Jurnal Teknik Informatika (JUTIF)
Vol. 3, No. 2, April 2022, hlm. 249-253

DOI: https://doi.org/10.20884/1.jutif.2022.3.2.117
p-ISSN: 2723-3863
e-ISSN: 2723-3871

NETWORK SECURITY MONITORING WITH INTRUSION DETECTION SYSTEM

Muhammad Anis Al Hilmi[*1], Emah Khujaemah[2]

[1]Prodi Teknik Infromatika, Jurusan Teknik Informatika, Politeknik Negeri Indramayu, Indonesia
[2]Prodi Rekayasa Perangkat Lunak, Jurusan Teknik Informatika, Politeknik Negeri Indramayu, Indonesia
Email: [1]alhilmi@polindra.ac.id, [2]khuza.emah24@gmail.com

(Naskah masuk: 21 Januari 2022, Revisi : 25 Februari 2022, diterbitkan: 25 April 2022)

Abstract

Computer network security is an issue that needs attention, along with the valuable and confidential information that passes through the network. The increasing use of networked computer systems has also led to an increase in cybercrimes worldwide, including Indonesia. The types of attacks carried out vary and go through several phases. Among the initial phases of the attack is the port scanning process. The process uses specific programs, such as Nmap (Network Mapper), to check on the target/victim side which ports are open and can be exploited for further attacks. IDS (Intrusion Detection System) is here to anticipate external attacks; IDS is used to detect suspicious activity in the system or network. This study aims to create a computer network security system that is lightweight, based on open-source, easy to set up, and can be analyzed by administrators by using Maltrail. Maltrail itself is a monitoring service used to detect dangerous traffic/traffic in a computer network, by utilizing a blacklist containing a list of dangerous or suspicious elements/sources. This study describes the stages of Maltrail installation and how Maltrail can detect the suspicious network, in this case, the port scanning business using Nmap. As a result, Maltrail can be relied on to log and notify network administrators of illegal system entry attempts/intrusions when there is a port scanning process from outside. Thus, it is hoped that with the existence of IDS, handling of an attack can be carried out earlier and prevent fatal consequences.

Keywords: *Intrusion Detection System, Maltrail, Network Security, Nmap, Port Scanning.*

PEMANTAUAN KEAMANAN JARINGAN DENGAN SISTEM DETEKSI INTRUSI

Abstrak

Keamanan jaringan komputer merupakan isu yang perlu diperhatikan, seiring dengan berharga dan rahasianya informasi yang melewati jaringan. Dengan meningkatnya penggunaan jaringan sistem komputer, hal ini membuat meningkat pula kejahatan siber di seluruh dunia, termasuk Indonesia. Tipe serangan yang dilakukan bermacam-macam dan melalui beberapa fase. Di antara fase awal serangan adalah proses *port scanning*. Proses tersebut menggunakan program tertentu, seperti Nmap (*Network Mapper*) untuk memeriksa di sisi target/korban, *port* mana yang terbuka dan dapat dimanfaatkan untuk serangan lebih lanjut. IDS (*Intrusion Detection System*) hadir untuk mengantisipasi adanya serangan dari luar, IDS digunakan untuk mendeteksi aktifitas mencurigakan dalam sistem atau jaringan. Penelitian ini bertujuan menciptakan sistem keamanan jaringan komputer yang ringan, berbasis *open source*, mudah diatur, dan dapat dianalisis oleh administrator, yaitu dengan menggunakan Maltrail. Maltrail sendiri adalah sebuah *service monitoring* yang digunakan untuk mendeteksi lalu lintas/*traffic* berbahaya dalam suatu jaringan komputer, dengan memanfaatkan *blacklist* yang berisi daftar unsur/sumber berbahaya atau mencurigakan. Dalam penelitian ini dijelaskan tahapan instalasi Maltrail dan bagaimana Maltrail dapat mendeteksi jaringan yang mencurigakan tersebut, dalam hal ini usaha *port scanning* menggunakan Nmap. Hasilnya, Maltrail dapat diandalkan untuk mencatat log dan memberi tahu bagian administrator jaringan jika ada usaha masuk sistem secara ilegal/*intrusion* ketika ada proses *port scanning* dari luar. Dengan demikian, harapannya dengan adanya IDS, penanganan atas sebuah serangan bisa dilakukan lebih awal dan mencegah akibat yang fatal.

Kata kunci: *Intrusion Detection System, Keamanan Jaringan, Maltrail, Nmap, Port Scanning.*

1. PENDAHULUAN

Banyak jalan yang dapat dieksploitasi oleh para pelaku kriminal siber. Mereka memanfaatkan celah keamanan demi mencuri data atau mengambil keuntungan dari peretasan ke dalam sistem. Para peretas memanfaatkan ketidaksiapan dari pengelola web maupun pengguna web itu

sendiri. Salah satu cara untuk mengantisipasi adanya peretasan, adalah menggunakan deteksi intrusi [1]. IDS (*Intrusion Detection System*) dapat diartikan sebagai *software*, *hardware*, atau gabungan keduanya. Yang jelas fungsinya adalah sebagai sistem pendeteksi adanya *intrusion*/usaha masuk ke sebuah sistem secara ilegal.

Intrusion adalah aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan memonitor lalu lintas data pada sebuah jaringan atau mengambil data dari berkas *log*.[2] Tujuan ilegal ini misalnya ingin mengumpul informasi tentang *internal system*, jaringan, sistem operasi, *software* dan komponen lain yang ada pada suatu sistem. Hal ini dilakukan orang atau organisasi (dapat berasal dari eksternal dan juga internal) yang tidak bertanggung jawab untuk kemudian melakukan penyalahgunaan atau penyerangan terhadap sistem. Cara IDS melakukan deteksi adalah dengan mengamati aktifitas yang ada pada sistem, utamanya oleh pengguna/*user*. IDS akan memberikan *alert*/tanda peringatan ketika ada aktifitas yang mencurigakan.

IDS melengkapi *firewall* dengan melakukan pemeriksaan pada paket *header* dan kontennya sehingga melindungi sistem serangan, yang mungkin oleh *firewall* dianggap sebagai lalu lintas "normal" – tidak berbahaya dalam jaringan. Jadi, IDS ini adalah pengamanan lapis ke-2. *Firewall* bekerja dengan melihat *rule*/aturan [9], apakah suatu paket dibolehkan lewat atau dilarang. Dalam melakukan pengecekan, *firewall* hanya memeriksa *header* paket dari protokol TCP/IP seperti FTP, HTTP, atau Telnet. Jadi *firewall* tidak memeriksa isi konten yang lewat, meskipun ternyata data yang melewatinya mengandung kode berbahaya.

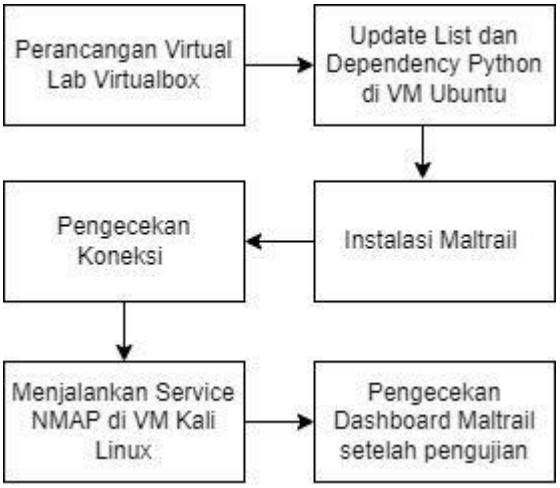
Server dengan IDS akan dapat mendeteksi seluruh aktivitas *port scanning* yang dilakukan dari internet menuju ke jaringan dalam (intranet). Kemampuan IDS dalam mendeteksi seluruh aktivitas *port scanning* adalah karena IDS ditempatkan pada komputer yang menjadi *gateway* dan sekaligus difungsikan sebagai *firewall*. Penempatan IDS pada *server gateway* ini akan melindungi data yang ada di *server gateway* dari serangan *hacker*. Selain itu, IDS juga dapat ditempatkan pada *host* tertentu yang penting untuk dilindungi, misalnya *web server* atau FTP *server*, agar dapat melindungi data pada *host* tersebut jika serangan yang dilancarkan lolos dari pengawasan IDS yang ditempatkan pada *server gateway*.[2] IDS berdasarkan kedudukan/posisinya, dibagi menjadi 2 yaitu:

- *Network* IDS (NIDS): memantau lalu lintas jaringan
- *Host* IDS (HIDS): melindungi di sisi *end system* atau sumber jaringan [14].

Penelitian ini juga memperjelas [8] dan [15] dalam penginstalan *service* Maltrail dan tahapan pengujiannya.

2. METODE PENELITIAN

Tahapan penelitian dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

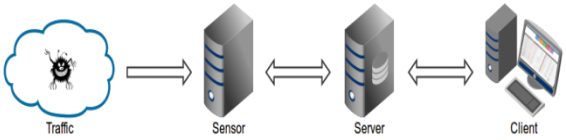
Penelitian ini diawali dengan pembuatan *Virtual Lab* dengan *software* Virtual Box, yaitu menggunakan Sistem Operasi Ubuntu sebagai target serangan dan Kali Linux sebagai penyerang. Untuk penginstalan Maltrail, dilakukan update Ubuntu dan *dependency* Python. Ada dua file Maltrail yang dijalankan, yaitu *sensor.py* untuk *client* dan *server.py* untuk *server*-nya. Kemudian *dashboard* Maltrail bisa dijalankan.

Setelah konfigurasi Maltrail di Ubuntu selesai, kemudian Kali Linux dapat dijalankan sebagai penyerang dengan memastikan koneksi jaringan berjalan lalu jalankan *scanning service* Nmap. Kemudian cek hasil *scanning* dengan membuka *browser* dengan URL alamat IP Ubuntu *server* dengan port 8338, menjadi 10.0.2.6:8338 di *dashboard* Maltrail.

2.1. Arsitektur Sistem

Maltrail didasarkan pada Traffic → Sensor <-> Server <-> Client arsitektur [3]. Sensor adalah komponen mandiri yang berjalan pada *node* pemantauan (misalnya *platform* Linux terhubung secara pasif ke SPAN/*mirroring port* atau *inline* secara transparan pada *bridge* Linux) atau pada mesin yang berdiri sendiri (misalnya *honeypot*) di mana ia "memantau" lalu lintas yang lewat untuk *item*/jejak yang masuk daftar hitam (yaitu nama *domain*, URL, dan/atau IP). Dalam kasus *true positive*, ia mengirimkan detail *event* ke *server* (pusat) di mana mereka disimpan di dalam direktori *logging*. Jika sensor dijalankan pada mesin yang sama dengan *server* (konfigurasi *default*), *log* disimpan langsung ke direktori *logging* lokal. Jika

tidak, mereka akan dikirim melalui pesan UDP ke *server*.



Gambar 2. Arsitektur Sistem

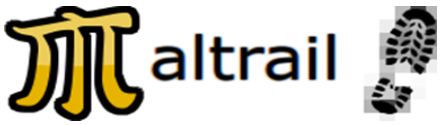
Peran utama *server* adalah menyimpan *detail event* dan menyediakan dukungan *back-end* untuk aplikasi *web* pelaporan. Dalam konfigurasi *default*, *server* dan sensor akan berjalan pada mesin yang sama. Laporan akhir dibuat dalam bentuk yang sangat padat, yang secara praktis memungkinkan penyajian jumlah *event* yang hampir tidak terbatas.

2.2. IDS

Intrusion Detection System (IDS) adalah sistem pencegahan dengan menggunakan *software* atau *hardware* yang bekerja secara otomatis untuk memonitor keadaan pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan. IDS adalah *tools*, metode, dan sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan computer [3][13].

2.3. Maltrail

Maltrail adalah sistem pendeteksi lalu lintas berbahaya, memanfaatkan daftar publik (hitam) yang berisi jalur berbahaya atau secara umum mencurigakan, bersama dengan jejak statis yang dikumpulkan dari berbagai laporan *Anti-Virus* dan daftar yang ditetapkan pengguna khusus, jejak tersebut dapat berupa nama *domain*, URL, dan alamat IP [3].



Gambar 3. Logo Maltrail

2.4. Python

Python adalah bahasa pemrograman yang memungkinkan Anda bekerja lebih cepat dan mengintegrasikan sistem Anda lebih efektif.. Tidak seperti bahasa lain yang susah untuk dibaca dan dipahami, python lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks [4].

Gambar 4. Logo Python

2.5. Pcapy

Pcapy adalah modul ekstensi Python yang berinteraksi dengan libpcap paket *capture library*. Pcapy memungkinkan skrip python untuk menangkap paket pada jaringan [5]. Pada Gambar 5, ditunjukkan tampilan penginstalan pcapy dalam Sistem Operasi Ubuntu.

Gambar 5. Contoh Tampilan Penginstalan Pcapy

2.6. Nmap

Nmap adalah alat yang digunakan untuk mengetahui *service* yang diberikan oleh suatu komputer melalui *scanning port*. Nmap banyak digunakan penyerang untuk mengetahui *port* komputer korban yang aktif, kemudian menggunakan *port* yang aktif tersebut untuk masuk ke sistem komputer korban [6][12].

2.7. *Port Scanning*

Port scanning atau pemindaian port merupakan teknik untuk menemukan *port* dan layanan yang terbuka di sisi target. Ada berbagai jenis dalam teknik pemindaian ini. Sebetulnya teknik tersebut kebanyakan tidak berbahaya, tetapi beberapa di antaranya dimaksudkan dengan tujuan jahat. Ada sejumlah besar *port* yaitu 65.535 *port* TCP dan 65.535 *port* UDP. Nomor *port* mulai dari nol hingga 1024 adalah yang paling dikenal. Sebut saja, *port* 80 terkait dengan HTTP; *port* 21 dipetakan ke FTP, *port* 25 ke SMTP, dan sebagainya. Pemindaian port adalah metode pengintaian, memindai *host* untuk mendapatkan informasi *port* dan layanan yang terbuka. Teknik ini juga sering kali sekaligus mengirim pesan ke masing-masing *port* yang terbuka dan mendeteksi *port* mana yang bisa dibuka [10][11].

2.8. *Firewall*

Firewall adalah istilah yang biasa digunakan untuk menunjuk pada suatu komponen atau sekumpulan komponen jaringan, yang berfungsi membatasi akses antara dua jaringan, lebih khusus lagi, antara jaringan internal dengan jaringan global Internet. [7].

2.9. Virtual Box

Virtual Box adalah Teknik Virtualisasi merupakan istilah yang mengacu pada pembuatan

suatu versi maya/virtual (daripada versi actual), termasuk virtual machine, yang menyerupai mesin yang dapat menjalankan program layaknya seperti mesin actual/fisik sesungguhnya.

Oracle VM Virtual Box adalah salah satu aplikasi virtualisasi (*Hypervisor*), dimana dapat di-install pada komputer *Physical*, baik yang berbasis Intel maupun AMD, tidak membutuhkan fitur *processor* yang dibangun dalam *hardware* baru seperti Intel Vt-x atau AMD-V. Bahkan Oracle VM Virtualbox dapat digunakan pada *hardware/processor* lama yang tidak mendukung *hardware virtualization*. [8].

3. HASIL DAN PEMBAHASAN

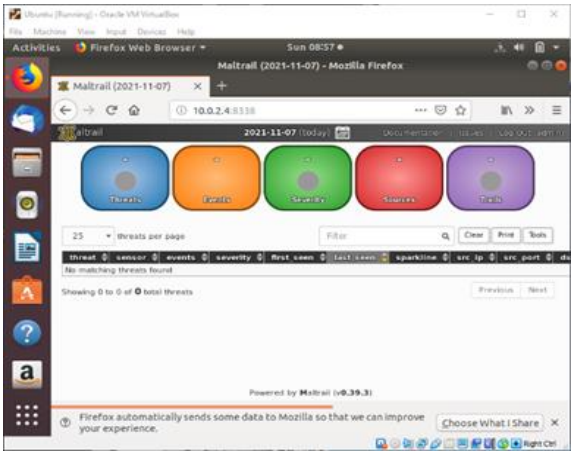
Penelitian ini membahas tentang bagaimana sistem pendeteksi mengetahui adanya *intrusion*/usaha masuk ke sebuah secara ilegal. *Intrusion* dapat diartikan dengan sesuatu yang tidak diinginkan, tidak memiliki hak akses yang sah, dan umumnya dengan tujuan tidak baik. Untuk itu penting untuk kita supaya mengetahui bagaimana cara mencegahnya.

1. Dalam penelitian ini, digunakan sistem operasi Ubuntu 18.04 (mode *virtual machine*) sebagai target, di dalamnya sudah ter-install Maltrail untuk mendeteksi serangan yang mungkin terjadi di sistem. Sedangkan untuk penyerang, menggunakan Kali Linux versi 2020 dengan mode *virtual machine*.
2. Alamat IP target dan penyerang masing-masing dicek dengan perintah ip a. Setelahnya dipastikan keduanya terhubung dengan masing-masing mengirimkan ping.

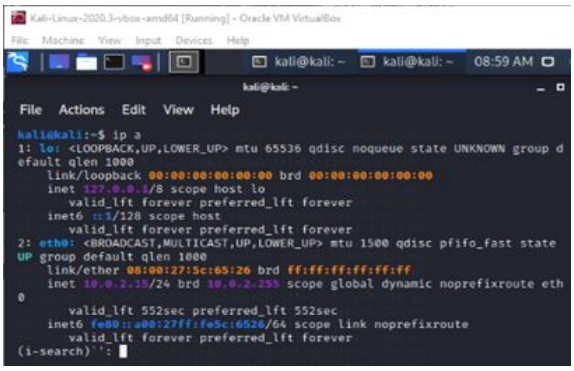
Gambar 6. Tangkapan Layar Desktop Linux Ubuntu

Setelah dijalankan Maltrail lewat CLI, kemudian lewat *browser* dengan memasukkan ip VM Ubuntu-nya kemudian tambah *port* untuk Maltrail. Contohnya : 10.0.2.4:8338

Setelah tampilan *dashboard* muncul dilakukan pengujian dengan penyerang yang menggunakan Sistem Operasi Kali Linux.



Gambar 7. Tangkapan Layar Dashboard Maltrail



Gambar 8. Tangkapan Layar cek IP

Setelah dipastikan sudah terhubung dilakukan uji serangan terhadap Ubuntu (target) menggunakan teknik *port scanning* dengan Nmap pada sisi Kali Linux (penyerang).

Gambar 9. Tangkapan Layar Cek Koneksi

Gambar 10. Tangkapan Layar Tampilan

Hasil Maltrail yang mendeteksi adanya usaha intrusi dari Nmap Kali Linux terlihat pada Gambar 10 (muncul grafik naik, dan ada ***alert*** warna merah).

4. KESIMPULAN

Setelah dilakukan perancangan, implementasi, dan pengujian, dapat dihasilkan kesimpulan sebagai berikut, bahwa *Intrusion Detection System* adalah sistem pencegahan dengan menggunakan *software* atau hardware yang bekerja secara otomatis untuk memonitor keadaan pada jaringan komputer dan dapat menganalisis masalah keamanan jaringan. Dari pengujian, didapatkan bahwa Maltrail dapat mendeteksi lalu lintas berbahaya dan adanya usaha dari luar yang melakukan *port scanning*, memanfaatkan daftar publik (hitam). Selain itu, dari hasil pengujian usaha intrusi dari Kali Linux, menggunakan Nmap dengan target Ubuntu, IDS Maltrail dapat mendeteksi dengan baik adanya usaha intrusi tersebut dengan menampilkan grafik naik dan peringatan berwarna merah. Hal ini dapat menjadi informasi bagi administrator jaringan untuk mencegah adanya kerusakan yang lebih fatal pada sistem/*server*.

DAFTAR PUSTAKA

[1] K. A. CAHYANTO, M. A. AL HILMI, and M. MUSTAMIIN, 'Pengujian Rule-Based pada Dataset Log Server Menggunakan Support Vector Machine Berbasis Linear Discriminat Analysis untuk Deteksi Malicious Activity', Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 9, no. 2, 2021.

[2] J. Gondohanindijo, 'Sistem Untuk Mendeteksi Adanya Penyusup (IDS: Intrusion Detection System)', Majalah Ilmiah INFORMATIKA, vol. 2, no. 2, 2011.

[3] M. Kasimov, 'Maltrail; Malicious traffic detection system', 2016. https://github.com/stamparm/maltrail.

[4] V. Siahaan and R. H. Sianipar, Konsep dan Implementasi Pemrograman Python. SPARTA PUBLISHING|, 2019.

[5] J. M. Ortega, Mastering Python for Networking and Security. Packt Publishing, 2018.

[6] G. A. Sandag, J. Leopold, and V. F. Ong, 'Klasifikasi Malicious Websites Menggunakan Algoritma K-NN Berdasarkan Application Layers dan Network Characteristics', CogITo Smart Journal, vol. 4, no. 1, pp. 37–45, 2018.

[7] E. Mulyana and O. W. Purbo, 'Firewall: Sekuriti Internet', Computer Network Research Group, ITB, Bandung, 2000.

[8] H. Hudzaifah, A. Sularsa, and D. R. Suchendra, 'Membangun Sistem Monitoring Malicious Traffic Di Jaringan Dengan Maltrail', eProceedings of Applied Science, vol. 4, no. 3, 2018.

[9] M. A. A. Hilmi, Superlab cybersecurity : pengantar keamanan komputer dengan praktikum. Manggu Makmur Tanjung Lestari, 2021.

[10] M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan and Ata-ur-rehman, "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool," 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2019, pp. 1-6, doi: 10.1109/ICOMET.2019.8673520.

[11] S. K. Patel and A. Sonker, "Internet Protocol Identification Number Based Ideal Stealth Port Scan Detection Using Snort," 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), 2016, pp. 422-427, doi: 10.1109/CICN.2016.89.

[12] R. R. Rohrmann, V. J. Ercolani and M. W. Patton, "Large scale port scanning through tor using parallel Nmap scans to scan large portions of the IPv4 range," 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 185-187, doi: 10.1109/ISI.2017.8004906.

[13] A. Borkar, A. Donode and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," 2017 International Conference on Inventive Computing and Informatics (ICICI), 2017, pp. 949-953, doi: 10.1109/ICICI.2017.8365277.

[14] K. A. Cahyanto, M. A. A. Hilmi, M. Mustamiin, and N. Qonita, Deteksi Intrusi Menggunakan Python: Implementasi Machine Learning untuk Analisis Keamanan Server. Penerbit Manggu Makmur Tanjung Lestari, 2020.

[15] A. Katkar, S. Shukla, D. Shaikh and P. Dange, "Malware Intrusion Detection For System Security," 2021 International Conference on Communication information and Computing Technology (ICCICT), 2021, pp. 1-5, doi: 10.1109/ICCICT50803.2021.9510161.