IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN *SECURITY POLICY DEVELOPMENT LIFE CYCLE*

(Studi Kasus : Kantor DPRD Kabupaten Pohuwato)

Oleh : FAISAL ALAMRI
T3119045 SKRIPSI

PROGRAM SARJANA FAKULTAS ILMU KOMPUTER
UNIVERSITAS ICHSAN GORONTALO GORONTALO
2024

PERSETUJUAN SKRIPSI

IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN *SECURITY POLICY DEVELOPMENT LIFE CYCLE*

(Studi Kasus : Kantor DPRD Kabupaten Pohuwato)

Oleh

FAISAL ALAMRI

T3119045

SKRIPS

Untuk memenuhi salah satu syarat
ujian Guna memperoleh gelar
Sarjana Program Studi Teknik
Informatika

Pembimbing I	Pembimbing II
Irvan Abraham Salihi, M.Kom	**Zulfrianto Y. Lamasigi, M.Kom**
NIDN : 0928028101	**NIDN: 0914089101**

PENGESAHAN SKRIPSI

IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN *SECURITY POLICY DEVELOPMENT LIFE CYCLE*

(Studi Kasus : (Studi Kasus : Kantor DPRD Kabupaten Pohuwato)

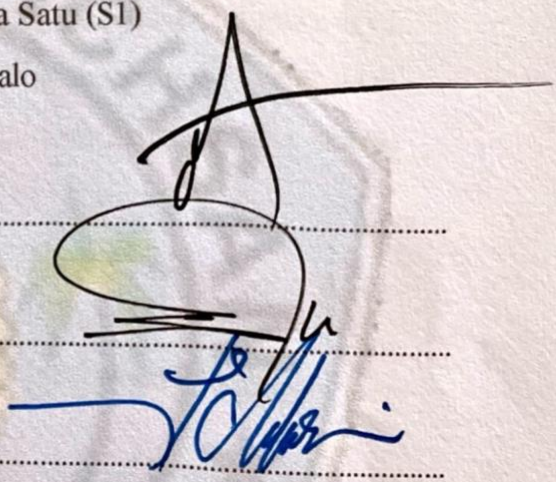
Oleh

FAISAL ALAMRI

T3119045

Diperiksa oleh Panitia Ujian Strata Satu (S1)

Universitas Ichsan Gorontalo

1. Ketua penguji
   Sudirman Panna, M.Kom ..... 
2. Anggota
   Sunarto Taliki, M.Kom .....
3. Anggota
   Serwin, M.Kom .....
4. Anggota
   Irvan Abraham Salihi, M.Kom .....
5. Anggota
   Zufrianto Y. Lamasigi, M.Kom .....

Dekan Fakultas Ilmu Komputer

Irvan A. Salihih M.Kom

NIDN : 0928028101

Ketua Program Studi

Sudirman S. Panna M.Kom

NIDN : 0924038205

PERNYATAAN SKRIPSI

Dengan ini saya menyatakan bahwa :

1. Karya tulis (Skripsi) saya ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana) baik di Universitas Ichsan Gorontalo maupun diperguruan tinggi lainnya.
2. Karya tulis (Skripsi) saya ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan dari Tim Pembimbing.
3. Karya tulis (Skripsi) saya ini tidak lain, kecuali secara tertulis dicantumkan sebagai acuan/sitasi dalam naska dan dicantumkan pula dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar, yang telah diperoleh karena karya tulis ini, serta sanksi lainnya dengan norma-norma yang berlaku di Universitas Ichsan Gorontalo.

Gorontalo, Desember 2024

Membuat Pernyataan,

Faisal Alamri

ABSTRAK

FAISAL ALAMRI. T3119045. IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN *SECURITY POLICY DEVELOPMENT LIFE CYCLE*

Bot Telegram menjadi solusi yang praktis dan efisien untuk monitoring dan manajemen jaringan Mikrotik. Penelitian ini bertujuan untuk mengimplementasikan sistem monitoring jaringan dan kontrol server berbasis bot Telegram dengan pendekatan Security Policy Development Life Cycle (SPDLC). Sistem dirancang untuk mendeteksi ancaman keamanan, seperti serangan brute force SSH, melalui analisis log pada perangkat Mikrotik, serta memberikan notifikasi real-time kepada admin melalui bot Telegram. Hasil penelitian menunjukkan bahwa sistem yang dibangun mampu mendeteksi ancaman secara efektif, mengirimkan notifikasi tepat waktu dengan informasi yang akurat, dan menyediakan fitur kontrol yang responsif melalui perintah Telegram.

Kata kunci: bot telegram, Mikrotik, monitoring, Security Policy Development Life Cycle, Brute Force SSH

ABSTRACT

FAISAL ALAMRI. T3119045. THE IMPLEMENTATION OF TELEGRAM BOT MESSAGES FOR NETWORK MONITORING AND SERVER CONTROL USING THE SECURITY POLICY DEVELOPMENT LIFE CYCLE APPROACH

Telegram bot is a practical and efficient solution for monitoring and managing Mikrotik networks. This study aims to implement a network monitoring and server control system based on Telegram bots with the Security Policy Development Life Cycle (SPDLC) approach. The designed system detects security threats, such as SSH brute force attacks, through log analysis on Mikrotik devices and provides real-time notifications to admins via Telegram bots. This study's results show that the system can detect threats effectively, send timely notifications with accurate information, and provide responsive control features via Telegram commands.

Keywords: telegram bot, Mikrotik, monitoring, Security Policy Development Life Cycle, SSH Brute Force

KATA PENGANTAR

Alhamdulillah, penulis dapat menyelesaikan skripsi ini dengan judul "**IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN SECURITY POLICY DEVELOPMENT LIFE CYCLE** " Pada Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.

Penulis menyadari sepenuhnya bahwa skripsi ini tidak mungkin terwujud tanpa bantuan dan dorongan dari berbagai pihak, baik bantuan moril maupun materil. Untuk itu, dengan segala keikhlasan dan kerendahan hati, penulis mengucapkan banyak terima kasih dan penghargaan yang setinggi-tingginya kepada :

1. Ibu Dr. Dra Juriko Abdussamad, M.si, selaku Ketua Yayasan Pengembangan Ilmu Pengetahuan dan Teknologi (YPIPT) Ichsan Gorontalo;
2. Bapak Dr. Abdul Gaffar La Tjokke, M.si, selaku Rektor Universitas Ichsan Gorontalo;
3. Bapak Irvan Abraham Salihi, M.Kom, selaku Dekan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo Sekaligus Pembimbing Utama yang telah memberikan bimbingan dan arahan kepada penulis untuk menyelesaikan Skripsi ini;
4. Bapak Sudirman Melangi, M.Kom, selaku Wakil Dekan I Bidang Akademik Fakultas Ilmu Komputer Universitas Ichsan Gorontalo;
5. Ibu Irma Surya Kumala Idris, M.Kom, selaku Wakil Dekan II Bidang Administrasi Umum dan Keuangan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo;
6. Bapak Sudirman S. Panna, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo;
7. Zulfrianto Y. Lamasigi, M.Kom, selaku Pembimbing II, yang telah memberikan bimbingan dan arahan kepada penulis untuk menyelesaikan Skripsi ini;

8. Bapak dan Ibu Dosen Universitas Ichsan Gorontalo yang telah mendidik dan mengajarkan berbagai disiplin ilmu kepada penulis;
9. Kedua orang tua saya yang tercinta, atas segala kasih sayang, jerih payah, doa restu serta telah mendukung penulis mencapai cita-cita untuk menjadi seorang sarjana;
10. Rekan-rekan seperjuangan yang telah banyak memberikan bantuan dan dukungan moril yang sangat besar kepada penulis;
11. Kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini tak sempat penulis sebutkan satu-persatu.

Semoga Allah SWT melimpahkan balasan atas jasa-jasa mereka kepada kami. Penulis menyadari sepenuhnya bahwa apa yang telah dicapai ini masih jauh dari kesempurnaan dan masih banyak terdapat kekurangan. Oleh karena itu, penulis sangat mengharapkan adanya kritik dan saran yang konstruktif. Akhirnya penulis berharap semoga hasil yang telah dicapai ini dapat bermanfaat bagi kita semua, Aamiin.

Gorontalo, Desember 2024

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan merupakan salah satu masalah terbesar bagi pengguna internet terutama penyedia sebuah server maupun sistem jaringan komputer, dalam sebuah jaringan tentunya memerlukan *administrator* sebagai pemantauan *server* dengan melihat kinerja *server* yang sedang berjalan. Apabila tidak ada sistem yang baik pada jaringan, maka serangan dapat dengan mudah menyerang jaringan tersebut. Serangan berikut dilakukan oleh penyerang melalui paket jaringan untuk mendapatkan informasi dari jaringan yang diserang dan juga menyebabkan komputer menjadi *crash*. Serangan dilakukan dengan mencari *port* terbuka di *server* dan kemudian melakukan serangan pada jaringan tersebut. [1]

Monitoring jaringan komputer merupakan proses untuk pengumpulan data dan melakukan sebuah analisis terhadap sebuah data pada lalu lintas jaringan dengan tujuan untuk memperbaiki kelemahan sistem yang ada pada jaringan komputer [1]. Agar kegiatan yang dilakukan melalui jaringan internet selalu berjalan dalam keadaan lancar, maka digunakan sebuah mekanisme monitoring jaringan untuk mengontrol jaringan yang berada pada wilayah atau area yang memanfaatkan topologi jaringan tertentu. Monitoring jaringan dapat mempermudah seorang teknisi atau administrator dalam memantau sistem jaringan [2].

Salah satu yang digunakan untuk memonitoring jaringan adalah server mikrotik yang terintegrasi dengan social media Telegram. Mikrotik router operating system (OS) adalah sistem operasi maupun perangkat lunak yang berfungsi membuat komputer menjadi router network yang dilengkapi dengan fitur untuk IP Network maupun jaringan *wireless*. Monitoring jaringan tentunya menggunakan Model Referensi OSI Layer, Osi layer yang digunakan dalam monitoring jaringan yaitu *Data Link Layer, Network Layer, Session Layer dan Aplication Layer* [2].

Dewan Perwakilan Rakyat Daerah (DPRD) Kabupaten Pohuwato adalah salah satu lembaga legislative unicameral yang berkedudukan di Kabupaten Pohuwato, Provinsi Gorontalo. DPRD Kabupaten Pohuwato merupakan lembaga perwakilan rakyat yang dipilih langsung oleh rakyat Kabupaten Pohuwato pada pemilihan umum legislative setiap lima tahun sekali. DPRD Kabupaten Pohuwato memiliki jaringan internet dengan bandwidth 100 Mbps dengan pengguna meliputi karyawan atau staf yang bekerja di DPRD Kabupaten Pohuwato. Penggunaan internet di DPRD Kabupaten Pohuwato saat ini memiliki akses yang cukup tinggi, untuk itu perlu adanya optimasi jaringan salah satu nya yaitu dengan cara melakukan management user serta bandwidth pada jaringan DPRD Kabupaten Pohuwato dengan menggunakan hostpot pada mikrotik dengan jumlah perangkat wireless yang berjumlah 20 perangkat.

Staf admin yang bertugas mengelolah jaringan komputer dan server mikrotik pada Kantor DPRD Kabupaten Pohuwato mengalami beberapa permsalahan dalam memonitoring perangkat jaringan wireless dan server mikrotik jika terjadi masalah, selama ini staf harus mengecek langsung jika terjadi permsalahan jaringan dimana hal ini menjadi masalah jika staf berada diluar kantor. Pemasalahn lain yaitu system jaringan yang tidak aman, adanya penyusup yang berusaha masuk kejaringan komputer dan server mikrotik yang tidak dapat terdeksi oleh staf karena tidak adanya informasi yang diterimah oleh staf dikarenakan tidak adanya sistem pemberiathuan yang oleh staf admin jaringan pada kantor DPRD Kab. Pohuwato

Oleh karena itu, perlu adanya monitoring keamanan jaringan dengan tujuan meminimalisir jika terjadinya percobaan penyusupan atau percobaan intrusi. Salah satu aplikasi yang digunakan IDS (Intrusion Detection System) adalah Snort. Aplikasi open source tersebut memiliki kemampuan mendeteksi adanya penyusupan terhadap sistem keamanan jaringan yang sesuai dengan aturan (rule) yang telah ditetapkan didalam IDS (Intrusion Detection System). Peringatan deteksi adanya penyusupan atau percobaan intrusi tersebut dapat memanfaatkan aplikasi instant messaging sebagai media untuk memberitahu kepada seorang Administrator didalam jaringan komputer jika terdapat indikasi penyusupan yang terjadi pada server di dalam jaringan komputer serta dapat dilakukan antisipasi penanganan

awal dengan kontrol langsung terhadap server secara real time. Aplikasi instant messaging saat ini populer digunakan oleh berbagai kalangan. Salah satu aplikasi tersebut yang memiliki berbagai fitur adalah Telegram. [3]

Pada penelitian ini penulis memanfaatkan bot telegram sebagai media notifikasi ketika adanya gangguan perangkat wireless atau masalah pada server mikrotik. Diketahui bahwa telegram sebagai salah satu aplikasi instant messaging, dan sangat populer pada saat ini, mengklaim dapat menutupi beberapa kekurangan yang ada pada aplikasi lain. Telegram merupakan aplikasi cloud based dan alat enkripsi, telegram. Menyediakan enkripsi end-to-end, self destruction messages, dan infrastruktur multi-data center. Selain itu telegram juga menyediakan wadah bagi pengembang yang ingin memanfaatkan Open API dan Protocol yang disediakan melalui pengembangan telegram bot yang didokumentasikan pada web resminya. [4]

Keamanan jaringan komputer sangat penting untuk memberikan perlindungan sistem atas gangguan yang mungkin timbul, baik gangguan dari dalam maupun dari luar jaringan komputer terutama kondisi perangkat jaringan komputer. Monitoring jaringan dilakukan untuk memastikan keamanan jaringan dari berbagai gangguan. Security Policy Development Life Cycle (SPDLC) merupakan salah satu metode dalam pengembangan keamanan jaringan komputer. SPDLC adalah metode yang menetapkan strategi untuk melakukan pembaharuan suatu organisasi dari sistem jaringan, siklus pengembangan sistem jaringan didefinisikan pada sejumlah fase. Strategi yang dilakukan untuk memastikan kondisi perangkat jaringan yaitu mengimplementasikan bot telegram menggunakan SPDLC pada sistem monitoring yang dibangun dengan menerapkan mikrotik dalam jaringan area lokal sehingga informasi gangguan jaringan komputer diperoleh secara efektif dan efisien. [5]

Terdapat penelitian tentang monitoring jaringan komputer. Penelitian dilakukan oleh Faris Jawad dkk, 2023. dengan judul Optimalisasi Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi. Untuk metode pengembangan sistem informasi penulis menggunakan metode waterfall dengan beberapa basic dari fundamental keamanan jaringan dan ketentuan keamanan

jaringan dan data. Bertujuan untuk memanfaatkan sumber daya internet dan memaksimalkan bandwidth yang tersedia agar lebih effisien dan stabil [6].

Kemudian pada penelitian tentang Security Policy Development Life Cycle (SPDLC) dilakukan oleh Muhammad Jufri, Heryanto, 2021. dengan judul Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall. Metode penelitian yang digunakan adalah Security Policy Development Life Cycle (SPDLC) dengan melewati beberapa tahapan, yaitu:. Analysis, Desain, Implementation, Enforcement, Enchancement. Hasil penelitian menyimpulkan bahwa serangan yang dilakukan oleh penyerang pada jaringan dapat diketahui dan ditangani sebelum kerusakan yang lebih luas terjadi serta penggunaan wireshark yang dapat menganalisa serangan dengan baik melalui flow graph yang disediakan. [6]

Berdasarkan latar belakang, maka penulis mengangkat judul **"Implementasi Pesan Bot Telegram Untuk Monitoring Jaringan Dan Kontrol Server Dengan Pendekatan *Security Policy Development Life Cycle"***. (Studi Kasus : Kantor DPRD Kabupaten Pohuwato).

1.2 Identifikasi masalah

Berdasarkan uraian latar belakang masalah di atas, maka identifikasi masalahnya adalah perlunya Implementasi Pesan Bot Telegram Untuk Monitoring Jaringan Dan Kontrol Server Dengan Pendekatan *Security Policy Development Life Cycle*.

1.3 Rumusan masalah

Berdasarkan identifikasi masalah diatas, maka rumusan permasalahannya adalah Bagaimana hasil Implementasi Pesan Bot Telegram Untuk Monitoring Jaringan Dan Kontrol Server Dengan Pendekatan *Security Policy Development Life Cycle*?

1.4 Tujuan Penelitian

Berdasarkan Rumusan permasalahan diatas, maka tujuan dari penelitian ini adalah Untuk Mengetahui Hasil Implementasi Pesan Bot Telegram Untuk

Monitoring Jaringan Dan Kontrol Server Dengan Pendekatan *Security Policy Development Life Cycle*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan mempunyai manfaat, yaitu

1. Secara Teoritis, Memberikan masukan bagi perkembangan ilmu pengetahuan dan teknologi, khususnya pada bidang ilmu computer, yaitu berupa implementasi pesan bot telegram untuk monitoring jaringan komputer.
2. Secara Praktis, Sumbangan pemikiran, karya, bahan pertimbangan agar dapat menghasilkan system yang berkualitas.

BAB II
LANDASAN TEORI

2.1. Tinjauan Studi

Berikut ini adalah penelitian terdahulu yang terkait dengan Monitoring Jaringan, yaitu :

Tabel 2. 1 Penelitian Terkait

No	Peneliti	Judul	Tahun	Hasil
1.	Faris Jawad dkk. [4]	Optimalisasi Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi	2023	Untuk metode pengembangan sistem informasi penulis menggunakan metode waterfall dengan beberapa basic dari fundamental keamanan jaringan dan ketentuan keamanan jaringan dan data. Bertujuan untuk memanfaatkan sumber daya internet dan memaksimalkan bandwidth yang tersedia agar lebih effisien dan stabil
2.	Muhammad Jufri, Heryanto, [5]	Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall	2021	Metode penelitian yang digunakan adalah Security Policy Development Life Cycle (SPDLC) dengan melewati beberapa tahapan, yaitu:. Analysis, Desain, Implementation, Enforcement, Enchancement. Hasil penelitian menyimpulkan bahwa serangan yang dilakukan oleh penyerang pada jaringan dapat diketahui dan ditangani sebelum kerusakan yang lebih luas terjadi serta penggunaan wireshark yang dapat

				menganalisa serangan dengan baik melalui flow graph yang disediakan.
3.	Julianto Dkk. [6]	Analisis Keamanan Jaringan Mikrotik ISP Indonesia Menggunakan Search Engine Scada Shodan	2020	Dengan Metode Exploit Winbox Critical Vulnerability bahwa mikrotik mempunyai celah keamanan yang dikenal dengan CVE-2018-14847 yang kerentanannya memungkinkan alat khusus untuk menyambung ke port winbox dan meminta file database pengguna sistem mikrotik

2.2. Tinjauan Pustaka

2.2.1. Monitor Jaringan

Monitor jaringan adalah sebuah kegiatan admin dalam memantau, merawat dan menjaga jaringan supaya selamanya di dalam kondisi yang maksimal. Keseluruhan kondisi dan kesibukan jaringan perlu diketahui dan terkontrol oleh seorang admin jaringan. Monitoring jaringan juga dapat mengumpulkan dan menganalisa data-data yang tersedia dalam suatu lalu lintas jaringan dengan objek memaksimalkan seluruh sumber kekuatan yang tersedia terhadap Jaringan Komputer tersebut [5]

2.2.2. Instant Messaging Telegram

Instant Messaging Telegram adalah sebuah perangkat lunak atau aplikasi saat ini yang sangat populer di kalangan masyarakat. Tujuan utama aplikasi tersebut yaitu menyajikan fitur obrolan yang berjalan secara real time sehingga pesan langsung dapat terkirim dan diterima. Aplikasi instant messaging berjalan secara online atau dengan kata lain membutuhkan koneksi Internet. Saat ini terdapat banyak aplikasi instant messaging yang digunakan oleh masyarakat untuk mengobrol dengan individu maupun komunitas. Fitur yang disajikan aplikasi

tersebut tidak hanya melalui text based saja, tetapi bisa juga untuk melakukan obrolan melalui suara, bertukar foto, audio, video hingga dokumen digital. Salah satu aplikasi yang memiliki fitur tersebut yaitu Telegram.

Telegram secara definisi menurut telegram.org merupakan alternatif layanan aplikasi perpesanan untuk ponsel (mobile) maupun desktop yang berbasis cloud dengan keamanan tingkat tinggi serta kecepatan aksesnya. Aplikasi instant messaging tersebut tersedia untuk berbagai device seperti ponsel yang berjalan pada system operasi Android, iOS, Windows Phone. Tidak hanya berjalan pada perangakt mobile, tetapi juga dapat berjalan system desktop seperti Windows dan Linux. Meskipun terlihat sederhana aplikasi instant messaging Telegram memiliki fitur yang lebih unggul dibandingkan aplikasi instant messaging lainnya. Telegram diklaim sebagai aplikasi yang aman dimana menyediakan pilihan pesan end-to-end yang akan di enskripsi [3].

2.2.3. Telegram Bot API

Telegram Bot API (Application Progamming Interface) adalah sebuah perangkat lunak atau aplikasi yang digunakan untuk berinteraksi antara Bot dengan penggunannya maka dari itu dibutuhkanlah sebuah API [5]. Bot tersebut dapat melakukan beberapa pekerjaan yaitu:

1. Mengintegrasikan dengan layanan lainnya, Bot dapat mengirimkan komentar jarak jauh atau mengendalikan smart home. Selain itu, bot juga mampu mengirimkan pemberitahuan melalui Telegram ketika terjadi sesuatu di suatu tempat
2. Menciptakan alat khusus, Bot mampu memberikan pemberitahuan maupun memberikan sebuah peringatan, ramalan cuaca, terjemahan, atau layanan lain.
3. Membangun single player ataupun multiplayer game, Keunggulan lainnya yaitu bot mampu memainkan permainan seperti catur.
4. Membangun layanan social, Sebuah bot dapat menghubungkan orang-orang untuk mencari mitra percakapan berdasarkan kepentingan bersama

2.2.4. Snort

Snort merupakan aplikasi atau perangkat lunak berbasis opensource yang memiliki keunggulan untuk mengetahui adanya indikasi penyusupan pada jaringan berbasis TCP/IP secara real time (Mutaqin, 2016). Jika terindikasi adanya penyusupan, Snort akan melakukan pencatatan atau logging terhadap paket-paket yang telah terdeteksi sebagai intrusi berdasarkan aturan yang telah ditetapkan [5].

2.2.5. Keamanan Jaringan

Keamanan jaringan merupakan suatu cara pengamanan jaringan agar dapat terhindar dari berbagai ancaman yang berasal dari jaringan luar dan bertujuan untuk merusak atau mencuri data. Oleh karena itu, Anda harus mengambil tindakan pencegahan untuk menghadapi ancaman ini. Pertahanan dapat diimplementasikan melalui firewall, deteksi melalui IDS (Intrusion Detection System) dan kombinasi keduanya melalui IPS (Intrusion Prevention System) [5].

Jaringan komputer merupakan kumpulan sejumlah besar komputer otonom yang saling berhubungan. Secara umum jaringan komputer dapat digambarkan sebagai kumpulan komputer yang dihubungkan oleh media perantara. Media perantara dapat berupa kabel ataunirkabel. Informasi berupa data mengalir dari satu komputer ke komputer lainnya, dan setiap komputer yang terhubung dapat bertukar data atau berbagi perangkat keras [7].

2.2.6. Jaringan Komputer

Jaringan Komputer merupakan kumpulan dari beberapa komputer dengan terhubung pada perangkat jaringan lainnya yang saling bekerja sama untuk mencapai pertukaran informasi dan data melalui kabel atau tanpa kabel sehingga memungkinkan pengguna di jaringan komputer untuk saling bertukar dokumen atau data, serta bisa berbagi sumber daya seperti perangkat keras atau perangkat lunak yang terhubung ke jaringan. [7]

Jaringan Komputer mempunyai beberapa keunggulan dibandingkan dengan komputer yang berdiri sendiri (stand-alone) yaitu:

5. Jaringan memaksimalkan sumber daya manajemen yang lebih baik, seperti pengguna / user bisa saling berbagi layanan printer dengan kualitas tinggi, selain

itu untuk penggunaan lisensi pada software jaringan lebih murah dari pada menggunakan lisensi tunggal dalam penggunaan jumlah yang sama.

6. Jaringan yang menggunakan internet membantu menjaga informasi agar tetap andal dan mutakhir, serta jika ada sistem penyimpanan terpusat yang dikelola dengan baik memungkinkan banyak pengguna yang bisa mengakses data dari banyak lokasi berbeda dan membatasi akses ke data saat sedang diproses.
7. Jaringan memudahkan dan mempercepat proses sharing data (berbagi file). Saat ini transfer data menggunakan jaringan dengan kecepatan tinggi lebih cepat dibanding dengan sarana tranfer data lainnya seperti menggunakan media flashdisk, disket, cd atau lainnya.
8. Jaringan membuat komunikasi antar kelompok dalam bekerja menjadi lebih efisien. Seperti pengiriman surat elektronik (email) merupakan kebutuhan dengan menggunakan sistem jaringan. Selain itu sebagian besar sistem jaringan digunakan untuk pemantauan proyek, meeting online, kerja group untuk membantu pekerja agar lebih produktif

Agar Sistem kerja jaringan komputer bisa mencapai tujuan, maka setiap bagian dari jaringan komputer akan melakukan permintaan (request) dan layanan (service). Adapun pihak yang melakukan permintaan disebut sebagai client dan pihak memberikan layanan disebut server. Pada jaringan komputer konsep ini disebut sebagai sistem Client-Server, dan digunakan pada hampir smua aplikasi jaringan komputer.

Berikut merupakan beberapa type jaringan berdasarkan skala areanya :.

1. PAN (Personal Area Network)

   PAN adalah jaringan komputer yang terdiri dari: Transmisi antara beberapa komputer atau antara komputer dan perangkat non-komputer seperti printer, mesin faks, telepon seluler, PDA, telepon seluler. Jangkauan PAN sangat terbatas, sekitar 9-10 meter. Semacam PAN dapat dibangun menggunakan teknologi kabel dan nirkabel Internet. Teknologi kawat PAN dapat terhubung melalui USB dan FireWire. Wireless PAN dapat dihubungkan melalui teknologi Bluetooth, WiFi dan inframerah.
2. LAN (Local Area Network)

LAN adalah jaringan komputer yang hanya mencakup satu area kecil. seperti jaringan komputer kampus, gedung, kantor, rumah, sekolah atau kurang. Saat ini, sebagian besar jaringan area lokal didasarkan pada Teknologi IEEE 802.3 Ethernet menggunakan perangkat switching yang Kecepatan transfer data adalah 10, 100 atau 1000 Mbps.

3. MAN (Metropolitan Area Network)

   MAN Merupakan Jaringan dengan skala jarak jangkau antar kota, dengan teknologi yang digunakan oleh MAN mirip dengan LAN. itu hanya daerah lebih besar dan lebih banyak komputer yang terhubung ke jaringan MAN dibandingkan dengan jaringan area lokal. MAN adalah jaringan komputer Mencakup area berukuran kota atau kombinasi dari beberapa LAN yang terhubung menjadi jaringan yang besar. Jaringan metro dapat digabungkan Jaringan komputer beberapa sekolah atau beberapa kampus. MAN bisa di Diimplementasikan pada jaringan kabel dan nirkabel.

4. WAN (Wide Area Network)

   WAN adalah jaringan komputer yang mencakup area yang luas besar (lebar). Misalnya, jaringan komputer antar wilayah, kota atau kota bahkan sebuah negara, atau dapat didefinisikan sebagai jaringan komputer Diperlukan router dan saluran komunikasi umum. WAN digunakan untuk menghubungkan satu jaringan lokal ke jaringan lokal lainnya, sehingga pengguna atau komputer di lokasi yang sama dapat berkomunikasi dengan pengguna dan komputer di lokasi lain

2.2.7. Jenis Serangan atau Ancaman Keamanan di Jaringan

1. DoS (Denial of Service)

Serangan Denial of Service (Serangan DoS) adalah jenis serangan pada komputer atau server di Internet yang menghabiskan semua sumber daya komputer, dan mencegah komputer menjalankan fungsinya dengan benar, dan memungkinkan pengguna lain untuk mengakses layanan tersbut akan terganggu. [9]

2. DDoS (Distributed Denial of Service)

DDoS adalah singkatan dari Distributed Denial of Service dan dalam bahasa Indonesia dapat diartikan sebagai Distributed Denial of Service. DDOS adalah jenis serangan yang dilakukan dengan membanjiri lalu lintas di Internet atau server [8]

3. UDP Flooding

UDP atau User Diagram Protocol adalah protokol jaringan tanpa sesi, yang membanjiri port server dari jarak jauh secara acak. Dengan demikian, server host harus melakukan pengecekat port ini dan melaporkan pengguna yang menggunakan paket ICMP agar Layanan pada host server lumpuh dan tidak bisa diakses. [9]

Jika sistem mengenali bahwa tidak ada aplikasi yang terkait dengan data, sistem akan mengirimkan paket "Destination Unreachable". Makan Semakin banyak paket UDP yang dikirim penyerang, semakin banyak paket yang dikirim sistem, membebani sistem dan menolak koneksi lain yang mencoba masuk atau keluar dari sistem.

4. SYN Flooding

Paket SYN adalah jenis paket protokol protokol kontrol transmisi yang dapat digunakan untuk membuat koneksi antara dua host dan dikirim oleh host yang ingin membuat koneksi sebagai langkah pertama dalam membangun koneksi pada "TCP three-way" Akan dilakukan. Handshake ". Proses. Dalam serangan banjir SYN, penyerang mengirimkan paket SYN ke port "pendengaran" host target. Biasanya, paket SYN yang dikirim berisi alamat sumber yang mewakili sistem yang sebenarnya, tetapi paket SYN untuk serangan ini dirancang untuk memiliki alamat sumber yang tidak mewakili sistem yang sebenarnya. [10]

5. ICMP Flood

ICMP Flood atau di kenal dengan Ping Flood Adalah Ping serangan DDOS yang membuat crash atau crash target. Ping flood dapat dikirim dalam jumlah yang sangat besar, dan target dapat gagal atau lumpuh. Sasaran dari ping flood biasanya adalah server hosting website yang dapat membuat website tidak dapat diakses, sehingga sangat merugikan, namun jika paket yang dikirim tidak sesuai dengan permintaan pelaku maka seramgan ping flood akan dihentikan [11]

6. IP Spoofing

Spoofing atau lebih sering dikenal dengan IP Spoofing merupakan suatu teknik atau cara yang digunakan untuk mendapatkan akses yang tidak berhak kepada komputer korban, dengan cara penyerang/penyusup mengirim pesan ke sebuah komputer dengan sebuah alamat IP yang menandakan pesan tersebut berasal dari host yang terpercaya. Dengan kata lain IP Spoofing adalah merubah/memodifikasi alamat sumber IP penyerang/penyusup pada IP Headers menjadi sebuah alamat IP baru yang terpercaya. [12]

7. Sniffing

Packet Sniffing merupakan pencegatan data paket-paket yang mengalir pada jaringan. Dengan sebuah program Sniffer yang bekerja pada layer 2 serta kombinasi dari NIC yang berada pada mode promiscuous (mode mendengar) untuk men-capture semua traffic yang mengalir dari dan ke internet pada suatu jaringan. Dengan demikian, semua aktivitas yang dilakukan oleh komputer yang berada pada jaringan tersebut dapat diketahui. Sniffing merupakan ancaman keamanan yang bersifat pasif karena tidak melibatkan penyerangan secara langsung, hanya mendengarkan traffic yang ada di jaringan. [13]

8. Port Scanning

Port Scanning merupakan suatu usaha mengumpulkan informasi/ reconnaissance terhadap suatu komputer target (biasanya server), yang dimana informasi yang dicari berupa layanan-layanan apa saja yang disediakan, sistem operasi komputer target dan lain-lain. Sehingga dari informasi yang didapatkan, dapat menentukan langkah selanjutnya dalam melakukan penyerangan.

9. Hijacking

MITM merupakan sebuah teknik yang mengambil keuntungan dari kelemahan protocol stack TCP/IP, dan bagaimana cara header-header dibangun. MITM terjadi ketika ada seseorang diantara 2 titik yang dimana kedua titik itu saling berkomunikasi, tetapi seseorang tersebut secara aktif memonitor, mencapture, dan mengontrol komunikasi 2 titik tersebut secara transparan. Dan

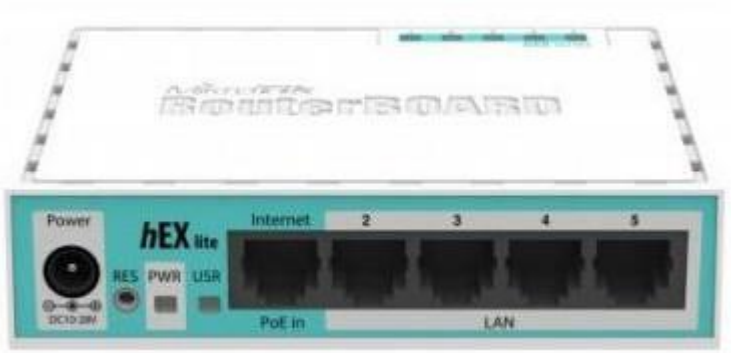
pada akhirnya kedua titik tersebut tidak sadar bahwa mereka tidak berkomunikasi satu sama lain, tetapi padahal berkomunikasi dengan seseorang tersebut.

10. Trojan

Trojan merupakan sebuah program berbahaya yang pada penampilannya hanya berupa sebuah software/paket biasa yang dimana software/paket tersebut berisi kode-kode berbahaya begitu diluncurkan dan masuk ke komputer korban. Kebanyakan program remote control spyware merupakan jenis ini. [5]

2.2.8. Mikrotik

Mikrotik adalah perangkat router yang mengirimkan paket data melalui jaringan atau Internet ke tujuannya melalui proses yang disebut perutean. Router bertindak sebagai penghubung antara dua atau lebih jaringan, meneruskan data dari satu jaringan ke jaringan lain. Router Mikrotik adalah perangkat jaringan komputer yang menggunakan sistem operasi Mikrotik RouterOS dengan kernel Linux untuk router jaringan. Router mikrotik memiliki banyak utiliti seperti bandwidth management, firewall dengan access point untuk akses dan operasi, Winbox GUI administrator untuk remote dan routing.

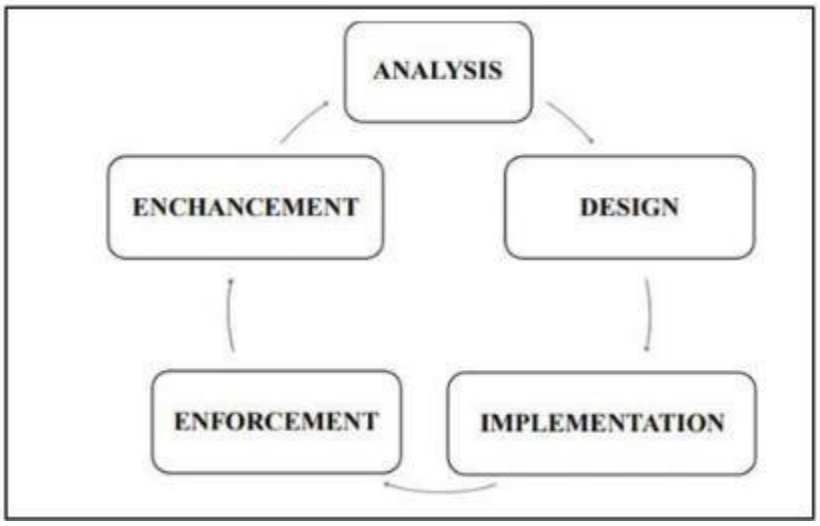


Gambar 2.1 Router Mikrotik

2.2.9. Security Policy Development Life Cycle (SPDLC)

Metode SPDLC merupakan metode yang melakukan tahap secara berskala untuk memperbarui organisasi jaringan. Metode yang digunakan pada penelitian ini

adalah Security Policy Development Life Cycle (SPDLC). SPDLC atau siklus hidup pengembangan kebijakan keamanan memiliki tahapan sebagai berikut [6] :



Gambar 2.2. Security Policy Development Life Cycle (SPDLC)

1. Analysis

   Tahap ini melakukan Perumusan masalah dan Pengumpulan data berupa informasi tentang IDS dalam peningkatan keamanan jaringan dan serangan yang terjadi. Hasil informasi yang di dapatkan dijadikan sebagai landasan dalam pemecahan masalah Ilmiah.

2. Design

   Membuat perancangan berupa topologi jaringan yang akan dibangun dan merancang penggunaan sistem operasi dan aplikasi pada server dan client.

3. Implementation

   Kemudian tahap ini akan dilakukan implementasi dari rancangan topologi jaringan yang telah dibuat yaitu dengan melakukan instalasi perangkat yang dibutuhkan dan menkonfigurasi software yang diperlukan. Detail Rancangan akan digunakan sebagai intruksi agar pembangunan sistem dapat berjalan dengan relavan.

4. Enforcement

   Pada tahap ini, akan dilakukan pengujian sistem sesuai dengan perencanaan awal. Pertama, sistem intruksi akan dilakukan percobaan yang bertujuan

untuk mengetahui serangan yang dilakukan serta port yang digunakan oleh attacker. Kedua, pengujian wireshark untuk mendapatkan hasil bagaimana sebuah packet data dengan protocol tertentu bergerak pada flow graph.

5. Enchancement

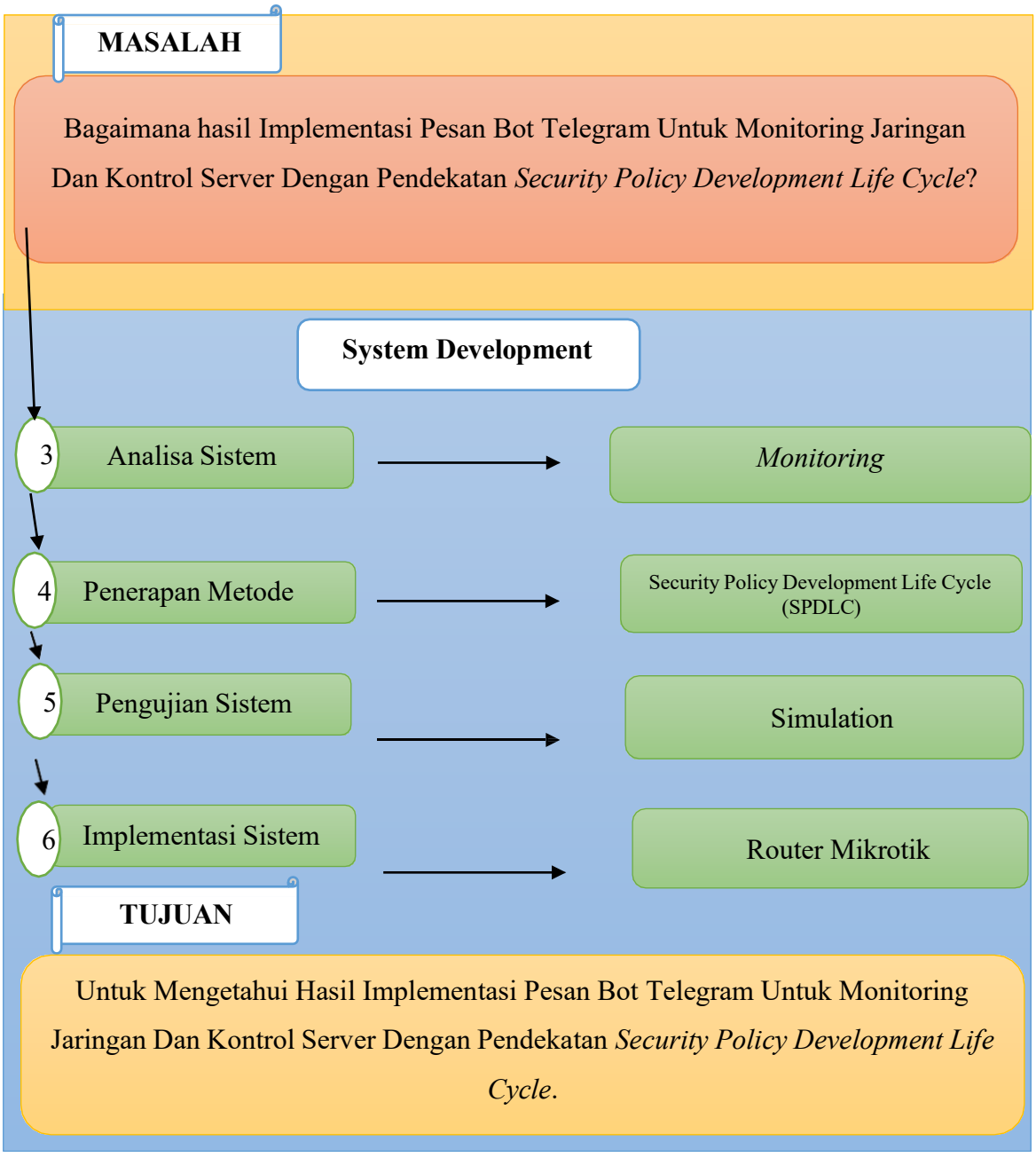
   Pada tahap ini, penulis melakukan perbaikan sistem yang telah dibangun meliputi kesalahan yang terjadi pada penelitian sebelumnya, melakukan penginkatan fungsionalitas atas komponen spesifik dan melakukan pembaruan sistem.

2.2.10. Pengujian Sistem

Pengujian sistem merupakan elemen penting dari jaminan kualitas perangkat lunak dan merupakan tinjauan komprehensif dari spesifikasi, desain, dan pengkodean. Tujuan dari tes ini adalah untuk menemukan berbagai potensi kesalahan dan konfigurasi jaringan komputer Anda dengan sedikit usaha dan waktu.

Pada Fase ini menguji sistem yang dibuat. Pengujian berfokus pada bagian dalam yang logis dan bagian luar yang fungsional dari perangkat lunak. Mengarahkan pengujian untuk menemukan bug dan memastikan bahwa input yang dibatasi menghasilkan hasil aktual yang sesuai dengan hasil yang diperlukan. Pengujian operasional juga dilakukan selama fase ini, yang mengarah pada kematangan implementasi

2.3. Kerangka Pemikiran



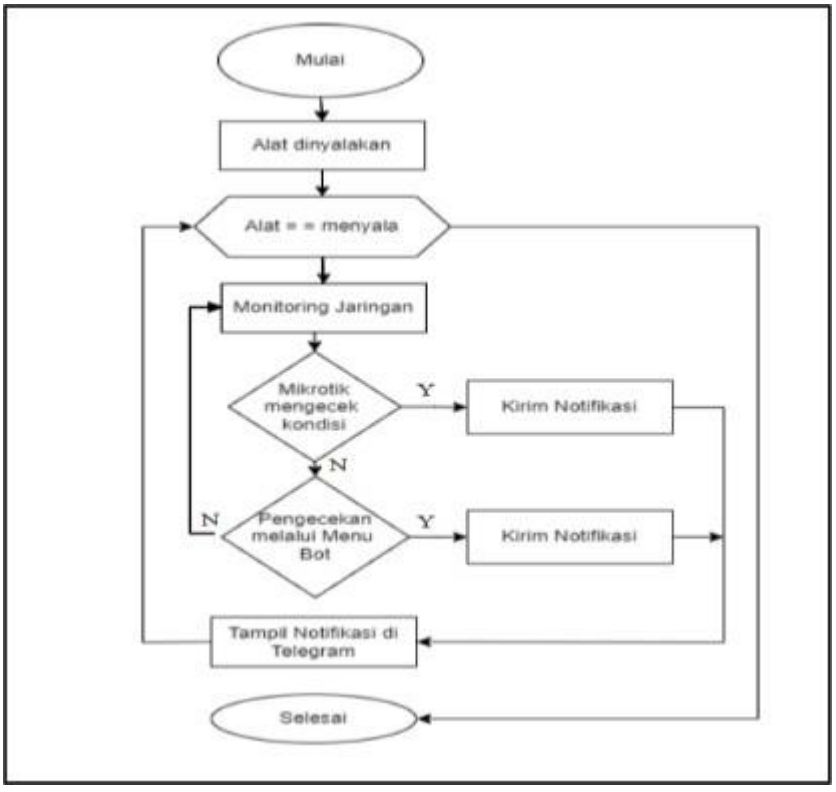
Gambar 2.3 Kerangka Pikir

BAB III
METODE PENELITIAN

3.1. Jenis, Metode, Subjek, Objek, Waktu, dan Lokasi Penelitian

Penelitian ini menggunakan metode penelitian studi kasus. Dengan demikian jenis penelitian ini adalah penelitian deskriptif.

Berdasarkan latar belakang dan kerangka pemikiran seperti yang telah diuraikan diatas maka yang menjadi objek penelitian adalah Implementasi Pesan Bot Telegram Untuk Monitoring Jaringan Dan Kontrol Server Dengan Pendekatan *Security Policy Development Life Cycle*. Penelitian ini dimulai dari 01 Agustus 2024 s/d November 2024 yang berlokasi di Kantor DPRD Kabupaten Pohuwato.



Gambar 3. 1 Alur Sistem Monitoring Jaringan Menggunakan Bot Telegram

3.2. Pengumpulan Data

Adapun jenis pengumpulan data ini yaitu data primer dan data sekunder data Primer yaitu data yang dikumpulkan langsung dilapangan berupa wawancara dengan admin teknisi jaringan dan observasi langsung setingan pada router mikrotik Kantor DPRD Kabupaten Pohuwato, mendata jumlah accespoint yang digunakan, sistem monitoring dan keamanan jaringan yang digunakan, jumlah user, dan management bandwith pada Kantor DPRD Kabupaten Pohuwato.

Sedangkan data sekunder ialah data yang dikumpulkan dari penelitian sebelumnya seperti jurnal yang membahas rancang bangun sistem serta membahas, terkait dari internet yang berhubungan dengan kemanan komputer, monitoring jaringan, bot telegram, seting mikrotik dan server dan metode *Security Policy Development Life Cycle* (SPDLC).

3.3. Pengembangan Sistem

Prosedur atau langkah-langkah pokok dalam menerapkan sistem monitoring jaringan menggunakan bot telegram, kinerja sistem monitoring dimulai setelah seluruh perangkat jaringan aktif. Jika seluruh perangkat jaringan aktif maka selanjutnya proses monitoring sudah berjalan. Melalui fasilitas mikrotik, dapat dicek oleh admin terkait kondisi jaringan komputer, jika terjadi perubahan pada jaringan maka perangkat mikrotik mengirimkan notifikasi ke bot telegram. Proses selanjutnya pengecekan kondisi jaringan melalui menu pada bot telegram. Jika tidak terjadi perubahan atau pengecekan melalui melalui bot telegram maka telegram tidak akan menerima notifikasi apapun dari mikrotik..

3.3.1. Desain Sistem

Desain Arsitektur Jaringan menjelaskan topologi serta gambaran sistem jaringan yang diimplementasikan. Sistem monitoring diterapkan pada topologi jaringan *local area.* Mikrotik digunakan untuk konfigurasi sistem monitoring dan pemanfaatan bot telegram sebagai media komunikasi dan informasi. Telegram *bot server* sebagai jembatan penghubung antara mikrotik dan *smarphone*. *Smartphone* harus terhubung dengan internet untuk bisa mendapatkan pesan notifikasi dan mikrotik harus terhubung dengan internet untuk bisa mengirim pesan notifikasi.

3.3.2. Konstruksi Sistem

Pada tahap ini dilakukan Desain Arsitektur Jaringan menjelaskan topologi serta gambaran sistem jaringan yang diimplementasikan. Sistem monitoring diterapkan pada topologi jaringan local area. Mikrotik digunakan untuk konfigurasi sistem monitoring dan pemanfaatan bot telegram sebagai media komunikasi dan informasi, pada tahap ini penulis melakukan tahap perancangan sistem dan desain sistem sebelumnya.

3.3.3. Pengujian Sistem

Pada pengujian ini penulis menggunakan konsep Pengujian berfokus pada persyaratan fungsional dengan melihat apakah sistem menghasikan output yang diinginkan dan sesuai dengan fungsi tersebut. Pengujian dilakukan dengan disable atau menonaktifkan interface pada router Mikrotik dan mencabut kabel LAN pada device yang terhubung.

BAB IV
HASIL PENELITIAN

4. 1. Analisa Kebutuhan dan Implementasi Sistem

4.1.1 Analisa Kebutuhan Sistem

Untuk membuat sistem monitoring Mikrotik dengan bot Telegram, kebutuhan utama mencakup penerimaan dan pengolahan perintah admin melalui bot Telegram, seperti pengecekan status jaringan. Selain itu, notifikasi otomatis harus tersedia untuk melaporkan aktivitas mencurigakan, seperti serangan brute force, dengan respons waktu yang cepat.

Sebelum melakukan implementasi pesan bot telegram untuk monitoring , maka dilakukan terlebih dahulu adalah menentukan topologi yang akan digunakan, serta perangkat keras berupa router mikrotik, dan kebutuhan terhadap perangkat lunak yang bisa dilihat pada tabel berikut :

Tabel 4. 1 Kebutuhan Perangkat Keras

Hardware	Jumlah Unit	Keterangan
Router Mikrotik	1	CHR
Access Point 2,4 Ghz	1	TP-Link
Laptop	1	Lenovo

Adapun untuk kebutuhan perangkat lunak ataupun tools yang digunakan dalam perancangan sistem monitoring dengan bot telegram pada penelitian ini seperti pada tabel dibawah berikut :

Tabel 4. 2 Kebutuhan Perangkat Lunak

Software	Keterangan
Virtual Box	Aplikasi Untuk menjalankan Sistem Operasi Virtual Mikrotik
Winbox	Tool untuk mengkonfigurasi Mikrotik
Telegram App	Aplikasi pesan instan sekaligus sebagai bot monitoring

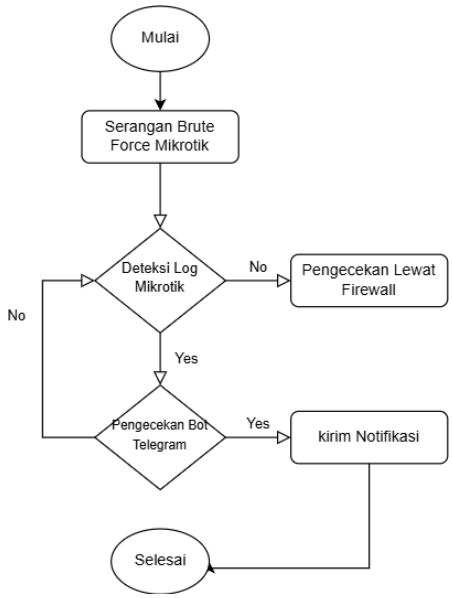
4. 2. Implementasi Sistem

Pada penelitian ini, implementasi bot mikrotik menggunakan pendekatan dengan metode *Security Policy Development Life Cycle* (SPDLC), yaitu pendekatan sistematis yang digunakan untuk merancang, mengimplementasikan, dan memelihara kebijakan keamanan dalam sebuah organisasi atau sistem. metode SPDLC terdiri dari lima tahapan utama: Analysis, Design, Implementation, Enforcement, dan Enhancement.

1. Tahapan Analysis bertujuan untuk memahami kebutuhan keamanan organisasi dengan mengidentifikasi risiko, ancaman, dan kelemahan yang ada.
2. Tahap Design, kebijakan keamanan dirancang berdasarkan hasil analisis dengan mempertimbangkan standar keamanan dan kebutuhan spesifik organisasi.
3. Tahap Implementation dilakukan dengan mengintegrasikan kebijakan keamanan ke dalam sistem yang ada, termasuk konfigurasi perangkat keras dan perangkat lunak.
4. Pada tahap Enforcement, kebijakan yang telah diimplementasikan dipantau dan dijalankan secara ketat untuk memastikan kepatuhan terhadap prosedur yang telah ditetapkan. Terakhir,
5. Enhancement berfokus pada evaluasi dan perbaikan kebijakan keamanan yang sudah ada untuk mengakomodasi perubahan lingkungan teknologi atau ancaman baru yang muncul.

4.3.1. Analysis

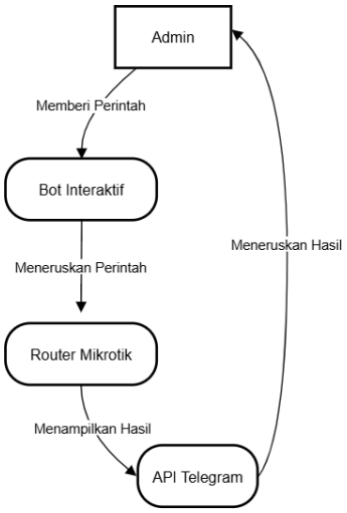
Analisis masalah monitoring jaringan dan kontrol server befokus pada media komunikasi data berupa pesan yang dikirim dan direspon oleh mikrotik. Pada penelitian ini, sistem monitoring deteksi serangan menggunakan log dari Mikrotik, firewall, dan bot Telegram untuk memberikan notifikasi kepada pengguna. Prosesnya dimulai dari adanya serangan, diikuti dengan langkah-langkah deteksi, pengecekan, hingga pemberitahuan kepada pengguna seperti pada diagram berikut.



Gambar 4. 1 Diagram Alir Monitoring Serangan

Berdasark alur keterangan pada gambar diatas, sistem monitoring dimulai dengan mendeteksi potensi serangan Brute Force pada perangkat Mikrotik, yang biasanya berupa percobaan login berulang menggunakan kombinasi username dan password. Serangan ini dicatat sebagai log di Mikrotik dan dianalisis untuk mencari pola mencurigakan, seperti login gagal berulang atau aktivitas dari IP tertentu. Jika log tidak mendeteksi ancaman, sistem melanjutkan pengecekan melalui firewall untuk memeriksa aktivitas abnormal. Jika ancaman terdeteksi, sistem memverifikasi integrasi dengan bot Telegram, termasuk validasi token dan konfigurasi notifikasi, sebelum mengirimkan informasi serangan kepada pengguna. Proses ini selesai setelah notifikasi, berisi detail serangan dan rekomendasi tindakan, berhasil diterima oleh pengguna.

Sedangkan pada kontrol server berbasis bot interaktif yang memanfaatkan API Telegram untuk komunikasi. Admin memberikan perintah melalui bot interaktif, yang kemudian meneruskan perintah tersebut ke perangkat Mikrotik. Setelah perangkat Mikrotik memproses perintah, hasilnya dikirimkan kembali ke bot melalui API Telegram untuk ditampilkan kepada admin seperti pada gambar berikut :

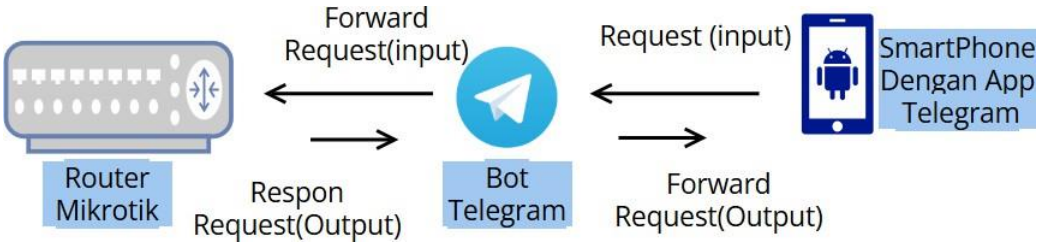


Gambar 4. 2 Alur kerja kontrol Server

Pada Sistem kontrol dengan bot Telegram melibatkan peran admin sebagai pengguna utama yang memberikan perintah kepada bot interaktif, seperti pengecekan status jaringan atau melakukan restart ketika terjadi masalah pada jaringan. Bot akan bertindak sebagai perantara dengan menerima perintah, kemudian meneruskannya ke router Mikrotik untuk dieksekusi. setelah itu Router menjalankan perintah, dan mengirimkan hasilnya kembali melalui API Telegram, yang menjadi saluran komunikasi antara bot dan admin. Setelah itu, bot menampilkan hasil kepada admin dalam bentuk pesan Telegram.

4.3.2. Design

Design Arsitektur sistem yang dirancang untuk monitoring serangan brute force SSH dan implementasi bot Telegram sebagai bot kontrol server / bot interaktif, terdiri dari tiga komponen utama: Router Mikrotik, Bot Telegram, dan Smartphone dengan aplikasi Telegram. Dalam arsitektur ini, router Mikrotik bertugas mendeteksi aktivitas mencurigakan, seperti serangan brute force SSH, dengan menganalisis log dan mengirimkan data tersebut sebagai permintaan (request) ke bot Telegram. Bot Telegram berfungsi sebagai perantara yang meneruskan data dari router Mikrotik ke admin melalui aplikasi Telegram di smartphone.



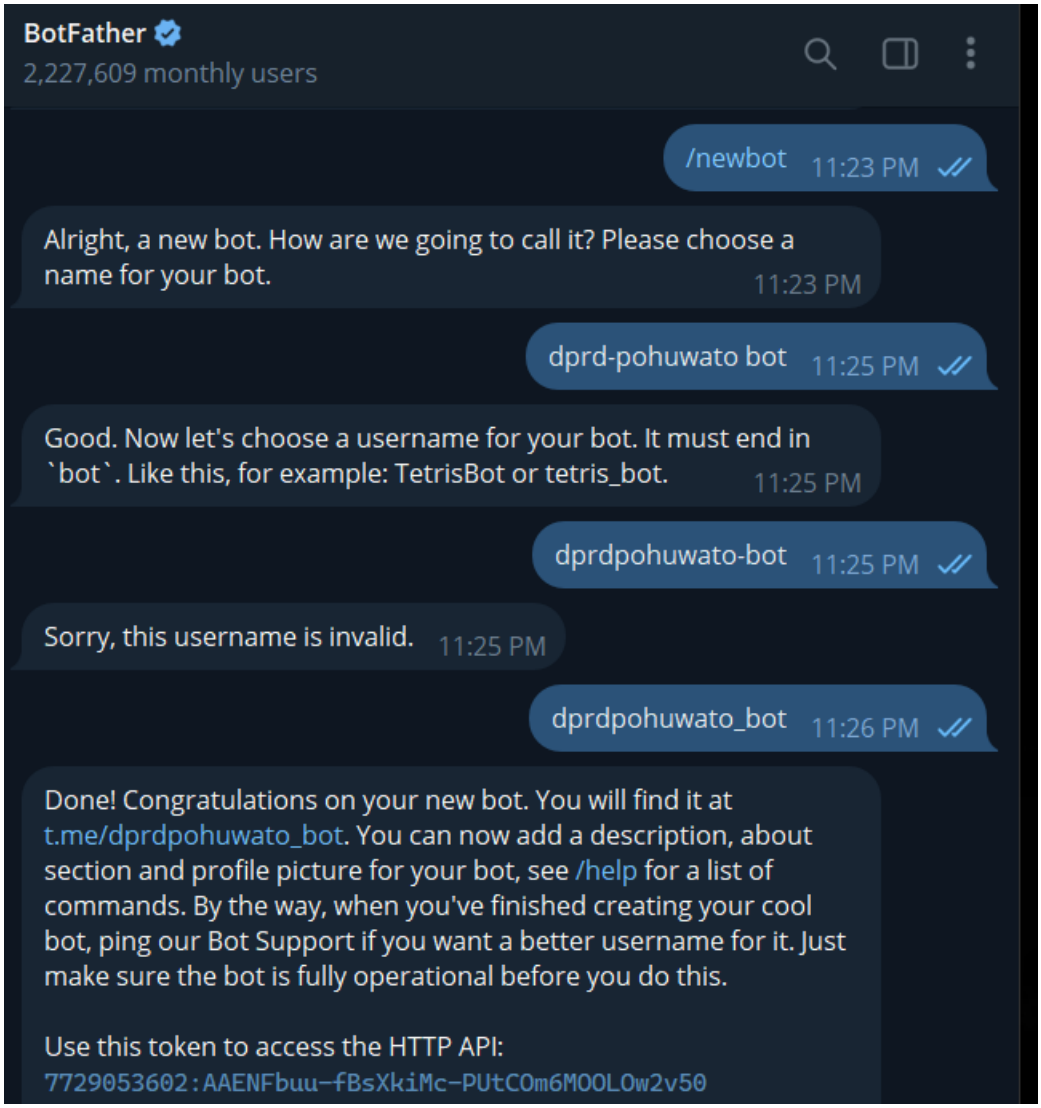
Gambar 4. 3 Desain Arsitektur Sistem Monitoring Telegram

Sebagai kontrol server, admin dapat berinteraksi secara langsung dengan bot Telegram melalui smartphone untuk memberikan perintah (input), seperti pengecekan status jaringan atau pengelolaan firewall. Bot kemudian meneruskan perintah tersebut ke Mikrotik untuk diproses dan mengembalikan hasilnya dalam bentuk notifikasi atau data monitoring yang relevan. Dengan desain ini, sistem mampu memberikan notifikasi real-time kepada admin sekaligus menyediakan kemampuan kontrol yang interaktif dan responsif."

4.3.3. Implementation

4.3.3.1 Pembuatan Bot Telegram

Pada tahap implementasi bot telegram sebagai monitoring dan kontrol server, di perlukan pembuatan bot terlebih dahulu, pada penelitian ini penulis menggunakan Bot Father. BotFather sendiri adalah bot resmi telegram yang digunakan untuk membuat dan mengelola bot.



Gambar 4. 4 Proses Pembuatan Bot

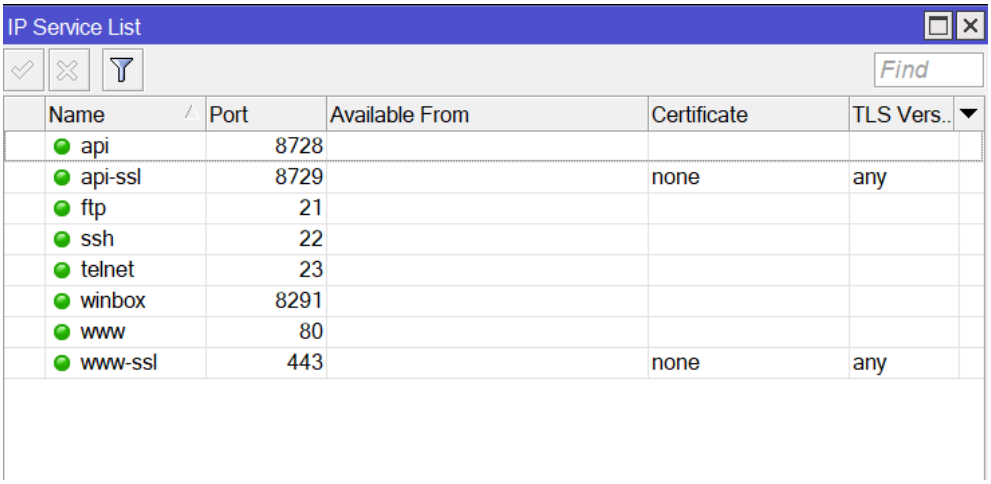
Untuk membuat bot Telegram pada BotFather, langkah pertama yang perlu dilakukan adalah membuka aplikasi Telegram dan mencari BotFather melalui kolom pencarian. Setelah ditemukan, penulis melakukan interaksi dengan BotFather dengan mengetikkan /start, yang akan memunculkan daftar perintah untuk pembuatan dan pengelolaan bot. Langkah ini adalah awal dari proses pembuatan bot yang nantinya akan memiliki fitur dan fungsi sesuai kebutuhan pengguna.

Setelah BotFather aktif, langkah berikutnya adalah membuat bot baru dengan mengetikkan /newbot. BotFather kemudian akan meminta nama untuk bot

yang akan dibuat. pada penelitian ini penulis memberi nama "dprdpohuwato-bot" dan pembuatan user name dengan nama "dprdpohuwato_bot". Setelah proses pembuatan bot kemudian BotFather akan memberikan Token API. Token ini adalah kunci unik yang nantinya akan digunakan untuk menghubungkan bot dengan sistem mikrotik yang akan mengelola komunikasi dengan bot.

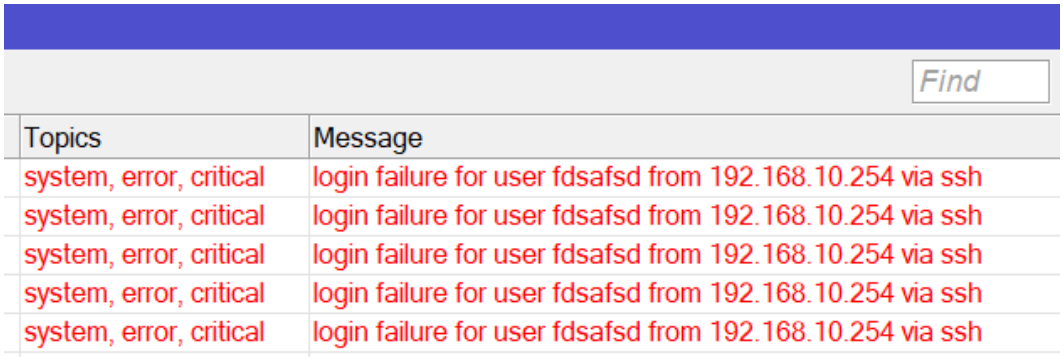
4.3.3.2 Implementasi Bot Telegram Pada Mikrotik

Tahap pertama dalam penerapan bot Telegram dengan Token API pada Mikrotik adalah mempersiapkan infrastruktur yang mendukung komunikasi antara bot dan perangkat Mikrotik. selanjutnya memastikan fitur API pada Mikrotik harus diaktifkan melalui Winbox dengan memastikan service API dalam menu IP > Services sudah berjalan.



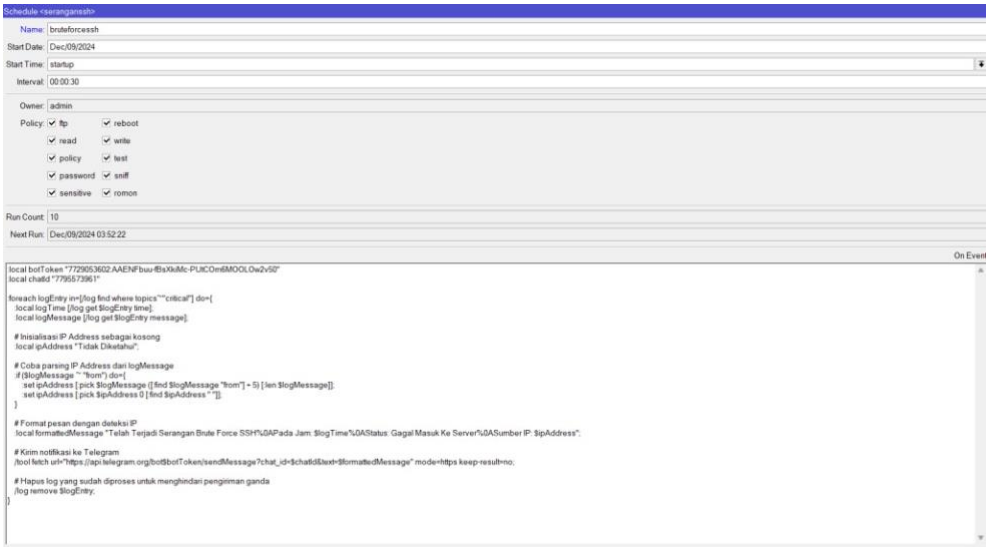
Gambar 4. 5 Daftar Service di Mikrotik

Pembuatan script di Scheduler Mikrotik untuk mendeteksi serangan brute force melalui log dimulai dengan membuat filter yang mendeteksi topic tertentu, seperti "login failure" atau "brute force", yang dicatat dalam log Mikrotik. Script ini menggunakan perintah bawaan Mikrotik seperti : log untuk membaca log secara berkala dan mencari pola mencurigakan, seperti percobaan login berulang dari IP tertentu. Setelah mendeteksi pola tersebut, script menggunakan API Telegram untuk meneruskan notifikasi ke bot Telegram milik admin.



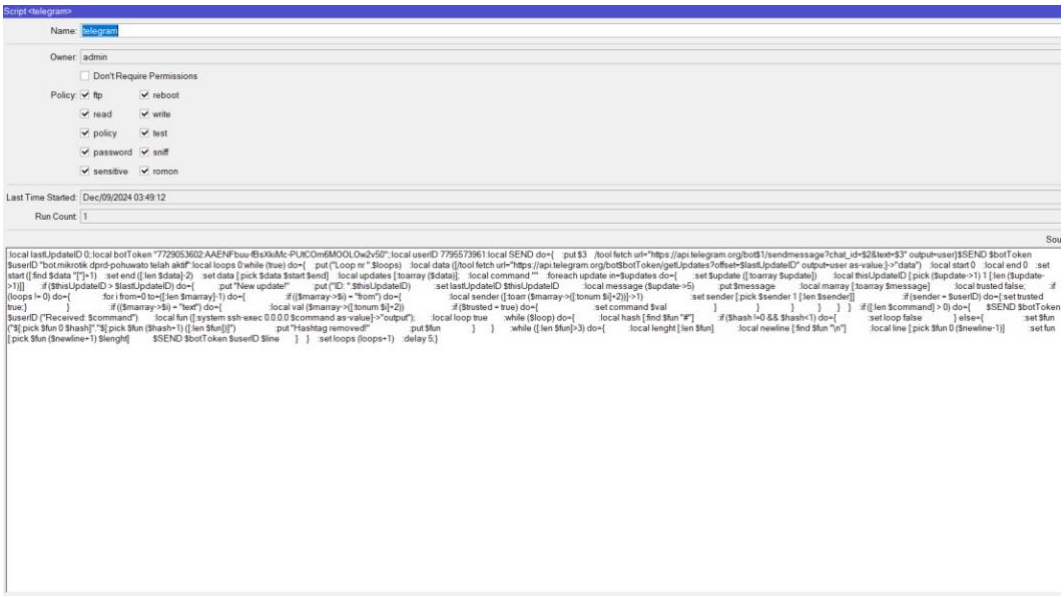
Gambar 4. 6 Log Serangan Bruteforce SSH

Tahapan selanjutnya melakukan konfigurasi Scheduler Mikrotik untuk mendeteksi serangan brute force SSH berdasarkan log dengan topik "critical" dan mengirimkan notifikasi ke Telegram. Scheduler diberi nama "bruteforcessh" dan dijalankan secara otomatis setiap 30 detik setelah startup.. Script kemudian akan memeriksa log Mikrotik untuk mencari entri dengan topik "critical". Jika ditemukan, script mengambil waktu kejadian (logTime) dan pesan log (logMessage). Alamat IP sumber serangan dicoba diambil dari pesan log, jika tersedia. Pesan atau format notifikasi menggunakan informasi waktu, status serangan, dan IP sumber, lalu dikirimkan ke Telegram menggunakan perintah melalui API Telegram. Setelah notifikasi berhasil dikirim, log yang telah diproses dihapus untuk mencegah pengulangan pengiriman.



Gambar 4. 7 Pembuatan Script Detekse Serangan

Dalam penerapan bot sebagai kontrol server atau sebagai bot interaktif, perlu dilakukan konfigurasi script di Mikrotik yang dapat menerima perintah dari pengguna Telegram, memprosesnya, dan mengembalikan respons ke admin. Script dimulai dengan mendefinisikan beberapa variabel penting, seperti botToken (token API bot Telegram), userID (ID Telegram pengguna yang diizinkan berinteraksi dengan bot), dan lastUpdateID (untuk melacak pesan terakhir yang diproses). Script ini bekerja dalam sebuah loop yang terus-menerus mengambil pesan terbaru dari bot Telegram menggunakan API getUpdates. Jika ada pesan baru, script mengekstrak informasi seperti pengirim, jenis pesan, dan isi perintah. Kemudian, perintah tersebut diproses sesuai logika yang ditentukan, misalnya menjalankan perintah Mikrotik.

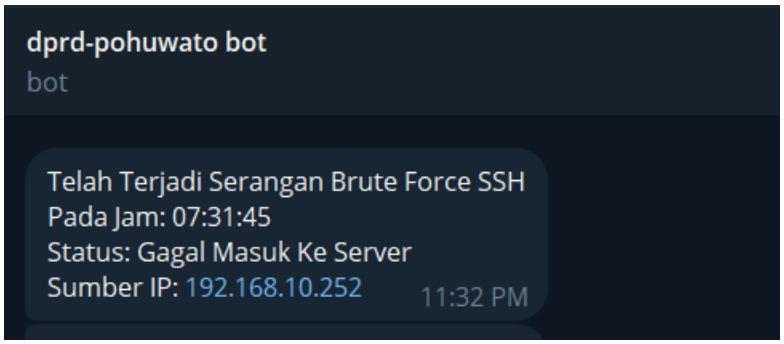


Gambar 4. 8 Konfigurasi Bot Interaktif

4.3.4. Enforcement dan Enhancement

Setelah tahap implementasi selanjutnya adalah tahap kegiatan pelaksanaan pengujian dengan berdasarkan perancangan yang telah dibuat dalam proses implementasi. Pengujian berfokus pada persyaratan fungsional dengan melihat apakah sistem menghasikan output yang diinginkan dan sesuai dengan fungsi tersebut.

Skenario pengujian sistem bot Telegram yang terintegrasi dengan Mikrotik mencakup pengujian fungsionalitas dasar bot untuk memastikan respons terhadap perintah, serta pendeteksian serangan brute force dari log Mikrotik dengan pengiriman notifikasi ke Telegram.



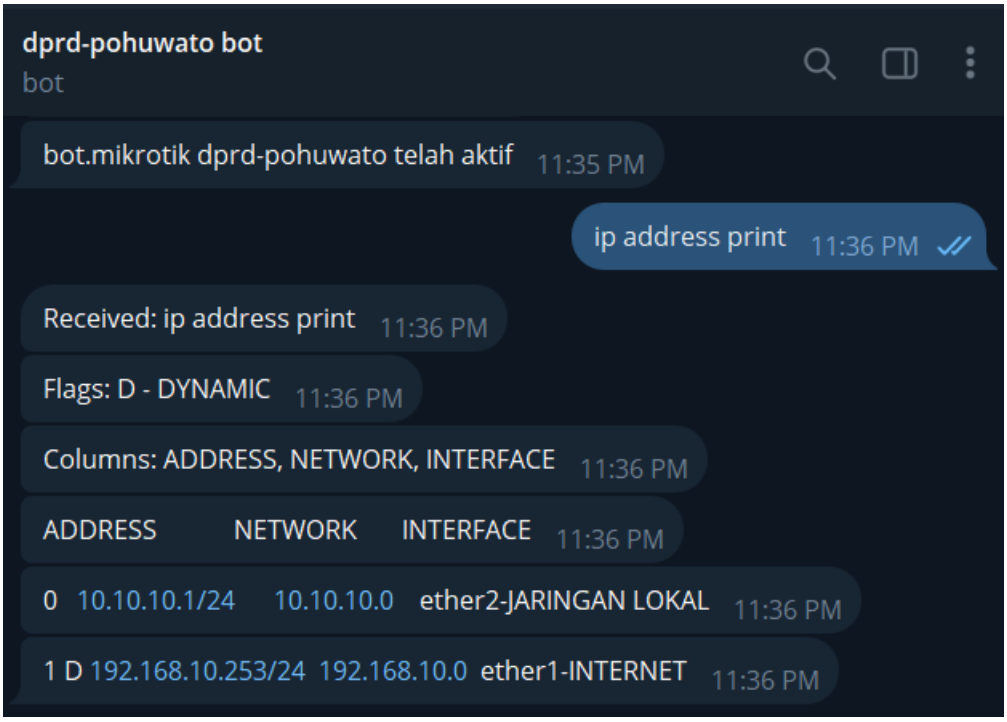
Gambar 4. 9 Pengujian Notifikasi Serangan Brute Force SSH

Berdasarkan gambar diatas mikrotik berhasil mengirimkan notifikasi yang dikirimkan oleh bot Telegram dengan nama "dprd-pohuwato bot", yang memberi peringatan tentang adanya serangan brute force SSH pada sebuah server. Notifikasi tersebut berisi detail kejadian, yaitu:

1. Jam: "07:31:45" menunjukkan waktu saat serangan brute force terdeteksi
2. Status serangan: "Gagal Masuk Ke Server" berarti upaya brute force tidak berhasil mendapatkan akses ke server.
3. Sumber IP: "192.168.10.252" menunjukkan alamat IP yang melakukan serangan brute force, yang merupakan informasi penting untuk memitigasi ancaman, seperti memblokir IP ini di firewall.

Selanjutnya melakukan pengujian terhadap bot sebagai kontrol server (interaktif) dengan mengirimkan perintah ip address print, yang merupakan perintah standar untuk menampilkan daftar alamat IP yang dikonfigurasi di router. Bot merespons dengan menampilkan hasil :

1. Alamat IP 10.10.10.1/24 berada di interface ether2-JARINGAN LOKAL dengan jaringan 10.10.10.0.
2. Alamat IP 192.168.10.253/24 berada di interface ether1-INTERNET dengan jaringan 192.168.10.0.



Gambar 4. 10 Hasil Pengujian Bot Interaktif

Untuk memastikan sistem bot Telegram yang terintegrasi dengan Mikrotik berjalan sesuai dengan fungsionalitas yang diharapkan, serangkaian skenario pengujian akan dilakukan. Pengujian ini bertujuan untuk mengevaluasi kemampuan bot dalam mendeteksi aktivitas jaringan, mengolah perintah yang diberikan oleh admin, serta mengirimkan notifikasi secara real-time melalui Telegram. Selain itu, skenario ini juga dirancang untuk menguji respons sistem terhadap potensi ancaman, seperti serangan brute force, dan memastikan bahwa waktu pengiriman notifikasi, format pesan, serta akurasi informasi yang diberikan telah sesuai dengan standar yang diharapkan. Hasil dari skenario pengujian ini akan digunakan untuk mengevaluasi efektivitas dan keandalan sistem secara keseluruhan, yang hasilnya bisa dilihat pada tabel berikut :

Tabel 4. 3 Skenario Pengujian Bot Telegram

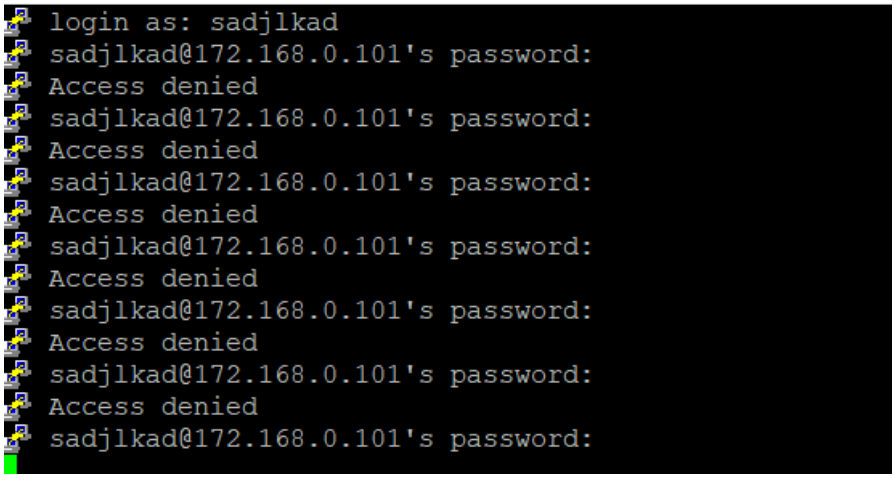
No	Skenario Pengujian	Waktu Respon Pengiriman Notifikasi	Output	Status
1	Melakukan Simulasi Brute force SSH ke Mikrotik	10 Detik	Tampil notifikasi di Telegram: "Serangan brute force SSH terdeteksi, IP: 192.168.1.5"	Berhasil
2	Mengirim perintah “system resource print” melalui bot Telegram	5 Detik	Bot menampilkan informasi Resource Penggunaan status CPU, RAM	Berhasil
3	Mengirim perintah “ip address print” melalui bot Telegram	6 Detik	Bot Menampilkan Informasi IP Address Pada Mikrotik	Berhasil
4	Mengirim perintah “interface print” melalui bot Telegram	5 Detik	Bot Menampilkan Daftar Interface Pada Mikrotik	Berhasil
5	Mengirim perintah “system reboot” melalui bot Telegram	4 Detik	Bot mengirim notifikasi: "Router berhasil di-reboot pada 12:34:56	Berhasil

BAB V
PEMBAHASAN PENELITIAN

5. 1. Pembahasan Sistem

5.1.1. Serangan Brute Force SSH

Pada tahap ini akan dilakukan uji coba serangan brute force SSH menggunakan aplikasi PuTTY untuk menguji sistem deteksi yang telah dirancang.



Gambar 5. 1 Uji Coba Serangan Brute Force SSH

Gambar di atas menunjukkan upaya login berulang dengan kredensial yang salah ke alamat IP target 172.168.0.101, yang menghasilkan Access Denied sebagai respons. Aktivitas ini mensimulasikan serangan brute force, di mana penyerang mencoba berbagai kombinasi username dan password untuk mendapatkan akses tidak sah ke server.

Uji coba ini bertujuan untuk memastikan bahwa sistem monitoring berbasis Mikrotik dan Bot Telegram dapat mendeteksi pola serangan brute force melalui analisis log, mengirimkan notifikasi secara real-time kepada admin, serta memberikan informasi detail seperti sumber IP penyerang dan waktu kejadian. Hasil dari uji coba ini akan digunakan untuk mengevaluasi keefektifan sistem dalam memberikan respons terhadap ancaman keamanan jaringan seperti pada gambar berikut.

5.1.2. Running Script Via Terminal

pada tahap ini penulis melakukan pengujian sistem dengan menjalankan script bot Telegram melalui terminal Mikrotik menggunakan perintah /system script run 0 seperti pada gambar berikut :

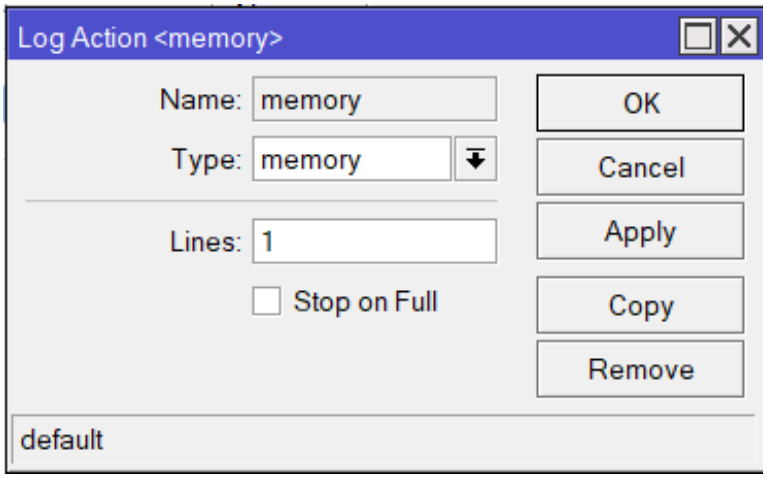
```
[admin@MikroTik] /system/script> run 0
bot.mikrotik dprd-pohuwato telah aktif
      status: finished
  downloaded: 0KiBC-z pause]
       total: 0KiB
    duration: 2s
        data: {"ok":true,"result":{"message_id":67,
              "from":{"id":7729053602,"is_bot":true,
              "first_name":"dprd-pohuwato bot",
              "username":"dprdpohuwato_bot"},
              "chat":{"id":7795573961,"first_name":"58348",
              "last_name":"Alamri","type":"private"},
              "date":1733715314,"text":"bot.mikrotik
              dprd-pohuwato telah aktif"}}
```

Gambar 5. 2 Menjalankan Script via Terminal

Gambar di atas menunjukkan bahwa script berhasil dijalankan dengan status finished, dengan durasi eksekusi dalam waktu 2 detik. Adapun Respons dari bot Telegram, seperti ditampilkan pada log, memberikan konfirmasi bahwa bot "dprd-pohuwato" telah aktif dengan mengirimkan pesan ke chat ID admin yang terdaftar. Adapaun data tambahan, seperti informasi username bot, ID pengirim, serta teks pesan yang dikirimkan, menunjukkan bahwa komunikasi antara Mikrotik dan API Telegram berjalan dengan baik. Uji coba ini bertujuan untuk memastikan integrasi bot Telegram berfungsi dengan benar dan dapat mengirimkan notifikasi sesuai dengan perintah yang dijalankan melalui terminal.

5.1.3. Pengaturan Sistem Logging

Pada bagian ini, dilakukan pengaturan logging log pada perangkat Mikrotik melalui antarmuka Winbox untuk memastikan informasi log yang ditampilkan sesuai kebutuhan sistem.



Gambar 5. 3 Pengaturan Logging Log Mikrotik

Gambar di atas merupakan konfigurasi log action dengan nama memory, di mana jumlah baris log yang akan ditampilkan diatur menjadi 1 melalui opsi Lines. Pengaturan ini berguna untuk membatasi jumlah log yang tersimpan dalam memori perangkat, sehingga dapat mengoptimalkan penggunaan sumber daya sistem. Opsi Stop on Full tidak dicentang, yang berarti log akan terus ditambahkan tanpa penghentian otomatis meskipun memori penuh. opsi ini penting untuk memastikan bahwa log tetap dapat dipantau dengan efisien selama proses monitoring dan evaluasi sistem berlangsung

BAB VI
KESIMPULAN

1. Kesimpulan

Berdasarkan Hasil penelitian dan pembahasan yang telah diuraikan sebelumnya, maka dapat ditarik kesimpulan bahwa implementasi pesan bot telegram untuk monitoring jaringan dan kontrol server dengan pendekatan Security Policy Development Life Cycle (SPDLC) berhasil diterapkan pada router mikrotik. Sistem yang dibangun mampu mendeteksi serangan brute force SSH secara real- time melalui analisis log Mikrotik dan mengirimkan notifikasi otomatis ke Telegram dengan informasi yang lengkap, seperti waktu kejadian, status serangan, dan sumber IP. Selain itu, bot Telegram berfungsi sebagai alat interaktif yang memungkinkan admin mengontrol dan memonitor server dengan perintah lewat telegram.

2. Saran

Setelah melakukan penelitian dalam implementasi sistem monitoring dengan bot telegram, ada beberapa saran yang perlu diperhatikan untuk mencapai tujuan yang diharapkan :

a. Masih perlu dilakukan Analisa dan penelitian lebih lanjut tentang sistem monitoring jaringan dan kontrol server menggunakan bot telegram dengan pendekatan Security Policy Development Life Cycle (SPDLC
b. Perlu dilakukan penelitian lebih lanjut untuk monitoring serangan dengan jenis yang lain dengan bot telegram

DAFTAR PUSTAKA

[1] R. Syahfitra, "Rancang Bangun Serta Memonitoring Server Menggunakan Aplikasi The Dude Dengan Notifikasi Bot Telegram Di Fakultas Teknik Universitas Islam Kuantan Singingi," *JuPerSatek,* vol. III,no. 2, pp. 634-639, 2020.

[2] .R. D. Jayanto, "Rancang Bangun Sistem Monitoring Jaringan Menggunakan Mikrotik Router Os," *JATI,* vol. III, no. 4, pp. 391-395, 2019.

[3] Julianto Dkk. Analisis Keamanan Jaringan Mikrotik ISP Indonesia Menggunakan Search Engine Scada Shodan," *Photosynthetica*, vol. 2, no. 1, pp. 1–13, 2020.

[4] Abdullah. (2016). Kung-Fu Hacking Dengan Nmap (Automatic Vulnerability Scanning) Nmap Scanning Report. Yogyakarta: Penerbit Andi.

[5] M. Jufri and Heryanto, "Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall," *JOISIE,* vol. V, no. 2, pp. 98-108, 2021.

[6] Faris Jawad dkk, 2023. Optimalisasi Keamanan Dan Monitoring Jaringan Infrastruktur Di Kantor DPRD Bekasi.

[7] Ari Muzakir. Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan, 2020

[8] Sasut, Tasmi Deris Setiawan. Identifikasi Serangan Port Scanning Dengan Metode String Matching," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 118–124, 2016.. *Media Infotama*, vol. 13, no. 2, pp. 73–84, 2016.

[9] A. Hidayat and I. P. Saputra, "Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750Ra Dan Rb750Gr3 Dengan Metode Penetration Testing (Studi Kasus: Warnet Aulia.Net, Tanjung Harapan Lampung

Timur)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 118–124, 2018.

[10] H. Kurniawan and S. Kosasi, "Penerapan Network Development Life Cycle Dalam Perancangan Intranet," *Penerapan Netw. Dev. Life Cycle Dalam Peranc. Intranet Untuk Mendukung Proses Pembelajaran*, vol. 5, no. 2, pp. 178–188, 2015.

[11] L. Menggunakan and S. Kerja, "Perancangan dan implementasi monitoring jaringan lokal menggunakan sistem kerja," 2011.

[12] N. E. I. N. U. Tara, "PENGEMBANGAN SISTEM KEAMANAN JARINGAN KOMPUTER BERBASIS MIKROTIK PADA SMK NEGERI 1 INDRALAYA UTARA C OMPUTER N ETWORK S ECURITY S YSTEM D EVELOPMENT B ASED ON M IKROTIK AT SMK Imam Solikin , 2 Suryayusra , 3 Maria Ulfa Pendahuluan Perkembangan Jaringan in," pp. 61–70.

[13] "Pendeteksian Serangan Ddos (Distributed Denial of Service) Menggunakan Ids (Intrusion Detection System) Universitas Pasundan November 2016," no. November, 2016.

[14] R. TOWIDJOJO, *MIKROTIK KUNGFU*, KITAB 1. JASAKOM.

[15] Y. Kristianto and M. Salman, "Implementasi dan Analisa Unjuk Kerja Keamanan Jaringan pada Infrastuktur Berbasis IDPS (Intrusion Detection and Prevention System)," p. 10, 2010.

Lampiran Script :

1. Script Detekesi Serangan BruteForce SSH

```
:local botToken ""
:local chatId ""

:foreach logEntry in=[/log find where topics~"ssh"] do={
   :local logTime [/log get $logEntry time];
   :local logMessage [/log get $logEntry message];

   # Format Notifikasi
   :local formattedMessage "Telah Terjadi Serangan Brute Force SSH%0APada Jam: $logTime%0AStatus: Gagal Masuk Ke Server%0ASumber IP: $ipAddress";

   # Kirim notifikasi ke Telegram
   /tool fetch url="https://api.telegram.org/bot$botToken/sendMessage?chat_id=$chatId&text=$formattedMessage" mode=https keep-result=no;

   # Hapus log yang sudah diproses untuk menghindari pengiriman ganda
   /log remove $logEntry;
}
```

2. Script Bot Kontrol Server (Interaktif)

```
/system script add name=telegram source={
:local lastUpdateID 0;
:local botToken "";
:local userID XXX
:local SEND do={
   :put $3
   /tool fetch url="https://api.telegram.org/bot$1/sendmessage?chat_id=$2&text=$3" output=user
}
$SEND $botToken $userID "Telegram script initiated."
:local loops 0
:while (true) do={
   :put ("Loop nr ".$loops)
   :local data ([/tool fetch url="https://api.telegram.org/bot$botToken/getUpdates?offset=$lastUpdateID" output=user as-value;]->"data")
   :local start 0
   :local end 0
   :set start ([:find $data "["]+1)
   :set end ([:len $data]-2)
   :set data [:pick $data $start $end]
   :local updates [:toarray ($data)];
```

```
:local command ""
:foreach update in=$updates do={
  :set $update ([:toarray $update])
  :local thisUpdateID [:pick ($update->1) 1 [:len ($update->1)]]
  :if ($thisUpdateID > $lastUpdateID) do={
    :put "New update!"
    :put ("ID: ".$thisUpdateID)
    :set lastUpdateID $thisUpdateID
    :local message ($update->5)
    :put $message
    :local marray [:toarray $message]
    :local trusted false;
    :if (loops != 0) do={
      :for i from=0 to=([:len $marray]-1) do={
        :if (($marray->$i) = "from") do={
          :local sender ([:toarr ($marray->([:tonum $i]+2))]->1)
          :set sender [:pick $sender 1 [:len $sender]]
          :if (sender = $userID) do={:set trusted true;}
        }
        :if (($marray->$i) = "text") do={
          :local val ($marray->([:tonum $i]+2))
          :if ($trusted = true) do={
```

```
                    :set command $val
                }
            }
        }
    }
}
:if ([:len $command] > 0) do={
    $SEND $botToken $userID ("Received: $command")
    :local fun ([:system ssh-exec 0.0.0.0 $command as-value]->"output");
    :local loop true
    :while ($loop) do={
        :local hash [:find $fun "#"]
        :if ($hash !=0 && $hash<1) do={
            :set loop false
            } else={
                :set $fun ("$[:pick $fun 0 $hash]"."$[:pick $fun ($hash+1) ([:len
$fun])]")
                :put "Hashtag removed!"
                :put $fun
            }
    }
    :while ([:len $fun]>3) do={
```

```
        :local lenght [:len $fun]
        :local newline [:find $fun "\n"]
        :local line [:pick $fun 0 ($newline-1)]
        :set fun [:pick $fun ($newline+1) $lenght]
        $SEND $botToken $userID $line
      }
    }
    :set loops (loops+1)
    :delay 5;
}
}
```

DAFTAR RIWAYAT HIDUP

Nama : Faisal Alamri

TTL : Tomini, 16 Desember 2000

Alamat : Kecamatan Tomini Kabupaten Parigi Moutong

Email : isalalamri161220@gmail.com

Riwayat Pendidikan :

1. Tahun 2013, Menyelesaikan Pendidikan di SDN Inpres 1 Tomini Kab Parigi Moutong
2. Tahun 2016, Menyelesaikan Pendidikan di MTA Al-Mubarok Marisa
3. Tahun 2019, Menyelesaikan Pendidikan di SMK Negeri 1 Marisa
4. Tahun 2019, Mendaftar dan Diterima Menjadi Mahasiswa di Universitas Ichsan Gorontalo.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
LEMBAGA PENELITIAN
Jl. Achmad Nadjamuddin No.17, Kampus Unisan Gorontalo Lt.1 Kota Gorontalo 96128
Website: lemlitunisan.ac.id, Email: lembagapenelitian@unisan.ac.id

Nomor : 66/PIP/B.04/LP-UIG/2024
Lampiran : -
Hal : Permohonan Izin Penelitian (Pengambilan Data)

Kepada Yth.,

Sekretariat DPRD Kabupaten Pohuwato

di -
Tempat

Yang bertandatangan di bawah ini:

Nama	:	Dr. Rahmisyari, ST., SE., MM
NIDN	:	0929117202
Pangkat Akademik	:	Lektor Kepala
Jabatan	:	Ketua Lembaga Penelitian Universitas Ichsan Gorontalo

Meminta kesediaannya untuk memberikan izin pengambilan data dalam rangka penyusunan **Proposal/Skripsi,** kepada:

Nama	:	Faisal F.Alamri
NIM	:	T3119054
Fakultas	:	Ilmu Komputer
Program Studi	:	Teknik Informatika
Judul Penelitian	:	IMPLEMENTASI PESAN BOT TELEGRAM UNTUK MONITORING JARINGAN DAN KONTROL SERVER DENGAN PENDEKATAN SECURITY POLICY DEVELOPMENT LIFE CYCLE
Lokasi Penelitian	:	DPRD Pohuwato

Demikian surat ini saya sampaikan, atas bantuan dan kerjasamanya diucapkan banyak terima kasih.

Dikeluarkan di Gorontalo
Tanggal, 27/09/2024
Ketua Lembaga Penelitian

Dr. Rahmisyari, ST., SE., MM
NIDN: 0929117202

PEMERINTAH KABUPATEN POHUWATO
SEKERTARIAT DPRD

Alamat : Jalan Jenderal Sudirman Kec. Marisa Kab. Pohuwato Tlp. (0443)210003 fax 210003

Marisa, 14 Oktober 2024

Nomor : 790/SETWAN-PHWT/335/X/2024

Lamp : -

Perihal : **Pelaksanaan Penelitian**

Kepada Yth,

Kepala Lembaga Penelitian

Universitas Ichsan Gorontalo

Di –

Tempat

Memperhatikan Surat Nomor : 66/PIP/B.04/LP-UIG/2024, HAL Permohonan Izin Penelitian (Pengambilan Data) Tanggal 01 Oktober Tahun 2024 Dalam rangka penyusunan Proposal/Skripsi Mahasiswa :

Nama	: Faisal F. Alamri
NIM	: T3119054
Fakultas	: Ilmu Komputer
Program Studi	: Teknik Informatika
Judul Penelitian	: Implementasi Pesan Bot Telegram untuk Monitoring Jaringan dan Kontrol Server dengan pendekatan security Policy Depelopment Life Cycle

Maka dengan ini disampaikan bahwa kami menerima untuk pelaksanaan penelitaan serta pengambilan Data Dukung terkait penyusunan Proposal / Skripsi dimaksud yang rencana pelaksanaannya sejak tanggal 04 Oktober s/d 11 Oktober Tahun 2024 dengan harapan data dukung tersebut dapat digunakan sebagaimana mestinya.

Demikian disampaikan atas bantuan dan kerjasamanya di ucapkan terima kasih.

Marisa, 14 Oktober 2024

Kabag Umum dan Keuangan

RUSLY R. UMAR, S.Sos
Pembina Tk.1 / IV b
NIP. 197201022006041008

Mengetahui
Sekretaris DPRD

HAMKAWATY M. MBUINGA, S.Pd.MM
Pembina Utama Muda / IV c
NIP. 197103112007032004

Fikom05 Unisan

SKRIPSI

FAKULTAS ILMU KOMPUTER

Fak. Ilmu Komputer

LL Dikti IX Turnitin Consortium

Document Details

Submission ID
trn:oid:::1:3115986368

Submission Date
Dec 16, 2024, 7:09 AM GMT+7

Download Date
Dec 16, 2024, 7:10 AM GMT+7

File Name
TURNITIN-FAISAL.pdf

File Size
858.3 KB

37 Pages

6,415 Words

41,726 Characters

14% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Top Sources

0% Internet sources
12% Publications
7% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we fl it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

0% Internet sources
12% Publications
7% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Publication
Taufiq Syaiful Huda, Subektiningsih Subektiningsih. "Analisis Keamanan Jaringan ... 2%

2 Publication
Rahmad Kartolo, Edi Surya Negara. "Analisis Kinerja Private Cloud Computing Me... 1%

3 Student papers
UPN Veteran Yogyakarta 1%

4 Publication
Rico Rinaldo. "IMPLEMENTASI SISTEM MONITORING JARINGAN MENGGUNAKAN ... 1%

5 Student papers
UIN Syarif Hidayatullah Jakarta 1%

6 Publication
Susanto Susanto, Basworo Ardi Pramono, Sri Handayani. "Analisis Sniffing Passw... 1%

7 Student papers
SDM Universitas Gadjah Mada 1%

8 Student papers
LL Dikti IX Turnitin Consortium 1%

9 Publication
Husdi Husdi, Hastuti Dalai. "Penerapan Metode Regresi Linear Untuk Prediksi Ju... 1%

10 Student papers
Universitas Putera Batam 0%

11 Student papers
Universitas Budi Luhur 0%

12	Publication	
wa Haris Sembiring. "Perancangan jaringan menggunakan CISCO", Open Scienc...		0%
13	Publication	
atha Gilang Saputra, Hinova Rezha Ulinuha, Anisah Romdhiyatun Noor. "ANALIS...		0%
14	Publication	
imara Kusuma Hakim, Septian Adi Nugroho. "Implementasi Telegram Bot untuk...		0%
15	Student papers	
Jniversitas Jember		0%
16	Publication	
alentino Wiku Nduku. "APLIKASI SISTEM INFORMASI PENYEWAAN LAPANGAN FU...		0%
17	Publication	
uryanto Suryanto, Fitrah Agus Permadi. "Optimalisasi Jaringan Internet Hotspot...		0%
18	Publication	
Windy Dwiparaswati. "SIMULASI ALAT PENGENDALI LAMPU JARAK JAUH MENGGU...		0%
19	Publication	
Filia Meitri Alelo, Remuz MB Kmurawak, Mingsep Rante Sampebua. "Sistem Infor...		0%
20	Student papers	
Jniversitas Esa Unggul		0%
21	Student papers	
Jniversitas Islam Malang		0%
22	Publication	
Muhamamad Wahyu, Arif Senja Fitrani, Hindarto Hindarto. "Penerapan Bot Teleg...		0%
23	Publication	
Muhammad Ikhsan Azhari, Tengku Mohd. Diansyah, Ari Usman. "PERBANDINGA...		0%
24	Student papers	
Jniversitas International Batam		0%