IMPLEMENTATION OF A NETWORK SECURITY SYSTEM USING THE PORT KNOCKING METHOD AT TARUNA SATRIA VOCATIONAL SCHOOL PEKANBARU

PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN METODE *PORT KNOCKING* PADA SMK TARUNA SATRIA PEKANBARU

Zahra Amanda Indira Azmi[1], Dahliyusmanto[2]
[1,2]Prodi Teknik Informatika, Universitas Riau, Jl. HR Soebrantas KM 12.5, Simpang Baru, Pekanbaru
Email: zahra.amanda4750@student.unri.ac.id [1], dahliyusmanto@lecture.unri.ac.id [2]

Abstract - *SMK Taruna Satria Pekanbaru utilizes its network for teaching and school administration activities. However, security issues have led to incidents where intruders gained access to the MikroTik webfig and altered configurations, such as changing hotspot passwords and adding unauthorized user profiles. Initial data shows that the network experienced up to a 30% performance drop due to illegal access, with a high potential for attacks, especially on HTTP (80), SSH (22), Telnet (23), and Winbox (8291) ports if left open.To address these issues, the Port Knocking method was implemented, which hides ports and only allows access to users who knock on the ports in a specific sequence. Legitimate users must knock on the ports in a designated order to activate access, which then adds their IP address to the whitelist. Access to services is granted only if the correct knocking sequence is followed within a specific timeframe. Testing through simulations of Port Scanning, brute force, and DDoS attacks has demonstrated this method's effectiveness in hiding ports from scanning detection and reducing brute force and DDoS attack risks. Although effective, this method relies on accurate configuration patterns. Implementing Port Knocking is expected to enhance network security and reduce unauthorized access risks at SMK Taruna Satria Pekanbaru.*

Keywords – *Network Security, Port Knocking, Port Scanning, Brute Force*, DDoS.

Abstrak – SMK Taruna Satria Pekanbaru memanfaatkan jaringan untuk kegiatan belajar mengajar dan administrasi sekolah. Namun, kurangnya keamanan menyebabkan beberapa insiden keamanan, di mana penyusup berhasil mengakses webfig MikroTik dan mengubah konfigurasi, seperti mengganti kata sandi hotspot dan menambah profil pengguna ilegal. Berdasarkan data awal, jaringan mengalami penurunan performa hingga 30% akibat akses ilegal, serta potensi serangan yang cukup tinggi terutama pada port HTTP (80), SSH (22), Telnet (23), dan Winbox (8291) jika dibiarkan tetap terbuka. Untuk mengatasi masalah ini, diterapkan metode *Port Knocking*, yang bekerja dengan menyembunyikan port dan hanya mengizinkan akses bagi pengguna yang melakukan "ketukan" port secara berurutan sesuai aturan yang ditetapkan. Pengguna sah harus mengetuk port dalam urutan tertentu untuk mengaktifkan akses, yang akan menambahkan alamat IP mereka ke daftar izin. Akses ke layanan hanya diberikan jika urutan ketukan benar dan dilakukan dalam jangka waktu yang ditentukan. Pengujian melalui simulasi Port Scanning, brute force, dan DDoS menunjukkan efektivitas metode ini dalam menyembunyikan port dari deteksi scanning dan mengurangi risiko serangan brute force dan DDoS. Meskipun efektif, metode ini memiliki keterbatasan dalam hal ketergantungan pada pola konfigurasi yang tepat. Implementasi *Port Knocking* diharapkan dapat meningkatkan keamanan jaringan dan mengurangi risiko akses tidak sah di SMK Taruna Satria Pekanbaru.

Kata Kunci – Keamanan Jaringan, *Port Knocking*, *Port Scanning, Brute Force*, DDoS.

I. PENDAHULUAN

Di era digital ini, perkembangan teknologi dan informasi yang pesat telah meningkatkan efisiensi dan konektivitas, salah satunya melalui jaringan komputer. Jaringan digunakan oleh individu, institusi, dan perusahaan untuk berbagai keperluan, sehingga keamanan jaringan menjadi aspek penting dalam melindungi jaringan dari ancaman eksternal guna menjaga kinerja, integritas data, dan keamanan informasi penting [1]. Ketika aspek ini diabaikan, jaringan menjadi rentan terhadap serangan, terutama melalui port yang terbuka. Beberapa jenis serangan umum melalui port adalah Port Scanning, Brute Force, dan DDoS[2]. SMK Taruna Satria Pekanbaru adalah salah satu institusi yang memanfaatkan jaringan untuk mendukung proses belajar mengajar dan administrasi sekolah. Berdasarkan hasil wawancara, ditemukan bahwa jaringan sekolah ini pernah mengalami akses tidak sah yang berhasil masuk melalui web sistem manajemen jaringan dan melakukan perubahan konfigurasi. Hal ini menyebabkan kinerja jaringan melambat dan mengganggu pengguna sah.

Analisis lebih lanjut menunjukkan bahwa penyusup memanfaatkan port terbuka untuk mendapatkan akses, di mana port 80 (HTTP), port 22 (SSH), port 23 (Telnet), dan port 8291 (Winbox) terdeteksi terbuka selama proses Port Scanning. Hal ini membuktikan bahwa SMK Taruna Satria Pekanbaru membutuhkan sistem keamanan yang lebih efektif untuk mencegah dan meminimalisir akses tidak sah. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan di SMK Taruna Satria Pekanbaru melalui penerapan metode *Port Knocking* pada port 80 (HTTP), port 22 (SSH), port 23 (Telnet), dan port 8291 (Winbox) yang terdeteksi terbuka dan rentan menjadi celah keamanan. *Port Knocking* dipilih sebagai solusi karena metode ini tidak hanya menyembunyikan port dari deteksi tetapi juga membatasi akses hanya kepada pengguna yang mengetahui urutan ketukan yang tepat[1]. Hal ini memberikan lapisan tambahan keamanan yang lebih kuat dibandingkan metode lain seperti firewall statis atau pengaturan akses berbasis IP, yang dapat dengan mudah dieksploitasi oleh penyerang yang lebih berpengalaman.[3]

Port Knocking bekerja dengan cara menyembunyikan port, sehingga hanya pengguna yang mengetahui dan melakukan ketukan dengan benar dan sesuai konfigurasi yang dapat mengaksesnya[4]. Penelitian ini berhipotesis bahwa penerapan metode *Port Knocking* pada port-port rentan (HTTP, SSH, Telnet, dan Winbox) dapat meningkatkan keamanan jaringan dengan mencegah akses tidak sah dan menyembunyikan port dari deteksi scanning. Untuk membuktikan hipotesis ini, penelitian ini akan menguji efektivitas *Port Knocking* dalam mengurangi serangan melalui simulasi Port Scanning, brute force, dan DDoS. Penelitian ini diharapkan memberikan manfaat langsung bagi SMK Taruna Satria Pekanbaru dalam memperkuat keamanan jaringan, khususnya dalam mengurangi risiko akses tidak sah pada port-port yang terdeteksi terbuka dan rentan. Dengan penerapan *Port Knocking*, port-port layanan tersebut tidak akan mudah dideteksi melalui Port Scanning, dan akses hanya akan diberikan kepada pengguna yang memiliki izin sesuai dengan konfigurasi ketukan yang telah ditentukan.

II. SIGNIFIKANSI STUDI

A. Penelitian Terdahulu

Penelitian [4] berhasil meningkatkan keamanan jaringan dari masuknya akses yang tidak sah dengan menerapkan sistem keamanan jaringan menggunakan metode *Port Knocking* yang diterapkan pada port 80 (HTTP), port 22 (SSH), port 23 (Telnet), dan port (8291). Hasilnya, *port* layanan yang diterapkan sistem keamanan *Port Knocking* hanya dapat diakses ketika pengguna melakukan aturan ketukan sesuai dengan yang sudah diatur (konfigurasi) sebelumnya. Penelitian [5] mengangkat permasalahan kemanan jaringan dan data yang sangat penting terutama bagi instansi pendidikan seperti SMKN 1 Sumbawa Besar. Serangan melalui celah- celah *port* yang dalam keadaan terbuka dapat menyebabkan hilang atau dicurinya data penting yang tersimpan. Penelitian ini berhasil mengatasi hal tersebut dengan melakukan atan keamanan jaringan menggunakan metode *Port Knocking*. Sehingga, hanya user tertentu saja yang dapat mengakses *port* yang telah ditentukan dengan cara mengetuk terlebih dahulu di knock-1000. Penelitian [6] berhasil menyelesaikan permasalahan yang diangkat yaitu *port* - *port* yang dalam keadaan terbuka secara tidak langsung mengundang pihak yang tidak bertanggung jawab untuk membobol dan menyerang server melalui *port* tersebut. Penyelesaian yang dilakukanlah beberapa konfigurasi menggunakan metode *Port Knocking* yang akan membatasi siapa saja yang dapat mengakses server. Sehingga, hanya pengguna tertentu saja yang dapat masuk dan mengakses secara penuh ke *port* yang sudah dikonfigurasi dengan cara melakukan aturan ketukan yang sesuai.

Penelitian ini berbeda dari penelitian sebelumnya dengan fokus pada penerapan sistem keamanan *Port Knocking* pada port yang lebih rentan dan terbuka. Pada penelitian ini dilakukan pengujian menyeluruh untuk mengukur efektivitas Port Knocking dalam mengurangi serangan melalui simulasi *Port Scanning, brute force*, dan DDoS. Penelitian ini juga mengeksplorasi dampak penerapan *Port Knocking* terhadap kinerja jaringan, yang belum banyak diteliti sebelumnya. Dengan demikian, penelitian ini tidak hanya berkontribusi pada aspek keamanan, tetapi juga memberikan wawasan baru tentang penerapan metode ini untuk meningkatkan keamanan jaringan di SMK Taruna Satria Pekanbaru. Dengan memperdalam pemahaman tentang keamanan jaringan, penelitian ini menekankan pentingnya penerapan *Port Knoc*king dalam konteks pendidikan, yang sering kali menghadapi tantangan unik terkait keamanan jaringan[7]. SMK Taruna Satria Pekanbaru memiliki kebutuhan keamanan yang berbeda dibandingkan dengan sekolah lainnya, mengingat salah satu jurusan yang ada berhubungan langsung dengan jaringan, yaitu Teknologi Komputer Jaringan. Oleh karena itu, perlindungan terhadap jaringan dan data sensitif sangatlah penting. Penelitian ini diharapkan memberikan wawasan baru tentang bagaimana Port Knocking tidak hanya berfungsi sebagai langkah keamanan, tetapi juga dapat diadaptasi untuk memenuhi kebutuhan spesifik lingkungan pendidikan. Dengan demikian, penelitian ini berkontribusi tidak hanya dalam aspek keamanan tetapi juga dalam memperluas pemahaman tentang penerapan metode ini di institusi pendidikan.

B. Landasan Teori

1. Keamanan Jaringan

Keamanan jarinagn merupakan salah satu aspek terpenting yang prosesnya untuk mencegah masuknya orang yang tidak punya izin atau akses terhadap sebuah jaringan. Tujuan utama dari adanya keamanan jaringan ini adalah mengurangi resiko terjadinya ancaman pencurian data, kerusakan sistem, dan masalah jaringan komputer lainnya [8].

2. *Port Knocking*

Port Knocking merupakan metode keamanan jaringan yang memungkinkan akses ke *port-port* layanan yang sebelumnya telah ditutup[9]. *Port Knocking* memiliki konsep yang pada dasarnya menyembunyikan *port* memberikan akses hanya kepada pengguna yang mengetahui dan mengikuti aturan knocking yang telah ditetapkan [10].

3. Port Scanning

Port Scanning merupakan teknik megidentifikasi *port-port* yang dalam keadaan terbuka pada jaringan[11]. Teknik ini biasanya menggunakan *tools* seperti Nmap dan Nessus oleh Admin Jaringan untuk mendapatkan informasi mengenai sistem target. Tidak jarang pula, *attacker* memanfaatkan teknik ini dengan tujuan yang sama dan memanfaatkan informasi tersebut untuk melakukan serangan terhadap jaringan [12]. Tiga jenis status port yang muncul pada hasil *Port Scanning* adalah '*open'* yang menandakan dalam keadaan terbuka dan aktif menjalankan *service*, '*filtered'* yang menandakan port tidak teridentifikasi jelas statusnya karena dihalagi ole firewall, dan '*closed'* yang menandakan dalam keadaan tertutup

4. Brute force

Brute Force merupakan salah satu serangan yang umum dilakukan untuk menembus suatu jaringan. Serangan ini memiliki metode dimana penyerang mencoba berbagai kombinasi kata sandi secara berulang untuk mendapatkan akses tidak sah terhadap suatu jaringan atau sistem layanan target[13]. Serangan yang berhasil tidak hanya memberi penyerang akses ke data, aplikasi, dan sumber daya, tetapi juga dapat berfungsi sebagai titik masuk untuk serangan lebih lanjut.

5. DDoS (Distributed Denial of Services)

DDoS adalah serangan yang dirancang untuk membanjiri jaringan atau server target dengan sejumlah besar paket data yang dikirimkan secara berulang dan berturut-turut[14]. Tujuan utama dari serangan ini adalah untuk membebani kapasitas jaringan atau server, sehingga sumber daya yang tersedia tidak dapat menangani lonjakan lalu lintas yang tinggi [5].

C. Metode Penelitian

Penerapan sistem keamanan menggunakan metode *Port Knocking* ini diterapkan pada jaringan SMK Taruna Satria Pekanbaru. Metode penelitian ini berfokus pada suatu kasus dalam konteks nyata yang dieksplorasi menggunakan berbagai sumber data dan teknik pengumpulan data [15]. Tahapan pada penelitian ini disajikan dalam bentuk flowchart seperti yang terlihat pada Gambar 1 berikut.

Gambar 1. *Flowchart* Tahapan Penelitian

1. Identifikasi Masalah

Merupakan tahap awal dimana peneliti akan mengidentifikasi dan menentukan area spesifik atau fokus permasalahan yang akan diteliti mencakup situasi yang ada, perumusan masalah, tujuan, dan batasan studi kasus dalam penelitian.

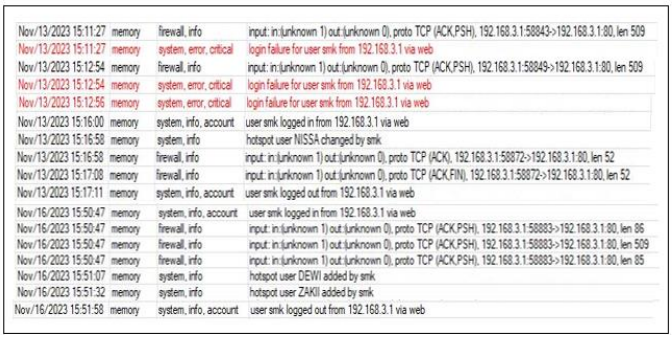
2. Pengumpulan Data

2.1 Wawancara

Berdasarkan hasil wawancara yang dilakukan, dapat disimpulkan bahwa kendala jaringan yang terjadi pada SMK Taruna Satria Pekanbaru adalah adanya akses tidak sah yang masuk dan melakukan perubahan konfiguarsi untuk kepentingan pribadinya. Selain itu, akses tidak sah ini juga menyebabkan turunnya kinerja jaringan karena adanya aktivitas dari pengguna yang tidak seharusnya.

2.2 Log Aktivitas Tidak Sah

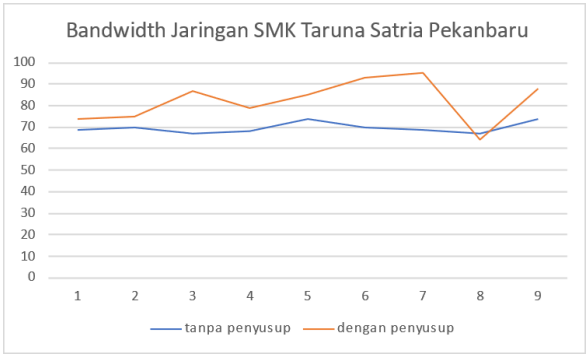
Analisis lebih lanjut yang dilakukan untuk mengumpulkan data dalam penelitian ini mendapatkan adanya aktivitas akses tidak sah yang terekam pada log file MikroTik SMK Taruna Satria Pekanbaru.



Nov/13/2023 15:11:27	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,PSH), 192.168.3.1:58843->192.168.3.1:80, len 509
Nov/13/2023 15:11:27	memory	system, error, critical	login failure for user smk from 192.168.3.1 via web
Nov/13/2023 15:12:54	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,PSH), 192.168.3.1:58849->192.168.3.1:80, len 509
Nov/13/2023 15:12:54	memory	system, error, critical	login failure for user smk from 192.168.3.1 via web
Nov/13/2023 15:12:56	memory	system, error, critical	login failure for user smk from 192.168.3.1 via web
Nov/13/2023 15:16:00	memory	system, info, account	user smk logged in from 192.168.3.1 via web
Nov/13/2023 15:16:58	memory	system, info	hotspot user NISSA changed by smk
Nov/13/2023 15:16:58	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK), 192.168.3.1:58872->192.168.3.1:80, len 52
Nov/13/2023 15:17:08	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,FIN), 192.168.3.1:58872->192.168.3.1:80, len 52
Nov/13/2023 15:17:11	memory	system, info, account	user smk logged out from 192.168.3.1 via web
Nov/16/2023 15:50:47	memory	system, info, account	user smk logged in from 192.168.3.1 via web
Nov/16/2023 15:50:47	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,PSH), 192.168.3.1:58883->192.168.3.1:80, len 86
Nov/16/2023 15:50:47	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,PSH), 192.168.3.1:58883->192.168.3.1:80, len 509
Nov/16/2023 15:50:47	memory	firewall, info	input: in:(unknown 1) out:(unknown 0), proto TCP (ACK,PSH), 192.168.3.1:58883->192.168.3.1:80, len 85
Nov/16/2023 15:51:07	memory	system, info	hotspot user DEWI added by smk
Nov/16/2023 15:51:32	memory	system, info	hotspot user ZAKII added by smk
Nov/16/2023 15:51:58	memory	system, info, account	user smk logged out from 192.168.3.1 via web

Gambar 2. Log Akses Tidak Sah

Dari Gambar 2 terlihat bahwa penyusup melakukan percobaan *login* beberapa kali sebelum akhirnya berhasil mengubah password salah satu user guru di SMK Taruna Satria Pekanbaru. Keluhan pengguna jaringan akhirnya membuat admin jaringan menulusuri lebih lanjut mengenai kondisi jaringan saat ini. Pengukuran Bandwidth dilakukan untuk mengetahui sejauh mana kinerja jaringan turun akibat adanya akses tidak sah yang masuk. Grafik perbandingan bandwidth jaringan SMK Taruna Satria menunjukkan bahwa adanya kenaikan pemakaian bandwidth setelah masuknya akses tidak sah yang dapat dilihat pada Gambar 3 berikut.



Gambar 3. Grafik Perbandingan *Bandwidth*

Gambar 3 menunjukkan grafik dimana saat ada penyusup, terjadi peningkatan bandwidth hingga sekitar 30% dibandingkan kondisi normal tanpa penyusup. Dalam kondisi normal,

bandwidth berkisar antara 60-70 Mbps, sedangkan dengan adanya penyusup, angka ini meningkat hingga mendekati 100 Mbps. Kenaikan ini menunjukkan tambahan lalu lintas signifikan akibat akses tidak sah, yang membebani jaringan dan memengaruhi stabilitas koneksi.

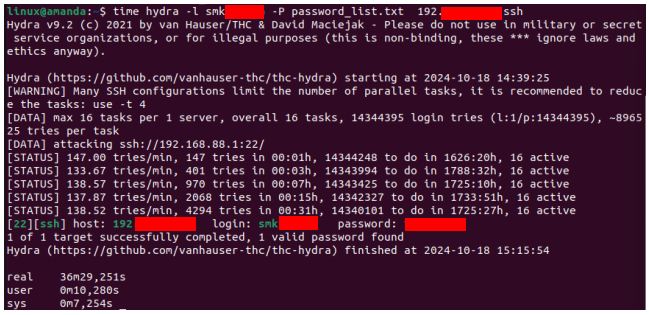
2.3 Kerentanan Yang Terdeteksi

Pada penelitian ini, *tools* yang digunakan untuk mendeteksi kerentanan adalah Nmap. Hasil dari *Port Scanning* yang dilakukan menggunakan Nmap menampilkan hasil bahwa beberapa port pada Jaringan SMK Taruna Satria Pekanbaru yaitu port 80 (HTTP), port 22 (SSH), port 23 (Telnet), dan port 8291 (Winbox) terdeteksi dengan status *open* yang artinya terbuka. Hal ini berpotensi menjadi titik masuk bagi penyerang.

2.4 Potensi Serangan terhadap Jaringan

2.4.1 Serangan *Brute Force*

Serangan brute force melibatkan penyerang yang mencoba berbagai kombinasi kata sandi secara terus-menerus hingga menemukan yang benar. Pada port 80 (HHTP), 22 (SSH), 23 (Telnet), dan 8291 (Winbox), serangan ini sangat berisiko karena akses langsung ke sistem manajemen jaringan bisa didapatkan jika kata sandi bisa didapatkan. Serangan brute force



(a)

Time	Buffer	Topics	Message
Sep/12/2024 11:57:06	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:08	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:09	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:10	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:12	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:13	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:14	memory	system, error, critical	login failure for user smktaruna from 192 via web
Sep/12/2024 11:57:15	memory	system, error, critical	login failure for user smktaruna from 192 via web

(b)

Gambar 4. Serangan *Brute Force* (a) Log MikroTik (b)

Gambar 4 menampilkan serangan *brute force* yang dilakukan terhadap jaringan SMK Taruna Satria Pekanbaru yang diarahkan ke salah satu port yang terbuka yaitu port 80 (HTTP). Serangan ini berhasil membobol jaringan yang ditandai dengan ditemukannya kata sandi dari username 'smktaruna' melalui percobaan berulang dalam waktu 36 menit. Serangan ini juga terdeteksi dalam log sistem MikroTik dengan pesan '*login failure for user smktaruna from 192.xxx.xxx.xxx via web*' yang mengindikasikan adanya upaya login gagal melalui port 80 (HTTP).

2.4.2 Serangan DDoS (*Distributed Denial of Service*)

Serangan DDoS (*Distributed Denial of Service*) bertujuan untuk membanjiri port dengan lalu lintas berlebihan sehingga perangkat atau layanan mengalami gangguan besar pada ketersediaan jaringan atau bahkan tidak dapat merespons. Pada penelitian ini, tools yang digunakan adalah LOIC (*Low Orbit Ion Cannon*) dan serangan diarahkan kepada port yang terdeteksi terbuka dan paling rentan yaitu port 80 (HHTP), 22 (SSH), 23 (Telnet),

dan 8291 (Winbox). Serangan DDoS yang dilakukan terhadap Jaringan SMK Taruna

Satria Pekanbaru dapat dilihat pada Gambar 7 berikut.

Gambar 7. Serangan DDoS

Gambar 7 menunjukkan serangan DDoS yang dilakukan berhasil membebani cpu dan jaringan karena mengirimkan paket dalam jumlah yang besar dan berturut-turut mencapai lebih dari 1.013.884 paket hanya dalam waktu 15 menit. Dampak dari serangan ini adalah beban CPU perangkat mengalami kenaikan drastis hingga mencapai 100%, yang sangat berisiko menimbulkan kerusakan pada perangkat jaringan. Kondisi ini tidak hanya membebani perangkat secara fisik tetapi juga berpotensi menyebabkan kegagalan sistem atau mempengaruhi kinerja jaringan secara keseluruhan akibat overload yang berkepanjangan.

2.5 Studi Literatur

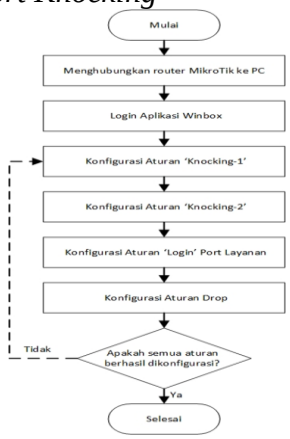
Studi Literatur merupakan tahapan dimana peneliti akan mempelajari dan mengeksplorasi teori – teori terkait Sistem Keamanan Jaringan dengan kendala atau permasalahan jaringan yang relevan dengan penelitian ini. Sumber informasi didapat dari berbagai sumber literatur seperti jurnal penelitian, skripsi, artikel, buku, laporan penelitian dan sejenisnya.

3. Analisis Data

Pada tahapan ini, seluruh data yang sudah dikumpulkan melalui beberapa teknik sebelumnya akan dianalisis untuk dipahami lagi mengenai masalah yang teridentifikasi dan menjadi fokus dalam penelitian ini. Melalui analisis ini, peneliti akan menentukan solusi yang sesuai dalam menyelesaikan masalah tersebut.

4. Penerapan Sistem Keamanan Jaringan

4.1 Konfugurasi Sistem Keamanan *Port Knocking*

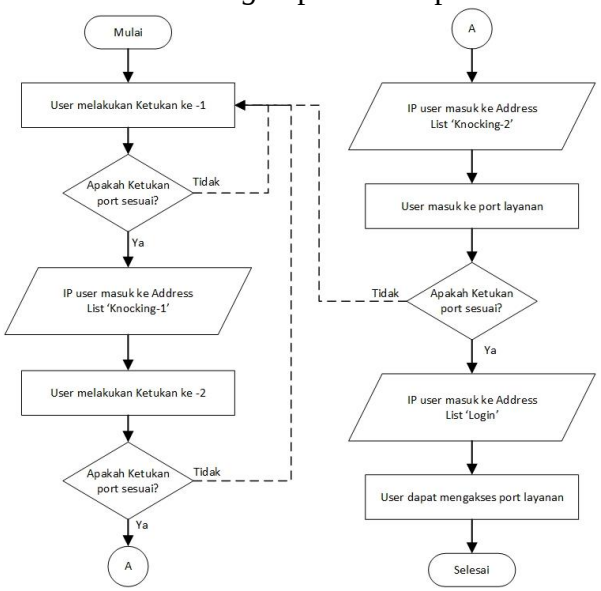


Gambar 10. *Flowchart* Konfigurasi *Port Knocking*

Gambar 10 menunjukkan proses perancangan konfigurasi sistem keamanan jaringan menggunakan metode *Port Knocking* pada MikroTik dalam bentuk flowchart. Penerapan dimulai dengan menghubungkan MikroTik ke PC dan *login* menggunakan aplikasi Winbox. Konfigurasi dilakukan dengan membuat beberapa aturan "*knocking*" secara bertahap pada menu *Firewall*. Pertama, dibuat aturan "*Knocking*-1" untuk menandai sumber alamat IP yang melakukan *knocking* pada port tertentu dalam jangka waktu 10 detik. Selanjutnya, aturan "*Knocking*-2" disusun dengan ketentuan bahwa IP harus dicatat di "*Knocking*-1" untuk dapat masuk dalam daftar. Aturan terakhir adalah konfigurasi port layanan, di mana IP yang sudah melalui tahap *knocking* diberikan akses ke port tujuan. Terakhir, dibuat aturan *Drop* untuk menolak akses ke port bagi IP yang tidak termasuk dalam daftar "*Login*". Setelah semua aturan tersimpan dan muncul dalam *Firewall Rule*, konfigurasi *Port Knocking* pun selesai dan aktif untuk memperkuat keamanan jaringan.

4.2 Mekanisme Authentikasi *Port Knocking*

Prinsip dasar dari *Port Knocking* adalah menyembunyikan port layanan dari pandangan publik dan hanya membukanya untuk pengguna yang memang memiliki akses dan mengetahui urutan "*knocks*" yang benar[16]. Adapun cara kerja dari Sistem Keamanan Jaringan menggunakan metode *Port Knocking* dapat dilihat pada Gambar 11 berikut.



Gambar 11. Cara Kerja *Port Knocking*

Gambar 11 menunjukkan cara kerja *Port Knocking* dimana Pengguna membuat skrip PowerShell berisi daftar port dan alamat IP router MikroTik yang akan diakses, kemudian menjalankan skrip untuk melakukan ketukan pertama pada port secara berurutan. PowerShell akan menampilkan status koneksi pada setiap port; jika ketukan sesuai konfigurasi, IP pengguna akan tercatat dalam "Knocking-1" pada MikroTik, namun jika tidak, ketukan harus diulang. Pengguna kemudian melakukan ketukan kedua dengan cara serupa untuk masuk ke daftar "Knocking-2" jika ketukan sesuai aturan. Setelah semua ketukan selesai dengan urutan yang benar, IP pengguna akan masuk ke daftar "Login," memungkinkan akses ke port layanan yang diinginkan. Jika ada kesalahan urutan, pengguna harus mengulangi ketukan dari awal hingga benar.

4.3 Alat dan Bahan

Perangkat yang dibutuhkan dalam penerapan sistem kemanaan jaringan menggunakan metode *Port Knocking* ini terdiri atas perangkat keras (hardware) dan juga perangkat lunak (software) yaitu :

TABEL I
ALAT DAN BAHAN

Perangkat Keras dan Lunak yang Dibutuhkan		
NO	**Perangkat**	**Keterangan**
1	Laptop Lenovo Ideapad Slim 3	Berfungsi sebagai alat untuk mengembangkan dan menguji sistem keamanan jaringan menggunakn *Port Knocking*.
2	MikroTik CCR1009-7G-1C-1S+	Sebagai titik akses utama jaringan yang akan diterapkan sistem keamanan jaringan menggunakan *Port Knocking*
3	Kabel LAN UTP	Sebagai penghubung MikroTik dengan PC
4	Ethernet Adapter	
5	Winbox	Digunakan untuk mempermudah konfigurasi sistem keamanan jaringan menggunakan metode *Port Knocking*.
6	PuTTY	Digunakan untuk melakukan pengujian akses terhadap *port* 22 (SSH) dan 23 (Telnet)
7	Nmap dan Nessus	Digunakan untuk deteksi kerentanan pada *port* dengan teknik *Port Scanning.*
8	PowerShell	Digunakan untuk melakukan aturan ketukan menggunakan *script* yang dibuat.

5. Pengujian Sistem Keamanan Jaringan

Pengujian sistem keamanan jaringan menggunakan metode *Port Knocking* dalam penelitian ini dilakukan melalui beberapa jenis pengujian, yaitu *Port Scanning* , serangan *brute force* , dan serangan *DDoS* . Pengujian *Port Scanning* bertujuan untuk mengidentifikasi apakah port-port yang telah dikonfigurasi dengan metode *Port Knocking* dapat tersembunyi dari deteksi pihak yang tidak sah. Serangan *brute force* digunakan untuk menguji ketahanan akses terhadap port yang telah dikunci, guna memastikan bahwa hanya pengguna yang memiliki izin yang dapat membuka akses ke port tersebut. Sementara itu, serangan *DDoS* dilakukan untuk menguji kemampuan sistem dalam menghadapi serangan lalu lintas jaringan yang tinggi, yang bertujuan untuk melihat sejauh mana sistem tetap stabil dan tidak mudah diakses oleh pihak yang tidak berwenang. Melalui pengujian ini, diharapkan efektivitas metode *Port Knocking* dalam meningkatkan keamanan jaringan dapat diukur dengan baik.

III. HASIL DAN PEMBAHASAN

1. Hasil Uji *Port Scanning*

Pada penelitian ini, pengujian Port Scanning dilakukan menggunakan Nmap (Network Mapping). Pengujian ini tidak hanya membantu dalam mengidentifikasi titik lemah dalam jaringan, tetapi juga menilai apakah langkah-langkah sistem keamanan *Port Knocking* yang diterapkan sebelumnya sudah diterapkan dengan benar. Hasil dari pengujian Port Scanning dapat dilihat pada Tabel II berikut.

TABEL II
HASIL UJI PORT SCANNING

NO	PORT	STATUS PORT
1	80 (HTTP)	Filtered
2	22 (SSH)	Filtered
3	23 (Telnet)	Filtered
4	8291 (winbox)	Filtered

Tabel II menunjukkan hasil uji Port Scanning yamg dilakukan setelah sistem Port Knocking diterapkan, status semua port yang diuji, yaitu port 80 (HTTP), port 22 (SSH), port 23 (Telnet), dan port 8291 (Winbox) berubah menjadi 'filtered'. Artinya, port-port tersebut tidak terdeteksi terbuka atau tertutup saat dilakukan pemindaian jaringan. Kondisi ini menunjukkan bahwa Port Knocking efektif dalam menyembunyikan port dari potensi serangan awal, seperti *port scanning* yang sering kali dilakukan oleh penyerang untuk menemukan celah keamanan.

2. Hasil Uji *Brute Force*

Serangan *Brute Force* yang dilakukan pada penelitian ini menggunakan Sistem Operasi Linux Ubuntu dengan bantuan alat hydra. Serangan ini dilakukan untuk mendapatkan hak akses yang tidak sah dengan cara mencoba semua kemungkinan kombinasi *username* dan *password.* Selama proses ini, hydra akan mengirimkan sejumlah permintaan login dengan berbagai kombinasi *password* hingga berhasil. Hasil dari pengujian brute force dapat dilihat pada Tabel III berikut.

TABEL III
HASIL UJI BRUTE FORCE

NO	PORT	USERNAME	WAKTU YANG DIBUTUHKAN	STATUS
1	80 (HTTP)	smktaruna	1 menit 30 detik	Can not connect
2	22 (SSH)	smktaruna	32,9 detik	Connection refused
3	23 (Telnet)	smktaruna	1 menit 28 detik	Can not connect
4	8291 (winbox)	smktaruna	11, 36 detik	Error : timed out

Tabel III menunjukkan bahwa serangan *brute force* yang dilakukan terhadap port yang sudah diamankan dengan *Port Knocking* sebelumnya gagal mendapatkan kombinasi kredensial (*password*) untuk mengakses layanan manajemen melalui port jaringan SMK Taruna Satria Pekanbaru. Waktu yang dibutuhkan untuk menyerang pun sangat singkat karena port atau jalan masuknya serangan sudah tertutup dan diamankan dari pengguna tidak sah menggunakan sistem keamanan *Port Knocking*.

3. Hasil Uji DDoS (*Distributed Denial of Service*)

Serangan DDoS (Distributed Denial of Service) pada penelitian ini dilakukan menggunakan Sistem Operasi Linux Ubuntu, LOIC (Low Orbit Ion Cannon) dan hping3. Serangan ini bertujuan untuk menguji seberapa tangguh sistem jaringan dalam menahan arus lalu lintas yang berlebihan. Dengan mengirimkan sejumlah besar permintaan dalam waktu singkat ke server target, serangan ini berupaya membuat layanan menjadi tidak tersedia bagi pengguna sah. Hasil pengujian DDoS dapat dilihat pada Tabel IV berikut.

TABEL IV
HASIL UJI DDOS

NO	PORT	Durasi	Jumlah Requested	Beban CPU	STATUS
1	80 (HTTP)	15 menit	0	20 %	Gagal
2	22 (SSH)	15 menit	0	22 %	Gagal
3	23 (Telnet)	15 menit	0	25 %	Gagal
4	8291 (winbox)	15 menit	0	22 %	Gagal

Tabel IV menunjukkan bahwa tidak ada permintaan yang berhasil mencapai server target pada port yang sudah diamankan oleh Port Knocking, dan beban CPU tetap dalam kondisi stabil meski serangan berlangsung selama 15 menit.

Hasil pengujian ini menunjukkan bahwa penerapan Port Knocking secara signifikan memperkuat keamanan jaringan di SMK Taruna Satria Pekanbaru dengan mencegah akses tidak sah dan melindungi port dari serangan *Port Scanning*, *brute force*, dan DDoS. Dalam perbandingan dengan penelitian sebelumnya, penelitian ini menambah pemahaman dengan menguji ketangguhan Port Knocking dalam konteks pendidikan dan menunjukkan bahwa metode ini dapat menjaga stabilitas layanan jaringan serta melindungi data sensitif di lingkungan sekolah.

IV. KESIMPULAN

Berdasarkan hasil pengujian, didapatkan kesimpulan bahwa penerapan Port Knocking pada port 80 (HTTP), 22 (SSH), 23 (Telnet), dan 8291 (Winbox) berhasil meningkatkan keamanan jaringan di SMK Taruna Satria Pekanbaru, sesuai dengan tujuan awal penelitian. Metode Port Knocking efektif dalam menyembunyikan port dari deteksi *Port Scanning*, mencegah akses tidak sah, dan menjaga stabilitas jaringan meskipun mendapat serangan seperti *brute force* dan DDoS. Penelitian ini membuktikan bahwa Port Knocking memberikan lapisan keamanan yang cukup kuat dibandingkan metode lain dengan membatasi akses hanya pada pengguna yang mengetahui urutan ketukan yang benar. Penerapan Sistem Keamanan ini penting dalam instansi pendidikan yang membutuhkan perlindungan lebih pada data dan layanan jaringan, sehingga jaringan sekolah menjadi lebih aman dan stabil.

REFERENSI

[1] R. Rizal, R. Ruuhwan, and K. A. Nugraha, “Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941,” *J. ICT Inf. Commun. Technol.*, vol. 19, no. 1, pp. 1–8, 2020, doi: 10.36054/jict-ikmi.v19i1.119.

[2] M. Mudzakkar, S. Siaulhak, and J. Jumarniati, “Analisis Deteksi Dan Pencegahan Eksploitasi Jaringan Brute Force Exploit Menggunakan Firewall Pada Kantor Bappeda Kota Palopo,” *SIBATIK J. J. Ilm. Bid. Sos. Ekon. Budaya, Teknol. dan Pendidik.*, vol. 2, no. 4, pp. 1097–1106, 2023, doi: 10.54443/sibatik.v2i4.718.

[3] T. Brades and Irwansyah, “Pemanfataan Metode Port Knocking Dan Blocking,” *Semin. Has.*

Penelit. Vokasi, vol. 3, no. No.2, pp. 1–9, 2022.

[4] F. Baso and M. Ardiansyah, "Implementasi Metode Port Knocking pada MikroTik RouterOS untuk Mendukung Keamanan Jaringan," *J. Secur. Comput. Information, Embed. Network, Intell. Syst.*, vol. 8329, pp. 31–35, 2023, doi: 10.61220/scientist.v1i1.235.

[5] Yudi mulyanto, M. Julkarnain, and A. Jabi Afahar, "Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar," *J. Inform. Teknol. dan Sains*, vol. 3, no. 2, pp. 326–335, 2021, doi: 10.51401/jinteks.v3i2.1016.

[6] P. D. Oktaviansyah, "Penerapan Sistem Pengamanan Port pada Mikrotik Menggunakan Metode Port Knocking," *NetPLG J. Netw. Comput. Appl.*, vol. 1, no. 2, pp. 13–24, 2022.

[7] M. Dewi, A. Budiono, and U. Y. K. S. Hediyanto, "Vulnerability Assessment pada Website Rekruitasi Asisten (IRIS) Fakultas Rekayasa Industri menggunakan Nikto dan Nessus," *e-Proceeding Eng.*, vol. 10, no. 2, pp. 1631–1636, 2023.

[8] Tedyyana, Agus, and Osman Ghazali. "Real-time Hypertext Transfer Protocol Intrusion Detection System on Web Server using Firebase Cloud Messaging." (2023): 385-392.

[9] R. Ernawati, I. Ruslianto, S. Bahri, J. Rekayasa, and S. Komputer, "Implementasi Metode Port Knocking Pada Sistem Keamanan," *J. Komput. dan Apl.*, vol. 10, no. 01, pp. 158–169, 2022, [Online]. Available: https://jurnal.untan.ac.id/index.php/jcskommipa/article/download/54226/75676593086.

[10] M. Xu *et al.*, "AHAC: Advanced Network-Hiding Access Control Framework," *Appl. Sci.*, vol. 14, no. 13, pp. 1–20, 2024, doi: 10.3390/app14135593.

[11] S. Dwiyatno, "Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 2, pp. 108–115, 2020, doi: 10.30656/prosisko.v7i2.2522.

[12] Z. Arifin, "Keamanan dan Ancaman pada Cyberspace," pp. 1–37, 2019.

[13] R. A. Febrian, Y. Muhyidin, and D. Singasatia, "ANALISIS PENYERANGAN BRUTEFORCE TERHADAP SECURE SHELL (SSH) MENGGUNAKAN METODE PENETRATION TESTING," vol. 2, pp. 151–162, 2024.

[14] R. Nurbahri and G. W. Nurcahyo, "Jurnal Sistim Informasi dan Teknologi Analisis Penggunaan Metode Port Knocking pada Sistem Keamanan Jaringan Komputer (Studi Kasus di Universitas Baiturrahmah)," *Sistim Inf. dan Teknol.*, vol. 5, no. 1, pp. 102–108, 2023, doi: 10.37034/jsisfotek.v5i1.211.

[15] R. K.Yin, *Case Study Research : Metode and Design edition : 5*. 2014.

[16] I. Marzuki, "Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux," *J. Teknol. Inf. Indones.*, vol. 2, no. 2, pp. 18–24, 2019, doi: 10.30869/jtii.v2i2.312.