	server
6	Server Hello Done		1	DTLS	server
7	Client Key Exchange		1	DTLS	client
8	Change Cipher Spec		1	DTLS	client
9	Encrypted Handshake		1	DTLS	client
10	Change Cipher Spec		1	DTLS	server
11	Encrypted Handshake		1	DTLS	server
12	Application		1	DTLS	client
13	Alert		1	DTLS	client
14	Alert		1	DTLS	server

Figure 11. BreakingPoint's Granular Configuration

BreakingPoint and DevOps

BreakingPoint can help as an agent of change as part of the DevOps process by verifying that infrastructure changes don't degrade performance and validating that new application implementations are ready for production. Using the GUI simply won't suffice in this situation, and as expected, there are two primary ways of interacting with BreakingPoint that lend themselves to DevOps norms.

The first is a RESTful API, which is simple to use and consists of about two dozen different tasks that can be implemented with **POST** and **GET** requests utilizing **JSON**. This API is helpful for normal user interactions like reserving ports, executing a test and obtaining the results of a test. To successfully integrate BreakingPoint into your DevOps program, we recommend dedicating specific internal networks to systems/applications needing to be tested and correlating those networks with dedicated ports on the BreakingPoint appliance to create a dedicated template for testing.

While the API does support modifying the Network Neighborhood, we found it easier to reuse the same network configuration when conducting similar tests because it reduced the chance of testing the wrong devices. The next step we took was writing a script to leverage the API to run custom strikes against our target instance, generate reports and move the application through the pipeline when passing results were achieved. See Figure 12.

```
HTTP/1.1 200 OK
Date: Mon, 26 Mar 2018 06:15:59 GMT
Content-Type: application/json
Connection: close
Server: Jetty(8.1.9.v20130131)

{
 "links" : [ {
   "rel" : "self",
   "href" : "https://10.42.42.133/bps/api/v1/bps/ports"
 }, {
   "rel" : "reserve operation",
   "href" : "https://10.42.42.133/bps/api/v1/bps/ports/operations/reserve",
   "method" : "POST"
 }, {
   "rel" : "getSystemDescription operation",
   "href" : "https://10.42.42.133/bps/api/v1/bps/ports/operations/getsystemdescription",
   "method" : "POST"
 }, {
   "rel" : "rebootCard operation",
   "href" : "https://10.42.42.133/bps/api/v1/bps/ports/operations/rebootcard",
   "method" : "POST"
 }, {
```

Figure 12. Script to Run Custom Strike

The second is the Enhanced Shell. This shell consists of a collection of Bash scripts that provided us with a more familiar way of administering the system at a more fundamental level and executing tasks such as applying updates, adding strikes to a strike list and altering host settings. Automating updates, configuring and executing tests, handling errors, producing reports and performing other such tasks in an automated fashion lend themselves well to a DevOps program, as shown in Figure 13.

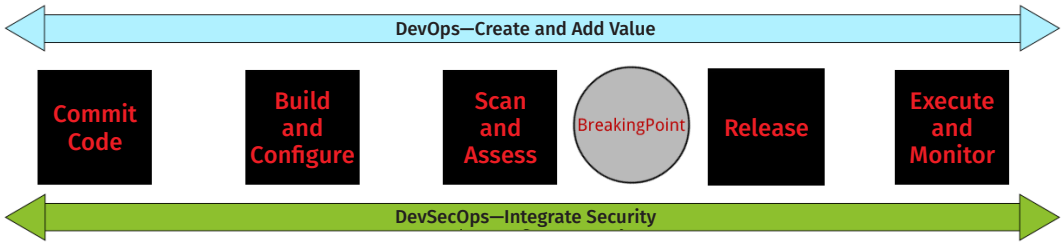


Figure 13. BreakingPoint and the DevOps Process

Conclusion

BreakingPoint is an enterprise tool that can be used for robust network security testing. We found it more than capable of measuring throughput in hardware appliances, sending malicious traffic at security devices and providing actionable information. As a network testing tool, BreakingPoint sends traffic to a device or series of assets to simulate denial-of-service conditions and sends far more granular traffic for the purpose of understanding how the target system(s) is able to keep pace or otherwise handle the traffic.

BreakingPoint can help security teams select the right technology. It augments security testing and integrates well with a DevOps approach. We used the tool to inundate networking appliances with high volumes of traffic to learn what their throughput and application latency was by default and what it was after turning on additional features.

We leveraged BreakingPoint to identify which assets were capable of supporting TLS 1.2 and to automate the configuration, testing and reporting. The granularity of the application and protocol-specific settings exceeded our expectations. We also liked the ability to create custom strike lists specific to our environment.

BreakingPoint is more than just a network testing tool to send DoS traffic. BreakingPoint provides a unique solution that enables security assessment, vendor selection and change management. It integrates well and, after initial setup, is easy to use. For those reasons, we believe the tool has great value to the security community and specifically larger enterprises in the midst of infrastructure updates and those optimizing information security programs.

About the Author

Serge Borso, a SANS community instructor and analyst, teaches the Defending Web Applications Security Essentials and Web Application Penetration Testing and Ethical Hacking courses for SANS. As owner and principal consultant of an information security organization, he leads penetration-testing engagements and has helped dozens of organizations improve their security posture. Serge's accomplishments include developing vulnerability management programs, creating security awareness training solutions and implementing a biometric security system for online banking. An active member in the InfoSec community, he serves on the board of directors of the large, active Denver chapter of Open Web Application Security Project (OWASP). Serge holds several security certifications, including CISSP, GPEN, GCFA, GWEB and GWAPT.

Sponsor

SANS would like to thank this paper's sponsor:

ixia
A Keysight Business

Last Updated: May 26th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Atlanta 2018	Atlanta, GAUS	May 29, 2018 - Jun 03, 2018	Live Event
SEC487: Open-Source Intel Beta Two	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS Rocky Mountain 2018	Denver, COUS	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS London June 2018	London, GB	Jun 04, 2018 - Jun 12, 2018	Live Event
DFIR Summit & Training 2018	Austin, TXUS	Jun 07, 2018 - Jun 14, 2018	Live Event
Cloud INsecurity Summit - Washington DC	Crystal City, VAUS	Jun 08, 2018 - Jun 08, 2018	Live Event
Cloud INsecurity Summit - Austin	Austin, TXUS	Jun 11, 2018 - Jun 11, 2018	Live Event
SANS Milan June 2018	Milan, IT	Jun 11, 2018 - Jun 16, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, JP	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, NO	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Philippines 2018	Manila, PH	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS ICS Europe Summit and Training 2018	Munich, DE	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Crystal City 2018	Arlington, VAUS	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, AU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, MY	Jul 16, 2018 - Jul 21, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Amsterdam May 2018	OnlineNL	May 28, 2018 - Jun 02, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced