Analysis of Intrusion Detection System Performance for the Port Scan Attack Detector, Portsentry, and Suricata

T Ernawati¹, M F Fachrozi², D D Syaputri³
Informatics Engineering Department, Politeknik TEDC Bandung, Cimahi, Indonesia

Email : ¹ernawati12@gmail.com

Abstract. The purpose of this study is to analyze the performance of IDS (PSAD, Portsentry and Suricata). The research methodology used was the Network Development Life Cycle (NDLC). The system has designed through several stages (system requirements analysis, system/software installation, configuration and testing software attacks). The system detects and monitors the number of suspicious activities that occur on the server (using a cloud service) or computer network. In the event of a threat, the system will issue a warning and keep records for analysis. The IDS performance tests are differentiated based on three types of attack (port scanning, DDoS SYN flood and brute force attack), the parameters tested include a speed of detection, detection accuracy and resources usage. Test results showed Suricata and PSAD are superior in detection accuracy (100%). Suricata showed better performance in resources usage (average 1.64% CPU, 8.42% disk), portsentry is only superior to RAM usage (26.89%). PSAD was better in the speed of detection (average 4.21s.). The result concluded Suricata and PSAD better performance to be used as network IDS.

Introduction

Increase the use of computers in human life has provided significant changes in assisting productivity, this will be offset by problems such as network security [1]. The security and confidentiality of data/information are a very important problem that requires awareness of the issue [2]. Based on the Symantec report by the year 2017, indicates the number reported of vulnerabilities increased by 13%; malware variants are up by 88%. An average web attack was blocked by Symantec 611,141 day, the malicious URLs grew by 2.8% [3]. Therefore, it is important to require a system capable of detecting the occurrence of adverse events intruder or a network. Various methods used in cyber attacks such as Viruses, Worms, Trojans, Bots, IP Spoofing, Denial of Services Attack [4], so an effort is needed to secure computer network systems to overcome various types of attack methods. One of several efforts in securing a network system is the application of an Intrusion Detection System (IDS). IDS monitor and detect networks from various anomalous activities that indicate a threat of hacker attacks, malware or vulnerability on network systems [5]. All IDS have advantages and disadvantages, therefore it is important to understand choices of IDS software types that can be used by network administrators to secure the network [6].

This paper has organized as follows: the background of the study in the first section; examines kinds of literature related to IDS and type of attack in the second section; in the third section is presented a research method. The study findings have outlined in section 4. The final section has drawn some conclusions.

This study aims to provide recommendations for network administrators to decide the right IDS software based on the managed network conditions. The present paper examines the Port Scan Attack...
Detector (PSAD), PortSentry and Suricata performance based on three types of attack (port scanning, DDoS SYN flood, and brute force attack). We analyze the IDS performance by using parameters speed of detection, detection accuracy and resources usage. The research method used is the Network Development Life Cycle (NDLC). The system is designed through several stages (system requirements analysis, system/software installation, configuration and testing of software attacks). The results of the study concluded that the performance of Suricata and PSAD is better for use as network IDS.

Research Method

Network Development Life Cycle (NDLC) used as the methodology [7]. Six stages of design are shown in Figure 1. as follows:

![Figure 1. Stages of Network Development Life Cycle [7]](image)

In this study, the authors used 4 stages namely analysis, design, implementation, and monitoring. The authors did not use the simulation method because using experiments directly. Meanwhile, the management stage has not explained because related to policies will depend on level management policies and the company's business strategy. Analysis phase, include analysis of emerging problems, analysis of system requirements and other supporting applications. The problems and system requirements (hardware and software requirements for server and client) have obtained by content analysis techniques from various references based on the problem under study. On the design stage, a small scale network topology will be created between the IDS and the client to be built. The implementation phase is focused on installing systems and supporting software and configuring according to requirements. The final stage will be done through monitoring and conducting observations during experiments on the performance of IDS based on the testing scenario.

Results and Discussion

The system designed to detect and monitor a number of suspicious activities on a server or computer network. If a threat occurs, the system will issue a warning to be analyzed. Hardware and software specifications used (Tables 1 and 2), a design of network topology (See Figure 2).

| Table 1. Hardware Specifications Used. |
|----------------------------------------|
| **Server** | **Client (Attacker)** |
| Processor | 1 Ghz | 1.5 Ghz |
| RAM | 1 GB | 2 GB |
| Harddisk | SSD 25 GB | 500 GB |
Table 2. Software Specifications Used

|           | Version       | Explanation                                                |
|-----------|---------------|------------------------------------------------------------|
| Linux Ubuntu | 18.04.1       | The Operating System used for IDS servers                  |
| Portsentry | 1.2-14 build 1| IDS application used to detect attacks                      |
| PSAD       | 2.4.3-1.2     | IDS application used to detect attacks                      |
| Suricata   | 4.0.5-1.2     | IDS application used to detect attacks                      |
| Putty      | 0.62          | The application used to remote servers.                    |
| Zenmap     | 7.70          | The application used to scan port attacks.                  |
| Metasploit | 4.16.48-dev   | The application used to scan DDoS attacks.                  |

Figure 2. Design of network topology

A server in the cloud system act as IDS meanwhile the admin can access the server for network administration purposes, the attacker attacks by accessing the server. The server's IP Address has automatically set according to the IP address provided by the Cloud Server service provider. The IP address admin and the attacker will be different according to the network provider used because of the experiment will be carried out several times (see Table 3).

Table 3. IP Address scheme.

| IP Address Scheme | IP Address     | Subnet mask    |
|-------------------|----------------|----------------|
| Server            |                |                |
| PSAD              | 206.189.90.169 | 255.255.240.0  |
| Portsentry        | 206.189.152.118| 255.255.240.0  |
| Suricata          | 128.199.213.61 | 255.255.240.0  |
| Admin             | -              | -              |
| Client/Attacker   | -              | -              |

The network system device configuration divided into 3 (three) parts, the first from the server side (the registration process to DigitalOcean; Ubuntu server installation process, IDS application installation), the second from the admin side (Remote Admin Configuration to Server with putty application) and the third is from client/attacker (zenmap, metasploit and armitage configuration). The scenario of the attack as follows:

- Port scanning
Port scanning testing aims to find out which port is open. This attack was carried out 10 times on September 15, 2018.

- **DDoS (Distributed Denial of Service)**
  Performing a DDoS attack (SYN Flood), the attacker will send an SYN request to the target server with the aim of consuming resources from the server. This attack was carried out ten times with a duration of two minutes on September 17, 2018.

- **Brute force attack**
  The brute force attack aims to get more data to access the target system, was done by peeping, seizing, and guessing the password. The attack was carried out 10 times on September 18, 2018.

The parameters used to test the performance capabilities of PSAD, portsentry and Suricata (see Table 4).

| Table 4. Parameter testing. |
|-----------------------------|
| Explanation                 |
| **Speed of detection**      |
| This test is conducted to find out which IDS is superior in the time of detection when the IDS successfully detects an attack activity. This test is done by 10 times in 2 minutes |
| **Detection accuracy**      |
| This test is done to find out how accurate PSAD, portsentry and suricata are in detecting attacks |
| **Resources usage**         |
| Measurements on CPU, RAM and Disk Usage resource usage during PSAD, portsentry and Suricata detect attacks |

System functionality testing is conducted to determine the performance of the system whether it can function accordingly (see Table 5).

| Table 5. System functionality testing result. |
|----------------------------------------------|
| Type of testing | Result    |
|-----------------|-----------|
| 1               | The server can be accessed via the internet | Successful |
| 2               | The system can detect attacks | Successful |
| 3               | The system can monitor attacks | Successful |

The results of testing speed detection:

- **PSAD**
  PSAD’s response to port scanning attacks, attacker’s IP Address 120.188.94.169 (see Figure 3); DDoS SYN Flood attack, attacker’s IP Address 120.188.93.171 (see Figure 4); Brute Force attack, attacker’s IP Address 120.188.4.230 (see Figure 5).
Figure 3. PSAD response to port scanning attacks

Figure 4. PSAD response to DDNS SYN Flood attacks

Figure 5. PSAD response to brute force attacks and history on auth.log file Linux

- Portsentry
  Portsentry’s response to port scanning attacks, attacker’s IP Address 120.188.94.169 (see Figure 6); DDoS SYN Flood attack, attacker’s IP Address 120.188.67.203 (see Figure 7); Brute Force attack, attacker’s IP Address 120.188.4.230 (see Figure 8).
Figure 6. Portsentry response to port scanning attacks

Figure 7. Portsentry response to DDNS SYN Flood attacks

Figure 8. Portsentry does not detect when an attack brute force both in the syslog file or files portsentry.history

- **Suricata**

  Suricata’s response to port scanning attacks, attacker’s IP Address 120.188.94.169 (see Figure 9); DDoS SYN Flood attack, attacker’s IP Address 114.4.82.176. (see Figure 10); Brute Force attack, attacker’s IP Address 120.188.4.230 (see Figure 11).

Figure 9. Suricata response to port scanning attacks
The results of testing detection accuracy:
The number of attacks carried out to measure the accuracy of detection in each IDS is 10 (ten) attacks, the results in Table 6.

**Table 6.** Detection accuracy test results.

|                  | PSAD | Portsentry | Suricata |
|------------------|------|------------|----------|
| Port Scanning    | 10   | 10         | 10       |
| SYN Flood        | 10   | 10         | 10       |
| Brute Force Attack | 10   | 0          | 10       |

The results of testing resource used during an attack (see Tables 7,8 and 9).

**Table 7.** Resource used test results (CPU, RAM, Disk Usage) for PSAD based on Port Scanning, SYN Flood and Brute Force Attack

|                  | Port Scanning | DDoS SYN Flood | Brute Force Attack |
|------------------|---------------|----------------|-------------------|
| **Time**         | CPU | RAM | Disk Usage | Time | CPU | RAM | Disk Usage | Time | CPU | RAM | Disk Usage |
| 1                | 99.96 | 77.07 | 53.77 | 14:14 | 99.97 | 44.48 | 41.91 | 06:18 | 7.49 | 34.22 | 56.24 |
| 2                | 100  | 81.93 | 53.71 | 16:51 | 99.97 | 45.52 | 42.17 | 06:20 | 4.81 | 34.08 | 56.24 |
| 3                | 99.60 | 38.55 | 53.18 | 16:55 | 99.89 | 37.36 | 42.67 | 06:22 | 16.41 | 27.04 | 56.25 |
Evaluate the test results of PSAD, portsentry and Suricata had shown in Table 10, the value is an average of 10 attacks.

Table 10. Evaluate test results IDS

| Metric              | PSAD | Portsentry | Suricata |
|---------------------|------|------------|----------|
| Speed of detection  | 2.18 | 6.94       | 3.51     |
|                     | 4.21 | 2.09       | 2.09     |
|                     | 2.09 | 6.14       | 3.44     |
|                     | 2.56 | 4.34       | 5.85     |

...
Based on all test parameters performed the three types of attacks for the PSAD and Suricata IDS accuracy detection parameters can detect 100% for all three attacks. While Suricata is superior in resource usage (average 1.64% CPU; 8.42% disk usage) and portsentry is better at the RAM usage (26.89%). PSAD is better at the speed of detection (average 4.21s) than Suricata (average 6.85s).

Portsentry in detection speed and accuracy has the disadvantage of not being able to detect a brute force attack. Graph of test results based on three test parameters had shown in Figures 12 and 13.

Our research showed that selecting IDS required repeated experiment and evaluation, the test result indicates:

- The best detection accuracy did by PSAD and Suricata. The results in line with the previous researches, [8] that Suricata has better detection accuracy for the port scanning and Brute Force attacks, [9] stated Suricata good accuracy in the multi-cores environment.
- The resources usage in experiments depends on the simulated attack where the smallest value shows the best results [10]. When comparing resources usage particularly RAM usage we found that Suricata has the largest average percentage of RAM usage compared to PSAD and Portsentry, the results of the test are alignment with the results of study [11] using 6 types of attacks including Brute Force and DDoS show that Suricata has a higher RAM usage on Linux or Windows platforms.
- The experiment’s result indicates Portsentry not optimally handle Brute Force attack, but effective handle port scanning attacks [12] and suitable for prevention of Denial of Service attacks [13].
Conclusions

This paper analyzes the performance of IDS (PSAD, Portsentry and Suricata). IDS performance test results are differentiated based on the type of attack, namely port scanning, DDoS SYN flood and brute force attack, the parameters tested include a speed of detection, detection accuracy and resources usage. The result concluded Suricata and PSAD better performance to be used as network IDS. Portsentry has a weakness in speed and accuracy of detection because it cannot detect brute force attacks. Further studies are needed to estimate more diverse types or attack techniques, such as sniffing, exploit. We hope that further testing will be carried out on parameters other than detection speed, detection accuracy and use of resources such as network scalability, bandwidth, latency, availability.

References

[1] Kurniawan, B. (2018, August). Integrated Information System for Radio Frequency Identification Based Administration and Academic Activities on Higher Education. In IOP Conference Series: Materials Science and Engineering, 407(1), p. 012097. IOP Publishing.

[2] Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75 (2), 24-35.

[3] Soegoto, E. S., & Jayaswara, M. R. (2018, August). Web and Android Programming Course Information System. In IOP Conference Series: Materials Science and Engineering, 407(1), p. 012063). IOP Publishing

[4] Muresan, D., & Sinuraya, R. (2018, August). Relation between internet and social media to support sales in business. In IOP Conference Series: Materials Science and Engineering, 407(1), p. 012062). IOP Publishing

[5] Soegoto, E. S., & Jayaswara, M. R. (2018, August). Web and Android Programming Course Information System. In IOP Conference Series: Materials Science and Engineering, 407(1), p. 012063). IOP Publishing

[6] Setiawan, E. B., & Setiyadi, A. (2018, August). Web vulnerability analysis and implementation. In IOP Conference Series: Materials Science and Engineering, 407(1), p. 012081). IOP Publishing

[7] Riza, L. S., Handian, D., Megasari, R., Abdullah, A. G., Nandiyanto, A. B. D., & Nazir, S. (2018). Development of r package and experimental analysis on prediction of the co2 compressibility factor using gradient descent. Journal of Engineering Science and Technology,
[8] Vicente, F., Huang, Z., Xiong, X., De la Torre, F., Zhang, W., & Levi, D. (2015). Driver gaze tracking and eyes off the road detection system. *IEEE Transactions on Intelligent Transportation Systems, 16*(4), 2014-2027.

[9] Alickovic, E., Kevric, J., & Subasi, A. (2018). Performance evaluation of empirical mode decomposition, discrete wavelet transform, and wavelet packed decomposition for automated epileptic seizure detection and prediction. *Biomedical signal processing and control, 39* (2),94-102.

[10] Hemavathi, P., & Nandakumar, A. N. (2018). Novel Scheme for Minimal Iterative PSO Algorithm for Extending Network Lifetime of Wireless Sensor Network. *International Journal of Electrical and Computer Engineering, 8*(2), 1084.

[11] Darabkh, K. A., & Muqat, R. Z. (2018, March). An efficient protocol for minimizing long-distance communications over wireless sensor networks. In *2018 15th International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 671-676). IEEE.

[12] Munir. (2015). The use of multimedia learning resource sharing (MLRS) in developing sharing knowledge at schools. *International Journal of Multimedia and Ubiquitous Engineering, 10*(9), 61-68

[13] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2011). Surveying port scans and their detection methodologies. *The Computer Journal, 54*(10), 1565-1581.