RANCANG BANGUN KEAMANAN JARINGAN DENGAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *ZEEK* DAN *FIREWALL* MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA

SKRIPSI

MUHAMMAD HARITS SOFWAN

2007422017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

RANCANG BANGUN KEAMANAN JARINGAN DENGAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *ZEEK* DAN *FIREWALL* MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

MUHAMMAD HARITS SOFWAN

2007422017

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2024

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama	:	Muhammad Harits Sofwan
NIM	:	2007422017
Jurusan/Program Studi	:	Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan
Judul Skripsi	:	RANCANG BANGUN KEAMANAN JARINGAN DENGAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *ZEEK* DAN *FIREWALL* MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut

Depok, 28 Agustus 2024

Muhammad Harits Sofwan
NIM 2007422017

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Muhammad Harits Sofwan

NIM 2007422017

Program Studi : Teknik Multimedia Jaringan

Judul Skripsi :RANCANG BANGUN KEAMANAN JARINGAN DENGAN INTRUSION DETECTION SYSTEM MENGGUNAKAN ZEEK DAN FIREWALL MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis

Tanggal 19, Bulan Agustus, Tahun 2024. dan dinyatakan **LULUS.**

Disahkan oleh		Tanda Tangan
Pembimbing I	: Ayu Rosyida Zain, S.ST., M.T.	(.....)
Penguji I	: Maria Agustin, S.Kom., M.Kom.	(.....)
Penguji II	: Asep Kurniawan, S.Pd., M.Kom.	(.....)
Penguji III	: Iik Muhammad Malik Matin, S.Kom., M.T.	(.....)

Mengetahui :

Ketua Jurusan Teknik Informatika dan Komputer

Dr., Anita Hidayati, S.Kom., M.Kom.
NIP. 197802112009121003

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT. karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan skripsi ini dengan judul **"Rancang Bangun Keamanan Jaringan dengan *Intrusion Detection System* menggunakan *Zeek* dan *Firewall* Mikrotik di PT Artha Media Lintas Nusa."**

Penulisan laporan tugas akhir ini dilakukan dalam rangka memenuhi syarat untuk memperoleh gelar Diploma IV Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer pada Politeknik Negeri Jakarta. Penulisan skripsi ini tidak akan selesai tepat pada waktunya tanpa bantuan, bimbingan dan doa dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa yang senantiasa melimpahkan hikmah dan rahmat-Nya dalam kehidupan serta dalam penyelesaian penelitian ini.
2. Dr. Syamsurizal, S.E., M.M. selaku Direktur Politeknik Negeri Jakarta.
3. Dr. Anita Hidayati, S.Kom., M.Kom selaku Ketua Jurusan Teknik Informatika dan Komputer.
4. Ayu Rosyida Zain, S.ST., M.T. selaku Ketua Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta, sekaligus dosen pembimbing yang telah menyediakan waktu, tenaga, pikiran, arahan, dan dorongan yang tiada henti selama proses penyusunan skripsi ini.
5. Seluruh Staf pengajar Jurusan Teknik Informatika dan Komputer yang telah memberikan ilmu pembelajaran kepada penulis selama berkuliah di Politeknik Negeri Jakarta.
6. Seluruh Staf Administrasi dan pendukungnya yang telah membantu memberikan arahan dan mengurus keperluan terkait administrasi selama berada di Jurusan Teknik Informatika dan Komputer.
7. Pak Bakti selaku pemilik PT Artha Media Lintas Nusa yang telah memberikan kesempatan kepada penulis untuk menjadikan perusahaan

ini sebagai studi kasus dalam skripsi ini, serta Mas Muhyi yang selalu mendampingi dan memberikan ilmu kepada penulis.

8. Orang tua dan keluarga yang selalu memberikan doa, materi, dan dukungan serta kasih sayang kepada penulis selama ini.
9. Febrida Azzahra Putri, A.Md.AB yang telah memberikan doa, dukungan, serta selalu menjadi sumber inspirasi dan semangat kepada penulis untuk menyelesaikan skripsi ini.
10. Teman-teman hibernatot yang sudah memberikan canda tawa, semangat, dan pelajaran tentang pertemanan.
11. Kepada diri sendiri, karena tidak menyerah dalam menempuh Pendidikan dan berhasil menyusun skripsi ini dengan baik.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan skripsi ini, Oleh karena itu, penulis sangat terbuka terhadap kritik dan saran yang membangun, demi perbaikan dan peningkatan kualitas penulisan di masa mendatang. Semoga skripsi ini mudah dipahami oleh pembaca serta menjadi ilmu yang bermanfaat.

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama : Muhammad Harits Sofwan

NIM : 2007422017

Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul: **RANCANG BANGUN KEAMANAN JARINGAN DENGAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *ZEEK* DAN *FIREWALL* MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA**.

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 28 Agustus 2024

Muhammad Harits Sofwan
NIM 2007422017

RANCANG BANGUN KEAMANAN JARINGAN DENGAN *INTRUSION DETECTION SYSTEM* MENGGUNAKAN *ZEEK* DAN *FIREWALL* MIKROTIK DI PT ARTHA MEDIA LINTAS NUSA.

Abstrak

Perkembangan teknologi informasi mengalami pertumbuhan yang sangat pesat, khususnya internet. Internet sangat berdampak positif jika digunakan dengan tepat. Seiring dengan banyaknya pengguna internet di dunia khsususnya Indonesia, semakin banyak juga kejahatan di dunia internet. Kejahatan tidak hanya datang dari luar, tetapi juga dapat terjadi dari dalam perusahaan, di mana ancaman internal seringkali lebih sulit dideteksi dan dapat merusak integritas serta kepercayaan organisasi. Keamanan jaringan merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan informasi di sebuah perusahaan. PT Artha Media Lintas Nusa, sebagai perusahaan yang bergerak di bidang teknologi, memerlukan sistem keamanan yang andal untuk melindungi jaringan dari berbagai ancaman siber. Maka dilakukan implementasi sistem keamanan jaringan dengan menggunakan *Intrusion Detection System* (IDS) *Zeek* yang dikombinasikan dengan *Firewall* Mikrotik. Sistem ini dirancang untuk mendeteksi serangan seperti *Port Scanning, Flooding Attack, dan Brute Force*, serta membuat *System* secara otomatis untuk memblokir IP penyerang dengan bantuan Mikrotik dan *Fail2ban*. Penelitian ini diawali dengan konfigurasi *Zeek* pada server Ubuntu untuk mendeteksi aktivitas mencurigakan dalam jaringan. Kemudian, *Firewall* MikroTik dan *Fail2ban* digunakan untuk mengambil tindakan pencegahan dengan memblokir IP yang terdeteksi melakukan serangan. Hasil implementasi menunjukkan bahwa kombinasi *Zeek* dan *Firewall* Mikrotik efektif dalam meningkatkan keamanan jaringan di PT Artha Media Lintas Nusa.

Kata kunci: *Brute Force, Flooding Attack, Firewall* Mikrotik, *Port Scanning, Zeek*

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME ..... **i**
LEMBAR PENGESAHAN ..... **ii**
KATA PENGANTAR ..... **iii**
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS ..... **v**
Abstrak ..... **vi**
DAFTAR ISI ..... **vii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xii**
BAB I **1**
PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan dan Manfaat 3
1.4.1 Tujuan 4
1.4.2 Manfaat 4
1.5 Sistematika Penulisan 4
BAB II **5**
TINJAUAN PUSTAKA **5**
2.1 Keamanan Jaringan 5
2.2 *Intrusion Detection System* 6
2.3 *Zeek* 6
2.4 *Firewall* Mikrotik 6
2.5 *Fail2ban* 7
2.6 Internet 7
2.7 Server 7
2.8 Ubuntu Linux 8
2.9 VirtualBox 9
2.10 Mikrotik 9
2.10.1 Mikrotik RouterOS 9

2.10.2 Mikrotik RouterBoard 10
2.11 Winbox 10
2.12 *Port Scan*ner 11
2.13 *Flooding Attack* 11
2.14 *Brute Force* 12
2.15 Penelitian Sejenis 12
BAB III 15
PERANCANGAN DAN REALISASI ATAU RANCANG BANGUN 15
3.1 Rancang Penelitian 15
3.2 Tahapan Penelitian 15
3.3 Objek Penelitian 17
BAB IV 18
HASIL DAN PEMBAHASAN 18
4.1 Analisis Kebutuhan 18
4.1.1 Kebutuhan Perangkat Keras 18
4.1.2 Kebutuhan Perangkat Lunak 18
4.2 Perancangan Sistem 19
4.2.1 Cara Kerja Sistem 19
4.3 Implementasi Sistem 23
4.3.1 Installasi Perangkat Lunak 23
4.4 Pengujian 26
4.4.1 Deskripsi Pengujian 27
4.4.2 Prosedur Pengujian 27
4.4.2.1 Prosedur Pengujian Terhadap Serangan *Port Scan*ning 27
4.4.2.2 Prosedur Pengujian Terhadap Serangan *Flooding Attack* 28
4.4.2.3 Prosedur Pengujian Terhadap Serangan *Brute Force* 28
4.4.3 Data Hasil Pengujian 29
4.4.3.1 Data Hasil Pengujian Terhadap Serangan *Port Scan*ning 29
4.4.3.2 Data Hasil Pengujian Terhadap Serangan *Flooding Attack* 31
4.4.3.3 Data Hasil Pengujian Terhadap Serangan *Brute Force* 32
4.4.4 Analisis Pengujian Sistem 33
4.4.4.1 Analisis Pengujian Terhadap Serangan *Port Scan*ning 34
4.4.4.2 Analisis Terhadap Serangan *Flooding Attack* 35
4.4.4.3 Analisis Terhadap Serangan *Brute Force* 37

BAB V **39**
PENUTUP **39**
5.1 Kesimpulan 39
5.1 Saran 40
DAFTAR PUSTAKA ..... **xiii**
DAFTAR RIWAYAT HIDUP ..... **xvi**
LAMPIRAN ..... **xvii**

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Keamanan Jaringan 5
Gambar 2.2 *Zeek* 6
Gambar 2.3 Ilustrasi Internet 7
Gambar 2.4 *Ubuntu Linux* 8
Gambar 2.5 *VirtualBox* 9
Gambar 2.6 Mikrotik RouterOS 10
Gambar 2.7 Mikrotik RouterBoard 10
Gambar 2.8 Winbox 10
Gambar 3.1 *Flowchart* Tahapan Penelitian 16
Gambar 4.1 Skema Cara Kerja Sistem Keamanan Jaringan 20
Gambar 4.2 *Flowchart* deteksi serta respon dari serangan *Port Scan* pada Mikrotik 21
Gambar 4.3 *Flowchart* deteksi terhadap serangan *Port Scan*, *Flooding Attack*, dan *Brute Force* pada *Zeek* 22
Gambar 4.4 *Flowchart* deteksi dan respon terhadap serangan *Flooding Attack* pada Mikrotik 22
Gambar 4.5 *Flowchart* respon *Fail2ban* terhadap *Brute Force* pada *Ubuntu* 23
Gambar 4.6 Instalasi *Zeek* dan *Library* 24
Gambar 4.7 *Repository Zeek* 24
Gambar 4.8 Installasi *Nmap* 25
Gambar 4.9 Instalasi *Hping3* 25
Gambar 4.10 Installasi *Hydra* 25
Gambar 4.11 Installasi *Fail2ban* 26
Gambar 4.12 Winbox 26
Gambar 4.13 Tampilan serangan *Nmap* ke Mikrotik 27
Gambar 4.14 Tampilan serangan *Nmap* ke Ubuntu 28
Gambar 4.15 Tampilan serangan *Flooding Attack* ke Mikrotik 28
Gambar 4.16 Tampilan serangan *Flooding Attack* ke *Ubuntu* 28
Gambar 4.17 Tampilan serangan *Brute Force* ke Mikrotik 29
Gambar 4.18 Tampilan serangan *Brute Force* ke Ubuntu 29

Gambar 4.19 Tampilan *Firewall* Mikrotik ketika terjadi serangan *Port Scan* ke Mikrotik 34
Gambar 4.20 Respon *Firewall* Mikrotik pada serangan *Port Scan* 35
Gambar 4.21 Tampilan tidak berhasilnya percobaan serangan *Port Scan* 35
Gambar 4.22 Tampilan Notice pada *Zeek* ketika terjadi serangan *Port Scan* 35
Gambar 4.23 Tampilan *Firewall* Mikrotik ketika terjadi serangan *Flooding Attack* 36
Gambar 4.24 Respon *Firewall* Mikrotik pada serangan *Flooding Attack* 36
Gambar 4.25 Tampilan Address List pada *Firewall* Mikrotik 37
Gambar 4.26 Tampilan Notice pada *Zeek* ketika terjadi serangan *Flooding Attack* 37
Gambar 4.27 Tampilan tidak berhasilnya percobaan masuk ke sistem 38
Gambar 4.28 Tampilan log dari *Fail2ban* setelah serangan *Brute Force* terjadi . 38

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait 12
Tabel 4.1 Daftar Perangkat Keras 18
Tabel 4.2 Daftar Perangkat Lunak 18
Tabel 4.3 Pecobaan serangan *Port Scan* sebelum diterapkan keamanan 29
Tabel 4.4 Pecobaan Serangan *Port Scan* setelah diterapkan keamanan 30
Tabel 4.5 Pecobaan Serangan *Flooding Attack* sebelum diterapkan keamanan .. 31
Tabel 4.6 Pecobaan Serangan *Flooding Attack* setelah diteapkan keamanan 31
Tabel 4.7 Percobaan Serangan *Brute Force* sebelum diteapkan keamanan..... 32
Tabel 4.8 Percobaan Serangan *Brute Force* setelah diterapkan keamanan 33

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mengalami pertumbuhan yang sangat pesat, khususnya internet. Internet sangat berdampak positif pada perkembangan dunia bisnis, pendidikan, entertain, dan lainnya. Dengan internet, mempermudah kita untuk berbagi informasi dan bekomunikasi kepada siapapum, kapanpun, dan dimanapun dari berbagai penjuru dunia. Dilansir dari apjii.or.id, berdasarkan survey terbaru mengenai jumlah pengguna internet di Indonesia mencapai 221.563.479 dari total jumlah penduduk Indonesia tahun 2023 yaitu 278.696.200 jiwa. Seiring dengan banyaknya pengguna internet di dunia khsususnya Indonesia, semakin banyak juga kejahatan di dunia internet. Kejahatan tidak hanya datang dari luar, tetapi juga dapat terjadi dari dalam perusahaan, di mana ancaman internal seringkali lebih sulit dideteksi dan dapat merusak integritas serta kepercayaan organisasi. Hal tersebut didukung dengan laporan tahunan terakhir 2023 yang dikeluarkan oleh BSSN (Badan Siber Sandi Negara) bahwa sepanjang tahun 2021 telah terjadi serangan siber sebanyak 43.902.996 ke negara Indonesia.

Keamanan jaringan merupakan aspek yang sangat penting bagi setiap organisasi atau perusahaan. Kebutuhan akan keamanan jaringan semakin meningkat seiring dengan berkembangnya teknologi informasi dan komunikasi. PT Artha Media Lintas Nusa sebagai perusahaan yang bergerak di bidang teknologi informasi dan komunikasi juga menghadapi tantangan yang sama dalam menjaga keamanan jaringan mereka. Keamanan jaringan tidak hanya tentang melindungi data sensitif dari akses yang tidak sah, tetapi juga melibatkan upaya untuk mendeteksi dan mencegah serangan yang mungkin terjadi. Serangan terhadap jaringan dapat berasal dari berbagai sumber, termasuk malware, serangan DoS (Denial of Service), *Brute Force*, dan upaya phishing yang dilakukan oleh pihak yang tidak bertanggung jawab. DoS merupakan serangan yang bertujuan untuk mempengaruhi trafik jaringan sehingga jaringan tersebut tidak dapat digunakan oleh pengguna yang berhak atau sah. Serangan DoS dilakukan dengan cara membanjiri ip address jaringan target dengan request sehingga sistem menjadi crash, hang, atau turun

kinerjanya karena beban CPU tinggi. Ini adalah salah satu metode serangan cyber paling populer dalam keamanan jaringan. (Antony & Gustriansyah, 2021)

Pada penelitian Farhan Maulana yang berjudul "Analisis Perbandingan Performa *Intrusion Detection System* (IDS) Dalam Mendeteksi Serangan *Port Scan*ning dan Distributed Denial of Service (DDoS)" menjelaskan bahwa *Suricata* unggul dalam mendeteksi intrusi pada serangan PS dan DDoS, hal ini dapat ditunjukan dengan nilai persentase TPR yang dimiliki *Suricata* paling tinggi dibandingkan nilai persentase TPR *Zeek* dan *Snort*. *Zeek* unggul dalam kecepatan mendeteksi serangan per menit, hal ini dapat ditunjukan dengan nilai DR/m yang dimiliki *Zeek* paling tinggi dibandingkan nilai DR/m *Snort* dan *Suricata*, hal ini membuat *Zeek* sangat cocok untuk diterapkan pada lalu lintas jaringan kecepatan tinggi. Parameter resource usage pada penelitian ini memiliki hasil yang variatif. Pada CPU usage, *Snort* lebih unggul karena nilai persentasenya CPU usage paling minimum dibandingkan *Zeek* dan *Suricata*, sedangkan pada memory usage, *Snort* unggul dalam serangan PS karena memiliki nilai persentase memory usage yang paling minimum, pada case serangan DDoS *Suricata* unggul karena memiliki nilai persentase memory usage yang paling minimum. Kemudian, pada network usage, *Suricata* unggul karena memiliki nilai kb/s paling tinggi dibandingkan *Snort* dan *Zeek*.

Keamanan jaringan merupakan aspek krusial yang harus dijaga dengan baik, terutama dalam menghadapi berbagai ancaman seperti serangan berbahaya dan penyusupan. Untuk memastikan stabilitas dan perlindungan yang optimal, perusahaan seperti PT Artha Media Lintas Nusa memerlukan sistem yang handal dalam mendeteksi serta mengamankan jaringan dari potensi serangan. Administrator jaringan memiliki tanggung jawab besar dalam mengelola kondisi jaringan, khususnya dalam menjaga keamanan sistem agar terhindar dari ancaman luar maupun dalam perusahaan. Kejahatan dalam perusahaan ini dilakukan oleh karyawan dengan akses ke sistem internal, menjadi ancaman serius yang perlu diatasi dengan pengawasan ketat serta teknologi keamanan yang canggih, sehingga insiden penyalahgunaan data dan serangan dapat diminimalisir.

Dari latar belakang diatas maka penulis mengambil judul "Rancang Bangun Keamanan Jaringan dengan *Intrusion Detection System* menggunakan *Zeek* dan Mikrotik pada PT Artha Media Lintas Nusa". Dimana rancang bangun sistem keamanan menggunakan *Zeek*, *Fail2ban*, dan MikroTik untuk meningkatkan keamanan jaringan PT Artha Media Lintas Nusa. Langkah-langkah yang diambil termasuk pemasangan dan konfigurasi untuk memantau lalu lintas jaringan serta pengaturan aturan dan kebijakan keamanan pada *Fail2ban* dan perangkat MikroTik, serta integrasi antara *Zeek* dan mikrotik untuk mendeteksi dan merespons terhadap aktivitas mencurigakan dalam jaringan.

1.2 Rumusan Masalah

Dari latar belakang dapat disimpulkan terdapat beberapa perumusan masalah sebagai berikut:

a. Bagaimana membangun sebuah sistem keamanan yang dapat mendeteksi serta mengamankan dari penyerang yang tidak bertanggung jawab?
b. Bagaimana penerapan *Intrusion Detection System* menggunakan *Zeek* dan *Firewall* Mikrotik?
c. Bagaimana hasil dari pengujian sistem keamanan jaringan di PT Artha Media Lintas Nusa?

1.3 Batasan Masalah

Terdapat Batasan masalah yang bertujuan agar pembahasan menjadi lebih terfokus. Adapun batasan masalah dapat dijelaskan sebagai berikut:

a. Penelitian ini berfokus bagaimana cara implementasi keamanan jaringan menggunakan IDS *Zeek*, *Fail2ban*, dan Mikrotik.
b. Tools yang digunakan dalam penelitian ini adalah *Nmap*, *Hping3*, *Hydra*, *Zeek*, Winbox, dan *Fail2ban*
c. Pengujian dalam penelitian ini menggunakan jaringan lokal serta topologi yang menyesuaikan pada kondisi PT Artha Media Lintas Nusa

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari dilakukannya penelitian ini adalah sebagai berikut:

1.4.1 Tujuan

Tujuan dilakukannya penelitian ini adalah untuk membuat sistem rancang bangun menggunakan IDS *Zeek*, serta keamanan jaringan menggunakan *Fail2ban*, dan Mikrotik. Tools tersebut digunakan untuk mendeteksi dan mengamankan dari serangan *Port Scan*ner, *Flooding Attack*, dan *Brute Force* pada jaringan internet di PT Artha Media Lintas Nusa.

1.4.2 Manfaat

Adapun manfaat dari dilakukannya penelitian ini adalah untuk mengetahui seberapa aman dan membantu meningkatkan keamanan jaringan internet di PT Artha Media Lintas Nusa.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan laporan dari penelitian ini adalah sebagai berikut:

a. BAB I PENDAHULUAN
   Berisi latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan.
b. BAB II TINJAUAN PUSTAKA
   Berisi uraian pembahasan mengenai teori yang mendukung dan membantu penelitian
c. BAB III METODOLOGI PENELITIAN
   Berisi metode pembahasan metode penelitian, tahapan penelitian, objek penelitian, teknik pengumpulan data, dan jadwal penelitian.
d. BAB IV PEMBAHASAN
   Berisi pembahasan proses serta hasil kegiatan selama penelitian yang dilakukan sesuai dengan tahapan dan metode yang telah ditentukan sebelumnya.
e. BAB V KESIMPULAN DAN SARAN
   Berisi kesimpulan dan saran dari penelitian yang telah dilaksanakan

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa kombinasi lapisan keamanan yang diterapkan pada jaringan PT Artha Media Lintas Nusa memiliki peran yang signifikan dalam meningkatkan keamanan jaringan. Beberapa poin penting dari kesimpulan tersebut adalah:

1. Mikrotik berhasil menjalankan peran pentingnya sebagai *Firewall* yang responsif terhadap serangan, terutama dalam menghadapi serangan *Port Scan*ning dan *Flooding Attack*. Dengan menerapkan filter pada *Firewall*, MikroTik mampu mendeteksi, merespons, dan memblokir serangan secara otomatis, sehingga serangan *Port Scan*ning tidak berhasil dan *Flooding Attack* dapat diminimalkan dampaknya.
2. Deteksi Serangan oleh *Zeek* di Ubuntu: *Zeek*, yang digunakan pada Ubuntu, menunjukkan kemampuan deteksi yang baik terhadap aktivitas mencurigakan di jaringan. Namun, *Zeek* hanya berfungsi sebagai alat deteksi dan tidak melakukan aksi pencegahan atau mitigasi secara langsung. Log yang dihasilkan oleh *Zeek* memberikan informasi penting mengenai serangan yang terjadi, seperti *Port Scan*ning dan *Flooding Attack*, namun tidak diiringi dengan tindakan pencegahan otomatis.
3. Peran *Fail2ban* dalam Mengatasi Serangan *Brute Force*: Pada Ubuntu, *Fail2ban* efektif dalam melindungi sistem dari serangan *Brute Force* dengan cara memblokir IP yang gagal melakukan login sebanyak tiga kali. Hal ini menunjukkan bahwa meskipun MikroTik tidak diterapkan untuk menghadapi serangan *Brute Force* demi kemudahan akses bagi pengguna, *Fail2ban* berhasil mengisi kekosongan tersebut dengan memberikan lapisan keamanan yang memadai.
4. Keterbatasan dan Kekuatan Kombinasi Keamanan: Meskipun setiap komponen (MikroTik, *Zeek*, dan *Fail2ban*) memiliki keterbatasannya masing-masing, kombinasi ketiganya memberikan perlindungan yang cukup kuat terhadap berbagai jenis serangan. MikroTik berperan aktif

dalam pencegahan serangan *Port Scan*ning dan *Flooding Attack*, sedangkan *Zeek* dan *Fail2ban* di Ubuntu berfungsi sebagai alat deteksi dan mitigasi yang saling melengkapi.

5.1 Saran

Saran yang dapat penulis berikan terkait penulisan ini adalah alat mikrotik yang belum optimal dalam integrasi dengan ubuntu mengakibatkan kinerja mikrotik sebagai router belum bekerja dengan maksimal. Perlu dilakukan penelitian lebih lanjut agar mikrotik dapat menjadi solusi yang lebih efektif dan efisien dalam mengintegrasikan sistem keamanan pada server Ubuntu. Penelitian tersebut mencakup pengembangan metode atau skrip otomatisasi yang lebih canggih untuk mendeteksi dan merespons ancaman secara real-time, serta memastikan kompatibilitas penuh antara perangkat Mikrotik dan sistem operasi Ubuntu. Dengan demikian, diharapkan Mikrotik dapat berfungsi sebagai alat yang handal dalam menjaga keamanan jaringan dari berbagai serangan yang mungkin terjadi.

DAFTAR PUSTAKA

Antony, F., & Gustriansyah, R. (2021). Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *21*(1), 43–52. https://doi.org/10.30812/matrik.v21i1.1078

Dimas Prakoso, R. (2018). *Implementasi dan Perbandingan Performa Proxmox dalam Virtualisasi dengan Tiga Virtual Server (Studi Kasus : Jurusan Teknik Informatika UNESA) IMPLEMENTASI DAN PERBANDINGAN PERFORMA PROXMOX DALAM VIRTUALISASI DENGAN TIGA VIRTUAL SERVER (Studi Kasus : Information Technology of UNESA) Asmunin*.

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan *Intrusion Detection System* (IDS) Sebagai Keamanan Jaringan dan Komputer. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *4*(2), 413. https://doi.org/10.30865/mib.v4i2.2037

Farida, T. (2019). *PENGEMBANGAN MEDIA PEMBELAJARAN VIRTUAL BOX UNTUK MENGUKUR KELAYAKAN MODUL PADA MATA PELAJARAN KOMPUTER DAN JARINGAN DASAR DI SMKN 7 SURABAYA* (Vol. 4).

Fauzi, R., Muhyidin, Y., & Singasatia, D. (2023). Sistem Keamanan Jaringan Komputer Berbasis Teknik *Intrusion Detection System* (IDS) Untuk Mendeteksi Serangan Distrubuted Denial Of Service (DDOS). In *Jurnal Sains Komputer & Informatika (J-SAKTI* (Vol. 7, Issue 1).

Gondokusuman Yogyakarta, K., Alif Mustofa, T., Sutanta, E., & Triyono, J. (2019). *PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING JARINGAN WI-FI MENGGUNAKAN MIKHMON ONLINE DI WISMA MUSLIM*. *7*(2).

Gunawan AMIK Tunas Bangsa Jl Sudirman Blok No, I. A., & Pematang Siantar, K. (2016). *PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS*.

Gunawan, H., & Ghiffari, M. (2018). PENGELOLAAN JARINGAN DENGAN ROUTER MIKROTIK UNTUK MENINGKATKAN EFEKTIFITAS PENGGUNAAN BANDWITH INTERNET (STUDI KASUS SMK KI HAJAR DEWANTORO KOTA TANGERANG). In *Jurnal Ilmu Komputer* (Vol. 3, Issue 1).

Husna, M. A., & Rosyani, P. (2021). Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram. *JURIKOM (Jurnal Riset Komputer)*, *8*(6), 247. https://doi.org/10.30865/jurikom.v8i6.3631

Kuliah, M., Keamanan, :, Komputer, J., Pengampu, D., & Stiawan, D. (2019). *Scanning*.

Pratomo, A. B. (2023). *https://bufnets.tech https://doi.org/10.59688/bufnets BULLETIN OF NETWORK ENGINEER AND PENGEMBANGAN SISTEM FIREWALL PADA JARINGAN KOMPUTER BERBASIS MIKROTIK ROUTEROS DEVELOPING A FIREWALL*

SYSTEM ON A COMPUTER NETWORK BASED ON MIKROTIK ROUTEROS. *1*(2). https://doi.org/10.59688/bufnets

Ramadhani, Y., & Sholeh, M. (2022). *Jurnal Teknik Informatika dan Komputer Online Learning Uhamka (OLU)*. https://journal.uhamka.ac.id/index.php/jutikom

Ryan Permana, Dochi Ramadhani, & Isnania Lestari. (2019). *Keamanan Jaringan*.

Sahara, D. D., Sapri, A. ;, & Akbar, S. (2024). The Design And Implementation Of Computer Network Monitoring And Security *System* Using Linux Ubuntu Server. In *Jurnal Media Computer Science* (Vol. 3, Issue 1). ARTICLE HISTORY.

DAFTAR RIWAYAT HIDUP

Muhammad Harits Sofwan, lahir di Bogor, 23 Februari 2001. Merupakan anak ke-2 dari tiga bersaudara. Saat ini penulis bertempat tinggal di Cibinong, Bogor. Penulis telah menempuh pendidikan Sekolah Menengah Atas di SMA PLUS PGRI CIBINONG (2016-2019). Penulis juga telah menempuh pendidikan professi CEP-CCIT Fakultas Teknik Universitas Indonesia (2019-2021) konsentrasi Network Administrator Professional dan meneruskan pendidikan di Perguruan Tinggi Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer program studi Teknik Multimedia dan Jaringan dengan konsentrasi Sistem Keamanan Jaringan.

LAMPIRAN

Studi Kasus PT Artha Media Lintas Nusa

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
Jalan Prof. Dr. G. A.Siwabessy, Kampus UI, Depok 16425
Telepon (021) 7270036, Hunting, Fax (021) 7270034
Laman: http://www.pnj.ac.id Posel: humas@pnj.ac.id

Nomor : 1474 PL3 PK.01.09 2024 — 21 Februari 2024
Perihal : Permohonan Izin Observasi

Yth.
Kepala Bagian NOC PT Artha Media Lintas Nusa
Jl. Margonda No.441, Pondok Cina, Kecamatan Beji, Kota Depok, Jawa Barat 16424

Dengan hormat,
Sehubungan dengan mata kuliah skripsi yang dilaksanakan pada semester 8 (delapan) Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta. Dengan ini kami mohon kesediaan Bapak/Ibu agar dapat mengizinkan mahasiswa kami untuk melakukan observasi di PT Artha Media Lintas Nusa pada tanggal 21 Februari 2024.

Tugas mata kuliah ini bertujuan untuk menambah wawasan terkait dengan aplikasi teori yang sudah dipelajari di Kampus dengan kondisi lapangan sebagai wadah pembelajaran dan penambah informasi mengenai mata kuliah tersebut. Adapun berikut adalah nama mahasiswa kami:

No.	Nama dan Nim	Semester/Program Studi	Keterangan
1	Muhammad Harits Sofwan (2007422017)	8 / Program Studi Teknik Multimedia dan Jaringan (TMJ CCIT SEC)	Permohonan Penelitian Skripsi

Demikian surat ini kami buat, atas kerjasama Bapak/Ibu kami ucapkan terima kasih.

a.n. Direktur,
Wakil Direktur Bidang Kemahasiswaan

Iwa Sasmidjat, S.T., M.T
NIP. 196106071986011002

Tembusan :
1. Direktur;
2. Wakil Direktur Bidang Akademik;
3. Ketua Jurusan Teknik Informatika dan Komputer;
4. Kepala Bagian Akademik dan Kemahasiswaan;
5. Kepala Bagian Keuangan dan Umum

Politeknik Negeri Jakarta