BAB II

TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Penelitian terdahulu ini menjadi satu acuan penulis dalam membuat laporan akhir sehingga dapat memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Berikut merupakan penelitian terdahulu berupa beberapa jurnal yang terkait dengan judul laporan akhir penulis.

Pada penelitian sebelumnya yang dilakukan (Riska dkk, 2018) dalam jurnal yang berjudul **"Sistem Keamanan Jaringan Komputer dan Data Dengan Menggunakan Metode PortKnocking"**. Permasalahannya adalah Keamanan data dan informasi membuat teknologi informasi harus diperbaharui setiap saat. Banyak serangan yang dilakukan oleh orang-orang yang tidak bertanggung jawab melakukan serangan terhadap server. Serangan-serangan tersebut sering dilakukan pada suatu port–port yang dalam keadaan terbuka, sehingga nantinya akan membuat orang–orang yang tidak mempunyai hak akses maupun yang tidak berkepentingan dapat dengan mudah mengendalikan port–port yang telah dimasuki. Metode yang digunakan adalah metode *Port Knocking* merupakan sebuah metode untuk membangun komunikasi dari mana saja, dengan perangkat komputer yang tidak membuka *port* komunikasi apapun secara bebas. Dengan kata lain, perangkat komputer ini tidak memiliki *port* komunikasi yang terbuka bebas untuk dimasuki, tetapi perangkat ini masih tetap dapat diakses dari luar. Berdasarkan ujicoba yang telah dilakukan maka dapat diperoleh hasil analisa antara lain, Program *port knocking* dapat menentukan *port* yang dapat diakses oleh klien, Program *port knocking* dapat menentukan *port* yang tidak dapat diakses oleh klien, Apabila tidak mendapat akses, *klien* tidak dapat melakukan *sharing* file atau berkomunikasi dengan server.

Pada penelitian sebelumnya yang dilakukan (Mardiyana, 2015) dalam jurnal yang berjudul **"Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik**

Pada Laboratorium Komputer STIKOM Bali". Permasalahannya adalah bentuk ancaman yang datang baik langsung maupun tidak langsung akan mengganggu kegiatan yang sedang berlangsung dalam jaringan di laboratorium komputer. Dalam rangka melindungi kemungkinan serangan-serangan tersebut perlu di terapkan konsep firewall. Metode Penelitian yang digunakan adalah pengumpulan informasi, analisis, perancangan / *selection design*. Penelitian tersebut menghasilkan kesimpulan yaitu Sistem yang dirancang dapat memenuhi kebutuhan sistem khususnya dalam melakukan *packet filter* sesuai dengan kebutuhan pada Laboratorium Komputer STIKOM Bali mampu mengamankan jaringan pada Laboratorium Komputer dengan melakukan filter terhadap lalu lintas data yang melewati router sesuai dengan ketentuan yang telah rancang.

Pada penelitian sebelumnya yang dilakukan oleh (Muzakir dkk, 2019) yang berjudul **"Analisis Kinerja Packet Filtering Berbasis Mikrotik Routerboard Pada Sistem Keamanan Jaringan"**. Permasalahannya adalah sistem keamanan dari pengguna yang terhubung secara langsung kedalam jaringan internet bisa mendapat berbagai jenis serangan baik secara langsung maupun tidak langsung yang akan memberikan dampak pada aktifitas yang terjadi pada jaringan internet tersebut. Metodologi penelitian yang diterapkan yaitu eksperimen, dimana dimulai dari pembentukan dan pemeliharaan kelompok, kontrol, memberikan keputusan yang terjadi, mengontrol pada setiap faktor-faktor yang relevan, melakukan perubahan yang diizinkan, dan pada akhirnya adalah monitoring terhadap hasil pengukuran. Hasil yang didapatkan dari penelitian tersebut adalah sistem keamanan filtering rule dapat memblokir akses protokol http maupun https serta kinerja sistem keamanan filtering mampu melakukan blokir terhadap beberapa akses ke situs web tertentu.

Pada penelitian sebelumnya yang dilakukan oleh (Imam Marzuki, 2017) yang berjudul **"Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux"**. Permasalahannya adalah Suatu jaringan komputer biasanya terdiri dari server dan *client*. Server dikendalikan oleh seorang administrator. Salah satunya dengan

melakukan *remote* server. Administrator yang me-*remote* suatu server haruslah orang yang berhak untuk mengakses server tersebut. Namun ada juga *attacker* yang dengan sengaja masuk kedalam sistem dan kemudian melakukan perubahan serta pengrusakan terhadap server. Salah satu upaya yang dilakukan untuk meningkatkan keamanan sebuah server adalah dengan menggunakan firewall. Tetapi firewall tidak mampu membedakan user yang dapat dipercaya. Firewall hanya mampu membedakan alamat IP yang diasumsikan digunakan oleh orang yang tidak dapat dipercaya. Sehingga dicari solusi untuk mengurangi kelemahan yang ada. metode ini salah satunya adalah dengan menggunakan metode port knocking. Metodologi yang digunakan pada jurnal ini yaitu dimulai dengan studi literatur, perancangan dan diakhiri dengan implementasi. Berdasarkan ujicoba yang telah dilakukan dapat diperoleh hasil analisa antara lain metode *port knocking* dapat mencegah penyerang dari pemindai sistem seperti *service* SSH dengan melakukan port *scanning*, sehingga *service* SSH tidak mudah dilacak dan diakses orang lain.

Dari penelitian-penelitian terdahulu berupa beberapa jurnal yang terkait dengan judul laporan akhir penulis. Pada judul laporan akhir penulis disini menggunakan metode *port knocking* untuk mengamankan router seperti pada penelitian (Riska dkk, 2018). Penulis juga menggunakan fitur firewall pada mikrotik seperti pada penelitian (Mardiyana, 2015) dan juga pada penelitian (Muzakir dkk, 2019) yang memakai metode *packet filtering* yang menutup situs-situs yang tertentu sedangkan penulis menggunakan metode *port knocking* dalam hal mengamankan jaringan. Penulis juga mengimplementasikan metode ini pada sistem operasi *Windows* sedangkan pada penelitian yang dilakukan (Imam Marzuki, 2017) mengimplementasikan pada sistem operasi *Linux.*

2.2. Router

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sasarannya melalui sebuah proses yang dikenal sebagai *routing*. *Router* berfungsi sebagai penghubung

antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. *Router* bertugas untuk menyampaikan paket data dari satu jaringan ke jaringan lainnya, jaringan pengirim hanya tahu bahwa tujuan jauh dari *router*. Selain itu, *router* juga memilih jalur untuk mencapai tujuan (Cartealy,2013).

Menurut (Cartealy,2013) *Router* dipasaran terbagi menjadi tiga yaitu:

1. *Router* PC (*Personal C*omputer) merupakan komputer dengan sistem operasi yang memiliki fasilitas untuk membagi dan men-sharing IP *address*, dimana perangkat (PC) yang terhubung ke komputer tersebut akan dapat menikmati IP *Address* atau koneksi yang disebarkan oleh sistem operasi tersebut.
2. *Router* Aplikasi merupakan suatu aplikasi yang dapat diinstal pada sistem operasi dimana memiliki kemampuan seperti *router*.
3. *Router Hardware* merupakan *hardware* yang memiliki kemampuan seperti router dari berbagai *hardware* yang memancarkan atau membagi IP *address* dan men-*sharing* IP *address*.

Gambar Mikrotik Router RB1100AHx4 dapat dilihat pada Gambar 2.1.

Gambar 2. 1 Mikrotik Router RB952Ui-5ac2nD (hAP-AC-Lite)

(Sumber**:** *www.mikrotik.co.id*)

2.3 MikroTik RouterOS

MikroTik *Router* OS, merupakan sistem operasi *Linux base* yang diperuntukkan sebagai sistem *network router*. Didesain untuk memberikan kemudahan untuk penggunanya. Administrasinya bisa dilakukan melalui *Windows Application* (WinBox). Selain itu instalasi dapat dilakukan pada *Standard* komputer PC (*Personal Computer*). PC yang akan dijadikan *router* mikrotik tidak memerlukan *resource* yang cukup besar untuk penggunaan standard, misalnya bertindak sebagai *gateway*. Untuk keperluan beban yang besar (*network* yang kompleks, *routing* yang rumit) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai (Fahlevi, 2013).

2.4 Winbox

2.4.1 Pengertian Winbox

Winbox adalah *utility* yang digunakan untuk konektivitas dan konfigurasi MikroTik menggunakan MAC Address atau protokol IP. Dengan winbox kita dapat melakukan konfigurasi MikroTik RouterOS dan RouterBoard menggunakan mode GUI dengan cepat dan sederhana. Winbox dibuat menggunakan win32 binary tetapi dapat dijalankan pada *Linux*, Mac OSX dengan menggunakan Wine. Semua fungsi winbox didesain dan dibuat semirip dan sedekat mungkin dengan fungsi console, sehingga Anda akan menemukan istilah-istilah yang sama pada fungsi console (Risyan, 2019).

2.4.2 Fungsi Winbox

Menurut (Risyan, 2019), Fungsi utama winbox adalah untuk setting yang ada pada mikrotik, berarti tugas utama windox adalah untuk mensetting atau mengatur mikrotik dengan GUI, fungsi winbox lebih rinci adalah:

1. *Setting* mikrotik router.
2. Untuk setting bandwith jaringan internet.
3. Untuk setting blokir sebuah situs.

2.5. ICMP (Internet Control Message Protocol)

Internet Control Message Protocol (ICMP) adalah protokol yang digunakan untuk memperoleh status dari suatu perangkat jaringan dengan mengirimkan pesan-pesan khusus yang dapat memicu pesan *reply* dari perangkat jaringan komputer. Pada kondisi perangkat jaringan normal, perangkat tersebut komputer dapat melakukan operasi dengan memanfaatkan infrastruktur komunikasi. Namun ada beberapa kondisi dimana koneksi jaringan terganggu, misalnya karena komputer *crash*, putusnya *link* komunikasi, atau perangkat jaringan mati. Pada situasi tersebut, protokol ICMP membantu untuk mendapatkan status dari perangkat-perangkat jaringan dengan mengirimkan *request* kepada perangkat tujuan. Perangkat tujuan jika dalam kondisi baik maka akan merespon pesan tersebut, sehingga komputer monitoring dapat mengambil kesimpulan bahwa perangkat tersebut berjalan dengan nomal. Contohnya, hubungan suatu perangkat monitoring dengan perangkat jaringan mengalami masalah (komputer), maka perangkat monitoring akan mengirimkan paket ICMP ke komputer tujuan yang bersifat *request*. Perangkat monitoring yang mengirimkan ICMP *Request* dapat mengetahui kondisi dari komputer tujuan dengan mengamati respon dari komputer yang bersangkutan. Jika perangkat monitoring tidak pernah mendapatkan ICMP *Reply* dari *host* yang dituju kemungkinan komputer tersebut dalam kondisi mati (Heryanto dkk, 2017).

2.6 TCP/IP (Transmission Control Protocol) / (Internet Protocol)

TCP/IP adalah protokol gabungan antara TCP (*Transmission Control Protocol*) dan IP (*Internet Protocol*). Kedua protokol ini mengatur komunikasi data dalam suatu proses pertukaran data antara komputer klien dan komputer server di dalam jaringan internet dan memastikan bahwa pengiriman data sampai ke alamat yang dituju. TCP berfungsi untuk melakukan proses koneksi, sementara IP bertugas memberikan pelabelan atau penomoran terhadap komputer yang akan menjadi tujuan dalam komunikasi pertukaran data. Komunikasi pertukaran data antara komputer di dalam suatu jaringan dengan protokol TCP/IP memerlukan antarmuka pemrograman aplikasi

(*Aplicaton Programming Interface*). Salah satu antarmuka tersebut dikenal dengan sebutan pemrograman socket. Rancangan perangkat lunak akuisisi data modul detektor gamma RosRoa menggunakan pemrograman socket (Amin dkk).

2.7. Firewall

2.7.1 Pengertian Firewall

Firewall adalah suatu mekanisme untuk melindungi keamanan jaringan komputer dengan menyaring paket data yang keluar dan masuk di jaringan. Paket data yang ’baik’ diperbolehkan untuk melewati jaringan dan paket data yang dianggap ’jahat’ tidak diperbolehkan melewati jaringan. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak yang dapat menfilter paket data.

Firewall juga berfungi untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Keamanan jaringan komputer akan tetap terjaga dengan disaringnya paket data yang keluar dan masuk didalam jaringan (Nanang dkk, 2011).

2.7.2 Fungsi Firewall

Menurut (Nanang dkk, 2011) Fungsi firewall, antara lain :

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.

   Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :

   a. Alamat IP dari komputer sumber

   b. Port TCP/UDP sumber dari sumber

   c. Alamat IP dari komputer tujuan

d. Port TCP/UDP tujuan data pada komputer tujuan

e. Informasi dari header yang disimpan dalam paket data

2. Melakukan autentifikasi terhadap akses.

3. Aplikasi proxy

Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.

4. Mencatat semua kejadian di jaringan

Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

2.8. Port Knocking

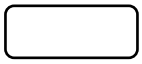
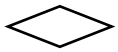
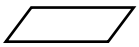
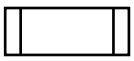
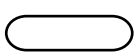
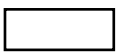
Port Knocking adalah sebuah metode sederhana untuk memberikan akses remote tanpa meninggalkan port dalam keadaan selalu terbuka. Hal ini akan memberikan perlindungan kepada server dari port scanning dan serangan scripts kiddies. Port Knocking memiliki metode buka port kepada suatu klien bila klien itu meminta, dan tutup kembali bila klien telah selesai. Untuk menjalankan metode ini, sebuah server haruslah memiliki firewall dan daemon untuk menjalankan metode port knocking yang berjalan di server tersebut. Dengan metode tersebut, *user* dituntut untuk memberikan autentikasi ke server agar firewall menulis ulang rulenya sehingga user diberi izin untuk mengakses port yang dimaksud. Dan setelah selesai, user mengirimkan autentikasi kembali untuk menutup port agar firewall menghapus rulenya yang ditulis sebelumnya untuk membuka port. Port Knocking adalah suatu metode komunikasi 2 arah yaitu (client dan server) di mana metode ini diterapkan dalam suatu sistem dengan port tertutup. Pada dasarnya cara kerja dari port knocking adalah

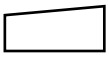
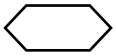
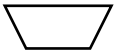
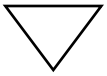
menutup semua port yang ada, dan hanya user tertentu saja yang dapat mengakses sebuah port yang telah ditentukan (Muzawi, 2016).

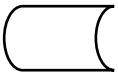
2.9. Flowchart

Menurut I Gusti Ngurah Suryantara (2009), badan alir (*flowchart)* adalah bagan (*chart*) yang menunjukan alir (*flow*) di dalam program atau prosedur sistem secara logika. Bagan alir digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi.

Tabel 2. 1. Simbol Flowchart

No.	Simbol	Nama Simbol	Keterangan
1.		*Alternate Process*	Menyatakan segala jenis operasi yang diproses dengan menggunakan mesin yang memiliki keyboard
2.		*Decision*	suatu penyelesaian kondisi dalam program
3.		*Data*	Mewakili data *input* atau *output*
4.		*Predefined Process*	Suatu operasi yang rinciannya di tunjukkan di tempat lain
5.		*Document*	Document *input* dan *output* baik untuk proses manual, mekanik atau komputer
6.		*Terminator*	Untuk menunjukkan awal dan akhir dari suatu proses
7.		*Process*	Kegiatan proses dari operasi program komputer

8.		*Manual Input*	*Input* yang menggunakan *online keyboard*
9.		*Conector*	Penghubung ke halaman yang masih sama
10.		*Off-Page Connector*	Penghubung ke halaman lain
11.		*Display*	*Output* yang ditampilkan di monitor
12.		*Delay*	Menunjukkan penundaan
13.		*Preparation*	Memberi nilai awal suatu besaran
14.		*Manual Operation*	Pekerjaan manual
15.		*Card*	*Input* atau *output* yang menggunakan kartu
16.		*Punch Tape*	*Input* atau *output* menggunakan pita kertas berlubang
17.		*Merge*	Penggabungan atau penyimpanan beberapa proses atau informasi sebagai salah satu
18.		*Dirrect Access Storage*	*Input* atau *output* menggunakan drum magnetik

19.		*Magnetic Disk*	*Input* atau *output* menggunakan *hard disk*
20.		*Sequential Access Storage*	*Input* atau *output* menggunakan pita magnetik
21.		*Sort*	Proses pengurutan data di luar komputer
22.		*Stored Data*	*Input* atau *output* menggunakan *diskette*
23.		*Extract*	Proses dalam jalur paralel
24.		*Arrow*	Menyatakan jalan atau arus suatu proses
25.		*Summing Junction*	Untuk berkumpul beberapa cabang sebagai proses tunggal

(Sumber : Suryantara, 2009)