JTERA (Jurnal Teknologi Rekayasa), Vol. 9, No. 2, Desember 2024, Hal. 33-44 p-ISSN 2548-737X
Terakreditasi "**Peringkat 3**" oleh Kemenristek/BRIN, Nomor SK: 85/M/KPT/2020 e-ISSN 2548-8678
DOI: 10.31544/jtera.v9.i1.2024.69-76

Optimalisasi Keamanan Web Server Ubuntu dengan Teknologi IPS Berbasis Iptables

Lalu Delsi Samsumar[1*], Bahtiar Imran[2], Muhamad Masjun Efendi[3], Rudi Muslim[4], Zumratul Muahidin[5], Zaenul Mutaqin[6]

[1,2,3,4,5,6]Universitas Teknologi Mataram
Jalan Pelor Mas III, Kampus Universitas Teknologi Mataram, Kekalik, Kota Mataram, Indonesia

samsumarld@utmmataram.ac.id

Abstrak

Keamanan jaringan merupakan faktor krusial dalam melindungi data dan informasi penting dalam suatu organisasi. Salah satu metode untuk mengamankan web server adalah dengan menerapkan *Intrusion Prevention System* (IPS) berbasis iptables. Penelitian ini bertujuan untuk mengoptimalkan keamanan web server Ubuntu dengan menggunakan teknologi IPS berbasis iptables. Iptables berfungsi tidak hanya sebagai firewall, tetapi juga sebagai sistem deteksi dan pencegahan intrusi (IDS/IPS) yang efektif untuk melindungi server berbasis Linux. Dalam penelitian ini, Snort digunakan sebagai alat deteksi intrusi yang diintegrasikan dengan iptables untuk memantau dan memitigasi potensi serangan pada jaringan lokal. Metodologi penelitian ini mencakup analisis kebutuhan sistem, instalasi sistem operasi dan web server, serta konfigurasi iptables sebagai IPS untuk mendeteksi dan mencegah serangan yang mengancam integritas server. Pengujian dilakukan dengan mengidentifikasi kerentanannya dan menguji efektivitas implementasi IPS pada web server Ubuntu. Hasil penelitian menunjukkan bahwa iptables berhasil menjalankan fungsinya sebagai IPS dalam mengamankan web server dari serangan DDoS. Iptables efektif dalam memblokir serangan yang masuk ke dalam web server. Sistem ini juga berhasil mendeteksi serangan yang dilakukan menggunakan Snort yang berfungsi sebagai IDS. Snort mampu mendeteksi serangan yang masuk dan memberikan peringatan yang berguna dalam memperkuat lapisan keamanan pada web server.

Kata kunci: Intrusion Prevention System, Iptables, Keamanan, Web server, Ubuntu

Abstract

Network security is a crucial factor in protecting important data and information in an organization. One method to secure a web server is to implement an iptables-based Intrusion Prevention System (IPS). This study aims to optimize the security of an Ubuntu web server using iptables-based IPS technology. Iptables functions not only as a firewall, but also as an effective intrusion detection and prevention system (IDS/IPS) to protect Linux-based servers. In this study, Snort is used as an intrusion detection tool integrated with iptables to monitor and mitigate potential attacks on the local network. The research methodology includes system requirements analysis, operating system and web server installation, and iptables configuration as an IPS to detect and prevent attacks that threaten server integrity. Testing is done by identifying its vulnerabilities and testing the effectiveness of IPS implementation on the Ubuntu web server. The results of the study show that iptables successfully performs its function as an IPS in securing the web server from DDoS attacks. Iptables is effective in blocking attacks that enter the web server. This system also successfully detects attacks carried out using Snort which functions as an IDS. Snort is able to detect incoming attacks and provide warnings that are useful in strengthening the security layer on the web server.

Keywords: *Intrusion Prevention System, iptables, security, web server, Ubuntu*

I. PENDAHULUAN

Keamanan jaringan merupakan aspek yang sangat penting dalam dunia teknologi informasi saat ini, terutama untuk melindungi data dan informasi sensitif yang dimiliki oleh organisasi atau perusahaan. Dengan semakin berkembangnya teknologi, ancaman terhadap keamanan jaringan semakin beragam, mulai

Diterima: 13 Desember 2024; Direvisi: 27 Desember 2024; Disetujui: 29 Desember 2024
JTERA, Vol. 9, No. 2, Desember 2024

© 2024 JTERA (Jurnal Teknologi Rekayasa), Politeknik Sukabumi

dari serangan malware hingga upaya peretasan yang dapat merusak reputasi dan operasi sebuah entitas. Oleh karena itu, perlindungan terhadap jaringan menjadi prioritas utama dalam menjaga integritas dan kerahasiaan data. Salah satu pendekatan yang dapat digunakan untuk mengamankan web server adalah penerapan *Intrusion Prevention System* (IPS), yang berfungsi untuk mendeteksi dan mencegah potensi ancaman yang mengarah pada kerusakan sistem. Iptables, sebagai alat firewall yang sering digunakan pada sistem berbasis Linux, dapat dimanfaatkan untuk mendukung penerapan IPS dalam meningkatkan keamanan web server [1].

Penelitian sebelumnya oleh Diponegoro (2019) menunjukkan bahwa kombinasi penggunaan Snort sebagai sistem deteksi intrusi dan iptables sebagai firewall dapat memantau dan memitigasi berbagai jenis serangan pada jaringan lokal. Pendekatan ini sangat relevan dalam konteks web server, yang sering menjadi target utama serangan dari pihak luar [2]. Selain itu, Muhaimi et al. (2019) mengembangkan konsep integrasi antara Snort, iptables, dan aplikasi komunikasi seperti Telegram untuk memberikan pemberitahuan real-time kepada administrator ketika terdeteksi adanya potensi ancaman. Integrasi ini memungkinkan pengelolaan dan respons terhadap insiden keamanan jaringan menjadi lebih cepat dan efisien [3]. Dalam konteks ini, penelitian ini bertujuan untuk mengoptimalkan penerapan IPS berbasis iptables pada web server Ubuntu guna meningkatkan perlindungan terhadap serangan yang mungkin terjadi, sehingga dapat menjaga keamanan dan kelancaran operasi sistem.

Anugrah et al. juga meneliti implementasi IPS menggunakan Suricata untuk melindungi web server dari serangan SQL Injection. Penelitian ini menunjukkan efektivitas penggunaan aturan dan parameter response time dalam mendeteksi dan mencegah serangan [4]. Hal ini sejalan dengan penelitian oleh Huda, yang mengintegrasikan IDS dan IPS dengan notifikasi real-time, memberikan gambaran tentang bagaimana teknologi ini dapat digunakan untuk meningkatkan keamanan jaringan secara keseluruhan [5].

Dalam konteks yang lebih luas, penelitian oleh Barends mengusulkan desain IPS berbasis Snort dan iptables yang terintegrasi dengan honeypot dalam arsitektur Software Defined Network. Ini menunjukkan bahwa kombinasi teknologi dapat meningkatkan tingkat akurasi deteksi serangan dan mempercepat respons terhadap ancaman [6]. Penelitian ini menyoroti pentingnya integrasi berbagai teknologi dalam menciptakan sistem keamanan yang lebih komprehensif.

Keamanan web server telah menjadi isu yang sangat penting dalam era digital saat ini, mengingat peran vital server sebagai pusat penyedia layanan dan pengolahan data dalam suatu jaringan [7]. Server web berfungsi sebagai komponen utama dalam menjalankan berbagai aplikasi dan layanan yang diakses oleh pengguna, sehingga potensi ancaman terhadapnya dapat berdampak besar pada keberlanjutan operasional suatu organisasi atau perusahaan. Kinerja server sangat bergantung pada paket data yang dikirim oleh klien melalui jaringan, sehingga penting untuk memastikan bahwa komunikasi data tersebut terlindungi dari berbagai ancaman yang dapat merusak integritas dan ketersediaannya [8]. Sebagai solusi untuk mengatasi masalah ini, penelitian tentang penerapan IPS menjadi sangat relevan, karena IPS dapat berfungsi untuk mendeteksi dan mencegah serangan yang mengancam stabilitas dan keamanan server [9].

Selain itu, server yang terhubung dengan jaringan online memiliki kerentanannya sendiri, karena dapat menjadi target serangan dari berbagai ancaman eksternal. Salah satu jenis serangan yang sering ditemui pada web server adalah *cross-site scripting* (XSS), yang dapat digunakan oleh pihak jahat untuk menyisipkan skrip berbahaya ke dalam aplikasi web yang dijalankan server, mengancam keamanan data dan privasi pengguna [10]. Oleh karena itu, penerapan IPS yang efektif sangat dibutuhkan untuk memitigasi risiko serangan semacam ini dan memastikan bahwa server tetap berfungsi secara optimal tanpa mengorbankan keamanan data yang dikelola.

Keamanan web server merupakan aspek yang sangat penting dalam menjaga integritas dan ketersediaan layanan serta data yang dikelola oleh suatu sistem [11]. Dalam rangka meningkatkan perlindungan terhadap serangan yang dapat merusak sistem, penelitian ini bertujuan untuk mengonfigurasi iptables sebagai IPS guna mendeteksi dan mencegah potensi ancaman yang mengincar web server berbasis Ubuntu [12]. Iptables, yang merupakan alat firewall berbasis Linux, memiliki fleksibilitas yang memungkinkan konfigurasi untuk berfungsi ganda sebagai sistem deteksi dan pencegahan intrusi yang efektif.

Penelitian ini akan menggunakan pendekatan yang sistematis, dimulai dengan analisis kebutuhan sistem yang akan dibangun, diikuti dengan instalasi sistem operasi Ubuntu dan web server yang akan diuji [13]. Selanjutnya, konfigurasi iptables akan dilakukan untuk mengoptimalkan fungsinya sebagai IPS, dengan tujuan meminimalkan risiko serangan terhadap server. Proses pengujian dan analisis keamanan sistem akan dilakukan untuk mengevaluasi efektivitas implementasi IPS berbasis iptables dalam menghadapi ancaman yang mungkin terjadi. Diharapkan hasil dari penelitian ini dapat memberikan kontribusi signifikan dalam

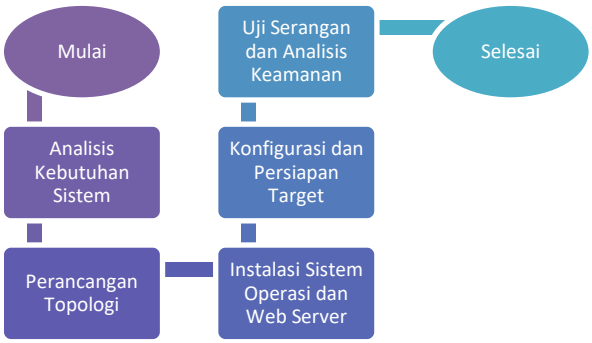
meningkatkan keamanan web server Ubuntu secara efektif, dengan memanfaatkan teknologi IPS berbasis iptables sebagai solusi untuk melindungi data dan layanan penting yang dikelola oleh server.

Penelitian ini bertujuan untuk mengoptimalkan keamanan web server Ubuntu menggunakan teknologi IPS berbasis iptables. Iptables dapat dimanfaatkan sebagai IDS (*Intrusion Detection System*) dan IPS untuk mengamankan server Linux [14]. Implementasi IPS menggunakan Snort dan iptables dapat memantau dan memitigasi serangan pada jaringan lokal [15]. Integrasi IPS berbasis Snort dengan iptables dan Telegram juga dapat digunakan untuk mengamankan server internet [16].

II. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen untuk mengoptimalkan keamanan web server Ubuntu dengan teknologi IPS berbasis iptables. Dua sistem operasi yang akan digunakan dalam penelitian ini adalah Ubuntu dan Kali Linux.

Langkah-langkah penelitian yang dilakukan adalah sebagai berikut:



Gambar 1. Langkah-langkah Penelitian

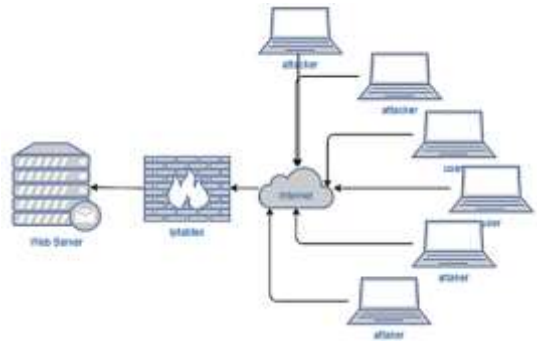
1. Analisis Kebutuhan Sistem
   a) Mengidentifikasi kebutuhan sistem untuk mengamankan web server Ubuntu menggunakan IPS berbasis iptables.
   b) Menganalisis serangan-serangan yang mungkin terjadi pada web server dan bagaimana iptables dapat digunakan untuk mendeteksi dan mencegahnya.
2. Instalasi Sistem Operasi dan Web Server
   a) Menginstal sistem operasi Ubuntu pada salah satu server.
   b) Menginstal sistem operasi Kali Linux pada server lainnya untuk digunakan sebagai mesin penyerang.
   c) Menginstal web server pada server Ubuntu.
3. Konfigurasi Iptables sebagai IPS
   a) Mengkonfigurasi iptables pada server Ubuntu untuk mendeteksi dan mencegah serangan yang masuk.
   b) Mengintegrasikan iptables dengan tools IPS lainnya seperti Snort untuk meningkatkan kemampuan deteksi dan pencegahan serangan.



Gambar 2. Langkah-langkah Konfigurasi Iptables dan Snort

4. Pengujian dan Analisis Keamanan
   a) Melakukan serangan-serangan terhadap web server Ubuntu dari server Kali Linux.
   b) Mengamati dan menganalisis kemampuan iptables dalam mendeteksi dan mencegah serangan yang masuk.
   c) Mengevaluasi efektivitas implementasi IPS berbasis iptables dalam meningkatkan keamanan web server Ubuntu.

Dengan menggunakan metode eksperimen ini, penelitian ini diharapkan dapat mengoptimalkan keamanan web server Ubuntu secara efektif menggunakan teknologi IPS berbasis iptables.



Gambar 3. Topology serangan DdoS dan Keamanan IPTable



Gambar 4. Topologi Keeamanan IPTable

III. HASIL DAN PEMBAHASAN

3.1. Hasil

Proses yang dilakukan pada pengujian penerapan *Iptables* untuk keamanan *web server ubuntu* ini meliputi perancangan sistem, persiapan target, pengujian serangan, pengujian keamanan, dan pebandingan. Pada kemanan *web server ubuntu* ini berfokus pada *Iptables* untuk menjadi keamanannya.

Perancangan sistem yang dilakukan dalam penelitian ini mencakup pengaturan perangkat lunak yang diperlukan untuk mengaktifkan dua sistem operasi (OS) secara bersamaan menggunakan virtual machine. Untuk itu, digunakan Oracle VM VirtualBox 7.0 sebagai platform virtualisasi, yang memungkinkan pembuatan dan pengelolaan virtual machine.

Dalam konfigurasi ini, dua sistem operasi diinstal pada virtual machine yang sama, yaitu Ubuntu dan Kali Linux. Sistem operasi Ubuntu berperan sebagai target serangan, sedangkan Kali Linux digunakan sebagai platform untuk melakukan uji penetrasi dan serangan. Dengan konfigurasi ini, diharapkan dapat dilakukan simulasi serangan terhadap web server berbasis Ubuntu, guna mengevaluasi efektivitas mekanisme keamanan yang diterapkan.

Untuk persiapan target, digunakan web server Ubuntu yang akan dijadikan sasaran serangan. Web server tersebut telah terinstal dengan Apache 2 dan dikonfigurasi dengan alamat IP 192.168.43.65, yang beroperasi pada port 80.



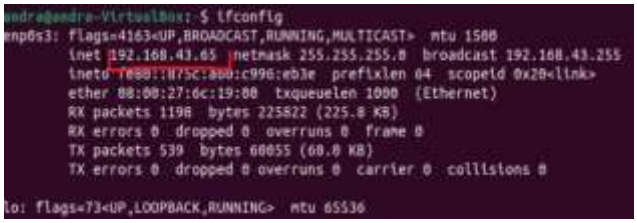
Gambar 5. Target serangan web *server ubuntu*

Sebagai langkah pengamanan, iptables telah dipasang untuk mengelola lalu lintas jaringan dan mencegah akses yang tidak sah. Selain itu, Snort juga diinstal untuk mendeteksi potensi serangan yang masuk, memberikan lapisan perlindungan tambahan untuk memantau dan menganalisis pola serangan yang terjadi. Konfigurasi ini memungkinkan simulasi serangan terhadap web server Ubuntu, dengan fokus pada evaluasi sistem keamanan yang diterapkan, baik dari segi pencegahan maupun deteksi intrusi.

Pengujian Serangan

a. Cek IP Address Target

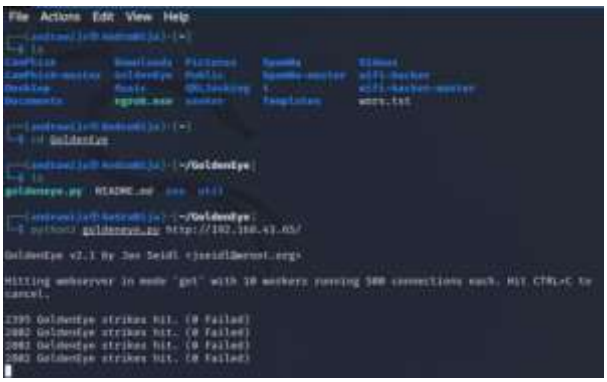
Pada tahap pengujian serangan, langkah pertama yang dilakukan adalah pengecekan IP address pada target yang akan diserang. Pengecekan ini dilakukan pada sistem operasi Ubuntu dengan cara membuka terminal dan mengetik perintah ifconfig. Perintah ini akan menampilkan IP address yang digunakan web server target, seperti yang terlihat pada Gambar 6.



Gambar 6. IP Address Ubuntu

b. Serangan Pertama: DDoS menggunakan tools GoldenEye.

Serangan ini dilakukan dengan cara mengakses sistem operasi Kali Linux, kemudian membuka terminal dan menjalankan tools GoldenEye. Setelah tools GoldenEye aktif, perintah yang diperlukan akan dijalankan untuk memulai serangan, yang bertujuan untuk memenuhi permintaan berulang-ulang pada target, sehingga server mengalami kelebihan beban. Perintah yang digunakan adalah paython3 goldeneye.py http://192.168.43.65/.Gambar 7 menunjukkan ilustrasi serangan DDoS yang dilakukan menggunakan GoldenEye.

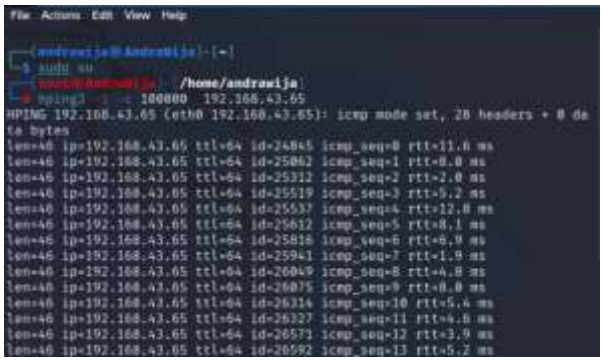


Gambar 7. Serangan DdoS menggunakan *tools* GoldenEye

c. Serangan Kedua: DDoS menggunakan tools Hping3

Metode serangan kedua yang diuji adalah DDoS menggunakan Hping3, sebuah tool yang digunakan untuk mengirimkan paket ICMP atau pesan kesalahan yang dapat membanjiri web server target. Serangan ini menyebabkan server menjadi tidak responsif atau bahkan down. Perintah yang digunakan dalam

serangan ini adalah hping3 -1 –c 10000 192.168.43.56 -1, yang mengindikasikan serangan menggunakan paket ICMP, sementara -c digunakan untuk menentukan jumlah paket yang akan dikirim. Gambar 8 menunjukkan ilustrasi serangan DDoS yang dilakukan menggunakan Hping3.

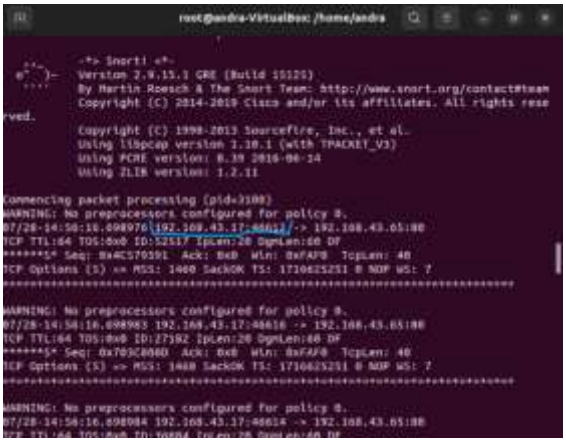


Gambar 8. Serangan DDoS yang dilakukan menggunakan Hping3

Pengujian Keamanan

a. Deteksi IP Penyerang Menggunakan Snort

Untuk mendeteksi serangan yang terjadi, digunakan Snort -v, yang merupakan sistem deteksi intrusi (IDS). Seperti yang terlihat pada Gambar 9.

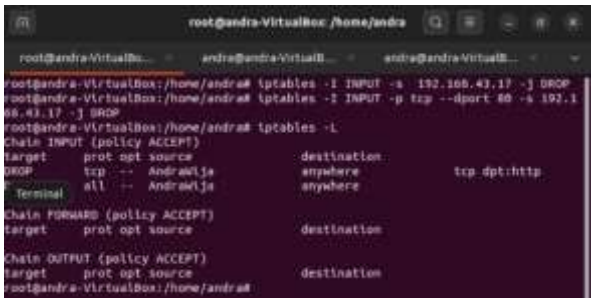


Gambar 9. Deteksi serangan menggunakan snort

Snort berhasil mendeteksi IP penyerang, yaitu 192.168.43.17. Deteksi ini terjadi ketika perintah untuk mengaktifkan Snort dijalankan, dan Snort memberikan peringatan bahwa serangan terdeteksi. Hal ini menunjukkan efektivitas Snort dalam mengidentifikasi potensi ancaman yang berasal dari alamat IP tertentu.

b. Blokir Serangan Menggunakan Iptables

Setelah IP penyerang terdeteksi, langkah berikutnya adalah melakukan pemblokiran serangan menggunakan Iptables.

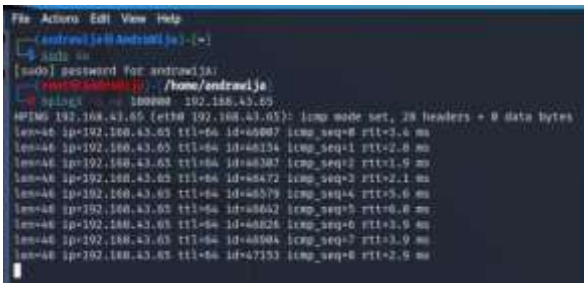


Gambar 10. Rules bloking pada *Iptables*

Aturan (rules) untuk memblokir serangan ditambahkan pada Chain INPUT Iptables. Perintah yang digunakan adalah IpTables –I INPUT –s 192.168.43.17 –j DROP akan menghalangi akses lebih lanjut dari penyerang terhadap web server, sehingga serangan dapat dihentikan. Setelah aturan pemblokiran diterapkan dengan perintah IpTables –I INPUT –p tcp –dport 80 –s 192.168.43.17 –j DROP, penyerang tidak lagi dapat mengakses web server atau melanjutkan serangan terhadap target.

Blokir Serangan Menggunakan Iptables

Pada Gambar 11, dapat dilihat bahwa setelah aturan pemblokiran (rules) dimasukkan pada Iptables, serangan yang dilancarkan terhadap target langsung berhenti dan tidak dapat dilanjutkan.



Gambar 11. Serangan DdoS berhenti

Hal ini menunjukkan efektivitas pemblokiran serangan menggunakan Iptables. Gambar 12 menggambarkan kondisi web server yang tidak dapat diakses lagi oleh penyerang setelah IP address penyerang diblokir, memastikan bahwa serangan tidak dapat mengakses atau merusak server lebih lanjut.



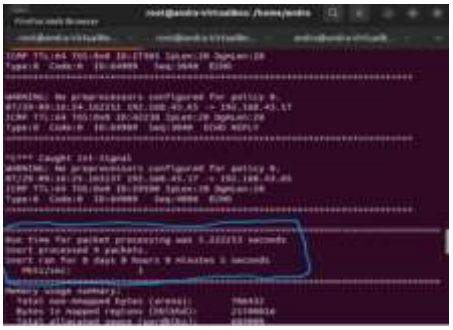
Gambar 12. *Web server* tidak bisa di akses penyerang

Perbandingan Serangan Menggunakan Tools GoldenEye dan Hping3

Dalam pengujian serangan DDoS, dua tools yang digunakan adalah GoldenEye dan Hping3. Perbandingan antara kedua tools ini dalam melancarkan serangan DDoS dapat dilihat pada beberapa aspek berikut:

a. Deteksi Paket Serangan Menggunakan Hping3

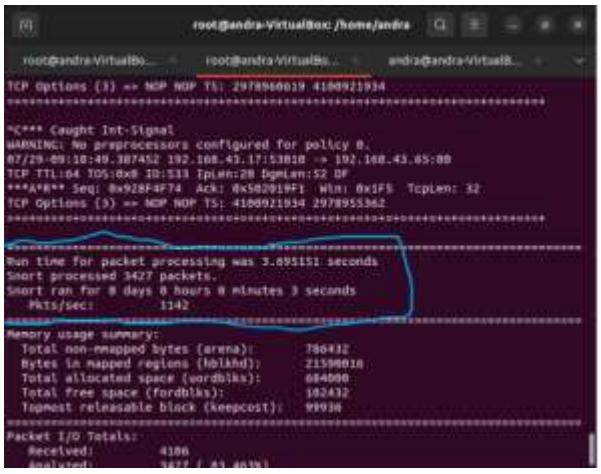
Pada serangan DDoS menggunakan Hping3, web server menerima sebanyak 9 paket serangan dalam waktu 5.222253 detik, dengan rata-rata lebih dari satu paket serangan per detiknya.



Gambar 13. Deteksi serangan *hping3*

b. Deteksi Paket Serangan Menggunakan GoldenEye

Sebaliknya, pada serangan yang dilakukan menggunakan GoldenEye, web server menerima 3.427 paket serangan dalam waktu 3.695151 detik, yang berarti lebih dari 1.142 paket diterima setiap detiknya, sebagaimana terlihat pada Gambar 14.



Gambar 14. Deteksi serangan DDoS *Goldeneye*

Tabel Perbandingan Hasil Serangan 1 dan 2

Tabel 1 menyajikan perbandingan antara hasil serangan pertama (menggunakan Hping3) dan serangan kedua (menggunakan *GoldenEye*):

Tabel 1. Perbandingan hasil serangan ke 1 dan 2

Serang-an Ke	Tools	Jumlah Serangan Masuk	Waktu	Pkts/detik
1	Hping3	9	5 detik	1
2	GoldenEye	3.427	3 detik	1.142

Dari tabel dan penjelasan di atas, dapat dilihat bahwa jumlah paket serangan yang dihasilkan oleh serangan kedua menggunakan GoldenEye jauh lebih banyak dibandingkan dengan serangan pertama menggunakan Hping3. Hal ini disebabkan oleh percepatan paket serangan yang lebih tinggi pada serangan kedua, yang memungkinkan lebih banyak paket diterima oleh server dalam waktu yang lebih singkat.

3.2. Pembahasan

Pada tahap implementasi sistem, dilakukan konfigurasi dua sistem operasi (OS) pada mesin virtual menggunakan Oracle VM VirtualBox 7.0, yaitu Ubuntu dan Kali Linux. Ubuntu berperan sebagai target serangan, sedangkan Kali Linux digunakan sebagai alat untuk melancarkan serangan.

Web server Ubuntu yang menjadi target telah terinstal Apache 2 dan dikonfigurasi dengan alamat IP 192.168.43.65 pada port 80. Untuk mengamankan server, telah dipasang iptables sebagai firewall dan Snort sebagai IDS untuk mendeteksi potensi serangan yang masuk.

Pada pengujian sistem dilakukan dengan melancarkan dua jenis serangan DDoS menggunakan dua tools yang berbeda, yaitu GoldenEye dan Hping3.

Setelah pengujian dilakukan, beberapa parameter yang dianalisis antara lain jumlah paket serangan yang diterima oleh server dan waktu yang dibutuhkan untuk melakukan serangan.

Hasil pengujian menunjukkan bahwa serangan dengan GoldenEye lebih cepat dan lebih berat, karena jumlah paket yang diterima oleh server jauh lebih banyak dalam waktu yang lebih singkat.

Setelah serangan terdeteksi oleh Snort, langkah selanjutnya adalah memblokir akses dari penyerang menggunakan iptables. Setelah aturan ini diterapkan, penyerang tidak dapat lagi mengakses server.

Hasil penelitian ini sejalan dengan penelitian yang dilakukan oleh [2], yang menunjukkan bahwa penggunaan Snort dan iptables dapat memberikan perlindungan yang efektif terhadap serangan DDoS pada web server. Namun, perbedaan utama terletak pada jenis serangan yang diuji dan penggunaan tool yang lebih beragam dalam penelitian ini, yakni GoldenEye dan Hping3, yang menghasilkan jumlah paket serangan yang lebih tinggi dibandingkan

dengan penelitian sebelumnya yang menggunakan tool standar lainnya.

Selain itu, penelitian ini lebih fokus pada implementasi dan pengujian langsung menggunakan virtual machine untuk mengisolasi lingkungan uji coba, yang memungkinkan pengamatan lebih mendalam terhadap respons server dalam menghadapi serangan. Hasil yang diperoleh memberikan gambaran lebih jelas tentang efektivitas iptables dan Snort dalam mendeteksi dan memitigasi serangan DDoS pada web server berbasis Ubuntu.

Dari hasil yang diperoleh, dapat dilihat bahwa GoldenEye lebih efektif dalam melancarkan serangan DDoS dengan jumlah paket yang lebih banyak dan waktu serangan yang lebih singkat. Hal ini menunjukkan bahwa GoldenEye lebih cepat dalam membanjiri web server dengan permintaan yang tidak sah, berpotensi membuat server tidak dapat diakses dalam waktu yang lebih cepat. Di sisi lain, Hping3 lebih rendah dalam jumlah paket yang diterima per detik, namun tetap dapat menyebabkan gangguan pada server jika tidak ada sistem pertahanan yang memadai.

Dalam hal pencegahan dan deteksi, kombinasi antara Snort dan iptables terbukti efektif dalam mendeteksi dan memblokir serangan DDoS. Snort mampu mendeteksi alamat IP penyerang secara tepat, sedangkan iptables dapat memblokir akses dari alamat IP yang terdeteksi, sehingga serangan dapat dihentikan sebelum menyebabkan kerusakan yang signifikan pada web server.

IV. KESIMPULAN

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa Iptables berhasil menjalankan fungsinya sebagai IPS dalam mengamankan web server dari serangan DDoS. Iptables efektif dalam memblokir serangan yang masuk ke dalam web server yang menggunakan Ubuntu sebagai sistem operasi target, dengan Kali Linux berperan sebagai alat serangan.

Selain pemblokiran, sistem ini juga berhasil mendeteksi serangan yang dilakukan menggunakan Snort, yang berfungsi sebagai IDS. Snort mampu mendeteksi serangan yang masuk dan memberikan peringatan yang berguna dalam memperkuat lapisan keamanan pada web server.

Dua jenis alat serangan DDoS yang digunakan dalam penelitian ini, yaitu GoldenEye dan Hping3, menunjukkan perbedaan signifikan dalam jumlah paket yang diterima oleh web server. Pada serangan menggunakan Hping3, web server menerima 9 paket dalam waktu 5.222253 detik, dengan lebih dari 1 paket diterima per detiknya, yang menunjukkan intensitas serangan yang sedang berlangsung.

Secara keseluruhan, penelitian ini membuktikan bahwa kombinasi Iptables dan Snort dapat secara efektif melindungi web server dari serangan DDoS, dengan kemampuan untuk mendeteksi dan memblokir serangan secara real-time.

REFERENSI

[1] E. S. J. Atmadji, B. M. Susanto, and R. Wiratama, “Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server,” *Teknika*, vol. 6, no. 1, pp. 19–23, 2017.

[2] R. Suwanto, I. Ruslianto, and M. Diponegoro, “Implementasi intrusion prevention system (IPS) menggunakan snort dan IPTABLE pada monitoring jaringan lokal berbasis website,” *Coding Jurnal Komputer dan Aplikasi*, vol. 7, no. 01, 2019.

[3] A. Muhaimi, I. P. Hariyadi, and A. Juliansyah, “Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram,” *Jurnal Bumigora Information Technology (BITe)*, vol. 1, no. 2, pp. 167–176, 2019.

[4] F. T. Anugrah, S. Ikhwan, and J. G. AG, “Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection,” *Techné: Jurnal Ilmiah Elektroteknika*, vol. 21, no. 2, pp. 199–210, 2022.

[5] T. S. Huda and S. Subektiningsih, “Analisis Keamanan Jaringan Komputer Menggunakan Metode IDS dan IPS dengan Notifikasi Telegram: Computer Network Security Analysis Using IDS and IPS Methods with Telegram Notifications,” *Indonesian Journal of Computer Science*, vol. 13, no. 1, 2024.

[6] J. K. Barends, F. Dewanta, and N. B. A. Karna, “Perancangan dan Analisis Intrusion Prevention System Berbasis SNORT dan IPTABLES dengan Integrasi Honeypot pada Arsitektur Software Defined Network,” *MULTINETICS*, vol. 7, no. 2, pp. 163–176, 2021.

[7] L. R. Ananda *et al.*, “Jaringan Komputer,” 2024, *PT Penamuda Media*.

[8] L. D. Samsumar and K. Gunawan, “Analisis dan Evaluasi Tingkat Keamanan Jaringan

Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram," *Jurnal Ilmiah Teknologi Infomasi Terapan*, vol. 4, no. 1, 2017.

[9] H. Suhendi and W. D. Cahyo, "Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI ITB," *Naratif: Jurnal Nasional Riset, Aplikasi dan Teknik Informatika*, vol. 3, no. 2, pp. 60–68, 2021.

[10] M. Awad, M. Ali, M. Takruri, and S. Ismail, "Security vulnerabilities related to web-based data," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 2, pp. 852–856, 2019.

[11] R. Komalasari *et al.*, *PENGANTAR ILMU KOMPUTER: TEORI KOMPREHENSIF PERKEMBANGAN ILMU KOMPUTER TERKINI*. PT. Sonpedia Publishing Indonesia, 2023.

[12] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi intrusion prevention system (IPS) menggunakan snort dan IPTABLE pada monitoring jaringan lokal berbasis website," *Coding Jurnal Komputer dan Aplikasi*, vol. 7, no. 01, 2019.

[13] L. D. Samsumar, B. A. Hidayatulloh, Z. Zaenudin, and P. N. D. Pitaloca, "ANALYSIS OF THE QUALITY OF CLOUD STORAGE SERVICES ON NEXTCLOUD AND PYDIO," *Journal of Information Technology and Its Utilization*, vol. 6, no. 1, pp. 1–8, 2023.

[14] A. Zaerani, L. D. Samsumar, M. N. Karim, and E. Suryadi, "Analisis Sistem Keamanan Wireless Local Area Network (WLAN) Menggunakan Akses Tethering: Analisis Sistem Keamanan Wireless Local Area Network (WLAN) Menggunakan Akses Tethering," *Jurnal Rekayasa Sistem Informasi dan Teknologi*, vol. 2, no. 1, pp. 588–594, 2024.

[15] Y. W. Pradipta, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IP Tables Berbasis Linux," *Jurnal Manajemen Informatika*, vol. 7, no. 1, pp. 21–28, 2017.

[16] A. R. Aulia, E. I. Alwi, and A. W. M. Gaffar, "Perancangan Sistem Keamanan Jaringan Intrusion Prevention System Menggunakan Suricata Dan IPTables," *LINIER: Literatur Informatika dan Komputer*, vol. 1, no. 3, pp. 235–240, 2024.