Testing IDS using GENESIDS: Realistic Mixed Traffic Generation for IDS Evaluation

Felix Erlacher and Falko Dressler
[erlacher,dressler]@ccs-labs.org
Heinz Nixdorf Institute and Dept. of Computer Science
Paderborn University, Germany

ABSTRACT

Evaluating signature-based Network Intrusion Detection Systems (NIDS) is a necessary but in general difficult task. Often, live or recorded real-world traffic is used. However, real-world network traffic is often hard to come by at larger scale and the few available traces usually do not contain application layer payload. Furthermore, these traces only contain a small amount of malicious traffic, which does not suffice to thoroughly test a NIDS. We solve this problem by proposing a complete stateful traffic generation system that mixes realistic traffic with user definable malicious HTTP traffic with the purpose of evaluating a NIDS. By relying on the Snort syntax for traffic definition, we guarantee a large dataset of realistic up-to-date attack patterns.

CCS CONCEPTS

• **Security and privacy → Intrusion detection systems**;

1 INTRODUCTION

NIDS are the primary tool of choice when it comes to defend against the increasing number of threats in the Internet [9]. Established taxonomies (e.g., [2]) categorize NIDS according to the applied detection method: Anomaly-based NIDS use behavior-based techniques by defining a model of normal network behavior and then detecting deviations to this model. Rule-based systems use a precise definition of events to match incoming traffic against. While the methods proposed in this paper can, to a certain extend, also be used for anomaly-based systems, we focus on rule-based NIDS.

SIGCOMM Posters and Demos '18, August 20–25, 2018, Budapest, Hungary

ACM ISBN 978-1-4503-5915-3/18/08…$15.00
https://doi.org/10.1145/3234200.3234204

The most widely used method to evaluate such systems is to use real traffic from a live network or one of the publicly available network traces [5, 7]. Except for carrier grade networks to which very few researchers have access to, network traces are the first choice for such tests. Among other drawbacks [6, 8], the problem with publicly available traces is that they almost never contain application layer payload, and, secondly they only contain very few detectable attack pattern, i.e., security events.

Thus, most publications suggesting novel NIDS [1, 3], ours included, choose a subset of manually crafted attacks and multiply and distribute them over a given network trace. This results in a so called mixed workload containing benign and malicious traffic [2]. The problem, and this is frequently also reflected in review comments, is, that it is hard to prove that such traces are realistic and, possibly even worse, they still contain only a very small subset of all possible real-world attacks. Thus, no convincing evidence of the overall coverage of the tested system can be provided.

In this demo, we propose to showcase a complete system for signature-based NIDS evaluation. We use the TRex traffic generator to generate realistic and timely precise benign traffic including application layer payload. In addition, our GENESIDS event generator [4] mixes in traffic that mimics user definable attacks. Both the benign traffic and the attack traffic can be widely adapted to the application scenario of interest. All of the tools are available as open source software at the following locations: TRex: https://trex-tgn.cisco.com, GENESIDS: https://github.com/felixe/idsEventGenerator.

2 ARCHITECTURE

The architecture of our system is sketched in Figure 1. At the core of the system is the Cisco TRex traffic generator. TRex is free and open source software and uses DPDK[1] for fast (up to 200 Gbit/s) network traffic generation maintaining a very precise timing. We chose TRex because of its ability to flexibly and accurately configure and generate application layer payload. TRex generates stateful traffic that is analyzed by the Intrusion Detection System (IDS) under test. The traffic to be generated is defined by a traffic template. Such a template may include multiple TCP flow samples in the

[1] http://www.dpdk.org

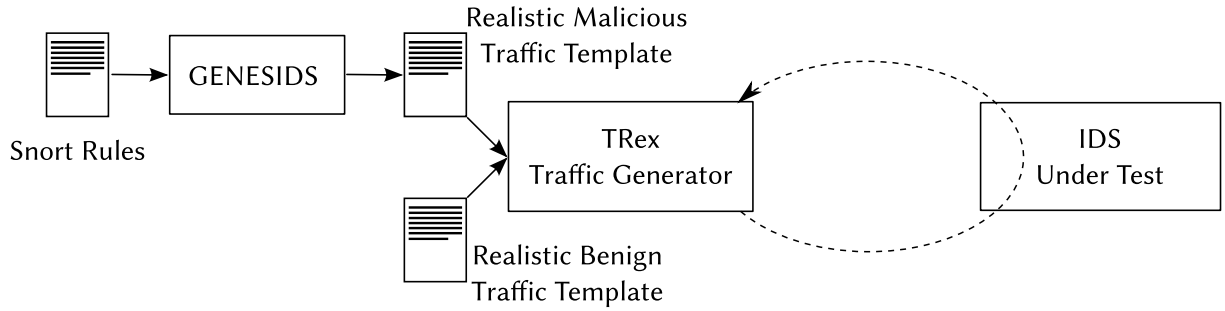

Figure 1: Outline of the proposed system architecture

form of pcap files. Traffic properties like flow connections per second, inter packet timing, etc. can be configured in the traffic template according to the application scenario. TRex ships with different examples of realistic benign traffic templates.

To add malicious traffic, we use our free and open source GENESIDS traffic generator. GENESIDS automatically generates user definable malicious HTTP network traffic. The input format follows the Snort syntax, so the user can take advantage of thousands of readily available realistic attack definitions. The generated attacks are labeled with a special HTTP header field which contains the unique SID number of the attack. This makes the verification of the alerts triggered by the NIDS under test straightforward.

To use the attack traffic generated by GENESIDS with TRex, the following steps are necessary: First, generating the attack traffic with GENESIDS using as input the desired attack description in the Snort syntax (or take existing Snort rules). Second, capturing the generated traffic and splitting the captured network dump into its single TCP flows. Third, using a TRex template file containing the desired benign traffic and including the attack TCP flows in this template, configuring them according to the application scenario.

3 DEMONSTRATION

In our demonstration, we use our proposed system to "evaluate" the IDS Snort. As benign realistic traffic, we use a template that has been defined by SFR France.[2] According to the TRex manual, this template is also used by Cisco to benchmark their ASR1k/ISR-G2 routers. As malicious traffic, we generate 1000 flows with GENESIDS using 1000 different Snort rules as attack descriptions. Using the configuration options in the traffic template, these flows are then equally distributed over the benign traffic resulting in a mixed traffic set.

TRex provides statistics about the generated traffic as well as the packets dropped by the workstation running Snort. Snort, acting as the IDS under test, will provide statistics making it possible to assess how many of the attacks it was able to detect.

The used configuration files, generated network traces and other additional material can be found on the author's homepage.[3]

4 CONCLUSION

In this work, we presented a mixed traffic generation system focusing on the evaluation of signature-based Network Intrusion Detection Systems (NIDS). To generate timely precise and realistic traffic, we use the TRex traffic generator in combination with realistic traffic sets used by Cisco. We then add malicious HTTP traffic by using the GENESIDS traffic generator, which uses attack definitions in the form of Snort rules. This guarantees realistic traffic mixed with a high number of real-word events.

REFERENCES

[1] Waleed Bul'ajoul, Anne James, and Mandeep Pannu. 2015. Improving Network Intrusion Detection System Performance through Quality of Service Configuration and Parallel Technology. *Elsevier Journal of Computer and System Sciences* 81, 6 (Sept. 2015), 981–999. https://doi.org/10.1016/j.jcss.2014.12.012

[2] Hervé Debar, Marc Dacier, and Andreas Wespi. 1999. Towards a Taxonomy of Intrusion-Detection Systems. *Elsevier Computer Networks* 31, 8 (April 1999), 805–822. https://doi.org/10.1016/S1389-1286(98)00017-6

[3] Felix Erlacher and Falko Dressler. 2018. FIXIDS: A High-Speed Signature-based Flow Intrusion Detection System. In *IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*. IEEE, Taipei, Taiwan.

[4] Felix Erlacher and Falko Dressler. 2018. How to Test an IDS? GENESIDS: An Automated System for Generating Attack Traffic. In *ACM SIGCOMM 2018, Workshop on Traffic Measurements for Cybersecurity (WTMC 2018)*. ACM, Budapest, Hungary. to appear.

[5] Romain Fontugne, Pierre Borgnat, Patrice Abry, and Kensuke Fukuda. 2010. Mawilab: Combining Diverse Anomaly Detectors for Automated Anomaly Labeling and Performance Benchmarking. In *6th International Conference on emerging Networking Experiments and Technologies (CoNext 2010)*. ACM, Philadelphia, PA. https://doi.org/10.1145/1921168.1921179

[2] French telco operator: https://www.sfr.fr

[3] http://ccs-labs.org/~erlacher/resources/

[6] John McHugh. 2000. Testing Intrusion DetectionSystems: A Critique Of The 1998 And 1999 Darpa Intrusion Detection System Evaluations As Performed By Lincoln Laboratory. *ACM Transactions on Information and System Security (TISSEC)* 3, 4 (Nov. 2000), 262–294. https://doi.org/10.1145/382912.382923

[7] Nour Moustafa and Jill Slay. 2016. The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set. *ACM Information Security Journal: A Global Perspective* 25, 1-3 (Jan. 2016), 18–31. https://doi.org/10.1080/19393555.2015.1125974

[8] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. 2018. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In *4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*. INSTICC, Funchal, Portugal, 108–116. https://doi.org/10.5220/0006639801080116

[9] Benjamin Stritter, Felix Freiling, Hartmut König, Rene Rietz, Steffen Ullrich, Alexander von Gernler, Felix Erlacher, and Falko Dressler. 2016. Cleaning up Web 2.0's Security Mess - at Least Partly. *IEEE Security & Privacy* 14, 2 (March 2016), 48–57. https://doi.org/10.1109/MSP.2016.31