IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING*

SKRIPSI

Oleh:
Yuniaman Mendrofa
190210054

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING*

SKRIPSI

Untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana

Oleh:
Yuniaman Mendrofa
190210054

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2023

SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Yuniaman Mendrofa

Npm : 190210054

Fakultas : Teknik dan Komputer

Program Studi : Teknik Informatika

Menyatakan Bahwa "Skripsi" yang saya buat dengan judul:

IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING*

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau di terbitkan oleh orang lain, kecuali yang secara tertulis dikutip di dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah skripsi ini digugurkan dan gelar yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun.

Batam, 2 Agustus 2023

Materai 10000

Yuniaman Mendrofa

190210054

iii

IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING*

SKRIPSI

Untuk memenuhi salah satu syarat
Memperoleh gelar Sarjana

Oleh:
Yuniaman Mendrofa
190210054

Telah disetujui oleh Pembimbing pada tanggal
Seperti tertera di bawah ini

Batam, 3 Agustus 2023

Rahmat Fauzi, S.Kom., M.Kom
Pembimbing

ABSTRAK

Perkembangan teknologi dari hari kehari semakin meningkat, dimana para ahli mengembangkan ilmu pengetahuannya baik dalam bidang industri, kesehatan, keamanan jaringan dan lainnya. PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto merupakan perusahaan air dibatam yang menjaga keamanan pengelolahan air minum. Namun pada sistem yang digunakan oeh perusahaan masih terdapat Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadapa keamanan data, selain itu dalam suatu sistem jaringan komputer terdapat bentuk ancaman baik dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya, Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port. Port Knocking* memang merupakan salah satu metode keamanan yang digunakan untuk mengamankan akses ke port-port tertentu di sebuah perangkat jaringan, seperti server. Prinsip utama dari port knocking adalah bahwa akses ke port yang dibatasi hanya akan dibuka jika ada rangkaian permintaan koneksi yang tepat dari sumber yang sah. Selain Port Knocking, ada banyak metode keamanan lainnya yang dapat digunakan untuk melindungi jaringan, seperti penggunaan VPN, firewall yang dikonfigurasi dengan baik, dan manajemen hak akses yang ketat. Penting untuk mempertimbangkan kebutuhan keamanan dan fleksibilitas yang tepat untuk lingkungan jaringan tertentu saat memilih dan mengimplementasikan metode keamanan yang sesuai.

Kata kunci: Jaringan; Keamanan; *Port Knocking*

ABSTRACT

Technological developments are increasing day by day, where experts develop their knowledge both in the fields of industry, health, network security and others. PT Air Batam Hulu is a company whose address is Building A-WTP Moya Muka Kuning Jl. Letjend Supranto, which is a water company in Batam that maintains the security of drinking water management. However, in the system used by the company there are still parties who are not authorized to hack so that it is vulnerable to infiltration of data security, besides that in a computer network system there are forms of threats both physically and logically such as Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Cracker and others. One of the intrusions that are currently successfully hacked and are often carried out are UML sites, Malware, Trojans, Viruses, and port scanning. Port Knocking is a security system that aims to open or close block access to certain ports using a firewall on network devices by sending certain packets or connections. Connections in the form of TCP, UDP, and ICMP protocols. So to enter and use access to certain ports that have been restricted, the user must first tap by entering the rule which must be done first. Rules which are only known by the network provider (network administrator). A system must have a balance between security and flexibility. One way to achieve such a system is by using firewall access. By using a firewall, we can indirectly define trustworthy and untrusted users by using the IP device as a filter criterion.

Keywords: Network; Security; Port Knocking

KATA PENGANTAR

Atas berkat dan rahmat Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratn untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati. Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terimakasi kepada:

1. Ibu DR.Nur Elfi Husda,S.Kom.,M.Si Selaku Rektor Universitas Putera Batam;
2. Bapak Welly Sugiyanto,S.T.,M.M Selaku Dekan Fakultas Teknik dan Komputer;
3. Bapa Andi Maslan,S.T.,M.Si Selaku Ketua Program Studi Teknik Informatika;
4. Bapak Sunarsan Sitohang, S.Kom., M.Kom Selaku Pembimbing Akademik pada Program Studi Teknik Informatika Universitas Putera Batam;
5. Bapak Rahmat Fauzi, S.Kom., M.Kom Selaku Pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam;
6. Dosen dan Staff Universitas Putera Batam;
7. Selaku Kedua orang tua penulis yang selalu mendoakan dan memberikan dukungan sehingga skripsi ini dapat terselesaikan;
8. Keluarga penulis yang selalu memberikan dukungan dan motivasi kepada penulis;
9. Teman-teman seperjuangan yang bersedia membagi ilmu dan sharing pendapat;
10. Semua pihak yang telah bersedia meluangkan waktu, tenaga dan pikiran dalam memberikan data dan informasi selama penulis membuat skripsi ini yang tidak dapat disebutkan satu persatu.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan berkatNya, Amin.

Batam, 3 Agustus 2023

Yuniaman Mendrofa

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan jamandari hari kehari semakin meningkat, dimana para ahli mengembangkan ilmu pengetahuannya baik dalam bidang industri, kesehatan, keamanan jaringan dan lainnya. Semakin meluasnya perkembangan pembangunan terhadap teknologi semakin banyak juga pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan, oleh sebab itu maka aplikasi yang digunakan oleh pengguna yang terhubung secara langsung dengan internet harus mewaspadain terjadinya penyusupan oleh pihak yang tidak berwenang, karena pada saat sekarang ada banyak pengguna internet menjadi korban penyusupan. Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML*, *Malwere*, *Trojan*, *Virus*, dan pemindaian *port*. Menggunakan jaringan, pemindaian *port* adalah sebuah metode untuk menemukan *port* komputer yang terbuka.

PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto merupakan perusahaan air dibatam yang menjaga keamanan pengelolahan air minum. Namun pada sistem yang digunakan oleh perusahaan masih terdapat Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadapa keamanan data, selain itu dalam suatu sistem jaringan komputer terdapat bentuk ancaman baik

dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya, Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port.*

Jaringan komputer adalah sekumpulan terminal komunikasi atau perangkat yang saling terhubung dengan tujuan memungkinkan berbagi informasi dan data secara efisien. Jaringan komputer memungkinkan komputer-komputer client untuk berkomunikasi, berbagi sumber daya, dan mengakses data dari server. Namun, bersama dengan manfaatnya, jaringan komputer juga menghadapi berbagai ancaman keamanan. Beberapa bentuk kerawanan pada jarinngan yang umum termasuk:, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker dan lainnya (Amien et al., 2020).

Security jaringan komputer memiliki kaitannya atas kerawanan data, karena itu kerawanan jaringan memiliki peran berharga dalam lindungi data sama sekali tiada memiliki wewenang. Serbuan bisa bertujukan kepada intansi,perusahaan atau lembaga tertentu. Penyusupan terhadap data dilakukan dengan melihat celah-celah pada jaringan komputerdan salah satunya melalui *port-port*. Untuk mengatasi serangan pada *port* itbuatlah langkah yang sesuai dengan security keamanan yaitu *port knocking. Port Knocking* adalah bentuk sistem *security* guna untuk menjaga jaringan dengan cara menutup akses *port* yang tidak memiliki hak untuk dapat megakses nya (Riska et al., 2018).

Port Knocking yakni metode keselamatan yang menggunakan firewall agar berfungsi buka dan tutup akses ke port yang digunakan untuk pengguna tertentu.

dengan mengirimkan paket atau koneksi tertentu dalam urutan yang telah ditentukan sebelumnya. Metode ini memungkinkan akses ke port-port yang sebelumnya diblokir hanya jika pola koneksi yang benar terdeteksi. *Port Knocking* memanfaatkan protokol TCP, UDP, atau ICMP untuk mengirimkan paket-paket tersembunyi dalam pola tertentu, sehingga firewall dapat mendeteksi dan meresponsnya dengan membuka jalan masuk pada port tersebut sesuai dengan aturan telah ditentukan. Sebab itu untuk dapat mengakses dan menggunakan port yang telah dibatasin pengguna diharuskan untuk mengetuk dan memasukan aturan yang harus dilakukan terdahulu. Aturan dibuat untuk hanya diketahui oleh *adimistrator* atau penyedia layanan. Sistem yang baik adalah sistem yang mempunyai tingkat seimbang antar *security* dengan fleksibelitas dengan melakukan hal yaitu pemakaian *firewall* dengan alat IP sebagai kriteria filter, maka dengan menggunakan tersebut dapat membedakan pengguna yang bisa diberikan kepercayaan dan yang tidak bisa (Sembiring et al., n.d.)

Konfigurasi routing pada *Router* dapat memakai statistik dan dinamis *routing* untuk mengatur raouting. Statistik tidak membutuhkan sumber daya sehingga dapat dipergunakan untuk jaringan komputer yang tidak terlalu besar. Namun statik *routing* akan sulit untuk admin dalam menjaga dan mengatur *konfogurasi table routing* sehingga dapat tetap digunakan jika pada jaringan yang lebih besar. Karena itu, *routing* dinamis sebagai pelengkap proses *routing* jaringan dengan otomatis,.

Proses dari isi data pada *routing table* dilakukan dengan otomatis dikenal sebagai *routing* dinamis. Dynamic *routing* diperlukan dalam kasus dimana ada pemakaian aturan lebih yang mungkin untuk pencapaian yang sama pada jaringan.

Protokol *routing* menata *router-router* untuk bisa melakukan komunikasi sama lainnya dan membagikan fakta *routing* yang dapat membarui isi *forwarding table* pada situasi jaringan yang dapat memungkinkan *router* untuk melihat situasi jaringan mana paling akhir dan melanjutkan data ke arah yang lebih tepat.

Berlandaskan uraian yang terdapat di atas maka peneliti mengambil judul penelitian ”**IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN *PORT KNOCKING***

1.2 Identifikasi Masalah

Dari penyampaian latar belakang maka dapat diidentifikasi sebagai berikut:

1. Pihak-pihak yang tidak berwenang melakukan peretasan sehingga rentan terjadinya penyusupan terhadapa keamanan data.
2. Dalam suatu sistem jaringan komputer terdapat bentuk-bentuk ancaman baik dari segi fisik ,maupun logika seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole, Hacker, Craker* dan lainnya
3. Salah satu penyusupan yang saat ini berhasil di retas dan sering dilakukan adalah situs *UML, Malwere, Trojan, Virus*, dan pemindaian *port.*

1.3 Batasan Masalah

Adapun batasan pada permasalahan penelitian ini yaitu:

1. Hanya mengimplementasikan *Knocking port* pada *Board Router Mikrotik*
2. Menggunakan alat pendukung yaitu 1 laptop untuk membuatnya.
3. Pengecekan soket port dilakukan dengan menggunakan aplikasi PuTTY.

1.4 Rumusan Masalah

Dari uraian yang ada pada penelitian, maka di bawah ini adalah rumusan masalah:

1. Bagaimana cara peningkatan keamanan jaringan komputer dengan metode *port knock?*
2. Bagaimana cara mengetikkan *port knock* pada *Router Board Mikrotik??*
3. Bagaimana cara administrator jaringan memantau jaringan?

1.5 Tujuan Penelitian

Tujuan penelitian yang akandi capai oleh peneliti yaitu:

1. Meningkatkan keamanan jaringan komputer
2. Untuk mengurangi terjadinya serangan terhadap komputer
3. Mencegah dan mengidentifikasi pengguna yang tidak berwenang di komputer.

1.6 Manfaat Penelitian

Dibedakan atas dua golongan manfaat penelitian yaitu:

1.6.1 Manfaat Teoritis

1. Bagi Peneliti

   Sebagai ilmu pengetahuan baru tentang cara implemetasi *security* jaringan mempergunakan *port Knocking*

2. Bagi Pembaca

   Sebagai masukan kepada pembaca agar mengetahui dalam keamanan *Router OS Mikrotik* serta monitoring jaringan.

3. Bagi Akademisi

   Sebagai refernsi tambahan bagi peneliti selanjutnya tentang keamanan jaringan

1.6.2 Manfaat Praktis

1. Untuk dapat membantu mengamankan jaringan komputer

2. Untuk memudahkan banyak organisasi saling bertukar informasi tanpa perlu khawatir tanpa ada gangguan dari serangan *cracker*

BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Pengertian Jaringan Komputer

Jaringan komputer adalah sekumpulan jumlah terminal komunikasi-komunikasi dan berbagi informasi antara dua komputer atau lebih. Jaringan komputer memungkinkan integrasi data pada tiap komputer *client*, agar data yang diperoleh lebih relavan dapat diakses dan digunakan oleh pengguna dengan mudah. di dalam sistem jaringan komputer terdapat berbagai bentuk ancaman yang dapat membahayakan keamanan dan integritas jaringan serta data yang ada di dalamnya. Ancaman-ancaman ini dapat berasal dari segi fisik maupun logika, seperti *Sniffer, Spoofing, Preaking, Remote Attack, Hole*, *Hacker*, *Craker* dan lainnya (Amien et al., 2020).

2.1.2 Standart Jaringan Komputer

Untuk menjaga standar teknologi komunikasi yang konsisten, standar jaringan komputer sagat penting. Oleh sebab itu di bawah ini merupaka standar organisasi komputer yang berperan(Amien et al., 2020).

a. Internet Engineering Task Force (IETF)

Merupakan kunci dibalik pengembangan internet biasanya menggunakan jalan demokratis, terbuka, *Open standard* praktis dalam mengangkat yang ada dilapangan.

Gambar 2. 1 *Internet Engineering Task Force*
Sumber: (Amien et al., 2020)

b. International Telecomunications Union (ITU)

Merupaka strandar jaringan komputer dengan h sebuah kumpulan dari web regulator dan operator telekomunikasi secara tradisional pilih alur formal dan resmi.

Gambar 2. 2 *International Telecomunications Union*
Sumber: (Amien et al., 2020)

c. Internasional Standards Organizations (ISO)

ISO adalah organisasi internasional yang mengembangkan standar internasional dalam berbagai bidang, termasuk teknologi informasi dan komunikasi.

Gambar 2. 3 *Internasional Standards Organizations*
Sumber: (Amien et al., 2020)

d. *American National Standart Insitute (ANSI)*

Ini adalah organisasi pemerintah dan sektor bisnis yang bekerja dengan standar nasional.

Gambar 2. 4 *American National Standart Insitute*
Sumber: (Amien et al., 2020)

e. *Institute of Electrical and Electronics Engeeners (IEEE)*

Meupakan organisasi standar jaringan komputer internasional dengan mendahulukan kemajuan teknologi.

Gambar 2. 5 *Institute of Electrical and Electronics Engeeners*
Sumber: (Amien et al., 2020)

f. *Electronic Industries Association (EIA)*

Merupakan stadarisasi jaringan kompuer yang bertanggung jawab dalam mengembangkan standar industri untuk antar muka pemrosesan dan komunikasi data.

Gambar 2. 6 *Electronic Industries Association*
Sumber: (Amien et al., 2020)

g. Federal Communications Commision (FCC)

Adalah organisasi dalam mengatur dalam telekomunikasi raddio, vidio dan komunikasi satelit.

Gambar 2. 7 *Federal Communications Commision*
Sumber: (Amien et al., 2020)

2.1.3 Jaringan Berdasarkan Area

Menurut (Amien et al., 2020) menetapkan adanya jaringan pada komputer dapat dibagi atas kelompok area sehingga dapat diakses dan dilayani. Jaringan komputer terbagi atas empat macam area cakupan geografisnya:

1. PAN *(Personal Area Network),*

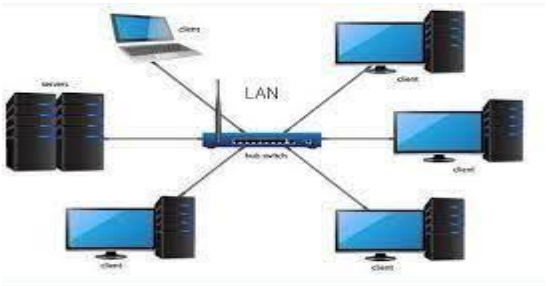
PAN adalah jaringan komputer yang sangat kecil dan biasanya mencakup area pribadi seseorang. Contoh PAN adalah jaringan antara perangkat pribadi seperti laptop, smartphone, tablet, dan perangkat wearable seperti smartwatch yang saling terhubung menggunakan teknologi seperti Bluetooth.

Gambar 2. 8 *Personal Area Network*
Sumber: (Firdaus et al., 2018)

2. LAN *(Local Area Network),*

Jaringan komputer lokal adalah jaringan komputer yang mencakup area yang lebih kecil, seperti kampus, gedung, kantor, rumah, sekolah, atau tempat lain. Saat ini, kebanyakan LAN menggunakan perangkat switch yang berbasis pada teknologi IEEE 802.3 Ethernet, yang memiliki kecepatan transfer data 10, 100, atau 1000 Mbps. Selain teknologi Ethernet, teknologi 802.11b (juga dikenal sebagai Wi-Fi) juga sering digunakan dalam pembentukan LAN.

.

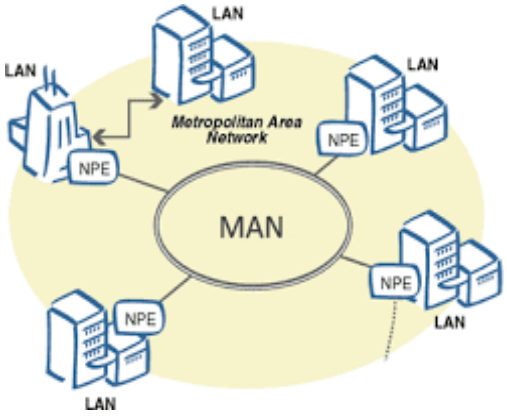


Gambar 2. 9 *Local Area Network*
Sumber: (Firdaus et al., 2018)

3. MAN (*Metropolitan Area Network),*

MAN yaitu jaringan komputer meliputi area geografis dengan luas dari pada LAN, biasanya mencakup wilayah kota atau daerah perkotaan. MAN

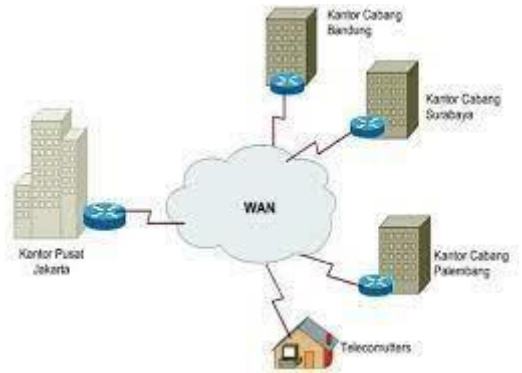
difungsikanuntuk menghubungkan beberapa LAN atau menghubungkan kantor-kantor yang berlokasi di berbagai bagian kota.. MAN dapat digunakan pada jaringan kabel dan nirkabel.



Gambar 2. 10 *Metropolitan Area Network*
Sumber: (Firdaus et al., 2018)

4. WAN *(Wide Area Network).*

Jaringan kompur dengan area yang cukup luas disebut dengan WAN atau Wide Area Network. Sebagai contoh dalam penerapan jaringan WAN adalah jaringan komputer yang menghubungkan wilayah, kota ataupun negara. Dengan demikian, penggunaan komputer di jaringan lokal bisa komunikasi antar pengguna komputer di jaringan lokal lainnya.



Gambar 2. 11 *Wide Area Network*
Sumber: (Firdaus et al., 2018)

2.1.4 Perangkat Jaringan

Berikut beberapa berbagai periferal jaringan komputer untuk mendukung dan mengoptimalkan kinerja sistem jaringan:

1. *Server,* bermanfaaat untuk media dalam menyimpan informasi berupa data pada komputer dengan mempunyai spesifikasi yang tinggi dari client karena tujuan utama server untuk melayani komputer client.
2. NIC (*Network Interface Card*), NIC atau dikenal dengan LAN Card *Expansion Board* yang digunakan supaya komputer dapat terhubung dengan jaringan. Ethernet terbagi menjadi empat jenis, yaitu ethernet (10 Mbit/detik), fast ethernet (100 Mbit/detik), gigabit ethernet (1000 Mbit/detik), dan tengig (10000 Mbit/detik)
3. Kabel jaringan, yakni media yang digunakan dalam penggabungan antar perangkat. Jenis kabel yakni:: *kabel coaxial, fiber optic dan twisted pai.*
4. *Hub and Switch,* yakni suatu perangkat jaringan pada komputer dengn manfaat untuk dapat menghubungkan beberapa komputer yang memiliki dua tipe yaitu *unmanaged switch* yang merupakan tipe termurah dan managed tipe termahal.
5. *Router,* bermanfaat sebagai penggabungan anatara jaringan LAN ke dalam suatu jaringan WAN serta mengelola lalu lintas dari data didalamnya. *Router* dapat melakukan jalur terbaik, karena memiliki tabel *routing* untuk melakukan perncatatan terhadap semua alamat dalam jaringan.
6. *Bridge,* berfungsi sebagai melanjutkan lalu lintas antar segmen jaringan dengan berlandaskan pada informasi sebuah titik.

7. Modem, adalah piranti dengan fungsi sebagai penggabungan perangkat komputer sebagai penyedia layanan internet atau ISP (*Internet Service Provider).* Modem bertugas mengubah sinyal digital dari komputer menjadi sinyal analog yang dapat ditransmisikan melalui jalur telepon atau kabel, dan sebaliknya, mengubah sinyal analog dari ISP menjadi sinyal digital yang dapat dimengerti oleh komputer.
8. Repeater: Repeater berfungsi untuk memperkuat dan meregenerasi sinyal jaringan yang lemah. Ketika sinyal jaringan melintasi kabel atau media transmisi tertentu, akan mengalami penurunan kekuatan sinyal seiring jarak perjalanannya.
9. Wireless Card: Wireless Card, juga dikenal sebagai wireless network adapter atau wireless NIC (Network Interface Card), yakni piranti wajib yang di pakai jika ingin terhubung ke jaringan nirkabel atau Wi-Fi.

2.2 Teori Khusus

2.2.1 Manfaat Jaringan Komputer

Terdapat fungsi atau manfaat pada jaringan komputer yakni:

1. Untuk dapat membagikan okumen ke piranti komputer lain dengan menggunakan jaringan internet .
2. Agar dapat menjaga managemen keamanan data, data akan semakin baik jika disimpan secara lebih terpusat selain itu dapat memudahkan admin dalam melakukan managemen data perusahaan yang penting.

3. Memudahkan dalam komunikasi antara team maupun denga orang lain yang berbeda geografis secara cepat dan akurat.
4. Menyampaikan informasi secara cepat tanpa batas waktu dan tempat
5. Membantu aktifitas manusia, sehingga kegiatan lebih efektif dan efisien.

2.2.2 Keamanan Jaringan

Security jaringan komputer memiliki kaitannya atas kerawanan data, karena itu kerawanan jaringan memiliki peran berharga dalam lindungi data sama sekali tiada memiliki wewenang. Serbuan bisa bertujukan kepada intansi,perusahaan atau lembaga tertentu. Penyusupan terhadap data dilakukan dengan melihat celah-celah pada jaringan komputerdan salah satunya melalui *port-port*. Untuk mengatasi serangan pada *port* itbuatlah langkah yang sesuai dengan security keamanan yaitu *port knocking. Port Knocking* adalah bentuk sistem *security* guna untuk menjaga jaringan dengan cara menutup akses *port* yang tidak memiliki hak untuk dapat megakses nya (Riska et al., 2018). Berikut beberapa jenis keamanan jaringan:

1. *Web Security,* berperan dalam melindungi alat pencarian atau website serta melindungi ribuan bahkan jutaan data pelanggan pada e-commerce. Bentuk *wwb security* biasanya seperti *secure socket layer*.
2. *Email Security,* bekerja untuk memblokir serangan-jerangan yang membahayakan dan berpotensi mencuri data-data penting, pada umumnya email security dilengkapi dengan sistem softare anti spam yang melindungi semua penggunanya.
3. *Wireless Security,* digunakan untuk mengantisipasi serangan virus dari luar.

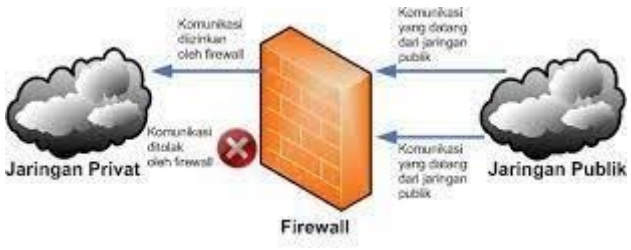
4. *Aplication Security,* digunakan untuk meningkatkan keamanan yag lebih tinggi dan terbebas dari serangan ciber.
5. *End Point Security,* bermanfaat untuk keamanan pada piranti yang slaing berhubungan dengan jaringan bisnis.
6. *Firewall,* digunakan untuk memblokir traffic yang berpotensi membahayakan
7. *Data Loss Prevention,* digunakan untuk menjaga data sensitif yang dirancang bekerja secara otomatis sehingga bisa mempermudah dalam proses pemeriksaan data pada jaringan tersebut.
8. *Behavioral Analytics,* berfungsi untuk melakukan analisis pada suatu jaringan dan memberikan notifikasi saat melakukan aktifitas-aktifitas mencurigakandan pelanggaran.
9. *Antivirus dan Maware,* bekerja dengan menghapus semua virus dan malware yag sudah tertanam pada perangkat yang digunakan.

2.2.3 Firewall

Sistem *Firewall* adalah mekanisme yang digunakan pada piranti keras dan pirantik lunak sebagai pencapaian dalam melindungi, membartasi atar bahkan menolak aktivitas suatu segmen di jaringan lokal ke jaringan eksternal yang tidak berada dalam cakupannya. *Firewall* bertanggung jawab untuk memastikan bahwa tidak ada yang ditambahkan di luar rentang yang diizinkan (Riska et al., 2018).

Menurut (Santoso et al., 2022) terdapat kelemahan potensial pada implementasi firewall tradisional. Firewall memang bekerja berdasarkan alamat IP dan port sumber dan tujuan dari paket data. Ini berarti bahwa firewall mungkin tidak

dapat secara langsung membedakan user atau pengguna individual yang dapat dipercaya dari yang tidak dapat dipercaya hanya berdasarkan informasi ini.



Gambar 2. 12 *Firewall*
Sumber: (Santoso et al., 2022)

2.2.4 Mikrotik

Menurut (Frado Pattipeilohy, 2016) Mikrotik merupakan sistem operais linux yang dibangun sebagai router network sehingga pengguna dapat mengaturnya dengan mudah melalui PC. (Asep & Dedi, 2020) Mikrotik pertama kali dibangun oleh JohnTrully dan Arnis pada tahu 1995. Banyak saat ini menganggap bahwa proxy sebagai router perusahaan. Sedangkan menurut (Ontoseno et al., 2017) Mikrotik adalah sistem operasi dan perangkat lunak komputer yang digunakan untuk mengubah komputer tradisional menjadi router dengan sistem operasi berbasis linux yang digunakan sebagai router network.

Gambar 2. 13 *Mikrotik*
Sumber: (Ontoseno et al., 2017)

2.2.4.1 Jenis-jenis mikrotik

Ada beberapa jenis mikrotik yang dapat diketahui diantaranya sebagai berikut:

1. Microtic Router OS

Mikrotik RouterOS adalah sistem operasi berbasis UNIX yang memiliki fitur seperti router, bridge, firewall, proxy server, dan hotspot. Anda dapat membuat router sendiri dengan menggunakan operating system (OS). Mikrotik Router OS adalah versi perangkat lunak Mikrotik yang dirancang khusus untuk router network. Ini memiliki banyak fitur yang dapat digunakan untuk jaringan IP dan nirkabel dan dapat diinstal pada CD-ROM pada komputer rumahan atau PC. Di antaranya adalah routing, hotspot, protocol tunneling point-to-point, DNS server, DHCP server, firewall, NAT, routing dan static routing, Date Rate Management (DRM) 9, Ipsec, Webproxy, caching DNS client, VRRP, Universal client, dan VRR. Berikut adalah kelebihan router OS:

1. Orang awam dapat memakainnya dengan mudah
2. Memiliki harga yang tejangkau dengan kualitas yang bagus
3. Terdapat fitur keamanan yang baik dalam menyimpan data.
4. Memiliki fitur yang baik dalam mengatur dan mengelola jaringan komputer.

Berikut ini beberapa kekurangan dari router OS:

1. Dalam pengolahan network sekala besar belum memiliki kemampuan
2. Apabila lupa password untuk log in sulit untuk melakukan setting ulang
3. Tidak sesuai di pakai dengan komputer yang spesifikasi rendah.
4.

2. *Microutic Router Board*

RouterBoard adalah perangkat keras *(hardware)* yang dikembangkan oleh Mikrotik. RouterBoard berukuran kecil dan lebih mudah digunakan, dan kita juga dapat melakukan proses instalasi RouterOS pada RouterBoard yang telah dikonfigurasi dengan baik. Fungsi RouterBoard Mikrotik adalah untuk memungkinkan pengguna menjalankan fungsi Router tanpa tergantung pada PC karena fungsi RouterBoard sudah ada pada RouterBoard. RouterBoard lebih kuat dan lebih kecil daripada PC yang diinstal pada RouterOS.

Kelebihan *Router*Board

1. Hemat biaya, karena *Router*board hanya membutuhkan daya sekitar 2.5 watt saja. 2. Proses Instalasinya yang mudah, karena hanya mengatur *Router* dan jaringan yang digunakan.
2. Spesifikasi untuk komputer tidak begitu tinggi.

2.2.5 VirtualBox

Merupakan software virtualisasi untuk mengistal suatu OS “Operating System yang mengacu pada kamus Oxford yaitu *“Convert (something)* untuk komputer *generated simulation or reality* yang berarti mengubah atau mengkonversi sesuatu ke dalam bentuk simulasi dari bentuk yang nyata atau real (Jurnal & Teknologi, 2021). Terdapat beberapa manfaat virtual box sebagai berikut:

1. Dapat digunakan oleh pemula tanpa harus mengistal operating sistem dan tanpa mengcopy data ke hardisk

2. Dapat menginstal sebagian operating sistem dengan cara Cuma-Cuma tanpa harus mempermanetkan e hardisk.
3. Tidak perlu membeli hardware-hareware baru untuk menggunakan banyak operating sistem

Berikut fungsi dari virtual box:

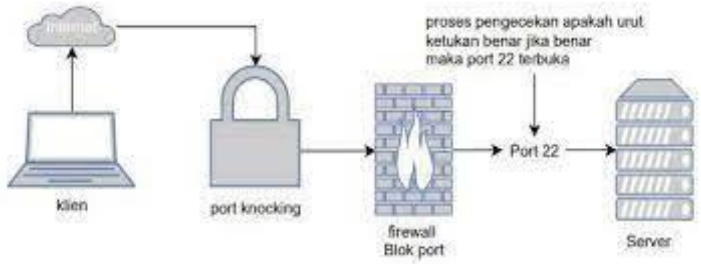
1. Berfungsi untuk dapat mencoba sistem operasi selain dari sistem operai utama
2. Berfungsi untuk menguji sistem operasi yang baru saja di rilis atau masih dalam tahap pengujian
3. Berfungsi untuk melakukan simulasi jaringan
4. Berfungsi untuk aplikasi virtual mechine pengganti fisik PC
5. Dapat digunakan untuk mensimulasikan tes keamanan terlepas dari sistem operasi atau web.

Gambar 2. 14 *Virtual Box*
Sumber: (Jurnal & Teknologi, 2021)

2.2.6 Port Knocking

Sistem keamanan disebut juga dengan *port knocking* yaitu dengan menggunakan *firewall* pada perangkat jaringan untuk membuka atau menutup akses *block ke port* tertentu dengan mengirimkan paket atau koneksi tertentu seperti

protokol TCP, UDP maupun ICMP. adalah sistem keamanan yang bertujuan untuk membuka atau menutup akses port tertentu dengan menggunakan firewall pada perangkat jaringan dengan mengirimkan paket atau koneksi tertentu. Koneksi berupa TCP, UDP dan ICMP. Maka untk dapat mengakses dan menggunakan port yang telah dibatasin pengguna diharuskan untuk mengetuk dan memasukan rule yang harus dilakukan terlebih dahulu. Aturan yang hanya diketahui oleh admisistrator jaringan atau penyedia layanan. Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Salah satu cara untuk mencapai keseimbangan adalah dengan menggunakan akses firewall. Dengan menggunakan alat IP sebagai kriteria filter, secara tidak langsung dapat membedakan antara pengguna yang dipercaya dan tidak dipercaya (Sembiring et al., n.d.)

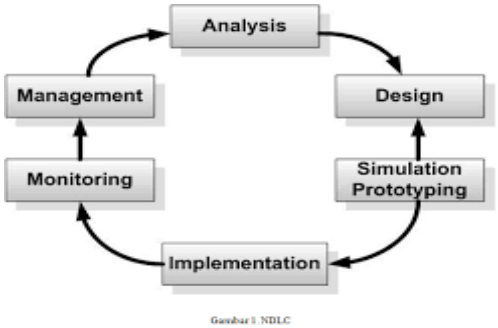


Gambar 2. 15 *Port Knocking*
Sumber : (Ontoseno et al., 2017)

2.3 Metode Network Development Life cycle (NDLC)

Merupakan suatu teknik analisis terstrutur yang digunakan dalam merencanakan dan mengelola proses pengembangan sistem. Meskipun belum ada standar yang ditetapkan untuk NDLC yang secara universal telah disepakati, namun desainer jaringan banyak yakin bahwa NDLC dapat menggantikan SDLC. NDLC adalah model yang mendeskripsikan proses siklus pengembangan dan perancangan

suatu jaringan komputer. Sebagaimana model pengembangan sistem jaringan yang berisi tahapan, fase, langkah atau prosedur yang spesifik. Kata lain dari NDLC merupakan pusat deskriptif dari siklus pembangunan sistem jaringan yang digambarkan secara menyeluruh, agar proses dan tahapan pembangunan sistem jaringan dalam berjalan secara berkesianmbungan(Ontoseno et al., 2017).



Gambar 2. 16 *NDLC*
Sumber : (Ontoseno et al., 2017)

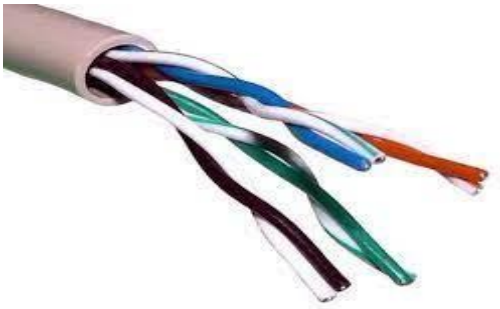
2.4 *Tools*/*Software* Pendukung

Adapun tools yang digunakan pada penelitian ini yaitu:

1. *Laptop,* merupakan komputer pribadi yang berukuran relatif kecil dan ringan yang di gunakan sebagai perangkat untuk melakukan implementasi

Gambar 2. 17 Leptop
Sumber: (Riska et al., 2018)

2. Kabel UTP (Unshileded Twisted Pair), merupakan kabel yang digunakan secara khusus untuk transmisi data, yang terdiri atas pasang (biru, orange, hijau dan coklat) kabel tersebut dipilih menurut aturan tertentu dan digunakan untuk mentrasfer atau menerima data. Fungsi utama kabel ini untuk menghubungkan antar peralatan yang berhubungan dengan komputer network. Kabel ini sering disebut juga dengan kabel LAN.



Gambar 2. 18 Kabel UTP
Sumber: (Riska et al., 2018)

3. Konektor RJ45, merupakan kabel konektor ethernet yang memiiki fungsi sebagai konektor topologi jaringan komputer . RJ adalah singkatan dari Registered Jack yang merupakan standar peralatan pada jaringan yang mengatur tentang pemasangan kepala konektor dan urutan kabel yang menghubungkan dua atau lebih peralatan telekomunikasi.

Gambar 2. 19 Rj45
Sumber: (Riska et al., 2018)

4. Switch, adalah komponen jaringan yang digunakan untuk menggabungkan beberapa perangkat komputer dalam sebuah jaringan sehingga pengguna dapat melakukan pertukaran informasi atau data.

Gambar 2. 20 Switch
Sumber: (Riska et al., 2018)

5. Modem, merupakan sebuah perangkat yang berfungsi untuk menyambungkan perangkat komputer, leptop dan smartphone ke jaringan internet.

Gambar 2. 21 Modem
Sumber: (Riska et al., 2018)

6. Winbox, merupakan software atau unity yang digunakan untuk meremote sebuah server mikrotik kedalam mode GUI *(Graphical User Interface)* melalui operating system windows.

Gambar 2. 22 Winbox
Sumber: (Riska et al., 2018)

2.4 Penelitian Terdahulu

Pada penelitian ini akan memaparkan penelitian sebelumnya yang relavan terhadap topik yang akan diteliti oleh peneliti, adapun penelitian sebelumnya sebagai berikut:

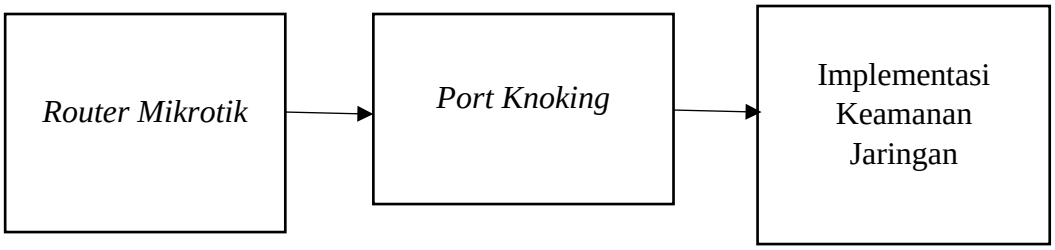
1. Berdasarakan penelitian yang dilakukan oleh (Firdaus et al., 2018) dengan judul "Implementasi Keamanan Mikrotik Menggunakan Metode *Simple Port Knocking* Pada SMA N1 Ngantang" Jurnal Teknologi Informasi ISSN 2086-2989 vol 9 no 2 tahun 2018 memberi kesimpulan bahwa dengan dilakukan *port Knocking* membuat admin tidak lagi merasa khawatir akan *user* yang tidak memiliki orientasi login kedalam mikrotik.
2. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Jurnal & Teknologi, 2021) dengan judul"Implementasi *Port Knocking* Untuk Keamanan Jaringan SMKN1 Sumbawa Besar" Jurnal Informatika Tekologi dan Sains ISSN 2686-3359 vol 3 no 2 tahun 2021 menarik kesimpulan bahwa dalam meningkatkan keamanan jaringan dan dapat membantu adminisrator dalam mengamankan **Mikrotik** Routerboard pada jaringan komputer .

3. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Amien et al., 2020) dengan judul "Implementasi Keamanan Jaringan Dengan Iptables Sebagai *Firewall* Menggunakan Metode *Prort Knoking*" Jurnal Fasilkom ISSN 2089-3353 vol 10 no 2 tahun 2020, menarik kesimpulan bahwa konfigurasi yang dikembangkan ternyata memberikan kinerja yang cukup untuk keamanan serangan dari luar yang memanfaatkan *port*.
4. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Santoso et al., 2022)dengan judul "Implementasi Keamanan Jaringan Menggunakan *Port Knocking* " Jurnal Janitra Informatika dan Sistem Informasi vol 2 no 2 tahun 2022 memberi kesimpulan bahwa dengan pendekatan *port Knocking* untuk keamanan jaringan dimungkinkan dapat mengurangi insiden pihak yang tidak bertanggung jawab menyalahgunakan akses *Router*.
5. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Riska et al., 2018) dengan judul "Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode *Port Knocking*" Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI) vol 1no 2 tahun 2018, Memberi kesimpulan bahwa perancangan dan pembangunan program *port Knocking* dapat menentukan *port* mana saja yang dapat diakses *client.*
6. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Ulum, 2018) dengan judul "Desain Keamanan Jaringan Pada Mikrotik *Router* OS Menggunakan Metode *Port* Knoking" Jurnal TeknoInfo vol 2 no 2 tahun 2018 ISSN 2615-224X menyimpulkan bahwa *port Knocking* sangat cocok di terapkan untuk menjaga *Router* dari akses orang lain yang tidak berhak mengaksesnya.

7. Berdasarkan jurnal penelitian yang telah dilakukan oleh (Sistem et al., 2017) dengan judul "Penerapan Sistem Pengamanan *Port* Dalam Layanan Jaringan Menggunakan*Port Knocking*" Jurnal LPKIA vol 10 no 2 tahun 2017, menyimpulkan bahwa pengujian yang telah dilakukan menggnakan metode *port Knocking* yang dikombinasikan dengan *firewall* di mikrotik dapat memberikan sistem keamanan autentifikasi pada server layanan jaringan dan dapat mengamankan server dari 3 serangan yaitu hydra,DoS dan Telnet yang menggunakan protocol TCP.

2.5 Kerangka Pemikiran

Berdasarkan teori-teori yang telah diperoleh dan dijelaskan, maka ruang lingkup penelitian ini diuraikan sebagai berikut:



Gambar 2. 23 Kerangka Pemikiran

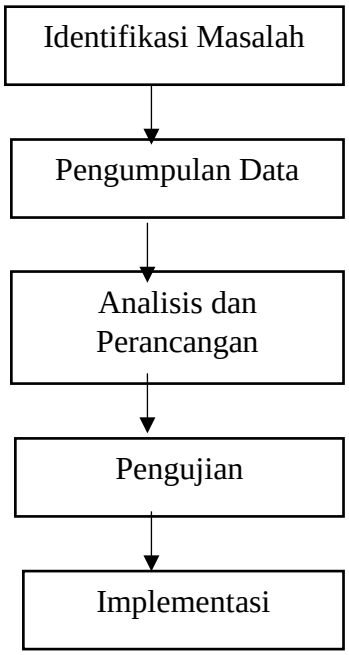
Sistem keamanan jaringan untuk melindungi *Router* mikrotik dengan menggunakan *port Knocking* dalam memengimplementasi keamanan jaringan informasi mecegah penyerang mengakses *Router* mikrotik.

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Langkah berikutnya yang perlu diperbuat yaitu membuat desain penelitian dan membuat rancangan langkah-langkah yang mendeskripsikan proses penelitian berupa tabel dan diagram agar penelitian lebih terfokus pada tujuan, sasaran yang ingin dicapai.



Gambar 3. 1 Desain Penelittian
Sumber : Data Penelitian 2023

Keterangan:

1. Identifikasi Masalah pada penelitian ini adalah sistem jaringan komputer terdapat bentuk-bentuk ancaman baik dari segi fisik, maupun logika seperti *Sniffer, Spoofing,* dan penyusupan yang saat ini berhasil di retas dan sering

dilakukan adalah situs *UML, Malwere, Trojan, Virus,* dan pemindaian *port* sehingga perlu dilakukan keamanan jaringan.

2. Pengumpulan Data, merupakan langkah untuk mendapatkan data yaitu dnegan cara melakukan wawancara, observasi dan studi pustaka
3. Analisis dan desain, merupakan penguraian suatu subjek menjadi suatu kesatuan untuk mencari solusi dan faktor-faktor penting dalam pemecahannya
4. Pengujian, merupakan tahap proses pengujian terhadap sistem yang telah dirancang yaitu mikrotik.
5. Implementasi, merupakan tahap dilakukannya penerapan *port Knocking* pada mikrotik untuk keamanan jaringan.

3.2 Metode Pengumpulan Data

Langkah ini dilakukan untuk menganalisis kebutuhan permasalah yang ada analisis keinginan pengguna dan analisis topologi jaringan yang ada saat itu. Metode yang digunakan adalah sebagai berikut:

A. Wawancara dilakukan dengan para pemangku kepentingan, dalam hal ini PT Air Batam Hulu, termasuk tentang manajemen saat ini dan harapan yang diinginkan.
B. Observasi, Observasi langsung di PT Air Batam Hulu untuk hasil yang lebih otentik, yang nantinya akan menjadi preview desain untuk memasuki tahap desain selanjutnya.

3.3 Tahap Analisis

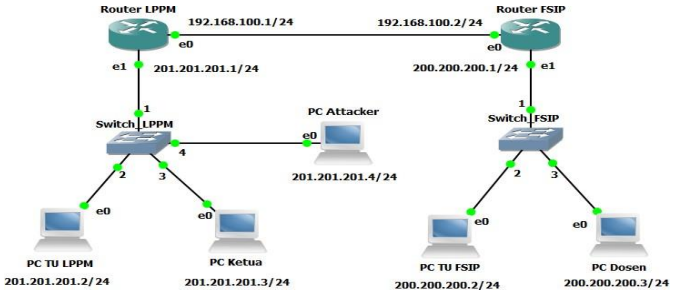
Adapun analisis yang digunakan adalah degan menggunakan metode *Network Development Life Cycle* (NDLC) dengan tahapan-tahapan sebagai berikut:

1. Analisis, tahapan ini merupakan tahapan dimana dilakukan dalam menganalisis kebutuhan, analisis permasalahan yang muncul, analisa keinginan *user*, dan analisa jaringan yang sudah ada saat ini yaitu dengan melakukan metodde wawancara, *survey*, dokumentasi dan menelaah data yang ada.
2. Desain, dari data yang telah ada sebelumnya, maka dilakukan desain jaringan yang dibangun secara interkoneksi dengan harapan desain tersebut dapat meggambarkan kebutuhan secara keseluruhan dari desain akses data, perkabelan dan lainnya.
3. *Simulation*, merupakan bantuan tools yang digunakan untuk melihat kinerja awal dari *network* yang akan dibangun dan sebagai bahan presentasi dan sharing dengan team work, pada kasus ini menggunakan **virtual box.**
4. *Implementation,* merupakan tahapan yang dilakukan untuk menerapkan semua yang telah direncanakan dan didesain sebelumnya.
5. *Monitoring,* merupakan tahapan yang penting untuk mengamati apakah berjalan sesuai dengan keinginan dan tujuan awal.

3.3.1 Desain Keamanan jaringan lama

Pada tahap ini dilakukan desain topologi jaringan yang ada pada PT Air Batam Hulu dengan menggunakan simulator prototype yaitu dengan GNS3.

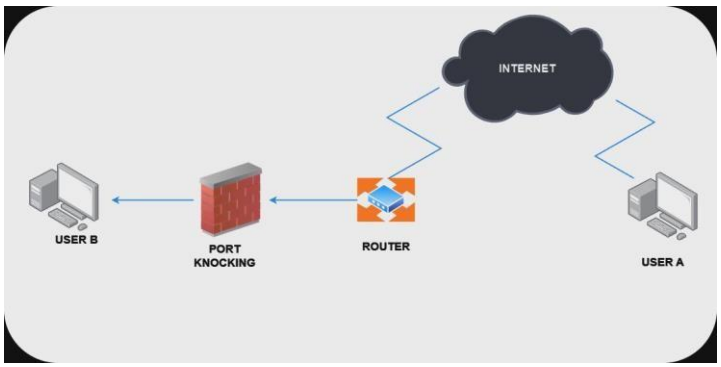
Adapun komponen yang diperlukan antara lain dua buah *Router* , dua buh switch , 4 pc client dan 1 buat pc sebagai attacker.



Gambar 3. 2 *Desain*
Sumber: Data penelitian 2023

3.3.2 Desain Keamanan jaringan baru

Dalam perancangan topologi sistem jaringan pada Pt Air Batam Hulu dengan menggunakan topologi jaringan star karena topologi tersebut kerusakan jaringan yang sedang berjalan dan cukup baik digunakan sebagai keamanan jaringan, karena menggunakan router yang *diremote* menggunakan winbox. Berikut ini merupakan gambaran topologi yang akan dibangun.



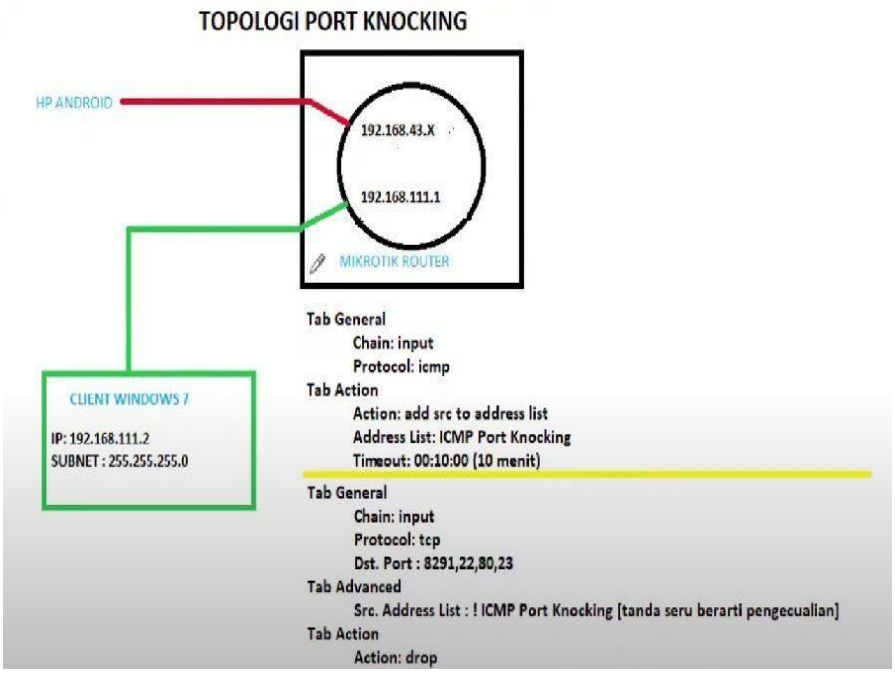
Gambar 3. 3 Desain jaringan
Sumber: Data penelitian 2023

Berdasarkan topologi jaringan pada gambar diatas maka Konfigurasikan *firewall* seperti *Port Knocking Authentication* yang terpasang di router. Aturan *firewall* dibangun sebagai aturan yang harus dibangun oleh pengguna/admin saat

mengakses router sebagai administrator. Sementara itu, fungsi PC penyerang adalah untuk menguji fungsi *port Knocking* pada kedua router untuk melihat apakah berhasil bekerja.

3.3.3 Desain *port* Kocking

Pada tahap ini dilakukan desain *port* knocking keamanan jaringan dengan menggunakan *simulator prototype*



Gambar 3. 4 Desain jaringan
Sumber: Data penelitian 2023

3.4 Lokasi dan Jadwal Penelitian

Penelitian yang baik adalah penelitian yang dapat dikerjakan dan selesai dengan waktu yang tepat. Berikut di bawah ini lokasi penelitian dan jadwal penelitian yang digunakan oleh peneliti untuk menyelesaikan hasil penelitian nya.

3.4.1 Lokasi Penelitian

Lokasi tempat diadakan penelitian atau tempat peneliti memperoleh data penelitian beradda di PT Air Batam Hulu adalah sebuah perusahaan yang beralamat Gedung A-WTP Moya Muka Kuning Jl.Letjend Supranto

Gambar 3. 5 Lokasi Penelitian
Sumber: Data Penelitian 2023

3.4.2 Jadwal Penelitian

Jadwal penelitian merupakan waktu yang ditempuh oleh peneliti menyelesaikan perancangan maupun laporan penelitian sehingga dapat terselesaikan dengan baik. Berikut jadwal penelitian yang dibuat kedalam bentuk tabel

Tabel 3. 1 Jadwal Penelitian

No	Kegiatan	Tahun 2023																				
		Feb 2023				Maret 2023				April 2023				Mai 2023				Juni 2023		Juli 2023		
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	1	2
1	Pengajuan Judul																					
2	Susun Bab I																					
3	Susun Bab II																					
4	Susun Bab III																					
5	Susun Bab IV																					
6	Susun Bab V, Daftar Pustaka, Lampiran																					

Sumber : Data Penelitian 2023