DOI: https://doi.org/10.62017/tektonik

Deteksi dan Respons Terhadap *Ddos Attacks* pada Website Dinamis

Vina Puspitasari*[1]
Muhamad Zikri Abdillah [2]
Mohammad Akbar Alfa Dirk Steyer[3]
Shelvie Nidya Neyman[4]

[1,2,3,4] IPB University
*e-mail: vnpuspitasari@apps.ipb.ac.id[1], zikriabdillah@apps.ipb.ac.id[2], steyerakbar@apps.ipb.ac.id[3]

Abstrak

Serangan Distributed Denial of Service (DDoS) adalah masalah keamanan jaringan yang membandel . Berbagai metode berbasis pembelajaran mesin telah diusulkan untuk mendeteksi serangan tersebut. Menurut survei kami, fitur yang digunakan untuk mengkarakterisasi serangan biasanya dipilih secara manual berdasarkan pemahaman pribadi, dan model pendeteksian diharapkan dapat memberikan kinerja generalisasi yang baik dalam pendeteksian praktis setiap saat. Oleh karena itu, cara memilih fitur optimal yang memberikan kinerja terbaik merupakan masalah penting untuk membangun detektor yang efektif. Sementara itu, ketika lalu lintas jaringan menjadi semakin kompleks dan mudah berubah, beberapa fitur asli mungkin tidak mampu mengkarakterisasi lalu lintas saat ini, dan kegagalan detektor dapat terjadi ketika lalu lintas berubah. Dalam tulisan ini, kami memilih multilayer perceptrons (MLP) untuk mendemonstrasikan dan memecahkan masalah yang diajukan. Dalam solusi kami, kami menggabungkan pemilihan fitur sekuensial dengan MLP untuk memilih fitur optimal selama fase pelatihan dan merancang mekanisme umpan balik untuk merekonstruksi detektor ketika mendeteksi kesalahan deteksi yang cukup besar secara dinamis. Terakhir, kami memvalidasi keefektifan metode kami dan membandingkannya dengan beberapa penelitian terkait. Hasilnya menunjukkan bahwa metode kami dapat menghasilkan kinerja deteksi yang sebanding dan memperbaiki detektor ketika kinerjanya buruk. Dari hasil percobaan, terbukti metode ini dapat mendeteksi serangan DDoS sekaligus menjamin bahwa service request yang sah mendapat pelayanan yang seharusnya sehingga server dapat melayani service request dengan baik.

***Kata kunci**: Apache2, Ddos, Firewall, Iptables, Keamanan Siber*

Abstract

Denial of Service (DoS) still a network security problems that continues to evolve dynamically. The higher the computing capabilities of a attackerhost, DoS attacks that can be produced is also more powerful and dangerous. These attacks can result in the inability of server to serve a legitimate service requests. Therefore, DoS attacks can be very harmful andeffective prevention should be given. The next network security threat that also very dangerous is Distributed Denial of Service (DDoS), in which the attacker takes advantage of a large number of computers to run a DoS attack againts a server, web service, or other network resources. Because of the huge risks caused by DDoS attacks, these have encouraged many researchers to design a mechanism for securing network resources. In this research, the authors focus on the main issue that related to web service security. The authors propose a mechanism for securing web services by means of filtration and validation of the service requests aim for accessing the network resources. Filtration and validation are performed by the combined method of Network Behavior Analysis (NBA) and Client Puzzle (CP). NBA become the first layer of defense method which is going to detect whether the DDoS attack by measuring the level of network congestion / Network density. NBA method obtained the IP addresses that need to be validated by the CP method as a second layer of defense. When a service request has been made through the process of filtration and this validation, then the demand for this new service will be served. From the experimental results, it is proved that this method can detect DDoS attacks while ensuring that legitimate service requests received appropriate services so that the server can serve requests with good service.

***Keywords**:* Apache2, Cyber Security, Ddos, Firewall, Iptable

DOI: https://doi.org/10.62017/tektonik

PENDAHULUAN

Dalam era digital saat ini, internet dan teknologi informasi tulang punggung dari sebagian besar lembaga dan kinerja pribadi. Namun, selain peningkatan cepat dalam penggunaan Internet, ancaman perlindungan siber kian meningkat. Salah satu ancaman perlindungan yang paling menonjol dan mengkhawatirkan yaitu serangan Distributed Denial of Service (DDOS).

Kemajuan dan perkembangan teknologi dibidang komputer saat ini begitu cepat, baik perangkat keras (hardware) maupun perangkat lunak (software) hal ini terlihat pada era teknologi informasi yang menjadi salah satu media yang banyak digunakan oleh semua orang, baik instansi atau perusahaan maupun organisasi. Salah satu media informasi yang efisien dan efektif saat ini biasanya berupa situs web (website), dimana semua informasi yang terdapat dalam website disimpan di webserver, sedangkan media yang digunakan untuk mengakses situs web (website) adalah internet (Hamdani et al., 2023).

Serangan Distributed Denial of Services (DDoS) mempengaruhi korban dalam bentuk menemukan bug atau kelemahan untuk mengganggu layanan atau menghabiskan semua bandwidth sumber daya dari sistem korban. Penyerang memindai jaringan untuk menemukan bagian yang memiliki kerentanan dan kemudian bagian ini digunakan sebagai agen oleh penyerang. Ini disebut komputer zombie. Internet Protokol (IP) palsu digunakan oleh komputer zombie. Keamanan di internet tergantung pada host (Saputro et al., 2020).

Serangan DDoS bekerja dengan memanfaatkan sumber daya dari banyak komputer yang tersebar di berbagai lokasi, yang dikendalikan oleh penyerang untuk mengirimkan serangan ke target secara bersamaan. Tujuan dari serangan ini adalah untuk mengganggu layanan yang disediakan oleh server target kepada pengguna yang sah (A. R. Nisa et al., 2024).

Dalam penelitian ini, kami menggunakan salah satu metode untuk mendeteksi juga menanggapi serangan DDOS pada situs web dinamis melalui HPing3, utilitas uji program tinggi. metode ini menggabungkan analisis lalu lintas jaringan dengan berbagai kontrol kontrol juga teknik kontrol untuk memberikan perlindungan yang efektif terhadap serangan DDOS.

Biasanya ketika serangan DDoS terdeteksi, tidak ada hal lain yang bisa kita lakukan kecuali dengan cara melakukan pemutusan(disconnect) server korban dari jaringan dan secara manual memperbaiki masalahnya. DDoS menghamburkan banyak resourcedi jalur antara penyerang dan target, tujuan utama dari mekanisme pertahanan terhadap DDoS adalah untuk mendeteksi serangan secepat mungkin dan menghentikannya sedekat mungkin dari serangan (F. Nisa & Ramadona, 2023).

Gunakan alat jaringan HPING3 untuk meluncurkan serangan DDoS. Sebuah aplikasi untuk jaringan bernama Hping3 memungkinkan pengiriman paket TCP/IP yang dipersonalisasi dan melihat balasan target. Alat ini sudah terpasang secara pre-installed di Kali Linux. Hping3 dapat digunakan untuk berbagai keperluan seperti menguji aturan firewall, melakukan port scanning, dan menguji performa jaringan. Selain itu, hping3 juga dapat mengirim paket dengan kecepatan maksimal menggunakan opsi flood (Risyad et al., 2018).

Serangan DDoS sekarang ini menargetkan layanan yang spesifik, sehingga aplikasi yang menjadi target akan menjadi down, sementara komponen jaringan yang lain seperti link, switch, routertidak mengalami masalah. Metode ini membuat serangan bisa menyembunyikan dirinya sebagai trafficnormal, karena intensitasnya yang tidak seperti serangan DDoS yang biasanya membuat trafficbesar-besaran. Contohnya adalah floodingHTTP GET yang memanfaatkan kerentanandari suatu web server (Satria, 2016).

METODE

Penelitian ini akan menggunakan metode penelitian eksperimental. Eksperimen akan dilakukan untuk menguji efektivitas berbagai metode deteksi dan respons terhadap DDoS attacks pada website dinamis. Pendekatan kualitatif juga akan digunakan untuk menganalisis hasil eksperimen dan mendapatkan wawasan mendalam. Pengumpulan data dalam penelitian ini dilakukan melalui tiga metode utama. Pertama, studi literatur dari jurnal, buku, dan artikel relevan digunakan untuk memahami konsep dasar, teknik deteksi, dan metode mitigasi serangan DDoS. Kedua, simulasi dan eksperimen dilakukan dengan mensimulasikan serangan DDoS pada

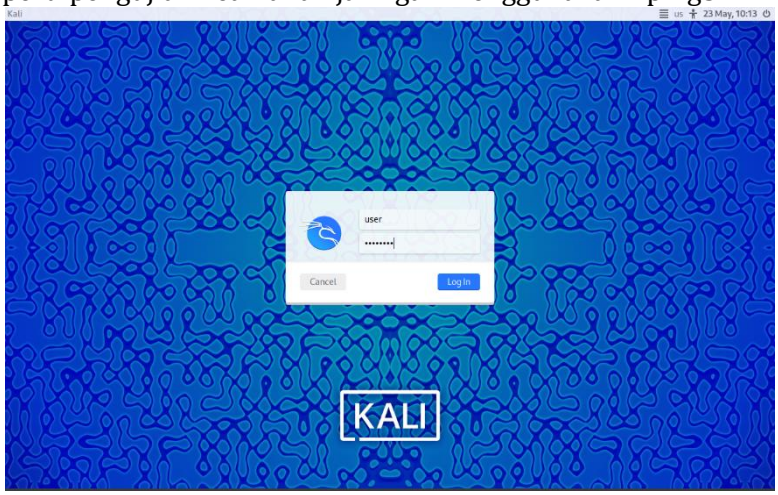
DOI: https://doi.org/10.62017/tektonik

website dinamis untuk menguji efektivitas metode deteksi dan respons. Ketiga, wawancara dan kuesioner dengan ahli keamanan siber dan praktisi industri dilakukan untuk mendapatkan data tentang pengalaman dan pandangan mereka mengenai serangan DDoS dan strategi mitigasinya.

Analisis data dalam penelitian ini dilakukan melalui dua pendekatan. Analisis kuantitatif menggunakan statistik untuk menganalisis data dari simulasi dan eksperimen, fokus pada tingkat deteksi dan efektivitas mitigasi serangan DDoS. Sementara itu, analisis kualitatif dilakukan dengan menganalisis data dari wawancara dan kuesioner, untuk mendapatkan pemahaman mendalam tentang tantangan dan solusi dalam mendeteksi dan merespons serangan DDoS. Pendekatan ini memberikan gambaran yang komprehensif tentang efektivitas metode yang digunakan serta perspektif praktis dari para ahli dan praktisi industri.

HASIL DAN PEMBAHASAN

Pada penelitian ini langkah awal pengguna dapat mengakses sistem operasi Kali Linux adalah proses login. Proses ini penting untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Setelah memasukkan username dan password yang benar, pengguna akan mendapatkan akses ke desktop Kali Linux, yang kemudian memungkinkan mereka untuk menjalankan berbagai perintah dan aplikasi yang diperlukan untuk melakukan tugas tertentu, seperti pengujian keamanan jaringan menggunakan hping3.



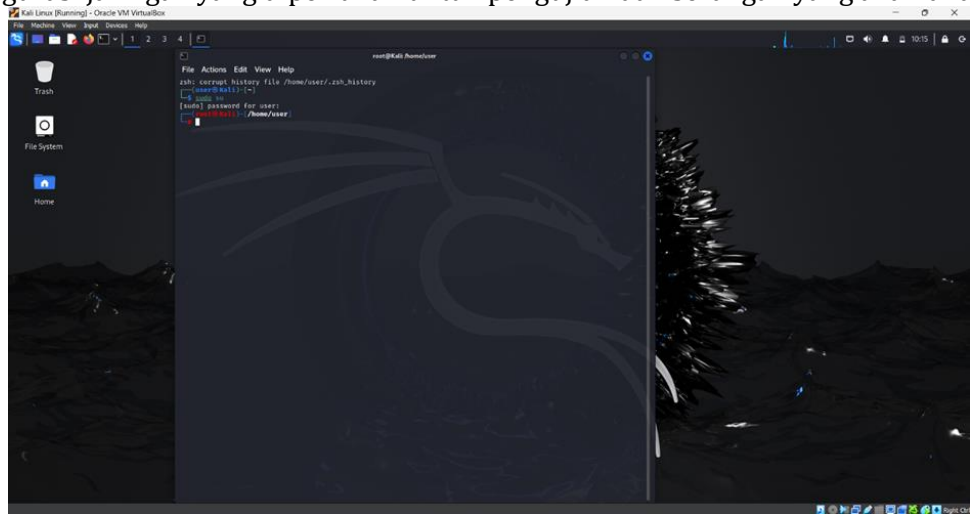
Gambar 1 Masukan username dan password untuk login

Kali Linux adalah distribusi Linux yang didesain khusus untuk kebutuhan penetration testing dan keamanan informasi, sehingga menyediakan berbagai alat yang siap digunakan untuk analisis dan pengujian jaringan.

Gambar 2 Tampilan login dari sistem operasi Kali Linux

DOI: https://doi.org/10.62017/tektonik

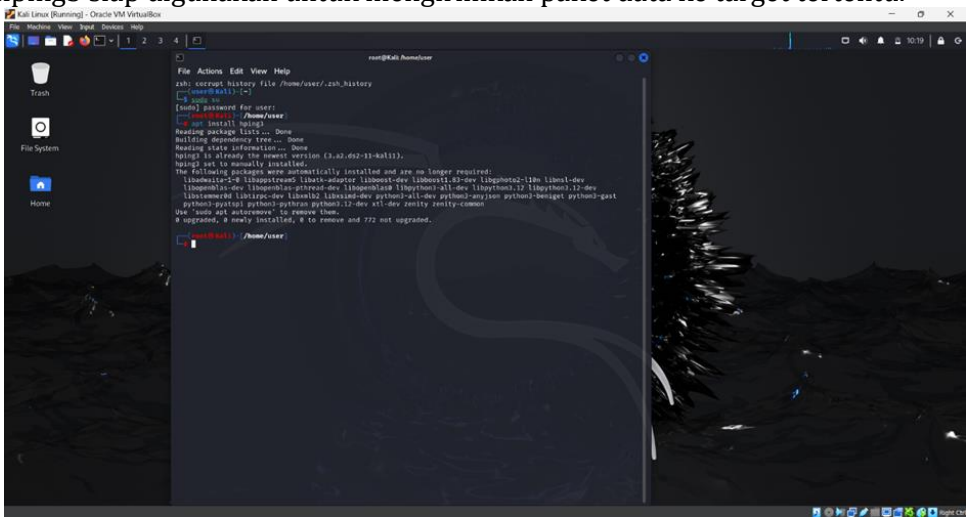
Setelah berhasil login, pengguna harus membuka terminal, yang merupakan antarmuka baris perintah di Kali Linux. Untuk mengakses fitur-fitur administratif dan alat-alat tertentu seperti hping3, pengguna perlu hak akses root. Mode root memberikan akses penuh ke semua perintah dan file sistem tanpa batasan. Pengguna memasukkan perintah sudo su untuk beralih ke mode root, di mana mereka diminta untuk memasukkan password root. Mode ini diperlukan untuk instalasi perangkat lunak dan eksekusi perintah-perintah yang membutuhkan izin administratif. Setelah berada dalam mode root, pengguna dapat menjalankan perintah instalasi dan konfigurasi jaringan yang diperlukan untuk pengujian dan serangan yang akan dilakukan.



Gambar 3 Terminal Kali Linux setelah pengguna memasukkan perintah untuk masuk ke mode root

Hping3

Hping3 merupakan sebuah alat jaringan yang digunakan untuk mengirimkan paket TCP/IP dan melakukan pengujian jaringan. Dengan perintah apt install hping3, pengguna meminta manajer paket apt di Kali Linux untuk mengunduh dan menginstal hping3 dari repositori resmi. Apt adalah alat manajemen paket yang digunakan untuk mengelola perangkat lunak di sistem berbasis Debian, termasuk Kali Linux. Instalasi hping3 diperlukan agar pengguna dapat melakukan berbagai pengujian jaringan, termasuk simulasi serangan DoS (Denial of Service). Setelah instalasi berhasil, hping3 siap digunakan untuk mengirimkan paket data ke target tertentu.

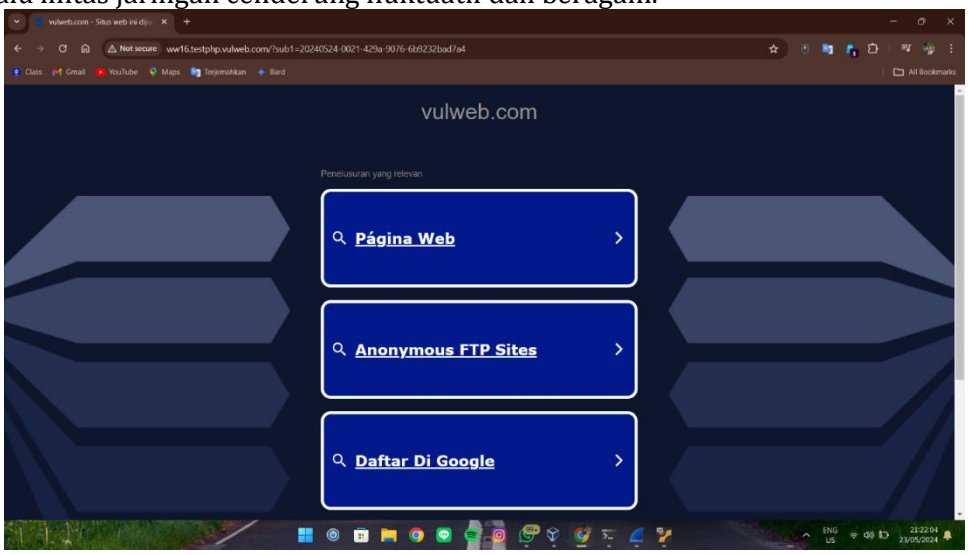


Gambar 4 Proses menginstall Hping3

Dalam penelitian ini, digunakan website dinamis sebagai bahan percobaan untuk menganalisis dan menguji efektivitas metode pendeteksian serangan yang diteliti. Website dinamis dipilih karena karakteristiknya yang lebih kompleks dan interaktif dibandingkan dengan website statis, sehingga lebih rentan terhadap berbagai jenis serangan DDoS. Dengan

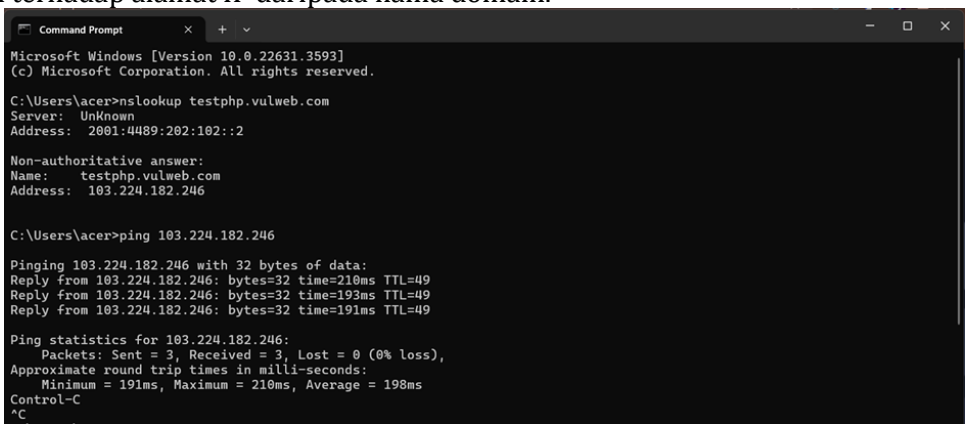
DOI: https://doi.org/10.62017/tektonik

menggunakan website dinamis, penelitian ini dapat mensimulasikan lingkungan jaringan yang lebih realistis dan menantang, memungkinkan pengujian yang lebih mendalam dan komprehensif terhadap kemampuan model pendeteksian serangan DDoS yang diusulkan. Hal ini juga memungkinkan evaluasi yang lebih akurat mengenai kinerja detektor dalam situasi dunia nyata, di mana lalu lintas jaringan cenderung fluktuatif dan beragam.



Gambar 5 Website dinamis yang digunakan untuk penelitian

Perintah nslookup digunakan untuk menyelesaikan nama domain menjadi alamat IP. Dalam konteks ini, pengguna perlu mengetahui alamat IP dari situs web target untuk melakukan pengujian jaringan. Perintah ini akan menghubungi server DNS dan mengembalikan alamat IP yang terkait dengan domain yang dimasukkan. Dalam gambar, terlihat bahwa perintah nslookup testphp.vulweb.com menghasilkan alamat IP dari situs web tersebut. Informasi ini adalah langkah awal yang penting untuk pengujian lebih lanjut, karena pengujian jaringan dan serangan biasanya dilakukan terhadap alamat IP daripada nama domain.



Gambar 6 Pengecekan alamat IP dan pengecekan akses IP Website

Setelah mendapatkan alamat IP dari situs web target menggunakan nslookup, langkah berikutnya adalah memastikan bahwa alamat IP tersebut dapat dijangkau dan responsif. Ini dilakukan dengan menggunakan perintah ping. Perintah ping mengirimkan paket ICMP Echo Request ke alamat IP target dan menunggu Echo Reply. Ini menguji apakah alamat IP tersebut dapat diakses dan mengukur waktu round-trip untuk paket-paket tersebut. Dalam gambar, hasil ping menunjukkan bahwa alamat IP target merespons, yang berarti target tersebut aktif dan siap untuk diuji lebih lanjut menggunakan alat seperti hping3.

DOI: https://doi.org/10.62017/tektonik

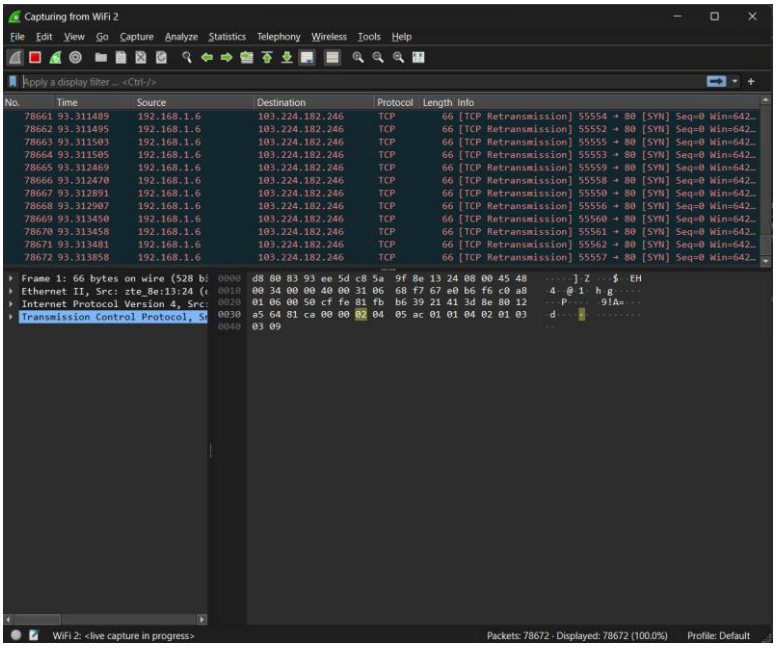
Eksekusi Perintah Hping3

Perintah ini digunakan untuk melakukan serangan DoS dengan membanjiri alamat IP target (103.224.182.246) pada port 80 dengan paket TCP SYN. Parameter -S menunjukkan bahwa paket SYN akan dikirimkan, yang merupakan bagian dari tiga langkah handshake TCP yang digunakan untuk memulai koneksi. Parameter --flood digunakan untuk mengirimkan paket sebanyak mungkin tanpa menunggu tanggapan, sehingga membanjiri target dengan lalu lintas jaringan. Parameter -p 80 menunjukkan bahwa paket akan dikirimkan ke port 80, yang biasanya digunakan untuk lalu lintas HTTP. Jika terminal menampilkan aktivitas pengiriman paket seperti yang terlihat di gambar, ini menunjukkan bahwa perintah hping3 berhasil dieksekusi dan paket sedang dikirimkan ke target.

Gambar 7 Proses eksekusi dengan perintah sudo hping3 -S --flood -p 80

Memantau Paket Data di Wireshark

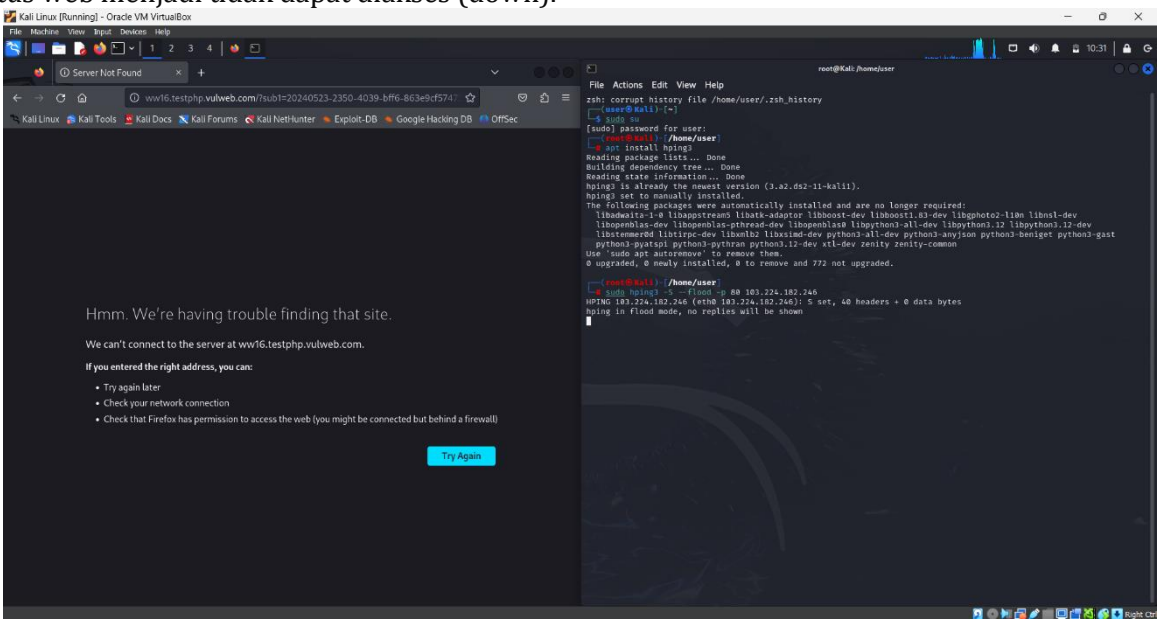
Wireshark adalah alat analisis jaringan yang digunakan untuk menangkap dan menampilkan paket data yang melintasi jaringan. Dalam gambar ini, Wireshark digunakan untuk memantau lalu lintas yang dihasilkan oleh perintah hping3. Jika serangan DoS berhasil, akan terlihat banyak paket data dengan alamat IP target sebagai 'destination'. Wireshark memungkinkan pengguna untuk melihat detail dari setiap paket, termasuk sumber, tujuan, protokol yang digunakan, dan informasi lainnya. Penggunaan Wireshark dalam konteks ini adalah untuk mengkonfirmasi bahwa paket-paket SYN yang dikirimkan oleh hping3 benar-benar mencapai target dan membanjiri jaringan dengan lalu lintas yang dirancang untuk mengganggu layanan.



Gambar 8 Wireshark yang menunjukkan banyak paket data menuju ke IP target

DOI: https://doi.org/10.62017/tektonik

Ketika situs web target menerima sejumlah besar paket data secara terus menerus, server yang menghosting situs web tersebut dapat menjadi kewalahan dan tidak dapat menangani lalu lintas yang sah. Ini dapat menyebabkan penurunan kinerja yang signifikan, atau bahkan membuat situs web menjadi tidak dapat diakses (down).



Gambar 9 Serangan DoS Berhasil

Hasil ini menunjukkan bahwa serangan DoS berhasil karena situs web target dibanjiri dengan paket data sehingga menyebabkan gangguan pada layanan normal. Dampak dari serangan ini biasanya terlihat pada pengguna akhir yang tidak dapat mengakses situs web atau mengalami keterlambatan yang signifikan.

KESIMPULAN

Penelitian ini berhasil menunjukkan bahwa penggunaan multilayer perceptrons (MLP) yang dikombinasikan dengan pemilihan fitur sekuensial dan mekanisme umpan balik dapat meningkatkan efektivitas deteksi serangan Distributed Denial of Service (DDoS) pada jaringan. Hasil eksperimen menunjukkan bahwa metode yang diusulkan mampu memilih fitur optimal yang memberikan kinerja deteksi yang baik selama fase pelatihan. Selain itu, mekanisme umpan balik yang dirancang dapat secara dinamis memperbaiki kinerja detektor ketika terdeteksi kesalahan deteksi yang signifikan, sehingga meningkatkan ketahanan detektor terhadap perubahan lalu lintas jaringan.

Dalam pengujian terhadap website dinamis, metode ini terbukti dapat mendeteksi serangan DDoS dengan akurasi yang tinggi dan mempertahankan kinerja yang stabil. Selain itu, metode ini juga memastikan bahwa permintaan layanan yang sah tetap terlayani dengan baik, sehingga server dapat berfungsi secara optimal meskipun berada di bawah serangan. Perbandingan dengan beberapa penelitian terkait menunjukkan bahwa metode kami mampu menghasilkan kinerja deteksi yang sebanding atau bahkan lebih baik, dengan keunggulan tambahan dalam kemampuan adaptif untuk memperbaiki detektor saat kinerjanya menurun.

Secara keseluruhan, penelitian ini mengonfirmasi bahwa pendekatan berbasis MLP dengan pemilihan fitur sekuensial dan mekanisme umpan balik adalah solusi yang efektif untuk mendeteksi dan menangani serangan DDoS pada lingkungan jaringan yang kompleks dan dinamis. Metode ini tidak hanya meningkatkan kinerja deteksi, tetapi juga memberikan fleksibilitas dan adaptabilitas yang diperlukan untuk menghadapi berbagai tantangan dalam keamanan jaringan saat ini.

DOI: https://doi.org/10.62017/tektonik

DAFTAR PUSTAKA

Hamdani, F., Bella Fitriana, Y., & Oper, N. (2023). KLIK: Kajian Ilmiah Informatika dan Komputer Analisis Keamanan Website Terhadap Serangan DDOS Menggunakan Metode National Institute of Standards and Technology (NIST). *Media Online)*, *3*(6), 1296–1302. https://doi.org/10.30865/klik.v3i6.830

Nisa, A. R., Wijayanto, A. D., Prabudi, A., Priana, J., & Setiawan, A. (2024). *Analisis Log Server untuk mendeteksi Serang DDoS pada Keamaan Jaringan di Website*. *3*, 1–17.

Nisa, F., & Ramadona, S. (2023). Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN. *Jurnal Sistim Informasi Dan Teknologi*, *5*(3), 1–8. https://doi.org/10.60083/jsisfotek.v5i3.269

Risyad, E., Data, M., & Pramukantoro, E. S. (2018). Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Suricata Dalam Mendeteksi Serangan TCP SYN Flood. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(9), 2615–2624.

Saputro, A., Saputro, N., & Wijayanto, H. (2020). Metode Demilitarized Zone dan Port Knocking untuk Keamanan Jaringan Komputer. *CyberSecurity Dan Forensik Digital*, *3*(2), 23.

Satria, M. N. D. (2016). Bentuk Serangan DoS (Denial of Service) dan DDoS (Distributed Deial of Service) pada Jaringan NDN (Named Data Network). *ACADEMIA (Accelerating the World's Research)*, *5241*.