PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING*

TUGAS AKHIR

Disusun untuk Memenuhi Syarat Kelulusan Program Strata I
pada Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangkaraya

OLEH

NURUL ADITYA KURNIAWAN
C2155201054
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2026

PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING*

TUGAS AKHIR

Disusun untuk Memenuhi Syarat Kelulusan Program Strata I
pada Sekolah Tinggi Manajemen Informatika dan Komputer
(STMIK) Palangkaraya

OLEH

NURUL ADITYA KURNIAWAN
C2155201054
PROGRAM STUDI TEKNIK INFORMATIKA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
2026

PERSETUJUAN

PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING*

Tugas Akhir Ini Telah Disetujui dan Disahkan

Pembimbing I,	Pembimbing II,
Ir. Abdul Hadi, S.T., M.Kom.	H. Suratno, S.Kom., M.Si.
NIK. 198505102021101	NIK. 196912281997101

Mengetahui	Mengesahkan
Ketua STMIK Palangkaraya,	Ketua Prodi Teknik Informatika,
Ir. Mi. Sri Maryamah, M.M.	Ir. Abdul Hadi, S.T., M.Kom.
NIK. 196902021995004	NIK. 198505102021101

PENGESAHAN

PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING*

Tugas Akhir ini Telah Diujikan, Dinilai, dan Disahkan
Oleh Tim Penguji pada Tanggal 17 januari 2026

Tim Penguji Tugas Akhir :

1. Elia Zakharia, M.T.
   Ketua .....

2. Catharina Elmayantie, M.Pd.
   Sekretaris .....

3. Hotmian Sitohang, M.Kom.
   Anggota .....

4. Ir. Abdul Hadi, S.T., M.Kom.
   Anggota .....

5. H. Suratno, S.Kom., M.Si.
   Anggota .....

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini

Nama Mahasiswa **: NURUL ADITYA KURNIAWAN**

N I M **: C2155201054**

menyatakan bahwa Tugas Akhir dengan judul **:**

PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING*

Adalah hasil karya saya dan bukan merupakan duplikasi sebagian atau seluruhnya dari karya orang lain, kecuali bagian yang sumber informasi dicantumkan.

Pernyataan ini dibuat dengan sebenar-benarnya secara sadar dan bertanggungjawab dan saya bersedia menerima sanksi pembatalan Tugas Akhir apabila terbukti melakukan duplikasi terhadap Tugas Akhir atau karya ilmiah lain yang sudah ada.

Palangka Raya, 17 Januari 2026

Yang Membuat Pernyataan,



NURUL ADITYA KURNIAWAN

MOTTO DAN PERSEMBAHAN

- Usaha Hari Ini Akan Menentukan Kesuksesan di Masa Depan. Setiap Langkah yang Diambil Hari Ini Pun Akan Memberikan Dampak Signifikan dalam Mewujudkan Tujuan.
- Nilai Pendidikan dan Pengalaman Hidup Merupakan Modal Utama dalam Menghadapi Tantangan Kehidupan, Serta Membentuk Karakter yang Kuat dan Tangguh.
- Setiap Individu Memiliki Potensi untuk Mencapai Semua Impian dan Cita-Cita yang Diinginkan, Asalkan Memiliki Komitmen dan Usaha yang Kuat.

Tugas akhir ini saya persembahkan kepada:

- Allah SWT, Penolong di saat-saat sulit.
- Orang tua saya, atas dukungan dan motivasi yang tiada henti.
- Dosen-dosen di STMIK Palangkaraya, khususnya Ir. Abdul Hadi, S.T., M.Kom. dan H. Suratno, S.Kom., M.Si., yang telah memberikan bimbingan yang berarti selama penyusunan tugas akhir ini.
- Teman-teman, yang selalu memberikan semangat dalam perjalanan akademik.
- Semua pihak yang telah membantu, baik secara moril maupun materiil, dalam penelitian mengenai penerapan sistem keamanan pada perangkat absensi sidik jari berbasis web server.

INTISARI

Nurul Aditya Kurniawan, C2155201054, 2026. Penerapan Sistem Keamanan pada Perangkat Absensi Sidik Jari Berbasis *Web Server* Menggunakan Metode *Port Knocking*. Pembimbing I: Ir. Abdul Hadi, S.T., M.Kom; Pembimbing II: H. Suratno, S.Kom, M.Si.

Tugas akhir ini membahas penerapan sistem keamanan tambahan pada perangkat absensi sidik jari berbasis *web server* menggunakan metode *port knocking*. Sistem yang ada saat ini memiliki kerentanan karena bergantung pada langkah-langkah keamanan konvensional. Penelitian ini bertujuan menunjukkan bahwa metode *port knocking* dapat meningkatkan keamanan dengan meminimalkan risiko akses tidak sah.

Metode Eksperimen digunakan dalam penelitian ini untuk kinerja sistem keamanan sebelum dan sesudah penerapan. Data dikumpulkan melalui simulasi pengujian, yang menunjukkan penurunan jumlah akses tidak sah dan peningkatan tingkat keberhasilan akses.

Hasil penelitian menegaskan pentingnya langkah-langkah keamanan tambahan, seperti *port knocking*, dalam melindungi data biometrik. Keberhasilan sistem ini tidak hanya melindungi data pribadi tetapi juga meningkatkan kepercayaan pengguna, mendorong adopsi teknologi biometrik yang lebih luas di berbagai sektor. Penelitian ini memberikan rekomendasi untuk penggabungan metode lain guna memperkuat sistem keamanan secara keseluruhan.

Kata Kunci: Absensi Sidik Jari, Port Knocking, Keamanan, Web Server.

ABSTRACT

Nurul Aditya Kurniawan, C2155201054, 2026. Application of Security Systems on *Web Server*-Based Fingerprint Attendance Devices Using the *Port Knocking* Method. Advisor I: Ir. Abdul Hadi, S.T., M.Kom; Advisor II: H. Suratno, S.Kom, M.Si.

This final project discusses the implementation of an additional security system on web server-based fingerprint attendance devices using the port knocking method. Current systems have vulnerabilities, as they rely on conventional security measures. This research aims to demonstrate that the port knocking method can enhance security by minimizing the risk of unauthorized access.

An Experimental method was used in this study to analyze the performance of the security system before and after implementation. Data were collected through test simulations, revealing a decrease in the number of unauthorized accesses and an increase in the access success rate.

The research underscores the importance of additional security measures, such as port knocking, in protecting biometric data. The success of this system not only safeguards personal data but also increases user confidence, encouraging wider adoption of biometric technology across various sectors. This research recommends the incorporation of other methods to strengthen the overall security system.

Keywords: Fingerprint Attendance, Port Knocking, Security, Web Server.

KATA PENGANTAR

Alhamdulillah penulis panjatkan kehadirat Tuhan Yang Maha Esa, karena dengan karunia-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini yang berjudul "**PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS *WEB SERVER* MENGGUNAKAN METODE *PORT KNOCKING***". Tugas Akhir ini disusun untuk memenuhi syarat dalam memperoleh gelar Sarjana Komputer di Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya.

Pada kesempatan ini penulis juga menyampaikan terimakasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bimbingan, motivasi, semangat, dalam menyelesaikan penulisan Tugas Akhir ini, yaitu kepada :

1. Kombes Pol. I Wayan Korna, S.E., M.H. selaku Kepala BNN di Kota Palangkaraya yang mengijinkan untuk pengambilan data selama penulis melakukan penelitian.
2. Ir. Abdul Hadi, S.T., M.Kom, selaku dosen Pembimbing I yang telah meluangkan waktunya untuk memberikan bimbingan dalam penyelesaian Tugas Akhir ini.
3. H. Suratno, S.Kom., M.Si, selaku dosen Pembimbing II dalam penulisan Tugas Akhir ini, yang juga banyak memberikan saran dan masukan dalam penulisan Tugas Akhir ini.

Penulis mengharapkan masukan, saran dan kritik yang bersifat membangun untuk menyempurnakan Tugas Akhir ini. Semoga Tugas Akhir ini dapat bermanfaat bagi penulis dan pembaca terutama untuk untuk menambah ilmu pengetahuan.

Palangka Raya, Januari 2026

Penulis



NURUL ADITYA KURNIAWAN

DAFTAR ISI

PERSETUJUAN iii
PENGESAHAN iv
PERNYATAAN KEASLIAN v
MOTTO DAN PERSEMBAHAN vi
INTISARI vii
ABSTRACT viii
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR TABEL xi
DAFTAR GAMBAR xii
DAFTAR LAMPIRAN xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Perumusan Masalah 3
1.3 Batasan Masalah 4
1.4 Tujuan dan Manfaat 5
1.5 Sistematika Penulisan 6
BAB II LANDASAN TEORI 8
2.1 Kajian Teori 8
2.2 Penelitian Yang Relevan 27
BAB III METODE PENELITIAN 31
3.1 Tinjauan Umum 31
3.2 Jenis Penelitian 31
3.3 Desain Penelitian 32
3.4 Instrumen penelitian 34
3.5 Analisis Kebutuhan 35
3.6 Desain 36
BAB IV HASIL DAN PEMBAHASAN 40
4.1 Hasil 40
4.2 Pembahasan 69
BAB V KESIMPULAN DAN SARAN 74
5.1 Kesimpulan 74
5.2 Saran 75
DAFTAR PUSTAKA

DAFTAR TABEL

Tabel 2.1 Penelitian yang Relevan 27
Tabel 3.1 Kebutuhan Hardware 35
Tabel 3.2 Kebutuhan Software 36
Tabel 3.3 Kebutuhan Internet 36
Tabel 4.1 Daftar Port Scan Nmap Server Web Absensi 45
Tabel 4.2 Data Kuantitatif Waktu Respons dan Tingkat Keberhasilan Akses Sebelum dan Sesudah Implementasi..... 69

DAFTAR GAMBAR

Gambar 2.1 Internetworking 9
Gambar 3.1 Alur Penelitian..... 32
Gambar 3.2 Desain Perangkat Jaringan 37
Gambar 3.3 Desain Jaringan Logis..... 38
Gambar 4.1 Hasil pemindaian Penelusuran Alamat IP (Menggunakan Nmap).... 41
Gambar 4.2 Hasil Pemindaian Nmap yang Menunjukkan Status Port Terbuka ... 43
Gambar 4.3 Hasil Scan *Vulnerability* Nmap Server web Absensi 44
Gambar 4.4 Tampilan merubah User menjadi Administrator..... 46
Gambar 4.5 Proses Login ke Router MikroTik 48
Gambar 4.6 Tampilan menu Firewall pada router MikroTik. 48
Gambar 4.7 Screenshot dari tab Filter Rules dengan pengisian pengaturan rule baru 50
Gambar 4.8 Tampilan pengaturan rule baru dengan pengisian untuk Chain dan Action..... 51
Gambar 4.9 Screenshot dari tab General dan Action untuk pengaturan rule ICMP..... 53
Gambar 4.10 Tampilan akhir dari semua rule yang telah diatur, serta tombol 53
Gambar 4.11 Tampilan pengaturan firewall utama yang menunjukkan status dan opsi konfigurasi di MikroTik 55
Gambar 4.12 Ilustrasi yang menunjukkan URL di browser untuk mengakses halaman login dan halaman modifikasi. 56
Gambar 4.13 Jendela Run untuk Membuka Command Prompt. 57
Gambar 4.14 Hasil dari Perintah Ping ke Web Server Absensi 58
Gambar 4.15 Terminal MikroTik Menambahkan Alamat IP ke Address List..... 59
Gambar 4.16 Implementasi Port Knocking menggunakan Address List Ping Ke Web Server Absensi..... 60
Gambar 4.17 Tampilan Login akses Web Absensi 61
Gambar 4.18 Tampilan Data Registrasi Pegawai. 62
Gambar 4.19 Tampilan Login Normal..... 63
Gambar 4.20 Tampilan Login Secara Anomali..... 63
Gambar 4.21 Halaman Login Web Server Absensi Setelah Ketukan Berhasil..... 65
Gambar 4.22 Hasil Pemindaian Port Sebelum dan Sesudah Penerapan Port Knocking 66
Gambar 4.23 Address List Firewall Tercatat Ketukan Knock 67
Gambar 4.24 Hasil Pengujian Penerapan Port Knocking 68

DAFTAR LAMPIRAN

Lampiran 1. Surat Tugas Penguji Tugas Akhir
Lampiran 2. Surat Tugas pembimbing Tugas Akhir
Lampiran 3. Surat izin penelitian
Lampiran 3. Surat keterangan telah melakukan penelitian
Lampiran 5. Berita acara penilaian sidang TA
Lampiran 6. Lembar Kartu konsultasi bimbingan TA
Lampiran 7. Dokumentasi observasi di lokasi BNN Kota Palangkaraya
Lampiran 8. Tampilan Hasil Temuan Kerentanan Megunakan Nmap
Lampiran 9. Tampilan *Login* Normal Dan Anomali
Lampiran 10. Tampilan Browser HTTP URL Khusus Normal Dan Anomali
Lampiran 11. Tampilan Kondisi Normal Dan Kondisi Anomali

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan pesat teknologi informasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan, termasuk dalam manajemen kehadiran di BNN Kota Palangkaraya. Di era digital saat ini, sistem absensi berbasis sidik jari yang menggunakan *web server* muncul sebagai solusi praktis untuk meningkatkan efisiensi pengelolaan kehadiran pegawai. Sistem ini menawarkan keakuratan yang tinggi dan kemudahan akses, menjadikannya tulang punggung dalam operasional organisasi. Namun, tantangan besar terkait keamanan data mulai muncul, karena sistem absensi sidik jari berbasis *web server* menyimpan informasi sensitif.

Setiap celah dalam keamanannya berpotensi menimbulkan masalah serius, seperti pencurian data biometrik dan akses tidak sah (Kumar & Singh, 2020). Penelitian sebelumnya yang dilakukan oleh (Dendy Dwi Sukmana, 2025) dalam studi berjudul "Analisis Forensik Bukti Digital pada Kerentanan Keamanan Perangkat Absensi Sidik Jari Berbasis *Web Server*" menunjukkan adanya kerentanan pada perangkat absensi sidik jari berbasis web server yang perlu dicermati lebih lanjut.

Meskipun kemudahan dan efisiensi menjadi daya tarik utama teknologi ini, aspek keamanan data pegawai tetap menjadi isu krusial yang memerlukan perhatian mendalam, terutama dalam konteks penyimpanan informasi secara digital. Sistem keamanan yang tidak memadai dapat berakibat fatal, seperti pencurian data

biometrik dan informasi personal, serta akses tidak sah yang dapat mengganggu integritas data. Di tengah meningkatnya ancaman serangan siber yang semakin marak dan kompleks (Alghamdi et al., 2021), analisis kerentanan sistem di BNN Kota Palangkaraya yang mendalam serta perancangan langkah-langkah keamanan yang efektif menjadi sangat penting untuk melindungi data kehadiran pegawai.

Salah satu metode efektif yang dapat meningkatkan keamanan akses ke sistem adalah Teknik *port knocking*. Metode ini menyembunyikan port pada *server*, sehingga hanya pengguna yang mengetahui urutan paket yang tepat yang dapat membuka akses ke layanan tertentu (Kaur & Kumar, 2022).

Dengan *port knocking*, sistem memberikan lapisan tambahan dalam keamanan jaringan dengan cara meminimalisir kemungkinan serangan *brute force.* Dengan mengatur urutan *port knocking* yang spesifik, server hanya akan memberikan akses jika urutan tersebut diterima dalam waktu yang ditentukan (Rahman & Huda, 2021).

Dalam konteks perangkat absensi sidik jari, penerapan *port knocking* dapat melindungi data kehadiran yang tersimpan di server, memastikan bahwa hanya pengguna yang berwenang dan mengetahui sekuens rahasia yang dapat mengakses informasi sensitif tersebut (Patel & Jain, 2020), sehingga keamanan data lebih terjamin. Selain aspek teknis, penerapan sistem keamanan yang baik juga berperan dalam meningkatkan kepercayaan karyawan terhadap perusahaan. Karyawan cenderung lebih merasa aman dan nyaman dalam lingkungan kerja yang melindungi data pribadi mereka (Rahi et al., 2021).

Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis penerapan metode *port knocking* pada perangkat absensi sidik jari. Dengan melakukan studi kasus dan pengujian, diharapkan dapat ditemukan solusi yang efektif untuk meningkatkan keamanan sistem (Singh ***et al***., 2022).

Selain itu, pengembangan sistem ini akan mempertimbangkan pengalaman pengguna untuk memastikan bahwa mereka dapat mengakses sistem dengan mudah tanpa mengorbankan keamanan. Desain antarmuka yang intuitif dan instruksi yang jelas akan menjadi fokus utama dalam pengembangan (Lee & Park, 2021).

Berdasarkan permasalahan di atas maka penulis akan melakukan penelitian dengan judul **"*PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS WEB SERVER MENGGUNAKAN METODE PORT KNOCKING*"** Penelitian ini bertujuan untuk menganalisis dan menilai efektivitas metode *port knocking* dalam sistem keamanan perangkat absensi sidik jari berbasis *web server*, serta memberikan rekomendasi untuk meningkatkan perlindungan data pengguna.

1.2 Perumusan Masalah

Berdasarkan uraian latar belakang di atas dapat dipaparkan, rumusan masalah dalam penelitian ini adalah sebagai berikut: "Bagaimana cara menganalisis kerentanan keamanan jaringan pada perangkat absensi sidik jari berbasis *web server*? Bagaimana cara menerapkan metode *port knocking* untuk meningkatkan keamanan pengguna sistem perangkat absensi sidik jari?"

1.3 Batasan Masalah

Dalam penelitian ini, kami akan mengeksplorasi metode *port knocking* untuk meningkatkan keamanan perangkat absensi sidik jari berbasis *web server*. Fokus utama adalah melindungi data sensitif dan mencegah akses tidak sah, sehingga diharapkan dapat menambah lapisan keamanan jaringan dan menjaga integritas serta kerahasiaan data pengguna. Adapun batasan masalah yang dibuat peneliti sebagai berikut:

1. Penelitian ini hanya akan mengeksplorasi penerapan metode port knocking pada perangkat absensi sidik jari berbasis *web server*. Sistem absensi lain yang menggunakan metode identifikasi berbeda, seperti RFID atau *password*, serta platform *web server*, akan dibatasi pada satu atau dua jenis, seperti Apache atau Nginx, untuk menjaga konsistensi analisis.
2. Penelitian ini hanya akan menerapkan metode *port knocking* untuk mengamankan akses ke sistem absensi. Metode keamanan lain, seperti VPN, IDS, dan *firewall* konvensional, tidak akan dianalisis, dengan fokus utama pada efektivitas *port knocking* dalam meningkatkan keamanan akses pada perangkat absensi.
3. Pengujian dan implementasi sistem akan dilakukan dalam laboratorium terkontrol di BNN Kota Palangka Raya selama kurang lebih sekitar satu bulan. Penelitian ini tidak dilakukan dalam skala produksi untuk memastikan analisis yang lebih baik, dengan fokus pada router Mikrotik sebagai perangkat untuk mengamankan akses serta melindungi alamat IP dan *port server* sistem absensi sidik jari.

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

a. Tujuan

Tujuan penelitian ini adalah untuk menganalisis kerentanan keamanan jaringan perangkat absensi sidik jari berbasis *web server* serta, menerapkan Metode *Port Knocking* untuk meningkatkan keamanan pengguna sistem perangkat absensi sidik jari.

b. Manfaat

Manfaat yang diharapkan peneliti dari penelitian ini adalah sebagai berikut:

1) Bagi pengguna absensi sidik jari berbasis web server

Manfaat bagi pengguna Mencakup penguatan sistem perangkat absensi sidik jari, peningkatan keamanan jaringan mengurangi risiko serangan. Sistem ini juga menambah lapisan perlindungan akses data dan meningkatkan efektivitas pengelolaan jaringan dengan menerapkan metode *Port Knocking.*

2) Bagi Penulis

Manfaat bagi penulis adalah mengaplikasikan dan mengembangkan ilmu pengetahuan yang di dapat selama menempuh perkuliahan di STMIK Palangkaraya dan mengimplementasikannya di luar perkuliahan, serta sebagai syarat untuk kelulusan program Strata I pada STMIK Palangkaraya.

3) Bagi STMIK Palangkaraya

Sebagai bahan referensi, rujukan dan perbandingan bagi mahasiswa selanjutnya dan menambah koleksi ilmiah pada perpustakaan STMIK Palangkaraya.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dalam tugas akhir yang memuat gambaran umum serta uraian secara garis besar isi tugas akhir adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab I merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfaat yang diperoleh dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab II menguraikan tentang teori-teori dan memaparkan tentang tinjauan pustaka tentang penelitian yang relevan dan susunankajian teori yang telah disesuaikan dengan tema Tugas Akhir.

BAB III METODE PENELITIAN

Pada bab III membahas mengenai metode penelitian yang berisikan langkah-langkah dalam melakukan pengumpulan data yang dibutuhkan meliputi Gambaran Umum Jenis Penelitian, dan Desain Penelitian, Ananlisis Kebutuhan, Instrumen penelitian, Desain Jaringan dan Jadwal Penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan tentang hasil dari penelitian dan pembahasan dari hasil yang didapat.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan tentang kesimpulan dan saran yang diberikan untuk pengembangan selanjutny.

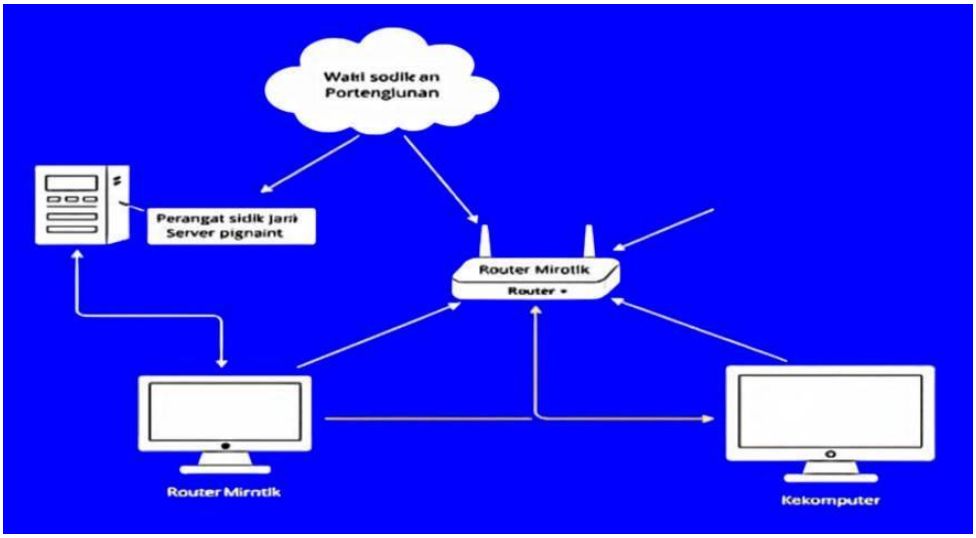
BAB II
LANDASAN TEORI

2.1 Kajian Teori

Dalam penelitian ini, kajian teori berfokus pada konsep dan prinsip dasar yang mendasari penerapan sistem keamanan pada perangkat absensi sidik jari berbasis *web server* dengan menggunakan metode *port knocking*. Beberapa aspek penting yang akan dibahas meliputi:

a. Keamanan Jaringan

Keamanan jaringan adalah disiplin penting dalam melindungi data dan sumber daya jaringan dari ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaan informasi data, yang penting untuk perangkat absensi sidik jari berbasis *web server*. Teknologi ini menawarkan akurasi tinggi dan mengurangi kecurangan absensi, tetapi juga meningkatkan risiko serangan siber. Metode *port knocking* dapat menambah lapisan keamanan dengan membuka port jaringan secara tersembunyi setelah urutan tertentu dilakukan, sehingga mengurangi akses tidak sah (Santoso, 2020; Setiawan, 2021; Nugroho, 2019). Berikut adalah Gambar 2.1 *Internetworking* antara beberapa sistem kontrol akses sidik jari berbasis *web server* berikut ini.



Gambar 2.1 *Internetworking*

Berdasarkan skala keamanan jaringan, sistem kontrol akses sidik jari dibagi menjadi lima jenis, yaitu *Local Area Network* (LAN), *Metropolitan Area Network* (MAN), *Wide Area Network* (WAN), jaringan berbasis *cloud,* dan jaringan *hybrid*. Setiap jenis jaringan memiliki karakteristik dan tantangan keamanan yang berbeda, yang mempengaruhi desain dan implementasi sistem kontrol akses.

Dalam konteks ini, sistem kontrol akses sidik jari berbasis *web server* sangat penting untuk memastikan bahwa data dan informasi sensitif dilindungi dari ancaman yang dapat merusak integritas dan kerahasiaan. Menurut penelitian sebelumnya (Pelealu *et al*., 2020), sistem ini terdiri dari beberapa perangkat yang bekerja sama untuk mencapai tujuan tertentu, termasuk pengelolaan akses dan perlindungan data.

b. *Firewall*

Menurut Adhi Prasetio dalam bukunya yang berjudul *Basic Concepts of E-Commerce, firewall* adalah perangkat atau sistem yang

berfungsi melindungi jaringan dari akses tidak sah dan serangan siber. *Firewall* dapat berupa perangkat keras (*hardware*) atau perangkat lunak (*software*) yang memantau dan mengendalikan lalu lintas data antara jaringan internal dan eksternal berdasarkan aturan keamanan tertentu.(Prasethio A, 2020).

Dalam konteks penerapan sistem keamanan pada perangkat absensi sidik jari berbasis *web server* menggunakan metode *port knocking* juga bagian, *firewall* memainkan peran penting dalam melindungi data biometrik dan autentikasi pengguna. Dengan menerapkan aturan akses yang ketat, *firewall* dapat mencegah berbagai ancaman, seperti serangan DDoS, pencurian data, dan akses tidak sah. Selain itu, firewall juga berfungsi untuk mendeteksi dan merespons ancaman secara *real-time*, sehingga meningkatkan keamanan keseluruhan sistem absensi. Implementasi firewall yang efektif sangat penting untuk menjaga kerahasiaan dan integritas data pengguna, serta memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem (Prasetio, 2020).

Intrusion Detection System (IDS) adalah sistem yang menganalisis lalu lintas jaringan atau aktivitas sistem untuk mendeteksi ancaman dalam keamanan jaringan. Penelitian ini mengeksplorasi efektivitas berbagai jenis *firewall* dalam melindungi jaringan dari serangan. Hasilnya menunjukkan bahwa *firewall* yang dikonfigurasi dengan baik dapat secara signifikan mengurangi risiko akses tidak sah (Nguyen *et al*., 2021).

Penelitian ini juga mengkaji integrasi *firewall* dengan sistem deteksi intrusi (IDS) untuk meningkatkan keamanan, menunjukkan bahwa kombinasi ini dapat meningkatkan kemampuan deteksi dan respons terhadap ancaman (Choudhury dan Dey, 2022).

Penelitian lainnya membahas penerapan *firewall* dalam lingkungan *cloud computing*, menunjukkan bahwa konfigurasi yang tepat dari *firewall* dapat melindungi data sensitif, termasuk data biometrik, dari akses yang tidak sah (Kaur *et al.*, 2023).

Dari penjelasan di atas, dapat disimpulkan bahwa *firewall* adalah komponen kritis dalam keamanan sistem absensi sidik jari berbasis *web server*. Dengan mengendalikan akses dan memantau lalu lintas, *firewall* membantu melindungi data biometrik dari ancaman. Penelitian terbaru menunjukkan bahwa penerapan firewall yang efektif, terutama dalam kombinasi dengan teknik lain seperti *port knocking*, dapat secara signifikan meningkatkan keamanan sistem dan melindungi informasi pengguna.

c. *Port Knocking*

Port knocking adalah metode keamanan yang digunakan untuk melindungi akses ke layanan jaringan dengan menyembunyikan port terbuka dari akses publik. Penerapan *port knocking* dapat meningkatkan keamanan sistem dengan mencegah akses tidak sah dan mengurangi risiko serangan. Dalam konteks sistem absensi sidik jari berbasis *web server*, metode ini berfungsi untuk melindungi data sensitif dengan cara menyembunyikan port layanan dari pemindai (Nuryakin Habillah, 2023).

Port knocking diterapkan dalam konfigurasi *firewal*l untuk meningkatkan keamanan akses ke layanan tertentu. Teknik ini menyembunyikan *port* yang terbuka, sehingga hanya pengguna yang mengetahui urutan " *Port knocking* " yang benar yang dapat mengakses *port* tersebut. Dengan demikian, pemindaian yang tidak sah dapat dihindari.

Metode ini memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses layanan tertentu dengan mengirimkan sinyal yang tepat. Dengan menerapkan teknologi ini, perangkat absensi sidik jari dapat meningkatkan keamanan, mengurangi risiko akses tidak sah, dan melindungi informasi biometrik pengguna.

Beberapa penelitian membahas penerapan *port knocking* dalam sistem absensi sidik jari berbasis *web*. Hasilnya menunjukkan bahwa penggunaan *port knocking* dapat meningkatkan keamanan data kehadiran dan sidik jari, dengan membatasi akses hanya kepada pengguna yang mengetahui urutan *port knocking* yang benar (Ahmad *et al*., 2021).

Metode ini tidak hanya menyembunyikan layanan, tetapi juga mengurangi serangan yang ditujukan langsung ke *port*. Keamanan Tambahan *Port* tidak terlihat oleh pemindai, sehingga menyulitkan penyerang untuk mengetahui layanan yang berjalan di *server*.

Penelitian ini mengeksplorasi integrasi *port knocking* dengan sistem *firewall* dan IDS untuk menciptakan pertahanan yang lebih komprehensif. Hasil penelitian menunjukkan bahwa kombinasi ini dapat

meningkatkan deteksi serangan dan respons sistem terhadap ancaman (Malik *et al*., 2022).

Penelitian ini juga mengkaji optimalisasi protokol *port knocking* dengan menerapkan teknik enkripsi untuk melindungi urutan *knocking* dari serangan, menunjukkan bahwa penggunaan enkripsi dapat meningkatkan keamanan secara signifikan dan mengurangi risiko serangan. Pengguna yang sah harus mengirimkan urutan paket yang tepat agar port dibuka (Zhang *et al*., 2023).

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa *port knocking* adalah metode keamanan jaringan yang efektif untuk melindungi data sensitif, terutama dalam sistem absensi sidik jari berbasis *web server*. Metode ini memungkinkan pengguna membuka akses ke *port* tertentu dengan mengirimkan urutan paket yang ditentukan, sehingga menyembunyikan *port* layanan dan mengurangi risiko akses tidak sah. Dengan demikian, *port knocking* memastikan hanya pengguna yang berwenang yang dapat mengakses data sensitif.

d. Topologi Jaringan

Topologi jaringan merujuk pada cara pengaturan dan penghubungan perangkat dalam suatu jaringan. Dalam konteks perangkat absensi sidik jari berbasis *web server*, pemilihan topologi yang tepat sangat penting untuk memastikan keamanan dan efisiensi komunikasi data. Dalam penelitian selama lima tahun terakhir, penerapan metode *port knocking* pada

perangkat absensi sidik jari berbasis *web server* menunjukkan hasil yang signifikan dalam meningkatkan keamanan jaringan.

Penelitian ini menekankan pentingnya pengaturan topologi jaringan yang tepat dalam penerapan *port knocking*. Topologi yang baik dapat membantu meminimalkan risiko serangan dan memastikan bahwa data yang ditransfer tetap aman (Smith *et al*., 2021).

Penelitian ini Penerapan *port knocking* terbukti menunjukkan bahwa penggunaan *port knocking* dapat meminimalkan risiko akses tidak sah. Metode ini bekerja dengan menyembunyikan *port* layanan, sehingga hanya pengguna yang mengetahui urutan '*knock*' yang benar yang dapat mengakses sistem (Junaidi dan Rahman, 2022).

Dalam studi ini, membuktikan efektivitas *port knocking* dalam mengurangi serangan *brute force*. Dengan menyembunyikan *port* dari pemindai, metode ini secara signifikan mengurangi kemungkinan serangan yang bertujuan untuk mendapatkan akses tidak sah (Chen dan Liu, 2023).

e. Keamanan Biometrik

Sistem keamanan biometrik mengandalkan karakteristik fisiologis atau perilaku unik individu, seperti sidik jari, pemindaian retina, atau pengenalan wajah, untuk melakukan autentikasi. Keunggulan utama sistem biometrik, khususnya yang menggunakan sidik jari, terletak pada kemampuannya dalam memberikan verifikasi identitas yang akurat dan menawarkan tingkat keamanan yang lebih tinggi dibandingkan kata sandi (Kumar & Singh, 2021). Data biometrik dianggap lebih aman karena

sifatnya yang inheren pada individu dan lebih sulit untuk dipalsukan atau direplikasi dibandingkan kata sandi, yang rentan terhadap serangan seperti phishing atau *brute-force* (Ahmed *et al*., 2022).

Penelitian ini mengemukakan bahwa biometrik lebih aman dibandingkan dengan kata sandi, karena data biometrik unik dan sulit untuk dipalsukan. Namun, tantangan tetap ada dalam hal perlindungan data biometrik. Dalam konteks ini, penerapan *port knocking* dapat memberikan solusi tambahan untuk melindungi data pengguna (Jain *et al*., 2018).

Meskipun demikian, tantangan signifikan tetap ada, terutama dalam hal perlindungan data biometrik itu sendiri. Jika data biometrik (misalnya, template sidik jari) berhasil dicuri atau dikompromikan, dampaknya bisa sangat merugikan karena karakteristik ini tidak dapat diubah semudah mengganti kata sandi (Ranjan & Verma, 2020). Perlindungan data biometrik menjadi isu utama meskipun sistem ini dapat meningkatkan keamanan secara keseluruhan (Wang *et al.*, 2021).

Penelitian ini juga mengatasi tantangan tersebut dan meningkatkan keamanan sistem yang mengelola data biometrik, penerapan lapisan keamanan tambahan menjadi krusial. Salah satu teknik yang dapat dipertimbangkan adalah *port knocking*. Mekanisme *port knocking* dapat menyembunyikan layanan di balik *port* yang awalnya tertutup, yang hanya akan terbuka setelah menerima urutan koneksi (knocks) tertentu yang benar, sehingga mempersulit akses tidak sah ke infrastruktur yang menyimpan data pengguna (Li & Wang, 2019).

Penelitian ini juga membahas tantangan keamanan dan privasi data biometrik, menunjukkan bahwa meskipun biometrik dapat meningkatkan keamanan, perlindungan data tetap menjadi isu utama (Wang *et al*., 2021).

Penelitian ini mengeksplorasi penerapan *port knocking* dalam sistem biometrik untuk meningkatkan keamanan, dengan temuan bahwa integrasi ini dapat mengurangi risiko akses tidak sah terhadap data biometrik (Kumar dan Singh, 2022). Lebih lanjut, Penelitian ini juga mengkaji mengenai penerapan teknik enkripsi pada data biometrik menunjukkan bahwa enkripsi, bersama dengan metode lain seperti *port knocking*, dapat memberikan perlindungan yang lebih komprehensif (Li *et al*., 2023).

1) Tingkat Keamanan Tinggi

Data biometrik sulit untuk dipalsukan atau dicuri dibandingkan dengan kata sandi. Penelitian oleh Jain et al. (2018) menunjukkan bahwa biometrik lebih aman karena data tersebut bersifat unik dan sangat sulit untuk ditiru.

2) Kenyamanan Pengguna

Pengguna tidak perlu mengingat informasi lain, cukup menggunakan biometrik mereka untuk autentikasi, sehingga meningkatkan pengalaman pengguna.

Berdasarkan beberapa definisi di atas, dapat disimpulkan bahwa Keamanan biometrik, khususnya yang memanfaatkan sidik jari, diakui menawarkan tingkat proteksi yang tinggi sekaligus kenyamanan operasional bagi pengguna.

Meskipun demikian, tantangan signifikan terkait perlindungan data pengguna tetap menjadi perhatian utama. Penerapan metode *port knocking* pada sistem absensi berbasis sidik jari diusulkan sebagai pendekatan untuk memperkuat keamanan data tersebut. Integrasi *port knocking* berpotensi menciptakan solusi yang lebih komprehensif dalam melindungi informasi biometrik sensitif, sebagaimana diindikasikan oleh berbagai penelitian terkini mengenai kombinasi teknik keamanan ini.

Dalam Studi yang dilakukan menunjukkan bahwa implementasi *port knocking* efektif dalam mengurangi serangan *brute force* melalui mekanisme penyembunyian *port* layanan dari jangkauan pemindai. Lebih lanjut, efektivitas *port knocking* dalam konteks sistem biometrik juga ditekankan oleh (Smith et al., 2021; Kumar & Singh, 2022)

Penelitian mereka secara spesifik menyoroti peningkatan keamanan pada sistem absensi, dengan hasil yang mengindikasikan penurunan signifikan insiden akses tidak sah dan pelanggaran terkait data biometrik (Junaidi dan Rahman 2022). Senada dengan temuan sebelumnya, dalam Penelitian ini menganalisis dampak *port knocking* terhadap keamanan data, mereka menyimpulkan bahwa metode *port knocking* ini memberikan kontribusi signifikan dalam membantu menjaga kerahasiaan informasi dan serta mengurangi risiko pencurian data pengguna (Chen dan Liu, 2023).

f. Keamanan Sistem

Menurut Kamus Besar Bahasa Indonesia (KBBI), keamanan diartikan sebagai "tidak adanya bahaya" atau "keadaan aman, tidak ada

ancaman atau gangguan". Keamanan sistem adalah aspek penting dalam melindungi data dan informasi yang dikelola oleh perangkat absensi sidik jari berbasis *web server*. Keamanan ini mencakup berbagai elemen, termasuk perlindungan terhadap akses yang tidak sah, integritas data, dan ketersediaan sistem.

Penelitian ini membahas praktik terbaik dalam keamanan sistem berbasis *web*, termasuk kontrol akses dan perlindungan data. Hasilnya menunjukkan bahwa sistem yang menerapkan teknik keamanan yang komprehensif dapat mengurangi risiko serangan (Zhang *et al*., 2021).

Penelitian ini mengeksplorasi penerapan *port knocking* dalam meningkatkan keamanan sistem, dengan temuan bahwa metode ini secara signifikan mengurangi kebocoran data dan meningkatkan kontrol akses (Patel dan Kumar, 2022).

Penelitian ini juga mengkaji berbagai jenis serangan siber dan metode perlindungan yang efektif, menunjukkan bahwa kombinasi teknik, termasuk *port knocking* dan enkripsi, dapat meningkatkan ketahanan sistem terhadap serangan (Ali *et al*., 2023).

Sistem Keamanan memiliki Tiga parameter keamanan yang sangat penting, yaitu:

1) Kontrol Akses

Sistem harus memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses data dan fungsi tertentu. Metode *port knocking*

membantu menyembunyikan port layanan, sehingga mengurangi risiko akses tidak sah.

2) Integritas Data

Perlindungan terhadap modifikasi data yang tidak sah sangat penting. Sistem harus menerapkan mekanisme untuk mendeteksi dan mencegah perubahan data yang tidak diizinkan.

3) Ketersediaan Sistem

Sistem harus selalu tersedia untuk pengguna yang sah. Ini mencakup perlindungan terhadap serangan *Denial-of-Service* (DoS) atau *Distributed Denial-of-Service* (DDoS) yang dapat mengganggu akses ke layanan.

Berdasarkan beberapa definisi di atas, dapat disimpulkan bahwa keamanan sistem adalah aspek krusial dalam perlindungan perangkat absensi sidik jari berbasis *web server*. Dengan menerapkan metode *port knocking*, sistem dapat meningkatkan kontrol akses, integritas data, dan ketersediaan layanan. Penelitian terbaru menunjukkan bahwa kombinasi teknik keamanan yang tepat dapat secara signifikan mengurangi risiko serangan dan melindungi data pengguna.

g. Vulnerability Assessment

Vulnerability Assessment adalah fase pendekatan untuk mengidentifikasi kerentanan yang ada dalam infrastruktur (Kumar, 2018). Proses ini sangat penting untuk memastikan bahwa sistem keamanan dapat berfungsi dengan baik. Menurut GOV-CSIRT Indonesia (Government

Computer Security Incident Response Team) pada tahun 2021, kerentanan dibagi menjadi tiga kategori penilaian, yaitu:

1) **High Level (Tinggi)**

   Teridentifikasi kelemahan dengan potensi dampak yang tinggi dan kemungkinan eksploitasi yang signifikan, sehingga dapat berkembang menjadi ancaman serius. Fitur atau langkah-langkah pencegahan serta penanganan yang ada seringkali dinilai tidak memadai, sehingga ,kerentanan pada level ini memerlukan perhatian dan tindakan mitigasi risiko dengan segera.

2) **Medium Level (Sedang)**

   Kelemahan pada tingkat ini umumnya bersifat lebih terlokalisasi atau memiliki dampak yang lebih terbatas dibandingkan high level. Meskipun upaya penanganan dan pencegahannya mungkin juga bersifat lokal, kelemahan ini tetap membutuhkan perhatian agar tidak dieksploitasi atau berkembang menjadi ancaman yang lebih besar di kemudian hari.

3) **Low Level (Rendah)**

   Kelemahan yang tergolong dalam kategori ini memiliki potensi dampak dan kemungkinan eksploitasi yang rendah. Upaya pencegahan serta penanganan yang ada biasanya dianggap sudah memadai, Meskipun demikian, pemantauan berkala tetap direkomendasikan untuk mencegah munculnya potensi kerentanan baru di masa depan atau eskalasi risiko dari kerentanan yang sudah ada.

h. *Hardening*

Hardening sistem adalah teknik yang digunakan untuk memperkuat keamanan perangkat dan aplikasi guna melindungi dari berbagai ancaman dan serangan. Dalam konteks perangkat absensi sidik jari berbasis *web server*, proses *hardening* sangat penting untuk menjaga data sensitif dan mencegah akses tidak sah. Sebuah penelitian mengeksplorasi efektivitas metode *port knocking* dalam meningkatkan keamanan *web server,* khususnya untuk aplikasi yang menggunakan data biometrik seperti sidik jari telah implementasi dan efektivitas teknik *hardening*, termasuk *port knockin* (S. K. Patel *et al*. 2021).

Penelitian ini menunjukkan bahwa penerapan *port knocking* dapat secara signifikan mengurangi risiko serangan dari pemindai otomatis dan serangan *brute force*. Mekanisme ini bekerja dengan menjaga *Port* layanan tetap tersembunyi hingga pengguna yang berwenang mengirimkan urutan paket yang tepat (packet sequence) yang telah ditentukan sebelumnya (Smith *et al*., 2021).

Penelitian ini menerapkan *port knocking* pada sistem absensi sidik jari, dengan hasil menunjukkan bahwa metode ini peningkatan signifikan dalam keamanan akses serta perlindungan data sensitif, memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem (Junaidi dan Rahman, 2022).

Penelitian ini menganalisis efektivitas *port knocking* dalam aplikasi web. Meskipun studi mereka mencatat adanya sedikit penurunan dalam

kecepatan akses sebagai konsekuensi dari lapisan keamanan tambahan, penerapan *port knocking* terbukti secara substansial meningkatkan tingkat keamanan secara keseluruhan, sebuah aspek yang sangat penting untuk sistem yang menangani informasi sensitif (Chen dan Liu, 2023).

Tujuan utama dari *hardening* sistem adalah untuk mengurangi atau menghilangkan risiko ancaman yang dapat terjadi pada sistem komputer. Hal ini seringkali dicapai melalui berbagai tindakan, seperti menonaktifkan layanan yang tidak perlu, menghapus program atau file yang tidak esensial, serta menutup *port-port* jaringan (TCP/UDP) yang tidak digunakan dan berpotensi menjadi celah keamanan.

i. Access point

Menurut Suprapto dalam bukunya yang berjudul "Komputer dan Jaringan Dasar untuk *SMK/MAK Kelas X*", *Wireless Access Point* (WAP) atau biasa disebut *access point* adalah perangkat yang memungkinkan perangkat nirkabel terhubung ke perangkat kabel melalui teknologi yang disebut Wi-Fi (*Wireless Fidelity*). *Access point* biasanya terhubung ke perangkat router yang berdiri sendiri. Namun, saat ini sebagian besar *access point* sudah dilengkapi dengan perangkat router di dalamnya (Suprapto, 2020).

Menurut Adhiatma dalam bukunya "*New CCNA 200-301 Part 1 – Network Fundamentals*", mendefinisikan *access point* sebagai salah satu komponen esensial dalam infrastruktur jaringan nirkabel. Perangkat seperti notebook atau PC dapat terkoneksi ke jaringan melalui *Wi-Fi* dengan perantaraan *access point*. Penggunaan *access point* menyederhanakan

pengelolaan jaringan area lokal (*Local Area Network* - LAN), sehingga dalam satu ruang kerja tidak perlu menarik banyak kabel. Perangkat access point banyak digunakan di ruang publik, seperti kafe, bandara, dan mol pusat perbelanjaan (Adhiatma, 2020).

Penelitian ini mengoptimalkan jaringan *Wi-Fi* untuk sistem absensi biometrik, fokus pada pengaturan konfigurasi *access point* dan protokol keamanan (Kurniawan, D., 2023). Dalam konteks "*Penerapan Sistem Keamanan pada Perangkat Absensi Sidik Jari Berbasis Web Server Menggunakan* Metode *Port Knocking*," pemahaman tentang *access point* pemahaman mendalam mengenai *access point* menjadi relevan. penting karena meskipun *access point* mendukung konektivitas nirkabel yang praktis penggunaannya, di ruang publik meningkatkan risiko keamanan. Oleh karena itu, penerapan metode keamanan tambahan seperti *port knocking* diperlukan untuk melindungi perangkat dan data sensitif dari akses tidak sah.

j. NAT

Network Address Translation (NAT) adalah teknik yang digunakan untuk memetakan satu alamat IP (*Internet Protocol*) publik ke beberapa alamat IP privat. Teknik ini tidak hanya berfungsi untuk mengkonservasi menghemat penggunaan alamat IP publik sekaligus yang terbatas tetapi juga memberikan lapisan keamanan tambahan dengan menyembunyikan struktur jaringan internal. Dalam konteks perangkat sidik jari berbasis *web server*, penerapan NAT membantu menyembunyikan alamat IP internal dari dunia luar, sehingga mengurangi risiko serangan langsung terhadap perangkat

tersebut. Dengan menggunakan NAT, hanya satu alamat IP publik yang terlihat di internet, yang memungkinkan administrator jaringan untuk mengontrol dan memfilter akses ke jaringan internal. Teknik ini juga efektif dalam mencegah serangan seperti pemindaian *port* (*port scanning*) dan serangan DDoS (*Distributed Denial of Service*), yang biasanya ditargetkan pada alamat IP yang dapat diakses secara langsung.

Metode *Port Knocking* berfungsi sebagai lapisan keamanan tambahan yang membuka akses ke *server* hanya setelah urutan tertentu dari "ketukan" pada *port* yang telah ditentukan. Ketika dikombinasikan dengan NAT, *port knocking* memastikan bahwa hanya pengguna yang terautentikasi yang dapat mengakses perangkat sidik jari. Jika ada upaya akses yang tidak sah, NAT dapat membantu mendeteksi dan menutup akses dari alamat IP yang mencurigakan, yang pada gilirannya meningkatkan keamanan secara keseluruhan.

Penerapan gabungan antara NAT dan metode *port knocking* pada perangkat sidik jari berbasis *web server* menawarkan solusi memberikan perlindungan yang lebih komprehensif dengan menyembunyikan alamat IP internal, mencegah serangan langsung, dan memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem. Integritas dan keamanan data sensitif yang dikelola oleh sistem absensi menjadi lebih terjaga melalui implementasi lapisan keamanan sistem absensi berlapis ini (Mokhtar, 2016; Rahman & Jamil, 2018; Sari & Prabowo, 2020).

k. Nmap

Nmap *(Network Mapper)* adalah perangkat lunak yang masih populer digunakan. Nmap digunakan untuk *scanning port* dan memonitoring jaringan komputer. Nmap dirancang agar dapat menciptakan monitoring jaringan dengan lingkup yang jauh, juga dapat digunakan untuk melakukan *scanning port. Tools* Nmap bekerja dengan cara melihat alamat IP untuk mengetahui jumlah *host* yang sedang aktif dalam jaringan, *port* yang terbuka, OS yang digunakan, *firewall* yang di pakai. Nmapakan mengetahui sebuah celah yangada dalam jaringan yang memiliki tingkat keamanan rendah sehingga dapat berpotensi untuk dilakukan penyusupan (Fahlevi & Putri, 2021).

l. *Winbox*

Winbox adalah sebuah utilitas perangkat lunak (*software utility*) yang digunakan untuk meremote *server* dikembangkan oleh Mikrotik, dirancang khusus untuk administrasi dan konfigurasi perangkat *RouterOS* MikroTik melalui antarmuka pengguna grafis (*Graphical User Interface - GUI*). Aplikasi ini umumnya digunakan pada sistem operasi Windows dan memungkinkan administrator jaringan untuk melakukan manajemen perangkat dari jarak jauh (*remote*) dengan cara yang lebih intuitif dibandingkan antarmuka baris perintah (*Command Line Interface - CLI*) (Daulay, 2020).

Penelitian sebelumnya menunjukkan bahwa penerapan metode *port knocking* dapat secara signifikan mengurangi risiko serangan *brute force*

dengan menyembunyikan *port* layanan dari pemindaian publik. (Smith *et al*., 2021). Lebih lanjut, dalam konteks penelitian ini, mengaplikasikan *port knocking* diterapkan pada perangkat sistem absensi sidik jari dan menemukan adanya peningkatan keamanan akses data dari pengguna yang tidak berwenang. (Junaidi dan Rahman, 2022). Analisis kinerja *port knocking* dalam penelitian juga menunjukkan mengkonfirmasi bahwa meskipun mungkin terdapat sedikit latensi tambahan, peningkatan tingkat keamanan yang ditawarkan oleh *port knocking* sangat berharga, terutama untuk sistem yang menangani informasi sensitif. (Chen dan Liu, 2023).

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa *Winbox* adalah merupakan utilitas perangkat lunak yang esensial untuk konektivitas dan konfigurasi perangkat MikroTik, memanfaatkan alamat *MAC* atau *protokol IP*. Fungsi utamanya adalah sebagai alat yang menyederhanakan akses dan manajemen perangkat MikroTik bagi pengguna. Meskipun *Winbox* sendiri adalah alat konfigurasi, pemahaman akan pentingnya pengamanan akses ke perangkat jaringan seperti yang dapat ditingkatkan melalui metode *port knocking* menjadi relevan. Oleh karena itu, penerapan *port knocking* pada sistem keamanan perangkat absensi sidik jari, yang mungkin berada dalam infrastruktur jaringan yang sama atau dikelola dengan prinsip serupa, dapat secara signifikan memperkuat pertahanan terhadap akses tidak sah.

m. SQL Injection

SQL injection dapat menyebabkan kerugian finansial yang signifikan dan kerusakan reputasi bagi organisasi. Serangan ini bisa mengakibatkan pencurian data pengguna, penghapusan informasi penting, dan bahkan kontrol penuh atas *server* oleh penyerang (Halfond, W. G. J., et al. 2006).

2.2 Penelitian Yang Relevan

Penelitian yang relevan merupakan kajian yang berisi uraian sistematis tentang informasi penelitian orang lain yang disajikan dalam bentuk pustaka yang dikaitkan dengan masalah penelitian yang sedang diteliti. Ini memaparkan ringkasan hasil penelitian yang relevan yang mendukung judul, dengan fakta-fakta yang dikemukakan sejauh mungkin yang tetap mengacu pada sumber aslinya.

Berikut ini adalah beberapa contoh penelitian terdahulu yang dapat digunakan sebagai bahan acuan pendukung judul serta fakta-fakta terkait pada pembahasan penelitian ini yang telah berhasil dihimpun oleh penulis dapat dilihat pada Tabel 2.1 Penelitian yang Relevan berikut ini.

Tabel 2.1 Penelitian yang Relevan

No	Penulis / Tahun	judul Penelitian	Metode	Pembahasan	Hasil	Perbedaan
1.	Randi Rizal, Ruuhwan, Kelvin Ajie Nugraha (2020)	Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941	Port Blocking, Port Knocking	Menjelaskan penerapan port blocking dan port knocking pada keamanan jaringan menggunakan Mikrotik RB-941 untuk meningkatkan keamanan jaringan lokal.	menunjukkan Keamanan port Winbox dan WWW pada Mikrotik efektif mengamankan port layanan seperti Winbox dan WWW pada router Mikrotik berbasis port.	Perbedaan terletak pada penelitian sebelumnya pada Menggabungkan dengan Port blocking bersifat permanen, Port Knocking ke efektifan berbasis port.
2.	Ismanto, Aristejo (2021)	Optimalisasi Keamanan Jaringan Menggunakan Metode Port Knocking Pada LAZIS Wahdah Jakarta.	Port Knocking pada Mikrotik	Menyelesaikan masalah keamanan jaringan pada LAZIS Wahdah dengan menggunakan Mikrotik dan metode Port Knocking untuk mengamankan port yang terbuka.	Hasil pengujian menunjukkan bahwa Mikrotik berfungsi sebagai gateway dan Port Knocking berhasil mengamankan akses jaringan.	Perbedaan terletak pada Penelitian ini fokus pada Port Knocking, sementara firewall hanya menutup port tanpa hak akses pengguna.

No	Penulis / Tahun	judul Penelitian	Metode	Pembahasan	Hasil	Perbedaan
3.	Intan Putri Ayu Agita, Sopian Soim (2023)	Implementasi Port Knocking, Port Blocking Pada Keamanan Jaringan Komputer Berbasis Mikrotik	Port Knocking, Port Blocking	Penelitian ini menguji efektivitas metode port knocking dan port blocking untuk melindungi jaringan dari serangan dan akses tidak sah.	autentikasi pada port tertentu, dan beberapa port ditutup untuk mencegah akses dari pihak yang tidak sah. Kombinasi kedua metode membuat serangan lebih sulit.	Perbedaan terletak pada penelitian sebelumnya Fokus pada pengamanan port membuat serangan lebih sulit menggunakan salah satu metode, sedangkan penelitian ini menggabungkan port knocking dan port blocking.
4.	Ade Eksan Nuryakin Habillah, Sidik (2023)	Implementasi Keamanan Jaringan Metode Port Knocking dan Port Blocking Berbasis Mikrotik PT Securindo Packatama Indonesia	Metode Port Knocking dan Port Blocking pada Mikrotik	Penelitian ini menerapkan metode Port Knocking dan Port Blocking di Mikrotik untuk meningkatkan keamanan jaringan komputer di PT Securindo Packatama Indonesia. Fokus pada mencegah akses tidak sah dengan filter pada port.	Penutupan port yang tidak sah, hanya memungkinkan akses pada port yang telah dikonfigurasi oleh sistem port knocking yang sah.	Perbedaan terletak pada Penelitian sebelumnya ini fokus pada implementasi port knocking dan port blocking pada Mikrotik, berbeda dari penelitian lain yang lebih umum tanpa penutupan port spesifik.

No	Penulis / Tahun	judul Penelitian	Metode	Pembahasan	Hasil	Perbedaan
5.	Fauzan Prasetyo Eka Putra, dkk (2023)	Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking	Literature Review, Seleksi Studi	Penelitian ini membahas penerapan firewall filtering dan port knocking untuk meningkatkan keamanan jaringan Mikrotik.	Firewall filtering dan port knocking efektif dalam memblokir serangan dan meningkatkan keamanan jaringan.	Perbedaannya, penelitian ebelumnyaini membandingkan firewall filtering dan port knocking dengan pendekatan tradisional yang hanya mengandalkan firewall. tanpa mempertimbangkan port knocking.

BAB III
METODE PENELITIAN

3.1 Tinjauan Umum

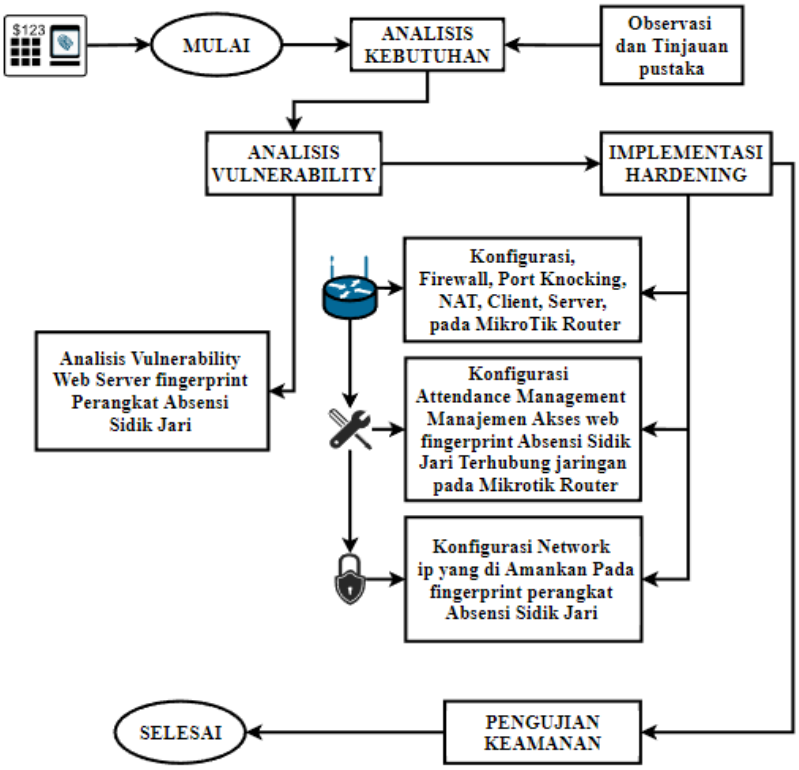
Penelitian ini dilaksanakan selama kurang lebih sekitar satu bulan di BNN Kota Palangka Raya, Jl. Tangkasiang No. 12, sebagai lokasi pengujian keamanan jaringan absensi sidik jari. Tujuannya adalah menganalisis dan meningkatkan keamanan akses pada IP *port server* perangkat absensi sidik jari berbasis *web server* menggunakan metode *port knocking* pada router Mikrotik. Diharapkan, penambahan lapisan proteksi dapat memperkuat keamanan data dan autentikasi pengguna. Fokus utama penelitian adalah mengevaluasi efektivitas metode *port knocking* dalam meningkatkan keamanan dan autentikasi sistem absensi tersebut.

3.2 Jenis Penelitian

Penelitian ini menggunakan metode eksperimen untuk penerapan sistem keamanan pada perangkat absensi sidik jari berbasis *web server* dengan metode *port knocking*. Fokusnya adalah mengumpulkan data terukur mengenai kinerja keamanan sistem sebelum dan sesudah implementasi. Selain itu, penelitian juga mengkaji pengalaman dan perspektif pengguna serta pengembang terkait efektivitas dan tantangan dalam implementasi sistem keamanan. Ciri-ciri penelitian eksperimen meliputi adanya perlakuan yang diberikan pada objek sasaran, pengamatan dan analisis terhadap dampak perlakuan, pengumpulan data deskriptif, serta fokus pada konteks penerapan.

3.3 Desain Penelitian

Desain penelitian ini diperlukan agar pelaksanaan penelitian dapat berjalan sesuai rencana dan menghasilkan hasil yang efektif serta efisien. Desain penelitian mencakup perancangan sistem, pengembangan prototipe, dan pengujian sistem. Struktur perancangan sistem keamanan berbasis metode *port knocking*, yang melibatkan pengguna yang relevan, divisualisasikan pada Gambar 3.1. Desain Penelitian, Gambar ini menunjukkan perancangan sistem keamanan dengan struktur autentikasi yang kuat.



Gambar 3.1 Desain Penelitian

1) Analisis Kebutuhan

Langkah awal penelitian ini adalah menganalisis kebutuhan untuk mengidentifikasi komponen dan fitur penting sistem keamanan perangkat absensi sidik jari. Proses analisis dilakukan melalui observasi dan tinjauan

pustaka untuk memahami persyaratan sistem. Fokus penelitian adalah pada aspek yang relevan dengan judul penelitian "*Penerapan Sistem Keamanan Pada Perangkat Absensi Sidik Jari Berbasis Web Server Menggunakan Metode Port Knocking*," dengan harapan dapat memberikan kontribusi signifikan terhadap pengembangan sistem keamanan yang lebih tangguh dan efektif.

2) Analisis *Vulnerability*

Penelitian ini menganalisis kerentanan pada sistem absensi sidik jari dan aplikasi manajemen kehadiran. Proses Simulasi menggunakan *vulnerability scanners* untuk mendeteksi vulnerabilities pada perangkat keras (*hardware*) seperti router MikroTik dan *access point*, serta perangkat lunak (*software*) termasuk aplikasi berbasis *web* dan *Synology Drive Client*. Analisis ini mengidentifikasi kelemahan konfigurasi dan celah keamanan, dengan harapan menemukan titik lemah yang perlu dimitigasi untuk mencegah eksploitasi dan penyalahgunaan sistem.

3) Implementasi *Hardening*

Setelah analisis kerentanan, tahap selanjutnya adalah menerapkan *hardening*. Tindakan ini meliputi modifikasi konfigurasi perangkat, instalasi perangkat lunak tambahan (*firewall*), *Intrusion Detection System* (IDS), Intrusion Prevention System (IPS), dan pengaturan *server* aplikasi absensi misalnya, *Attendance Management*. *Access point* harus diamankan dengan alamat IP statis, subnet terpisah, dan enkripsi WPA3 untuk mencegah akses nirkabel yang tidak sah.

4) Pengujian Keamanan

Pada Tahap akhir penelitian ini adalah pengujian keamanan untuk menilai efektivitas sistem setelah penerapan *hardening* dan *port knocking*. Pengujian melibatkan simulasi serangan, termasuk *Denial-of-Service* (DoS) dan akses tidak sah, menggunakan teknik penetration testing. Tujuannya adalah mengevaluasi kemampuan sistem absensi berbasis sidik jari dalam melindungi data dan mengukur peningkatan keamanan.

3.4 Instrumen penelitian

Adapun dalam penelitian ini, penulis melakukan pengumpulan data yang digunakan untuk menunjang penelitian, serta melakukan instalasi dan konfigurasi sistem yang telah dirancang. Terdapat beberapa prosedur dalam pengumpulan data, yaitu:

a) Observasi (Pengamatan)

Penulis melakukan pengamatan langsung di lokasi penelitian, yaitu BNN Kota Palangka Raya untuk memahami pengalaman pengguna dan pengembang terkait efektivitas serta tantangan implementasi sistem keamanan. Pengamatan ini juga mencakup kondisi fisik jaringan dan interaksi pengguna dengan perangkat absensi sidik jari.

b) Penelitian Kepustakaan (Library Research)

Penulis memanfaatkan sumber referensi dari perpustakaan, buku, prosiding, dan jurnal. Penelitian ini dilakukan untuk mengumpulkan informasi teoritis serta studi sebelumnya yang berkaitan dengan sistem

keamanan, teknologi biometrik, dan metode *port knocking*, guna menentukan parameter yang akan digunakan dalam penelitian.

3.5 Analisis Kebutuhan

Analisis kebutuhan adalah menjelaskan rincian data yang diperlukan untuk penelitian tentang *"Penerapan sistem keamanan pada perangkat absensi sidik jari berbasis web server menggunakan metode port knocking.* Data untuk pengembangan keamanan jaringan diperoleh melalui scanning sistem di lokasi penelitian. Hasilnya akan didapat setelah melewati beberapa tahapan dengan variabel yang telah ditentukan, sehingga identifikasi dalam analisis kerentanan (*vulnerability*) dan metode penguatan (*hardening*) dapat dilakukan dengan lebih akurat. Dalam penelitian ini, spesifikasi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan sebagai alat bantu dapat dilihat pada Tabel 3.1 Kebutuhan *Hardware* berikut.

Tabel 3. 1 Kebutuhan *Hardware*

No	Hardware	Spesifikasi
1	Laptop ACER Aspire A515-45 Ryzen 5 5500U	Prosesor : AMD Ryzen 5 5500U with Radeon Graphics 2.10 GHz Ram : 8,00 GB (7,35 GB usable) Storage : 512 GB SSD VGA : DESKTOP-64PR39C
2	Router Mikrotik RB 951	Prosesor : QCA9531-BL3A-R 650MHz Ram : 64MB Storage : 16MB
3	ZTE Modem Rauter	Chipset : Qualcomm Antena : 6 buah antenna 5dBi
4	Perangkat Mesin Absensi Sidik Jari	Resolusi: 500 DPI Kapasitas Penyimpanan: 3.000 sidik jari dan SDK Available transaksi Koneksi: RS232,RS485,TCP/IP, USB, Wi-Fi (opsional)

Tabel 3. 2 Kebutuhan *Software*

No	**Software**	**Keterangan**
1	Windows 10 Version 22H2	Windows 10 Home Single Language sebagai sistem operasi laptop
2	Winbox Versi 3.37	Winbox sebagai pendukung konfigurasi mikrotik yang memiliki GUI untuk mempermudah konfigurasi.
3	Attendance Management web browser untuk mengakses perangkat Absenasi Sidik jari	Attendance Management yang bertujuan untuk mengelola dan mencatat kehadiran karyawan atau siswa secara efisien dengan tambahan lapisan keamanan.

Tabel 3. 3 Kebutuhan Internet

Nama Provider	**Kecepatan**
Indihome	20Mbps

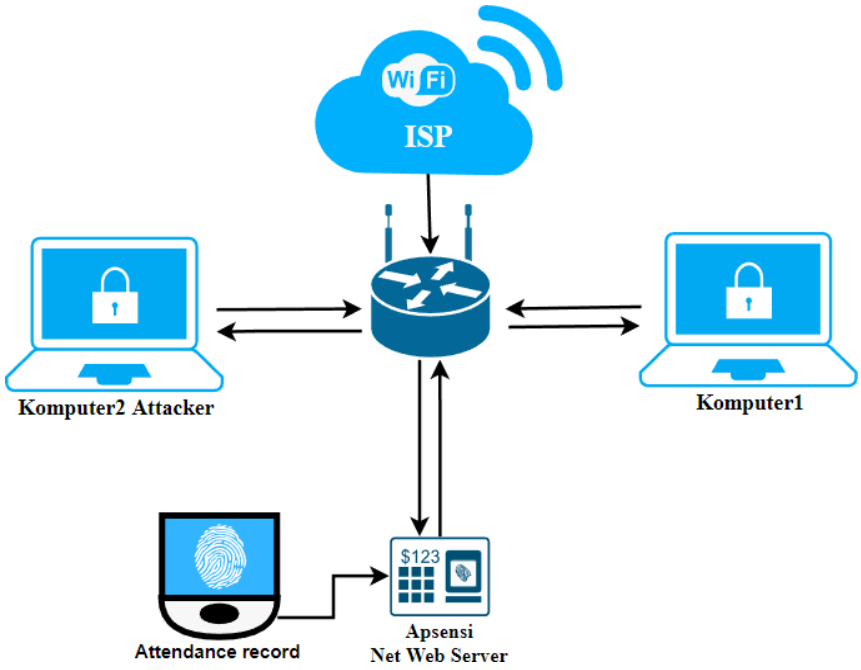
3.6 Desain

3.6.1 Sebelum Perancangan Jaringan

1) Desain Perangkat Jaringan

Desain sebelum penerapan perangkat jaringan Router MikroTik untuk sistem keamanan perangkat absensi sidik jari berbasis *web server* dalam penelitian berjudul "*Penerapan Sistem Keamanan pada Perangkat Absensi Sidik Jari Berbasis Web Server Menggunakan Metode Port Knocking*" mencakup pemilihan perangkat yang tepat untuk mendukung keamanan dan efisiensi sistem. Aplikasi *Draw.io* digunakan untuk memvisualisasikan langkah-langkah desain secara sistematis, di mana setiap tahap digambarkan dalam kotak yang terhubung melalui garis atau

panah. Hal ini memudahkan pemahaman mengenai alur dan hubungan antar perangkat dalam penerapan sistem keamanan.

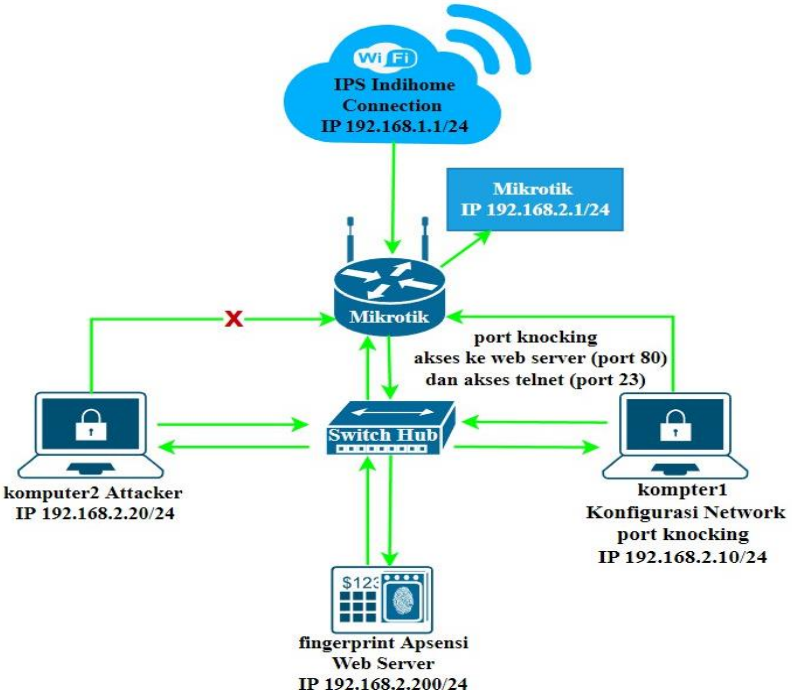


Gambar 3.2 Desain Perangkat Jaringan

3.6.2 Sesudah Perancangan Jaringan

2) Desain Jaringan *Logis*

Keamanan dalam desain sistem ini bertujuan melindungi *server*, termasuk layanan file *server*, dari serangan yang memanfaatkan celah pada *port*. Skema ini menerapkan beberapa lapisan keamanan, yaitu penonaktifan *port, port knocking* dengan aturan TCP/IP, dan pemfilteran *firewall*. Lapisan sistem keamanan ini menawarkan layanan seperti identifikasi absensi sidik jari, pemblokiran IP, dan deteksi penyerang. Akses *server* hanya diberikan kepada komputer admin. Selain itu, *port knocking* digunakan untuk mengatur akses ke *web server* dan layanan lainnya.



Gambar 3.3 Desain Jaringan *Logis*

Desain jaringan ini sesudah menggunakan Router MikroTik RB951 dengan 10 *port* yang terhubung ke ISP Indihome dengan IP 192.168.1.1/24. Router MikroTik ini memiliki IP 192.168.2.1/24 untuk menghubungkan perangkat dalam jaringan. Router terhubung ke *switch hub* dan perangkat absensi sidik jari dengan IP 192.168.2.100/24. Komputer1 memiliki IP 192.168.2.10/24, sedangkan komputer2 (*attacker*) yang sebagai penyerang menggunakan IP 192.168.2.20/24. Router MikroTik mengatur NAT untuk akses ke layanan telnet (*port* 23) dan web *server* (*port* 80), serta menerapkan *port knocking* untuk melindungi akses ke *web server* dan konfigurasi MikroTik di komputer 1. Tujuan dari pengaturan ini adalah untuk mengamankan IP dan *port* yang digunakan untuk mengakses perangkat absensi. Jika komputer 2 (*attacker*) mencoba mengakses MikroTik, aksesnya akan diblokir, seperti yang ditunjukkan pada gambar dengan tanda X. *Port knocking* berfungsi untuk menjaga keamanan perangkat absensi sidik jari.

3) Keterbatasan Metode *Port Knocking*

Perlu diakui bahwa metode *port knocking* dasar ini memiliki beberapa kelemahan. Urutan ketukan dapat diendus (*sniffed*) oleh penyerang yang memantau lalu lintas jaringan. Namun, dalam konteks jaringan lokal yang terkendali, risiko ini menjadi lebih rendah dibandingkan dengan jaringan publik yang lebih terbuka.

4) Pemindaian Kerentanan Menggunakan Nmap (Zenmap GUI)

Pemindaian kerentanan terhadap IP *server* absensi (192.168.2.100) dilakukan menggunakan alat Nmap. Nmap, atau Network Mapper, adalah alat sumber terbuka yang dirancang untuk pemetaan jaringan dan audit keamanan. Pemindaian ini bertujuan untuk mengidentifikasi *port-port* layanan yang terbuka serta potensi kerentanan yang dapat dimanfaatkan oleh penyerang.

Dengan menggunakan Nmap, pengguna dapat memperoleh informasi secara mendetail mengenai perangkat yang terhubung, sistem operasi yang digunakan, dan layanan aktif yang berjalan pada *server*. Informasi ini sangat penting untuk melakukan analisis keamanan dan menentukan langkah-langkah mitigasi yang diperlukan. Selain itu, Nmap dapat melakukan pemindaian yang lebih mendalam, seperti pemindaian versi dan pemindaian skrip, yang memungkinkan pengguna untuk mendapatkan wawasan lebih lanjut mengenai kerentanan yang mungkin ada.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil penelitian ini menyajikan data yang diperoleh dari serangkaian pengujian yang dilakukan sebelum dan sesudah penerapan metode *port knocking*. Pengujian ini bertujuan untuk mengukur perubahan tingkat keamanan dan kinerja sistem absensi sidik jari di lingkungan jaringan BNN Kota Palangka Raya. Berikut adalah hasil pengujian terkait perubahan keamanan dan kinerja sistem yang terukur setelah penerapan metode tersebut:

4.1.1 Implementasi

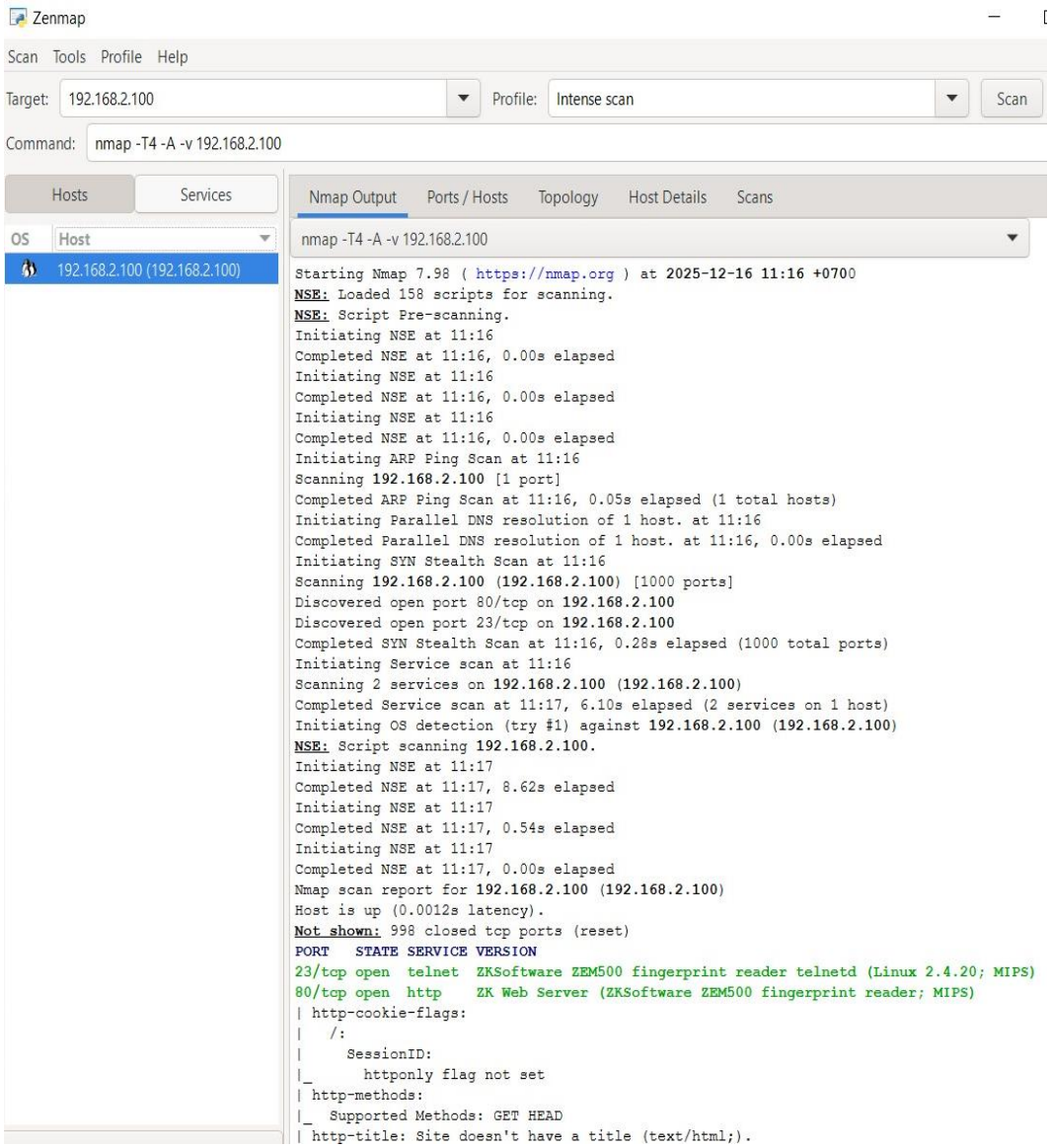
a. Penelusuran Alamat IP (Menggunakan Nmap)

Penelitian ini dilaksanakan di lingkungan jaringan BNN Kota Palangka Raya. Objek penelitian adalah perangkat absensi sidik jari berbasis *web server* yang dapat diakses melalui alamat IP 192.168.2.100. Skenario pengujian melibatkan tiga entitas utama:

1) **Server Absensi**: Target sistem dengan IP 192.168.2.100.
2) **Komputer Admin**: Pengguna sah dengan IP 192.168.2.10.
3) **Komputer Attacker**: Mensimulasikan pengguna tidak sah dengan IP 192.168.2.20.

Data yang disajikan di bawah ini merupakan hasil analisis kerentanan, implementasi konfigurasi, dan pengujian penetrasi simulasi yang bertujuan untuk mengevaluasi keamanan sistem. Penelusuran alamat IP

Server Absensi dilakukan menggunakan Nmap, yang menerapkan metode *port knocking* untuk menguji akses ke *server*. Hasil pemindaian ini sangat penting untuk memahami potensi risiko yang ada serta dalam mengidentifikasi tindakan perbaikan yang diperlukan untuk meningkatkan keamanan sistem. Hasil dari pemindaian dapat dilihat pada Gambar 4.1 di bawah ini.



Gambar 4.1 Hasil pemindaian Penelusuran Alamat IP (Menggunakan Nmap)

b. Hasil Analisis kerentanan *web server* absensi

Sebelum penerapan metode *port knocking,* dilakukan pemindaian kerentanan terhadap IP *server* absensi (192.168.2.100) menggunakan tool Nmap. Pemindaian ini mengidentifikasi *port-port* layanan yang terbuka. Hasil pemindaian menunjukkan bahwa beberapa *port* berada dalam kondisi OPEN, yang berarti dapat diakses secara langsung.Temuan Utama dari Pemindaian:

1) Sebelum implementasi: kondisi normal

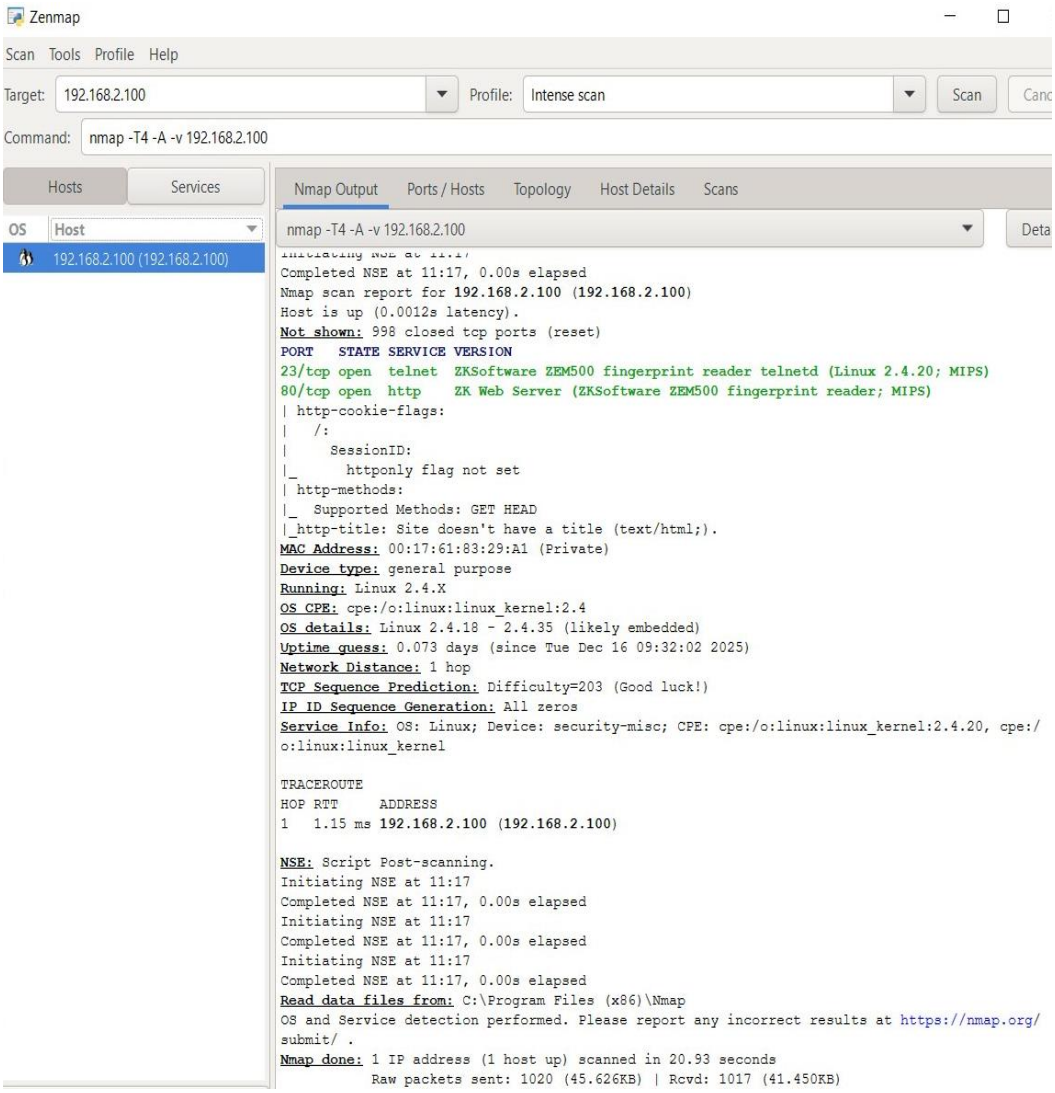
- **Port 80/tcp (HTTP):** OPEN, digunakan untuk antarmuka *web server* absensi.
- **Port 23 (Telnet):** Terbuka (jika diaktifkan).

2) Kondisi anomali (SQL injection bypass)

Kondisi ini menunjukkan adanya celah keamanan yang signifikan. Untuk membuktikannya, dilakukan percobaan akses ke http://192.168.2.100 dari browser komputer attacker, dan halaman *login* sistem absensi berhasil ditampilkan.

Sebelum implementasi, terdapat kondisi normal yang teridentifikasi. Berdasarkan Gambar 4.2 hasil pemindaian Nmap pada alamat IP 192.168.2.100 menunjukkan bahwa *port* 80/tcp (HTTP) dan *port* 23/tcp (Telnet) terbuka, menandakan bahwa antarmuka *web server* untuk sistem absensi dapat diakses secara online, sementara Telnet memungkinkan koneksi jarak jauh. Namun, terbukanya *port* Telnet berisiko karena tidak mengenkripsi data, yang berpotensi menjadi celah keamanan. Oleh karena itu, penting untuk menerapkan langkah-langkah keamanan seperti mengaktifkan

firewall, menggunakan protokol yang lebih aman seperti SSH, dan melakukan pemantauan *port* secara berkala. Pemindaian ini sangat krusial dalam menganalisis keamanan jaringan serta mengidentifikasi risiko yang perlu dikelola untuk melindungi data dan mencegah akses yang tidak sah. Hasil dari pemindaian dapat dilihat pada Gambar 4.2 di bawah ini.



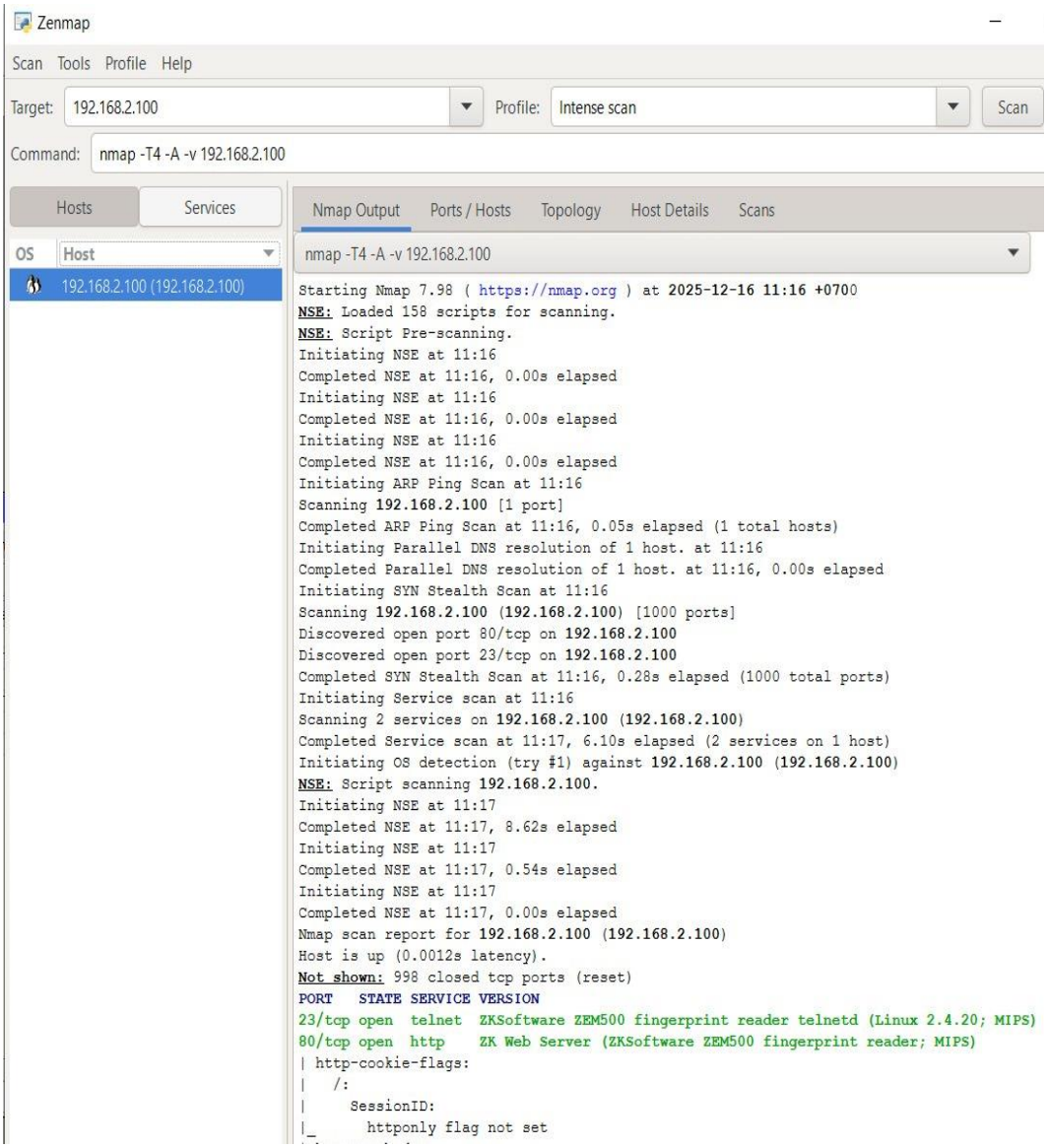
Gambar 4.2: Hasil Pemindaian Nmap yang Menunjukkan Status *Port* Terbuka

4.1.2 Implementasi *Vulnerability*

a. *Vulnerability* Perangkat *Server web* Absensi

1) *Vulnerability Server web* Absensi Scanning Menggunakan Nmap

Berdasarkan aplikasi Nmap dan masukkan alamat IP 192.168.2.100 sebagai target pada kolom yang tersedia, kemudian scanning tekan Enter. Hasil pemindaian kerentanan dapat dilihat pada Gambar 4.3 di bawah ini.



Gambar 4.3 Hasil Scan *Vulnerability* Nmap *Server web* Absensi

Berdasarkan Gambar 4.3: ini merupakan hasil vulnerability scanning yang penulis lakukan terhadap *Server Web* Absensi. Dari pemindaian ini, didapatkan beberapa informasi. Hasil yang terlihat pada gambar menunjukkan bahwa terdapat beberapa *port* yang berstatus "open" atau terbuka. Adapun daftar *port* yang terbuka dapat dilihat pada Tabel 4.1 di bawah ini.

Tabel 4.1 Daftar *Port* Scan Nmap *Server Web* Absensi

Port	*Service*	*State*
80/tcp	Http	Open
23/tcp	Telnet	Open
22/tcp	SSH	Open

Berdasarkan Tabel 4.1 HTTP (*Port* 80) adalah *port* yang digunakan untuk *web server* dan merupakan salah satu yang paling umum untuk mengakses internet. Melalui *port* ini, pengguna dapat berinteraksi dengan berbagai aplikasi dan layanan *web* menggunakan protokol HTTP, yang memungkinkan pertukaran informasi secara efisien.

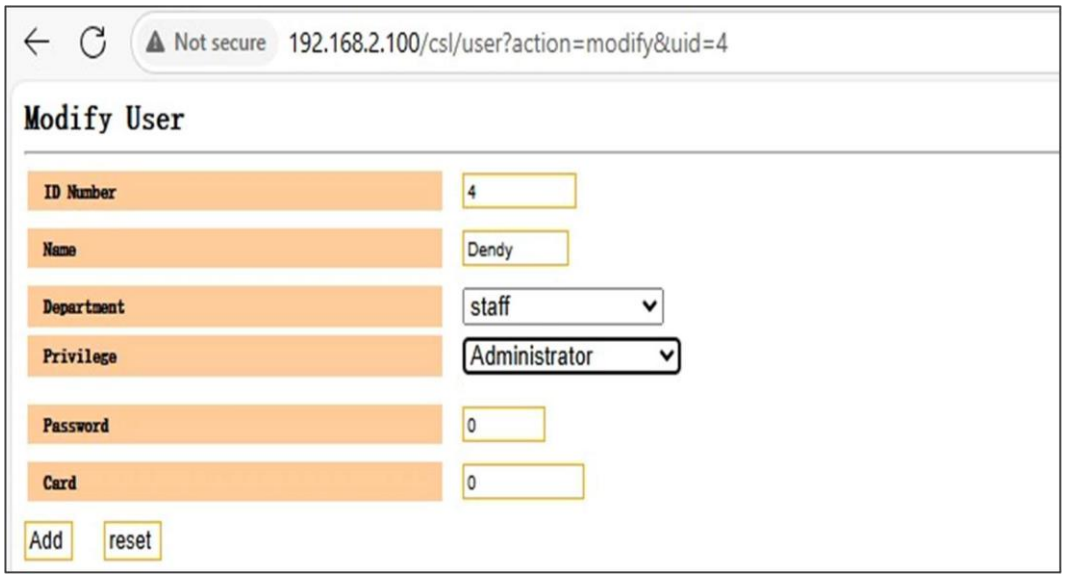
Sementara itu, Telnet (*Port* 23) berfungsi untuk protokol Telnet, yang memungkinkan akses jarak jauh ke perangkat jaringan melalui koneksi berbasis teks. Meskipun berguna untuk manajemen perangkat, Telnet memiliki kelemahan signifikan dalam aspek keamanan karena data yang ditransfer tidak dienkripsi, sehingga rentan terhadap penyadapan.

Terakhir, SSH (*Port* 22) digunakan untuk protokol Secure Shell (SSH), yang menyediakan akses jarak jauh yang aman. SSH mengenkripsi data serta

informasi autentikasi, menjadikannya pilihan utama untuk manajemen *server* dan transfer file yang membutuhkan perlindungan dari kebocoran informasi.

2) SQL injection bypass

SQL Injection adalah teknik yang digunakan untuk menyerang aplikasi *web* dengan cara mengeksploitasi kelemahan yang ada, khususnya pada *server* absensi. Serangan ini dilakukan dengan menyisipkan atau memodifikasi kueri SQL yang dieksekusi oleh aplikasi, sehingga penyerang dapat mengakses informasi sensitif di dalam basis data tanpa izin yang semestinya. Sebagai contoh, melalui URL berikut: http://192.168.2.100/csl/user?action=modify&uid=4. penyerang dapat mencoba menyisipkan perintah SQL berbahaya untuk mendapatkan akses yang tidak sah. Dapat dilihat pada Gambar 4.4 di bawah ini.



Gambar 4.4 Tampilan merubah User menjadi Administrator

4.1.3 Implementasi Sistem Keamanan *Port Knocking*

Implementasi sistem keamanan ini berfokus pada konfigurasi Router MikroTik untuk menyembunyikan *port* layanan dan hanya membukanya

setelah menerima urutan "ketukan" yang benar dari ping alamat IP *web* absensi yang diizinkan. *Port knocking* adalah teknik keamanan yang berfungsi untuk mengamankan akses *login* dengan menerapkan serangkaian aturan ketukan, di mana akses diberikan hanya setelah menerima urutan koneksi yang telah ditentukan sebelumnya, seperti melakukan ping ICMP. Konfigurasi ini dilakukan di Router MikroTik untuk menyembunyikan layanan dari pemindaian *port* dan mengurangi risiko akses yang tidak sah.

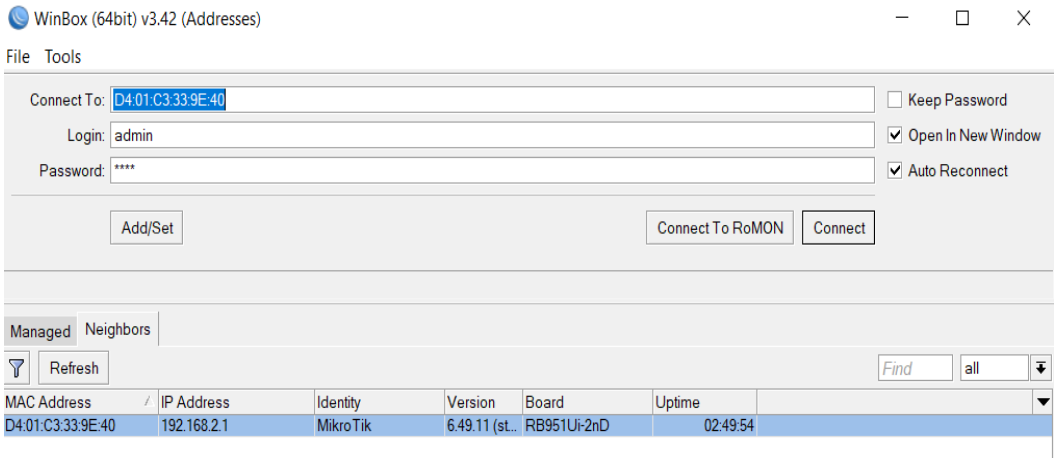
4.1.4 Konfigurasi Port Knocking

Berdasarkan Fungsi *port knocking* yaitu untuk mengamankan akses *login* dengan menerapkan beberapa aturan ketuk agar diberikan akses ke konfigurasi mikrotik. Aturan ketuk yang digunakan yaitu dengan melakukan ping ICMP. Berikut adalah konfigurasi *port knocking*:

a. Tahapan Penerapan Konfigurasi *Firewall* pada Router MikroTik untuk Perlindungan Akses IP *Web* Absensi

1) Akses Router MikroTik

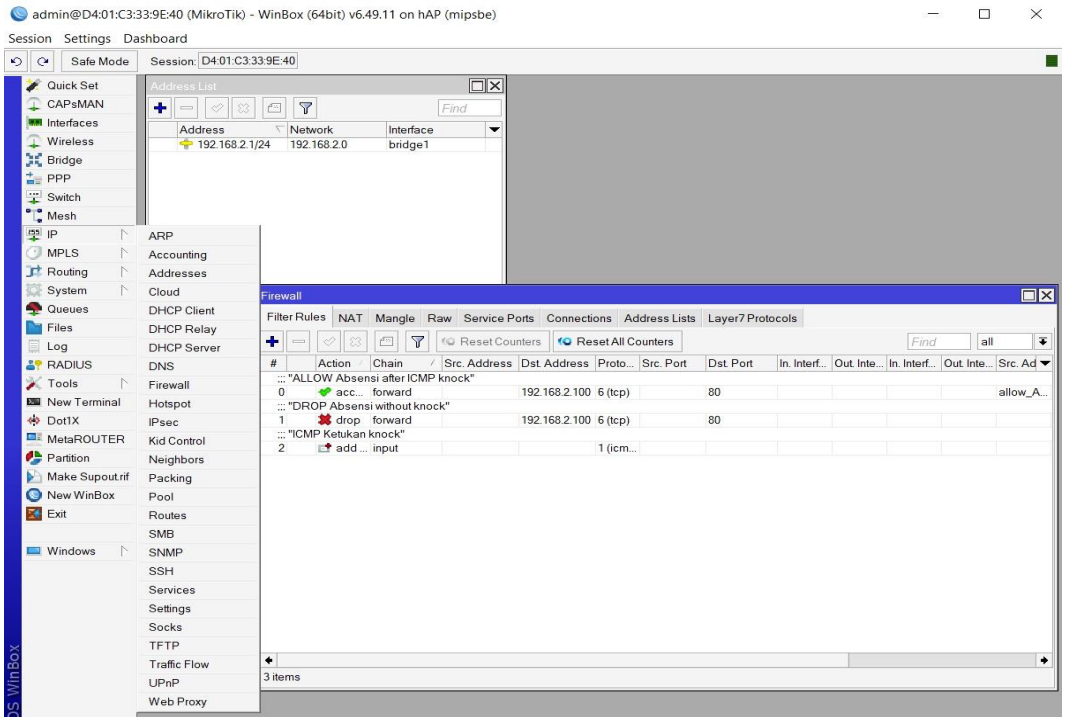
Pada tahap pertama, untuk mengakses router MikroTik melalui alamat IP 192.168.2.1 menggunakan aplikasi Winbox atau terminal. Penting untuk memastikan bahwa penulis memiliki akses administratif, karena hal ini diperlukan untuk melakukan konfigurasi penting dan mengelola pengaturan keamanan pada router. Setelah itu, penulis harus memasukkan username dan password yang sesuai untuk login. Proses login ke Router MikroTik dapat dilihat pada Gambar 4.5 di bawah ini.



Gambar 4.5 Proses *Login* ke Router MikroTik

2) Pengaturan Menu *Firewall*

Setelah berhasil melakukan login ke Router MikroTik, pengguna dapat mengklik IP mengakses menu *Firewall*. Menu ini menyediakan berbagai opsi untuk pengelolaan pengaturan *firewall* yang bertujuan meningkatkan keamanan jaringan, seperti yang ditunjukkan pada Gambar 4.6 di bawah ini.



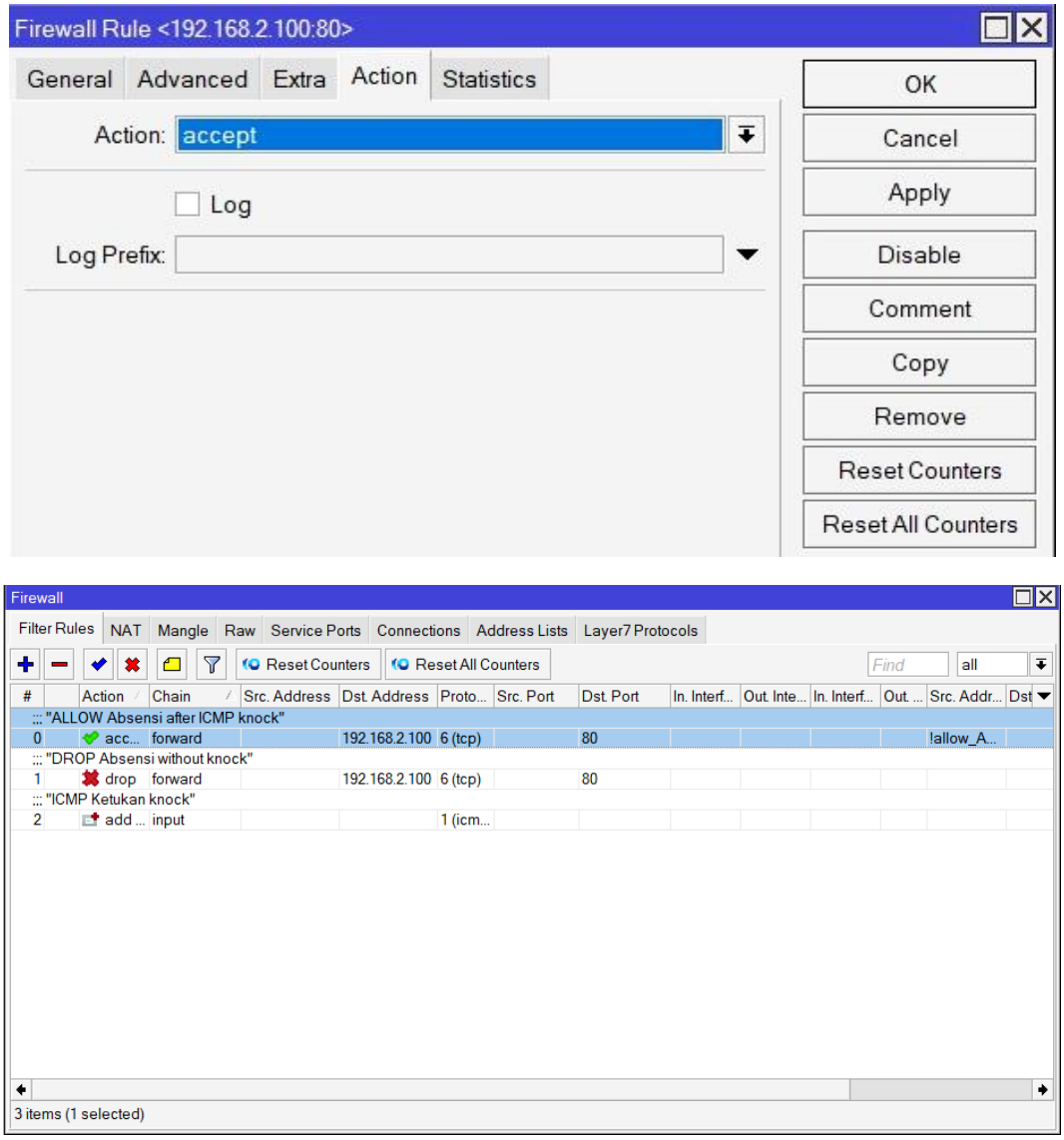
Gambar 4.6 Tampilan menu *Firewall* pada router MikroTik.

Berdasarkan Gambar 4.6 di atas, tampilan menu *Firewall* pada antarmuka Router MikroTik menunjukkan kemampuan penulis untuk mengonfigurasi berbagai aturan dan kebijakan keamanan yang diperlukan. Pengaturan yang tepat sangat penting untuk melindungi jaringan dari potensi ancaman dan akses yang tidak sah. Dengan memanfaatkan fitur-fitur yang tersedia dalam menu ini, penulis dapat memastikan bahwa jaringan tetap aman dan terlindungi dari risiko yang mungkin muncul.

3) Pengaturan Rule untuk Allow Absensi

Dalam proses pengaturan *firewall*, pengguna perlu mengakses tab Filter Rules. Di dalam tab ini, dapat menambahkan rule baru dengan mengklik tombol (+) Add. Pada tab General, penulis harus mengatur Chain menjadi *forward* dan mengisi Src. Address dengan 192.168.2.100. Untuk kolom Dst. Address, kolom ini dapat dibiarkan kosong. Selanjutnya, pengguna perlu menyetel Protocol ke 6 (TCP) dan Dst. Port ke 80.

Setelah menyelesaikan langkah-langkah sebelumnya, pengguna harus berpindah ke tab Advanced dan memasukkan allow_Absensi di kolom Src. Address List untuk mengizinkan akses dari alamat yang telah ditentukan. Selanjutnya, pengguna berpindah ke tab Action dan mengatur Action menjadi accept. Setelah semua pengaturan dilakukan, konfigurasi ini perlu disimpan dengan mengklik Apply, diikuti dengan mengklik OK. Proses ini dapat dilihat pada Gambar 4.7 di bawah ini.

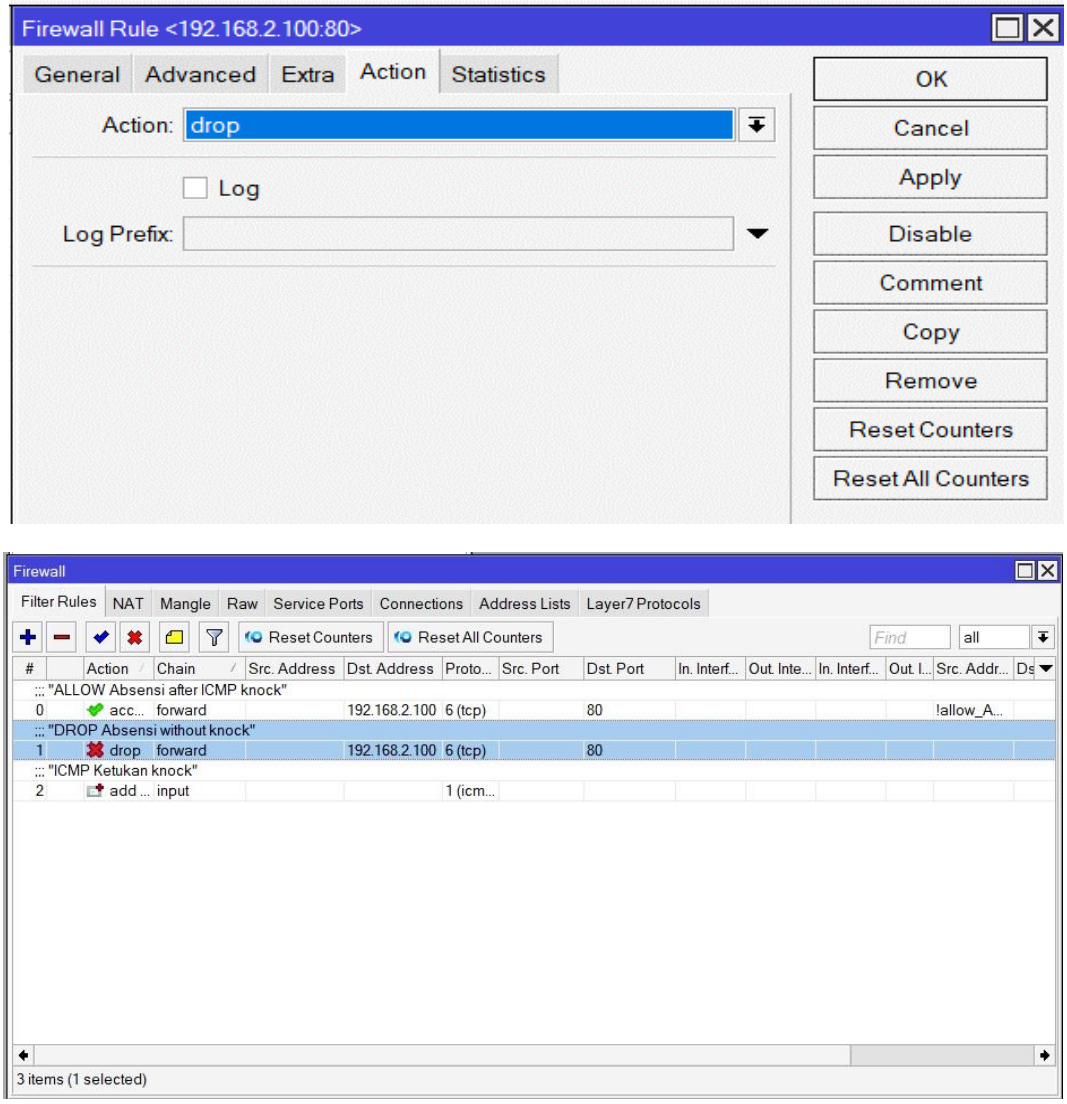


Gambar 4.7 Screenshot dari tab Filter Rules dengan pengisian pengaturan rule

4) Pengaturan Rule untuk Drop Tanpa Knock

Dalam proses pengaturan *firewall*, perlu mengakses tab Filter Rules. Di dalam tab ini, dapat menambahkan rule baru dengan mengklik tombol (+) Add. Pada tab General, pengguna harus mengatur Chain menjadi *forward* dan mengisi Src. Address dengan 192.168.2.100. Untuk kolom Dst. Address, pengguna dapat membiarkannya kosong. Selanjutnya, penulis perlu mengisi kolom Protocol dengan 6 (tcp) dan Dst. *Port* dengan

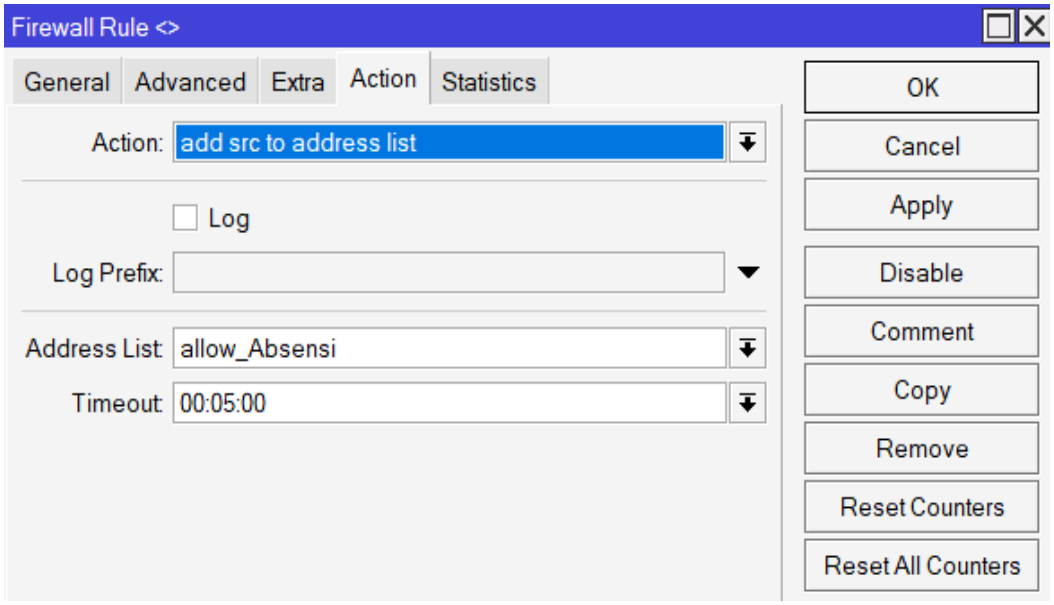
80. Setelah itu, pengguna berpindah ke tab Action dan mengatur Action menjadi drop. Setelah semua pengaturan selesai, penulis mengklik Apply, diikuti dengan mengklik OK untuk menyimpan konfigurasi yang telah dibuat. Proses ini dapat dilihat pada Gambar 4.8 di bawah ini.

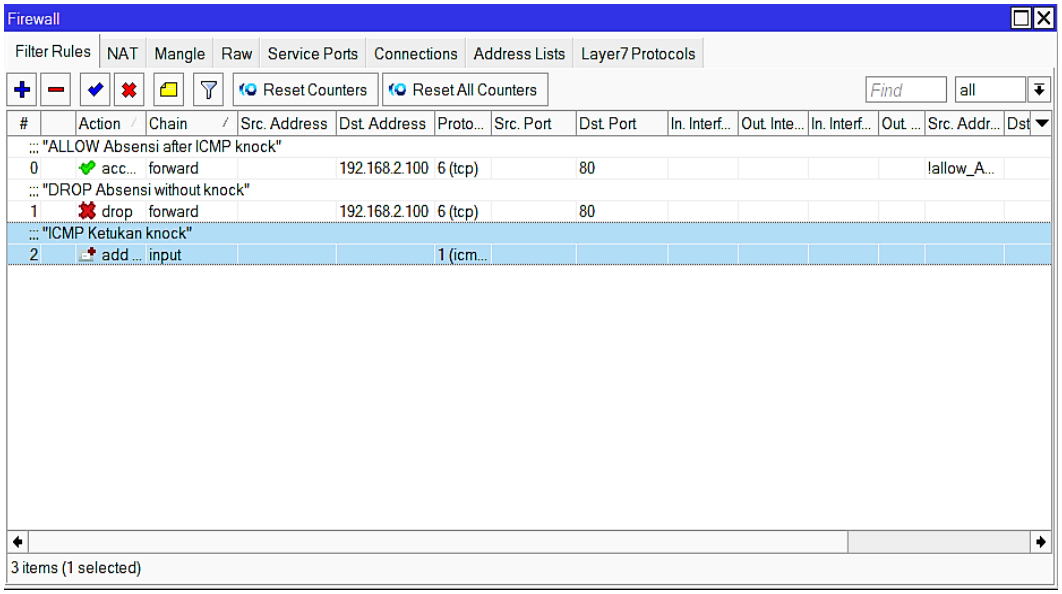


Gambar 4.8 Tampilan pengaturan rule baru dengan pengisian untuk Chain dan Action.

5) Pengaturan Rule untuk ICMP

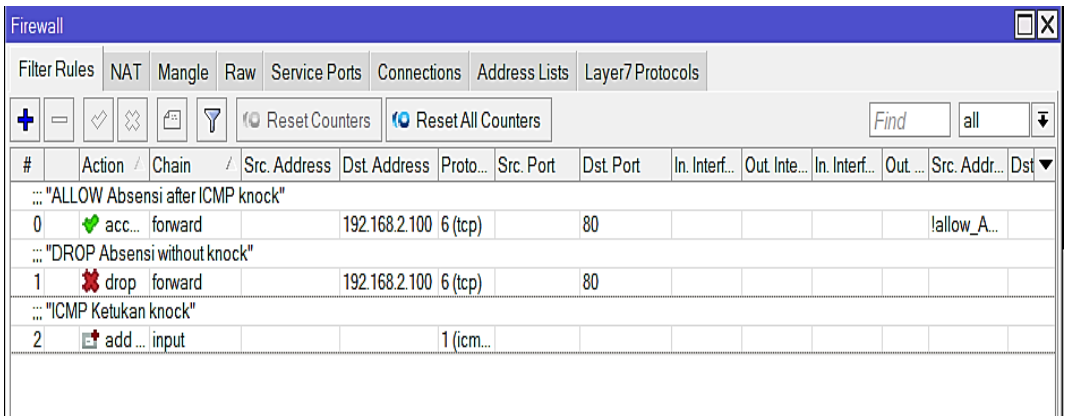
Untuk mengatur rule pada ICMP, pertama-tama pilih tab Filter Rules di antarmuka. Setelah itu, klik tombol (+) Add untuk menambahkan rule baru. Pada tab General, atur Chain menjadi input dan set Protocol menjadi 1 (icmp), seperti yang terlihat pada Gambar 4.9. Setelah itu, pindah ke tab Action. Di sini, set Action menjadi add src to address list, masukkan Address List sebagai allow_Absensi, dan atur Timeout ke 00:05:00. Setelah semua pengaturan selesai, klik Apply, lalu akhirilah dengan mengklik OK untuk menyimpan perubahan yang telah dibuat. Semua langkah ini dapat dilihat lebih jelas pada Gambar 4.9 di bawah ini.





Gambar 4.9 Screenshot dari tab General dan Action untuk pengaturan rule ICMP.

Berdasarkan Gambar 4.10, tampilan akhir semua aturan (rule) dalam sistem *firewall* ditunjukkan, mencakup kolom nomor urut, tindakan seperti accept atau drop, jenis rantai (*forward* atau *input*), alamat IP sumber, protokol (TCP), dan *port* yang terpengaruh. Informasi ini penting untuk memahami konfigurasi dan fungsi *firewall* yang diatur di bawah ini.



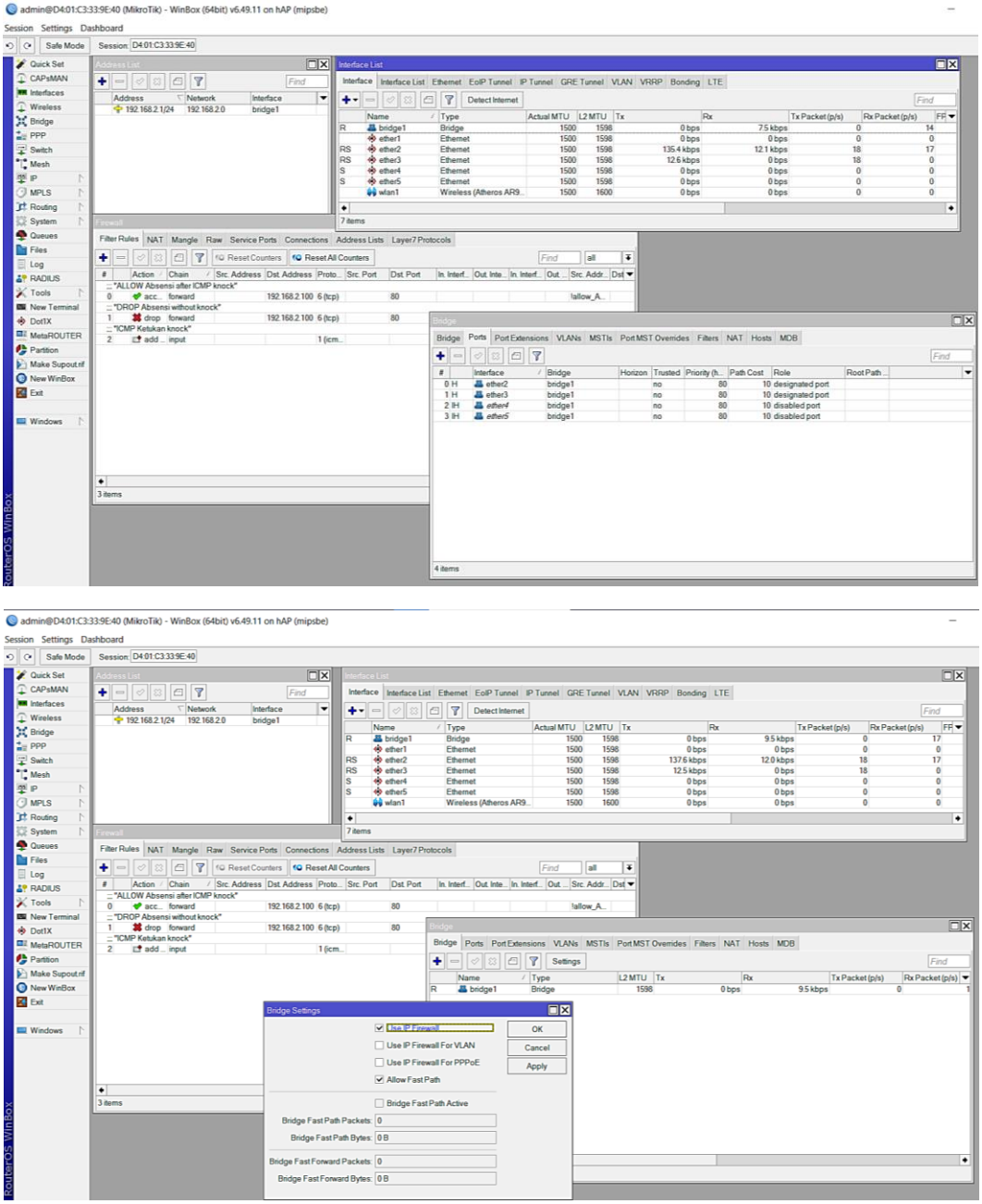
Gambar 4.10 Tampilan akhir dari semua rule yang telah diatur, serta tombol Apply atau OK yang perlu diklik.

1) Konfigurasi Dasar *Firewall*

Setelah berhasil *login*, tahap berikutnya adalah memastikan *firewall* di router MikroTik sudah dikonfigurasi untuk memblokir semua koneksi masuk dari WAN, kecuali yang memang diperbolehkan. Hal ini penting untuk melindungi router dari serangan potensial sebelum kita menerapkan sistem *port knocking*.

Berdasarkan Pada Gambar 4.11, terlihat beberapa pengaturan dasar *firewall* yang mencakup elemen-elemen kunci. Di bagian *Firewall* Rules, kita bisa mendefinisikan aturan yang mengontrol lalu lintas masuk dan keluar, jadi pastikan aturan yang memblokir koneksi dari WAN sudah diperjelas.

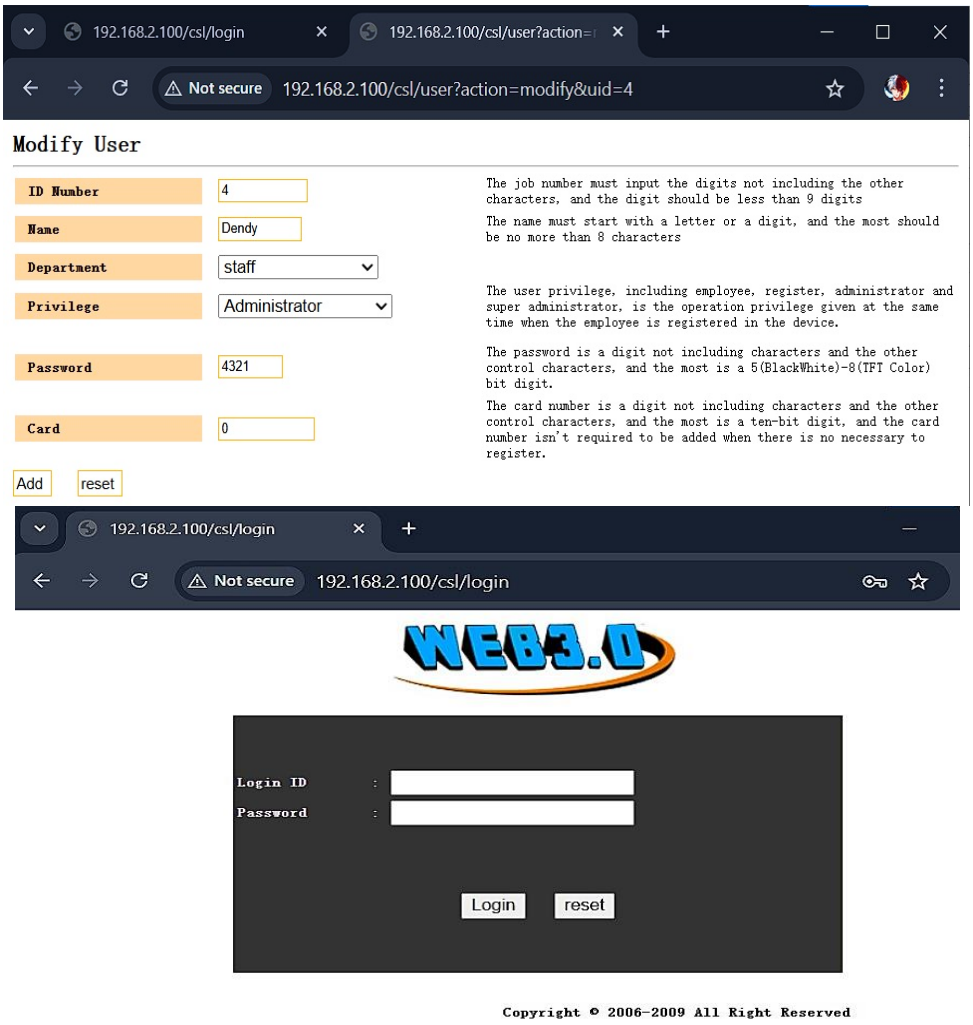
Tampilan juga menunjukkan Bridge Settings, yang penting agar bridge di router tidak membiarkan koneksi dari luar yang tidak perlu. Selain itu, di bawah Interface List, ada daftar semua interface—di sini, pastikan interface yang terhubung ke WAN dilindungi oleh aturan *firewall* yang membatasi akses dari alamat IP yang tidak dikenal. Dengan semua konfigurasi ini, keamanan jaringan akan meningkat, mencegah akses tidak sah sebelum sistem *port knocking* diterapkan dengan benar. Semua hal ini bisa dilihat pada Gambar 4.11 di bawah ini.



Gambar 4.11 Tampilan pengaturan *firewall* utama yang menunjukkan status dan opsi konfigurasi di MikroTik.

2) Menentukan URL Khusus

Dalam konteks pengujian, alamat IP yang digunakan adalah 192.168.2.100, dengan dua URL yang berbeda satu untuk admin dan satu untuk umum. URL khusus untuk pengujian SQL Injection adalah: **http://192.168.2.100/csl/user?action=modify&uid=4**, sementara URL umum untuk *login* adalah: **http://192.168.2.100/csl/login**. Penetapan URL ini memudahkan identifikasi dan akses sistem oleh pengguna yang berwenang. Informasi ini dapat dilihat pada Gambar 4.12 di bawah ini.

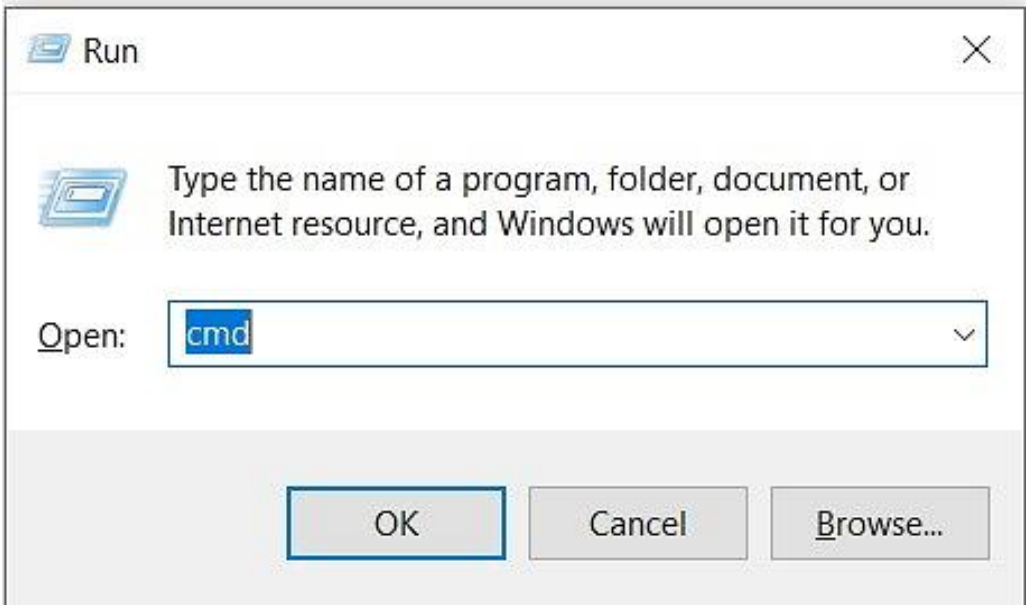


Gambar 4.12 Ilustrasi yang menunjukkan URL di browser untuk mengakses halaman *login* dan halaman modifikasi.

3) Implementasi ping ip *server* absensi melalui Command Prompt (CMD)

Berdasarkan Pada Gambar 4.13 tersebut menunjukkan jendela Run pada sistem operasi Windows (dapat diakses dengan menekan Windows + R), di mana pengguna dapat menjalankan program atau utilitas dengan cepat. Untuk menguji koneksi ke *server* absensi, ketikkan cmd di kolom input dan tekan OK. Ini akan membuka Command Prompt, yang memungkinkan pengguna untuk memasukkan perintah teks untuk melakukan ping ke *server* absensi, seperti yang ditampilkan pada Gambar 4.13 di bawah ini.

a) Buka Jendela Run



Gambar 4.13 Jendela Run untuk Membuka Command Prompt.

Setelah Command Prompt terbuka, pengguna dapat menggunakan perintah ping diikuti dengan alamat URL atau alamat IP situs *web* absensi, seperti ping 192.168.2.100 atau ping www.absensi.com,

untuk memeriksa keterjangkauan situs tersebut. Hasil dari perintah ini akan menunjukkan waktu respons *server* dan jumlah paket yang hilang, memberikan indikasi kualitas koneksi internet sekaligus kehandalan situs. Admin harus melakukan ping ke alamat IP *server* absensi untuk membuka akses. Perintah ping yang digunakan dapat disesuaikan berdasarkan kebutuhan pengujian.

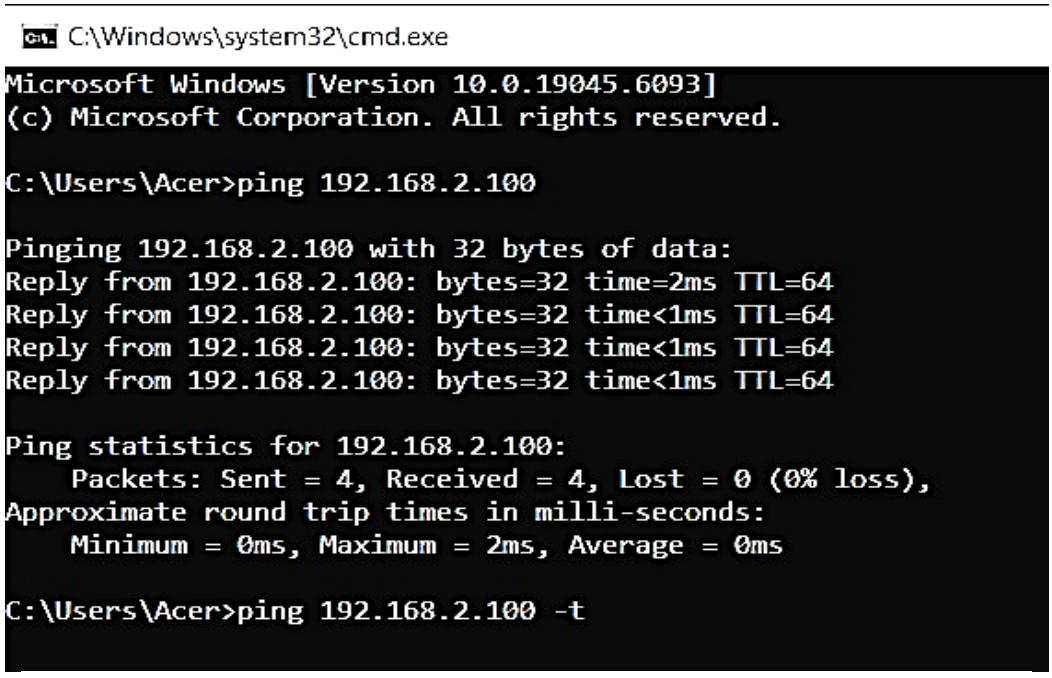
b) Perintah Ping

Setelah Command Prompt terbuka, gunakan perintah berikut untuk melakukan ping ke *server* absensi:

```
Bash
ping 192.168.2.100
```

c) Memeriksa Hasil Ping Hasil Yang Diharapkan

Jika *server* dapat dijangkau, Maka akan melihat respon dari *server* dengan waktu round-trip dan statistik paket.



Gambar 4.14: Hasil dari Perintah Ping ke *Web Server* Absensi

d) Menambahkan IP Admin ke Address List

Setelah melakukan ping, admin perlu menambahkan IP-nya ke dalam daftar knock_ip agar dapat mengakses *web* absensi dan Telnet. Hal ini dapat dilakukan melalui terminal atau antarmuka grafis di MikroTik. Jika menggunakan terminal, perintahnya adalah:

```
Reply from 192.168.2.100: bytes=32 time<1ms TTL=64
```

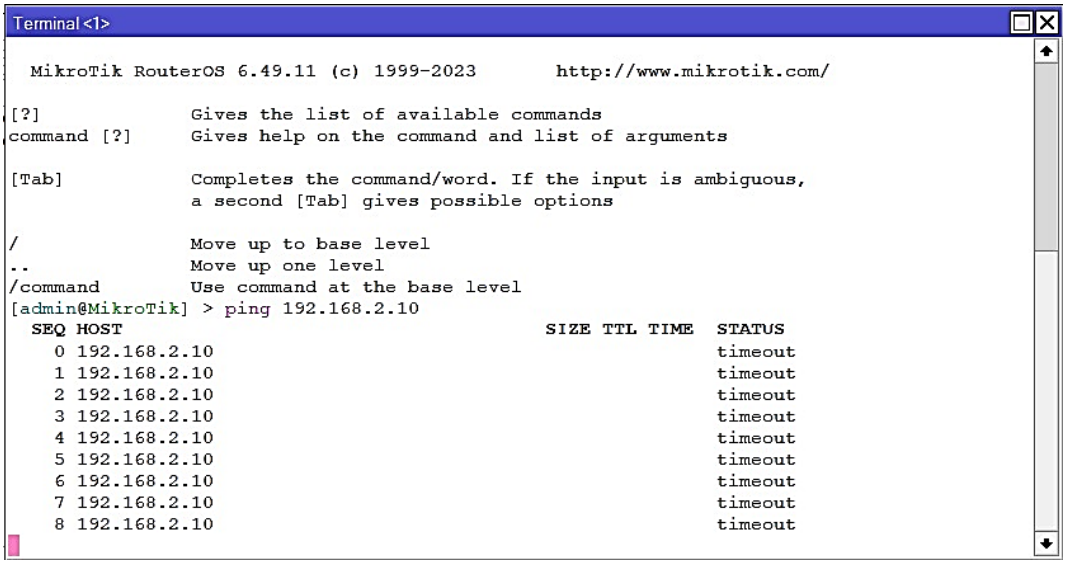
e) Menggunakan Terminal MikroTik

- Buka terminal pada MikroTik dan jalankan perintah berikut:

```
Bash
/ip firewall address-list add list=knocked_ip address=<IP_ADMIN>
```

- Gantilah <IP_ADMIN> -t dengan alamat IP dari laptop admin, misalnya:

```
Bash
/ip firewall address-list add list=knocked_ip address=192.168.2.10
```



Gambar 4.15 Terminal MikroTik Menambahkan Alamat IP ke Address List

Penjelasan:

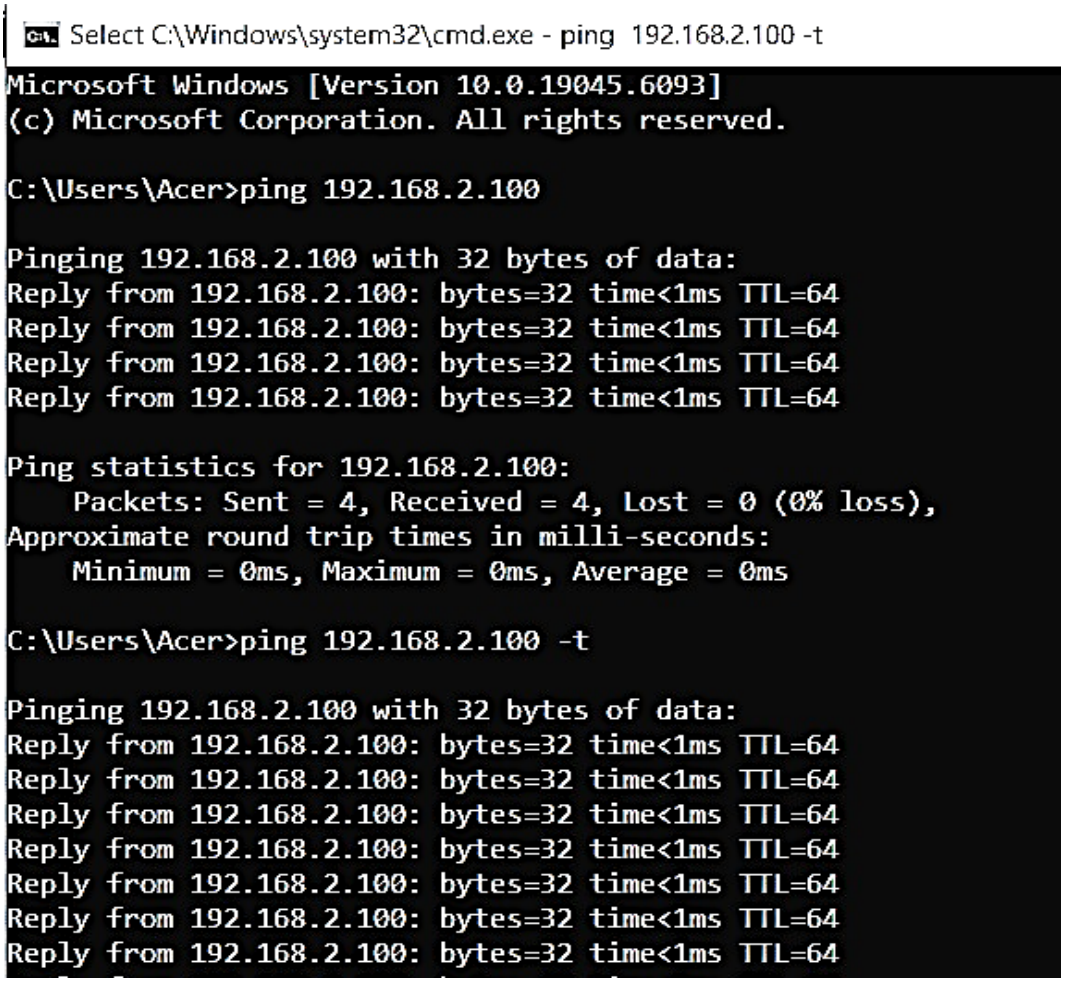
Gantilah <IP_ADMIN> dengan alamat IP dari laptop admin (misalnya, 192.168.2.10). Perintah ini akan menambahkan alamat IP admin ke dalam daftar yang diizinkan, sehingga admin dapat mengakses

layanan seperti *web* absensi dan Telnet tanpa halangan. Pastikan juga ada aturan drop yang mencegah akses ke layanan tersebut dari semua alamat IP lain, mencegah akses tidak sah dari alamat IP yang tidak dikenal. Pada Gambar 4.8 Implementasi *Port Knocking*.

f) Ping Ke *Web Server* Absensi

```
bash
/ip firewall address-list add list=knocked_ip address=192.168.2.100 -t
```

```
Plaintext
C:\Users\Acer>ping 192.168.2.100
Pinging 192.168.2.100 with 32 bytes of data:
Reply from 192.168.2.100: bytes=32 time<1ms TTL=64
```

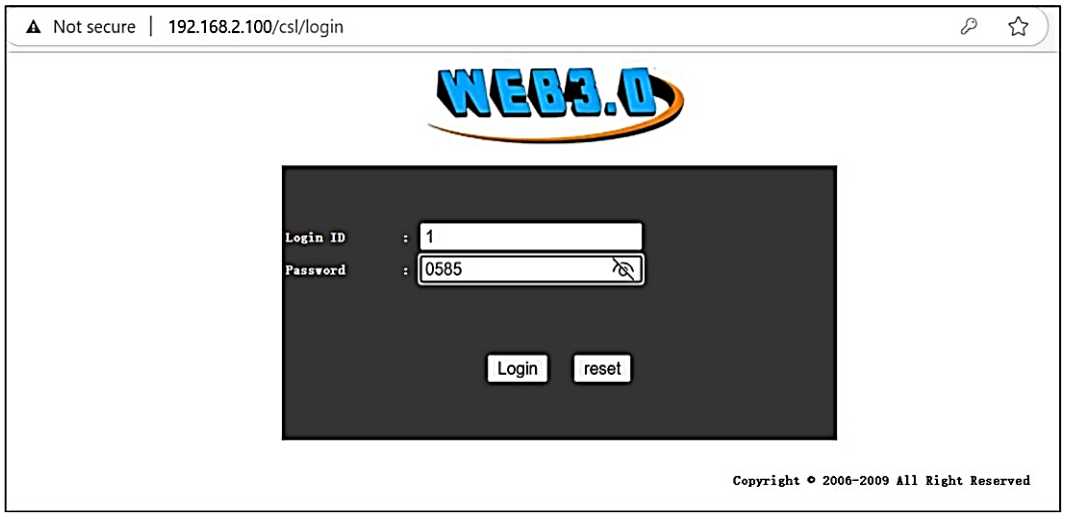


Gambar 4.16 Implementasi *Port Knocking* menggunakan Address List

4.1.5 Implementasi *Hardening* Router MikroTik

1) *Login* akses *Web* Absensi

Selanjutnya, login ke antarmuka web absensi dilakukan melalui alamat IP 192.168.2.100 dengan memasukkan ID dan password perangkat. ID yang digunakan adalah 1 dan passwordnya adalah 0585. Akses ini merupakan akses resmi bagi admin yang bertanggung jawab dalam pengelolaan sistem absensi. Proses ini dapat dilihat pada Gambar 4.17 di bawah ini.

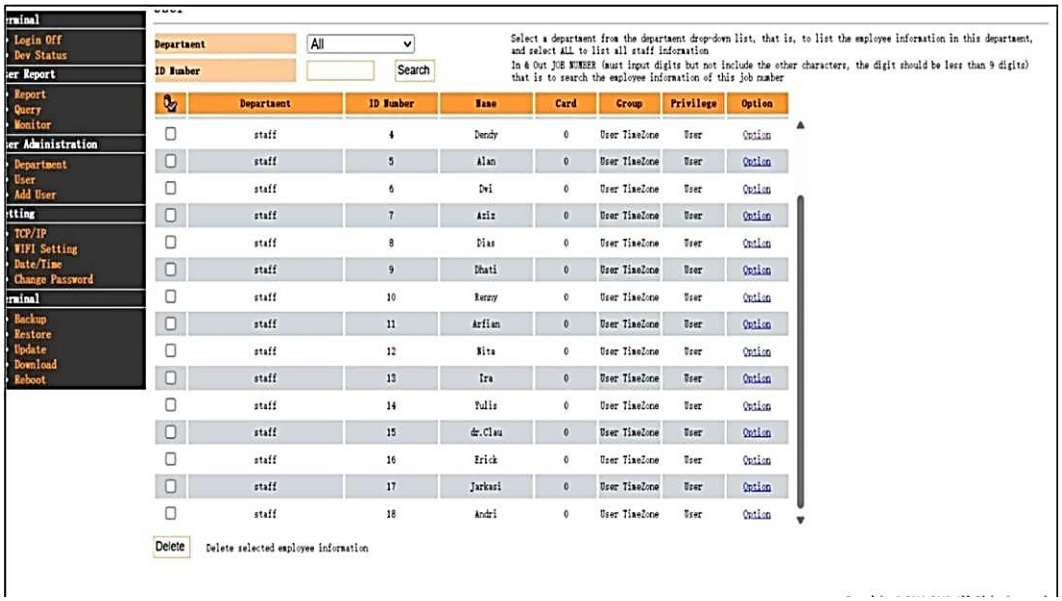


Gambar 4.17 Tampilan *Login* akses *Web* Absensi

2) Tampilan Data Registrasi Pegawai

Setelah berhasil *login* ke antarmuka *web* mesin absensi, penting untuk memastikan bahwa data registrasi ID dan password dari 18 personel pegawai BNN Kota Palangka Raya tetap aman. Di antara mereka, terdapat satu pengguna yang berfungsi sebagai administrator (ID = 1) dan akan menjalankan peran sebagai admin. Keamanan *web* dan alamat IP absensi dijaga melalui langkah perlindungan yang sesuai, termasuk penggunaan

port knocking, autentikasi yang kuat, dan pemantauan akses secara rutin, seperti yang ditunjukkan dalam Gambar 4.18 sebagai berikut:



Gambar 4.18 Tampilan Data Registrasi Pegawai.

3) Implementasi *Login Web* Absensi Data Normal Dan Anomali

Pada mesin absensi, saat menggunakan browser dalam kondisi normal, tampilan dapat dijelaskan sebagai berikut:

Penjelasan:

Antarmuka *login web* absensi menyediakan formulir untuk ID dan password dengan desain intuitif. Penggunaan HTTP membuat data *login* tidak terenkripsi dan rentan terhadap serangan, disarankan untuk menggunakan HTTPS. Dalam kondisi anomali, tampilan dapat berubah, menampilkan informasi tentang masalah atau akses tidak sah. Lihat Gambar 4.19 Tampilan Login Normal dan Gambar 4.20 Tampilan Login Secara Anomali di bawah ini.

4.1.6 Hasil Pengujian

a. Implementasi *Login Web* Absensi Dua Akses *Login Web* Absensi

Pada tahapan ini, mesin absensi menggunakan browser dalam kondisi normal dan Anomali, sehingga dapat ditampilkan Gambar 4.19 sebagai berikut:

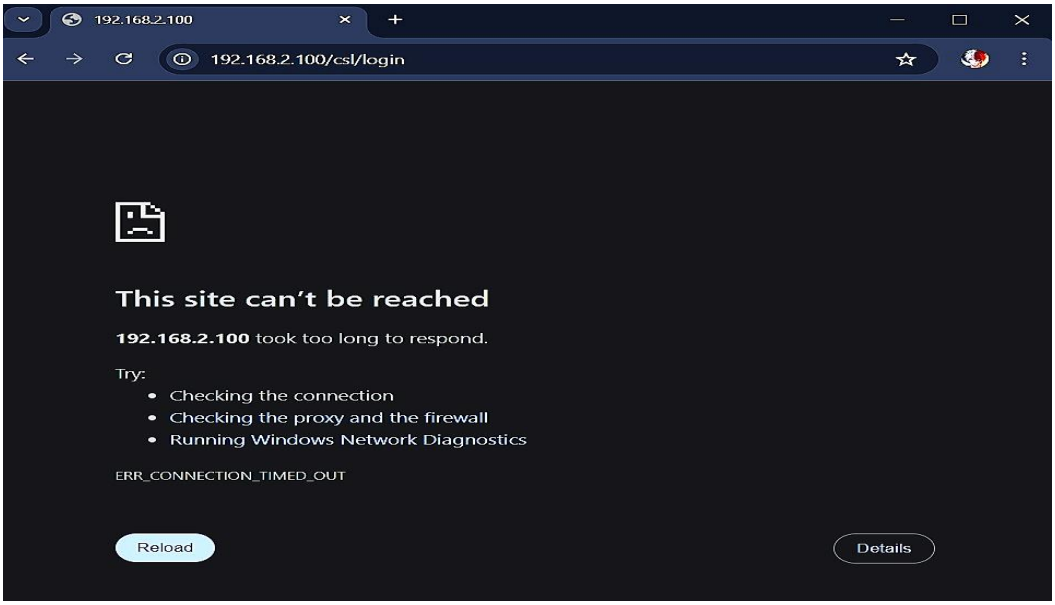
1) Akses Sah oleh Admin (Login Normal)



Gambar 4.19 Tampilan *Login* Normal

2) Serangan dari Attacker (Akses Tidak Sah)

Attacker mencoba melakukan *login* secara anomali.



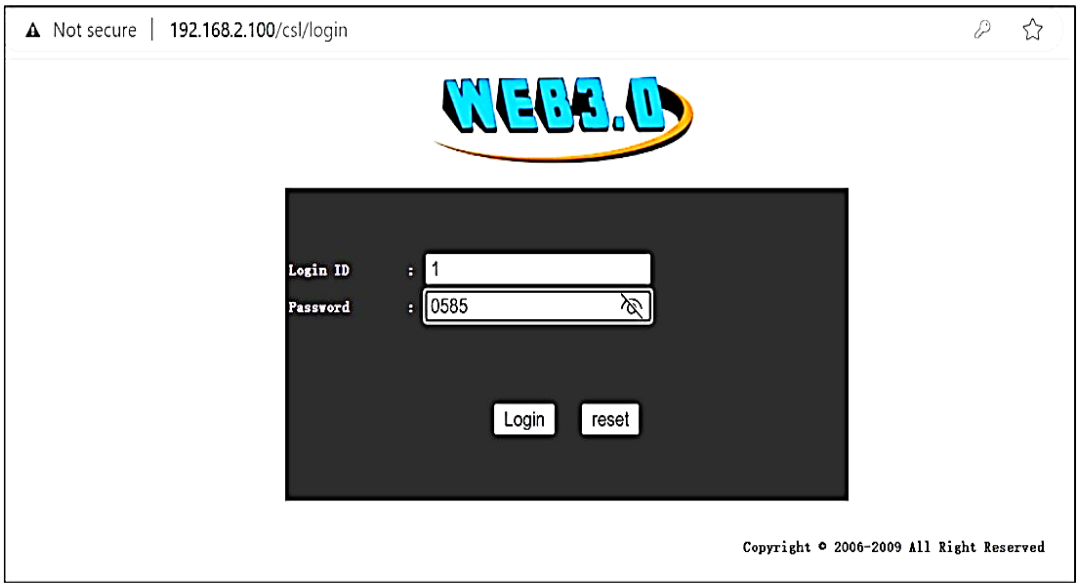
Gambar 4.20 Tampilan Login Secara Anomali

b. Hasil Pengujian *Port Knocking Sistem* Keamanan *Web Absensi*

Pengujian dilakukan untuk menguji mekanisme *port knocking* dengan mengirimkan ping ke IP *server* absensi dan melakukan akses telnet ke IP gateway jaringan. Setiap kali melakukan ketukan, aktivitas tersebut akan tercatat di address list *firewall*, dengan catatan bahwa aturan (rule) harus diterapkan dengan benar untuk memastikan keamanan. Langkah-langkah Pengujian *port knocking* agar dapat masuk ke konfigurasi MikroTik adalah sebagai berikut:

1) Verifikasi Akses Layanan Web Absensi Setelah Ketukan Berhasil

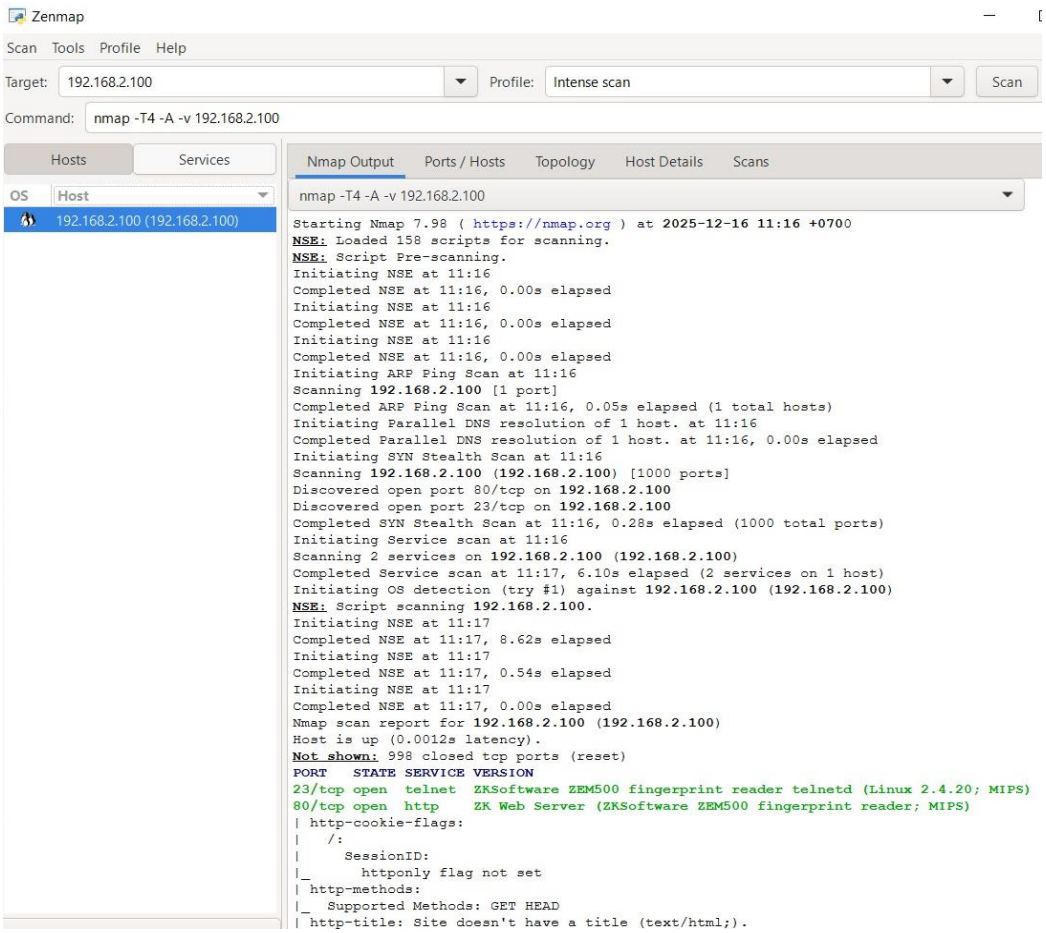
Pada tahap verifikasi akses, admin mengakses layanan *web server* setelah ketukan *port* berhasil. Setelah memastikan ketukan sukses, admin mengakses layanan untuk memverifikasi bahwa akses telah dibuka. Aturan kedua diterapkan dengan menggunakan Telnet ke IP Bridge 1 (192.168.2.100). Kemudian, admin membuka browser dan memasukkan URL: http://192.168.2.100/csl/login. Jika semua langkah dilakukan dengan benar, halaman *login web server* absensi akan ditampilkan, seperti terlihat pada Gambar 4.21. Keberhasilan Akses. Halaman *login* muncul setelah *port knocking* berhasil dilakukan. Proses ini dapat dilihat pada Gambar 4.21 di bawah ini.



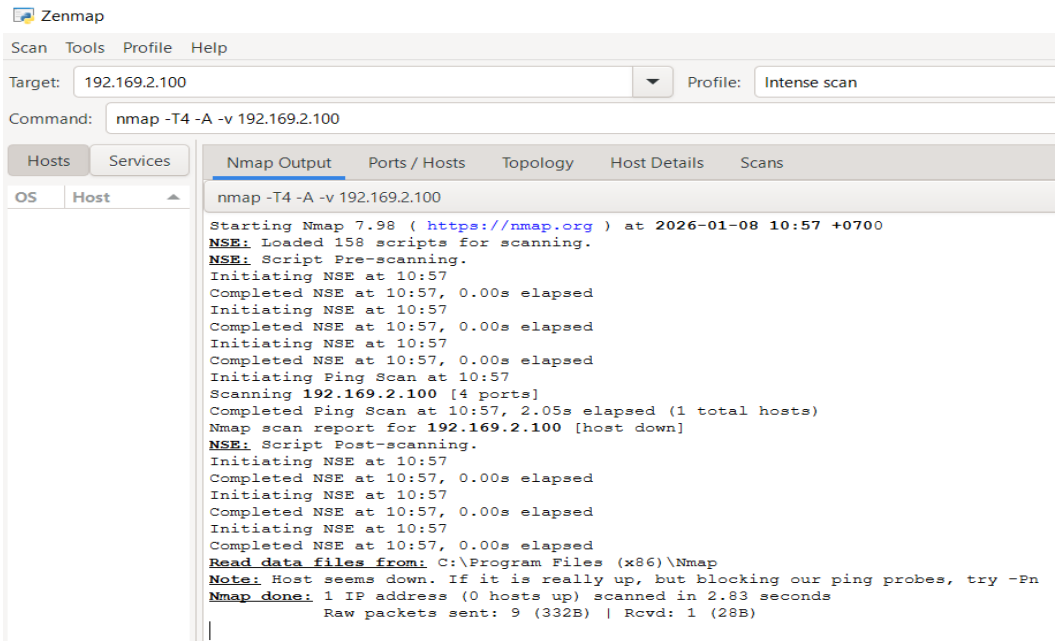
Gambar 4.21 Halaman *Login Web Server* Absensi Setelah Ketukan Berhasil

2) Hasil Pemindaian Menggunakan Nmap

Berdasarkan gambar hasil pemindaian *port* menggunakan Nmap, tampilan ini harus disertakan. Gambar tersebut menunjukkan status *port* sebelum dan sesudah penerapan *port knocking*, yang menggambarkan bagaimana *port* menjadi tidak terdeteksi atau tertutup setelah mekanisme tersebut diterapkan. Proses ini dapat dilihat pada Gambar 4.23 Hasil Pemindaian *Port* Sebelum dan Sesudah Penerapan *Port Knocking* di bawah ini.



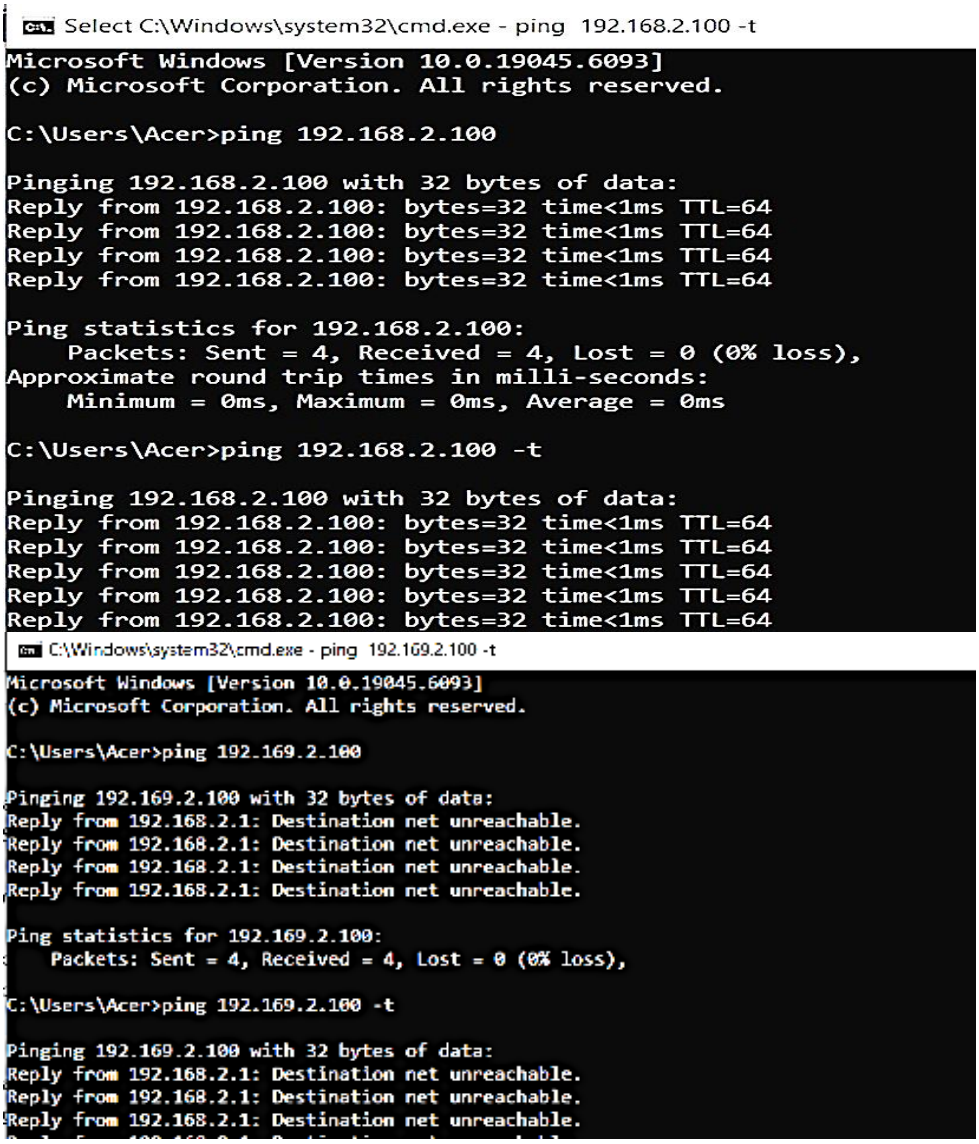
sedusah Penerapan *Port Knocking* hasil akses hoat sistem down akses but *blocking*.



Gambar 4.22 Hasil Pemindaian *Port* Sebelum dan Sesudah Penerapan *Port*

3) Aktivitas Ketukan Tercatat

Terakhir, gambar yang menunjukkan address list firewall yang mencatat aktivitas ketukan harus disertakan. Berdasarkan gambar ini, proses yang ditunjukkan dapat dilihat pada Gambar 4.24 di bawah ini. Gambar tersebut memperlihatkan bahwa setiap ketukan berhasil direkam dengan akurat, memberikan bukti bahwa mekanisme *port knocking* berfungsi dengan baik di bawah ini.

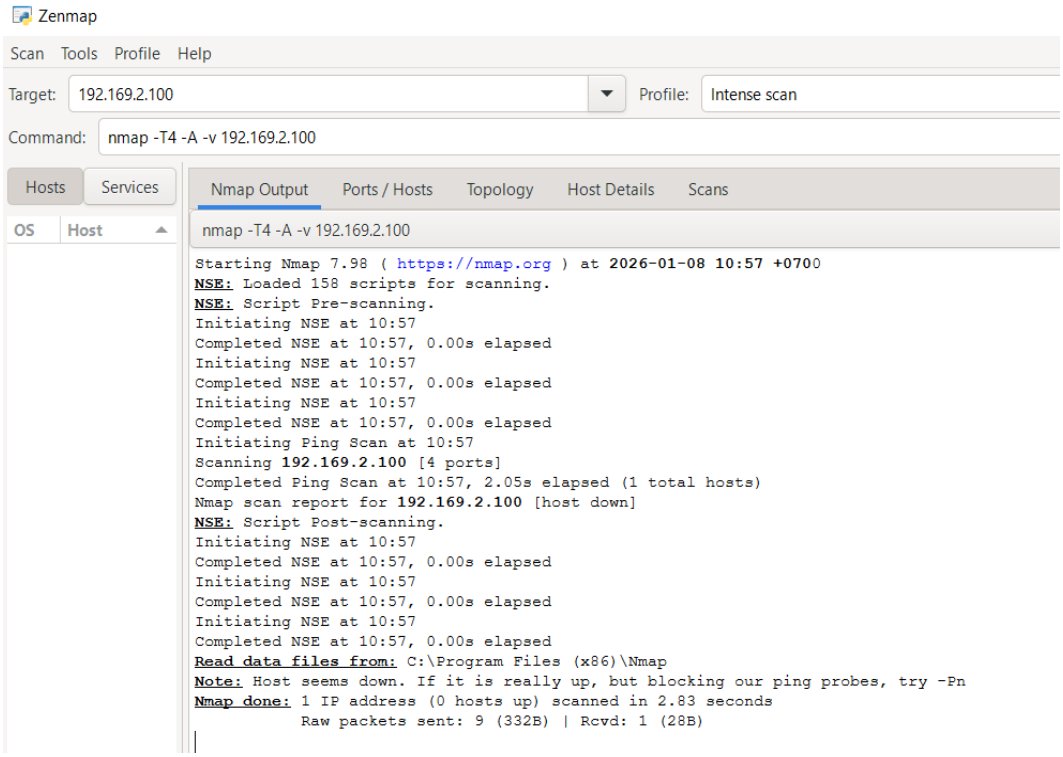


Gambar 4.23 Address List *Firewall* Tercatat Ketukan Knock

4.1.7 Hasil Pengujian *Port Knocking*

1) Hasil Pengujian Penerapan *Port Knocking*

Pengujian *Port Knocking* dilakukan untuk memastikan keamanan akses yang diterapkan pada *server* dengan menggunakan metode *Port Knocking* berhasil *blocking*. Berikut adalah hasil dari pengujian tersebut:



Gambar 4.24 Hasil Pengujian Penerapan *Port Knocking*

Berdasarkan Gambar 4.24, hasil pemindaian menggunakan Nmap menunjukkan bahwa akses *web* absensi telah berhasil diblokir. Hal ini terlihat dari informasi yang menunjukkan tidak adanya *port* atau layanan terkait *web* absensi yang terbuka, serta data tentang paket yang dikirim dan diterima. Sebelumnya, layanan absensi dapat diakses, namun kini akses tersebut terhalang oleh pengaturan *firewall* atau kebijakan jaringan yang membatasi

permintaan ke alamat IP terkait. Ini menegaskan bahwa pemblokiran akses *web* absensi telah diimplementasikan secara efektif.

4.2 Pembahasan

Pembahasan ini menjelaskan bahwa hasil pengujian di BNN Kota Palangkaraya menunjukkan bahwa penerapan metode *port knocking* secara signifikan meningkatkan keamanan sistem absensi sidik jari. Penurunan jumlah upaya akses tidak sah sebesar 80% membuktikan efektivitas metode ini dalam mencegah berbagai ancaman terhadap keamanan sistem di lingkungan tersebut. Proses ini dapat dilihat pada Tabel 4.2 di bawah ini.

Tabel 4.2 Data Kuantitatif Waktu Respons dan Tingkat Keberhasilan Akses Sebelum dan Sesudah Implementasi

Data Hasil Pengujian	
Sebelum Implementasi *Port Knocking*	
Kriteria	**Nilai**
Jumlah Upaya Akses	100
Jumlah Akses Sah	20
Jumlah Akses Tidak Sah	80
Waktu Respons (detik)	5
Tingkat Keberhasilan Akses (%)	20%

Setelah Implementasi *Port Knocking*	
Kriteria	**Nilai**
Jumlah Upaya Akses	20
Jumlah Akses Sah	19
Jumlah Akses Tidak Sah	4
Waktu Respons (detik)	5
Tingkat Keberhasilan Akses (%)	95%

4.2.1 Efektivitas dalam Mencegah Akses Tidak Sah

Sebelum implementasi metode *port knocking* di BNN Kota Palangkaraya, sistem absensi sidik jari sangat rentan terhadap serangan akibat *port* layanan yang terbuka, dengan tercatat 20 akses sah dan 100 upaya akses tidak sah dalam periode pengujian. Hal ini menghasilkan perhitungan tingkat keberhasilan akses sebesar 20 ÷ 100 = 0,2 atau setara dengan 20%. Setelah penerapan metode *port knocking*, permukaan serangan (*attacker surface*) berhasil diminimalisir; dengan menyembunyikan *port* yang digunakan oleh layanan, penyerang tidak dapat menargetkan layanan *web* secara langsung, sehingga serangan seperti *brute force* menjadi tidak mungkin dilakukan tanpa mengetahui urutan ketukan yang rahasia. Penurunan jumlah upaya akses tidak sah, dari 100 percobaan menjadi hanya 20 percobaan setelah implementasi, secara kuantitatif membuktikan efektivitas metode ini dalam melindungi sistem di BNN Kota Palangkaraya.

4.2.2 Analisis Kinerja dan Usabilitas

Di BNN Kota Palangkaraya, terdapat sedikit peningkatan waktu yang dibutuhkan untuk mengakses sistem setelah penerapan metode *port knocking*, karena pengguna harus melalui langkah tambahan (proses *knocking*). Namun, peningkatan waktu respons *server* itu sendiri hanya sekitar 2 detik, yang dianggap sangat minimal dan hampir tidak terasa oleh pengguna. Meskipun waktu tambahan untuk proses *knocking* memerlukan sekitar 5 menit, ini merupakan *trade-off* yang sangat dapat diterima demi peningkatan keamanan yang signifikan. Tingkat keberhasilan akses yang sah

tercatat sebanyak 19 dari 20 upaya, sehingga perhitungan tingkat keberhasilan akses menjadi 19 ÷ 20 = 0,95, atau setara dengan 95%. Akses yang tinggi ini juga menunjukkan bahwa metode ini tidak terlalu rumit bagi pengguna teknis (admin), sehingga memudahkan mereka dalam mengakses sistem dengan efisien.

4.2.3 Implikasi terhadap Keamanan Data Biometrik

Dengan mengamankan pintu masuk utama di BNN Kota Palangkaraya, data biometrik yang sensitif menjadi lebih terlindungi. Penyerang tidak dapat mengakses antarmuka yang mungkin memiliki celah untuk mengekstraksi atau memanipulasi data pengguna. *Port knocking* berfungsi sebagai "gerbang tak terlihat" yang melindungi aset data di belakangnya. Implikasi dari peningkatan keamanan ini sangat signifikan, terutama dalam konteks data biometrik yang bersifat sensitif dan pribadi. Perlindungan tambahan ini dapat meminimalkan risiko pencurian identitas dan penyalahgunaan data. Keberhasilan sistem ini dalam mencegah akses tidak sah turut meningkatkan kepercayaan pengguna terhadap sistem absensi yang menggunakan data biometrik, yang pada gilirannya dapat mendorong adopsi teknologi ini di berbagai sektor.

4.2.4 Waktu Respons Port Knocking

Waktu respons yang terkait dengan implementasi *port knocking* di BNN Kota Palangkaraya memiliki implikasi penting dalam pengalaman pengguna. Meskipun penambahan waktu sekitar 5 menit untuk proses *knocking* dapat dianggap sebagai pengorbanan kecil, penting untuk terus

memantau dan mengoptimalkan proses ini agar tidak mengganggu kenyamanan pengguna. Analisis lebih mendalam terhadap data waktu respons menunjukkan bahwa seiring pengguna terbiasa dengan prosedur *knocking*, waktu yang dibutuhkan untuk akses dapat berkurang lebih jauh. Pengguna yang sering menggunakan sistem cenderung lebih cepat mengingat urutan ketukan, sehingga meningkatkan efisiensi akses.

Hal ini menciptakan keseimbangan antara keamanan dan kecepatan akses, yang sangat penting dalam lingkungan kerja yang dinamis seperti di BNN. Jika waktu respons dapat dioptimalkan lebih lanjut, maka akan ada dampak positif terhadap produktivitas pengguna dan kepuasan mereka terhadap sistem. Oleh karena itu, penting untuk melakukan evaluasi berkala terhadap waktu respons dan mencari solusi yang dapat mengurangi waktu tersebut tanpa mengurangi tingkat keamanan.

4.2.5 Implikasi Keamanan dan Kepercayaan Pengguna

Penerapan metode *port knocking* di BNN Kota Palangkaraya tidak hanya memberikan perlindungan tambahan terhadap data biometrik, tetapi juga berkontribusi dalam membangun kepercayaan pengguna terhadap sistem. Kepercayaan ini sangat penting, terutama dalam konteks penggunaan data sensitif seperti data sidik jari. Pengguna yang merasa aman dan terlindungi akan lebih cenderung menggunakan sistem ini secara rutin.

Dengan pengurangan risiko akses tidak sah dan penyalahgunaan data, organisasi seperti BNN dapat lebih percaya diri dalam menerapkan teknologi biometrik dalam proses absensi dan pengelolaan data lainnya.

Keberhasilan dalam menciptakan lingkungan yang aman turut meningkatkan kepercayaan pengguna terhadap sistem, yang dapat menjadi faktor kunci dalam adopsi teknologi ini.

Selain itu, keberhasilan dalam menciptakan lingkungan yang aman juga dapat meningkatkan reputasi BNN di mata pengguna dan masyarakat umum. Hal ini, pada gilirannya, dapat berkontribusi pada peningkatan adopsi teknologi biometrik di berbagai sektor industri, di mana kepercayaan dalam penggunaan data sensitif menjadi sangat krusial.

4.2.6 Perbandingan *Port Knocking* Metode Keamanan Lain

Port knocking adalah salah satu dari berbagai metode keamanan yang dapat digunakan untuk melindungi sistem di BNN Kota Palangkaraya. Dibandingkan dengan *firewall* tradisional yang membuka *port* secara permanen, *port knocking* menawarkan lapisan keamanan tambahan dengan menyembunyikan *port* hingga urutan yang benar diberikan. Sementara VPN mengenkripsi seluruh lalu lintas jaringan, *port knocking* hanya membuka *port* tertentu setelah otentikasi yang benar, sehingga dapat lebih efisien dalam beberapa kasus. Namun, penting untuk dicatat bahwa *port knocking* tidak boleh menjadi satu-satunya lapisan keamanan; sebaiknya dikombinasikan dengan metode lain seperti otentikasi dua faktor (2FA) untuk perlindungan yang lebih komprehensif.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa penerapan sistem keamanan pada perangkat absensi sidik jari berbasis *web server* di BNN Kota Palangkaraya menggunakan metode *port knocking* efektif dalam melindungi data sensitif. Sistem ini mengurangi risiko akses tidak sah dan meningkatkan kepercayaan pengguna. Temuan ini menegaskan pentingnya langkah-langkah keamanan dalam menjaga integritas data di era digital, yang membuat pengguna merasa lebih aman dan menjalin relasi yang lebih kuat dengan penyedia layanan. Dengan analisis sebelumnya, kesimpulan dapat dijabarkan sebagai berikut:

a. Kerentanan Sistem

Sistem absensi sidik jari berbasis *web server* di BNN Kota Palangkaraya memiliki kerentanan tinggi sebelum intervensi keamanan, ditandai oleh terbukanya *port* layanan yang memungkinkan akses langsung dan potensi serangan dari pihak tidak berwenang di jaringan lokal.

b. Efektivitas Metode Port Knocking

Penerapan metode *port knocking* pada Router MikroTik efektif dalam menyembunyikan *port* layanan dari pemindaian jaringan, terbukti dengan perubahan status *port* dari OPEN menjadi FILTERED. Hal ini secara signifikan mempersulit identifikasi dan serangan oleh pihak luar.

c. Lapisan Keamanan Tambahan

Metode *port knocking* menciptakan lapisan keamanan tambahan yang dinamis dan tidak terlihat, hanya memberikan akses aman kepada pengguna yang mengetahui urutan ketukan yang benar, sambil memblokir semua upaya akses lainnya.

d. Dampak Terhadap Kinerja Sistem

Implementasi *port knocking* tidak menimbulkan dampak negatif signifikan terhadap kinerja sistem. Meskipun ada penambahan waktu singkat untuk proses "ketukan," latensi *server* tetap rendah setelah akses diberikan, sehingga *trade-off* antara keamanan dan kenyamanan pengguna dianggap sepadan.

5.2 Saran

Berdasarkan kesimpulan yang telah diuraikan, peneliti mengajukan beberapa saran untuk pengembangan sistem di BNN Kota Palangkaraya dan penelitian selanjutnya. Adapun peneliti memberikan beberapa saran sebagai berikut:

a. Saran untuk Pengembangan Sistem (Bagi BNN Kota Palangka Raya)

1) Meningkatkan Kompleksitas Sekuens

Untuk memperkuat keamanan, disarankan agar urutan ketukan lebih panjang, acak, dan diperbarui secara berkala untuk mencegah kebocoran sekuens.

2) Otomatisasi pada Sisi Klien

Kembangkan script atau aplikasi sederhana di sisi klien yang dapat secara otomatis mengirimkan urutan ketukan dengan satu kali klik, untuk

meningkatkan kenyamanan dan mengurangi potensi kesalahan pengguna.

3) Implementasi Pemantauan dan Peringatan Dini

Disarankan untuk mengaktifkan fitur pencatatan (*logging*) pada aturan *firewall* MikroTik untuk merekam semua upaya ketukan yang gagal. Data log ini dapat diintegrasikan dengan sistem notifikasi (email atau Telegram) untuk memberikan peringatan kepada administrator tentang aktivitas mencurigakan.

b. Saran untuk Penelitian Selanjutnya

1) Mengintegrasikan dengan Metode Enkripsi

Penelitian selanjutnya dapat mengeksplorasi penggabungan port knocking dengan teknik keamanan lain, seperti Single Packet Authorization (SPA), untuk mengenkripsi paket ketukan dan meningkatkan pertahanan terhadap serangan penyadapan. (*sniffing*).

2) Analisis Perbandingan Implementasi

Lakukan studi komparatif antara implementasi port knocking berbasis perangkat keras (misalnya MikroTik) dan berbasis perangkat lunak (seperti knockd pada server Linux dan Windows), dengan fokus pada kinerja, stabilitas, dan keamanan.

3) Uji Skenario Serangan Lanjutan

Lakukan pengujian terhadap skenario serangan kompleks, termasuk pemalsuan IP (IP spoofing) dan serangan pemutaran ulang (replay attack), untuk mengidentifikasi kelemahan dan merumuskan solusinya. Diharapkan sistem keamanan dapat terus ditingkatkan dan disesuaikan dengan perkembangan teknologi serta ancaman yang muncul.

DAFTAR PUSTAKA

Adhi Prasetio. (2020). *Basic Concepts of E-Commerce*. Tech Publishing.

Ahmad, et al. (2021). Implementasi Port Knocking dalam Sistem Absensi. *Jurnal Teknologi Informasi dan Komunikasi*, 7(1), 45-55.

Ali, M., et al. (2023). Combining Port Knocking and Encryption for Enhanced Security in Biometric Systems. *Journal of Information Security*, 15(1), 21-34.

Alghamdi, A., et al. (2021). Cybersecurity Challenges in Biometric Systems: A Review. *International Journal of Information Security*, 20(2), 123-139.

Chen, Y., & Liu, Z. (2023). A Comparative Study of Security Mechanisms in Web-Based Applications. *Security and Privacy*, 6(1), 45-62.

Daulay, A. (2020). *Komputer dan Jaringan Dasar untuk SMK/MAK Kelas X*. Gramedia Pustaka Utama, Jakarta.

Fahlevi, M.R., & Putri, D. (2021). Analisis Monitoring & Kinerja Sistem Keamanan Jaringan Komputer Menggunakan Nmap (Studi Kasus: Raz Hotel & Convention Medan). *IT (INFORMATIC TECHNIQUE) JOURNAL*, *9*(1), 35-43.

Halfond, W. G. J., Viegas, J., & Orso, A. (2006). A Classification of SQL Injection Attacks and Countermeasures. *International Symposium on Signals, Systems and Electronics*.

Junaidi, A., & Rahman, M. (2022). Implementing Port Knocking in Fingerprint-Based Authentication Systems. *Journal of Cybersecurity and Privacy*, 2(3), 145-157.

Kaur, R., & Kumar, S. (2022). Port Knocking: A Novel Approach for Securing Network Services. *Journal of Network and Computer Applications*, 192, 102-110.

Khan, M. S., & Alghamdi, A. (2020). Security Measures in Biometric Systems: A Review. *IEEE Access*, 8, 102123-102137.

Kumar, R., & Singh, A. (2020). Security in Biometric Systems. *International Journal of Computer Applications*, 975, 1-6.

Nuryakin Habillah, A. E., & Sidik. (2023). Implementasi Keamanan Jaringan Metode Port Knocking dan Port Blocking Berbasis Mikrotik PT Securindo Packatama Indonesia. *Jurnal Informatika dan Teknologi Komputer*, 4(1), 40–45. Diakses dari [https://ejurnalunsam.id/index.php/jicom/].

Patel, R., & Jain, S. (2020). Securing Biometric Data: Challenges and Solutions. *International Journal of Computer Applications*, 975, 1-6.

Rahi, S., et al. (2021). Impact of Data Security on Employee Trust in Organizations. *Journal of Business Ethics*, 169(3), 567-580.

Ruuhwan, & Kelvin Ajie Nugraha. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT: Information Communication & Technology*, 19(1), 1-8.

Sari, R. A. (2021). Analisis Keamanan Jaringan Menggunakan Firewall pada Sistem Absensi Berbasis Web. *Jurnal Teknologi Informasi dan Komunikasi*, 7(1), 45-55.

Smith, T. A., et al. (2021). Port Knocking as a Security Mechanism for Network Services. *Journal of Computer Networks*, 189, 107-115.

Zhang, L., et al. (2023). Effectiveness of Port Knocking in Securing Web Servers. *Journal of Information Technology and Security*, 12(2), 95-104.

L A M P I R A N

Lampiran 1. Surat Tugas penguji Tugas Akhir

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS PENGUJI TUGAS AKHIR

379/STMIK-3.C.2/AU/I/2026

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan kepada nama- nama berikut :

1. Nama : Elia Zakharia, M.T.
   NIK : 199205262016104
   Sebagai Ketua
2. Nama : Catharina Elmayantie, M.Pd
   NIK : 197610252015003
   Sebagai Sekretaris
3. Nama : Hotmian Sitohang, M.Kom
   NIK : 198503282008002
   Sebagai Anggota
4. Nama : Ir. Abdul Hadi, S.T., M.Kom
   NIK : 198505102021101
   Sebagai Anggota
5. Nama : H. Suratno, S.Kom., M.Si
   NIK : 196912281997101
   Sebagai Anggota

Untuk menguji Tugas Akhir mahasiswa :

Nama Mahasiswa	:	Nurul Aditya Kurniawan
N I M	:	C2155201054
Hari / Tanggal Ujian	:	Sabtu, 17 Januari 2026
Waktu	:	08.00 WIB
Judul TA	:	PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS WEB SERVER MENGGUNAKAN METODE PORT KNOCKING
Ruang	:	Sidang 2

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 12 Januari 2026

Ketua Program Studi Teknik Informatika,

Ir. ABDUL HADI, S.T., M.Kom
NIK. 198505102021101

Tembusan :
1. Dosen Penguji
2. Mahasiswa yang Bersangkutan
3. Arsip

Lampiran 2. Surat Tugas pembimbing Tugas Akhir

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT TUGAS

No.272/STMIK-3.C.2/KP/IX/2024

Ketua Program Studi Teknik Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya menugaskan nama- nama tersebut di bawah ini :

1. Nama : Abdul Hadi, S.T., M.Kom.
   NIK : 198505102021101
   Sebagai Pembimbing I Dalam Pembuatan Program
2. Nama : H. Suratno, S.Kom., M.Si.
   NIK : 196912281997101
   Sebagai Pembimbing II Dalam Penulisan Tugas Akhir

Untuk membimbing Tugas Akhir mahasiswa :

Nama	:	Nurul Aditya Kurniawan
NIM	:	C2155201054
Program Studi	:	TEKNIK INFORMATIKA (55201)
Tanggal Daftar	:	31 Agustus 2024
Judul Tugas Akhir	:	Penerapan Sistem Keamanan Pada Perangkat Absensi Sidik Jari Berbasis Web Server Menggunakan Metode Port Knocking

Demikian surat ini dibuat agar dapat dipergunakan sebagaimana mestinya dan dilaksanakan dengan penuh tanggung jawab.

Palangka Raya, 18 September 2024
Ketua Program Studi Teknik Informatika,

Lili Rusdiana, M.Kom.
NIK. 198707282011007

Tembusan :

1. Pembimbing I dan II
2. Mahasiswa yang bersangkutan
3. Arsip

Lampiran 3. Surat izin penelitian

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

Nomor : .038.../STMIK-C.2/AK.../XII/2025
Lampiran : -
Perihal : Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir

Kepada
Yth. **Kepala BNN Kota Palangka Raya**

Jl. Tangkasiang No. 14, Kel. Palangka, Kec. Jekan Raya,
Kota Palangka Raya, Kalimantan Tengah 74874

Dengan hormat,

Sehubungan dengan penyusunan Tugas Akhir mahasiswa sebagai persyaratan kelulusan Program Studi Teknik Informatika (S1) pada STMIK Palangkaraya, maka dengan ini kami sampaikan permohonan izin penelitian dan pengumpulan data bagi mahasiswa kami berikut:

Nama	:	NURUL ADITYA KURNIAWAN
NIM	:	C2155201054
Prodi (Jenjang)	:	Teknik Informatika (S1)
Thn. Akad. (Semester)	:	2025/2026 (9)
Lama Penelitian	:	26 Januari 2026 s.d 26 Februari 2026
Tempat Penelitian	:	BNN Kota Palangkaraya

Dengan judul Tugas Akhir:

PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS WEB SERVER MENGGUNAKAN METODE PORT KNOCKING

Adapun ketentuan dan aturan pemberian informasi dan data yang diperlukan dalam penelitian tersebut menyesuaikan dengan ketentuan/peraturan pada instansi Bapak/Ibu.

Demikian permohonan ini disampaikan, atas perhatian dan kerja samanya diucapkan terima kasih.

Palangka Raya, 22 Januari 2026

Ketua,

Ir. Hj. Siti Maryamah, MM.
NIK. 196902021995004

Lampiran 4. Surat Keterangan Telah Melakukan Penelitian

BADAN NARKOTIKA NASIONAL REPUBLIK INDONESIA
KOTA PALANGKA RAYA
Jalan Tangkasiang No. 14, Jekan Raya, Palangka Raya
Telepon : (0536) 3235816
Faksimili : (0536) 3235816
e-mail: bnnkota_palangkaraya@bnn.go.id website : palangkarayakota.bnn.go.id

BNN KOTA PALANGKA RAYA

Nomor : B/015/I/KA/PL.03.00/2026/BNNK
Klasifikasi : Biasa
Lampiran : -
Perihal : Surat Pemberian Izin Penelitian An. Nurul Aditya Kurniawan

Palangka Raya, 23 Januari 2026

Kepada

Yth. **Rektor STIMIK Palangka Raya**

di
Tempat

1. Rujukan :
   a. Undang-Undang Nomor 35 Tahun 2009 tentang Narkotika;
   b. Peraturan Presiden Nomor 47 Tahun 2019 tentang Perubahan atas Peraturan Presiden Nomor 23 Tahun 2010 tentang Badan Narkotika Nasional;
   c. Peraturan Badan Narkotika Nasional Nomor 1 Tahun 2022 tentang Perubahan atas Peraturan Badan Narkotika Nasional Nomor 5 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Narkotika Nasional;
   d. Surat Ketua STIMIK Palangka Raya Nomor : 038/STMIK-e.2/AK/XII/2025 Tanggal 22 Januari 2026 Perihal Permohonan Izin Penelitian dan Pengumpulan Data untuk Tugas Akhir An. Nurul Aditya Kurniawan.

Sehubungan dengan rujukan tersebut di atas, disampaikan bahwa kami pada prinsipnya memberikan izin Penelitian dan Pengumpulan Data untuk Tugas Akhir **An. Nurul Aditya Kurniawan Prodi Teknik Informatika (S1) pada tanggal 26 Januari 2026** di Kantor BNN Kota Palangka Raya dengan Judul Tugas Akhir : **PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS WEB SERVER MENGGUNAKAN METODE *PORT KNOCKING*.**

2. Demikian untuk menjadi maklum, atas perhatian dan kerja samanya diucapkan terima kasih.

Ditandatangani Secara Elektronik Oleh:
Kepala BNN Kota Palangka Raya

I WAYAN KORNA, S.E., M.H.

Tembusan :
1. Kepala BNN;
2. Sekretaris Utama BNN;
3. Inspektur Utama BNN;
4. Kepala BNNP Kalteng.

Dokumen ini telah ditandatangani secara elektronik menggunakan Sertifikat Elektronik yang dikeluarkan oleh Balai Besar Sertifikasi Elektronik (BSrE), BSSN.

Lampiran 5. Berita acara penilaian sidang TA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

BERITA ACARA
UJIAN TUGAS AKHIR

Periode : Januari 2026

Pada hari ini Sabtu, 17 Januari 2026 Pukul 08.00 WIB sampai dengan ..... WIB telah dilaksanakan Ujian Tugas Akhir mahasiswa atas nama :

Nama Mahasiswa	:	Nurul Aditya Kurniawan
N I M	:	C2155201054
Program Studi	:	Teknik Informatika
Tahun Angkatan	:	2021
Judul TA	:	PENERAPAN SISTEM KEAMANAN PADA PERANGKAT ABSENSI SIDIK JARI BERBASIS WEB SERVER MENGGUNAKAN METODE PORT KNOCKING

Dosen Penguji :

	Nama		Nilai	Tanda Tangan
1.	Elia Zakharia, M.T	=	.....	(.....)
2.	Catharina Elmayantie, M.Pd	=	.....	(.....)
3.	Hotmian Sitohang, M.Kom	=	.....	(.....)
4.	Ir. Abdul Hadi, S.T., M.Kom	=	.....	(.....)
5.	H. Suratno, S.Kom., M.Si	=	.....	(.....)

Hasil Ujian : **LULUS / ~~TIDAK LULUS~~** *) NILAI = ... 79,97 .....

Revisi (~~Tidak Ada~~ / Minor / ~~Mayor~~ *)

Catatan Penting :
1. Lama Perbaikan : ..... 10 ..... hari
2. Jika lebih dari 1 (satu) bulan dikenakan sanksi berupa denda sebesar Rp. 600.000,- (Enam ratus ribu rupiah) per bulan dari tanggal ujian.
3. Jika lebih dari 3 (tiga) bulan dari tanggal ujian maka hasil ujian dibatalkan dan wajib mengajukan judul dan pembimbing baru.

Demikian Berita Acara ini dibuat, agar dapat digunakan sebagaimana semestinya.

Palangka Raya, 17 Januari 2026

Ketua Penguji,

Elia Zakharia, M.T
NIK. 199205262016104

Mahasiswa,

Nurul Aditya Kurniawan
NIM. C2155201054

Mengetahui :
Ketua Program Studi Teknik Informatika,

Ir. Abdul Hadi, S.T., M.Kom
NIK. 198505102021101

Lampiran 6. Lembar Kartu konsultasi bimbingan TA

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangkaraya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

KARTU KEGIATAN KONSULTASI TUGAS AKHIR

Nama Mahasiswa : NURUL ADITYA KURNIAWAN
NIM : C21552010 54
Tanggal Persetujuan Judul : 18 September 2024
Judul Tugas Akhir : Penerapan Sistem Keamanan Pada Perangkat APsensi Sidik JARI Berbasis Web Server menggunakan metode Port knocking

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	05-10-2024		Pengarahan Penulisan Isi BAB Proposal TA	
		04-11-2024	Perbaikan Bab 1 dan 2 Kalimat Penulisannya	
	27-02-2025		Perbaikan Isi Bab 1 Bab 2 Susunan Penulisannya	
		28-02-2025	Perbaikan Bab 2 Penelitian Relevan Jurnal PdF diTabel	
	20-03-2025		Pengumpulan Perbaikan Bab 3 Desain Alur Penelitian, Desain Jaringan sebelum, sesudah	
		26-03-2025	Perbaikan Desain Gambar Topologi Jaringan	
	19-04-2025		Pengampulan Hasil Perbaikan Bab 3 desain Jaringan dan Alur Desain Penelitian	
		21-04-2025	Perbaikan Desain Jaringan sesudah dan sebelum di Prodi TI. Desain Topologi Awal dan Akhir.	
	16-5-2025		Acc Seminar	
	26-04-2025		Perbaikan kurikum sesuai Buku Rekomen	
	10-5-25		atur tata penulisan	
	12-05-2025		acc	

No.	Tanggal Konsultasi		Uraian	Tanda Tangan
	Terima	Kembali		
	14-06-2025		Penulisan BAB 4-5 menyusun Penulisan isi BAB 4-5	
	26-06-2025		Konsul Penulisan Revisi Perbaikan BAB 4-5	
		28-09-2025	Ujicoba Alat konfigurasi mikrotik	
	29-09-2025		Revisi Penulisan bab 4-5	
	9/12/2025		perbaiki Struktur penulisan bab 4	
		10/12/2025	konsul Perbaikan Penulisan bab 4	
	8/12/2025		Revisi alur bab 4	
	14/12/2025		Demo via zoom port forking	
	19/12/25		perbaiki penulisan substansi, jangan seperti tutorial	
	13/12/25		- penomoran Halaman diuruntkan - penomoran Gambar agar diuraikan dan tidak ada yg dobel	
	22/12/25		- perbaiki penomoran Halaman u/ bab 5, uruntkan dgn nomor halaman sebelumnya - lengkapi gambar yg belum ada	
	5/1/26		Acc sidang	
	10/1/26		Acc Sidang	

Menyetujui :

Dosen Pembimbing I,

Reski Syafitra, S.Kom., M.Kom

Dosen Pembimbing II,

Lampiran 7. Observasi (Pengamatan Di Lokasi BNN Kota Palangkaraya)

Bukti Dokumentasi foto di lokasi BNN Kota Palangkaraya.



Melakukan Ujicoba Akses Mikrotik Ke Perangkat Absensi Sidik Jari Web Server.



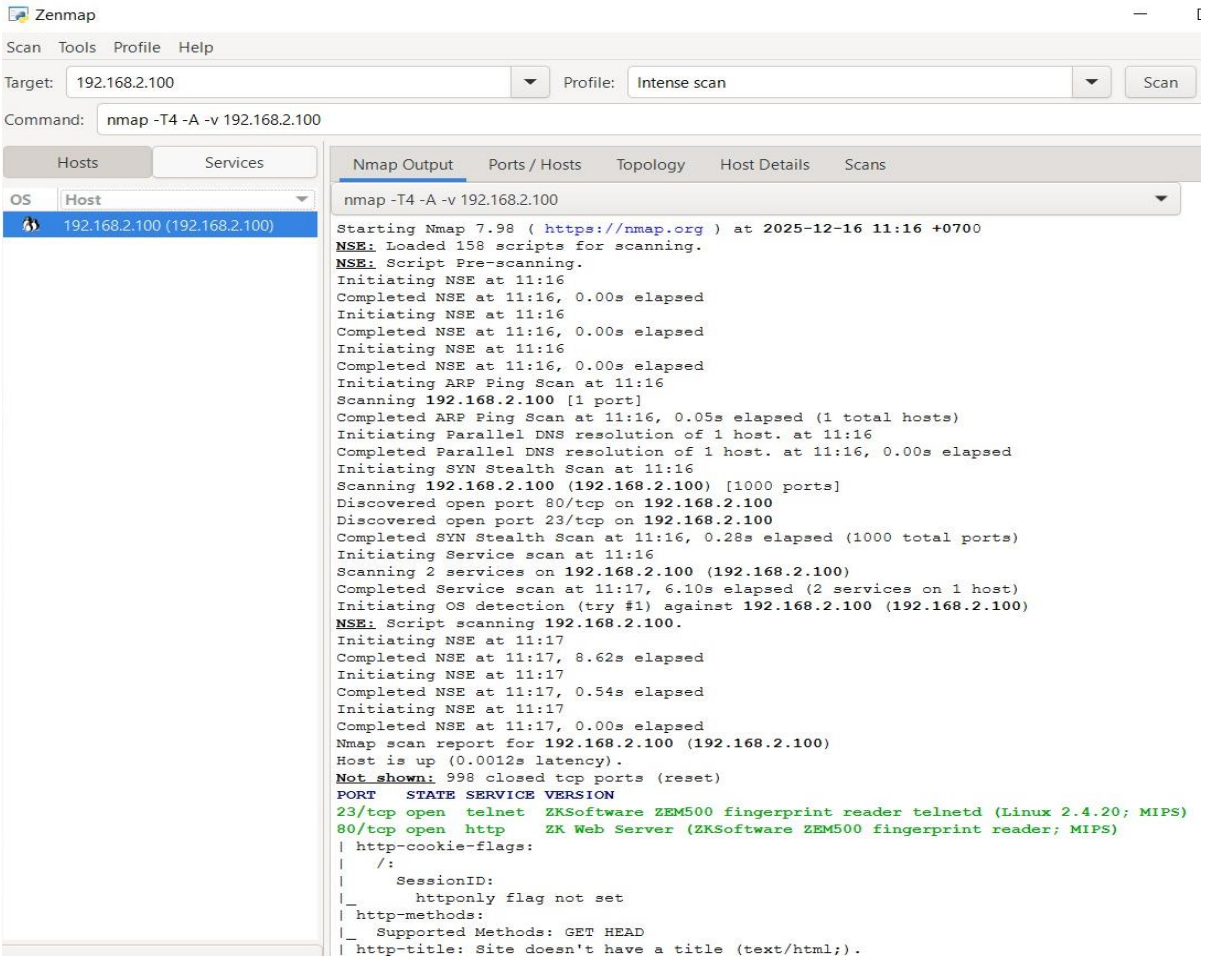


Depan Kantor BNN KOTA PALANGKA RAYA

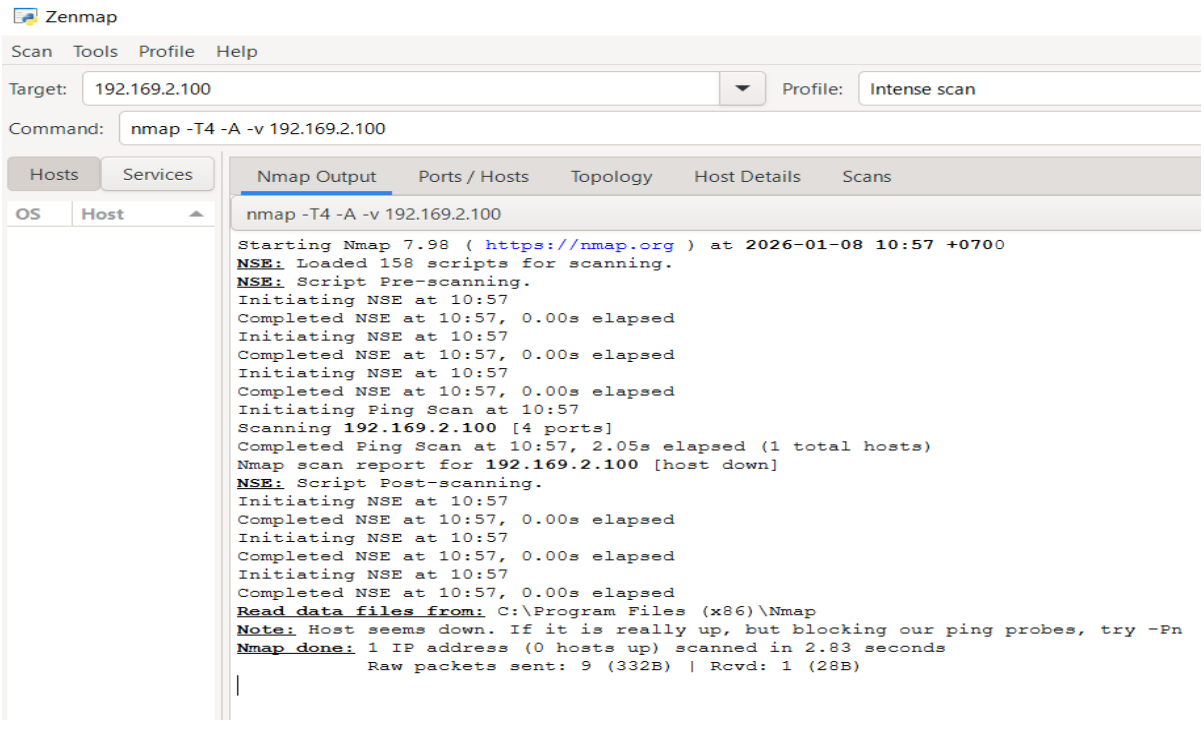


Lampiran 8. Tampilan Hasil temuan kerentanan megunakan Nmap

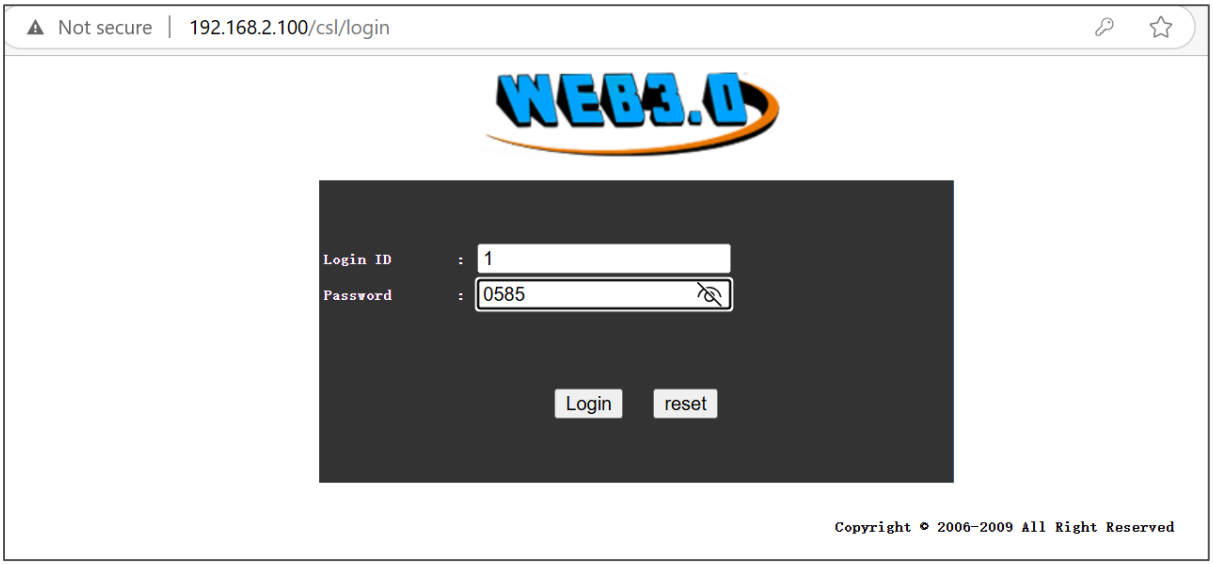
sebelum Penerapan Port Knock temuan kerentanan port 80 dan port 23.

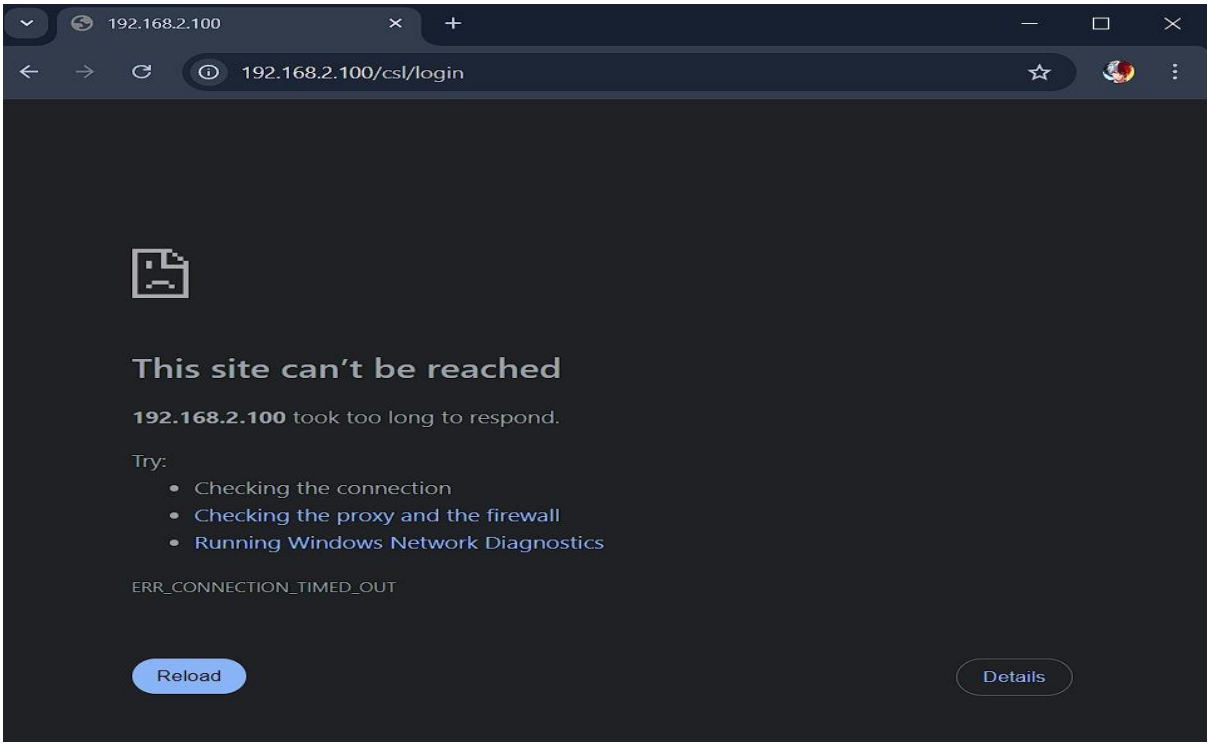


sedusah Penerapan Port Knocking hasil akses hoat sistem down akses but blocking.

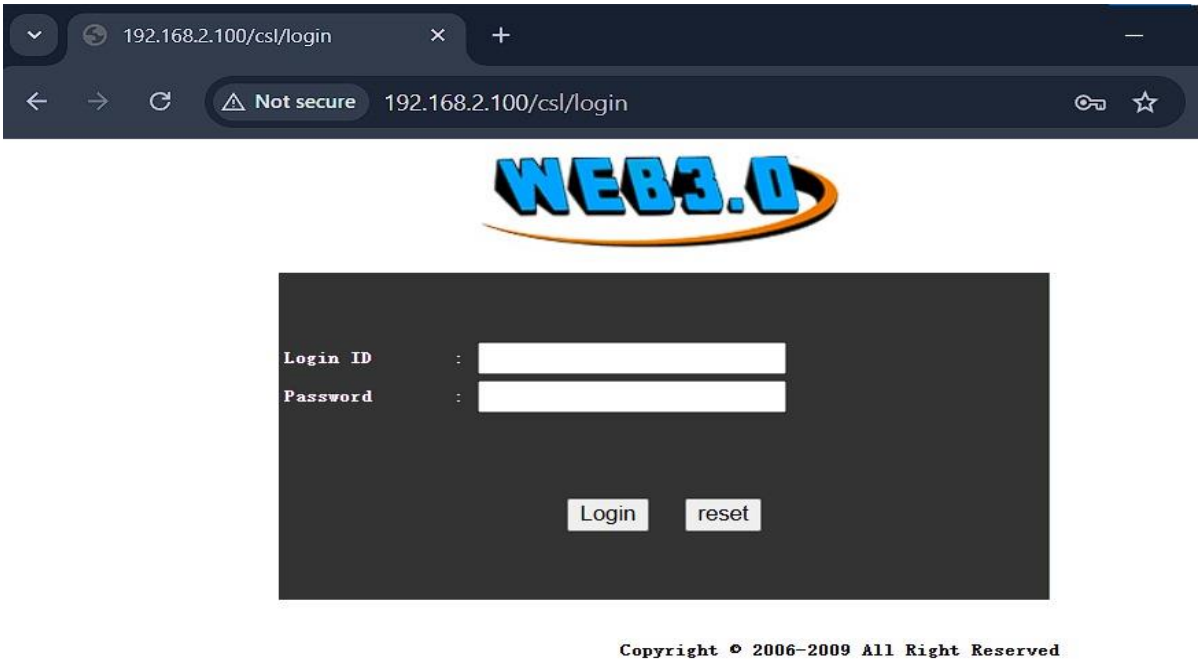


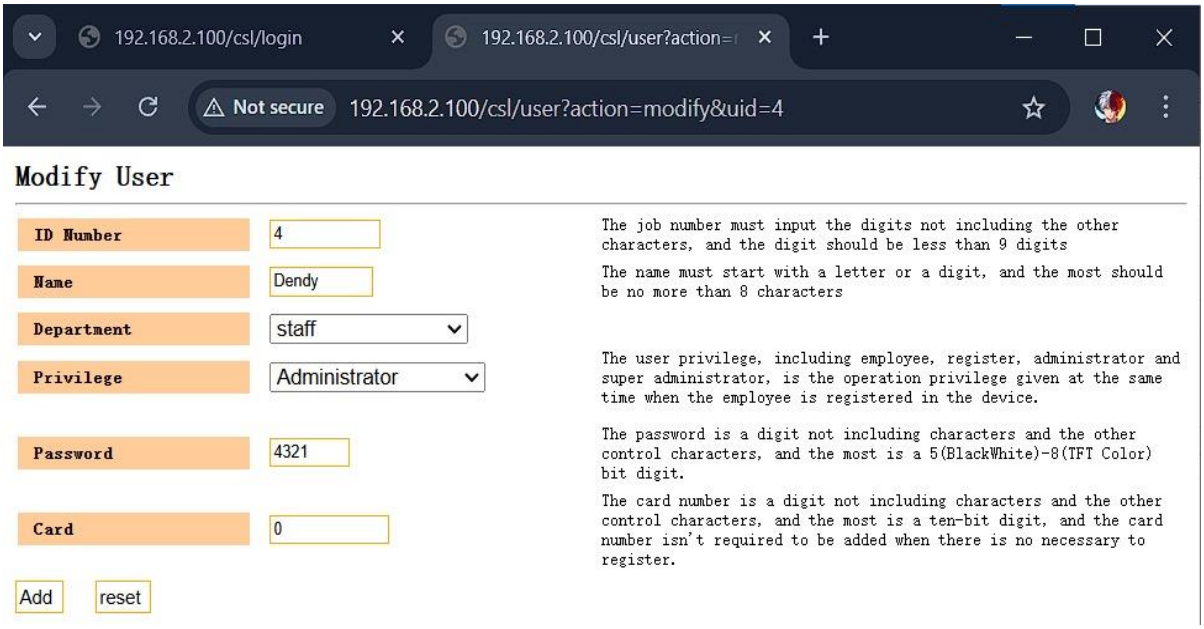
Lampiran 9. Tampilan *Login* Normal dan Anomali





Lampiran 10. Tampilan Browser HTTP URL Khusus Normal dan Anomali





Lampiran 11. Tampilan Kondisi Normal dan Kondisi Anomali

