STUDY COMPLETION PROGRAM

INTERNSHIP TRACK

LAPORAN AKHIR INTERNSHIP

PEMBELAJARAN STRATEGI PENGAMANAN JARINGAN MIKROTIK DARI SERANGAN DDOS DAN BRUTE FORCE DI PT BENTANG JOHAR AWAL

Oleh :

Nama : Tegar Pratama

NIM : 20210040036

FAKULTAS TEKNIK KOMPUTER DAN DESAIN

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS NUSA PUTRA

2025

LAPORAN AKHIR INTERNSHIP

PEMBELAJARAN STRATEGI PENGAMANAN JARINGAN MIKROTIK DARI SERANGAN DDOS DAN BRUTE FORCE DI PT BENTANG JOHAR AWAL

Diajukan Untuk Memenuhi Salah Satu Syarat

Dalam Menempuh Seminar Akhir Internship Pada Jalur Program Internship

Di Program Studi Teknik Informatika

Oleh :

Nama : Tegar Pratama

NIM : 20210040036

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

PROGRAM STUDI TEKNIK INFORMATIKA

UNIVERSITAS NUSA PUTRA

2025

LEMBAR PENGESAHAN

LAPORAN AKHIR INTERNSHIP

JUDUL :

Pembelajaran Strategi Pengamanan Jaringan Mikrotik Dari Serangan Ddos Dan Brute Force Di PT Bentang Johar Awal

Disusun Oleh :

Nama : Tegar Pratama

NIM : 20210040036

Laporan ini telah diseminarkan di hadapan penguji seminar akhir internship pada program internship di program studi Teknik Informatika.

Sukabumi, 20 Januari 2025

Ketua Penguji	Pembimbing Utama
Lusiana Sani Parwati, S.Pd., M.Mat	Anggun Fergina, M.Kom
NIDN.0423049702	NIDN.0407029301

Ketua Prodi Teknik Informatika

Ir. Somantri, S.T, M.Kom

NIDN.0419128801

ii

ABSTRAK

Serangan *Distributed Denial Of Service (Ddos)* dan *Brute Force* merupakan ancaman serius bagi keamanan jaringan yang dapat mengakibatkan gangguan layanan serta penurunan performa system [1]. PT Bentang Johar Awal *(Sawarga Network)*, perusahaan yang bergerak di bidang jaringan, memberikan materi dan pelatihan kepada mahasiswa untuk mempelajari serta mempraktikkan strategi pengamanan yang efektif menggunakan perangkat *mikrotik* [2]. Kegiatan ini tidak hanya berfokus pada pengamanan jaringan, tetapi juga mencakup pemahaman dasar-dasar arsitektur jaringan, seperti model *OSI Layer*, sistem operasi *linux*, dan alokasi jaringan pada perangkat *mikrotik*[3].

Dalam kegiatan magang ini, mahasiswa diperkenalkan pada berbagai metode pengamanan jaringan yang mencakup pengaturan *firewall* untuk menyaring lalu lintas jaringan, serta perlindungan terhadap serangan yang berulang seperti *brute force* dan *DdoS*[4]. Melalui simulasi serangan dan praktik konfigurasi langsung, mahasiswa belajar menerapkan teknik-teknik mitigasi untuk mencegah serangan dari berbagai sumber, menghalangi upaya *login* tidak sah, serta membatasi jumlah koneksi yang dapat menyebabkan jaringan menjadi lambat atau tidak stabil[5].

Pelatihan ini juga mencakup strategi keamanan pada perangkat *Mikrotik*, yang melibatkan penyesuaian pada aturan-aturan keamanan untuk mendeteksi dan menghentikan ancaman sejak awal[1]. Dengan pemahaman menyeluruh ini, mahasiswa diharapkan mampu mengenali potensi ancaman lebih baik dan dapat mengonfigurasi perangkat jaringan untuk menjaga stabilitas dan keamanan jaringan[2]. Hasil dari pelatihan ini diharapkan tidak hanya meningkatkan kemampuan mahasiswa dalam pengamanan jaringan, tetapi juga memberi kontribusi dalam pengembangan langkah-langkah keamanan yang lebih efektif dalam menghadapi ancaman serangan siber di masa depan[3].

Kata Kunci: Keamanan Jaringan, *Mikrotik*, *Distributed Denial of Service*, Serangan *DDoS*, *Brute Force*, *Firewall*, Proteksi Jaringan, *Sawarga Network*, Pengamanan Jaringan, Konfigurasi *Mikrotik*.

DAFTAR ISI

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital ini, keamanan jaringan menjadi prioritas utama bagi banyak perusahaan yang bergantung pada infrastruktur *IT* untuk operasional harian mereka. Serangan siber seperti *Distributed Denial of Service (DDoS)* dan *brute force* merupakan ancaman yang umum dihadapi oleh berbagai institusi dan dapat mengakibatkan gangguan pada stabilitas jaringan, kehilangan data, serta menurunkan performa sistem. Untuk mengantisipasi ancaman ini, strategi pengamanan jaringan yang efektif diperlukan, terutama melalui pemahaman menyeluruh tentang arsitektur jaringan dan pengelolaan perangkat seperti *Mikrotik*.

PT Bentang Johar Awal *(Sawarga Network)*, sebuah perusahaan yang bergerak di bidang jaringan, memberikan kesempatan bagi mahasiswa untuk belajar tentang berbagai aspek keamanan jaringan. Dalam kegiatan magang ini, mahasiswa tidak hanya mempelajari cara menangkal serangan *DDoS* dan *brute force*, tetapi juga diberikan pemahaman mendalam tentang konsep dasar jaringan, seperti model *OSI Layer*, dasar-dasar sistem operasi *Linux*, serta teknik alokasi jaringan pada perangkat *Mikrotik*. Mahasiswa diajarkan bagaimana mengonfigurasi jaringan, mengelola lalu lintas data, serta menerapkan langkah-langkah pencegahan terhadap berbagai ancaman siber.

Pelatihan ini bertujuan untuk memberikan mahasiswa keterampilan dan wawasan praktis tentang keamanan jaringan serta implementasinya di dunia industri. Dengan menggabungkan pemahaman konsep dasar dengan praktik langsung, mahasiswa diharapkan dapat mengembangkan keterampilan teknis yang siap diterapkan dalam dunia kerja, khususnya dalam bidang teknologi informasi dan jaringan.

1.2 Tujuan

Tujuan mengikuti kegiatan magang ini adalah untuk memenuhi syarat kelulusan dan sebagai bagian dari *Program Study Completion* (SCP) yang wajib diikuti oleh mahasiswa tingkat akhir di Universitas Nusa Putra. Adapun tujuan khusus yang ingin dicapai dari kegiatan magang ini adalah sebagai berikut:

1. Meningkatkan keterampilan teknis dan pengetahuan dalam bidang keamanan jaringan serta konfigurasi perangkat Mikrotik.
2. Memperoleh pengalaman praktis dalam mengatasi serangan DDoS, brute force, serta konfigurasi pengamanan jaringan di dunia industri.
3. Meningkatkan kemampuan dalam analisis dan pemecahan masalah terkait pengamanan jaringan.
4. Membekali mahasiswa dengan pengetahuan tentang dasar-dasar arsitektur jaringan, seperti model OSI Layer, sistem operasi Linux, serta teknik alokasi jaringan pada perangkat Mikrotik yang dapat diterapkan dalam pengamanan jaringan yang lebih luas.

1.3 Manfaat

1.3.1 Bagi Mahasiswa

a) Memperoleh pengetahuan dan keterampilan praktis dalam bidang keamanan jaringan, terutama dalam menghadapi serangan DDoS dan brute force.
b) Memahami dasar-dasar arsitektur jaringan, seperti model OSI Layer, sistem operasi Linux, dan teknik alokasi jaringan pada perangkat Mikrotik.
c) Meningkatkan kemampuan analisis dan problem-solving dalam menghadapi tantangan keamanan jaringan.
d) Memperoleh pengalaman kerja nyata yang dapat menjadi bekal untuk memasuki dunia kerja di bidang teknologi informasi.
e) Meningkatkan kemampuan komunikasi dan kerja sama dalam lingkungan kerja profesional.

1.3.2 Bagi Perusahaan

a) Berperan aktif dalam menciptakan SDM yang kompeten di bidang jaringan melalui program pelatihan yang relevan.
b) Memperoleh tenaga tambahan yang dapat membantu dalam proses simulasi dan pengujian konfigurasi jaringan.
c) Membangun hubungan yang lebih kuat dengan lembaga pendidikan untuk mengakses talenta muda berbakat.
d) Memperkuat citra perusahaan sebagai entitas yang mendukung pengembangan pendidikan dan keahlian praktis di bidang jaringan.

1.3.3 Bagi Lembaga

a) Meningkatkan hubungan kerja sama dengan dunia industri, khususnya di bidang teknologi informasi dan jaringan.
b) Menyediakan peluang bagi mahasiswa untuk mengembangkan keterampilan praktis yang relevan dengan kebutuhan pasar kerja.
c) Meningkatkan reputasi universitas melalui lulusan yang memiliki kompetensi dan pengalaman industri yang memadai.
d) Mendukung pencapaian kurikulum pendidikan tinggi yang berbasis praktik dan relevansi industri.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS

BAB II

PENUTUP

2.1 Kesimpulan

Magang di PT Bentang Johar Awal (Sawarga *Network*) memberikan pengalaman berharga dalam mempelajari dan mempraktikkan dasar-dasar pengelolaan jaringan. Beberapa poin penting yang dapat disimpulkan adalah:

1. Pemahaman Dasar Jaringan
   - Saya mempelajari konfigurasi perangkat Mikrotik, termasuk pengaturan routing, firewall, dan integrasi dengan perangkat lain.
   - Pengelolaan *switch Huawei* dan Juniper, mulai dari reset hingga konfigurasi *IP address*, membantu memahami peran perangkat ini dalam infrastruktur jaringan.
2. Langkah Pengamanan Jaringan
   - Saya menerapkan pengamanan sederhana dengan memblokir port yang tidak digunakan dan menyaring lalu lintas menggunakan firewall di Mikrotik.
   - Simulasi serangan dengan Nmap memberikan wawasan awal tentang deteksi dan pencegahan ancaman jaringan.
3. Pemahaman Konsep dan Teknologi Pendukung
   - Belajar dasar-dasar Linux untuk pengelolaan sistem jaringan, termasuk penggunaan aplikasi *Looking Glass*.
   - Memahami konsep OSI Layer untuk troubleshooting dan analisis jaringan, khususnya dalam komunikasi data antar perangkat.

2.2 Saran

Perlu adanya program lanjutan untuk memperdalam praktik pengelolaan dan pengamanan jaringan agar peserta magang dapat lebih siap menghadapi tantangan dunia kerja.

DAFTAR PUSTAKA

Achmad. (2020). Rancang Bangun Aplikasi Deteksi Dan Penanganan Serangan DDOS Dan Port Scanning Memanfaatkan Snort Pada Jaringan Komputer. Jurnal Teknologi Informasi. *Jurnal Teknologi Informasi*, 44-53.

Alhamri. (2022). Pemanfaatan API Client Berbasis Python untuk Konfigurasi IPS pada Router Mikrotik. *Jurnal Teknik Ilmu Dan Aplikasi*, 195-205.

Basorudin. (2021). Perancangan dan Implementasi Konfigurasi Wifi Router dan Jaringan Wireless dengan Rb951ui-2nd. *Building of Informatics, Technology and Science (BITS)*, 186-193.

Haris. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. . *Komputika: Jurnal Sistem Komputer*, 67-76.

Hendri. (2023). Analisa Keamanaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall. *JURNAL AMPLIFIER: JURNAL ILMIAH BIDANG TEKNIK ELEKTRO DAN KOMPUTER*, 33-39.

Pastara. (2021). KEAMANAN JARINGAN KOMPUTER DENGAN METODE PACKET FILTERING PADA KEMENTERIAN SOSIAL REPUBLIK INDONESIA JAKARTA.

PT BENTANG JOHAR AWAL *(Sawarga Network)*. (2024). Retrieved from sawarganetwork.co.id: https://sawarganetwork.co.id/

Ubaidillah. (2023). Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware. *TIM: Jurnal Teknologi Informasi Dan Multimedia*, 208-217.

Zulfikri, P. H. (2023). Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking. Digital Transformation Technology. *Digital Transformation Technology*, 857-863.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS