BAB II

LANDASAN TEORI

2.1. Tinjauan Pustaka

Pada penelitian ini, penulis melakukan tinjauan pustaka pada penelitian sebelumnya dan serupa.Sebagai pendukung penelitian yang dilakukan oleh penulis. Dibawah ini merupakan tinjauan pustaka yang sudah diteliti sebelumnya dan serupa :

Tabel 2. 1 Daftar Pustaka

No	Detai Jurnal	
1	Judul	Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode *Port Knocking*.
	Tahun Terbit	2018
	Penulis	Marina Apriani. Arif Harbani,
	Latar Belakang	*Router* sering menjadi salah satu target penyerang untuk tujuan mengambil informasi data yang melalui *router*. Hal ini mengakibatkan keamanan *router* rentan terhadap serangan dari luar maupun dalam. Selain itu *administrator* tidak bisa secara terus menerus memantau *router* yang berada di ruang NOC tempat *router mikrotik* di letakkan.
	Tujuan	Menjaga keamanan port menggunakan metode *port knocking*. Membatasi penggunaan *remote access* dari *client* yang yang tidak mempunyai hak untuk melakukan *remote access* dan *router* dapat melakukan pengiriman notifikasi *email* yang terkirim langsung kepada pihak *administrator* ketika terdeteksi adanya serangan.

	Hasil	Notifikasi *email* sudah bisa diterapkan dan sudah berjalan dengan fungsinya. Sehingga administrator mudah memantau *router* tanpa datang ke tempat *router* diletakkan dengan pesan notifikasi *email* yang masuk.
2	Judul	Implementasi Keamanan Jaringan Menggunakan Metode *Port Blocking* dan *Port Knocking* Pada *Mikrotik RB-941*
	Tahun Terbit	2020
	Penulis	Randi Rizal, Ruuhwan, Kelvin Ajie Nugraha
	Latar Belakang	Sistem *firewall* dimanfaatkan untuk mengatasi permasalahan ini, tetapi kesalahan penyalahgunaan serangan dalam perangkat lunak tingkat aplikasi tidak dapat dilindungi oleh sistem *firewall*. Pada penelitian ini implementasi metode *port knocking* dan *port blocking* dalam keamanan jaringan berhasil dilakukan untuk menangani permasalahan privasi data. Metode *port blocking* pada router *mikrotik* memblock permanen *port* www dan *port winbox* menggunakan layanan yang disediakan *router mikrotik.*
	Tujuan	Tujuan utamanya adalah untuk melindungi dari serangan yang dapat berfungsi dieksploitasi dengan melakukan pemindaian *port* dan pembatasan hak akses *user*, sehingga hanya *user* yang *legitimate* yang bisa mengkases secara penuh untuk membuka dan menutup akses *port* yang telah dikonfigurasi.
	Hasil	Kelebihan dari *Port Knocking* adalah Bisa mengatur manual ketukan *port* yang akan di set sebagai

		knocking, dan dapat mengakses *server mikrotik* dimana saja selama terhubung dalam satu jaringan. Selain itu terdapat kekurangannya, yaitu Perlu penyetingan yang lumayan rumit sehingga menjadikan *knocking* yang kuat, serta Adanya celah pembobolan *server mikrotik* dari segi *brute force*. Untuk kelebihan dari *Port Blocking* itu sendiri adalah *Simple* dalam penyetingan untuk *port* akses *blocking*, dan dapat menutup rapat celah pembobolan akses *service port server mikrotik*. Kelemahan *port blocking* hanya bisa mengakses *server mikrotik* menggunakan *mac address*, dan hanya bisa mangakses *server mikrotik* menggunakan kabel *utp Rj45*.
3	Judul	Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking
	Tahun Terbit	2018
	Penulis	Amarudin, Faruk Ulum
	Latar Belakang	Tidak sedikit jaringan komputer yang mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun sebuah jaringan komputer. Dikarenakan kelalaian tersebut sehingga dapat membuka peluang bagi para hacker untuk meretas dan merusak jaringan yang dibangun tersebut.
	Tujuan Penelitian	mengembangkan keamanan jaringan komputer dengan cara penggunakan metode Port Knocking.
	Hasil	hasil pengujian didapatkan hasil bahwasanya admin Router tidak bisa diakses dari PC1 karena PC1 hanya

		Ping Request ke PC2, maka Admin Router tetap tidak bisa diakses. Adapun pengujian kedua dilakukan dengan cara mengakses admin Router dari PC1 dengan cara *Ping Request* ke PC3 terlebih dahulu baru kemudian bisa *login* ke admin *Router*. Dengan demikian *admin Router* hanya bisa diakses dari PC1 jika PC1 telah melakukan *Ping Request* ke PC3 terlebih dahulu.
4	Judul	Penerapan Sistem Pengamanan *Port* Pada Layanan Jaringan Menggunakan *Port Knocking*.
	Tahun Terbit	2017
	Penulis	Devie Ryana Suchendra, Alfian Fitra Rahman, Setia Juli Irzal Ismail
	Latar Belakang	*port* yang terbuka atau akses yang tidak disertai dengan autentikasi dan otorisasi dapat mengakibatkan mudahnya *user* yang tidak berkepentingan dapat mengakses sistem tersebut.
	Tujuan Penelitian	proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari pengguna yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer.
	Hasil	1. Layanan jaringan dapat saling terintegrasi diantaranya *DNS, FTP*, dan *email*, dapat dibangun pada sistem operasi *Linux Ubuntu 14.0 2*. 2. Dari hasil pengujian yang telah dilakukan menggunakan metode *port knocking* yang dikombinasikan dengan *firewall* di *Mikrotik*, dapat memberikan sistem keamanan autentikasi pada *server* layanan jaringan dan dapat mengamankan *server* dari 3 serangan yaitu *Hydra, DoS*, dan *Telnet*

		yang menggunakan *ptotocol TCP*
5	Judul	Pemanfaatan *Notifikasi Telegram* Untuk *Monitoring* Jaringan
	Tahun Terbit	2019
	Penulis	Febriyanti Panjaitan
	Latar Belakang	Maraknya kegiatan *cyber crime* akhir-akhir ini yang bisa mencuri data dan penyadapan transmisi pada jaringan. Pemantauan *server* jaringan komputer sangat penting dilakukan untuk mempermudah seorang *administrator* dalam mengamati dan mengontrol sistem jaringan yang terpasang. *Server* harus mendapatkan perhatian yang lebih karena memiliki celah kelemahan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab. Salah satu perguruan tinggi yang ada di sumatera selatan pada Tahun 2017 pernah mendapatkan sebuah serangan pada situs *web* yang mengakibatkan terjadinya perubahan tampilan (*deface*). Berdasarkan data penelitian terlihat bahwa sistem pada *server* terdapat *port* yang cukup banyak terbuka, sehingga dapat berpotensi kembali oleh para *attacker* untuk mengambil alih sistem tersebut. Hasil dari *scanning* terdapat banyak *port* yang terbuka seperti *port* 80 *hypertext transfer protocol (http)*, *port* 22 *secure shell (ssh) port* 21 *ftp server*. *Port* 21 dan *port* 22 adalah *port* yang paling banyak digunakan oleh para *attacker* untuk menyerang suatu sistem demi mendapatkan akses ke sistem *server* dan file-file data yang akhirnya seorang *attacker* bisa membuat akses *root* yang mempunyai hak penuh terhadap *system* yang diserang.

	Tujuan Penelitian	1. Melakukan instalasi dan konfigurasi *snort* serta aplikasi pendukung lainnya. 2. Melakukan konfigurasi pada *IDS* sehingga dapat terhubung dengan Aplikasi *Telegram Messenger*. 3. Melakukan pengujian serangan terhadap *server* untuk mengetahui *system IDS* sudah berjalan sesuai dengan keinginan. *Attacker* akan mencoba melakukan serangan dengan cara mencari kelemahan sistem keamanan jaringan pada *Server*. *IDS* yang terpasang pada *server* akan melakukan pengawasan terhadap kegiatan-kegiatan yang mencurigakan terjadi pada *server*, ketika *attacker* melakukan usaha penyusupan atau penerobosan ke *server* maka *snort* akan secara otomatis mendeteksi adanya *intruder*. Setelah *snort* mendeteksi usaha penyusupan, *snort* akan membuat *log file* hasi *capture* paket penyusupan tersebut.
	Hasil	Hasil yang didapat menunjukkan sistem berhasi mendeteksi serangan yang dilakukan oleh *attacker*, namun hal tersebut belum dapat dijadikan acuan bahwa *system IDS* bekerja secara optimal, sebab semakin berkembangnya teknologi, maka metode penyerangan akan semakin beragam. *Adminstrator* dituntut untuk selalu meng*update rules* untuk keamanan *server*. Dengan demikian, akan mudah me*monitoring server* ketika ada serangan baru. Selain mendeteksi serangan, perlu adanya sistem yang mampu melakukan tindakan pencegahan yang sering dinamakan sebagai *IPS*. Pada kasus tertentu sebuah serangan dapat membahayakan sistem dan fungsi *IPS* untuk mencegah serangan agar tidak menggangu *server*.

2.1.1. Tinjauan pada Literatur 1

Pada Literatur 1 ini membahas tentang Pengembangan Notifikasi *Email* Untuk Keamanan Port Menggunakan Metode *Port Knocking*. Tujuan dari penelitian ini yaitu Membatasi penggunaan *remote access* dari *client* yang yang tidak mempunyai hak untuk melakukan *remote access* dan *router* dapat melakukan pengiriman notifikasi *email* yang terkirim langsung kepada pihak *administrator*.

Perbedaan literatur 1 dengan penelitian yang akan diteliti adalah terdapat pada media yang digunakan, pada penelitian yang akan diteliti penulis menggunakan media notifikasi *telegram* dan perbedaan lainya terdapat pada metode yang digunakan, pada penelitian ini penulis menambahkan metode *PSD* (*Port Scan Detection).*

2.1.2. Tinjauan pada Literatur 2

Perbedaan literatur 2 dengan penelitian yang akan diteliti adalah terdapat pada metode yang digunakan, pada penelitian yang akan diteliti penulis menggunakan metode PSD (*Port Scan Detection)* sedangkan pada literatur 2 menggunakan metode *Port Blocking*..

2.1.3. Tinjauan pada Literatur 3

Perbedaan Perbedaan penelitian yang akan diteliti dengan literatur 3 terdapat pada *device* yang digunakan pada literature 3 ini menggunakan *Mikrotik RB450G,* sedangkan pada penelitian ini menggunakan *Mikrotik RB941*.

2.1.4. Tinjauan pada Literatur 4

Perbedaan penelitian yang akan diteliti dengan literatur 4 terdapat pada metode yang dipakai, pada penelitian yang akan diteliti penulis menggunakan metode pengujian, yaitu metode *PSD* (*Port Scan Detection)* dan menggunakan *PuttY* sebagai *tools* untuk melakukan serangan *Bruteforce* sedangkan pada literature 4 hanya menggunakan 1 metode yaitu *Bruteforce* dengan *Hydra*. Selain itu juga penulis menggunakan media *telegram* sebagai notifikasi apabila adanya indikasi penyerangan.

2.1.5. Tinjauan pada Literatur 5

Perbedaan literatur 5 dengan penelitian yang akan diteliti adalah terdapat pada metode yang digunakan, penelitian sebelumnya menggunakan *Snort* sedangkan peneliti menggunakan metode *Port Knocking*.

Kesimpulan keseluruhan dari tinjauan literatur dengan penelitian yang saya buat ialah pada penelitian yang sedang dibuat menggunakan media notifikasi *telegram* dan menggunakan metode *port knocking* sebagai metode pengamanan *port*. Selain itu juga peneliti menguji keamanan jaringan dengan serangan *brute force* menggunakan tools *PuTTY* dan selain itu juga peneliti menguji kembali dengan metode *PSD* atau *Port Scan Detection* dengan menggunakan *tools Zenmap*. Selain menguji keamanan, dua metode tadi digunakan juga untuk memastikan apakah notifikasi *telegram* dapat merespon apabila terjadi serangan.

2.2. *Mikrotik*

Mikrotik adalah perangkat jaringan komputer yang berupa *hardware* dan *software* yang dapat difungsikan sebagai *Router*, sebagai alat *Filtering, Switching* maupun yang lainnya. Adapun *hardware Mikrotik* bisa berupa *Route*r PC (yang diinstall pada PC) maupun berupa *Router Board* (sudah dibangun langsung dari perusahaan *Mikrotik*). Sedangkan *software Mikrotik* atau yang dikenal dengan nama *RouterOS* (Amarudin and Ulum 2018)

2.3. *Telegram Messenger*

Telegram Messenger adalah aplikasi perpesanan gratis yang berfokus pada kecepatan dan keamanan. *Telegram* dapat digunakan di semua perangkat secara bersamaan, artinya pesan yang dikirim dan diterima disinkronkan secara *realtime* antara beberapa perangkat, baik itu ponsel, tablet, atau komputer. *Telegram Messenger* juga dapat mengirim semua jenis pesan teks, foto, video, *file* (dokumen, file zip, file mp3, dll.) dan membuat grup hingga 100.000 orang atau membuat saluran yang dapat dikirim ke pengguna tanpa batas. *Telegram* dapat membaca kontak di telepon dan menemukan orang dengan nama pengguna mereka. Hasilnya, *Telegram* seperti kombinasi SMS dan email dan dapat mengurus semua kebutuhan pribadi atau bisnis Anda. Selain itu, *Telegram* juga mendukung panggilan suara terenkripsi *end-to-end* (Ponco Wibowo and Rismayadi 2023).

2.3.1. *Telegram Bot*

Telegram Bot merupakan akun Telegram khusus yang didesain dapat meng-handle pesan secara otomatis. Pengguna dapat berinteraksi dengan *Bot* dengan mengirimkan pesan perintah *(Command)* melalui pesan *private* maupun *group*. Akun *Telegram Bot* tidak memerlukan tambahan nomor telepon pada penbuatannya. Akun ini hanya bertugas sebagai antarmuka dari kode yang berjalan di sebuah *Server*. *Telegram Bot* dapat dibangun sesuai dengan kebutuhan, semisal digunakan dengan mengintegrasikannya ke layanan lain untuk mengendalikan *smart home*, membangun *social services*, membangun *custom tools*, ataupun melakukan hal lain secara *virtual* (Soeroso et al. 2017).

2.4. *Router*

Router adalah perangkat keras jaringan komputer yang menghubungkan beberapa jaringan yang sama atau berbeda dan juga sebagai alat untuk mengatur keluar dan masuknya suatu data pada jaringan, *router* berada pada lapisan terluar yang terhubung langsung ke jaringan publik. (Harbani and Apriani 2019)

2.5. *Brute force attack*

Menurut (Sinaga and Nuraisana 2021) *Brute force* adalah sebuah pendekatan langsung (*straight forward*) untuk memecahkan suatu masalah, biasanya didasarkan pada pernyataan masalah (*problem statement*) dan definisi konsep yang dilibatkan. Algoritma *brute force* memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas (*obvious way*). Di dalam pencocokan *string*, terdapat istilah teks dan *pattern*. Teks merupakan kata yang dicari dan dicocokkan dengan *pattern*. Salah satu jenis serangan *brute force* ialah *dictionary attack*, Menurut (Kaspersky.com n.d.) *dictionary attack* atau serangan kamus adalah jenis serangan *brute force* di mana peretas mencoba menebak kata sandi pengguna untuk akun daring mereka dengan segera menelusuri daftar kata, frasa, dan kombinasi angka yang umum digunakan. Ketika serangan kamus berhasil memecahkan kata sandi, peretas kemudian dapat menggunakannya untuk mendapatkan akses ke hal-hal seperti rekening bank, profil media sosial,

Gambar 2.2 Alur Serangan *Brute Force*

dan bahkan file yang dilindungi kata sandi. Untuk menyusun daftar kata sandi potensial, penyerang sering kali menggunakan nama hewan peliharaan yang umum, karakter budaya pop yang dapat dikenali, atau tim dan atlet olahraga besar,. Hal ini karena banyak orang menggunakan jenis kata ini untuk membuat kata sandi yang memiliki arti bagi mereka dan mudah diingat.

2.6. Aplikasi *PuTTY*

Menurut (rumahweb.com 2023) *PuTTY* adalah aplikasi yang digunakan untuk remote access, seperti *SSH* atau *Telnet*. Dengan aplikasi ini, Anda dapat mengakses komputer server dari jarak jauh, tanpa perlu datang ke data center secara fisik. Selain itu, PuTTY juga termasuk sebagai aplikasi Open Source sehingga dapat digunakan secara gratis. Selain itu menurut Yasin K pada artikerlnya yang ditulis dalam situs (niagahoster.co.id 2018) PuTTY adalah aplikasi *open-source* yang sering digunakan untuk melakukan *remote access*, seperti RLogin, SSH, dan Telnet. *Remote access* merupakan aplikasi yang digunakan untuk mengendalikan sistem dari jarak jauh atau di tempat yang berbeda. *Remote access* masih terkoneksi dengan jaringan internet. Pemilik *server* kebanyakan menggunakan aplikasi ini untuk melakukan akses ke server mereka. Letak server yang jauh membuat *PuTTY* sangat berguna, karena tidak perlu datang langsung ke lokasi *server* untuk melakukan konfigurasi.

Gambar 2.4 Logo Aplikasi *PuTTY*

2.7. *Port Scan*

Menurut (fortinet.com 2020) *Port Scan* adalah teknik umum yang digunakan peretas untuk menemukan *open door* atau titik lemah dalam jaringan. Serangan *port scan* membantu *hacker* menemukan *port* terbuka dan mencari tahu apakah mereka menerima atau mengirim data. Itu juga dapat mengungkapkan apakah perangkat keamanan aktif seperti *firewall* digunakan oleh suatu organisasi. Selain itu juga mengutip dari *Avast Bussiness,2021* dalam situs (*EC-Council's* 2022) *Port Scan* adalah bertujuan untuk menentukan organisasi alamat IP, *host*, dan *port* dalam jaringan khususnya, *port* mana yang terbuka dan mengirim atau menerima data. Pemindaian *port* juga dapat mengungkap keberadaan *firewall* dan tindakan keamanan lainnya antara *server* dan perangkat pengguna.

2.8. *Port Knocking*

Port-knocking adalah konsep menyembunyikan layanan jarak jauh di dalam sebuah *firewall* yang memungkinkan akses ke *port* tersebut hanya untuk mengetahui *service* setelah klien berhasil diautentikasi ke *firewall*. Hal ini dapat membantu untuk mencegah pemindai untuk mengetahui *service* apa saja yang saat ini tersedia di *host* dan juga berfungsi sebagai pertahanan terhadap serangan *zero-day* (Amarudin and Ulum 2018). Selain itu menurut (Yudi mulyanto, M. Julkarnain, and Jabi Afahar 2021) *Port Knocking* adalah metode sistem autentikasi yang secara khusus dibuat untuk jaringan. Ide dasar dari sistem autentikasi ini telah lama digunakan namun baru pada tahun 2003. Pada dasarnya *port knocking* dapat didefinisikan sebagai suatu metode komunikasi antara dua komputer,dimana informasi yang dikirimkan di-*encode* dalam bentuk usaha koneksi ke *port–port* dalam urutan tertentu. Usaha membangun koneksi ini bisa disebut juga ketukan. Mekanisme *port knocking* akan menggunakan *file log* yang dibuat oleh *firewall* untuk mengetahui apakah suatu usaha koneksi telah dibuat oleh suatu *host* atau tidak.

2.9. *Zenmap*

Zenmap adalah aplikasi *multi platform* sebagai *interface* sederhana untuk apikasi *nmap.* Nmap *(Network Mapper)* sendiri adalah sebuah aplikasi *open source* untuk explorasi *network* dan audit keamanannya. Nmap bekerja dengan melakukan *scan* terhadap komputer *(host) stand alone* ataupun *host* yang terhubung dalam sebuah jaringan, menentukan *host-host* yang aktif dalam suatu jaringan, menentukan informasi sistem operasi, *port-port* yang terbuka dan jenis *firewall* yang digunakan.(Guntur Saputra 2019)