OPEN ACCESS
J. OF INISTA, VOL. 4, NO. 2, PP.032-045, MEI 2022

ISSN : 2622-8106 (ONLINE)
DOI: 10.20895/INISTA.V4I2

Journal of Informatics, Information System, Software Engineering and Applications

Implementasi HoneyPy Dengan *Malicious Traffic Detection System* (Maltrail) Guna Mendeteksi Serangan DOS Pada Server

Halim Alfidzar [#1], Bita Parga Zen [#2]

[#1,2]*Teknik Informatika*
[#1,2]*Institut Teknologi Telkom Purwokerto*
JL. D.I Panjaitan 128 Purwokerto, Jawa Tengah, Indonesia

[1] 18102195@ittelkom-pwt.ac.id
[2] bita@ittelkom-pwt.ac.id

Penulis korespondensi : bita@ittelkom-pwt.ac.id

accepted on 26-04-2022

Abstrak

Pada era sekarang ini, masih banyak serangan terhadap server yang membuat server akan mengalami kerusakan sistem operasi. Contoh yang sering ditemukan adalah serangan DoS. Dalam pencegahan, diperlukan keamanan atau referensi untuk mendukung keamanan server. Keamanan terhadap jaringan dan server merupakan hal yang sangat penting, karena sudah banyak serangan dilakukan oleh pihak yang tidak bertanggungjawab. Sehingga diperlukan suatu penanganan yang dapat menganalisis serangan terhadap beberapa ancaman. HoneyPy dengan Maltrail merupakan aplikasi yang bersifat *open source* yang bisa digunakan untuk metode pembuktian pada penelitian. Terdapat CentOs yang digunakan sebagai server tambahan dan Linux Mint sebagai server utama. Serangan-serangan yang dilakukan pada penelitian ini dilakukan oleh peneliti sendiri pada server menggunakan serangan DoS. Data yang dikumpulkan dari maltrail sudah dianalisis menggunakan analisis deskriptif, hasil penelitian ini yaitu HoneyPy dengan Maltrail mampu menjadi tolak ukur untuk digunakan sebagai peningkatan keamanan pada serangan di bagian server. Berdasarkan pengujian didapatkan bahwa hasil berupa lima laporan didapatkan tiga threats, enam events, severity terdeteksi low dan medium, satu sumber ancaman pada sources, dan empat trails.

Kata Kunci: Keamanan, Server, Maltrail, HoneyPy, DoS.

I. PENDAHULUAN

Kemajuan teknologi internet telah menjadikannya sebagai media utama untuk bertukar data. Tidak semua informasi tersedia untuk khalayak umum. Internet merupakan jaringan komputer publik yang bertindak sebagai pencegahan ekstra harus dilakukan untuk melindungi data dari kejahatan. Seseorang yang ahli dalam meretas atau meretas mekanisme keamanan jaringan komputer disebut sebagai hacker. Salah satu yang terjadi indonesia berdasarkan hasil monitoring yang dilakukan terhadap sistem elektronik yang berkaitan dengan penyelenggaran PON XX, tercatat terdapat sekitar 112.762.000 akses ke domain-domain yang berkaitan dengan PON 2021 Anomali trafik lainnya yang tercatat berdasarkan hasil pantauan BSSN berkaitan dengan sistem elektronik yang

berkaitan dengan penyelenggaraan PON XX 2021 yakni adanya percobaan DdoS (*Distributed Denial of Service*) [1].

Gambar 1. Traffic Serangan Ddos PON XX 2021

Terlepas dari kenyataan bahwa beberapa server telah menetapkan keamanan sesuai dengan persyaratan yang berlaku, mengingat dinamika peretasan global, masih ada risiko peretasan. Keamanan jaringan harus dijaga dari semua jenis serangan, bahkan yang tidak diketahui asal-usulnya. Tindakan sistem sebagai penyerang untuk mendapatkan akses dan data sensitif. Akibatnya, diperlukan sistem yang dapat mengidentifikasi serangan atau mengumpulkan informasi tentang penyerang dan pola intrusi tanpa menyebabkan kerusakan pada server [2].

Honeypot merupakan sistem yang diatur untuk menjadi target peretas, dan juga dapat digunakan untuk mengalihkan serangan ke sesuatu yang lebih penting atau berharga. Sistem tersebut dapat digunakan untuk membantu untuk mengelabui penyerang dalam membobol server [3]. Tujuan menemukan situs *web* yang rentan, penyerang akan memindai jaringan terlebih dahulu. Jika penyerang terhubung, *honeypot* akan segera melihat dan merekam tindakan secara langsung tidak diperlukan interaksi pengguna. Kemudian cara memanfaatkan *honeypot* lakukan konfigurasi terlebih dahulu di server sehingga jika ada penyerang yang menyerang akan segera merekam dan menampilkan semua informasi yang mungkin dari permintaan yang diinginkan. Untuk mengatasi situasi yang masih merepotkan dari segi keamanan jaringan, Dapat juga menggunakan *firewall*, tetapi hanya untuk memblokir jaringan yang digunakan oleh penyerang sehingga tidak dapat mengetahui apa yang sedang terjadi dan pola serangan digunakan.

Serangan yang paling umum yaitu *Port Scanning* dan DoS (Denial Of Service). *Port Scanning* merupakan serangan yang mencoba mendeteksi *port* yang terbuka pada jaringan komputer. Dalam pemindaian dapat digunakan untuk mengidentifikasi kelemahan jaringan komputer. DOS merupakan jenis serangan yang melibatkan pengiriman permintaan secara terus-menerus ke server sehingga server tetap sibuk dalam menanggapi *request* yang menyebabkan sistem mengalami kerusakan [4]. Server merupakan sistem komputer yang menyediakan penyimpanan data dan layanan lainnya. Informasi dan bentuk dokumen komplek lainnya merupakan salah satu jenis data yang disimpan di server serta dapat digunakan untuk implementasi sistem low interaction honeypot yang dapat ditargetkan tanpa membahayakan server asli [5]. HoneyPy sebagai pilihan honeypot dikarenakan peneliti melakukan perbandingan atau pembuktian metode dengan cara menambahkan *port* yang mudah diserang oleh penyerang sehingga aktivitas ditangkap dengan baik. Oleh karena itu, dibangunlah sebuah keamanan yaitu sistem honeypot yang dipasang di server untuk berpura-pura sebagai jebakan penyerang dan merekam permintaan yang dimaksud pada Maltrail.

Dalam penelitian ini menggunakan *malicious traffic detection system* (Maltrail) yang merupakan aplikasi bersifat open source. Langkah awal yang dilakukan install 3 server yaitu Kali Linux, Linux Mint, dan CentOs dan menerapkan Maltrail yang diberi tidak diberi dan diberi pertahanan menggunakan HoneyPy pada Linux Mint serta mencoba untuk melakukan serangan DoS dengan Kali Linux. Langkah terakhir menganalisis pada bagian Maltrail dengan menggunakan analisis deskriptif. Dengan masih adanya ancaman di dunia maya seperti beberapa situs yang mengalami kebocoran data, tentunya serangan tersebut akan memiliki dampak buruk bagi negara maupun masyarakat. Oleh karena itu, penulis mengimplementasikan serta menganalisis bagaimana

HoneyPy dengan Maltrail bisa bekerja dengan baik untuk keamanan sebuah server.

II. DASAR TEORI

A. Penelitian Sebelumnya

Dalam melakukan penelitian, literatur yang ada berupa karya tesis dan publikasi sebelumnya yang relevan dengan topik yang diteliti. Penelitian [6] membahas penggunaan honeyd dengan iptables, yang digunakan untuk menguji berbagai serangan di jaringan lokal, termasuk pemindaian host, DoS, dan Ddos. Honeyd mampu mengidentifikasi serangan yang dilakukan oleh Netscan android saat memindai host di jaringan dalam pengujian. Honeyd digunakan untuk membuat dan menjalankan host virtual di jaringan komputer, serta mendeteksi serangan oleh penyerang, saat dikonfigurasi. Untuk mencegah dan menghentikan serangan pada server menggunakan arsitektur sistem iptables yang sudah dikonfigurasi. Sedangkan penelitian [7] membahas CAIDA DDoS Attack 2007 dan data simulasi diri yang digunakan untuk mengumpulkan data pelatihan dan pengujian. Persentase rata-rata pengenalan tiga keadaan jaringan (normal, DDoS lamban, dan DDoS) adalah 90,52 persen dalam pengujian menggunakan teknik analisis statistik log jaringan dengan fungsi jaringan saraf sebagai metode deteksi. Pengenalan metode baru untuk mendeteksi serangan DDoS dimaksudkan untuk menjadi pelengkap Intrusion Detection System (IDS) dalam hal mengantisipasi terjadinya serangan DDoS. Dan juga pada penelitian [8] membahas dalam membangun sistem monitoring malicious traffic di Jaringan dengan Maltrail. Dalam hal ini melakukan pembuatan topologi jaringan berdasarkan satu jaringan yang sama. Hasil pengujiannya untuk menemukan sebuah malware di dalam jaringan sehingga bisa terdeteksi oleh Maltrail.

B. Insiden Keamanan Jaringan

Keamanan jaringan merupakan topik hangat saat ini, dan semakin berkembang. Kemajuan teknologi komputer memberikan banyak keuntungan, tetapi juga memiliki banyak kelemahan. Serangan terhadap sistem komputer yang terhubung ke internet adalah salah satunya. Banyak sistem atau jaringan komputer yang dirugikan atau diretas akibat serangan tersebut [9]. Keamanan jaringan komputer terdiri dari empat komponen utama: perangkat lunak, perangkat keras jaringan, layanan Internet of Things, dan sumber daya bersama. Keamanan jaringan komputer seperti yang didefinisikan oleh Organisasi Internasional untuk Standardisasi yang merupakan perlindungan perangkat keras, perangkat lunak, dan sumber daya data dalam sistem komputer dari kehancuran, perubahan atau lubang keamanan karena alasan yang tidak disengaja atau berbahaya sehingga sistem komputer dapat terus berfungsi dengan aman. terpercaya, dan layanan komputer juga tersedia secara berkala. Pengguna dapat membuat jaringan komunikasi menggunakan peralatan jaringan seperti router, hub, switch, dan kabel.

Jaringan komputer telah berkembang menjadi alat penting untuk komunikasi dan penyimpanan data dalam berbagai format dan lokasi. Berbagai penelitian telah menunjukkan bahwa sistem jaringan komputer sangat rentan terhadap beberapa serangan, dan keamanan jaringan meruapakan salah satu entitas paling dinamis untuk bisnis, dipengaruhi oleh perubahan tren teknologi dan pergeseran vektor ancaman dan aplikasi ancaman tingkat lanjut ke aplikasi yang lebih canggih [10]. Insiden keamanan jaringan merupakan serangan terhadap jaringan komputer yang memiliki pengaruh langsung atau tidak langsung terhadap keamanan sistem dan melanggar kebijakan keamanan sistem. Probe, scan, account compromize, root compromize, packet sniffer, denial of service, exploitation of trust, malicious code, dan infrastructure attacks merupakan contoh insiden.

C. DoS

DoS merupakan semacam serangan terhadap komputer atau server di jaringan internet yang menghabiskan sumber daya komputer hingga tidak dapat lagi menjalankan tugasnya dengan benar, mencegah pengguna lain mengakses layanan yang disediakan oleh komputer yang diserang. DoS pada penelitian ini menggunakan satu PC/Laptop untuk melakakukan serangan dengan bantuan tools seperti Virtual Box beserta OS Kali Linux.

D. Server

Dalam jaringan komputer, server merupakan sistem komputer yang menawarkan berbagai layanan. Server dilengkapi dengan sistem operasi tertentu dan memiliki RAM yang cukup. Server juga dapat menjalankan

aplikasi untuk mengelola akses dan sumber daya jaringan. Server DHCP, server Mail, server HTTP, server FTP, dan server DNS hanyalah beberapa contoh aplikasi server yang memanfaatkan arsitektur klien [8].

E. Honeypot

Honeypot merupakan perangkat keamanan rahasia yang digunakan untuk menarik penyusup untuk memberikan informasi sensitif. Untuk memastikan keberhasilan operasi, perlu untuk menyembunyikan identitasnya. *Honeypot* dimaksudkan untuk terlibat dengan penyerang untuk mempelajari lebih lanjut tentang mereka. Pada dasarnya, sebuah sistem yang dimaksudkan agar tampak seperti sistem aslinya untuk diserang dan belajar cara mengoperasikan atau menjebak penyerang [11].

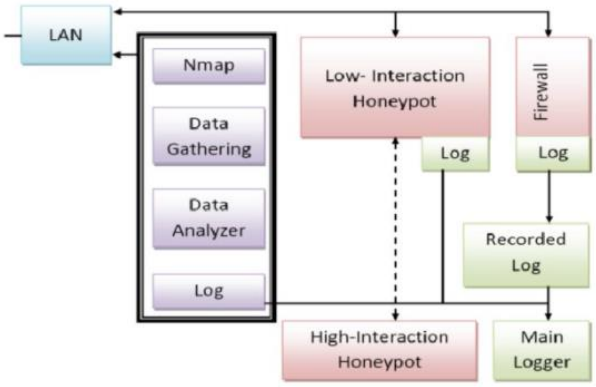
Terdiri dari 2 jenis *Honeypot* yaitu:

1. *Low Interaction Honeypot* (LIH)

Ini hanya meniru sejumlah layanan. Memasang listener pada port merupakan cara termudah untuk membuat layanan ini. Tidak ada sistem operasi asli di Low Interaction Honeypot untuk digunakan penyerang sebagai basis operasi. Karena kompleksitas sistem operasi telah berkurang, ini akan dapat sangat meminimalkan risiko. Honeypot dengan Interaksi Rendah mirip dengan koneksi satu arah.

2. *High Interaction Honeypot* (HIH)

Menyediakan sistem yang lengkap untuk berinteraksi. Artinya honeypot dengan tingkat interaktivitas yang tinggi tidak hanya mereplikasi layanan, fungsi, atau sistem operasi. Honeypot semacam ini mensimulasikan sistem dan layanan dunia nyata. Akibatnya, penyerang memiliki kendali penuh atas sistem honeypot. HIHAT adalah contoh aplikasi web honeypot dengan tingkat interaksi yang tinggi. HIHAT mengubah aplikasi PHP menjadi honeypot dengan interaksi tinggi [12].



Gambar 1. Alur Perbedaan LIH dan HIH

Alur perbedaannya pada letak tingkat keterlibatan pada sistem keamanannya, pada *Low Interaction Honeypot* hanya akan mengemulasikan sebagian service, sedangkan High Interaction Honeypot akan menggunakan keseluruhan dari resource sistem dimana Honeypot dibuat persis dengan sistem yang asli atau nyata dan juga menjadi keseluruhan pada sistem operasi seperti pada gambar 2.1.

F. HoneyPy

HoneyPy memiliki plugin yang disertakan. Fungsionalitas plugin menentukan jumlah keterlibatan. Lebih banyak interaktivitas dapat dicapai dengan membuat plugin yang mensimulasikan layanan berbasis UDP atau TCP. Secara default, setiap tindakan direkam dalam file. HoneyPy merupakan aplikasi honeypot kecil terbaru yang dapat diunduh dari github dan digunakan di komputer Linux atau Windows, akan digunakan dalam penelitian ini. Tujuan utama Honeypy yaitu mengirim data log kembali ke situs web HoneyPy. HoneyPy

dikembangkan dengan Python dan dirancang agar mudah dipasang dan digunakan, dengan kemampuan untuk menambahkan plugin dan menjalankan logger dengan pengaturan khusus [13].

G. Maltrail

Maltrail merupakan sistem deteksi lalu lintas berbahaya yang menggunakan daftar hitam yang dapat diakses publik dari jalur berbahaya dan umumnya mencurigakan, serta jejak statis dari laporan anti-virus yang berbeda dan daftar yang ditentukan pengguna khusus, di mana jejak tersebut dapat berkisar dari nama domain hingga alamat IP [14].

H. VirtualBox

VirtualBox merupakan program open source terkait virtualisasi. Virtualisasi yaitu teknologi yang memungkinkan untuk membangun komputer PC virtual yang dapat berfungsi secara independen dari sistem operasi. Komputer host mensimulasikan semua jenis perangkat keras yang terkait dengan mesin virtual. Jika seseorang ingin menguji dan meniru instalasi sistem tanpa kehilangan sistem yang ada, kemampuan ini sangat penting. Tampaknya kita dapat memiliki beberapa jenis perangkat PC dengan beberapa sistem operasi yang memanfaatkan VirtualBox tanpa harus memiliki peralatan yang sebenarnya [15].

I. Linux

Linux merupakan sistem operasi berbasis Unix yang tersedia secara bebas untuk umum dan diatur oleh GNU *General Public License* (GPL). Linux open-source ditawarkan dalam sejumlah distribusi, yang masing-masing mencakup satu set paket perangkat lunak yang dapat diinstal. Sangat penting untuk menjaga agar paket-paket ini tetap mutakhir untuk memanfaatkan fitur-fitur baru, perbaikan bug, dan patch keamanan [16]. Linux dikenal karena sistem operasinya yang dirancang terutama untuk server, serta keamanan akses data, sehingga masih dianggap sebagai sistem operasi yang mampu menembus dan melindungi jaringan. Berikut ini adalah sistem operasi yang digunakan dalam penelitian ini:

1. Kali Linux

Kali Linux adalah sistem operasi berbasis Debian yang dibangun oleh Offensive Security sebagai pengganti BackTrack, distribusi Linux perusahaan induknya. Perangkat lunak pengujian penetrasi untuk komputer. Dan juga sistem operasi open source yang tersedia secara bebas untuk umum dan dirancang untuk berbagai aktivitas keamanan informasi seperti pengujian penetrasi, penelitian keamanan, forensik komputer, dan rekayasa balik. Ada juga berbagai alat di Kali Linux yang dapat digunakan untuk pengujian dalam penelitian keamanan [17]. Dalam hal ini peneliti menggunakan Kali Linux untuk melakukan simulasi serangan terhadap server.

2. CentOs

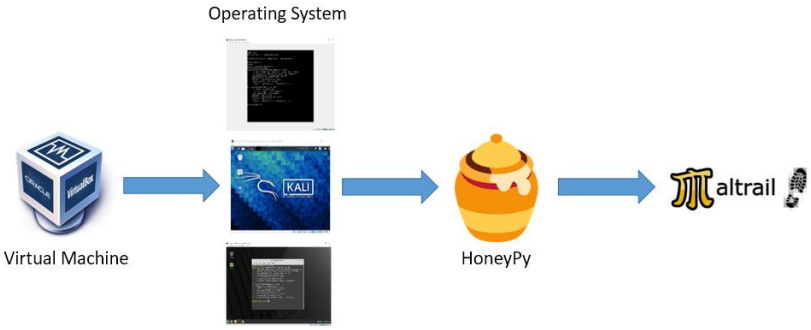
CentOS merupakan sistem operasi gratis berdasarkan kernel Linux yang pertama kali diterbitkan pada Mei 2004. RHEL adalah tempat CentOS dimulai. "Gregory Kurtzer" menciptakan CentOS, yang pertama kali dirilis sebagai build CAOS. Platform pengembangan yang merupakan salah satu distribusi terbaik dan paling kuat yang tersedia. Ini adalah proyek perangkat lunak bebas berbasis komunitas yang bertujuan untuk menciptakan fondasi yang stabil bagi komunitas open source untuk berkembang. Dan juga mencakup beberapa peningkatan keamanan tingkat perusahaan serta menjadikannya solusi yang fantastis untuk aplikasi apa saja [18]. Pada penelitian ini CentOs8 menjadi server tambahan yang berguna untuk dilakukannya sebuah uji coba serangan.

3. Linux Mint

Linux Mint merupakan distribusi berbasis Ubuntu dengan tujuan memberikan pengalaman desktop tradisional dengan berbagai alat yang berguna, unik dan kemampuan multimedia out-of-the-box. Desktop dan menu yang dipesan lebih dahulu, serta berbagai alat konfigurasi unik dan antarmuka instalasi paket berbasis web, semuanya disertakan. Repositori perangkat lunak Ubuntu kompatibel dengan Linux Mint [19]. Pada penelitian ini Linux Mint digunakan sebagai server utama dengan menerapkan sistem HoneyPy dan Maltrail.

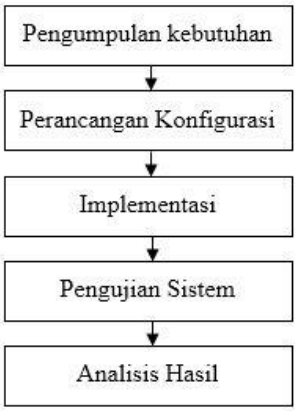
III. METODE PENELITIAN

Berdasarkan proses elaborasi pengumpulan data, penelitian ini menggunakan tiga server untuk melakukan pembuktian metode dalam implementasi secara virtual. Awal pertama yang dilakukan menggunakan VirtualBox sebagai virtual machine yang diinstall berbagai OS seperti server yang pertama yaitu Kali Linux untuk melakukan serangan terhadap beberapa server lainnya dengan tiga serangan DoS, bagian kedua yaitu CentOs sebagai server tambahan untuk dilakukan uji coba, dan bagian ketiga yaitu Linux Mint sebagai server utama dalam penerapan HoneyPy dengan Maltrail yang sudah dikonfigurasi. Berikutnya membandingkan serangan yang didapatkan ketika sudah menggunakan HoneyPy maupun belum menggunakannya. Langkah terakhir menganalisis pada bagian Maltrail.



Gambar 1. Arsitektur

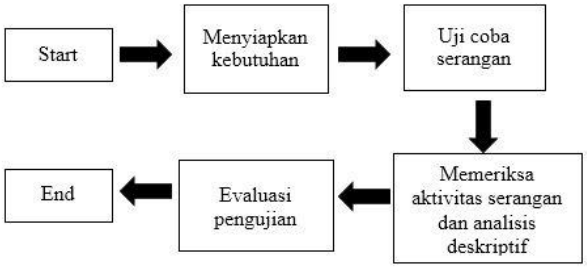
Dalam penelitian ini melakukan beberapa tahapan penelitian yang sudah ditentukan. Berikut merupakan gambar tahapan yang dilakukan:



Gambar 2. Diagram Alir Penelitian

Tahap perancangan sistem merupakan tindak lanjut terhadap data yang diperoleh. Pada tahap perancangan konfigurasi sistem yaitu membuat server utama dengan OS Linux Mint serta konfigurasi HoneyPy dengan Maltrail sebagai tempat menampung serangan terhadap Kali Linux serta dapat menangkap aktivitas serangan menggunakan Maltrail dan juga hasil analisis deskriptif yang ditampilkan.

Implementasi Tahap ini merupakan tahap tindak lanjut dari perancangan sistem dengan melakukan instalasi virtualbox, kali linux, linux mint, matrail dan melakukan Pengujian Sistem



Gambar 3. Diagram Alir Pengujian

IV. HASIL DAN PEMBAHASAN

Berdasarkan proses elaborasi pengumpulan data, penelitian ini menggunakan tiga server untuk melakukan pembuktian metode dalam implementasi secara virtual. Server yang pertama yaitu Kali Linux untuk melakukan serangan terhadap beberapa server lainnya dengan tiga serangan DoS, bagian kedua yaitu CentOs sebagai server tambahan untuk dilakukan uji coba, dan bagian ketiga yaitu Linux Mint sebagai server utama dalam penerapan HoneyPy dengan Maltrail yang sudah dikonfigurasi.

A. Pengelolaan Jaringan

Dalam proses pengelolaan jaringan, peneliti menggunakan suatu protokol DHCP yang merupakan layanan bersifat otomatis dalam pemberian nomor IP kepada setiap server. Pada bagian network untuk setiap server menggunakan Bridge adapter untuk memakai jaringan yang ada pada PC seperti Wifi. Bridged Adapter digunakan jika ingin bisa terkoneksi dengan jaringan nyata bukan virtual dan Qualcomm atheros merupakan nama driver untuk pengguna windows, pada setiap nama network berbeda-beda sesuai sistem operasi yang digunakan.

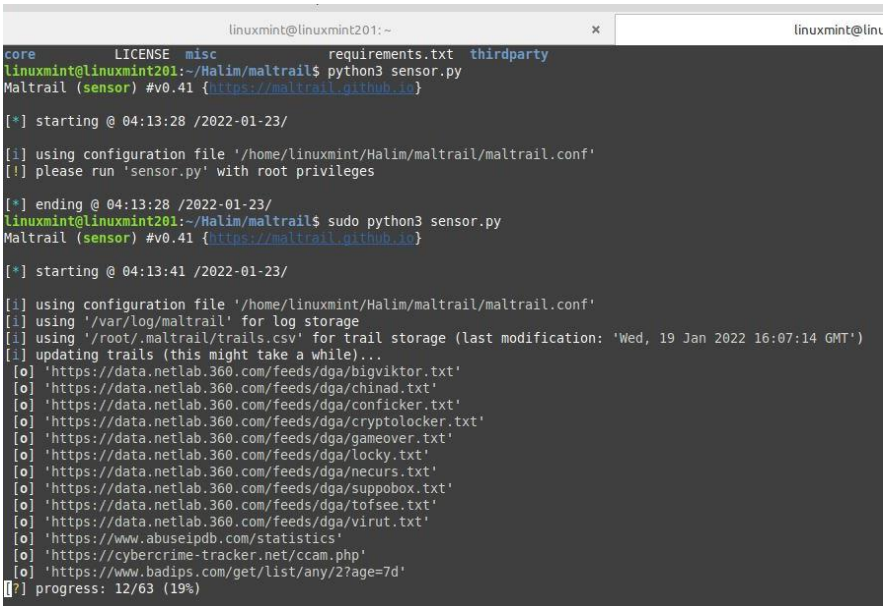
B. Pengecekan IP

Dalam proses pengecekan, peneliti menggunakan perintah ifconfig di setiap server. Ifconfig digunakan untuk konfigurasi antarmuka jaringan untuk memperoleh sebuah IP pada server. IP yang didapatkan pada pengujian kali ini mendapatkan IP Kali Linux 192.168.100.47, IP CentOs 192.168.100.48, dan IP Linux Mint 192.168.100.38.

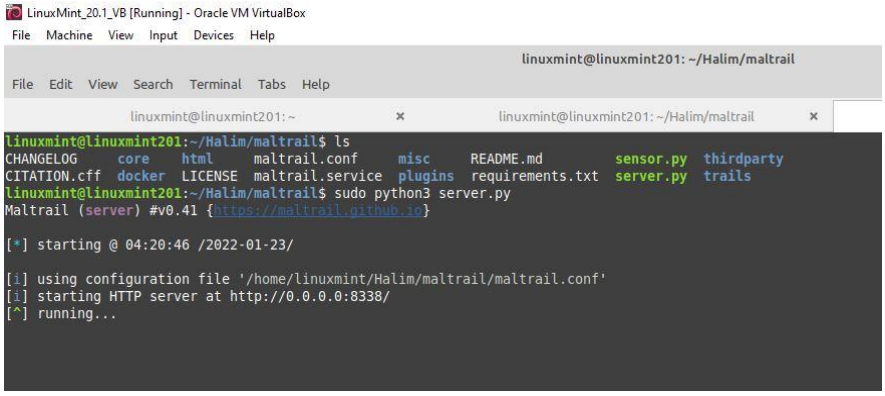
C. Konfigurasi

1. Maltrail

Pada proses ini terdapat dua langkah untuk menjalankan aplikasi bersifat open source. Bagian pertama jalankan terlebih dahulu sensor.py untuk mulai mengaktifkan data yang berada pada program sensor tersebut, selanjutnya bagian kedua jalankan server.py setelah sensor sudah running untuk menangkap atau menjalankannya di server Linux Mint.



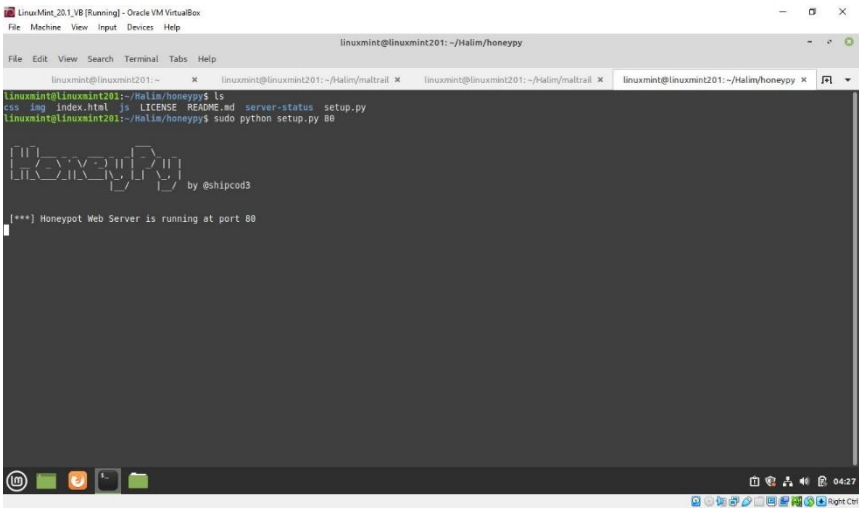
Gambar 1. Menjalankan Sensor.py



Gambar 2. Menjalankan Server.py

2. HoneyPy

Proses dilakukan dengan perintah “sudo python setup.py [port yang diinginkan]”. HoneyPy digunakan untuk membuat penyerang mengalami kesulitan dalam menemukan server utama yang ada dan dilakukan nantinya untuk membandingkan pada penggunaan HoneyPy dengan yang tidak menggunakannya.



Gambar 3. Menjalankan Setup.py

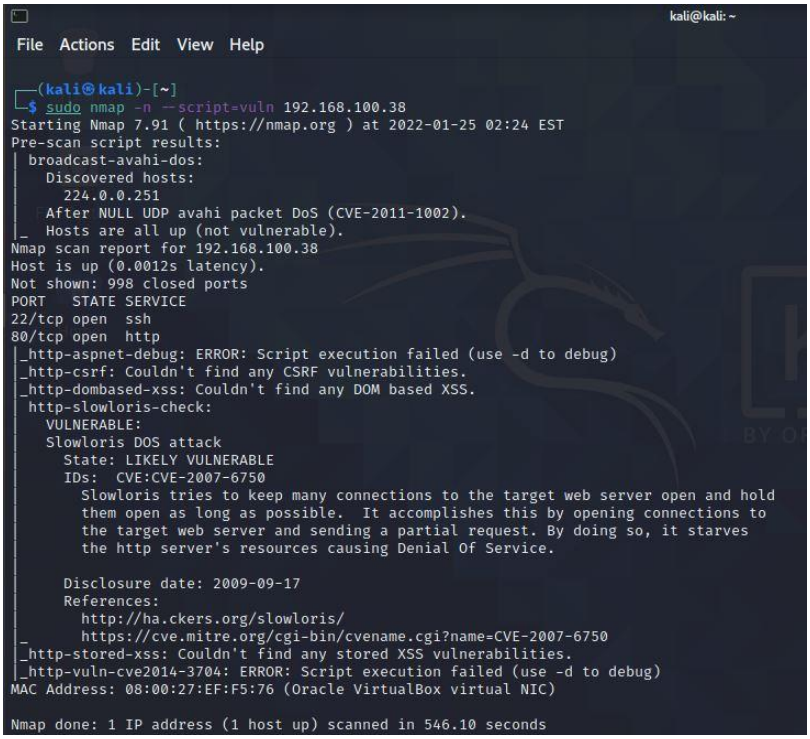
D. Hasil Serangan

TABLE I
HASIL SERANGAN

Aktivitas Pengujian	Hasil yang diharapkan	Hasil yang didapatkan	Kesimpulan
Scanning dengan NMAP (Belum diberikan HoneyPy)	Terdeteksi pada maltrail	Terdeteksi	Berhasil
Scanning dengan NMAP (Sudah diberikan HoneyPy)	Terdeteksi pada maltrail	Terdeteksi	Berhasil
DoS menggunakan PING yang sudah diubah packet size (Belum diberikan HoneyPy)	Terdeteksi pada maltrail	Tidak Terdeteksi	Tidak Berhasil
DoS menggunakan PING yang sudah diubah packet size (Sudah diberikan HoneyPy)	Terdeteksi pada maltrail	Tidak Terdeteksi	Tidak Berhasil
DoS menggunakan serangan hping3 (Belum diberikan HoneyPy)	Terdeteksi pada maltrail	Tidak Terdeteksi	Tidak Berhasil
DoS menggunakan serangan hping3 (Sudah diberikan HoneyPy)	Terdeteksi pada maltrail	Tidak Terdeteksi	Tidak Berhasil

Dalam proses uji coba serangan terhadap server CentOs dan Linux Mint dibagi menjadi 3 serangan DoS yaitu dengan Nmap, Ping yang sudah diubah packetsize, dan tool hping3 seperti pada Table I. Serangan-serangan yang dilakukan akan di analisis hasilnya dengan menggunakan Maltrail sebagai penangkapan aktivitas serangan.

Berdasarkan beberapa serangan yang dilakukan oleh peneliti bahwa didapatkan hasil yang sama seperti sebelumnya yang tidak menggunakan HoneyPy. Perbedaannya pada waktu peneliti melakukan scanning dengan Nmap pada IP Linux Mint. HoneyPy berfungsi untuk mengelabui atau menipu penyerang dengan menambahkan port tertentu misalnya pada penelitian ini menambahkan port 80 sebagai uji coba. Hasil perbedaan yang didapatkan dengan menggunakan HoneyPy mendapatkan dua port yang terbuka salah satunya HTTP/port 80 yang sudah dibuat sebelumnya oleh peneliti menggunakan HoneyPy. Oleh karena itu, jika penyerang akan melakukan serangan terhadap HTTP/port 80, Maltrail akan dengan mudah mendeteksi aktivitas penyerang.

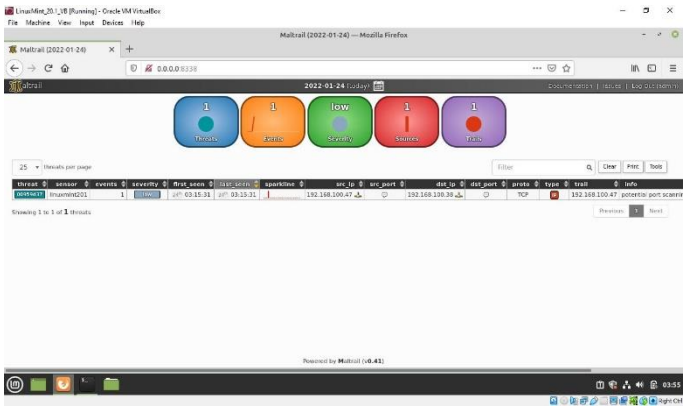


Gambar 4. Nmap IP Linux Mint Yang Sudah Menggunakan HoneyPy

Pada Gambar 4 didapatkan port tambahan yang sudah ditambahkan oleh peneliti sebelumnya yaitu HTTP/ port 80 dengan menggunakan HoneyPy sehingga juga terdapat celah yang bisa diserang penyerang untuk digunakan dalam penangkapan aktivitas penyerang oleh peneliti.

E. Perbandingan Hasil Serangan

1. Tanpa Menggunakan HoneyPy



Gambar 5. Hasil Tanpa HoneyPy

Pada Gambar 5 mendapatkan data berjumlah satu events dari beberapa contoh serangan yang dilakukan oleh peneliti. Serangan pertama dengan Nmap yang terdeteksi oleh Maltrail hanya pada server Linux Mint, selanjutnya pada serangan kedua dengan Ping yang sudah diubah packetsize dan juga serangan terakhir menggunakan Hping3 semuanya tidak terdeteksi oleh Maltrail.

2. Menggunakan HoneyPy

Gambar 6. Hasil Menggunakan HoneyPy

Pada Gambar 6 mendapatkan data berjumlah lima events dari beberapa contoh serangan yang dilakukan oleh peneliti. Beberapa serangan yang dilakukan oleh peneliti yang berhasil terdeteksi yaitu menggunakan Nmap seperti pada sebelumnya yang tidak menggunakan HoneyPy. Perbedaannya pada tingkat ancaman yang didapatkan beserta jumlah data yang terdeteksi lebih besar dibandingkan tidak menggunakannya.

F. Hasil Keseluruhan

1. Threats

Gambar 7. Threats

2. Events

Gambar 8. Events

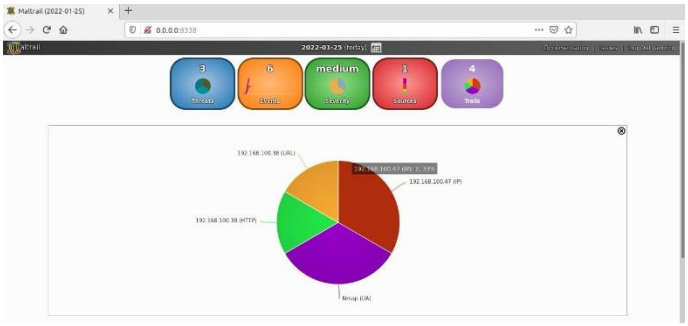
3. Severity

Gambar 9. Severity

4. Sources

Gambar 10. Sources

5. Trails



Gambar 11. Trails

V. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai implementasi HoneyPy dengan Maltrail untuk mendeteksi serangan DoS, dapat disimpulkan bahwa Implementasi HoneyPy dengan Maltrail merupakan metode pembuktian yang mampu menjadi tolak ukur untuk digunakan sebagai peningkatan keamanan pada serangan di bagian server serta jumlah yang didapatkan pada Maltrail terhadap serangan-serangan yang dilakukan oleh peneliti pada bagian yang tidak menggunakan HoneyPy terdapat satu events, sedangkan pada bagian yang menggunakan HoneyPy terdapat lima events yang terjadi dan juga Berdasarkan data keseluruhan dari lima laporan yang sudah dilakukan pengujian hanya mendeteksi serangan scanning Nmap yang dapat terdeteksi pada Maltrail. Pada hasil keseluruhan ini didapatkan tiga threats, enam events, severity terdeteksi low dan medium, satu sumber ancaman pada sources, dan empat trails.

REFERENCES

[1] Pusat Operasi Keamanan Siber Nasional, "Laporan Tahunan Hasil Monitoring Keamanan Siber 2020," *Bul. Jendela Data dan Inf. Kesehat.*, pp. 29–33, 2021.

[2] D. K. Rahmatullah, S. M. Nasution, and F. Azmi, "Implementation of low interaction web server honeypot using cubieboard," *ICCEREC 2016 - Int. Conf. Control. Electron. Renew. Energy, Commun. 2016, Conf. Proc.*, pp. 127–131, 2017.

[3] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, "A Survey on Honeypot Software and Data Analysis," 2016.

[4] B. R. Prasad, A. Abraham, V. Suhas, and K. Kumar, "DOS attack pattern generator for training the neural network based classifier to dynamically blacklist IP in honeypot based NIDS/NIPS," *Thinkquest~2010*, pp. 224–226, 2011.

[5] B. P. Zen, R. A. G. Gultom, and A. H. S. Reksoprodjo, "Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," *J. Teknol. Penginderaan*, vol. 2, no. 1, pp. 105–122, 2020.

[6] B. Mardiyanto, T. Indriyani, and I. M. Suartana, "Analisis dan Implementasi Honeypot dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) pada Jaringan Wireless," *Integer J.*, vol. 1, no. 2, pp. 32–42, 2016.

[7] A. W. Muhammad and I. Riadi, "Analisis Statistik Log Jaringan Untuk Deteksi," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 220–225, 2016.

[8] Hudzaifah, A. Sularsa, and D. R. Suchendra, "Membangun Sistem Monitoring Malicious Traffic Di Jaringan Dengan Maltrail," *e-Proceeding Appl. Sci.*, vol. 4, no. 3, pp. 2013–2018, 2018.

[9] Z. Amin, "Analisis Vulnerabilitas Host Pada Keamanan Jaringan Komputer Di Pt . Sumeks Tivi Palembang (Paltv) Menggunakan Router Berbasis Unix," *Teknol. dan Inform.*, vol. 2, no. 3, pp. 189–199, 2012.

[10] J. B. Bolanio, R. K. Paredes, A. L. Yoldan Jr., and R. E. Acapulco II, "Network Security Policy for Higher Education Institutions based on ISO Standards," *Mediterr. J. Basic Appl. Sci.*, vol. 05, no. 01, pp. 01–17, 2021.

[11] L. P. Aidin, S. M. Nasution, and F. Azmi, "Implementasi High Interaction Honeypot Pada Implementation of High Interaction Honeypot," *e-Proceeding Eng.*, vol. 3, no. 2, pp. 2172–2178, 2016.

[12] N. Naik, P. Jenkins, N. Savage, and L. Yang, "A computational intelligence enabled honeypot for chasing ghosts in the wires," *Complex Intell. Syst.*, vol. 7, no. 1, pp. 477–494, 2021.

[13] M. Mueter, F. Freiling, T. Holz, and J. Matthews, "A generic toolkit for converting web applications into high-interaction honeypots," *Univ. Mannheim*, 2008.

[14] D. W. Johnson *et al.*, "Application of Medihoney Antibacterial Wound Gel for the Prevention," *Society*, vol. 29, no. 2, pp. 303–309, 2009.

[15] J. Mack, Y.-H. (Frank) Hu, and M. A. Hoppa, "A Study of Existing Cross-Site Scripting Detection and Prevention Techniques Using XAMPP and VirtualBox," *Va. J. Sci.*, vol. 70, no. 3, p. 1, 2019.

[16] D. Legay, A. Decan, and T. Mens, "On Package Freshness in Linux Distributions," *Proc. - 2020 IEEE Int. Conf. Softw. Maint. Evol. ICSME 2020*, pp. 682–686, 2020.

[17] R. T. Gaddam and M. Nandhini, "An analysis of various snort based techniques to detect and prevent intrusions in networks: Proposal with code refactoring snort tool in Kali Linux environment," *Proc. Int. Conf. Inven. Commun. Comput. Technol. ICICCT 2017*, no. Icicct, pp. 10–15, 2017.

[18] B. Korniyenko and L. Galata, "Implementation of the information resources protection based on the CentOS operating system," *2019 IEEE 2nd Ukr. Conf. Electr. Comput. Eng. UKRCON 2019 - Proc.*, pp. 1007–1011, 2019.

[19] N. S. Sulaiman, A. Shafiq, and H. Ahmad, "Comparison of Operating System Performance Between Windows 10 and Linux Mint," vol. 2, no. 1, pp. 92–102, 2021.