



PeTeKa (Jurnal Penelitian Tindakan Kelas dan Pengembangan Pembelajaran)

Issn Cetak : 2599-1914 | Issn Online : 2599-1132 | Vol. 8 No. 1 (2025) | 293-300

DOI: <http://dx.doi.org/10.31604/ptk.v8i1.293-300>

IMPLEMENTASI PENGGUNAAN CYBER SECURITY DENGAN METODE PORT KNOCKING TERHADAP KEAMANAN JARINGAN DI KAMPUS 1 SMK MUHAMMADIYAH 1 PADANG

Riski Pratama*, Ami Anggraini Samudra, Rini Novita

Pendidikan Informatika, Universitas PGRI Sumatera Barat, Indonesia.

*e-mail: riskipratamalubis02@gmail.com

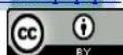


Abstrak. Perkembangan teknologi berarti berbagai aspek kehidupan, segala aspek kehidupan tidak lepas dari sentuhan teknologi dengan segala kenyamanannya. Namun setiap hal baru selalu mempunyai akibat baru. Salah satu dampak yang perlu kita lihat adalah kejahatan dunia maya. Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem keamanan jaringan dan monitoring jaringan terhadap serangan jaringan dan permintaan waktu yang ada di Kampus 1 SMK Muhammadiyah 1 Padang. Penelitian ini menggunakan metode gate dengan model pengembangan PPDIOO. Penelitian implementasi keamanan siber menggunakan metode gate dengan model pengembangan PPDIOO yang terdiri dari 6 tahapan yaitu persiapan, perencanaan, desain, implementasi, penggunaan, optimalisasi. Dalam pengujian tersebut diperoleh hasil penelitian yang dilakukan selama implementasi, khususnya keadaan port 22 tertutup, dari lima pengujian yang dilakukan, keadaan port 22 tertutup 100%. Tes ini juga dapat menunjukkan keberhasilan penerapan metode mendengarkan port server.

Kata Kunci: Implementasi, Metode, Portal Bank.

Abstract. The development of technology means various aspects of life, all aspects of life cannot be separated from the touch of technology with all its comforts. But every new thing always has a new result. One of the impacts we need to see is cybercrime. The purpose of this study is to implement a network security system and network monitoring against network attacks and time requests in Campus 1 of SMK Muhammadiyah 1 Padang. This study uses the gate method with the PPDIOO development model. Cybersecurity implementation research uses the gate method with the PPDIOO development model which consists of 6 stages, namely preparation, planning, design, implementation, use, and optimization. In the test, the results of research conducted during the implementation were obtained, especially the state of port 22 is closed, from the five tests carried out, the state of port 22 is 100% closed. This test can also demonstrate the successful implementation of the server port listening method.

Keywords: Implementation, Methods, Bank Portal.



PENDAHULUAN

Keamanan jaringan penting dan harus selalu dijaga, dan jaringan area lokal (LAN) serta jaringan nirkabel yang terhubung ke Internet pada dasarnya tidak aman dan selalu rentan terhadap peretas. Karena data harus melewati beberapa terminal untuk sampai ke sana, hal ini menciptakan peluang bagi pengguna lain yang tidak bertanggung jawab untuk mengubah, mengubah, merusak, atau bahkan mencuri data tersebut (penyerang). Salah satu bagian terpenting dari suatu jaringan adalah keamanan jaringan. Namun, masalah keamanan jaringan seringkali kurang mendapat perhatian. Untuk meningkatkan keamanan jaringan, administrator sistem mencoba hanya menggunakan perlindungan terbaik, seperti firewall dan sistem deteksi intrusi (IDS). (Desmira & Wiryadinata, 2022).

SMK Muhammadiyah 1 Padang merupakan salah satu sekolah menengah kejuruan swasta yang ada di Padang, Provinsi Sumatera Barat. SMK Muhammadiyah 1 Padang kini telah memiliki jaringan internet yang memudahkan siswa untuk mencari berbagai sumber informasi materi pembelajaran atau sekedar informasi umum dan sumber informasi yang cepat dan akurat dengan menggunakan dunia digital khususnya Internet SMK Kampus 1. Muhammadiyah 1 Padang.

Peranan internet dalam kegiatan pendidikan sangat penting, akses informasi semakin cepat. Dapat dikatakan bahwa akses informasi di Internet terkadang lebih mutakhir dibandingkan di buku cetak (Budi, 2021). Selain itu, siswa memiliki akses lebih cepat terhadap informasi valid, seperti jurnal atau literatur akademik, misalnya melalui Google Scholar. Internet juga membantu siswa untuk

memahami materi pembelajaran dengan lebih mudah. Setiap siswa dapat membuka informasi terkait topik dalam bentuk teks, gambar atau bahkan video visual yang menarik. Materi pembelajaran singkat dan praktis juga tersedia online. Jika pada umumnya siswa kesulitan memahami materi di buku, mereka dapat mencari metode pembelajaran yang lebih mudah dipahami melalui internet, seperti menonton video pembelajaran.

Berdasarkan hasil observasi yang dilakukan peneliti pada tanggal 26.3.2024 di SMK Muhammadiyah 1 Padang, ditemukan permasalahan pada pelatihan dimana jaringan mati mendadak di laboratorium jurusan TKJ pada saat melakukan PBM di laboratorium dan pelatihan atau Praktek Ini harus dihentikan setelah beberapa hari karena harus mengecek dan mengatasi masalah yang muncul, dan sebagai masalah ternyata beberapa komputer di jurusan TKJ mengalami blue screen karena akses internet kurang aman. jaringan, jadi ketika file diunduh, virus berbahaya masuk ke dalamnya, yang menyebabkan bootloader crash pada sektor tersebut atau kerusakan fisik pada hard drive. Oleh karena itu, penting untuk menerapkan perlindungan jaringan untuk mengatasi masalah ini.

Jaringan komputer adalah suatu sistem yang menghubungkan dua node atau lebih dengan menggunakan media komunikasi, baik kabel maupun nirkabel, sebagai perantara untuk berbagi sumber daya seperti perangkat lunak, data, perangkat keras seperti printer dan media penyimpanan antar perangkat berbeda yang terhubung. (PY, Samudra dan Untari, 2023).

Pembahasan keamanan jaringan ini menggunakan pendekatan gateway yang mampu melindungi, memfilter, membatasi, atau memblokir seluruh

koneksi jaringan dari segmen jaringan privat hingga jaringan eksternal di luar cakupannya. Penelitian ini menjelaskan keamanan jaringan dengan menggunakan metode port snooping, yaitu membuka akses pada port tertentu yang telah diblokir oleh firewall perangkat jaringan dengan mengirimkan paket atau koneksi tertentu (Rizal dkk., 2020).

Penelitian yang dilakukan oleh perusahaan (Prakos, 2022) berjudul "Implementasi Honeypot dan Gate Knocking dengan Interaksi Rendah untuk Meningkatkan Keamanan Jaringan" Penelitian ini dilakukan di Institut Teknologi Bisnis Muhammadiyah Purbalingga. Selama penerapan, Port Knocking dapat mencegah penyerang dari pemindai sistem seperti layanan SSH dengan mentransfer pemindaian port eksternal mencegah layanan SSH agar tidak mudah dilacak dan diakses oleh orang lain.

Penelitian yang dilakukan oleh perusahaan (Yudi Muliando dkk., 2021) tanda "Penerapan fungsi Port Knocking untuk mengamankan jaringan di SMKN 1 Sumbawa Besar" Penelitian ini valid Bank Pelabuhan Keamanan Jaringan SMKN 1 Sumbawa Besar dilengkapi dengan Routerboard Mikrotik RB750r2 dan aplikasi pendukung lainnya. Dengan menggunakan metode port vating untuk mengamankan jaringan SMKN 1 Sumbawa dapat membantu meningkatkan keamanan jaringan dan membantu administrator mengamankan Routerboard Mikrotik pada sistem jaringan komputer SMKN 1 Sumbawa Besar.

Salah satu yang dapat dilakukan adalah dengan membuka akses port tertentu yang telah diblokir oleh firewall perangkat jaringan dengan

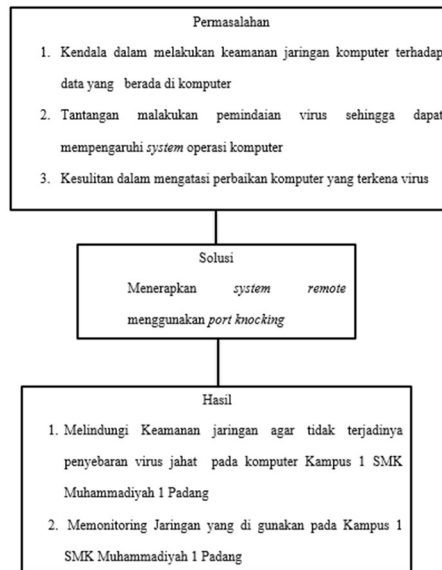
mengirimkan paket atau koneksi tertentu. Koneksi dapat berupa protokol TCP, UDP atau ICMP. Jika koneksi yang dikirim oleh host cocok dengan aturan mendengarkan yang digunakan, firewall secara dinamis mengizinkan akses ke port yang diblokir (Ernawati, 2022). Dengan cara ini, perangkat jaringan seperti router lebih aman karena administrator jaringan dapat memblokir port yang rentan terhadap serangan, seperti Winbox, SSH, Telnet atau webfig. Jika pemindaian port dilakukan, port tersebut tampak tertutup. Di sisi admin jaringan, Anda masih dapat mengkonfigurasi dan memantau, tetapi dengan langkah khusus (menekan) untuk mengizinkan firewall memberikan akses ke port dengan menghubungkan Telegram Boot, yang memudahkan admin untuk memantau melalui penerapan metode gateway untuk menyadap SMK Muhammadiyah 1 Padang Kampus 1.

METODE

Dalam penelitian ini, penulis menggunakan beberapa metode pengumpulan data sebagai pendukung. Penulis melakukan observasi langsung ke lapangan yang menjadi tempat penelitian penulis yaitu SMK Muhammadiyah 1 Kampus 1 Padang. Implementasi yang sudah selesai meliputi pengamanan jaringan di SMK Muhammadiyah 1 Padang Kampus 1. Pada tanggal 26 Maret 2024 penulis melakukan observasi di SMK Muhammadiyah 1 Padang Kampus 1.

(Farudin, 2022) Dalam penelitian ini penulis menggunakan metode PPDIOO. Salah satu kelebihan metode ini adalah dapat mengurangi biaya pembangunan jaringan komputer (Sandy, Sriyanto dan Novita, 2024). Pada

metode PPDIOO perencanaan jaringan harus melalui 6 tahapan.



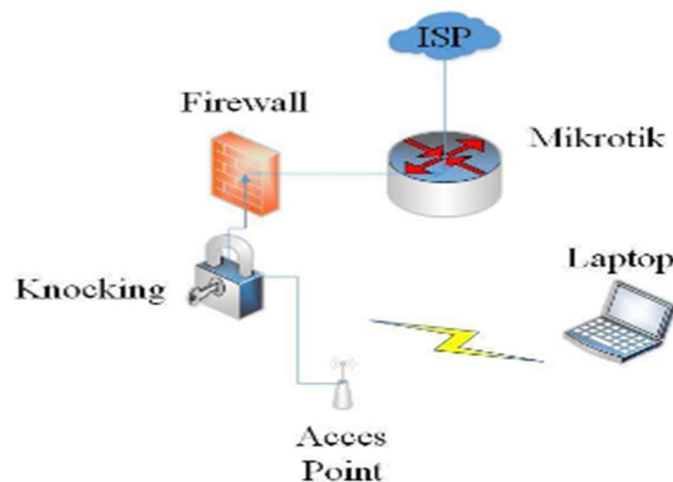
Gambar 1. Kerangka Berfikir

HASIL DAN PEMBAHASAN

Penerapan keamanan siber adalah proses penggunaan berbagai teknik dan alat untuk melindungi jaringan komputer dari ancaman seperti serangan dunia maya, akses tidak sah, dan kehilangan data. Hal ini mencakup beberapa langkah yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan data. Implementasi

keamanan siber dari program yang dibuat.

Langkah-langkah dalam proses implementasi merupakan rangkaian dari langkah konfigurasi awal hingga langkah implementasi akhir yang harus dilakukan untuk mengimplementasikan aplikasi Cyber. Istimewa Bpk. Perancangan yang dilakukan untuk mengimplementasikan metode Port Knocking biasanya ditunjukkan pada gambar di bawah ini.



Gambar 2. Topologi Knocking Gate

Gambar 2 menjelaskan bahwa biasanya topologi bank gateway memiliki jaringan yang menyediakan server proxy Internet dan terhubung ke titik akses.

Cyber-front Padang-ed Padang-ed Kampus 1 Cyber A, jaringan LAN

digunakan untuk menyiapkan server proxy pada tanggal 21 Agustus 2024.

Langkah pertama yang perlu Anda lakukan adalah login ke Mikrotik menggunakan Winbox. Caranya adalah sebagai berikut: Buka aplikasi Winbox yang sudah anda download dan install.



Gambar 3. Aplikasi Winbox

Hubungi kami Router Melalui Mikrotik PC atau Laptop menggunakan

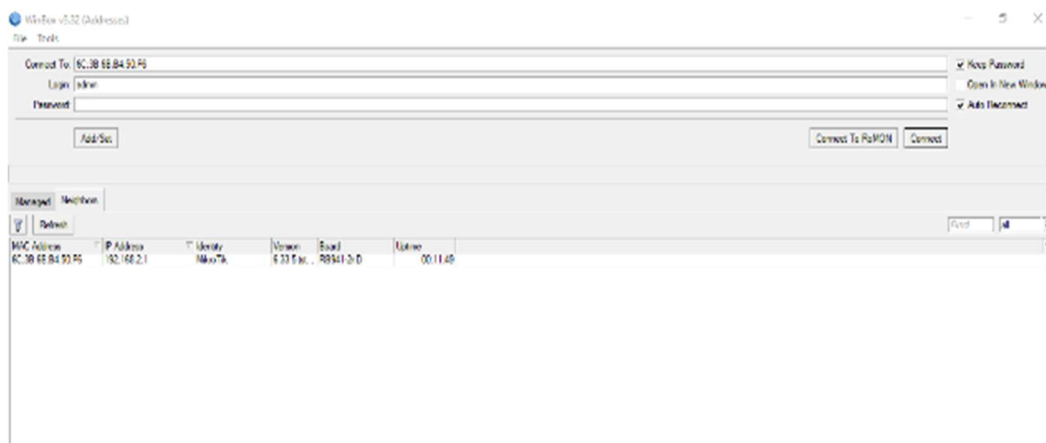
kabel UTP straight ke Ethernet port 2 Mikrotik



Gambar 4. Menghubungkan Mikrotik Ke Komputer Dengan Kabel UTP

Di Winbox, klik tab Neighbors dan klik Update. Alamat MAC dan

alamat IP Mikrotik ditunjukkan pada kolom di bawah ini



Gambar 5. Kemunculan Pertama Winbox

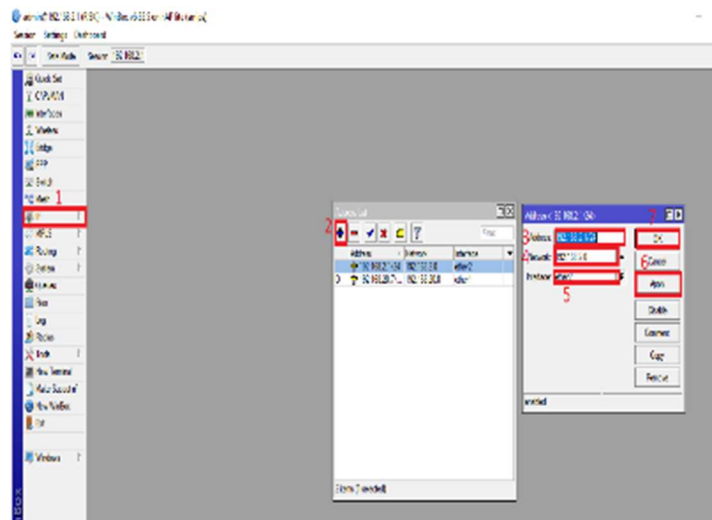
Langkah selanjutnya yang perlu Anda lakukan adalah mengatur alamat

IP untuk ether2. Alamat IP adalah pengidentifikasi unik yang ditetapkan

Riski Pratama, dkk. Implementasi Penggunaan Cyber Security...

untuk setiap perangkat yang terhubung ke jaringan. Alamat IP memungkinkan perangkat untuk berkomunikasi satu sama lain dan mengirim data. Dengan Mikrotik, kita bisa mengatur alamat IP secara manual atau otomatis. Pada tahap ini kita akan menggunakan ether2 secara manual yang merupakan gateway atau pintu gerbang bagi perangkat lain yang ingin terhubung ke Internet melalui Mikrotik.

Caranya adalah sebagai berikut: Di Winbox, klik menu IP dan pilih Alamat. Klik tanda tambah (+) untuk menambahkan alamat IP baru. Di formulir alamat, masukkan alamat IP dan awalan (/24) yang ingin Anda gunakan untuk ether2. Misalnya 192.168.2.1/24. Di formulir antarmuka pengguna, pilih ether2. Klik Terapkan dan OK.



Gambar 6. Pengaturan Alamat IP Ether2

Cara mengamankan router Mikrotik dengan port bank. Router mikrotik biasanya ditempatkan di antara jaringan publik yang tidak tepercaya dan jaringan lokal yang tepercaya. Oleh karena itu, sangat penting untuk mengaktifkan keamanan di router Mikrotik, jika tidak hacker dapat menyusupi router Mikrotik. Mikrotik RouterOS memiliki berbagai teknik firewall untuk melindungi Router Mikrotik, salah satunya adalah port vating.

Setelah Anda membuat aturan port banking dinding pelindung Pertama, sekarang kita akan membuat rule gate knocking yang lain untuk memblokir user yang ingin login ke Mikrotik dengan cara mengatur door to close dan pilih aksi drag and drop untuk memblokir user yang ingin login ke Mikrotik.

Pada setup kali ini, saya akan membuat sistem monitoring jaringan menggunakan Telegram. Untuk memonitor jaringan melalui Telegram kita bisa menggunakan fungsi Netwatch dan Fetch pada MikroTik.



Gambar 7. Mencari Botfather

Kemudian ditampilkan hasil pembuatan bot. Salin dan simpan ID untuk digunakan di masa mendatang. Salin dan simpan ID. keamanan siber dan pengawasan jaringan.

Pengujian ini menggunakan Telegram, Putty dan komputer server, dimana komputer server digunakan sebagai pengujian serangan, yang dilakukan pada Putty yang mencoba menyerang melalui port SSH dan Telnet, serta dimonitor oleh Telegram, dimana aplikasi ini memberikan informasi tentang Mikrotik.

Pengujian ini dilakukan dengan dua langkah, yaitu pengujian pada saat jaringan up dan down. Pengujian ini dilakukan dengan cara melepaskan kabel UTP dari proxy server ke komputer dan menyambungkan kembali kabel UTP dari proxy server ke komputer.

Dalam penelitian ini, untuk menyelidiki keamanan metode port eavesdropping yang digunakan untuk melindungi jaringan dari penyusup, beberapa serangan dilakukan, termasuk system eavesdropping dan brute force SSH dan Telnet. Tujuan dari pengujian ledakan sistem adalah untuk mengetahui keberhasilan penerapan metode pada sistem, hasilnya mungkin metode tersebut berhasil diterapkan

pada sistem. Hal ini ditunjukkan dengan membuka server yang harus ditekan terlebih dahulu, jika tidak maka port host 22 akan dalam keadaan tertutup.

Hasil yang didapat dari pengujian adalah keadaan port 22 dalam keadaan tertutup, dari 5 pengujian yang dilakukan keadaan port 22 100% dalam keadaan tertutup. Upaya ini mungkin juga terbukti berhasil.

SIMPULAN

Berdasarkan hasil implementasi dan pengujian yang dilakukan, disimpulkan bahwa berdasarkan hasil penelitian, metode port knocking berhasil melindungi server web service dengan cara memblokir port 22 dan membuka port SSH (22) saat layanan sedang berjalan. . diperlukan Dengan mengaktifkan penyetelan port, kami juga berhasil mengatasi masalah pemblokiran port firewall. Berdasarkan hasil pengujian yang dilakukan pada sistem dengan raw SSH dan Telnet, metode port monitoring mampu melindungi server. Dan langkah terakhir, server proxy dapat dihubungkan ke Telegram sehingga Telegram dapat dengan mudah memperingatkan pengguna dan memantau jaringan. Dengan keamanan

jaringan yang memadai dan mudah dipantau, sekolah tidak perlu lagi khawatir akan persaingan tingkat keamanan jaringan dan dapat dengan cepat menyelesaikannya jika suatu saat terjadi masalah pada sistem jaringan sekolah.

DAFTAR PUSTAKA

- Antariksa, MD dan Aranta, A. (2022). Analisis jaringan komputer Local Area Network (LAN) di RS UNRAM. *Jurnal Teknologi Informasi Begawe (JBegaTI)*, 3 (2).<https://doi.org/10.29303/jbegati.v3i2.748>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan keamanan siber untuk mewujudkan keamanan nasional di era masyarakat 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO)*, 3, 223-234.<https://doi.org/10.54706/senastindo.v3.2021.141>
- Desmira, D. dan Viryadinata, R. (2022). Rancang dan bangun secure shell (SSH) untuk keamanan port menggunakan metode penerusan port. *INSANTek*, 3 (1), 1-5.<https://doi.org/10.31294/instk.v3i1.552>
- Ernawati, R., Ruslianto, I., & Bahri, S. (2022). Implementasi metode port vating pada sistem keamanan virtual server Ubuntu berdasarkan pemantauan online. *Jurnal Komputasi dan Aplikasi Coding*, 10(01), 158.<https://doi.org/10.26418/coding.v10i01.54226>
- Fahrudin, E. dan Subaria, R. (2023). Pentingnya pemahaman keamanan siber di era transformasi digital di Pondok Pesantren Daar El Manshur. 2(1). *Era transformasi digital di Pondok Pesantren Daar El Manshour*. 2(1).
- Marcelina, D. & Iulianti, E. (2022). Workshop dasar keamanan siber di SMK Pgri Tanjung Raja Ogan Ilir (OI). 6(2).
- Nurbahri, R., & Nurchoyo, GW (2023). Analisis penggunaan metode gate knocking pada sistem keamanan jaringan komputer (studi kasus di Universitas Baiturrahmah). 5(1).
- Rizal, R., Ruuhwan, R., & Nugraha, KA (2020). Implementasi proteksi jaringan dengan metode portblocking dan port forwarding di Mikrotik RB-941. *majalah TIK: Telekomunikasi dan teknologi*, 19 (1), 1-8.<https://doi.org/10.36054/jict-ikmi.v19i1.119>