JUTINDA
Jurnal Teknik Informatika Unanda

Vol. 3, No. 1, Mei 2024
p-ISSN ……
e-ISSN 2963-0843
https://ojs.unanda.ac.id/index.php/jutinda

Rancang Bangun Sistem Keamanan Jaringan Menggunakan Metode Port Knocking Dan Port Blocking Dengan Notifikasi Email Pada SMK Kartika XX-2 Palopo

Dasril [1], Muhlis Muhallim[2], Solmin Paembonan[3], Syawal[4]
[123]Fakultas Teknik, Universitas Andi Djemma,Palopo, Indonesia
Email: [1]dasrilbachmid@gmail.com, [2]muhlismuhallim@gmail.com, [3]solmin.p@unanda.ac.id, syawalunanda@gmail.com[3]

Abstrak

Penelitian ini bertujuan untuk merancang dan membangun system keamanan jaringan menggunakan Port Knocking dan Port Blocking pada SMK Kartika Luwu untuk menyelesaikan permasalahan koneksi internet sering mengalami lost dan menjadi lambat, tidak adanya sistem pengamanan jaringan serperti firewall dan sistem notifikasi yang dapat memberitahuakan apabila koneksi putus atau diserang oleh hacker pada koneksi internet. Dengan sistem koneksi internet pada sekolah tersebut menjadi stabil dan terhindar dari serangan orang yang tidak berkepentingan serta dapat memberikan notifikasi apabila jaringan mengalami masalah atau serangan. Penelitian ini dilaksanakan di at SMK Kartika XX-2 Palopo. Penelitian ini menggunakan metode penelitian dan pengembangan (R&D). Metode pengumpulan data termasuk observasi langsung ke lokasi penelitian, wawancara dengan operator dan administrator jaringan sekolah, dan studi pustaka. Test dilakukan dengan browser, NMAP dan Email. Hasil penelitian yang telah dilakukan menggunakan metode port scanning dan port blocking yang, dalam kombinasi dengan firewall mikrotik, memiliki kemampuan untuk memberikan sistem keamanan pada jaringan, melindungi router mikrotik dari port scanning dan port blocking melalui aplikasi NMAP, dan mengirimkan serangan melalui email..

Kata kunci: *Port Knocking, Port Blocking, R&D, Email, NMAP*

1. PENDAHULUAN

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan komputer berkomunikasi satu sama lain dan bertukar data. Tujuan jaringan komputer adalah untuk mencapai tujuannya, dan setiap komponen jaringan komputer memiliki kemampuan untuk meminta dan menyediakan layanan. Klien adalah orang yang meminta layanan, dan server adalah orang yang memberikan layanan. (Fergina et al., 2023). Layanan jaringan adalah layanan yang disediakan oleh jaringan komputer yang fungsinya membuat penggunaan sumber daya bersama, termasuk perangkat lunak dan perangkat keras, menjadi lebih mudah. (Prayoga & Mukmin, 2021)

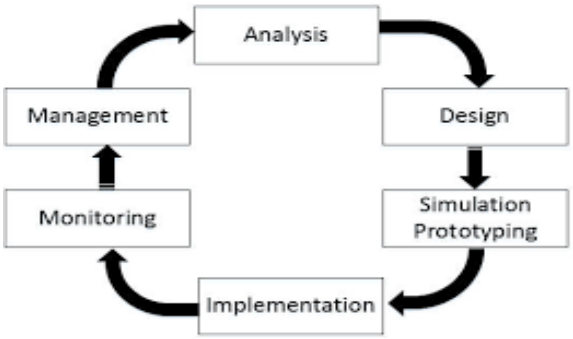
SMK Kartika XX-2 Palopo Saat ini sekolah telah menggunakan komputer dan jaringan local area network (LAN) sebagai aktifitas pembelajaran pada laboratorium komputer, dengan besar kuota 30 Mbps yang diberikan oleh ISP Indihome kemudian dibagikan melalui sebuah switch kepada 20 unit PC, permasalahan yang didapat pada saat observasi awal yaitu koneksi internet sering mengalami lost dan menjadi lambat, tidak adanya sistem pengamanan jaringan serperti firewall dan sistem notifikasi yang dapat memberitahuakan apabila koneksi putus atau diserang oleh hacker pada koneksi internet, membuat banyak komputer yang mengalami hang dan bluescreen akibat terkena serangan virus atau spam dari jaringan internet.

Pada penelitian ini akan dirancang dan dibangun sistem kemamanan jaringan menggunakan port knocking dan port blocking dengan notifikasi email pada SMK Kartika XX-2 Palopo, sehingga koneksi internet pada sekolah tersebut menjadi stabil dan terhindar dari serangan orang yang tidak berkepentingan serta dapat memberikan notifikasi apabila jaringan mengalami masalah atau seranga

2. METODE PENELITIAN

2.1 Metode Penelitian

Penulis menggunakan metode penelitian Research and Development (R&D) yang sudah dikembangkan berdasarkan kebutuhan untuk menghasilkan produk tertentu dan menguji keefektifan produk tersebut. Dalam penelitian ini, model atau tahapan penelitian yang digunakan adalah model Network Design Life Cycle (NDLC), sehingga rangkaian proses penelitian dapat d (Lusi & Suban Belutowe, 2023).



Gambar 1 Model NDLC
Sumber: (Safitri et al., 2019)

2.2 Teknik Pengumpulan Data

a. Observasi

Metode ini melibatkan terjun langsung di SMK Kartika XX-2 Palopo dan dokumentasi data tentang sistem keamanan jaringan.

b. Wawancara

Wawancara dilakukan terhadap kepala sekolah, guru lab, dan staf yang memiliki kemampuan dan informasi yang diperlukan untuk melengkapi temuan observasi.

c. Studi Pustaka

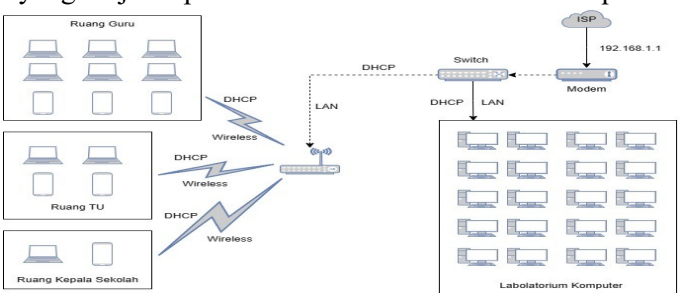
Studi kepustakaan adalah teknik pengumpulan data yang melibatkan membaca buku referensi atau dokumentasi yang berkaitan dengan penelitian tentang keamanan jaringan. Studi kepustakaan juga mencakup kegiatan browsing untuk mencari informasi atau dokumentasi yang terkait dengan subjek penelitian yang sedang dipelajari.

d. Kuesioner

Kuesioner adalah sebuah teknik penghimpun data dari 20 jumlah siswa atau responden melalaui seperangkat pertanyaan untuk di jawab. Dengan memberikan daftar pertanyaan tersebut, jawaban-jawaban yang di peroleh yaitu dari siswa kelas dua kemudian di kumpulkan sebagai data penelitian.

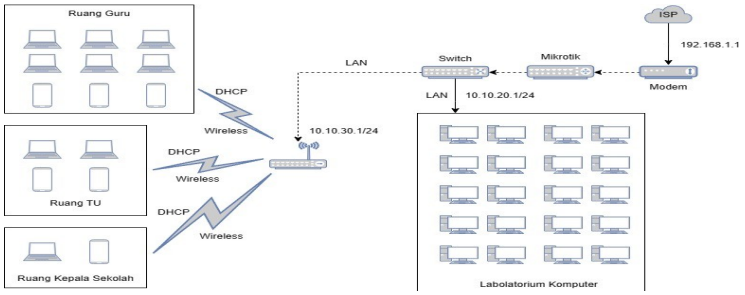
2.3 Analisis Sistem

Analisis sistem yang berjalan pada SMK Kartika XX-2 Kota Palopo sebagai berikut:



Gambar 2 Topologi sistem yang berjalan

Analisis sistem yang diusulkan pada SMK Kartika XX-2 Kota Palopo sebagai berikut:



Gambar 3 Topologi sistem yang diusulkan

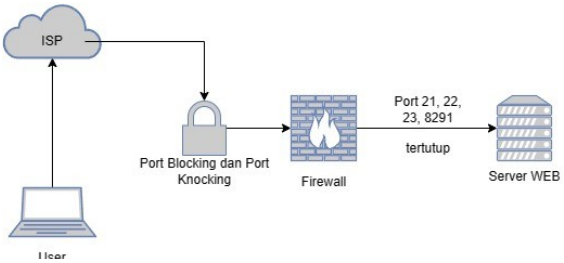
Berdasarkan gambar di atas, peneliti akan menerapkan mikrotik sebagai *router* dan merapkan *port knocking* dan *port blocking* kemudian membuat notifikasi melalui *email* apabila jaringan *lost* atau terjadi serangan oleh *hacker*. Jaringan dari *router* mikrotik akan dibagikan kepada 1 buah *switch* dan 1 buah *access point* menuju laboratorium komputer, ruang guru, ruang TU dan ruang kepala sekolah.

Analisis kebutuhan *hardware* dan *software* dapat dilihat pada tabel 1 sebagai berikut:

Tabel 1 *Hardware* dan *Software*

No	Jenis Komponen	Nama Komponen	Versi
1	*Hardware*	Mikrotik	RB-931-2nd-hap-mini
		Kabel UTP	Cat-6
2	*Software*	Winbox 64 bit	V3.3.1
		Cisco Packet Tracer	8.2.1
		Nmap	7.94

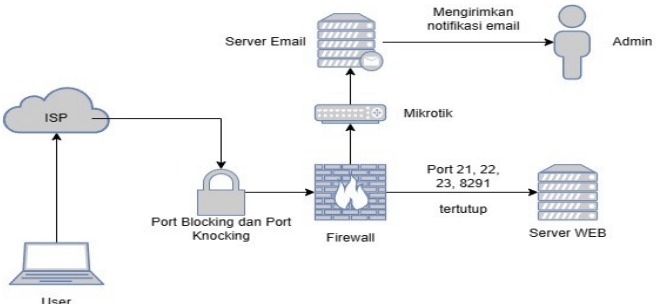
Untuk perancangan *Port Knocking* dan *Port Blocking*, seperti pada gambar 4.



Gambar 4 Alur *Port Knocking dan Port Blocking*

Pada tahap ini penulis melakukan perancangan *port knocking* dan *port blocking* menggunakan mikrotik *RB-931-2nd-hap-mini* dengan cara mengakses firewall pada menu IP menggunakan winbox. Kemudian penulis menkonfigurasi filter rules, NAT dan mangle untuk memblok port 21 (FTP), 22 (SSH), 23 (TELNET), dan 8291 (WINBOX).

Untuk perancangan notifikasi email, seperti pada gambar 5.



Gambar 5 Alur Notifikasi Email

JUTINDA
Jurnal Teknik Informatika Unanda
Vol. 3, No. 1, Mei 2024
p-ISSN ……
e-ISSN 2963-0843
https://ojs.unanda.ac.id/index.php/jutinda

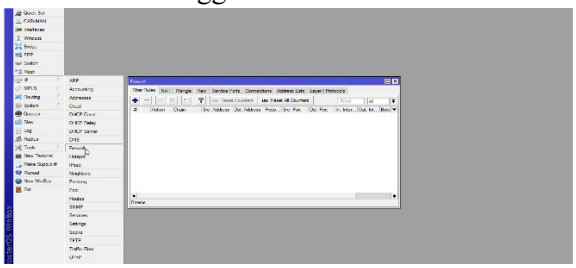
Pada tahap ini penulis melakukan perancangan notivikasi *email* menggunakan mikrotik *RB-931-2nd-hap-mini* dengan cara mengakses *netwatch host* dan *email setting* menggunakan winbox. *netwatch host* akan diberikan *script* agar apabila terjadi serangan akan mengikirimkan notifikasi ke *email* yang telah terdaftar pada *email* setting yang telah diisi dengan *email* admin.

3. HASIL DAN PEMBAHASAN

3.1 Impelementasi Mikrotik

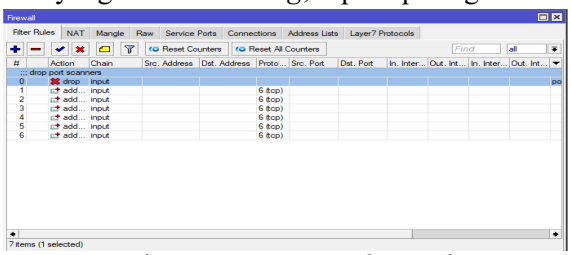
a. Setting mikrotik *port knocking* dan *port blocking*

Langkah pertama adalah membuka aplikasi Winbox. Setelah itu, klik menu "IP", lalu pilih "Firewall", dan selanjutnya klik "Filter Rules". Kemudian, untuk membuat aturan baru, klik tombol tambah (+) yang berwarna biru. Dengan langkah-langkah ini, dapat membuat rule baru dalam konfigurasi firewall Mikrotik menggunakan Winbox.



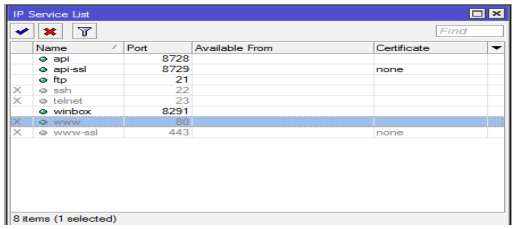
Gambar 6 Menu *Firewall*

List daftar semua *rule* yang sudah di *setting*, seperti pada gambar dibawah.



Gambar 7 Menu *List Filter Rules*

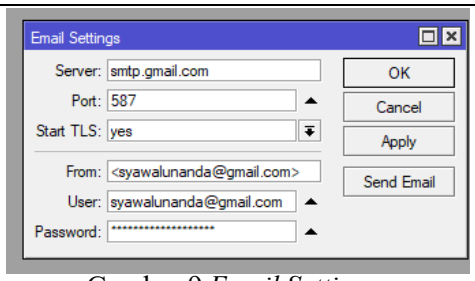
Implementasi dan Konfigurasi *Port Blocking* Pertama buka winbox, kemudian klik menu IP, *Services*, kemudian pilih *port* yang ingin di blok.



Gambar 8 *Port* yang Telah diblok

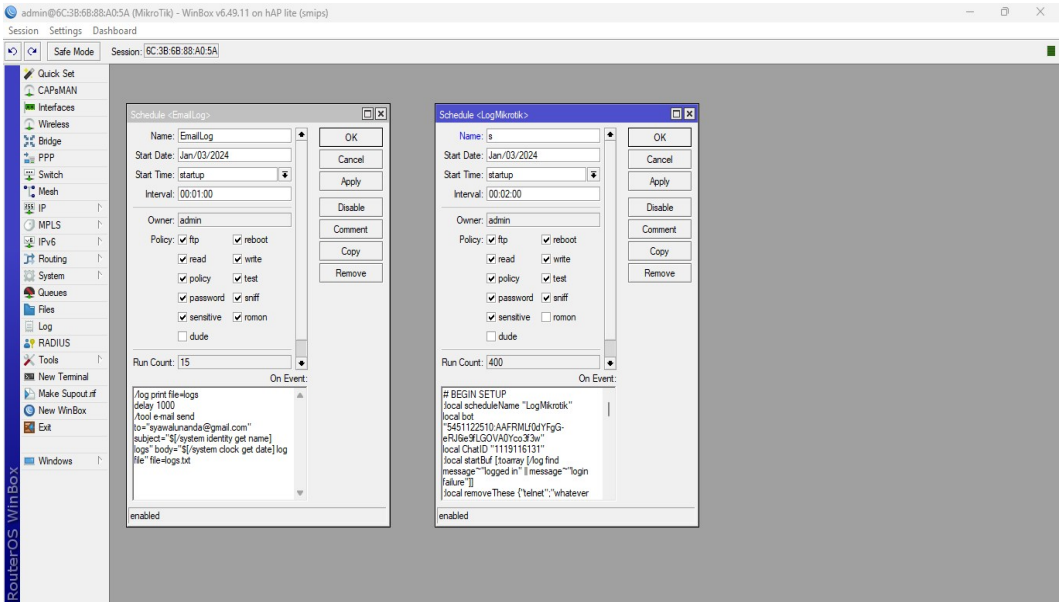
b. Setingg Notifikasi Email

Pertama buka winbox, kemudian klik menu *tools*, *email*, kemudian isi email *setting*, seperti pada gambar 9.



Gambar 9 *Email Settings*

Selanjutnya buat *scheduler* untuk proses mengirimkan serangan ke *log* mikrotik seperti pada gambar dibawah ini.

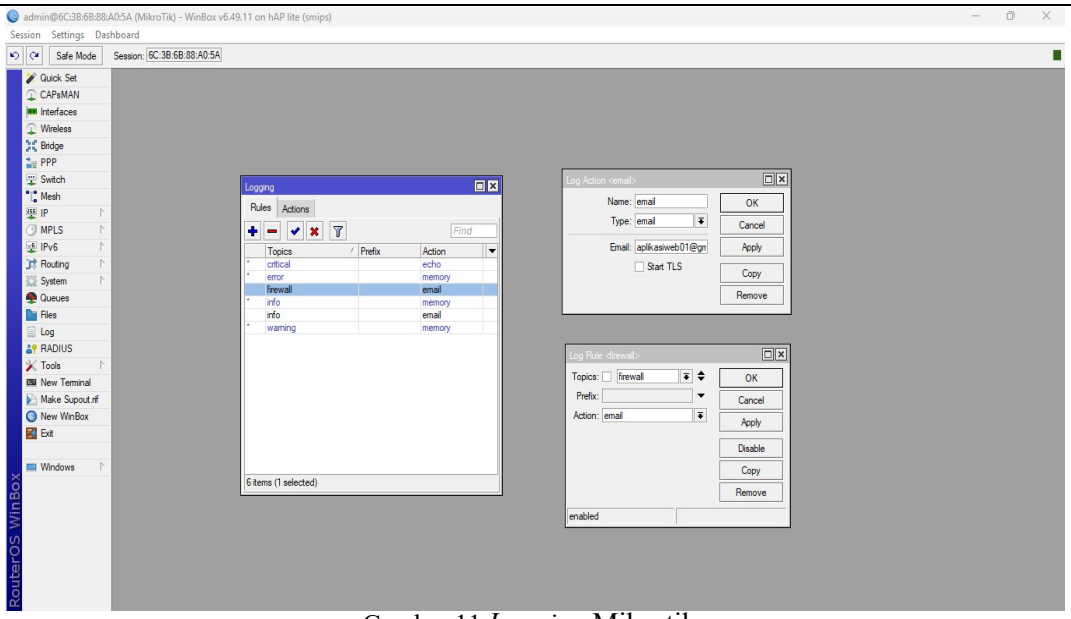


Gambar 10 *Scheduler* Email Log Mikrotik

Pada gambar diatas menjelaskan proses pembuatan scheduler email untuk proses pengiriman serangan ke email yang digunakan untuk menerima notifikasi serangan port scanning.

Selanjutnya buat logging untuk proses serangan ke log mikrotik seperti pada gambar 11 dibawah ini.

JUTINDA
Jurnal Teknik Informatika Unanda
Vol. 3, No. 1, Mei 2024
p-ISSN ……
e-ISSN 2963-0843
https://ojs.unanda.ac.id/index.php/jutinda



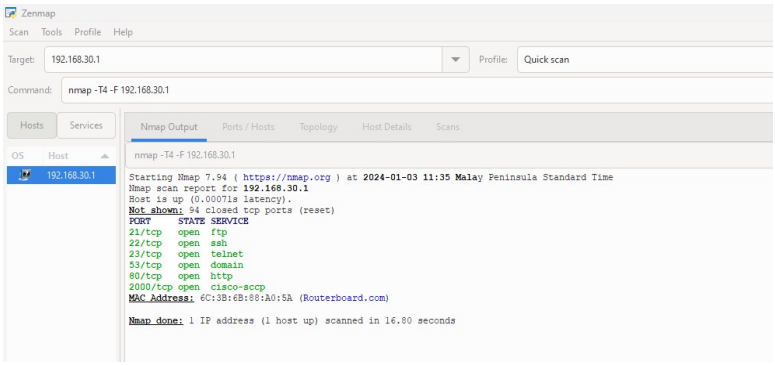
Gambar 11 *Logging* Mikrotik

Pada gambar diatas menjelaskan proses pembuatan *Logging* mikrotik untuk proses pengiriman serangan ke email yang digunakan untuk menerima notifikasi serangan *port scanning*.

3.2 Pengujian *Port Scanning* dan *Port Blocking*

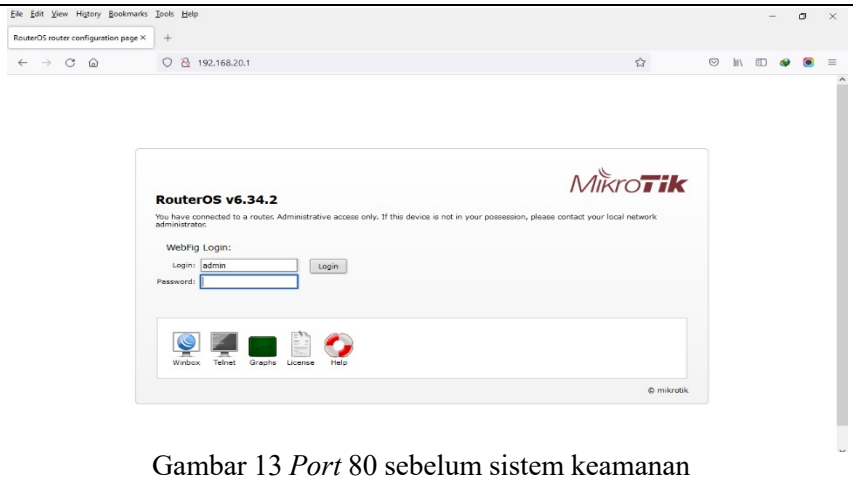
a. Pengujian sebelum *port scanning* dan *port blocking*

Sebelum *port scanning* diaktifkan, metode *port scanning* diuji pada aplikasi NMAP.. Dapat di lihat pada Gambar 12:



Gambar 12 Pengujian *Scanning Port* sebelum sistem keamanan

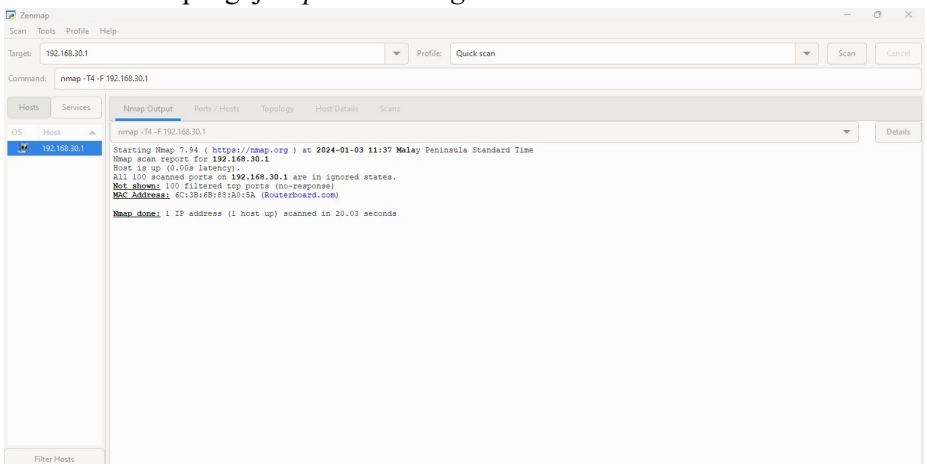
Sebelum port scanning diaktifkan, pengujian kedua dilakukan menggunakan metode port scanning pada aplikasi NMAP.. Dapat di lihat pada Gambar 13:



Gambar 13 *Port* 80 sebelum sistem keamanan

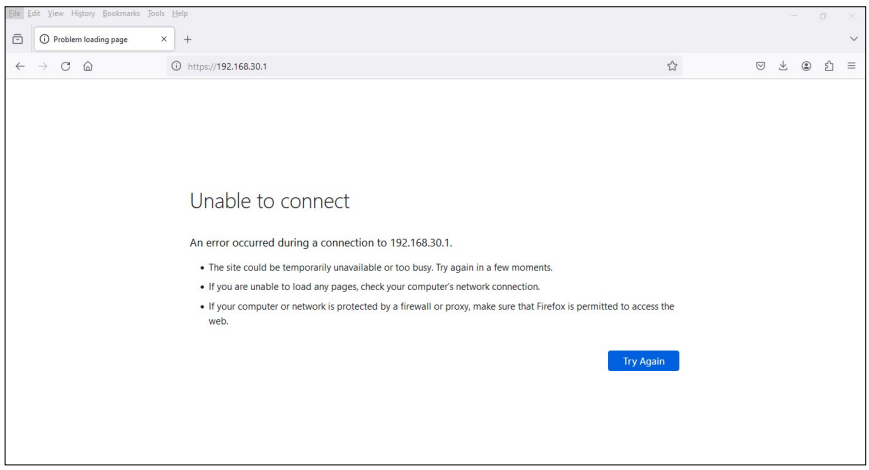
b. Pengujian setelah *port scanning* dan *port blocking*

Pengujian pertama dilakukan pada sistem yang telah dilindungi menggunakan *port scanning*. Berikut adalah hasil dari pengujian *port scanning*.



Gambar 14 *Scanning Por*t *NMAP* adanya sistem keamanan

Pengujian kedua dilakukan pada sistem yang diproteksi oleh sistem yaitu dengan menggunakan *port scanning.* Dapat di lihat pada Gambar 15:



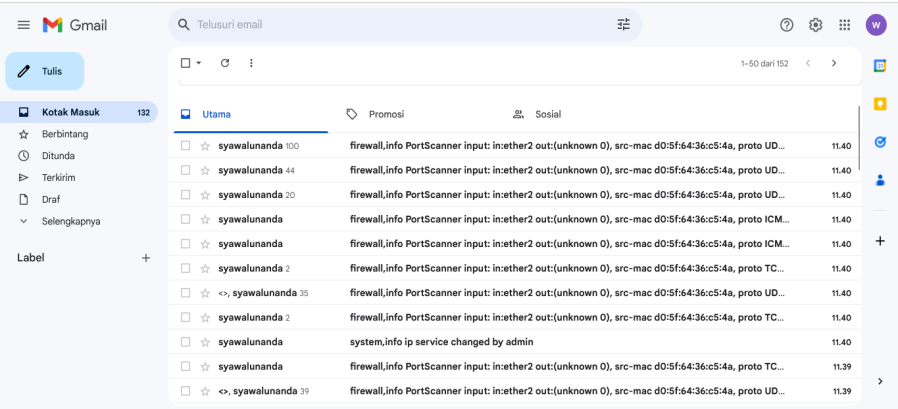
Gambar 15 *Port* 80 setelah sistem keamanan

JUTINDA Jurnal Teknik Informatika Unanda
Vol. 3, No. 1, Mei 2024
p-ISSN ……
e-ISSN 2963-0843
https://ojs.unanda.ac.id/index.php/jutinda

Dengan demikian, setelah menggunakan metode pemindaian port untuk port 43 untuk domain, dapat disimpulkan bahwa pemblokiran tidak dapat dilakukan karena port tersebut digunakan untuk akses DNS hotspot mikrotik., dapat dilihat pada tabel dibawah ini.

c. Hasil Pengujian Notifikasi *Email*

Pengujian notifikasi *email* yang dilakukan pada sistem yang diproteksi oleh sistem yaitu dengan menggunakan akun *gmail* dengan adanya serangan yang terjadi. Dapat di lihat pada gambar 16:



Gambar 16 Laporan Serangan pada *Email*

Setelah *port scanning* diaktifkan, terlihat bahwa upaya penetrasi tidak lagi dapat dilakukan. Ini terjadi karena *port scanning* menyebabkan pemutusan koneksi, sehingga upaya penetrasi tidak dapat menemukan target yang dituju. Berdasarkan hasil pengujian tersebut, kedua serangan, baik melalui NMAP atau metode serangan lainnya, telah berhasil dicegah. Sistem berfungsi dengan normal dan dapat mengamati semua hasil pengujian sistem menggunakan *port scanning* dan *port blocking* dari Tabel 4 sebagai berikut:

Tabel 2 Hasil Pengujian Sistem Keamanan Jaringan

No	Pengujian	Hasil Pengujian		Keterangan
		Berhasil	Gagal	
1.	Serangan *NMAP*	Ö		Tidak dapat menampilkan *port-port* yang terbuka pada router mikrotik.
2.	Akses mikrotik pada browser	Ö		Tidak dapat mengakses mikrotik lewat port 80.
3.	Notifikas Email	Ö		Dapat mengirim pesan ke email dengan adanya serangan *port scanning*.

3.3 Pengujian Kuesioner

Pengujian kuesioner dengan format usability menggunakan teknik analisis deskriptif, yang melibatkan perhitungan sebagai berikut:

$$Persentase\ kelayakan = \frac{Skor\ yang\ didapatkan}{Skor\ maksimal} \times 100\%$$

Setelah menghitung persentase dari skor yang diperoleh dalam pengujian, hasilnya akan dikonversi ke dalam pernyataan yang lebih spesifik sesuai dengan tabel persentase interval berikut: (Yusuf et al., 2021)

Tabel 3 Interval Persentase Kealayakan

No.	Persentase	Keterangan
1	0% - 25%	Sangat Tidak Layak
2	26% - 50%	Tidak Layak
3	51% - 75%	Layak
4	76% - 100%	Sangat Layak

Sumber : (Ernawati, 2017)

Maka hasil yang didapatkan dari perhitungan total skor tersebut adalah:

$$Persentase\ kelayakan = \frac{718}{810} \times 100\%$$
$$= 88\%$$

Berdasarkan perhitungan dengan teknik analisis data dan tabel persentase interval, implementasi sistem yang dilakukan dinilai sangat layak dengan skor persentase sebesar 88%.

4. KESIMPULAN

Berdasarkan hasil pengujian pada *router mikrotik* menggunakan metode *port scanning* pada jaringan SMK Kartika XX-2 Palopo, dapat disimpulkan beberapa kesimpulan diantaranya:

1. Dari hasil pengujian yang telah dilakukan menggunakan metode *port scanning* dan *port blocking* yang dapat digunakan bersama dengan firewall mikrotik untuk memberikan sistem keamanan jaringan dan melindungi router mikrotik dari port scanning dan blocking menggunakan aplikasi NMAP.
2. Dari hasil pengujian dapat melakukan pengiriman ke email dengan adanya serangan *port scanning* pada mikrotik.
3. Implementasi keamanan jaringan menggunakan metode port scanning dan port blocking dapat meminimalkan penyalahgunaan router oleh individu yang tidak bertanggung jawab..

5. SARAN

Adapun saran yang dapat dilakukan untuk penelitian berikutnya:

1. Banyak *software* sejenis yang dapat digunakan, mulai dari versi pro berbayar dan gratis dan berbagai metode, sehingga penelitian dapat memilih software sesuai kebutuhan.
2. Untuk penelitian berikutnya, pertimbangkan penggunaan sistem operasi selain Windows karena Nmap dapat berjalan pada berbagai platform.

6. DAFTAR PUSTAKA

Ernawati, I. (2017). Uji Kelayakan Media Pembelajaran Interaktif Pada Mata Pelajaran Administrasi Server. *Elinvo (Electronics, Informatics, and Vocational Education)*, *2*(2), 204–210. https://doi.org/10.21831/elinvo.v2i2.17315

Fergina, A., Setia, M. I., Yusuf, M., & ... (2023). Analisis Monitoring Sistem Keamanan Jaringan Komputer menggunakan Software NMAP (Studi Kasus Jaringan di Universitas Nusa Putra). *In Seminar Nasional Teknologi Informasi, Mekatronika, Dan Ilmu Komputer (SENTIMETER)*, *1*(1).

Lusi, D., & Suban Belutowe, Y. (2023). Analisis Dan Implementasi Desain Jaringan Hotspot Berbasis Mikrotik Menggunakan Metode Ndlc (Network Development Life Cycle) Pada Kantor Balai Pelaksanaan Jalan Nasional Ntt. *Jurnal Teknologi Informasi*, *7*(1).

Prayoga, R. A., & Mukmin, C. (2021). Analisis Peningkatan Jarak Jangkauan Signal Pada Jaringan Nirkabel SMK Muhammadiyah 2 Palembang. *Bina Darma Conference on Computer Science (BDCCS)*, *3*(2), 329–338.

Safitri, V. A., Sari, L., & Gamayuni, R. R. (2019). Research and Development, Environmental Investments, to Eco-Efficiency, and Firm Value. *The Indonesian Journal of Accounting Research*, *22*(03), 377–396. https://doi.org/10.33312/ijar.446

Yusuf, Z., Sarboini, & Ardiana, R. (2021). Pengaruh Pengembangan Sumber Daya Manusia Terhadap Kinerja Dosen dalam Meningkatkan Visi dan Misi Fakultas Ekonomi Universitas Serambi Mekkah. *JEMSI (Jurnal Ekonomi, Manajemen, Dan Akuntansi)*, *7*(2), 60–73. https://doi.org/10.35870/jemsi.v7i2.606