

**Analisis Tingkat Efektifitas Mitigasi Serangan DDoS Menggunakan
Firewall Mikrotik pada Jaringan LAN**

Laporan Tugas akhir

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang



Niti Anung

201910370311353

Bidang Minat:

Sistem Keamanan Jaringan

**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK**

UNIVERSITAS MUHAMMADIYAH MALANG

2024

LEMBAR PERSETUJUAN

Analisis Tingkat Efektifitas Mitigasi Serangan DDoS Menggunakan Firewall Mikrotik pada Jaringan LAN

TUGAS AKHIR

**Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang**

Menyetujui,

Malang, 29 Oktober 2024

Dosen Pembimbing 1



Ir Denar Regata Akbi S.Kom., M.Kom.

NIP. 10816120591PNS.

Dosen Pembimbing 2

=

NIP.

LEMBAR PENGESAHAN

Analisis Tingkat Efektifitas Mitigasi Serangan DDoS Menggunakan Firewall Mikrotik pada Jaringan LAN

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Disusun Oleh :

Niti Anung

201910370311353

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis pengujian
pada tanggal 29 Oktober 2024

Menyetujui,

Dosen Penguji 1



Luqman Hakim S.Kom., M.Kom.

NIP. 10819030658PNS.

Dosen Penguji 2



Bashor Fauzan Muthohirin S.Kom.,

M.Kom

NIP. 20230126071994PNS.

Mengetahui,
Ketua Jurusan Informatika



I. Galih Wasis Wicaksono S.kom. M.Cs.

NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : Niti Anung

NIM : 201910370311353

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul “**Analisis Tingkat Efektifitas Mitigasi Serangan DDoS Menggunakan Firewall Mikrotik pada Jaringan LAN**” beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing



Malang, 29 Oktober 2024
Yang Membuat Pernyataan

Niti Anung

Ir Denar Regata Akbi S.Kom., M.Kom.

Abstrak

Serangan DDoS adalah salah satu ancaman di era digital dikarenakan mengganggu ketersediaan layanan pada sistem dan infrastruktur dalam kehidupan sehari-hari. Teknik mitigasi serangan DDoS yang efektif sangat diperlukan dikarenakan beberapa teknik mitigasi tidak bekerja dengan baik dan bahkan tidak berfungsi sama sekali. Pada penelitian lanjutan ini, penulis melakukan pengujian *firewall* mikrotik sebagai mitigasi serangan DDoS karena mikrotik memiliki harga yang terjangkau dengan fitur yang sangat banyak sehingga sangat cocok digunakan pada jaringan LAN. Serangan yang digunakan dalam penelitian ini adalah *SYN flood*, *UDP flood*, *HTTP flood*, *DNS flood*, dan *smurf attack*. Pengukuran tingkat efektifitas diambil dari tingkat serangan DDoS serta penggunaan *resource* CPU dan RAM pada *server* dan *router* selama 60 detik pada saat sebelum dan sesudah dilakukan mitigasi. Teknik mitigasi menggunakan *firewall* mikrotik terbukti dapat menurunkan tingkat serangan dan penggunaan *resource* namun memiliki batasan pada *hardware* dalam mitigasi serangan.



Kata Pengantar

Dengan memanjatkan puji syukur kehadiran Allah SWT. Atas limpahan rahmat dan hidayah-NYA sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul:

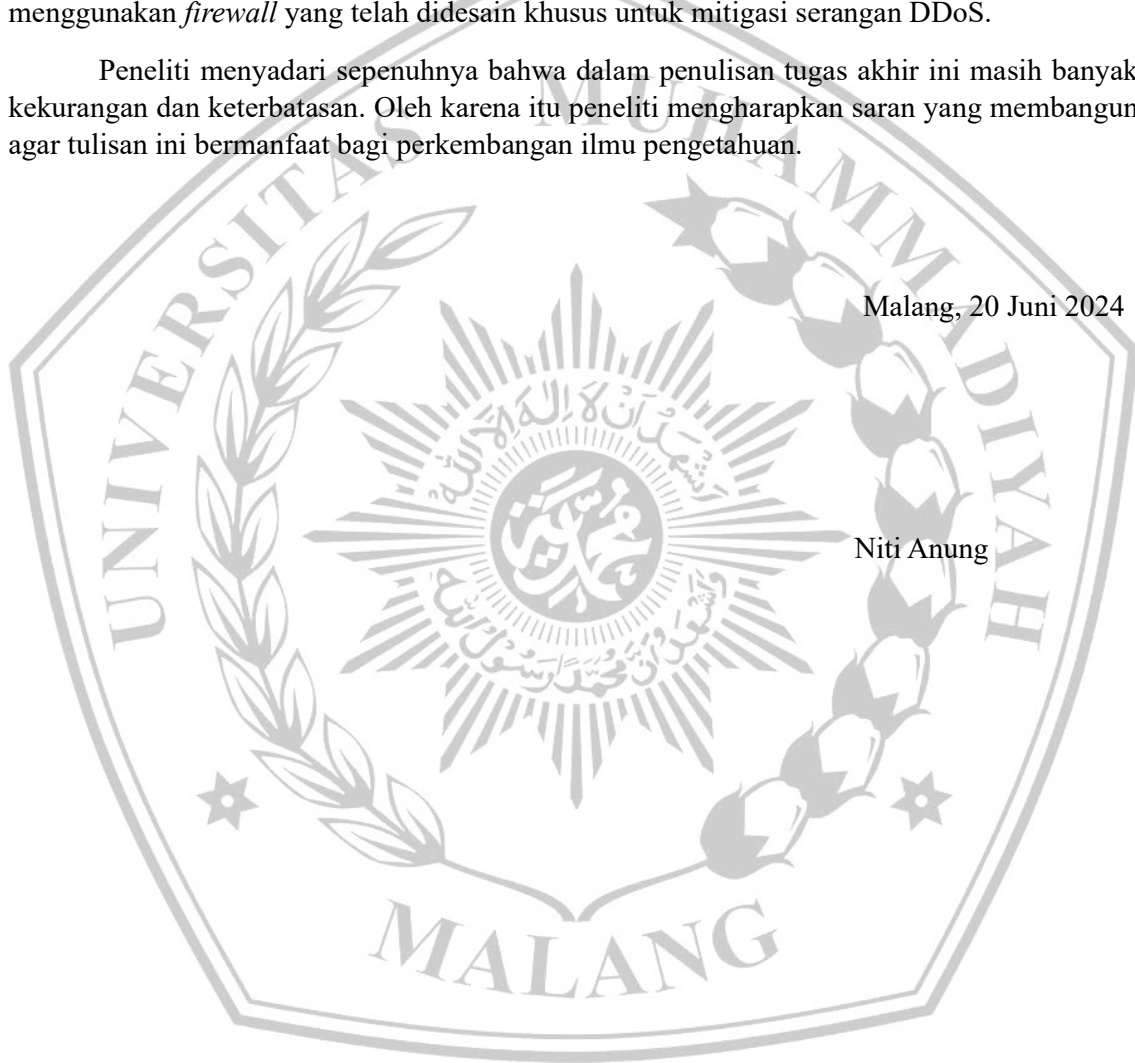
“Analisis Tingkat Efektifitas Mitigasi Serangan DDoS Menggunakan Firewall Mikrotik pada Jaringan LAN”

Di dalam tulisan ini disajikan pokok-pokok bahasan yang meliputi analisis tentang tingkat efektifitas *custom firewall* mikrotik dalam mitigasi serangan DDoS dan juga pentingnya menggunakan *firewall* yang telah didesain khusus untuk mitigasi serangan DDoS.

Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu peneliti mengharapkan saran yang membangun agar tulisan ini bermanfaat bagi perkembangan ilmu pengetahuan.

Malang, 20 Juni 2024

Niti Anung



Daftar Isi

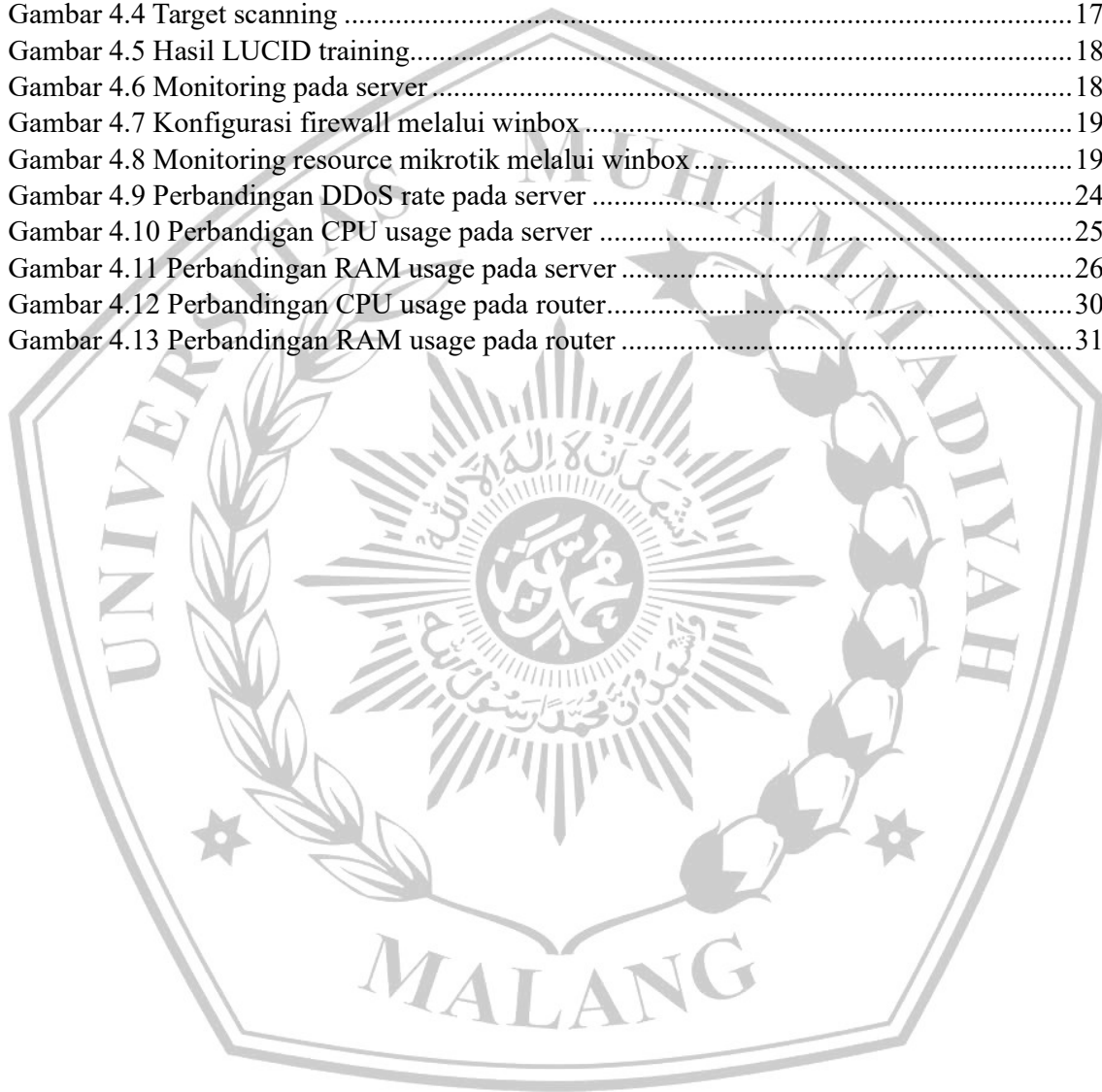
Lembar Persetujuan	ii
Lembar Pengesahan	iii
Lembar Pernyataan	iv
Abstrak.....	v
Kata Pengantar	vi
Daftar Isi	vii
Daftar Gambar	ix
Daftar Tabel	x
BAB I.....	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian.....	3
1.4. Batasan Masalah.....	3
BAB II.....	4
2.1. Landasan teori	4
2.1.1. Serangan DDoS.....	4
2.1.2. SYN flood.....	4
2.1.3. UDP flood.....	4
2.1.4. HTTP flood.....	4
2.1.5. DNS flood.....	4
2.1.6. Smurf attack.....	5
2.1.7. Firewall	5
2.1.8. Mikrotik	5
2.1.9. LUCID	5
2.1.10. Mausezahn	5
2.1.11. Hping3	6
2.1.12. Slowloris	6
2.2. Kajian Pustaka	6
BAB III.....	9
3.1. Mitigasi Serangan.....	9
3.2. Alur Penelitian.....	11
3.3. Topologi	13

3.4.	Skenario Pengujian.....	14
BAB IV.....		15
4.1.	Persiapan penyerangan.....	15
4.2.	Konfigurasi LUCID dan monitoring <i>software</i> pada <i>server</i>	18
4.3.	Konfigurasi <i>router</i>	19
4.4.	Skenario sebelum mitigasi pada sisi <i>server</i>	20
4.5.	Skenario setelah mitigasi pada sisi <i>server</i>	21
4.6.	Perbandingan dan Kesimpulan pada sisi <i>server</i>	24
4.7.	Skenario sebelum mitigasi pada sisi <i>router</i>	26
4.8.	Skenario setelah mitigasi pada sisi <i>router</i>	28
4.9.	Perbandingan dan Kesimpulan pada sisi <i>router</i>	30
BAB V.....		33
5.2.	Kesimpulan.....	33
5.3.	Saran.....	33
Daftar Pustaka.....		34
Lampiran.....		36



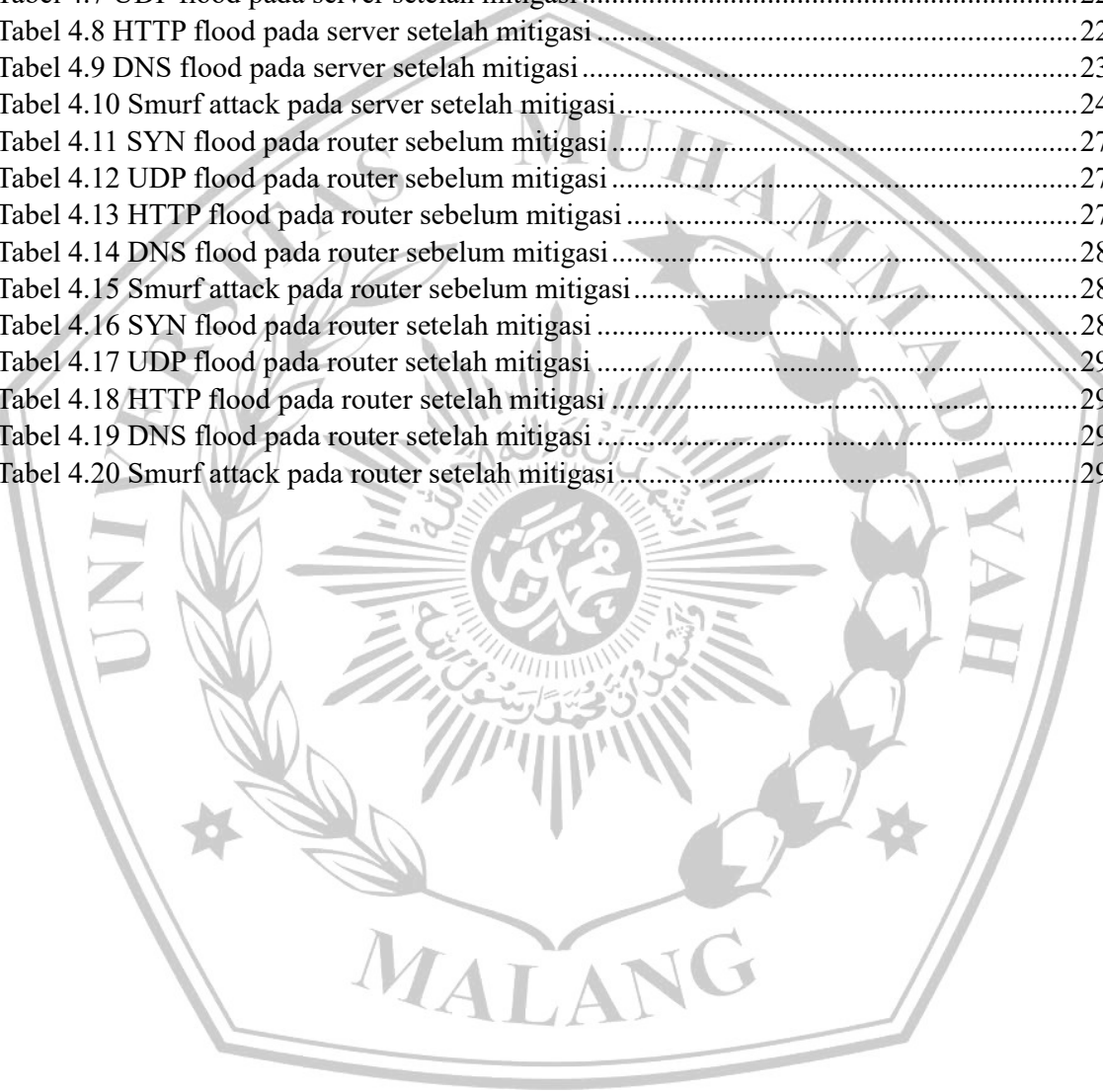
Daftar Gambar

Gambar 3.1 Konfigurasi firewall	9
Gambar 3.2 Konfigurasi custom firewall.....	9
Gambar 3.3 Alur penelitian.....	11
Gambar 3.4 Topologi penelitian.....	13
Gambar 4.1 Scanning jaringan LAN	15
Gambar 4.2 Scanning port komputer zombie	16
Gambar 4.3 Mendapatkan akses komputer zombie	16
Gambar 4.4 Target scanning	17
Gambar 4.5 Hasil LUCID training.....	18
Gambar 4.6 Monitoring pada server	18
Gambar 4.7 Konfigurasi firewall melalui winbox.....	19
Gambar 4.8 Monitoring resource mikrotik melalui winbox.....	19
Gambar 4.9 Perbandingan DDoS rate pada server	24
Gambar 4.10 Perbandigan CPU usage pada server	25
Gambar 4.11 Perbandingan RAM usage pada server	26
Gambar 4.12 Perbandingan CPU usage pada router.....	30
Gambar 4.13 Perbandingan RAM usage pada router	31



Daftar Tabel

Tabel 2.1 Penelitian terdahulu.....	6
Tabel 4.1 SYN flood pada server sebelum mitigasi.....	20
Tabel 4.2 UDP flood pada server sebelum mitigasi.....	20
Tabel 4.3 HTTP flood pada server sebelum mitigasi.....	20
Tabel 4.4 DNS flood pada server sebelum mitigasi.....	21
Tabel 4.5 Smurf attack pada server sebelum mitigasi.....	21
Tabel 4.6 SYN flood pada server setelah mitigasi.....	22
Tabel 4.7 UDP flood pada server setelah mitigasi.....	22
Tabel 4.8 HTTP flood pada server setelah mitigasi.....	22
Tabel 4.9 DNS flood pada server setelah mitigasi.....	23
Tabel 4.10 Smurf attack pada server setelah mitigasi.....	24
Tabel 4.11 SYN flood pada router sebelum mitigasi.....	27
Tabel 4.12 UDP flood pada router sebelum mitigasi.....	27
Tabel 4.13 HTTP flood pada router sebelum mitigasi.....	27
Tabel 4.14 DNS flood pada router sebelum mitigasi.....	28
Tabel 4.15 Smurf attack pada router sebelum mitigasi.....	28
Tabel 4.16 SYN flood pada router setelah mitigasi.....	28
Tabel 4.17 UDP flood pada router setelah mitigasi.....	29
Tabel 4.18 HTTP flood pada router setelah mitigasi.....	29
Tabel 4.19 DNS flood pada router setelah mitigasi.....	29
Tabel 4.20 Smurf attack pada router setelah mitigasi.....	29



Sertifikat Plagiasi



UNIVERSITAS
MUHAMMADIYAH
MALANG



FAKULTAS TEKNIK

INFORMATIKA

informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Niti Anung
NIM : 201910370311353
Judul TA : Analisis Tingkat Efektifitas Mitigasi Serangan DDoS
Menggunakan Firewall Mikrotik pada Jaringan LAN

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	8%
2.	Bab 2 – Daftar Pustaka	25 %	18%
3.	Bab 3 – Analisis dan Perancangan	25 %	13%
4.	Bab 4 – Implementasi dan Pengujian	15 %	7%
5.	Bab 5 – Kesimpulan dan Saran	5 %	3%
6.	Makalah Tugas Akhir	20%	15%

*) Hasil cek plagiarism diisi oleh pemeriksa (staf TU)

*) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)

Mengetahui,

Pemeriksa (Staff TU)



Kampus I
Jl. Bandung 1 Malang, Jawa Timur
P. +62 341 551 253 (Hunting)
F. +62 341 480 435

Kampus II
Jl. Bendungan Sutarni No 188 Malang, Jawa Timur
P. +62 341 551 149 (Hunting)
F. +62 341 582 080

Kampus III
Jl. Raya Tlogomas No 246 Malang, Jawa Timur
P. +62 341 464 316 (Hunting)
F. +62 341 480 435
E. webmaster@umm.ac.id

Daftar Pustaka

- [1] A. Rodiah Machdi, “Analisa dan Implementasi Sistem Keamanan Jaringan Intrusion Detection System (IDS) Berbasis Mikrotik,” 2021.
- [2] B. Jaya, Y. Yuhandri, and S. Sumijan, “Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS),” *Jurnal Sistim Informasi dan Teknologi*, pp. 115–123, Dec. 2020, doi: 10.37034/jsisfotek.v2i4.32.
- [3] “Serangan kegagalan layanan - Wikipedia bahasa Indonesia, ensiklopedia bebas.” Accessed: Nov. 08, 2024. [Online]. Available: https://id.wikipedia.org/wiki/Serangan_kegagalan_layanan
- [4] Nuroji, “Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning,” *Journal of Data Science and Information System (DIMIS)*, vol. 1, no. 2, pp. 41–49, 2023, doi: 10.58602/dimis.v1i2.35.
- [5] “SYN flood - Wikipedia bahasa Indonesia, ensiklopedia bebas.” Accessed: Jul. 23, 2024. [Online]. Available: https://id.wikipedia.org/wiki/SYN_flood
- [6] Mhd.Fakhmi and L. M. Gultom, “Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw,” 2021.
- [7] “What Is a UDP Flood DDoS Attack? | Akamai.” Accessed: Jul. 23, 2024. [Online]. Available: <https://www.akamai.com/glossary/what-is-udp-flood-ddos-attack>
- [8] “HTTP flood DDoS attack | Cloudflare.” Accessed: Jul. 23, 2024. [Online]. Available: <https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/>
- [9] “What is a DNS flood? | DNS flood DDoS attack | Cloudflare.” Accessed: Jul. 23, 2024. [Online]. Available: <https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/>
- [10] “Smurf DDoS attack | Cloudflare.” Accessed: Jul. 23, 2024. [Online]. Available: <https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/>
- [11] D. A. Jakaria and A. Yulianeu, “IMPLEMENTASI FIREWALL DAN WEB FILTERING PADA MIKROTIK ROUTEROS UNTUK Mendukung INTERNET SEHAT DAN AMAN (INSAN),” *JUTEKIN JURNAL TEKNIK INFORMATIKA*, vol. 8, no. 2, pp. 76–83, 2020.
- [12] M. Nadhir, U. Radiah, and M. Qomarudin, “Optimalisasi Keamanan Wide Area Network (WAN) Menggunakan Raw Firewall Berbasis Mikrotik pada PT. Permata Graha Nusantara,” *INTI Nusa Mandiri*, vol. 17, no. 1, pp. 16–23, Aug. 2022, doi: 10.33480/inti.v17i1.3401.
- [13] A. B. Pratomo, “PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS DEVELOPING A FIREWALL SYSTEM ON A COMPUTER NETWORK BASED ON MIKROTIK ROUTEROS,” 2023.
- [14] W. Yunus and M. E. Lasulika, “Security System Analysis against Flood Attacks Using TCP, UDP, and ICMP Protocols on Mikrotik Routers,” *International Journal of Advances in Data and Information Systems*, vol. 3, no. 1, pp. 11–19, Apr. 2022, doi: 10.25008/ijadis.v3i1.1231.
- [15] A. Maulana, N. Suharto, and A. Hariyadi, “Implementation of MikroTik Firewall for Website Access Restriction and Prevention of DoS (Denial of Service) Attacks on Internet Networks of Al-Mahrusiyah Vocational School Lirboyo,” *Journal of Telecommunication Network*, vol. 13, no. 1, 2023.
- [16] D. Apriyanto, Sudarmaji, and A. Hidayat, “PERANCANGAN FIREWALL FILTERING DAN MANAJEMEN BANDWIDTH MENGGUNAKAN ROUTER MIKROTIK PADA JARINGAN

KOMPUTER SMA NEGERI 1 SEPUTIH BANYAKLAMPUNG TENGAH,” *Journal of Computer Science and Informatics (JOCSI)*, vol. 1, no. 1, pp. 21–26, 2023.

- [17] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, “Implementasi Keamanan Jaringan Menggunakan Port Knocking,” *Jurnal Janitra Informatika dan Sistem Informasi*, vol. 2, no. 2, pp. 90–95, Oct. 2022, doi: 10.25008/janitra.v2i2.156.
- [18] D. Novianto, L. Tommy, and Y. Setiawan Japriadi, “Implementation of a Network Security System Using the Simple Port Knocking Method on a Mikrotik-Based Router Implementasi Sistem Keamanan Jaringan Menggunakan Metode Simple Port Knocking Pada Router Berbasis Mikrotik,” *JURNAL KOMITEK*, vol. 1, no. 2, pp. 407–417, 2021, doi: 10.53697/jkomitek.v1i2.
- [19] B. Santosa and A. A. Rismayadi, “Impelementasi Keamanan Jaringan Lan Menggunakan Mikrotik dengan Metode Firewall Filtering,” *E_PROSIDING TEKNIK INFORMATIKA*, vol. 3, no. 1, pp. 179–190, 2022.
- [20] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, “Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking,” *Jurnal Sistim Informasi dan Teknologi*, pp. 82–87, Jan. 2024, doi: 10.60083/jsisfotek.v5i4.329.
- [21] A. N. Hairun, M. R. Katili, R. Takdir, and M. S. Tuloli, “Penerapan firewall di router OS mikrotik pada aplikasi e-apor,” *Jambura Journal of Informatics*, vol. 5, no. 2, pp. 108–119, 2023, doi: 10.37905/jji.
- [22] E. S. R. O. B. langobelen, Y. R. Rr., and catur Iswahyud, “ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN FIREWALL MIKROTIK STUDI KASUS DI TAMAN PINTAR YOGYAKARTA,” *Jurnal JARKOM*, vol. 7, no. 2, pp. 95–102, 2019.
- [23] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-Del-Rincon, and D. Siracusa, “Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection,” *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 876–889, Jun. 2020, doi: 10.1109/TNSM.2020.2971776.
- [24] “Mausezahn - Wikipedia.” Accessed: Jul. 23, 2024. [Online]. Available: <https://en.wikipedia.org/wiki/Mausezahn>
- [25] “hping3 | Kali Linux Tools.” Accessed: Jul. 23, 2024. [Online]. Available: <https://www.kali.org/tools/hping3/>
- [26] “Slowloris (computer security) - Wikipedia.” Accessed: Jul. 23, 2024. [Online]. Available: [https://en.wikipedia.org/wiki/Slowloris_\(computer_security\)](https://en.wikipedia.org/wiki/Slowloris_(computer_security))

Lampiran

Video demonstrasi

https://drive.google.com/file/d/13mWBpCyr3dkU0dqgusEa2_f336kXjH2w/view?usp=drive_link

