1. **Pendahuluan**

Istilah malware berasal dari gabungan dari dua kata malicious dan software dan digunakan untuk mendemonstrasikan program yang tidak diinginkan [1]⁠. Seperti namanya malware dimaksudkan untuk membahayakan komputer dan pengguna komputer dengan mencuri informasi, merusak file atau dengan hanya melakukan kegiatan nakal untuk mengganggu pengguna [2]⁠.

Ada peningkatan besar dalam keamanan siber sejak beberapa dekade terakhir. Kerugian organisasi akibat serangan cyber ini telah meningkat pesat. Setiap hari ditemukan kerentanan dan eksploitasi baru. Menurut basis data CVE pada 2018 sekitar 16.556 kerentanan dicatat dibandingkan dengan 2016 sekitar 6.447 kerentanan sistem diseluruh dunia [3], [4]⁠.

Dengan pesatnya perkembangan internet dan teknologi informasi, Network Intrusion Detection System (NIDS) semakin menarik perhatian [3]. Data yang dikirimkan dan dihasilkan oleh teknologi informasi dan komunikasi ini tumbuh secara eksponensial. Lalu lintas di jaringan ini membutuhkan pengawasan yang efektif, analisis paket dan rules untuk mengatur lalu lintas menggunakan berbagai macam intrusion detection system (IDS) dan intrusion prevention system (IPS) [5]⁠.

Remote Access Trojan (RATs) adalah malware yang dirancang untuk mengontrol komputer target dengan tujuan tertentu. Peran utama RATs adalah untuk memberikan kontrol atas mesin korban, yang dapat dicapai dengan menyuntikkan dirinya ke dalam program yang sah untuk menyembunyikan kegiatan jahat mereka [6]⁠.

Salah satu cara untuk memberikan keamanan pada jaringan dari ancaman malware adalah dengan pengaplikasian Intrusion Prevention System (IPS). *Intrusion Prevention System* (IPS) pada intinya merupakan Intrusion Detection System (IDS) yang memiliki kemampuan mendeteksi dan memblokir secara otomatis serangan yang datang pada suatu sistem.

Sistem IPS bertujuan untuk menghentikan serangan sebelum berhasil dilakukan dan sistem yang dirancang mengambil beberapa tindakan untuk mencegah jaringan dari berbagai jenis serangan. Tidak seperti IDS pendahulunya, hanya pemindaian dan laporan saja, IPS dapat secara aktif menganalisis dan mengambil tindakan pada lalu lintas jaringan [4]⁠[1]⁠.

1. **Penelitian Terkait**

Pada penelitian sebelumnya [6]⁠ telah melakukan pendeteksian botnet-rats dengan 4 metode machine learning yang berbeda dan didapatkan hasil yang baik. Berikut adalah table perbandingan yang didapatkan.



Gambar 1 Perbandingan metode machine learning

 Di penelitian lain [7]⁠ juga melakukan pendeteksian botnet-rat dengan mengkombinasikan snort engine dengan algoritma random forest, dan didapatkan akurasi sebesar 96%. Menurut [7]⁠ juga, komunikasi yang terjadi antara server dan target botnet-rats dapat di deteksi dini menggunakan metode ini.

1. **Skenario**

Pada penelitian ini penulis megajukan scenario IPS menggunakan *snort engine*.Agar dalam pengujian penelitian berjalan sesuai dengan tujuan, maka diperlukan sebuah skenario yang baik agar tahap pengujian menjadi lebih terarah dan lebih teratur. Dalam penelitian ini akan dilakukan pengujian serangan sebagai berikut :

a. Konfigurasi awal sebelum melakukan serangan :

1. Terdapat host yang dijadikan target.

2. Terdapat satu server IPS yang berada dibelakang firewall

3. Tersambung melalui LAN

b. Proses yang dilakukan penyerang :

1. Melakukan remote terhadap computer host

2. Melakukan berbagai aktivitas seperti menjadikan *host botnet* DDoS.

1. **Hasil**
2. Pengujian serangan menggunakan dataset

Pada tahapan ini snort akan melakukan full scan pada dataset yang digunakan untuk memberikan *alert* pada paket-paket yang di anggap mencurigakan dan terindikasi sebagai *traffic botnet-rats*. Berikut ini adalah *alert* yang didapatkan oleh *snort engine*.



Gambar 2 Alert yang didapatkan oleh *snort engine*

Setelah didapatkan alert ini, penulis melakukan perbandingan antara snort, dataset yang telah di ekstrak, dan paket yang ada pada wireshark.



Gambar 3 Alert snort



Gambar 4 Feature extraction



Gambar 5 Paket wireshark

Pada ketiga gambar tersebut terlihat bahwa paket yang didapatkan dari snort ada pada *feature extraction* dan wireshark.

1. **Kesimpulan**
2. Penggunaan snort engine cukup baik dalam mendeteksi traffic botne.
3. Program ini baru sebatas IDS dan dan belum dijadikan IPS, sehingga hanya bisa mendeteksi serangan-serangan yang tercatat pada rule.
4. Hasil pengujian menunjukkan bahwa semakin banyak data pengujian program IDS akan semakin akurat dalam mendeteksi serangan.

**DAFTAR PUSTAKA**

[1] P. Jyotiyana and S. Maheshwari, “A Literature Survey on Malware and Online Advertisement Hidden Hazards,” pp. 449–460, 2016.

[2] R. Tahir, “A Study on Malware and Malware Detection Techniques,” no. March, pp. 20–30, 2018.

[3] Cvedetails.com, “Browse cve vulnerabilities by date,” 2019. [Online]. Available: https://www.cvedetails.com/browse-by-date.php. [Accessed: 01-Dec-2019].

[4] A. Sawant, “A Comparative Study of Different Intrusion Prevention Systems,” *Proc. - 2018 4th Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2018*, pp. 1–5, 2019.

[5] S. Das and M. J. Nene, “A survey on types of machine learning techniques in intrusion prevention systems,” *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2296–2299, 2018.

[6] A. A. Awad, S. G. Sayed, and S. A. Salem, “Collaborative Framework for Early Detection of RAT-Bots Attacks,” *IEEE Access*, vol. 7, pp. 71780–71790, 2019.

[7] L. Xiangyu, “Kernel Malware Core Implementation : A Survey,” 2015.

⁠