(2025), 3 (6): 116-129 **Scientica** 3021-8209

Jurnal Ilmiah Sain dan Teknologi

ANALISIS PENETRATION TESTING MELALUI SIMULASI SERANGAN DENIAL OF SERVICE (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KUBU RAYA)

Irani Kamil [1], Haried Novriando [2], Muhammad Azhar Irwansyah [3]
Jurusan Informatika, Fakultas Teknik, Universitas Tanjungpura
Jl. Prof. Dr. H. Hadari Nawawi, Pontianak 78124
[1] iranikamil7@gmail.com

Abstrak (Indonesia)
Keamanan jaringan menjadi salah satu aspek penting dalam mengantisipasi ancaman serangan siber yang terus berkembang, termasuk serangan Denial of Service (DoS). Penelitian ini bertujuan untuk mengevaluasi keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kubu Raya menggunakan metode Packet Filtering dan Penetration Testing. Implementasi metode ini dilakukan untuk mendeteksi, menganalisis, dan mencegah potensi ancaman yang dapat mengganggu operasional jaringan. Penelitian ini melibatkan beberapa tahapan, yaitu observasi lapangan, identifikasi masalah, perencanaan tindakan, pengumpulan informasi menggunakan tools seperti Nmap dan Nessus, serta simulasi serangan DoS meliputi UDP Flood, SYN Flood, dan ICMP Flood. Selanjutnya, dilakukan implementasi Packet Filtering pada router MikroTik menggunakan Firewall Filter Rule dan Firewall RAW untuk memitigasi serangan. Hasil penelitian menunjukkan bahwa sebelum implementasi Packet Filtering, serangan DoS menyebabkan penggunaan CPU router meningkat hingga 100%, yang mengganggu kinerja sistem. Setelah implementasi Firewall Filter Rule, penggunaan CPU turun signifikan hingga 22% pada serangan UDP Flood dan 6% pada serangan ICMP Flood. Dengan Firewall RAW, kesesuaian mitigasi serangan meningkat lebih baik, dengan penggunaan CPU hanya 13% pada serangan UDP Flood dan 3% pada serangan ICMP Flood. Kesimpulannya, metode Packet Filtering terbukti efektif dalam mencegah serangan DoS. Firewall RAW lebih efisien dibandingkan Firewall Filter Rule, terutama dalam meminimalkan penggunaan sumber daya router.

Sejarah Artikel
Submitted: 10 September 2025
Accepted: 13 September 2025
Published: 14 September 2025

Kata Kunci
keamanan jaringan, Packet Filtering, Penetration Testing, Denial of Service, MikroTik

I. PENDAHULUAN

Perkembangan internet telah memberikan dampak besar dalam berbagai aspek kehidupan, mulai dari komunikasi, pendidikan, hingga pemerintahan [1]. Namun di balik manfaat tersebut terdapat ancaman serius berupa serangan siber yang dapat mengganggu keamanan dan ketersediaan layanan jaringan. Salah satu serangan yang paling berbahaya adalah Denial of Service (DoS), yaitu upaya melumpuhkan layanan dengan membanjiri sistem menggunakan trafik berlebihan hingga sumber daya jaringan tidak dapat merespons pengguna yang sah [2]. Dinas Komunikasi dan Informatika Kabupaten Kubu Raya yang menggunakan perangkat MikroTik sebagai backbone jaringan juga menghadapi potensi gangguan seperti boom traffic dan brute force login, yang dapat mengancam kelancaran layanan publik berbasis jaringan. Untuk itu, diperlukan evaluasi keamanan melalui penetration testing guna mengidentifikasi kerentanan serta menguji efektivitas mekanisme pertahanan yang ada. Penelitian ini difokuskan pada pengujian dan analisis keamanan jaringan terhadap serangan DoS, dengan tujuan memberikan rekomendasi teknis yang dapat digunakan sebagai panduan praktis dalam meningkatkan keamanan jaringan di lingkungan pemerintah daerah.

II. METODE

Penelitian ini menggunakan metode pengujian Penetration Testing Execution Standart (PTES)terhadap router MikroTik RB941-2nD yang dikonfigurasi sebagai simulasi jaringan Dinas Komunikasi dan Informatika Kabupaten Kubu Raya. Penetration Testing Execution Standard (PTES) merupakan standar metodologi yang mengatur langkah-langkah pelaksanaan uji penetrasi secara terstruktur. PTES digunakan dalam penelitian ini karena menyediakan tahapan yang jelas dan praktis, sehingga memudahkan pemahaman dan penerapan oleh pengguna yang bukan spesialis keamanan [3].

A. *Alat Penelitian*

Penelitian ini menggunakan perangkat keras dan perangkat lunak untuk menganalisis serangan, perangkat yang dipakai adalah sebagai berikut:

a. Perangkat Keras

Perangkat keras yang digunakan meliputi:

No	Nama Perangkat	Spesifikasi	Keterangan
1	Laptop MSI GF63 Thin 9SCXR	Intel Core i5-9300H (2,4GHz up to 4,1 GHz) 8GB DDR4 RAM (2666MHz), 256 GB NVMe SSD, GTX 1650	Untuk Simulasi Penyerangan
2	Macbook Air 2013	Intel Core i5 1,3 GHz with HD Graphics 5000 VRAM1,5 GB, 4 GB RAM, 256 GB SSD	Untuk untuk memonitoring serangan
3	Mikrotik RB941-2nD	Processor 650Mhz, 4 Port Fast Ethernet	Untuk simulasi target serangan
4	PC	Processor i3-2, 2GB RAM	Untuk testing dampak serangan

b. Perangkat Lunak

Perangkat lunak yang digunakan meliputi:

No	Jenis Software	Versi
1	Winbox	3.21
2	Nmap	7.94
3	Nessus	10.8.3
4	Hping3	3.0.0-alpha-2
5	Dradis	4.8.0
6	OS Kali Linux	2024.2
7	MacOS Big Sur	11.7.9

B. *Langkah Penelitian*

Penelitian ini menggunakan metodologi yang mencakup beberapa Langkah yang dapat dilihat pada Gambar. 1

Gambar. 1 Langkah Penelitian

a. Studi Literatur
Penelitian diawali dengan studi literatur yang berfokus pada pengumpulan referensi mengenai metode packet filtering dan penetration testing. Sumber acuan meliputi buku, jurnal ilmiah, dan artikel daring yang terverifikasi. Studi ini dimaksudkan untuk memperkuat pemahaman teoritis mengenai konsep dan teknik yang digunakan serta menjadi landasan dalam menentukan data yang dibutuhkan pada tahap observasi lapangan.

b. Observasi Lapangan
Tahap berikutnya adalah observasi lapangan di Dinas Komunikasi dan Informatika Kabupaten Kubu Raya untuk memperoleh data teknis jaringan, seperti alamat IP, perangkat yang terhubung, dan konfigurasi yang digunakan. Berdasarkan hasil observasi, penelitian kemudian difokuskan pada simulasi serangan dari salah satu skenario, yaitu LAN atau WAN, sesuai dengan kondisi yang paling relevan dalam mengidentifikasi potensi kerentanan jaringan.

c. Identifikasi Masalah
Pada tahap identifikasi masalah, penelitian difokuskan pada pemetaan kondisi jaringan di Dinas Komunikasi dan Informatika Kabupaten Kubu Raya. Identifikasi dilakukan untuk menemukan gangguan koneksi, konfigurasi yang tidak efisien, maupun kerentanan pada sistem keamanan. Selain itu, dikaji pula riwayat adanya serangan dari dalam maupun luar jaringan sebagai dasar untuk memahami tingkat keamanan yang tersedia.

d. Perencanaan Tindakan
Perencanaan tindakan bertujuan menganalisis secara spesifik permasalahan yang teridentifikasi untuk menentukan akar penyebabnya. Dalam tahap ini dilaksanakan penetration testing awal sebagai uji coba sistem, sehingga kerentanan yang ada dapat diidentifikasi dan dijadikan landasan dalam merancang aturan packet filtering yang sesuai.

e. Implementasi Packet Filtering

Tahap implementasi packet filtering bertujuan mengonfigurasi sistem agar mampu mendeteksi dan memblokir trafik berbahaya [4]. Pada tahap ini firewall MikroTik dikonfigurasi dengan aturan khusus untuk memfilter jenis serangan yang diteliti, yaitu UDP Flood, ICMP Flood, dan SYN Flood, sehingga sistem dapat lebih terlindungi dari gangguan layanan. Packet filtering digunakan sebagai mekanisme pertahanan terhadap serangan DoS dengan cara memeriksa paket data dan koneksi sebelum diputuskan untuk diterima atau ditolak. Dalam konfigurasi penelitian, jumlah paket yang diizinkan dibatasi hingga 1.500 paket per detik agar konsumsi CPU tetap berada pada rentang 20–30%. Konfigurasi ini mengacu pada dokumentasi MikroTik Packet Flow yang menegaskan bahwa pengguna memiliki kontrol penuh atas setiap aspek pemrosesan paket dalam RouterOS [5].

f. Penetration Testing

Tahap penetration testing dilakukan untuk mengidentifikasi kerentanan jaringan dengan serangkaian proses meliputi perencanaan, information gathering, vulnerability assessment, eksploitasi, post-exploitation, serta reporting and clean up [6]. Pada tahap ini, serangan UDP Flood, ICMP Flood, dan SYN Flood disimulasikan guna menilai kemampuan sistem dalam menghadapi ancaman. Adapun tahapan penetration testing akan dijelaskan dibawah ini:

1) Pada tahap Information Gathering, peneliti akan mengumpulkan informasi sebanyak mungkin tentang target yang akan diuji, termasuk informasi mengenai port yang terbuka, protokol yang digunakan, sistem operasi, dan perangkat lunak (software) yang digunakan. Tahapan ini bertujuan untuk memahami struktur jaringan dan teknologi yang digunakan oleh target, sehingga dapat membantu peneliti dalam mengidentifikasi potensi celah keamanan yang dapat dieksploitasi pada tahap selanjutnya. Tools yang digunakan dalam tahap ini adalah Nmap dengan versi 7.94 pada sistem operasi Kali Linux.
2) Tahap Vulnerability Assessment meliputi klasifikasi, identifikasi, dan evaluasi kerentanan pada sistem jaringan yang diuji dengan tujuan menemukan kelemahan yang dapat dieksploitasi. Proses dilakukan menggunakan Nessus v10.8.3 (Kali Linux) untuk melakukan pemindaian dan pengklasifikasian celah keamanan pada perangkat target.
3) Tahap exploitation bertujuan menguji dan membuktikan bahwa celah yang ditemukan dapat dieksploitasi serta menilai dampak potensialnya. Pada tahap ini dilakukan simulasi serangan UDP Flood, SYN Flood, dan ICMP Flood untuk mengevaluasi sejauh mana kerentanan tersebut memengaruhi kinerja sistem.
4) Setelah eksploitasi, tahap post-exploitation berfokus pada penggalian informasi sensitif dan penilaian dampak lebih mendalam, tools yang digunakan tidak berbeda dari tahap eksploitasi.
5) Tahap terakhir meliputi penyusunan laporan dan kegiatan clean-up. Laporan merangkum hasil information gathering dan vulnerability assessment, memaparkan temuan kerentanan, metodologi pengujian, serta estimasi dampak teknis. Selanjutnya dilakukan pembersihan dan pemulihan sistem yang diuji sehingga kondisi operasional kembali normal tanpa meninggalkan artefak pengujian. Dokumentasi dan konsolidasi temuan dilakukan dengan bantuan Dradis v4.8.0 pada platform Kali Linux.

g. Analisis Data

Tahap analisis data bertujuan menilai penerapan packet filtering berdasarkan hasil penetration testing. Data yang diperoleh dianalisis melalui perbandingan kondisi jaringan sebelum dan sesudah implementasi, termasuk tingkat keberhasilan sistem dalam menahan serangan serta potensi celah keamanan yang masih terdeteksi. Hasil analisis menjadi dasar untuk menjelaskan dampak teknis penerapan packet filtering terhadap keamanan jaringan.

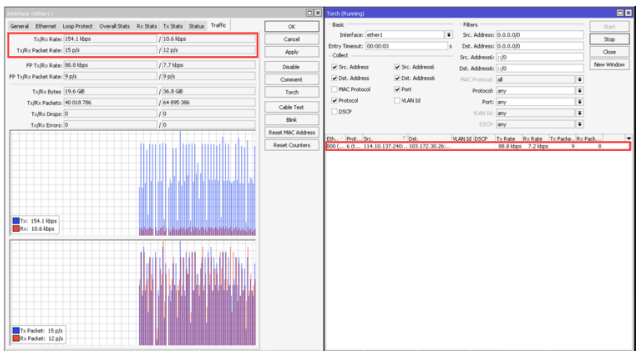
a. Kesimpulan

Kesimpulan disusun pada tahap akhir penelitian dengan merujuk pada hasil pengujian yang telah dilakukan. Bagian ini menekankan sejauh mana konfigurasi packet filtering mampu mendeteksi serta mengurangi dampak serangan selama proses penetration testing.

III. HASIL DAN PEMBAHASAN

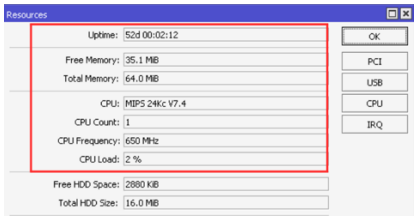
A. Sebelum Terjadi Serangan

Proses awal untuk menganalisis kondisi router sebelum atau saat menghadapi serangan DoS dilakukan dengan memanfaatkan fitur pemantauan pada Winbox, antara lain Traffic, Torch, dan Resources. Menu Traffic menampilkan grafik lalu lintas masuk (Rx) dan keluar (Tx), sedangkan Torch berfungsi sebagai pemantau lalu lintas real-time yang menunjukkan protokol, alamat IP sumber dan tujuan, port yang digunakan, serta volume data. Sementara itu, menu Resources memberikan informasi terkait performa sistem, meliputi versi OS, spesifikasi perangkat keras, penggunaan CPU, kapasitas memori, dan media penyimpanan.



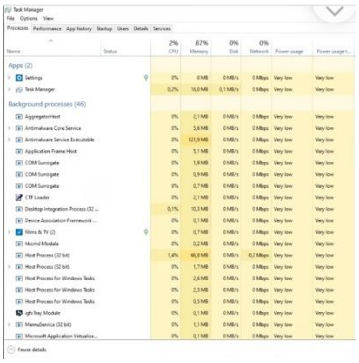
Gambar. 2 Trafic Sebelum Terjadi Serangan

Hasil pemantauan melalui menu Traffic menunjukkan bahwa lalu lintas jaringan masih normal, dengan nilai Tx/Rx rate masing-masing 15 p/s dan 12 p/s, serta ukuran paket 154,1 kbps (Tx) dan 10,6 kbps (Rx). Kondisi ini menandakan router beroperasi stabil tanpa indikasi serangan. Pemantauan melalui Torch juga memperlihatkan hanya satu komunikasi aktif antara klien dan router, sehingga aktivitas jaringan masih dalam batas wajar.



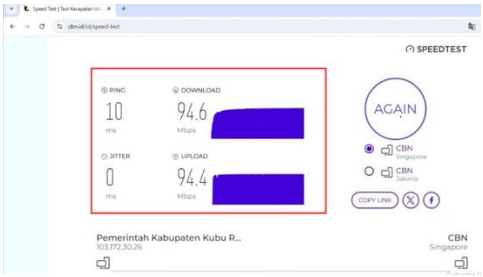
Gambar. 3 Resource Sebelum Terjadi Serangan

Pemantauan melalui menu Resources menunjukkan CPU load sebesar 2% dan memori bebas 35,1 MiB. Kondisi ini menandakan penggunaan sumber daya masih stabil dan belum ada indikasi serangan DoS yang memengaruhi kinerja router.



Gambar. 4 Task Manager pada PC Testing

PC testing digunakan untuk melakukan uji kecepatan jaringan, dengan pemantauan Task Manager menunjukkan penggunaan jaringan 0%. Hal ini mengindikasikan tidak ada aplikasi lain yang mengakses internet, sehingga hasil speedtest tidak dipengaruhi aktivitas eksternal pada perangkat.



Gambar. 5 Bandwith Sebelum Terjadi Serangan

Pengujian kecepatan pada komputer testing menunjukkan hasil unduh 94,6 Mbps dan unggah 94,4 Mbps. Kecepatan ini berasal dari jaringan DISKOMINFO Kuburaya dengan bandwidth dedicated 1 Gbps, namun terbatas hingga 100 Mbps karena router yang digunakan hanya mendukung Fast Ethernet.

B. Implementasi Penetration Testing

Penelitian ini menggunakan metode Grey-box Testing yang berlandaskan pada Penetration Testing Execution Standard (PTES). Pemilihan metode ini dilatarbelakangi oleh keterbatasan informasi yang tersedia, yakni hanya mencakup alamat IP target serta deskripsi umum topologi jaringan di Dinas Komunikasi dan Informatika Kabupaten Kubu Raya. Sebagai bentuk pengujian dengan akses terbatas, Grey-box Testing tidak memberikan kendali penuh terhadap sistem internal, namun tetap memungkinkan pemanfaatan sebagian informasi teknis yang relevan untuk mendukung proses pengujian.

a. Information Gathering

Peneliti menjalankan pemindaian port terhadap target menggunakan Nmap (dengan hak akses root) dan menyimpan hasil pemindaian yang rinci dalam format XML untuk keperluan analisis dengan perintah sudo nmap -Pn -T4 -A -v --reason -oX nmap_scan.xml 103.172.30.26 seperti pada Gambar. 2 dibawah ini:

Gambar. 6 Perintah Nmap

Selanjutnya peneliti akan membuka file nmap_scan.xml dengan zenmap seperti pada Gambar. 3 dibawah ini:

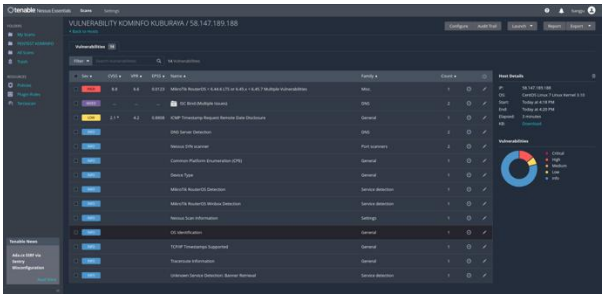
	Port	Protocol	State	Service	Version
×	25	tcp	filtered	smtp	
✓	53	tcp	open	domain	(generic dns response: NOTIMP)
×	445	tcp	filtered	microsoft-ds	
×	646	tcp	filtered	ldp	
✓	2000	tcp	open	bandwidth-test	MikroTik bandwidth-test server
✓	8291	tcp	open	winbox	MikroTik WinBox

Gambar. 7 Hasil Scan Nmap

Hasil pemindaian menunjukkan bahwa perintah Nmap digunakan untuk memastikan ketersediaan alamat IP target, mengidentifikasi port terbuka, mempercepat proses pemindaian, serta memperoleh informasi versi layanan yang berjalan. Dari hasil tersebut, terdeteksi beberapa port penting, antara lain: port 25/tcp (SMTP) dan 445/tcp (Microsoft-DS) dengan status filtered, port 53/tcp (DNS) terbuka namun memberikan respons kesalahan NOTIMP, port 646/tcp (LDP) dengan status filtered, port 2000/tcp terbuka menjalankan layanan MikroTik Bandwidth-Test, serta port 8291/tcp terbuka menjalankan layanan MikroTik Winbox.

b. Vulnerability Assessment

Setelah pengumpulan informasi selesai, pengujian dilanjutkan ke tahap identifikasi kerentanan terhadap target dengan menggunakan alat pemindaian Nessus.



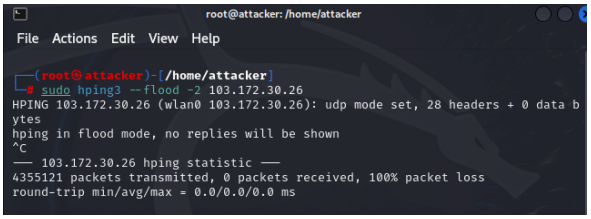
Gambar. 8 Hasil Pemindaian Nessus

Hasil pemindaian kerentanan menunjukkan bahwa RouterOS MikroTik versi sebelum 6.45.7 memiliki empat kelemahan utama, yaitu relative path traversal pada proses parsing NPK, CVE-2019-3977 terkait validasi paket pembaruan, perlindungan yang tidak memadai pada layanan DNS (berpotensi cache poisoning), serta penanganan respons DNS yang tidak tepat. Solusi yang direkomendasikan adalah melakukan pembaruan RouterOS ke versi terbaru. Selain itu, layanan DNS pada perangkat juga memiliki kerentanan berupa keterbukaan terhadap serangan DNS amplification dan recursive query dari IP eksternal, yang dapat dimanfaatkan untuk cache poisoning maupun penurunan kinerja server; mitigasi dapat dilakukan dengan membatasi akses DNS publik dan mengatur agar hanya melayani permintaan dari host internal. Kerentanan lain ditemukan pada layanan ICMP timestamp request, yang memungkinkan kebocoran informasi waktu sistem, sehingga perlu dibatasi melalui penyaringan atau pemblokiran respons ICMP tersebut.

c. Exploitation and Post-Exploitation

1) UDP Flood

Pengujian serangan UDP Flood dilakukan menggunakan hping3 untuk mengirimkan arus paket UDP berkelanjutan ke alamat target dengan tujuan mengevaluasi penurunan kinerja perangkat. Eksperimen dimulai dengan memperoleh hak akses root (perintah sudo su), kemudian mengeksekusi perintah serangan **hping3 -2 -flood <IP target>.** Serangan dijalankan selama 5 menit untuk mengamati dampak pada kinerja layanan, dan dihentikan secara manual oleh penguji.

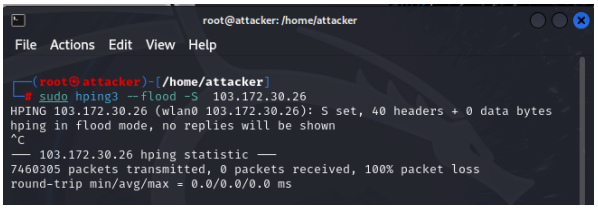


Gambar. 9 Menjalankan Tools UDP Flood pada Hping3

Selama serangan UDP Flood, penyerang mengirimkan total 4.355.121 paket UDP ke target; tidak ada paket yang diterima kembali (0 paket), sehingga tercatat packet loss 100%, yang mengakibatkan gangguan layanan dan penurunan kinerja sistem.

2) SYN Flood

Serangan kedua berupa SYN Flood dilaksanakan menggunakan hping3 dengan tujuan membanjiri permintaan koneksi TCP ke target sehingga menguras sumber daya dan menurunkan kinerja layanan. Pelaksanaan dimulai dengan memperoleh hak akses root (sudo su) lalu mengeksekusi perintah serangan **hping3 -S -flood <IP target>**. Serangan dijalankan selama 5 menit untuk mengevaluasi dampaknya terhadap kestabilan sistem dan dihentikan secara manual oleh penguji.

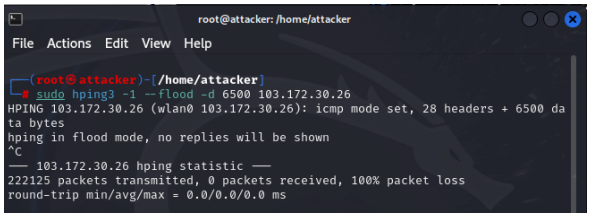


Gambar. 10 Menjalankan tools SYN Flood pada Hping3

Selama serangan SYN Flood, penguji mengirimkan total 7.460.305 paket SYN ke target; tidak ada paket balasan yang diterima (0 paket), sehingga tercatat packet loss 100%, kondisi yang menyebabkan gangguan layanan dan penurunan kinerja sistem.

3) ICMP Flood

Serangan terakhir berupa ICMP Flood dilaksanakan menggunakan hping3 dengan parameter yang menghasilkan pengiriman paket ICMP berukuran 6.500 byte secara terus-menerus untuk menguji dampak terhadap ketersediaan layanan. Pelaksanaan diawali dengan memperoleh hak akses root (sudo su) lalu mengeksekusi perintah **hping3 -1 -flood -d 6500 <IP target>**. Serangan dijalankan selama 5 menit untuk mengamati penurunan kinerja atau kegagalan layanan, dan dihentikan secara manual oleh penguji.



Gambar. 11 Menjalankan Tools ICMP Flood pada Hping3

Selama serangan ICMP Flood, penguji mengirimkan paket ICMP berukuran 6.500 byte secara masif hingga menyebabkan gangguan layanan dan penurunan kinerja sistem. Tercatat sebanyak 222.125 paket terkirim, tanpa ada paket balasan (0 paket), dengan hasil packet loss 100%.

d. Report and Clean Up

Pada tahap ini, peneliti menyusun laporan hasil pengujian dan simulasi serangan dengan memanfaatkan tools Dradis, yang digunakan untuk mendokumentasikan kegiatan penetration testing pada keamanan jaringan di Dinas Komunikasi dan Informatika Kabupaten Kubu Raya.

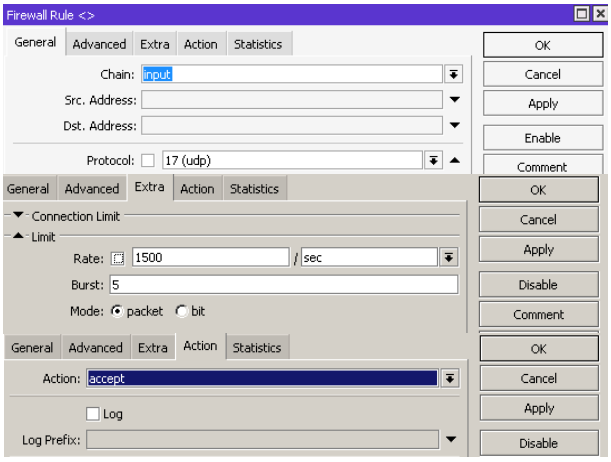
Gambar. 12 Hasil Laporan Dradis

Hasil konsolidasi Dradis, yang menggabungkan keluaran pemindaian Nmap dan Nessus, menunjukkan status port pada router MikroTik target: port 53, 2000, dan 8291 berstatus open, mengindikasikan layanan DNS, Bandwidth Test Server, dan antarmuka manajemen Winbox aktif dan dapat diakses dari luar, sedangkan port 25, 445, dan 646 berstatus filtered, menunjukkan adanya penyaringan oleh mekanisme keamanan atau konfigurasi jaringan. Pola konfigurasi ini mengindikasikan eksposur layanan sensitif—khususnya layanan manajemen—ke jaringan eksternal. Untuk serangan berbasis hping3, tidak disertakan entri terperinci dalam laporan karena tujuan pengujian adalah mengamati efek pembanjiran lalu lintas (flood) terhadap ketersediaan dan konsumsi sumber daya router, bukan mendokumentasikan respon aplikasi tingkat layanan.

C. Implementasi Packet Filtering

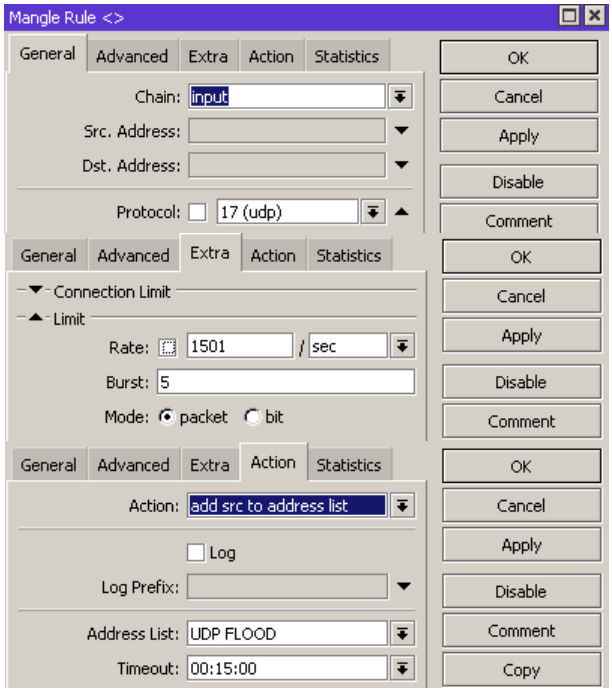
Sebagai bagian dari upaya mitigasi serangan DoS, penelitian ini menerapkan packet filtering pada router MikroTik. Penerapan ini dilakukan melalui konfigurasi firewall yang berfungsi memeriksa setiap paket data serta menentukan apakah lalu lintas diizinkan atau diblokir berdasarkan aturan yang ditetapkan.

a. Rule Firewall Filter Rule



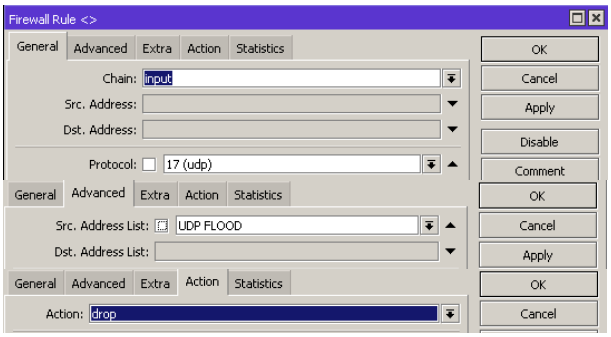
Gambar. 13 Konfigurasi Rule Accept

Peneliti mengonfigurasi firewall filter rule pada chain input untuk memfilter lalu lintas UDP (protocol 17) dengan batas maksimum 1.500 paket per detik dan burst bernilai 5, serta menetapkan action accept, sehingga hanya paket sesuai batas tersebut yang diizinkan masuk ke router.



Gambar. 14 Konfigurasi Mangle

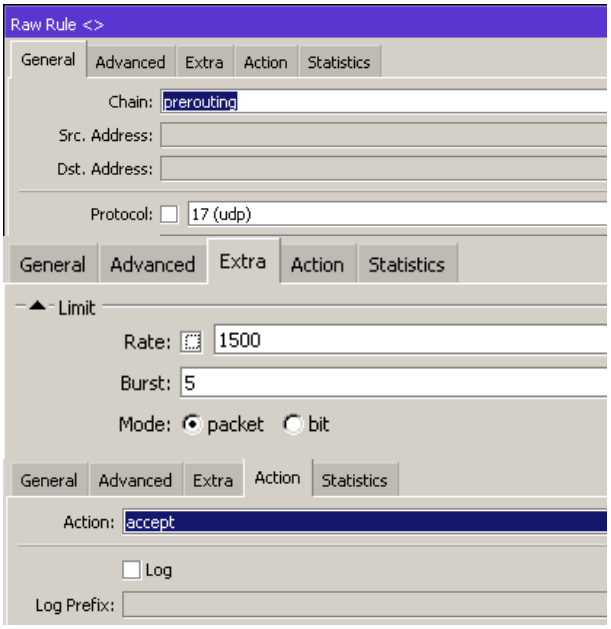
Setelah membuat aturan untuk mengizinkan lalu lintas masuk, peneliti menambahkan rule mangle pada chain input untuk mendeteksi potensi serangan UDP. Aturan ini membatasi lalu lintas hingga 1.501 paket per detik dengan burst 5, dan jika terlampaui, alamat sumber akan ditambahkan ke address list "UDP FLOOD" selama 15 menit.



Gambar. 15 Konfigurasi Rule Drop

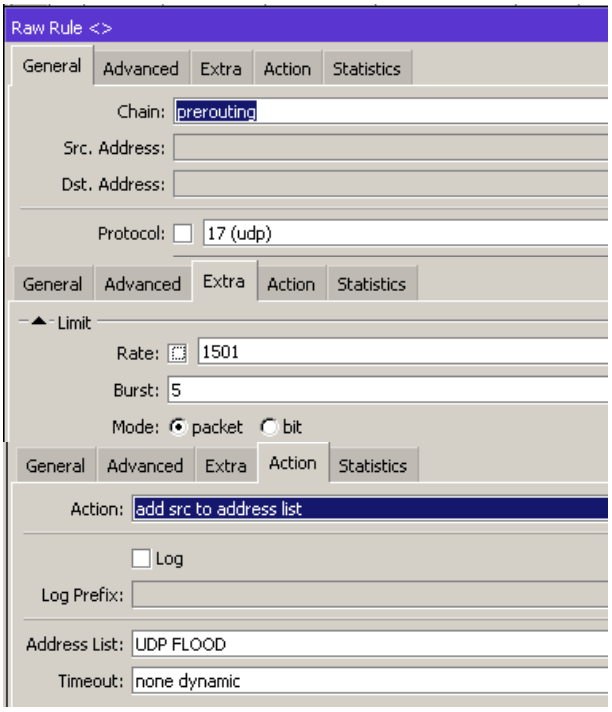
Setelah menetapkan aturan untuk menandai paket yang teridentifikasi sebagai serangan, peneliti menambahkan firewall filter rule pada chain input untuk menjatuhkan paket tersebut. Aturan ini difokuskan pada protokol UDP (protocol 17) dengan sumber alamat yang telah dimasukkan dalam address list "UDP FLOOD" dan diberikan action drop, sehingga seluruh paket pada daftar tersebut secara otomatis diblokir oleh router. Pendekatan yang sama juga diterapkan untuk serangan SYN Flood dan ICMP Flood, dengan penyesuaian pada jenis protokol yang digunakan.

b. Rule Firewall RAW



Gambar. 16 Konfigurasi Rule Accept

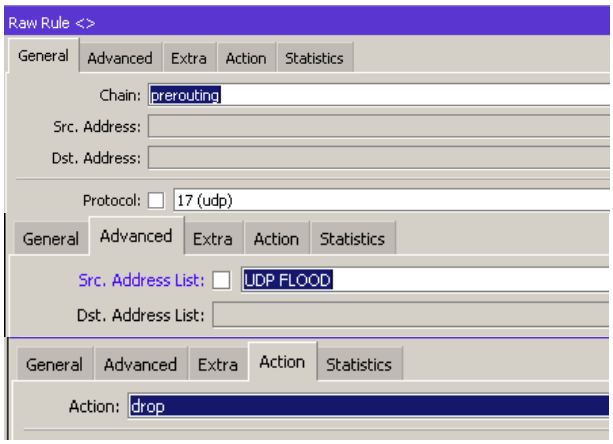
Peneliti menambahkan firewall RAW pada chain prerouting untuk memfilter paket UDP (protocol 17) sebelum diproses oleh router, dengan batas maksimum 1.500 paket per detik dan burst 5. Aturan ini dikonfigurasi dengan action accept, sehingga hanya lalu lintas dalam batas tersebut yang diteruskan ke proses routing.



Gambar. 17 Konfigurasi Address List

Setelah membuat aturan untuk mengizinkan paket diteruskan ke proses routing, peneliti menambahkan rule pada *chain prerouting* untuk mendeteksi potensi serangan UDP. Aturan ini membatasi lalu lintas hingga 1.501 paket per detik dengan *burst* 5, dan

jika melebihi batas, alamat sumber akan dimasukkan ke dalam *address list* "UDP FLOOD".

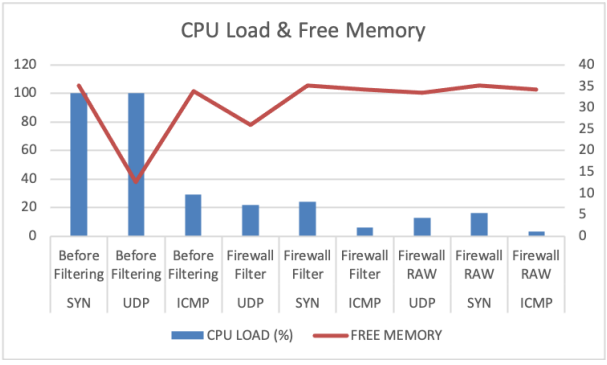


Gambar. 18 Konfigurasi Rule Drop

Setelah menetapkan aturan untuk menandai paket yang dikategorikan sebagai serangan, pada chain prerouting untuk menjatuhkan paket tersebut. Aturan ini difokuskan pada protokol UDP (protocol 17) dengan sumber alamat yang tercatat dalam address list "UDP FLOOD" dan diberikan action drop, sehingga seluruh paket pada daftar tersebut diblokir sebelum proses routing. Konfigurasi serupa juga diterapkan untuk serangan SYN Flood dan ICMP Flood, dengan penyesuaian pada jenis protokol yang digunakan.

c. Hasil Implementasi Kedua Firewall

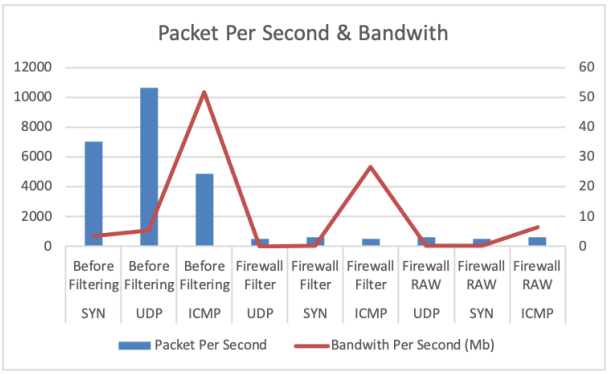
Berdasarkan hasil penelitian, diperoleh data dari implementasi packet filtering yang kemudian diuraikan untuk menjelaskan temuan pengujian keamanan jaringan serta langkah mitigasi terhadap serangan yang terjadi.



Gambar. 19 CPU Load & Free Memory

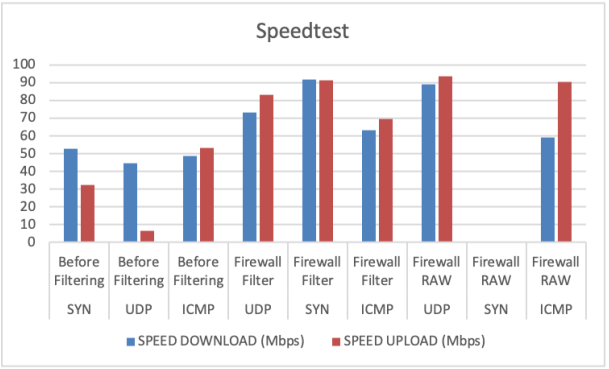
Sebelum implementasi packet filtering, simulasi serangan ICMP Flood, UDP Flood, dan SYN Flood yang diarahkan ke router menunjukkan peningkatan beban sistem. Serangan UDP Flood dan SYN Flood menyebabkan CPU load mencapai 100%, dengan penurunan memori pada UDP Flood dari 35,1 MiB menjadi 12,7 MiB. Sementara itu, serangan ICMP Flood meningkatkan CPU load hingga 29% dan menurunkan memori menjadi 33,9 MiB. Setelah penerapan firewall filter rule, beban CPU dan penggunaan memori mengalami perbaikan: CPU turun menjadi 22% pada UDP Flood, 24% pada SYN Flood, dan 6% pada ICMP Flood, dengan peningkatan kapasitas memori pada UDP dan ICMP Flood. Implementasi firewall RAW menunjukkan hasil yang lebih optimal, dengan penurunan CPU load menjadi 13% pada

UDP Flood, 16% pada SYN Flood, dan 3% pada ICMP Flood, disertai pemulihan memori hingga mendekati kondisi normal.



Gambar. 20 Packet per Second & Bandwith per Second

Sebelum implementasi packet filtering, simulasi serangan ICMP Flood, UDP Flood, dan SYN Flood pada router menunjukkan peningkatan lalu lintas signifikan. Serangan SYN Flood menghasilkan Rx Rate 7.041 p/s dengan trafik 3,6 Mbps, UDP Flood mencapai 5,4 Mbps, sedangkan ICMP Flood mencatat 4.852 p/s dengan 51,8 Mbps. Setelah penerapan firewall filter rule, terjadi penurunan lalu lintas, misalnya pada UDP Flood dari 8.696 p/s (4,4 Mbps) menjadi 536 p/s (121,8 kbps), SYN Flood dari 7.439 p/s menjadi 604 p/s (193,3 kbps), dan ICMP Flood dari 4.642 p/s (49 Mbps) menjadi 510 p/s (26 Mbps). Hasil yang lebih optimal terlihat setelah implementasi firewall RAW, di mana UDP Flood turun dari 8.539 p/s menjadi 607 p/s (137,4 kbps), SYN Flood dari 8.057 p/s menjadi 513 p/s (164,2 kbps), serta ICMP Flood dari 4.479 p/s (47,3 Mbps) menjadi 600 p/s (6,4 Mbps).



Gambar. 21 Hasil Speedtest

Sebelum penerapan packet filtering, simulasi serangan DoS menunjukkan penurunan signifikan pada hasil speedtest. Serangan SYN Flood menurunkan kecepatan menjadi 53 Mbps (unduh) dan 32,4 Mbps (unggah) dari kondisi normal 94,6/94,4 Mbps, UDP Flood menghasilkan 44,4 Mbps (unduh) dan 6,4 Mbps (unggah), sedangkan ICMP Flood tercatat 48,9 Mbps (unduh) dan 53,4 Mbps (unggah). Setelah implementasi firewall filter rule, kinerja jaringan membaik dengan hasil 73,3/83,3 Mbps (UDP Flood), 91,8/91,5 Mbps (SYN Flood), dan 63/69,5 Mbps (ICMP Flood). Penerapan firewall RAW menunjukkan peningkatan lebih lanjut, dengan kecepatan 88,9/93,7 Mbps (UDP Flood) dan 59,1/90,3 Mbps (ICMP Flood), sementara pada SYN Flood koneksi tidak dapat terbentuk.

IV. KESIMPULAN

Berdasarkan hasil penelitian dan analisis pada jaringan Dinas Komunikasi dan Informatika Kabupaten Kubu Raya dengan metode packet filtering dan penetration testing menggunakan tools Kali Linux, diperoleh beberapa temuan utama. Pertama, pengujian dilakukan secara terstruktur mulai dari identifikasi masalah, perencanaan, information gathering, vulnerability assessment, eksploitasi melalui serangan UDP Flood, SYN Flood, dan ICMP Flood, hingga tahap pelaporan. Kedua, proses information gathering menemukan port terbuka 53/tcp (DNS), 2000/tcp (bandwidth-test), dan 8291/tcp (Winbox), sementara vulnerability assessment dengan Nessus mendeteksi kerentanan tingkat rendah pada port 0 (ICMP), sedang pada port 53 (DNS), serta tinggi pada port 53 (DNS) dan 8291 (Winbox). Pada tahap eksploitasi, serangan UDP Flood berhasil mengirimkan 4.355.121 paket, SYN Flood 7.460.305 paket, dan ICMP Flood 222.125 paket berukuran 6.500 byte. Ketiga, laporan akhir melalui Dradis memuat informasi mengenai port terbuka, kerentanan, serta rekomendasi mitigasi. Keempat, hasil implementasi menunjukkan bahwa serangan DoS dapat diminimalisasi dengan packet filtering menggunakan firewall filter rule dan firewall raw. Filter rule hanya memblokir paket pada chain input tanpa memengaruhi trafik forward, sedangkan firewall raw mampu memblokir lebih awal namun berpotensi mengganggu koneksi sah jika tidak dikonfigurasi dengan tepat.

V. REFERENSI

[1] A. Saroji, T. Harmini and M. Taqiyuddin, "SEJARAH EVOLUSI GENERASI INTERNET," *Jurnal Lani:Kajian Ilmu Sejarah & Budaya*, vol. 2, no. 2, pp. 65-75, 2021.

[2] P. Rani, "Distributed Denial of Service: Serangan Siber Paling Merusak," Aplikas Servis Pesona, 9 April 2024. [Online]. Available: https://aplikas.com/blog/distributed-denial-of-service/.

[3] "ANALISIS PENGUJIAN KEAMANAN WEBSITE PENGELOLAAN INTERNET DESA KRAGAN MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 1, pp. 307-319, 2024.

[4] MikroTik, "Packet Flow in RouterOS," MikroTik, [Online]. Available: https://help.mikrotik.com/docs/spaces/ROS/pages/328227/Packet+Flow+in+RouterOS.

[5] L. F. Burhani and Priyawati Diah, "ANALISIS PENGUJIAN KEAMANAN WEBSITE PENGELOLAAN INTERNET DESA KRAGAN MENGGUNAKAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, pp. 307-319, 2024.

[6] F. P. E. Putra, "Impelementasi SistemKeamananJaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *Jurnal Sistim Informasi dan Teknologi*, p. 83, 2023.