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

SKRIPSI

Program Studi Sarjana Informatika
Jurusan Informatika

Oleh:
IRANI KAMIL
NIM D1041201026

FAKULTAS TEKNIK
UNIVERSITAS TANJUNGPURA
PONTIANAK
2025

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Irani Kamil

NIM : D1041201026

menyatakan bahwa dalam skripsi yang berjudul "Analisis Keamanan Jaringan Pada Komunikasi dan Informatika Kuburaya" tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi manapun. Sepanjang pengetahuan Saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Demikian pernyataan ini dibuat dengan sebenar-benarnya. Saya sanggup menerima konsekuensi akademis dan hukum di kemudian hari apabila pernyataan yang dibuat ini tidak benar.

Pontianak, 15 Juli 2025

Irani Kamil
NIM D1041201026

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon (0561) 740186, WA: +6282152280907
Email : ft@untan.ac.id Website : http://teknik.untan.ac.id

HALAMAN PENGESAHAN

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

Program Studi Sarjana Informatika
Jurusan Informatika

Oleh:

Irani Kamil
NIM D1041201026

Telah dipertahankan di depan Penguji Skripsi pada tanggal 15 Juli 2025
dan diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana.

Susunan Penguji Skripsi:

Ketua,

Haried Novriando, S.Kom., M.Eng.
NIP 198611132020121005

Penguji Utama,

Heri Priyanto, S.T., M.T.
NIP 197504122003121001

Sekretaris,

Ir. M. Azhar Irwansyah, ST., M.Eng.
NIP 198506062008121002

Penguji Pendamping,

Rickhy Artha Octaviyana, S.Kom., M.M., M.Kom.
NIP 199510302024061002

Pontianak, 15 Juli 2025
Dekan,

Dr.-Ing. Ir. Slamet Widodo, M.T., IPM.
NIP 196712231992031002

HALAMAN PERSEMBAHAN

Alhamdulillah dan puji syukur saya panjatkan kepada Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga saya masih diberikan kesempatan untuk menyelesaikan skripsi ini. Skripsi ini didedikasikan kepada kedua orang tua saya tercinta, Bapak Mingsilwani dan Ibu Mustiani yang selalu memberikan dukungan, motivasi dan selalu berdoa yang terbaik untuk saya sehingga saya dapat menyelesaikan skripsi ini. Terima kasih atas segala pengorbanan, kasih sayang dan cinta yang tulus. Terima kasih telah memenuhi kebutuhan dan memberikan fasilitas terbaik untuk saya hingga saat ini, sehingga saya dapat menempuh pendidikan jenjang Sarjana. Saya ucapkan terimakasih yang sebesar-besarnya juga kepada Muhammad Alfath Fadillah yang telah meminjamkan laptop untuk melancarkan penelitian saya. Kepada teman – teman seperjuangan magang saya terima kasih telah memberikan dorongan hingga saya dapat mengupgrade skill saya sampai saat ini, serta teman-teman “anak bangsa👍” yang selalu menemani sekarang dengan info perkopiannya dan teman teman informatika angkatan 2020 yang tidak bisa saya sebutkan satu persatu terima kasih telah membersamai dan menolong saya saat mengerjakan tugas perkuliahan.

KATA PENGANTAR

Puji syukur kehadirat Allah Subhanahu Wata'ala atas rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penelitian dengan judul "Evaluasi Keamanan Jaringan dengan Metode Penetration Testing pada Dinas Kominukasi dan Informatika Kabupaten Kubu Raya".

Penulis mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penelitian ini. Pihak-pihak yang telah berkontribusi dalam penelitian ini sebagai berikut. Bapak Haried Novriando, S.Kom., M.Eng. dan Bapak Ir. M. Azhar Irwansyah, ST, M.Eng selaku dosen pembimbing pertama dan dosen pembimbing kedua yang telah memberikan saran, motivasi, dan bimbingan sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Bapak Heri Priyanto, S.T., M.T. dan Bapak Rickhy Artha Octaviyana, S.Kom., M.M., M.Kom. selaku dosen penguji pertama dan dosen penguji kedua yang telah memberikan saran dan bimbingan sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Ibu Anggi Srimurdianti S., S.T., M.T. selaku Dosen Pembimbing Akademik. Bapak Ir. M. Azhar Irwansyah, ST, M.Eng. yang telah memberikan saran tempat untuk penelitian ini yaitu Dinas Komunikasi dan Informatika Kabupaten Kubu Raya. Bapak Usmantho selaku IT Support Dinas Komunikasi dan Informatika Kabupaten Kubu Raya yang bersedia membantu penulis dalam memberikan data dan informasi yang dibutuhkan pada penelitian ini. Terima kasih atas waktu dan sarannya yang sudah diberikan kepada penulis.

Penulis sudah berusaha maksimal dalam penelitian ini. Penulis sangat mengharapkan kritik dan saran dari semua pihak demi perbaikan penelitian di masa depan. Akhir kata penulis berharap agar penelitian ini dapat menambah wawasan dan memberikan pengetahuan yang bermanfaat.

Pontianak, 15 Juli 2025
Penulis,

Irani Kamil

ABSTRAK

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.

Kata kunci: keamanan jaringan, *Packet Filtering, Penetration Testing, Denial of Service,* MikroTik

ABSTRACT

Network security is a crucial aspect of addressing evolving cyber threats, including Denial of Service (DoS) attacks. This study aims to analyze network security at the Communication and Informatics Office of Kuburaya using Packet Filtering and Penetration Testing methods. These methods were implemented to detect, analyze, and prevent potential threats that could disrupt network operations. The study involves several stages, including field observation, problem identification, action planning, information gathering using tools such as Nmap and Nessus, and DoS attack simulations, including UDP Flood, SYN Flood, and ICMP Flood. Subsequently, Packet Filtering was implemented on MikroTik routers using Firewall Filter Rule and Firewall RAW to mitigate the attacks. The findings reveal that prior to implementing Packet Filtering, DoS attacks caused the router's CPU usage to spike to 100%, severely impacting system performance. After implementing Firewall Filter Rule, CPU usage significantly reduced to 22% during UDP Flood attacks and 6% during ICMP Flood attacks. With Firewall RAW, mitigation effectiveness improved further, with CPU usage dropping to 13% for UDP Flood attacks and 3% for ICMP Flood attacks. In conclusion, the Packet Filtering method is proven effective in preventing DoS attacks. Firewall RAW demonstrated greater efficiency compared to Firewall Filter Rule, particularly in minimizing router resource usage.

Keywords: network security, Packet Filtering, Penetration Testing, Denial of Service, MikroTik

DAFTAR ISI

Halaman Pernyataan ..... **i**
Halaman Pengesahan ..... **ii**
Halaman Persembahan ..... **iii**
Kata Pengantar ..... **iv**
Abstrak ..... **v**
ABSTRACT ..... ***vi***
Daftar Tabel ..... **ix**
Daftar Gambar ..... **x**
Daftar Lampiran ..... **xv**
Bab I Pendahuluan **1**
1.1 Latar Belakang **1**
1.2 Perumusan Masalah **3**
1.3 Tujuan Penelitian **3**
1.4 Pembatasan Masalah **3**
1.5 Sistematika Penulisan **4**
Bab II Tinjauan Pustaka **5**
2.1 Penelitian Terkait **5**
2.2 Landasan Teori **6**
2.2.1 Analisis 6
2.2.2 Metode 7
2.2.3 Flowchart 8
2.2.4 Keamanan Jaringan 9
2.2.5 *Denial of Service* 10
2.2.6 TCP/IP 10
2.2.7 UDP 12
2.2.8 ICMP 13
2.2.9 *Router* 13
2.2.10 Mikrotik 14
2.2.11 Winbox 15
2.2.12 *Firewall* 16
2.2.13 *Packet Filtering* 16
2.2.14 *Firewall Filter Rule* 17
2.2.15 *Firewall RAW* 17
2.2.16 Kali Linux 18
2.2.17 Topologi Jaringan 21
Bab III Metodologi Penelitian **23**

3.1 Alat Penelitian 23
3.1.1 Perangkat Keras 23
3.1.2 Perangkat Lunak 24
3.1.3 Langkah Penelitian 24
3.2 Metode Analisis 28
3.2.1 Perencanaan dan Penentuan Titik Pengujian Penelitian 28
3.2.2 Implementasi Packet Filtering 29
3.2.3 Implementasi Penetration Testing 31
Bab IV Hasil dan Analisis 37
4.1 Hasil Penelitian 37
4.1.1 Penentuan Titik Pengujian Penelitian 37
4.1.2 Hasil Implementasi Penetration Testing 39
4.1.3 Sebelum Terjadi Serangan 63
4.1.4 Hasil Serangan Sebelum Implementasi *Packet Filtering* 66
4.1.5 Hasil Implementasi Packet Filtering dengan Firewall Filter Rule 72
4.1.6 Hasil Implementasi Packet Filtering dengan Firewall RAW 97
4.2 Analisis Hasil 117
4.2.1 Data Penetration Testing 117
4.2.2 Data Packet Filtering 119
Bab V Kesimpulan dan Saran 125
5.1 Kesimpulan 125
5.2 Saran 126
5.3 Rekomendasi 127
Daftar Pustaka 129

DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Terkait 5
Tabel 2. 2 Tabel List Flowchart 8
Tabel 2. 3 Perbandingan Spesifikasi *Router* Mikrotik RB 941-2nD dengan Dinara V3 ros *level* 6 15
Tabel 3. 1 Daftar Hardware 23
Tabel 3. 2 Daftar Software 24
Tabel 4. 1 Fungsi Perintah Nmap 43

DAFTAR GAMBAR

Gambar 2. 1 Routerboard Mikrotik RB941-2nD 14
Gambar 2. 2 Topologi Star 22
Gambar 3. 1 Langkah Penelitian 25
Gambar 3. 2 Topologi Physical Jaringan Organisasi Perangkat Daerah Kuburaya 29
Gambar 3. 3 Alur Packet Filtering 30
Gambar 3. 4 Alur Penetration Testing 31
Gambar 3. 5 Flowchart serangan UDP Flood 33
Gambar 3. 6 Flowchart serangan SYN Flood 34
Gambar 3. 7 Flowchart serangan ICMP Flood 35
Gambar 4. 1 Settingan IP Pada Router Mikrotik 37
Gambar 4. 2 Bandwith Kafe Pekarangan 38
Gambar 4. 3 Arsitektur Secara Umum Router Penelitian dan Penetration Testing 39
Gambar 4. 4 IP Address Penyerang 40
Gambar 4. 5 Ping Perangkat Router Target 40
Gambar 4. 6 Perintah Nmap 41
Gambar 4. 7 Hasil Nmap File XML 41
Gambar 4. 8 Halaman Download Nessus 44
Gambar 4. 9 Instalasi Nessus 44
Gambar 4. 10 Perintah Memulai Nessus 45
Gambar 4. 11 Halaman Register Nessus 46
Gambar 4. 12 Halaman Login Nessus 46
Gambar 4. 13 Halaman Dashboard Nessus 47
Gambar 4. 14 Halaman Scan Templates Nessus 47
Gambar 4. 15 Konfigurasi Target 48
Gambar 4. 16 Running Scan Nessus 48
Gambar 4. 17 Hasil Scanning Nessus 49
Gambar 4. 18 Informasi Hasil Scanning Nessus 49
Gambar 4. 19 Informasi Kerentanan Level High 1 50
Gambar 4. 20 Informasi Kerentanan Level High 2 50
Gambar 4. 21 Informasi Kerentanan Level Medium 50
Gambar 4. 22 Informasi Kerentanan Level Low 51
Gambar 4. 23 Konfigurasi Target sesi 2 52
Gambar 4. 24 Hasil Running Scan Nessus sesi 2 53
Gambar 4. 25 Informasi Kerentanan Level High sesi 2 53
Gambar 4. 26 Informasi Kerentanan Level Medium sesi 2 53
Gambar 4. 27 Menjalankan Tools UDP Flood Pada Hping3 54
Gambar 4. 28 Menjalankan Tools SYN Flood Pada Hping3 55
Gambar 4. 29 Menjalankan Tools ICMP Flood Pada Hping3 56
Gambar 4. 30 Perintah Meng-install Dradis 57
Gambar 4. 31 Perintah Menjalankan Dradis 57
Gambar 4. 32 Halaman Login Dradis 58
Gambar 4. 33 Halaman Dashboard Dradis 58
Gambar 4. 34 Create Nodes 59
Gambar 4. 35 Create Sub-Nodes Nmap 59
Gambar 4. 36 Upload Hasil Scanning nmap.xml 60

Gambar 4. 37 Create Sub-Nodes Nessus 60
Gambar 4. 38 Upload Hasil Scanning Nessus 61
Gambar 4. 39 Laporan Hasil Dradis 1 61
Gambar 4. 40 Hasil Laporan Dradis 2 62
Gambar 4. 41 Trafic sebelum terjadi serangan 64
Gambar 4. 42 Resource sebelum terjadi serangan 65
Gambar 4. 43 Task Manager pada PC Testing 65
Gambar 4. 44 Bandwith sebelum terjadi serangan 66
Gambar 4. 45 Traffic saat terjadi serangan SYN Flood 67
Gambar 4. 46 Resource saat terjadi serangan SYN Flood 67
Gambar 4. 47 Bandwith saat terjadi serangan SYN Flood 68
Gambar 4. 48 Traffic saat terjadi serangan UDP Flood 69
Gambar 4. 49 Resource saat terjadi serangan UDP Flood 69
Gambar 4. 50 Bandwith saat terjadi serangan UDP Flood 70
Gambar 4. 51 Traffic saat terjadi serangan ICMP Flood 71
Gambar 4. 52 Resource saat terjadi serangan ICMP Flood 71
Gambar 4. 53 Bandwith saat terjadi serangan ICMP Flood 72
Gambar 4. 54 Konfigurasi Chain dan Protocol pada Firewall Filter untuk Rule Accept Serangan UDP Flood 73
Gambar 4. 55 Konfigurasi Limit pada Firewall Filter untuk Rule Accept Serangan UDP Flood 73
Gambar 4. 56 Konfigurasi Action pada Firewall Filter untuk Rule Accept Serangan UDP Flood 74
Gambar 4. 57 Konfigurasi Chain dan Protocol pada Mangle untuk serangan UDP Flood 75
Gambar 4. 58 Konfigurasi Limit pada Mangle untuk serangan UDP Flood 75
Gambar 4. 59 Konfigurasi Action pada Mangle untuk serangan UDP Flood 76
Gambar 4. 60 Konfigurasi Chain dan Protocol pada Firewall Filter untuk Rule Drop Serangan UDP Flood 77
Gambar 4. 61 Konfigurasi Src. Addressl List pada Firewall Filter untuk Rule Drop serangan UDP Flood 77
Gambar 4. 62 Konfigurasi Action pada Firewall Filter untuk Rule Drop serangan UDP Flood 78
Gambar 4. 63 Connection Tracking dan Torch pada saat terjadi serangan UDP Flood sesi 1 79
Gambar 4. 64 Traffic setelah terkena serangan UDP Flood sesi 1 79
Gambar 4. 65 Resource router pada saat terjadi serangan UDP Flood sesi 1 80
Gambar 4. 66 Bandwith setelah implementasi Firewall Filter Rule untuk UDP Flood 81
Gambar 4. 67 Konfigurasi Chain dan Protocol pada Firewall Filter untuk Rule Accept serangan SYN Flood 82
Gambar 4. 68 Konfigurasi TCP Flags pada Firewall Filter untuk Rule Accept serangan SYN Flood 82
Gambar 4. 69 Konfigurasi Limit pada Firewall Filter untuk Rule Accept serangan SYN Flood 83
Gambar 4. 70 Konfigurasi Action pada Firewall Filter untuk Rule Accept serangan SYN Flood 83
Gambar 4. 71 Konfigurasi Chain dan Protocol pada Mangle untuk serangan SYN

Flood 84
Gambar 4. 72 Konfigurasi TCP Flags pada Mangle untuk serangan SYN Flood84
Gambar 4. 73 Konfigurasi Limit pada Mangle untuk serangan SYN Flood 85
Gambar 4. 74 Konfigurasi Action pada Mangle untuk serangan SYN Flood 85
Gambar 4. 75 Konfigurasi Chain dan Protocol pada Firewall Filter untuk Rule Drop serangan SYN Flood 86
Gambar 4. 76 Konfigurasi Src. Address List pada Firewall Filter untuk Rule Drop serangan SYN Flood 86
Gambar 4. 77 Konfigurasi Action pada Firewall Filter untuk Rule Drop serangan SYN Flood 87
Gambar 4. 78 Connection Tracking dan Torch pada saat terjadi serangan SYN Flood sesi 1 87
Gambar 4. 79 traffic pada saat terjadi serangan SYN Flood sesi 1 88
Gambar 4. 80 Resource router pada saat terjadi serangan SYN Flood sesi 1 88
Gambar 4. 81 Bandwith setelah implementasi Firewall Filter Rule untuk SYN Flood 89
Gambar 4. 82 Chain dan Protocol pada Firewall Filter untuk Rule Accept serangan ICMP Flood 90
Gambar 4. 83 Limit pada Firewall Filter untuk Rule Accept serangan ICMP Flood 90
Gambar 4. 84 Action pada Firewall Filter untuk Rule Accept serangan ICMP Flood 91
Gambar 4. 85 Chain dan Protocol pada Mangle untuk serangan ICMP Flood ... 92
Gambar 4. 86 Limit pada Mangle untuk serangan ICMP Flood 92
Gambar 4. 87 Action pada Mangle untuk serangan ICMP Flood 93
Gambar 4. 88 Chain dan Protocol pada Firewall Filter untuk Rule Drop serangan ICMP Flood 93
Gambar 4. 89 Scr. Address List pada Firewall Filter untuk Rule Drop serangan ICMP Flood 94
Gambar 4. 90 Action pada Firewall Filter untuk Rule Drop serangan ICMP Flood 94
Gambar 4. 91 Connection Tracking dan Torch saat terjadi serangan ICMP Flood sesi 1 95
Gambar 4. 92 Traffic saat terjadi serangan ICMP Flood sesi 1 95
Gambar 4. 93 Resource Router saat terjadi serangan ICMP Flood sesi 1 96
Gambar 4. 94 Bandwith setelah implementasi Firewall Filter Rule untuk ICMP Flood 96
Gambar 4. 95 Konfigurasi Chain dan Protocol pada Firewall RAW untuk Rule No Track 97
Gambar 4. 96 Konfigurasi Action pada Firewall RAW untuk Rule No Track ... 98
Gambar 4. 97 Konfigurasi Chain dan Protocol pada Firewall RAW untuk Rule Accept serangan UDP Flood 98
Gambar 4. 98 Konfigurasi Limit pada Firewall RAW 99
Gambar 4. 99 Action Pada Firewall RAW untuk Rule Accept serangan UDP Flood 99
Gambar 4. 100 Konfigurasi Chain dan Protocol pada Firewall RAW untuk Address List serangan UDP Flood 100
Gambar 4. 101 Konfigurasi Limit pada Firewall RAW untuk Address List

serangan UDP Flood 100
Gambar 4. 102 Konfigurasi Action Pada Firewall RAW untuk Address List serangan UDP Flood 100
Gambar 4. 103 Chain dan Protocol pada Firewall RAW untuk Rule Drop serangan UDP Flood 101
Gambar 4. 104 Src. Address List pada Firewall RAW untuk Rule Drop serangan UDP Flood 101
Gambar 4. 105 Action Pada Firewall RAW untuk Rule Drop serangan UDP Flood 102
Gambar 4. 106 Connection dan Torch saat terjadi serangan UDP Flood sesi 2 102
Gambar 4. 107 Traffic saat terjadi serangan UDP Flood sesi 2 103
Gambar 4. 108 Resource router saat terjadi serangan UDP Flood sesi 2 104
Gambar 4. 109 Bandwith setelah implementasi Firewall RAW untuk UDP Flood 104
Gambar 4. 110 Chain dan Protocol pada Firewall RAW untuk Rule Accept serangan SYN Flood 105
Gambar 4. 111 TCP Flags pada Firewall RAW untuk Rule Accept serangan SYN Flood 105
Gambar 4. 112 Limit pada Firewall RAW untuk Rule Accept serangan SYN Flood 106
Gambar 4. 113 Action pada Firewall RAW untuk Rule Accept serangan SYN Flood 106
Gambar 4. 114 Chain dan Protocol pada Firewall RAW untuk Address List serangan SYN Flood 106
Gambar 4. 115 TCP Flags pada Firewall RAW untuk Address List serangan SYN Flood 107
Gambar 4. 116 Limit pada Firewall RAW untuk Address List serangan SYN Flood 107
Gambar 4. 117 Action Pada Firewall RAW untuk Address List serangan SYN Flood 107
Gambar 4. 118 Chain dan Protocol pada Firewall RAW untuk Rule Drop serangan SYN Flood 108
Gambar 4. 119 Src. Address List pada Firewall RAW untuk Rule Drop serangan SYN Flood 108
Gambar 4. 120 Action pada Firewall RAW untuk Rule Drop serangan SYN Flood 108
Gambar 4. 121 Torch dan Connection Tracking saat terjadi serangan SYN Flood sesi 2 109
Gambar 4. 122 Traffic saat terjadi serangan SYN Flood sesi 2 110
Gambar 4. 123 Resource router saat terjadi serangan SYN Flood sesi 2 110
Gambar 4. 124 Bandwith setelah implementasi Firewall RAW untuk SYN Flood 111
Gambar 4. 125 Chain dan Protocol pada Firewall RAW untuk Rule Accept serangan ICMP Flood 112
Gambar 4. 126 Limit pada Firewall RAW untuk Rule Accept serangan ICMP Flood 112
Gambar 4. 127 Action pada Firewall RAW untuk Rule Drop serangan ICMP Flood 112

Gambar 4. 128 Chain dan Protocol pada Firewall RAW untuk Address List serangan ICMP Flood 113
Gambar 4. 129 Limit pada Firewall RAW untuk Address List serangan ICMP Flood 113
Gambar 4. 130 Action pada Firewall RAW untuk Address List serangan ICMP Flood 113
Gambar 4. 131 Chain dan Protocol pada Firewall RAW untuk Rule Drop serangan ICMP Flood..... 114
Gambar 4. 132 Src. Address List pada Firewall RAW untuk Rule Drop serangan ICMP Flood..... 114
Gambar 4. 133 Action pada Firewall RAW untuk Rule Drop serangan ICMP Flood 114
Gambar 4. 134 Connection Tracking dan Torch saat terjadi serangan ICMP Flood sesi 2..... 115
Gambar 4. 135 Traffic saat terjadi serangan ICMP Flood sesi 2 115
Gambar 4. 136 Resource router saat terjadi serangan ICMP Flood sesi 2 116
Gambar 4. 137 Bandwith setelah implementasi Firewall RAW untuk UDP Flood 116

DAFTAR LAMPIRAN

LAMPIRAN A SURAT PERIJINAN PENGAMBILAN DATA A-1

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet telah membawa dampak besar dalam berbagai aspek kehidupan, mulai dari komunikasi, pendidikan, hingga dunia bisnis. Internet mempermudah akses terhadap informasi, mempercepat proses kerja, serta mendorong inovasi di berbagai sektor. Namun, di balik berbagai manfaat tersebut, terdapat risiko yang tidak bisa diabaikan, yaitu meningkatnya serangan siber (cyberattack) yang mengancam keamanan data dan kelangsungan operasional sistem jaringan. Lani Sidharta dalam (Saroji, 2021) menjelaskan, internet adalah suatu interkoneksi sebuah jaringan komputer yang dapat memberikan layanan informasi secara lengkap. *Internet* tidak hanya mempermudah akses informasi, tetapi juga mendorong inovasi di berbagai sektor, seperti pendidikan, bisnis, kesehatan, dan hiburan. Pembelajaran daring, perdagangan elektronik, dan layanan streaming hanyalah beberapa contoh bagaimana internet telah merubah kehidupan manusia.

Namun, di balik kemudahan dan manfaat yang ditawarkan oleh jaringan komputer, terdapat ancaman serius yang tidak bisa diabaikan, yaitu *cyberattack*. *Cyberattack* telah menjadi ancaman yang signifikan bagi banyak organisasi, dengan kerentanan yang dapat dieksploitasi oleh para penyerang untuk mencuri data sensitif, merusak sistem, atau bahkan mengganggu operasional keseluruhan. Salah satu jenis serangan siber yang paling merusak adalah serangan *Denial of Service (DoS)*. Serangan ini bertujuan untuk membuat layanan jaringan menjadi tidak tersedia bagi pengguna yang sah dengan cara menghabiskan sumber daya jaringan, seperti *bandwidth* atau kapasitas *CPU*, sehingga menyebabkan hambatan atau bahkan kegagalan dalam akses data dan komunikasi (Pilo, 2024).

Dalam ruang lingkup Dinas Komunikasi dan Informatika Kabupaten Kubu Raya menggunakan MikroTik Dinara v3 (RoS Level 6) sebagai *backbone* untuk memanajemen sistem jaringan mereka. Jaringan tersebut di distribusikan ke OPD (Organisasi Perangkat Daerah) Kuburaya. Menurut sumber dari pihak Dinas Komunikasi dan Informatika Kabupaten Kubu Raya (Pak Romi) mengatakan

bahwa masalah yang sering terjadi adalah adanya gangguan dari pihak luar. Gangguan tersebut melibatkan berbagai macam serangan siber seperti Brute Force Login dan Boom Trafic. Boom traffic merupakan kondisi ketika terjadi lonjakan lalu lintas jaringan secara tiba-tiba dan tidak normal. Lonjakan ini dapat berasal dari berbagai sumber, seperti perangkat terinfeksi, botnet, atau skrip otomatis yang mengirimkan permintaan dalam jumlah besar ke server atau perangkat jaringan tertentu. Boom traffic memiliki keterkaitan dengan serangan Denial of Service (DoS), yaitu serangan yang dirancang untuk membuat suatu layanan atau sistem tidak tersedia bagi pengguna. Dalam konteks tersebut, boom traffic dapat berfungsi sebagai indikator awal atau bagian dari mekanisme serangan DoS, di mana volume lalu lintas yang tinggi membebani sumber daya sistem seperti bandwidth, CPU, atau memori, sehingga menyebabkan gangguan atau penghentian layanan. Untuk mengatasi ancaman ini, penggunaan perangkat jaringan yang handal dan memiliki fitur keamanan yang mumpuni sangat diperlukan. MikroTik, sebagai salah satu penyedia solusi jaringan terkemuka, menawarkan beragam fitur yang dapat digunakan untuk melindungi jaringan dari serangan *Denial of Service* (DoS). *Router* MikroTik dilengkapi dengan kemampuan manajemen trafik, *firewall*, dan fitur keamanan lainnya yang dapat dioptimalkan untuk mencegah dan menangani serangan *DoS* (Lintasarta Cloudeka, 2023), misalnya, tidak hanya bertindak sebagai penghubung jaringan tetapi juga dilengkapi dengan fitur-fitur keamanan yang dapat diimplementasikan untuk mencegah *cyberattack*, termasuk serangan *DoS*.

Oleh sebab itu, untuk menguji sistem keamanan suatu jaringan agar dapat direalisasikan maka pengujian menggunakan metode *Penetration Testing* sebagai kegiatan dalam evaluasi keamanan jaringan komputer suatu sistem dengan tujuan meminimalkan kemungkinan yang akan terjadi seperti serangan DoS dari pihak luar dengan maksud merusak, mencuri, dan sebagainya. Dalam konteks ini, penelitian yang fokus pada pengamanan jaringan Dinas Komunikasi dan Informatika Kabupaten Kubu Raya dari serangan *DoS* melalui implementasi *router* Mikrotik menjadi sangat relevan dan krusial. Hasil dari penelitian dapat memberikan panduan praktis dan solusi yang sesuai bagi Dinas Komunikasi dan Informatika dalam menghadapi tantangan keamanan siber yang terus berkembang.

1.2 Perumusan Masalah

Berdasarkan latar belakang tersebut dapat dirumuskan suatu masalah seperti berikut:

a) Bagaimana cara menguji keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kubu Raya?
b) Apa saja metode yang digunakan dalam pengujian keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kubu Raya?
c) Metode apa yang digunakan dalam mengatasi serangan *DoS* yang mungkin terjadi?

1.3 Tujuan Penelitian

Berdasarkan perumusan masalah diatas didapatkan tujuan dari penelitian sebagai berikut:

a) Menguji celah keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kuburaya.
b) Mengetahui cara mengimplementasikan metode atau langkah-langkah yang digunakan dalam pengujian kerentanan celah keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kubu Raya.
c) Mengetahui cara mengimplementasikan metode atau langkah-langkah yang dapat digunakan untuk mengatasi kerentanan keamanan jaringan pada Dinas Komunikasi dan Informatika Kabupaten Kubu Raya.

1.4 Pembatasan Masalah

Dalam penelitian ini memiliki beberapa batasan masalah yang bertujuan agar penelitian lebih terarah dan tidak keluar dari fokus utama penelitian. Adapun Batasan masalah dalam penelitian ini adalah sebagai berikut:

a) Objek pada penelitian ini adalah *Router* MikroTik RB941-2nD.
b) Metode penyerangan menggunakan *Denial of Service (DoS)*.
c) Jenis serangan *Denial of Service (DoS)* yang diujikan menggunakan UDP Flood, Syn Flood, dan ICMP Flood.
d) Pada penelitian ini tidak dilakukan serangan *Distibuted Denial of Service (DDoS)*

1.5 Sistematika Penulisan

Dalam laporan tugas akhir ini, pembahasan disajikan dalam lima bab dengan sistematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan mengenai latar belakang masalah, perumusan masalah, tujuan penelitian, pembatasan masalah, metodologi penelitian, dan sistematika penulisan penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini berisi landasan teori yang digunakan sebagai dasar dalam penelitian yang dilakukan, dan juga uraian tentang kajian terkait.

BAB III METODOLOGI PENELITIAN

Pada bab ini berisikan pembahasan mengenai alat yang digunakan dalam penelitian dan metode yang digunakan dalam kegiatan analisa.

BAB IV HASIL DAN ANALISIS

Pada bab ini berisikan hasil dari Penetration Testing dan implementasi *Packet Filtering* oleh *Firewall RAW* dan *Firewall Filter Rule*, serta analisis hasil dari penelitian yang sebelumnya telah diuji.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan tentang kesimpulan yang diperoleh dari penelitian ini dan saran untuk pengembangan sistem ini.