6D-02

IDPS-Honeypot Hybrid Approach to High-Precision Cyberattack Detection and Prevention

Makoto Iwabuchi　　Akihito Nakamura

Computer Science Division, University of Aizu, Japan

1. Introduction

Cybersecurity is more important now than ever. One possible countermeasure is Intrusion Detection and Prevention System (IDPS), which enables detection of malicious activities in the network based on signature-matching and other detection methods. Signatures are the recorded characteristics of the attacker's behavior. However, it occasionally misses malicious traffic or raises false alerts when the detection method is not carefully configured with the latest information. That is, it is prone to false-positive or false-negative. Also, the creation of signatures requires in-depth knowledge of network and security.

This paper presents a high-precision threat detection system with automatic generation of tailored signatures and rapid response to emerging threats. It generates specific signatures by monitoring actual traffic on the network using honeypots. When a new unforeseen pattern is observed, the system generates a specific signature. Furthermore, generated signatures are immediately installed on the IDPS to block the following activities. As a result, the system enables real-time adaptive security with high-precision threat detection and prevention.

2. Automated IDPS signature generation

2.1 System architecture

The essence of our method is automation of the rule generation with IDPS-Honeypot hybrid system. Honeypot is software that dares to put on the soft-ware remained vulnerable and receives attacks in order to observe and record logs. This enables discovery of new attack patterns and the latest trends in attacks.

Figure 1 shows the architecture of the system. On the edge of a network, an IDPS analyzes incoming network traffic and responds to intrusion attempts based on the given signatures. Typically, it blocks attacks by dropping the packets from the offending IP addresses. In the second tier, honeypot(s) capture the packets evaded the IDPS. They identify malicious activities and log information. The core of the system is Automatic Signature Generation System (ASGS). It analyzes the honeypot logs and generates IDPS signatures if necessary.

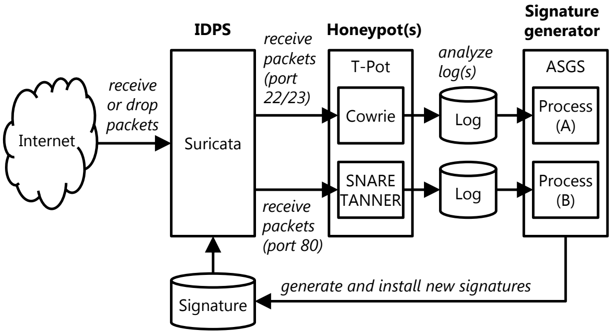

Figure 1: System architecture

2.2 Detection and prevention methods

Basically, we adopt signature-based detection method. That is, the IDPS compares incoming packets with predefined attack patterns known as signatures.

In addition, statistical anomaly-based detection method is utilized. The honeypots characterize malicious traffic and ASGS compares it against the established baseline. For example, the number of requests observed in a unit of time is defined to identify a brute force attack or pre-attack investigation. If traffic exceeds the baseline, the system generates a new signature to block it.

The sole prevention method defined in the signatures is dropping the matched packets and raising alerts. That is, the system responds to a detected threat by attempting to prevent it from succeeding.

2.3 Signature generation processes

ASGS generates two types of signature: IP-based and payload-based as shown in Figure 2. An IP-based signature is used to identify a series of access from a specific host, while a payload-based one inspects the content of the payload of packets.

In the current design, a few simple conditions and baselines are used based on heuristics. For example, the number of access per unit time is used to identify brute-force attack on SSH or Telnet.

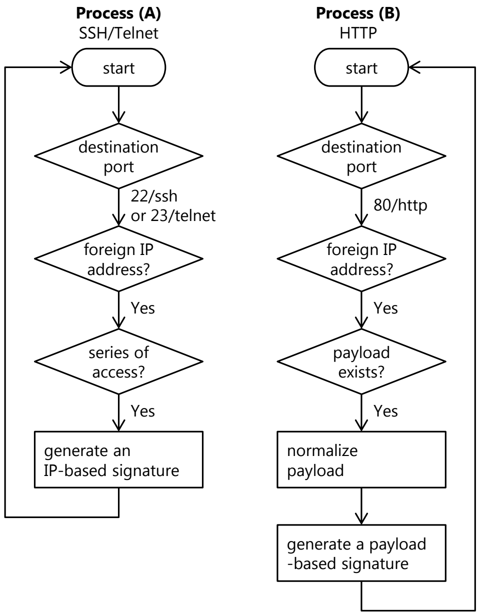

Figure 2: Signature generation processes

2.4 Implementation

We have developed the system in Python language and the number of lines in code is currently about 360. The code is maintained on GitHub and will be public soon. For other components, we employ open-source software. Suricata 6.0.0 [1] and T-Pot 20.06.1 [2] are used for IDPS and honeypot platform, respectively. Actually, two honeypots run on T-Pot; Cowrie [3] is used to log SSH and Telnet and SNARE [4], in combination with a data analyzer TANNER, is used for HTTP logging.

3. Evaluation

We evaluated the effectiveness of the method in a real environment for two weeks: from December 8 to 21, 2020. The system has been deployed on a host with an unprotected commercial Internet connection. For comparison, we also run Suricata solely on another host. The version 9627 of Suricata signature set was used at the start; it includes about 28,600 signatures.

Figure 3 shows the number of signatures generated by ASGS and the number of matched packets. The average number of incoming packets per day was about 1.2 million, whereas the number of generated signatures per day was 129.

Figure 4 shows the signature match rate. The rate is proportion of the matched packets to all the incoming ones. The averages were about 0.6% and 4.3% with and without ASGS, respectively.

We also evaluated the performance in terms of response time. Current ASGS is activated with a period of 30 seconds; it takes few seconds to generate signatures and Suricata takes about 15 seconds to reload the new signature set.

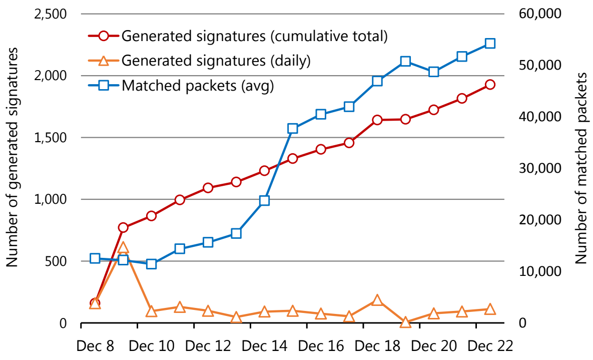

Figure 3: Generated signatures and matched packets

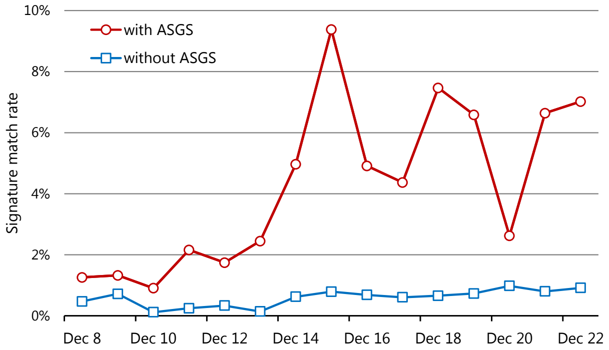

Figure 4: Signature match rate

4. Conclusion

We proposed a method and system for high-precision threat detection with automatic generation of tailored signatures and rapid response to emerging threats. The evaluation results demonstrate that the system supports expected features and improves the existing IDPS. Our plans for future work include optimization of signature generation [5] and lifecycle management of signatures.

References

[1] Suricata. https://suricata-ids.org/

[2] T-Pot. https://github.com/telekom-security/tpotce

[3] Cowrie. https://github.com/cowrie/cowrie

[4] SNARE/TANNER. http://mushmush.org/

[5] S. Ohashi, et al., “An Automated Tuning Method for NIDS Signature based on NIDS Alerts of Attack on Honeypots”, *80th National Convention of IPSJ*, 2018.