NAMA : RIZKY ADHITYA

KELAS :JK-A

NIM :105841114123

---

1. DEFINISI DOS

   Denial of Service (DoS) adalah jenis serangan siber yang bertujuan untuk membuat mesin, layanan, atau sumber daya jaringan tidak tersedia bagi pengguna yang sah (pengguna yang berhak).

   Serangan ini dilakukan dengan cara mengganggu layanan host yang terhubung ke internet, biasanya dengan membanjiri (flooding) mesin target dengan lalu lintas data yang berlebihan atau mengirimkan informasi yang memicu crash. Akibatnya, target kehabisan sumber daya (CPU, RAM, atau Bandwidth) dan tidak dapat melayani permintaan yang masuk.

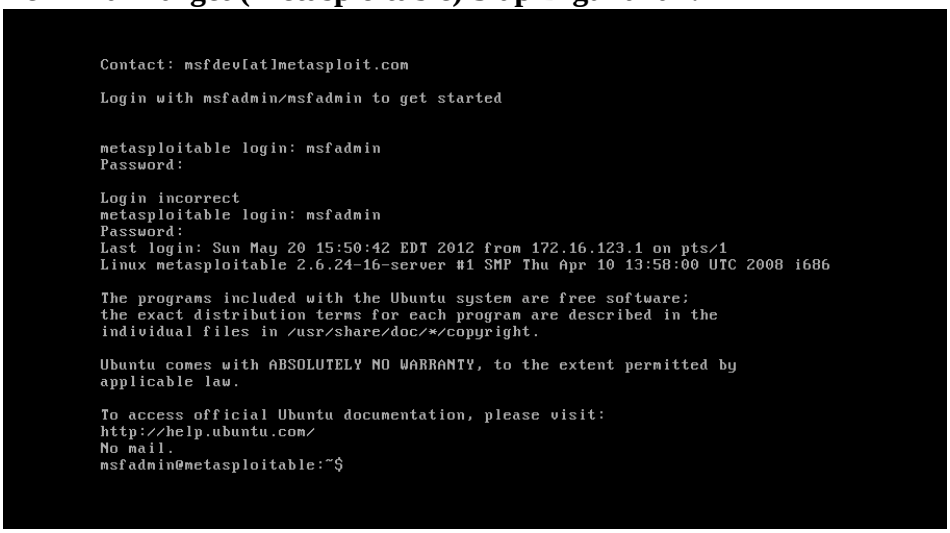
2. SKENARIO PRAKTIKUM

   Skenario praktikum ini mensimulasikan serangan Denial of Service (DoS) dalam lingkungan virtual menggunakan VMware yang menghubungkan Kali Linux sebagai penyerang dan Metasploitable sebagai target. Pengujian dimulai dengan melancarkan serangan SYN Flood menggunakan hping3 dan Slowloris yang mengakibatkan sistem target mengalami kelumpuhan sumber daya, ditandai dengan lonjakan Load Average mencapai 7.91 dan tingginya aktivitas proses kernel.

   Sebagai respons, diterapkan mekanisme pertahanan menggunakan konfigurasi firewall iptables untuk membatasi laju koneksi. Hasilnya, skenario ditutup dengan keberhasilan mitigasi di mana kinerja sistem target kembali stabil dengan Load Average turun menjadi 0.07, membuktikan bahwa paket serangan berhasil diblokir sebelum membebani prosesor utama.

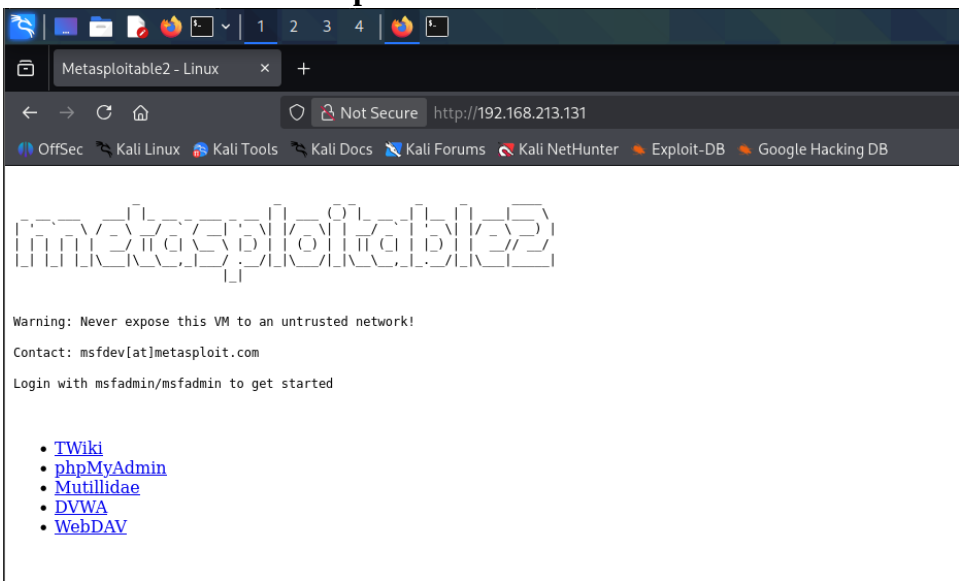
3. LANGKAH PRAKTIKUM

   a. Terminal Target (Metasploitable) Siap Digunakan.



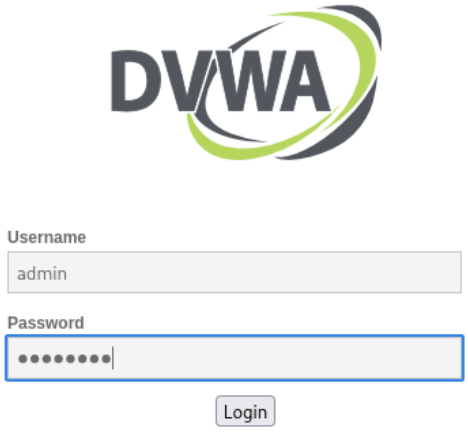
Sebelum dilakukan pengujian serangan, langkah pertama adalah memastikan mesin target (Metasploitable 2) telah berjalan dengan baik. Gambar di atas menunjukkan proses login berhasil dilakukan menggunakan kredensial default (msfadmin/msfadmin). Sistem target beroperasi pada kernel Linux versi 2.6.24 dan siap menerima koneksi jaringan. Terminal ini selanjutnya digunakan untuk memantau kondisi resource sistem (CPU dan RAM) selama simulasi serangan berlangsung.

b. Halaman Interface Metasploit



Melalui peramban web (browser), alamat IP target 192.168.213.131 dapat diakses dengan sukses dan menampilkan halaman antarmuka utama Metasploitable2. Hal ini mengonfirmasi bahwa layanan web (Port 80) dalam status terbuka (Open) dan dapat dijangkau dari jaringan luar, yang memvalidasi bahwa target siap menerima lalu lintas jaringan sebelum serangan dimulai.

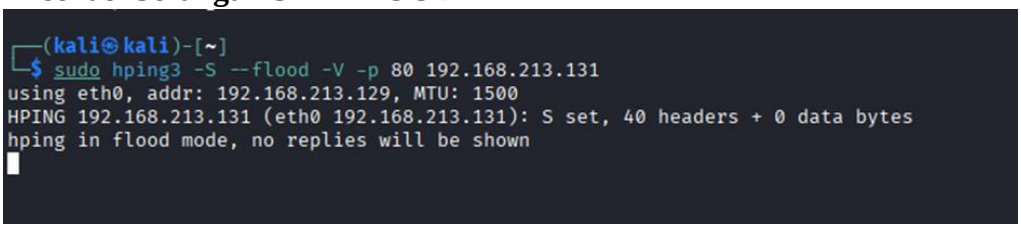
c. Halaman DVWA



Gambar ini memperlihatkan halaman otentikasi dari aplikasi Damn Vulnerable Web App (DVWA) yang di-hosting pada server target. Tampilan halaman login ini memvalidasi bahwa aplikasi web berfungsi dengan baik dan dapat

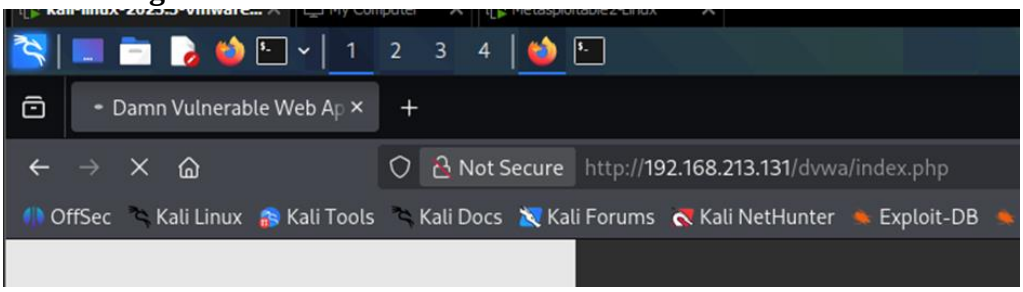
diinteraksikan oleh pengguna. Dalam konteks praktikum ini, DVWA menjadi salah satu target spesifik untuk menguji ketahanan aplikasi web terhadap lonjakan lalu lintas data

d. Eksekusi Serangan SYN FLOOD



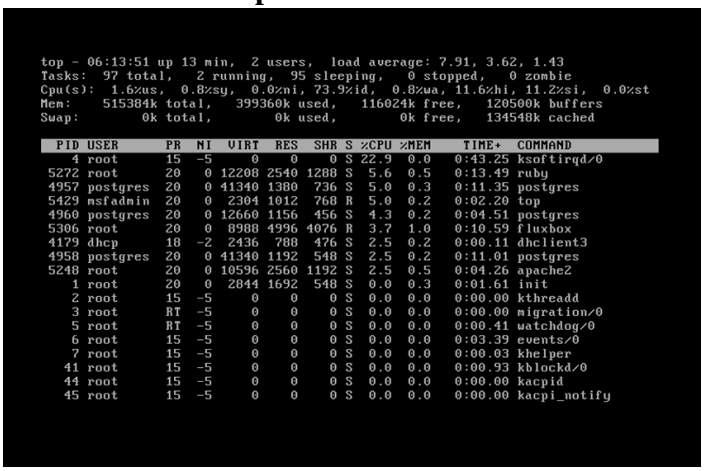
Gambar ini mendokumentasikan proses eksekusi serangan dari mesin penyerang (Kali Linux). Perintah hping3 dijalankan dengan parameter -S (mengirim paket SYN), --flood (mengirim paket secepat mungkin tanpa menunggu balasan), dan -p 80 (menargetkan port web server). Output 'hping in flood mode' menandakan bahwa alat tersebut sedang membanjiri target 192.168.213.131 dengan paket inisiasi TCP secara masif untuk menghabiskan sumber daya koneksi server.

e. Efek serangan ke Web



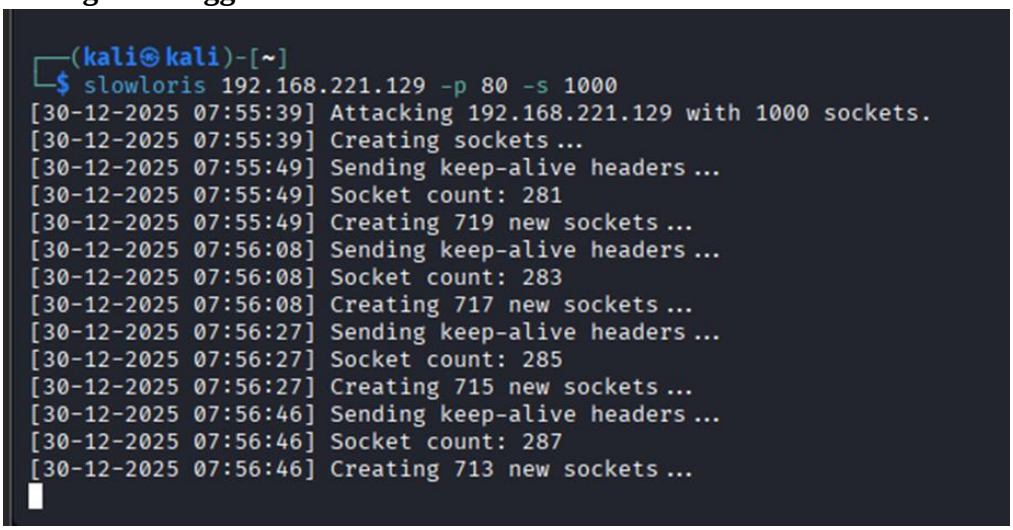
Gambar ini mendemonstrasikan dampak nyata serangan Denial of Service (DoS) dari sudut pandang pengguna (client-side). Saat pengguna mencoba mengakses aplikasi DVWA melalui alamat http://192.168.213.131/dvwa/index.php, peramban web (browser) mengalami kondisi loading yang berkepanjangan atau tidak merespons (hang). Kegagalan memuat halaman ini membuktikan bahwa layanan web server telah lumpuh dan tidak mampu memproses permintaan HTTP yang sah (legitimate request) karena sumber daya sistem sedang habis terkuras melayani banjir paket serangan

f. Tampilan CPU Load di metasploit



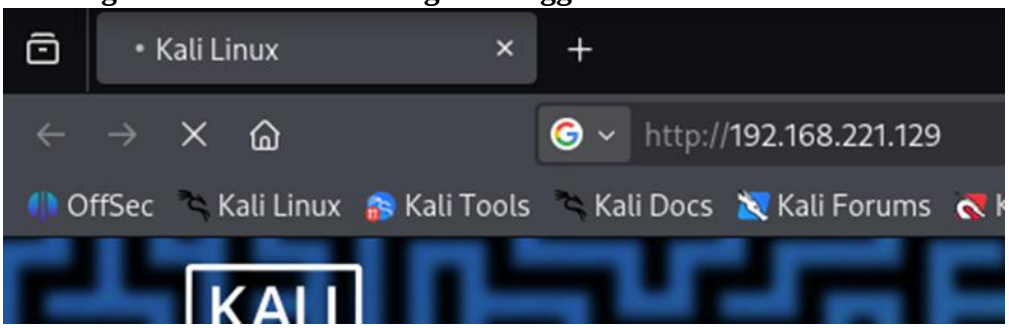
Gambar ini menyajikan bukti empiris dampak serangan DoS terhadap stabilitas sistem target. Berdasarkan pemantauan real-time menggunakan utilitas top, terlihat anomali kritis di mana Load Average (beban rata-rata sistem) melonjak drastis hingga mencapai angka 7.91 dalam satu menit terakhir. Indikator utama keberhasilan serangan terlihat pada tingginya aktivitas proses ksoftirqd/0 yang mendominasi penggunaan CPU sebesar 22.9%. Hal ini, diperkuat dengan nilai Hardware Interrupts (%hi) sebesar 11.6% dan Software Interrupts (%si) sebesar 11.2%, mengonfirmasi bahwa prosesor sedang terkuras dayanya hanya untuk menangani ribuan interupsi paket jaringan yang membanjiri antarmuka, sehingga menghambat kinerja layanan aplikasi lainnya.

g. Serangan Menggunakan Slowris



Gambar ini mendokumentasikan proses eksekusi serangan Application Layer DoS menggunakan alat Slowloris. Perintah dijalankan dengan parameter -s 1000 yang bertujuan membuka 1.000 koneksi secara bersamaan ke port 80 target. Output terminal secara jelas menampilkan aktivitas alat yang terus-menerus mengirimkan keep-alive headers untuk mempertahankan koneksi agar tetap 'hidup' (terbuka) dalam waktu lama tanpa menyelesaikannya. Mekanisme ini terlihat pada log 'Creating... new sockets' dan 'Sending keep-alive headers', yang bertujuan memenuhkan tabel koneksi server (connection pool) dengan koneksi gantung, sehingga server kehabisan sumber daya untuk menerima permintaan baru dari pengguna yang sah.

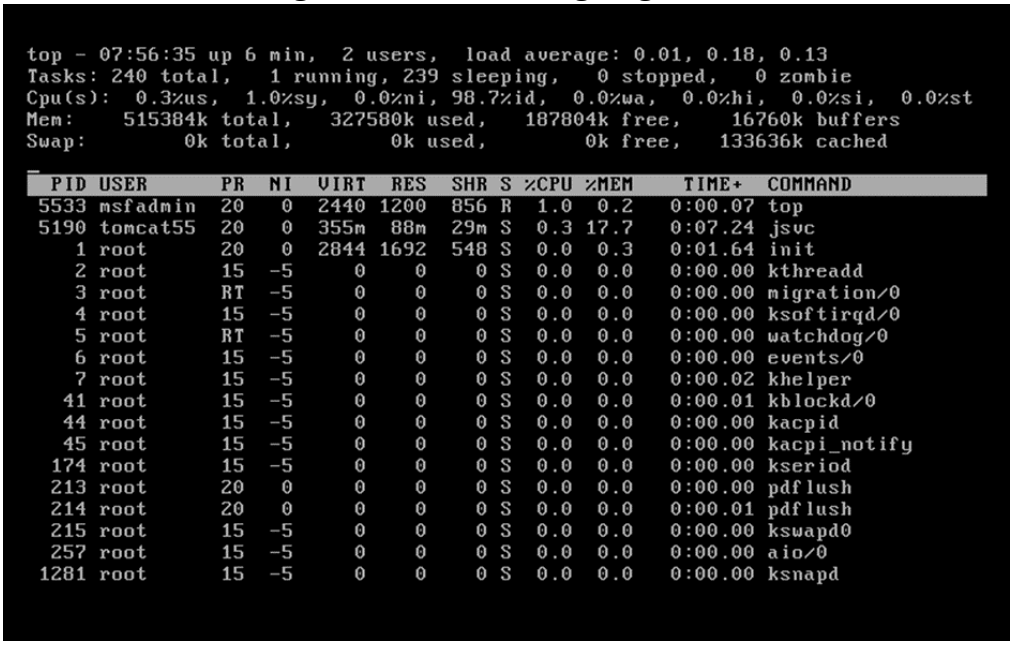
h. Loading Lama Efek dari serangan menggunakan Slowloris



Gambar ini memvisualisasikan dampak serangan Application Layer DoS (Slowloris) terhadap pengalaman pengguna. Saat peramban web mencoba mengakses alamat IP target 192.168.221.129, situs mengalami kondisi loading

yang tidak berkesudahan (infinite loading). Hal ini terjadi karena serangan Slowloris telah berhasil memenuhkan seluruh slot koneksi (connection pool) pada web server Apache dengan koneksi lambat. Akibatnya, permintaan akses yang sah dari browser ini diterima oleh server tetapi masuk ke dalam antrean panjang yang macet, sehingga server tidak pernah mengirimkan respon balik dan halaman web tetap kosong (stuck).

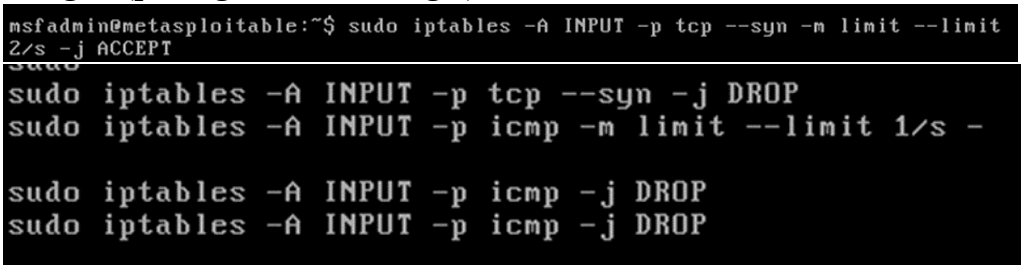
i. CPU Load saat serangan Slowloris berlangsung

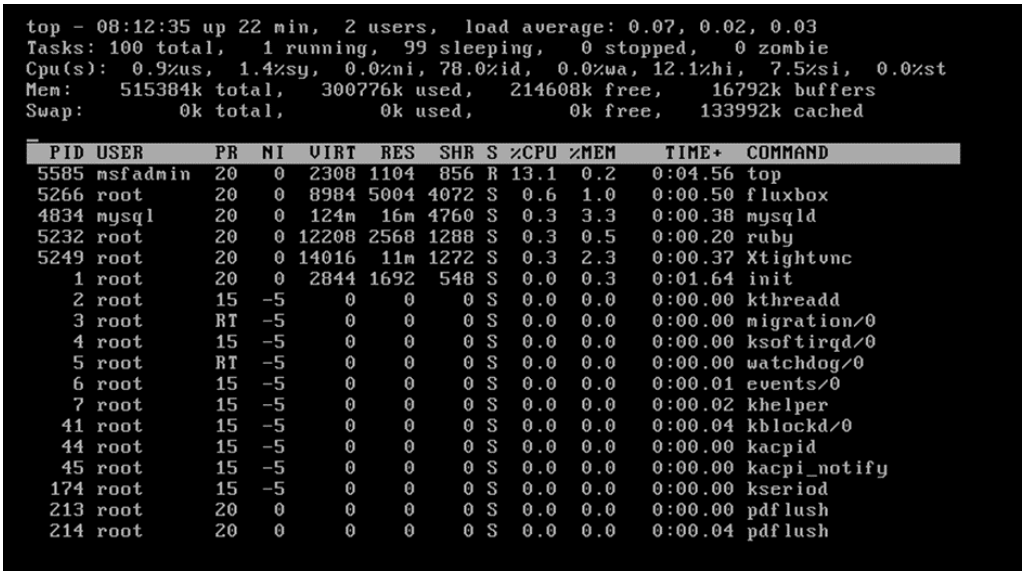


Gambar ini memperlihatkan fenomena menarik yang menjadi ciri khas serangan Application Layer DoS seperti Slowloris. Berbeda dengan serangan flooding yang membuat CPU melonjak, di sini terlihat Load Average sangat rendah di angka 0.01 dan CPU dalam keadaan 98.7% idle (menganggur).

Kondisi ini membuktikan bahwa serangan Slowloris tidak bertujuan menghabiskan kemampuan pemrosesan (processing power) server, melainkan menghabiskan ketersediaan slot koneksi (connection pool). Server 'tertipu' untuk menunggu ribuan koneksi yang menggantung tanpa melakukan aktivitas berat, sehingga secara statistik sistem terlihat sehat/santai, padahal layanan web sebenarnya sudah lumpuh total dan tidak dapat diakses oleh pengguna lain.

j. Mitigasi (pasang firewall di target)





Sebagai upaya penanggulangan serangan, diterapkan konfigurasi firewall menggunakan iptables untuk membatasi laju trafik berbahaya. Aturan disusun dengan mekanisme rate-limiting di mana sistem dikonfigurasi untuk hanya mengizinkan maksimal 2 paket SYN per detik dan secara otomatis membuang (DROP) sisa paket TCP maupun ICMP yang melebihi batas tersebut. Efektivitas mitigasi ini terbukti melalui hasil pemantauan sistem, di mana Load Average turun drastis ke angka stabil 0.07 yang menandakan pemulihan kinerja CPU, meskipun indikator Hardware Interrupts (%hi) yang bertahan tinggi di angka 12.1% menegaskan bahwa firewall sedang bekerja aktif memblokir gempuran trafik serangan yang masih terus menghantam antarmuka jaringan.

4. Kesimpulan

Berdasarkan hasil praktikum simulasi dan mitigasi serangan Denial of Service (DoS), dapat disimpulkan bahwa serangan DoS memiliki karakteristik dampak yang berbeda tergantung pada metodenya. Serangan SYN Flood yang dilakukan menggunakan hping3 terbukti melumpuhkan target dengan cara menghabiskan sumber daya komputasi, ditandai dengan lonjakan Load Average ekstrem hingga 7.91 dan tingginya aktivitas proses kernel ksoftirqd. Sebaliknya, serangan Slowloris pada Layer Aplikasi berhasil melumpuhkan layanan web dengan cara menghabiskan slot koneksi (connection exhaustion) tanpa membebani CPU, yang dibuktikan dengan Load Average yang tetap rendah (0.01) meskipun layanan tidak dapat diakses.

Penerapan mitigasi menggunakan firewall iptables dengan metode rate-limiting terbukti sangat efektif dalam menangani serangan berbasis volume seperti SYN Flood. Hal ini dikonfirmasi dengan pulihnya stabilitas sistem target di mana Load Average turun drastis menjadi 0.07. Temuan penting dalam praktikum ini adalah tingginya nilai Hardware Interrupts (%hi) sebesar 12.1% pasca-mitigasi, yang menunjukkan bahwa firewall bekerja secara efisien memblokir paket serangan tepat di antarmuka jaringan sebelum paket tersebut sempat membebani prosesor utama, sehingga ketersediaan layanan (Availability) tetap terjaga.