ANALISIS DAN IMPLEMENTASI SERANGAN BRUTE FORCE MENGGUNAKANAN HYDRA DENGAN METODE PENETRATION TESTING SERTA MELINDUNGI PORT ROUTER MIKROTIK BERBASIS FIREWALL DI PT. PLN (PERSERO) UP3 PADANG

SKRIPSI

Untuk Memenuhi Sebagian Persyaratan

Mencapai Gelar Sarjana Komputer

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1

OLEH :

ALDIAN RAHMAT INSANI

20101152630042

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PUTRA INDONESIA "YPTK" PADANG

PADANG 2024

DAFTAR ISI

DAFTAR ISI 2

BAB I PENDAHULUAN 3

1.1 Latar Belakang 3

1.2 Perumusahan Masalah 6

1.3 Hipotesa 6

1.4 Batasan Masalah 6

1.5 Tujuan Penelitian 7

1.6 Manfaat Penelitian 7

1.7 Gambaran Umum Objek Penelitian 9

1.7.1 Sekilas Tentang PT PLN (Persero) UP3 Padang 9

1.7.2 Visi & Misi PT PLN (Persero) UP3 Padang 10

1.7.3 Struktur Organisasi Toko 11

1.7.4 Tugas dan Tanggung Jawab 12

DAFTAR PUSTAKA 19

BAB I

PENDAHULUAN

1.1 Latar Belakang

PT PLN (Persero) UP3 Padang merupakan salah satu perusahaan energi terkemuka di Indonesia yang bertanggung jawab atas penyediaan dan distribusi listrik di seluruh wilayah. Sebagai infrastruktur vital bagi masyarakat dan industri, keamanan sistem informasi dan jaringan menjadi krusial dalam memastikan kelancaran operasional serta mencegah potensi kerentanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Saat ini, serangan siber menjadi ancaman yang nyata bagi pengguna internet di seluruh dunia. Salah satu ancaman yang persisten dan merugikan adalah serangan *brute force* (Bahri, 2023).

Brute force adalah salah satu serangan praktis yang dapat digunakan memecahkan teknik pengamanan kriptografi dengan cara mencoba seluruh kemungkinan kunci yang ada (Dewa Made Julijati Putra et al., 2022). Serangan *brute force* terdiri dari penyerang yang mengirimkan banyak kata sandi atau frasa sandi dengan harapan dapat menebak dengan benar. Penyerang secara sistematis memeriksa semua kemungkinan kata sandi dan frasa sandi sampai yang benar ditemukan. Atau, penyerang dapat mencoba menebak kunci yang biasanya dibuat dari kata sandi menggunakan fungsi derivasi kunci (Sampurna, 2022). Menurut (Rahmah, 2023), tujuan dari serangan *brute force* adalah untuk mendapatkan akses ke otoritas “Administrator” pada sistem target. Di samping itu, penelitian oleh penulis lain (Febrian et al., 2024), Serangan *brute force* yang berhasil tidak hanya memberi peretas akses ke data, aplikasi, dan sumber daya, tetapi juga dapat

berfungsi sebagai titik masuk untuk serangan lebih lanjut beberapa tanda dapat ditafsirkan sebagai indikator serangan *brute force*.

Hal ini relevan dengan situasi yang dihadapi PT PLN (Persero) UP3 Padang. Dimana infrastruktur jaringan rentan terhadap serangan *brute force* karena kurangnya sistem keamanan jaringan yang memadai untuk melindungi port router MikroTik. Selain itu, tidak ada pengujian sistem keamanan jaringan yang dilakukan untuk menemukan celah keamanan pada jaringan komputer di PT PLN (Persero) UP3 Padang. Kondisi ini menciptakan celah keamanan yang signifikan, memungkinkan penyerang untuk melakukan serangan *brute force* dan mendapatkan akses tidak sah ke jaringan PT PLN (Persero) UP3 Padang. Akses ini dapat disalahgunakan untuk berbagai tujuan berbahaya, seperti mencuri data sensitif, mengganggu operasi bisnis, atau bahkan menyebarkan malware.

Menurut laporan dari (Haryanto & Sutra, 2023), Indonesia menjadi negara dengan angka kejahatan teknologi informasi tertinggi di dunia. Indonesia menduduki peringkat kedua negara dengan tingkat kejahatan teknologi informasi tertinggi di dunia setelah Jepang. Badan Siber dan Sandi Negara (BSSN) mempublikasikan laporan tahunan monitoring keamanan siber tahun 2021. Laporan ini dipublikasikan pada situs resmi milik Direktorat Operasi Keamanan Siber BSSN tepatnya pada Id-SIRTII/CC (*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*), dari laporan tersebut dapat terlihat bahwa lebih dari 1,6 miliar atau tepatnya adalah 1.637.973.022 anomali trafik atau serangan siber (*cyberattack*) yang terjadi di seluruh wilayah Indonesia pada tahun 2021 (Vimy et al., 2022). Kasus-kasus serangan ini menunjukkan betapa pentingnya keamanan siber yang kuat untuk melindungi infrastruktur jaringan komputer.

Penting untuk melakukan *penetration testing* pada keamanan jaringan untuk mendeteksi serangan *brute force*. Berdasarkan studi yang dilakukan oleh (Hasibuan & Elhanafi, 2022), implementasi metode *penetration testing* terbukti efektif dalam mengidentifikasi kerentanan keamanan sebelum dimanfaatkan oleh peretas. Oleh karena itu, diperlukan implementasi serangan *brute force* dengan menggunakan *hydra* sebagai alat *penetration testing* pada jaringan komputer di PT PLN (Persero) UP3 Padang. Melalui pengujian serangan *brute force* terhadap port router MikroTik, dapat diidentifikasi celah keamanan yang ada di jaringan tersebut. Selain itu, akan dilakukan pengamanan jaringan terhadap serangan *brute force* menggunakan *firewall* dalam memperkuat keamanan jaringan. *Firewall* berfungsi sebagai filter antara komputer internal dan eksternal. Selain itu, *firewall* juga berfungsi mengatur dan mengontrol lalu lintas data yang diijinkan untuk mengakses jaringan privat (Hendita & Kusuma, 2021). Dengan adanya *firewall*, serangan *brute force* dapat dideteksi dan diblokir sebelum mencapai target (Mudzakkar et al., 2023). Konfigurasi *firewall* mencakup berbagai fitur seperti *filtering by ip address*, *port blocking*, *rate limiting*, serta *ip whitelisting/blacklisting*, digunakan untuk mengontrol akses ke jaringan dan mengurangi risiko serangan *brute force*.

Dari permasalahan tersebut penulis ingin mengangkat judul penelitian yaitu **"ANALISIS DAN IMPLEMENTASI SERANGAN BRUTE FORCE MENGGUNAKANAN HYDRA DENGAN METODE PENETRATION TESTING SERTA MELINDUNGI PORT ROUTER MIKROTIK BERBASIS FIREWALL PADA PT PLN (PERSERO) UP3 PADANG".**

1.2 Perumusahan Masalah

Berdasarkan latar belakang yang telah diuraikan di atas dapat disimpulkan permasalahan utama yang akan dipecahkan dalam laporan ini sebagai berikut:

1. Bagaimana penggunaan serangan *brute force* dengan metode *penetration testing* dapat mengidentifikasi celah keamanan jaringan di PT PLN (Persero) UP3 Padang?
2. Bagaimana penggunaan konfigurasi *firewall* dapat membantu PT PLN (Persero) UP3 Padang dalam melindungi port router Mikrotik dari serangan *brute force*?

1.3 Hipotesa

Hipotesa merupakan dugaan sementara dimana nantinya akan dibuktikan dengan hasil penelitian yang dilakukan. Berdasarkan permasalahan yang ada dapat dikemukakan beberapa hipotesa sebagai berikut:

1. Diharapkan dengan melakukan pengujian serangan *brute force* dengan metode *penetration testing* dapat secara efektif mengidentifikasi celah keamanan jaringan yang ada di PT PLN (Persero) UP3 Padang.
2. Diharapkan dengan menggunakan konfigurasi *firewall* secara efektif, dapat meningkatkan keamanan akses jaringan pada port router MikroTik terhadap serangan *brute force* di PT PLN (Persero) UP3 Padang.

1.4 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka peneliti memberikan batasan masalah yaitu, Penelitian ini memfokuskan pada pengujian serangan *brute force* terhadap port

router MikroTik menggunakan alat-alat dari Kali Linux, yaitu *hydra* dan c*runch*. Selain itu, penelitian ini juga akan mengeksplorasi metode pengamanan jaringan pada port router MikroTik dengan menerapkan berbagai konfigurasi *firewall* menggunakan aplikasi Winbox. Konfigurasi yang akan diterapkan dalam *firewall* mencakup *filtering by IP address*, *port blocking*, *rate limiting*, serta *IP whitelisting/blacklisting*. Selanjutnya, akan menggunakan aplikasi Cisco Packet Tracer sebagai pendukung visualisasi dari topologi jaringan yang ada di PT PLN (Persero) UP3 Padang.

1.5 Tujuan Penelitian

Dalam melaksanakan penelitian ini tujuan yang ingin dicapai diantaranya adalah:

1. Membantu PT PLN (Persero) UP3 Padang dalam menguji keamanan jaringan pada port router MikroTik dengan tujuan mengidentifikasi kelemahan keamanan jaringan melalui serangan *brute force* dengan metode *penetration testing.*
2. Membantu PT PLN (Persero) UP3 Padang dalam memperkuat langkah-langkah pengamanan pada port router MikroTik dengan tujuan untuk mengantisipasi dari serangan *brute force* melalui konfigurasi *firewall*.

1.6 Manfaat Penelitian

Manfaat dari penelitian ini yaitu:

1. Dengan menerapkan metode *penetration testing* menggunakan *hydra*, maka dapat membantu PT PLN (Persero) UP3 Padang dalam

mengidentifikasi celah keamanan yang kurang memadai dalam jaringan komputer.

2. Dengan adanya konfigurasi *firewall,* maka dapat melindungi dari penggunaan sumber daya yang tidak sah pada port router MikroTik, seperti pelanggaran privasi dan pencurian identitas.
3. Dengan adanya konfigurasi *firewall* menggunakan metode *filtering by IP address,* maka dapat membantu PT PLN (Persero) UP3 Padang untuk memblokir IP address dari penyerang secara *real-time.*
4. Dengan adanya konfigurasi *firewall* menggunakan metode *port blocking*, membantu PT PLN (Persero) UP3 Padang untuk memblokir port pada router MikroTik.
5. Dengan adanya konfigurasi *firewall* menggunakan metode *rate limiting,* memungkinkan untuk membatasi alamat IP yang melakukan *login* secara terus-menerus, sehingga dapat meminimalisir ancaman dari serangan *brute force*.
6. Dengan adanya konfigurasi *firewall* menggunakan metode *IP whitelisting/blacklisting*, memungkin untuk memasukkan alamat IP ke daftar hitam secara *real-time* untuk alamat IP yang sudah terblokir.
7. Manfaat bagi Universitas, penelitian ini berkontribusi pada pengembangan ilmu pengetahuan dengan menyumbangkan hasil penelitian yang dapat menjadi referensi bagi studi selanjutnya di bidang keamanan jaringan.

8. Manfaat bagi penulis, meningkatkan profil profesional penulis dengan menunjukkan kemampuan dalam mengatasi masalah keamanan siber yang nyata dan kompleks.

1.7 Gambaran Umum Objek Penelitian

Gambaran Umum Objek Penelitian adalah bagian yang berisi pernyataan umum tentang suatu objek penelitian.

1.7.1 Sekilas Tentang PT PLN (Persero) UP3 Padang

PT PLN (Persero) Unit Pelaksana Pelayanan Pelanggan (UP3) Padang merupakan bagian dari PT PLN (Persero), perusahaan listrik negara di Indonesia yang bertanggung jawab atas pengelolaan dan distribusi listrik di wilayah Padang dan sekitarnya. PT PLN (Persero) didirikan setelah kemerdekaan Indonesia pada tahun 1945, awalnya bernama Jawatan Listrik dan Gas, dan kemudian menjadi Perusahaan Negara Listrik dan Gas (PLN & PG) pada tahun 1961. Pada tahun 1972, sektor listrik dan gas dipisahkan, dan PLN berdiri sendiri sebagai entitas yang bertanggung jawab atas penyediaan listrik di Indonesia. Seiring dengan meningkatnya kebutuhan listrik di Sumatera Barat, PLN membentuk unit-unit pelaksana seperti UP3 Padang untuk meningkatkan efisiensi dan pelayanan. UP3 Padang bertanggung jawab mengelola distribusi listrik, menangani gangguan, memelihara jaringan, dan memastikan ketersediaan listrik yang cukup bagi masyarakat dan industri di wilayah operasionalnya.

Dalam beberapa tahun terakhir, PLN UP3 Padang telah mengadopsi berbagai teknologi baru dan melakukan modernisasi jaringan untuk meningkatkan kualitas pelayanan, termasuk pemasangan smart meter dan peningkatan infrastruktur.

Meskipun menghadapi tantangan geografis yang kompleks, dari pesisir hingga pegunungan, PLN UP3 Padang terus berupaya menjaga keandalan jaringan listrik dengan perencanaan dan pemeliharaan yang cermat. Berkat upaya tersebut, mereka berhasil meraih beberapa penghargaan dalam hal pelayanan pelanggan dan efisiensi operasional. Selain itu, PLN UP3 Padang aktif dalam program-program tanggung jawab sosial perusahaan (CSR), termasuk listrik masuk desa untuk memastikan seluruh wilayah, termasuk daerah terpencil, mendapatkan akses listrik. Mereka juga terlibat dalam berbagai kegiatan lingkungan dan komunitas untuk mendukung pembangunan berkelanjutan di wilayah Sumatera Barat. Secara keseluruhan, PT PLN UP3 Padang adalah bagian integral dari PT PLN (Persero) yang terus berkembang untuk memenuhi kebutuhan listrik yang semakin meningkat, sambil menghadapi tantangan geografis dan operasional dengan inovasi dan komitmen terhadap pelayanan pelanggan.

1.7.2 Visi & Misi PT PLN (Persero) UP3 Padang

1. Visi

   Menjadi perusahaan listrik terkemuka se-Asia Tenggara dan pilihan pertama pelanggan untuk solusi energi.

2. Misi

   a. Menjalankan bisnis kelistrikan dan bidang lain yang terkait, berorientasi pada kepuasan pelanggan, anggota perusahaan, dan pemegang saham.

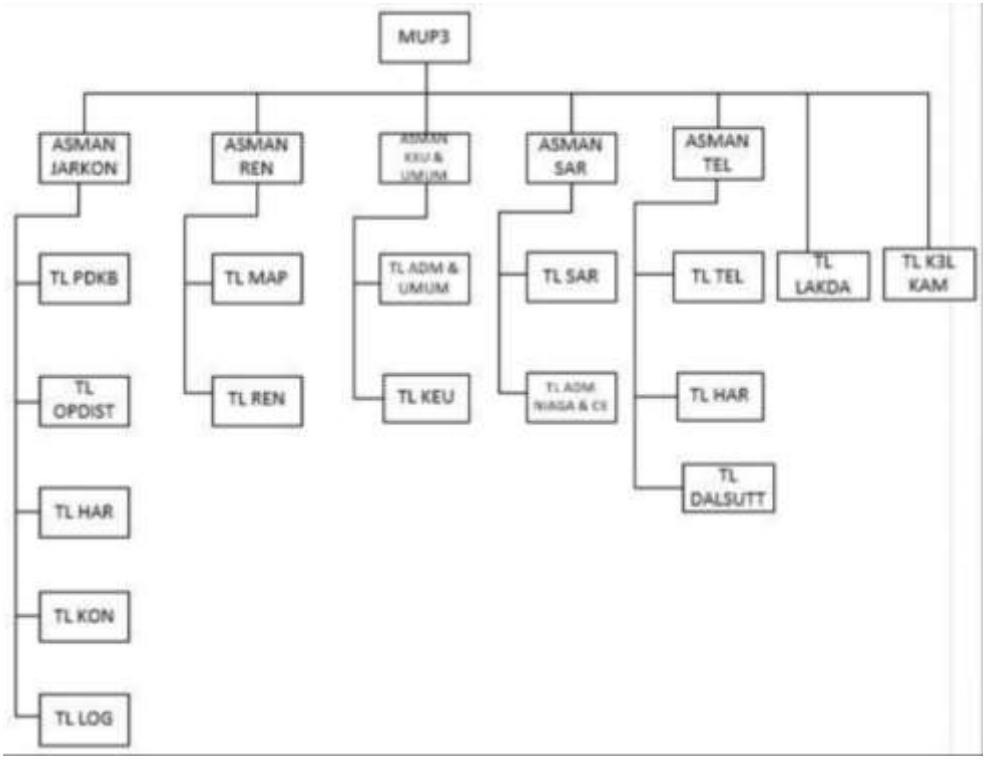
   b. Menjadikan tenaga listrik sebagai media untuk meningkatkan kualitas kehidupan masyarakat.

c. Mengupayakan agar tenaga listrik menjadi pendorong kegiatan ekonomi.

d. Menjalankan kegiatan usaha yang berwawasan lingkungan.

1.7.3 Struktur Organisasi Toko

Dengan adanya struktur organisasi diharapkan akan dapat diketahui dengan jelas mengenai tugas, wewenang, dan tanggung jawab di PT PLN (Persero) UP3 Padang. Adapun struktur organisasi PT PLN (Persero) UP3 Padang dapat dilihat pada gambar 1.1 sebagai berikut:



Sumber: PT PLN (Persero) UP3 Padang

Gambar 1. 1 Struktur Organisasi PT PLN (Persero) UP3 Padang

1.7.4 Tugas dan Tanggung Jawab

Berikut adalah uraian pekerjaan pada PT PLN (Persero) UP3 Padang:

1. MUP3 (Manager Unit Pelaksana Pelayanan Pelanggan) mempunyai tugas dan tanggung jawab atas pengelolaan unit pelaksana pelayanan pelanggan, termasuk layanan pelanggan, penagihan, dan manajemen hubungan pelanggan.
2. ASMAN JARKOM (Asisten Manager Jaringan dan Komunikasi) mempunyai tugas dan tanggung jawab atas manajemen, pemeliharaan, dan pengembangan infrastruktur jaringan komunikasi seperti telekomunikasi, internet, dan sistem komunikasi internal.
3. ASMAN REN (Asisten Manager Rencana) mempunyai tugas dan tanggung jawab atas perencanaan, pengembangan, dan pemeliharaan infrastruktur listrik, termasuk perencanaan kebutuhan listrik dan pemeliharaan jaringan distribusi.
4. ASMAN KEU & UMUM (Asisten Manager Keuangan & Umum) mempunyai tugas dan tanggung jawab atas manajemen keuangan dan administrasi umum, termasuk pengelolaan anggaran, akuntansi, dan administrasi SDM.
5. ASMAN SAR (Asisten Manager Sumberdaya Manusia) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Menyusun dan mengawasi implementasi kebijakan mutu Pendidikan.
    b. Bertanggung jawab atas akreditasi dan evaluasi program-program pendidikan di sekola Bertanggung jawab atas manajemen sumber

daya manusia, termasuk rekrutmen, pelatihan, pengembangan, dan manajemen kinerja pegawai.

6. ASMAN TEL (Asisten Manager Telekomunikasi) mempunyai tugas dan tanggung jawab atas manajemen infrastruktur telekomunikasi, termasuk pemeliharaan jaringan telepon dan sistem komunikasi radio.
7. TL PDKB (Pengatur Distribusi dan Kontrol Beban) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas pengaturan distribusi listrik di wilayah tertentu.
    b. Mengawasi dan mengkoordinasi aktivitas pemasangan, pemeliharaan, dan perbaikan infrastruktur distribusi.
    c. Memastikan penanganan gangguan distribusi listrik dan pemulihan layanan dalam waktu yang efisien.
8. TL HAR (Hubungan Masyarakat) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Mengelola hubungan masyarakat dengan pelanggan dan masyarakat umum di wilayah tertentu.
    b. Merencanakan dan melaksanakan program-program komunikasi dan pelayanan pelanggan.
    c. Menanggapi keluhan dan masukan dari pelanggan serta memastikan kepuasan pelanggan terjaga.
9. TL OPDIST (Operasi Distribusi) mempunyai tugas dan tanggung jawab sebagai berikut:

a. Bertanggung jawab atas operasi sehari-hari jaringan distribusi listrik di wilayah tertentu.
b. Memimpin tim lapangan untuk pemeliharaan rutin, inspeksi, dan penanganan keadaan darurat pada jaringan distribusi.
c. Memastikan pemantauan dan pengawasan yang tepat terhadap kinerja jaringan distribusi.

10. TL KON (Konstruksi) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Mengelola proyek-proyek konstruksi infrastruktur listrik di wilayah tertentu.
    b. Memimpin tim konstruksi dalam perencanaan, pelaksanaan, dan pemantauan proyek-proyek konstruksi.
    c. Memastikan kepatuhan terhadap standar konstruksi, anggaran, dan jadwal proyek.
11. TL LOG (Logistik) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Mengelola operasi logistik untuk memastikan pasokan dan distribusi material dan peralatan yang diperlukan untuk operasi listrik.
    b. Merencanakan dan mengkoordinasikan pengadaan, penyimpanan, dan pengiriman material serta peralatan.
    c. Memantau stok dan mengelola inventaris untuk memastikan ketersediaan yang memadai.

12. TL ADM & UMUM (Team Leader Administrasi & Umum) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim administrasi yang bertanggung jawab atas berbagai tugas administratif, termasuk pengelolaan dokumen, pengarsipan, dan administrasi umum kantor.
    b. Mengkoordinasikan pelayanan umum seperti layanan kebersihan, keamanan, dan fasilitas kantor lainnya.
    c. Menangani tugas-tugas administratif khusus seperti penjadwalan pertemuan, pengelolaan inventaris, dan pengelolaan surat-menyurat.
13. TL KEU (Team Leader Keuangan) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim keuangan yang bertanggung jawab atas manajemen keuangan dan akuntansi perusahaan.
    b. Merencanakan, mengawasi, dan melaksanakan kegiatan keuangan termasuk pengelolaan anggaran, pelaporan keuangan, dan pemantauan arus kas.
    c. Menjaga kepatuhan terhadap peraturan keuangan dan standar akuntansi yang berlaku..
14. TL SAR (Team Leader Sumber Daya Manusia) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim sumber daya manusia yang bertanggung jawab atas manajemen sumber daya manusia perusahaan.
    b. Mengelola proses rekrutmen, seleksi, dan penempatan karyawan.

c. Merencanakan dan melaksanakan program pelatihan dan pengembangan karyawan serta manajemen kinerja.

15. TL ADM NIAGA & CE (Team Leader Administrasi Niaga & Customer Experience) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas administrasi niaga dan pengalaman pelanggan.
    b. Menangani administrasi terkait dengan kegiatan niaga, seperti penjualan, pembelian, dan pelayanan pelanggan.
    c. Memastikan pengalaman pelanggan yang memuaskan melalui penanganan keluhan, umpan.
16. TL TEL (Team Leader Telekomunikasi) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas manajemen infrastruktur telekomunikasi perusahaan.
    b. Merencanakan, menginstalasi, dan memelihara sistem telekomunikasi seperti telepon, internet, dan jaringan komunikasi data.
    c. Memastikan ketersediaan layanan telekomunikasi yang handal dan berkualitas bagi seluruh unit kerja perusahaan.
17. TL DALSUTT (Team Leader Distribusi, Aliran Listrik, dan Sistem Utilitas) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas manajemen operasional distribusi listrik dan sistem utilitas perusahaan.

b. Melakukan pemeliharaan dan pemantauan terhadap jaringan distribusi listrik dan sistem utilitas lainnya.
c. Menangani penanganan gangguan dan pemulihan layanan serta perencanaan kapasitas dan pengembangan infrastruktur.

18. TL LAKDA (Team Leader Layanan Kepada Debitur dan Aset) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas manajemen layanan kepada debitur dan pengelolaan aset perusahaan.
    b. Mengelola proses penagihan, pembayaran, dan penyelesaian klaim dari pelanggan atau debitur.
    c. Menangani manajemen aset perusahaan termasuk pengadaan, pemeliharaan, dan pengelolaan inventaris..
19. TL K3L KAM (Team Leader Keselamatan dan Kesehatan Kerja & Kemitraan dan Aliansi) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Memimpin tim yang bertanggung jawab atas kegiatan keselamatan dan kesehatan kerja (K3) serta pengembangan kemitraan dan aliansi perusahaan.
    b. Melakukan pemantauan terhadap implementasi kebijakan K3 dan program-program kesehatan kerja.
    c. Mengelola hubungan dengan mitra, asosiasi, dan lembaga eksternal untuk membangun kemitraan dan aliansi yang strategis..
20. TL MAP (Team Leader Manajemen Aset dan Pengadaan) mempunyai tugas dan tanggung jawab sebagai berikut:

a. Mengelola inventarisasi aset perusahaan, termasuk pemantauan dan pemeliharaan aset, serta pembaruan inventaris.
b. Menangani proses pengadaan barang dan jasa perusahaan, mulai dari perencanaan hingga pelaksanaan kontrak.
c. Memastikan kepatuhan terhadap kebijakan dan prosedur pengelolaan aset serta peraturan pengadaan yang berlaku.

21. TL REN (Team Leader Manajemen Rencana) mempunyai tugas dan tanggung jawab sebagai berikut:
    a. Merumuskan dan mengimplementasikan rencana-rencana bisnis dan operasional untuk mencapai tujuan perusahaan.
    b. Melakukan analisis situasi dan lingkungan bisnis untuk mengidentifikasi peluang dan tantangan yang relevan.
    c. Mengkoordinasikan proses perencanaan dan pengambilan keputusan dengan unit kerja lainnya dalam perusahaan.

DAFTAR PUSTAKA

Bahri, S. (2023). Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router. *Indonesian Journal of Education And Computer Science*, *1*(3), 136–147. https://doi.org/10.60076/indotech.v1i3.239

Dewa Made Julijati Putra, I Nyoman Namo Yoga Anantra, Putu Adhitya kusuma, Putu Damar Jagat Pratama, Gede Arna Jude Saskara, & I Made Edy Listartha. (2022). Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada Password Attack. *Jurnal Informatika Teknologi Dan Sains*, *4*(4), 461–466. https://doi.org/10.51401/jinteks.v4i4.2192

Febrian, R. A., Muhyidin, Y., & Singasatia, D. (2024). ANALISIS PENYERANGAN BRUTEFORCE TERHADAP SECURE SHELL (SSH) MENGGUNAKAN METODE PENETRATION TESTING. *Jurnal Ilmiah Sain Dan Teknologi*, *2*, 151–162.

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1), 56–69. https://doi.org/10.34010/gpsjournal.v7i1.8141

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. *Sudo Jurnal Teknik Informatika*, *1*(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Hendita, G., & Kusuma, A. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing*, *2*. https://doi.org/10.1515/zwf-1997-921-220

Mudzakkar, M., Siaulhak, S., & Jumarniati, J. (2023). Analisis Deteksi Dan

Pencegahan Eksploitasi Jaringan Brute Force Exploit Menggunakan Firewall Pada Kantor Bappeda Kota Palopo. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *2*(4), 1097–1106. https://doi.org/10.54443/sibatik.v2i4.718

Rahmah, S. A. (2023). *Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web*. *2*(3), 112–119. https://doi.org/10.56427/jcbd.v2n3.235

Sampurna, M. R. (2022). *Implementasi Hydra, FFUF, dan WFUZZ dalam Brute Force DVWA*. *1*(2), 102–112. https://jurnal.netplg.com/

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal …*, *6*(1), 2319–2327. http://journal.upy.ac.id/index.php/pkn/article/view/2989