Implementasi *Port Knocking* Untuk Keamanan Jaringan Komputer Dengan Metode *Demilitarized Zone*

Andik Saputro[1)], Daniel Tunggono Saputro[2)], Dwi Remawat[3)]

[1]Program Studi Informatika, STMIK Sinar Nusantara
[2]Program Studi Teknik Informatika, Universitas AKI Semarang
[3]Program Studi Teknologi Informasi (D3), STMIK Sinar Nusantara
[1,3]Jl. K.H Samanhudi No.84-86, Purwosari, Kec. Laweyan, Surakarta, Jawa Tengah 57149
[2]Jl. Imam Bonjol No.15 -17, Dadapsari, Semarang, Jawa Tengah 50173
[1]18500102.andik@sinus.ac.id, [2]daniel.tunggono@unaki.ac.id, [3]remawati@sinus.ac.id

Abstrak

Keamanan jaringan sangat vital untuk jaringan komputer. Kelemahan keamanan pada jaringan komputer jika tidak terlindungi akan menimbulkan kerugian berupa hilangnya data atau file, kerusakan sistem server, tidak optimal melayani pengguna atau bahkan hilangnya aset institusi yang berharga. Di masa pandemi ini, seluruh kegiatan belajar mengajar dan ujian dilakukan secara daring. Dengan ujian online, SMAN 5 Surakarta menyediakan server khusus untuk diberikan kepada siswa. Di sisi lain, server harus dapat diakses secara online sementara ini dapat memicu berbagai serangan pada server dan dimungkinkan untuk menyerang server melalui IP server dan *port* yang dapat mengakibatkan kebocoran data rahasia, pertanyaan yang akan diuji dan data dari peserta atau bahkan serangan ini memungkinkan server turun. Mengetahui cara mengamankan jaringan menggunakan DMZ (zona demiliterisasi) dan *Port Knocking* adalah tujuan penelitian. Serangan yang paling sering digunakan adalah *Port Scanning* dan DDoS (*Distributed Denial of Service*). *Port Scanning* adalah tahap awal untuk mendeteksi port terbuka. Sedangkan DDoS adalah serangan DoS yang memanfaatkan beberapa sumber daya serangan terdistribusi. Biasanya, penyerang menggunakan sejumlah besar bot terkontrol (komputer *host/daemon*, juga disebut sebagai *zombie*) yang didistribusikan di beberapa lokasi berbeda untuk meluncurkan sejumlah besar serangan DoS terhadap satu target atau beberapa target. Untuk itu diperlukan teknik keamanan jaringan yang dapat menangkal ancaman serangan tersebut atau meminimalisir ancaman serangan yang dapat masuk ke dalam sistem jaringan. Pada penelitian ini dilaksanakan teknik DMZ (*demilitarized zone*) untuk mengakses server lokal sehingga dapat diakses dari luar dengan aman dan menggunakan teknik *Port Knocking* untuk membuka port akses yang disaring.

Kata kunci: Keamanan Jaringan, *Port Scanning*, *Distributed Denial of Service*, *Demilitarized Zone*, *Port Knocking*

Abstract

Network security is very vital for a computer network. Weaknesses in computer networks if not protected will cause losses in the form of loss of data or files, damage to server systems, not optimally serving users or even loss of valuable institutional assets. During this pandemic, all teaching and learning activities and exams are carried out online. With the online exam, SMAN 5 Surakarta provides a special server to be provided to students. On the other hand, the server must be accessible online while this can trigger various attacks on the server and it is possible to attack the server via the server IP and port which can result in leaking of confidential data, questions to be tested and data from participants or even these attacks allow the server down. Knowing how to secure a network using DMZ (demilitarized zone) and Port Knocking is the goal of the research. The most frequently used attacks are Port Scanning and DDoS (Distributed Denial of Service). Port Scanning is the initial stage to detect open ports. Whereas DDoS is a DoS attack that utilizes multiple distributed attack resources. Typically, attackers use a large number of controlled bots (host computers/daemons, also referred to as zombies) distributed across several different locations to launch a large number of DoS attacks against a single target or multiple targets. For this reason,

network security techniques are needed that can ward off the threat of these attacks or minimize the threat of attacks that can enter the network system. In this study, the DMZ (demilitarized zone) technique was implemented to access the local server so that it could be accessed from outside safely and using the Port Knocking technique to open filtered access ports.

Keywords: Network Security, Port Scanning, Distributed Denial of Service, Demilitarized Zone, Port Knocking

1. PENDAHULUAN

Di masa pandemi ini seluruh kegiatan belajar mengajar dan ujian dilaksanakan secara online. Server jaringan di sekolah harus dapat diakses secara online sedangkan hal tersebut dapat memicu timbulnya berbagai serangan terhadap server dan tidak menutup kemungkinan akan adanya penyerangan terhadap server melalui IP dan *Port server* yang dapat mengakibatkan bocornya data-data rahasia, soal-soal yang akan diujikan dan data-data dari peserta atau bahkan serangan-serangan tersebut memungkinkan *down*-nya server. Serangan yang paling sering digunakan adalah *Port Scanning* dan DDoS (*Distributed Denial of Service*). *Port Scanning* adalah tahapan awal untuk mendeteksi port-port yang terbuka. Sedangkan DDoS adalah serangan DoS yang memanfaatkan beberapa sumber daya serangan yang terdistribusi. Biasanya, para penyerang menggunakan sejumlah besar bots yang dikendalikan (komputer inang/*daemon*, juga disebut sebagai *zombie*) dan terdistribusi di beberapa lokasi yang berbeda untuk melancarkan sejumlah besar serangan DoS terhadap target tunggal atau beberapa target. Untuk itu diperlukan teknik keamanan jaringan yang dapat menangkal ancaman serangan tersebut atau meminimalisir ancaman serangan yang bisa memasuki sistem jaringan. Dalam penelitian ini dilakukan implemetasi teknik DMZ *(Demilitarized Zone)* untuk mengakses server lokal agar bisa diakses dari luar secara aman dan menggunakan teknik *Port Knocking* agar dapat membuka port akses yang di filter.

2. TINJAUAN PUSTAKA

a. Penelitian Sebelumnya

Pada penelitian sebelumnya yang berjudul "Metode *Demilitarized Zone* dan *Port Knocking* untuk Keamanan Jaringan Komputer" yang dilakukan di perguruan tinggi swasta di Surakarta juga memiliki metode yang sama, yang mana di penelitian selanjutnya akan diterapkan dengan membandingkan *resource* antara kedua objek penelitian. Objek penelitian yang sebelumnya memiliki *resource* yang standar operasi sedangkan di penelitian selanjutnya memiliki *resource* diatas rata – rata atau maksimal. [1]

b. Jaringan Komputer

Jaringan Komputer adalah sekelompok komputer otonom yang saling berhubungan antara satu dengan lainnya menggunakan protokol komunikasi melalui media komunikasi sehingga dapat saling berbagi informasi, program-program, penggunaan bersama perangkat keras seperti printer, harddisk, dan sebagainya. Suatu jaringan komputer terdiri dari komputer, *software*, dan perangkat jaringan yang bekerja bersama dalam satu ruang lingkup yang disebut jaringan. [2]

c. DDoS (*Distributed Denial of Service*)

DoS merupakan jenis serangan yang terstruktur, serangan DDoS (*Distributed Denial of Service*) adalah serangan yang mungkin bisa sering kita jumpai diantara serangan lainnya. Serangan DDoS merupakan teknik yang paling populer dan menjadi senjata pilihan *hacker* karena telah terbukti menjadi ancaman di internet, serangan ini telah ada sejak tahun 1990. Serangan DDoS mampu melumpuhkan server dengan membanjiri lalu lintas jaringan dan mengakibatkan *down*. [3]

d. *Port Scanning*

Port Scanning merupakan sebuah serangan yang dilakukan untuk mendeteksi *port* yang terbuka pada sistem jaringan komputer, dari hasil *port scanning* akan di dapat *port-port* yang terbuka, *Port* tersebut yang akan menjadi celah untuk melakukan penyerangan lebih lanjut. [4]

e. *De-Militarized Zone* (DMZ)

De-Militarized Zone (DMZ) merupakan mekanisme untuk melindungi sistem internal dari serangan *hacker* atau

pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Sehingga karena DMZ dapat diakses oleh pengguna yang tidak mempunyai hak, maka DMZ tidak mengandung rule. Secara esensial, DMZ memindahkan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua *port* terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika *hacker* menyerang dan melakukan *cracking* pada server yang mempunyai DMZ, maka *hacker* tersebut hanya dapat mengakses *host* yang berada pada DMZ, tidak pada jaringan internal. [5]

f. *Port Knocking*

Port Knocking adalah metode untuk menutup dan membuka *port* tertentu yang diamankan oleh *administrator* dengan menggunakan beberapa *key* atau kode untuk dapat membuka dan menutup *port*. [6]

3. METODE PENELITIAN

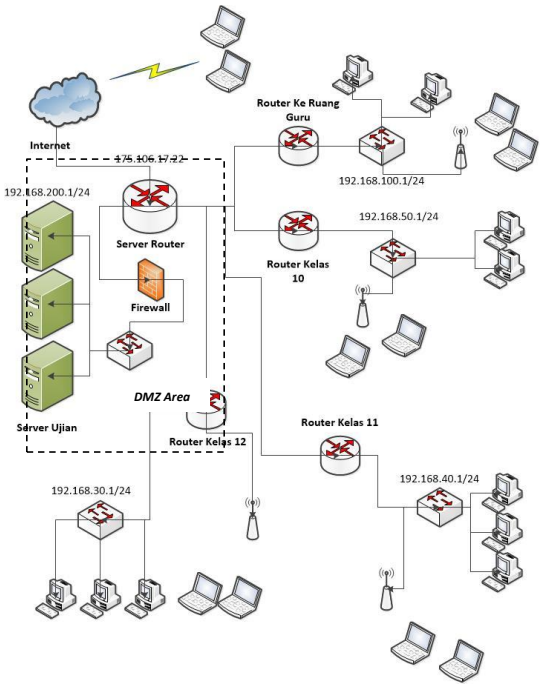
Metode penelitian yang digunakan dalam melaksanakan penelitian ini agar hasil yang dicapai tidak menyimpang dari tujuan yang telah ditetapkan sebelumnya melalui tahapan sebagai berikut ini :

a. Analisa Kebutuhan

Pada tahapan analisa kebutuhan mengidentifikasi masalah dari sistem keamanan jaringan komputer di SMAN 5 Surakarta. Di penelitian ini masalah yang ada siswa mengakses server ujian dari luar dan dalam, maka diperlukan keamanan server sedangkan server ujian online sekarang belum diberikan keamanan jaringan yang penuh agar terhindar dari serangan luar ketika siswa mengakses server tersebut. Admin server menginginkan *router* yang terhubung ke server ujian online dapat di akses dari luar (internet) dengan aman dan tidak adanya port yang terbuka ketika penyerang memindai jaringan SMAN 5 Surakarta dari internet.

b. Perancangan

Dalam perancangan ini dilakukan penentuan model dari topologi jaringan yang sudah ada dan konfigurasi jaringan di SMAN 5 Surakarta. Berikut gambar 1 adalah model dari topologi jaringan yang ada di SMAN 5 Surakarta:



Gambar 1. Topologi Jaringan

c. Implementasi

Tahap implementasi dibuat sistem keamanan jaringan komputer sesuai dengan desain model topologi jaringan. Di tahap ini, server ujian online akan disesuaikan konfigurasinya baik dari segi *software* maupun *hardware* dengan *server router*. Untuk *server router* akan dibuatkan *rule firewall* yang fungsinya untuk metode DMZ agar mengarahkan setiap trafik yang me-*request* ke alamat IP Publik *server router* dengan port 80 akan di teruskan ke *port server* ujian online. Dan setiap trafik yang dari penyerang dengan ditandai di *rule firewall* semua trafik tersebut akan di *drop* di *server router*. Untuk implementasi dari *Port Knocking* akan dibuatkan *rule firewall* terhadap setiap IP yang mengakses dari jaringan luar maupun dalam maka akan di masukkan ke list IP, jika ip tersebut melakukan *ping*, maka alamat IP tersebut akan diberikan hak untuk mengakses seluruh *port* yang ditutup. Jika alamat IP tersebut tidak melakukan *ping* maka dalam list IP akan dibuatkan *rule* lagi, jika IP tersebut melakukan *scanning port*, maka yang terjadi *rule firewall* akan memblokir semua *port* terhadap alamat IP yang melakukan *scanning* tersebut.

d. Pengujian

Pengujian metode dilakukan secara 2 tahap. Pada Metode DMZ dilakukan 2 tahap

pengujian, yang pertama server akan menggunakan DMZ dan yang kedua server tidak menggunakan DMZ. Di pengujian DMZ, server ujian online akan diserang alamat IP Publik dari jaringan luar dengan mengirimkan paket TCP *Flooding*, UDP *Flooding*, dan ICMP *Flooding* secara besar-besaran dalam setiap detik ke server ujian untuk mengetahui sejauh mana metode tersebut berfungsi. Sedangkan pada pengujian *Port Knocking*, akan dilakukan 2 tahapan. Tahapan pertama dengan melakukan *scanning* terhadap alamat IP publik dari server ujian tersebut menggunakan *software* tanpa melakukan *ping* ke alamat tersebut lalu mengakses *server router* tersebut ke *port* ssh (2299). Untuk tahapan kedua men-*scanning* alamat IP publik server ujian online dari jaringan luar akan tetapi sebelumnya melakukan *request ping* ke alamat tersebut dan setelah itu melakukan akses ke *server router* menggunakan *port* ssh (2299).

4. HASIL DAN PEMBAHASAN

a. Bahan

Untuk kebutuhan perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini disajikan dalam Tabel 1 dan Tabel 2 sebagai berikut:

Tabel 1. Spesifikasi Hardware Server

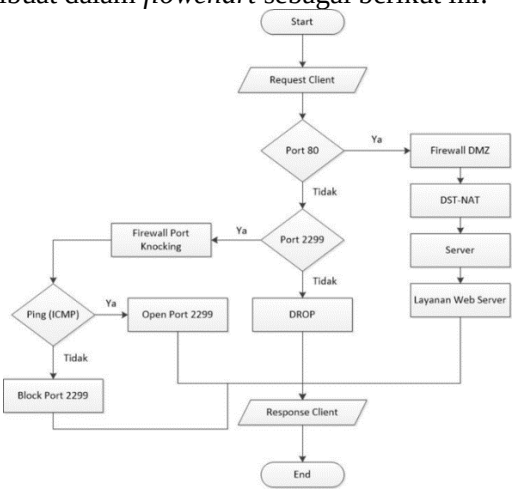
No	Perangkat	Jumlah	Spesifikasi
1	PC Server Web	1	OS : Windows 10 Hardware : Intel Core I9 RAM : 64GB SSD : 1TB VGA : 6GB
2	Mikrotik RB 1100AHx4 Rackmount	1	CPU : Alpine AL21400 1.4 GHz Quad Core RAM : 1 GB Main Storage : 128 MB LAN Ports : 13 Ports Dimensions : 1U case : 444x148x47mm RouterOS License : Level 6
3	Client (Testing)		OS : Linux Mint, Windows 8 Processor : Intel Pentium RAM : 8 GB HDD : 500 GB

Tabel 2. Spesifikasi Software Server

No	Software	Keterangan
1	Windows 10	Sebagai Web Server utama untuk menampilkan web ke client
2	Linux Mint 19	Sebagai monitoring dan penetration testing server
3	Windows 8	Sebagai penetration testing Port Knocking
4	NMAP	Tools yang digunakan untuk pentesting terhadap kerentanan suatu sistem dengan melihat port-port yang terbuka
5	Hping3	Sebagai tools penetration testing DDOS Attack
6	Putty	Software untuk mengkoneksikan client ssh ke ssh server

b. Perancangan

Dalam tahap perancangan ini setelah ditentukan model dari topologi jaringan, maka ditentukan model *mapping* ketika *client* dan server saling berkomunikasi. Model tersebut dibuat dalam *flowchart* sebagai berikut ini:



Gambar 2. *Flowchart* Metode *Port Knocking* yang dikembangkan

Dari gambar 2 diatas adalah model dari perancangan untuk implementasi di lapangan. Dari model tersebut dapat dijelaskan bahwa, pertama *client* akan melakukan *request* terhadap *server router*. Kemudian di *server router request* tersebut akan di-*mapping* yang mana *mapping* tersebut ada 2 yaitu *request* untuk *port* 80 dan *request* untuk *port* 2299. Jika *request* berupa *port* 80 maka akan masuk ke aturan *Firewall* DMZ dan pada akhirnya akan memberikan *response* ke *client* berupa layanan *web server*. Sedangkan jika pada *mapping*, *client* me-*request port* 2299 atau SSH maka akan masuk ke aturan *Firewall Port Knocking*. Pada *Firewall Port Knocking* akan di *mapping* jika *client* tersebut selama melakukan *request* ke *server router* dengan membawa *request* paket ICMP (*ping*) maka akan membuka *port* 2299 (SSH) dan seluruh *port* yang di *disable* oleh *router*. Jika *request* ke server, *client* tidak membawa *request* paket ICMP (*ping*) maka *request* tersebut akan di *drop*.

c. Implementasi

Dalam tahapan ini, akan dilakukan konfigurasi DMZ dan *Port Knocking* pada *server router*.

1) Konfigurasi DMZ

Untuk konfigurasi DMZ akan terfokus di konfigurasi *router*, yang mana akan membuat *firewall rule* untuk memblokir paket DDOS yang dikirimkan dari client penyerang, sehingga ketika adanya paket yang datang secara besar-besaran, *router* akan memblokir paket tersebut atau *drop*.

2) Konfigurasi *Port Knocking*

Pada konfigurasi *Port Knocking* maka akan dikonfigurasi untuk *openport* dan menonaktifkan *port* yang tidak digunakan (kecuali *port* 2299).

d. Pengujian

Dalam tahap pengujian, pengujian yang pertama dilakukan adalah pengujian DMZ dan selanjutnya adalah *Port Knocking*. Berikut adalah pengujian dari kedua metode tersebut:

1) Pengujian DMZ

Pada Metode DMZ dilakukan 2 tahap pengujian, yang pertama server akan menggunakan DMZ dan yang kedua server tidak menggunakan DMZ. Di pengujian DMZ, server ujian online akan diserang alamat IP Publik dari jaringan luar dengan mengirimkan paket TCP *Flooding*, UDP *Flooding*, dan ICMP *Flooding* secara besar-besaran dalam setiap detik ke server ujian untuk mengetahui sejauh mana metode tersebut berfungsi.

2) Pengujian *Port Knocking*

Pada pengujian *Port Knocking*, akan dilakukan 2 tahapan. Tahapan pertama dengan melakukan *scanning* terhadap alamat IP publik dari server ujian tersebut menggunakan software tanpa melakukan ping ke alamat tersebut lalu mengakses *server router* tersebut ke *port* ssh (2299). Untuk tahapan kedua men-*scanning* alamat IP publik server ujian online dari jaringan luar akan tetapi sebelumnya melakukan *request ping* ke alamat tersebut dan setelah itu melakukan akses ke *server router* menggunakan *port* ssh (2299). Dari 2 pengujian *Port Knocking* maka akan didapatkan perbedaan ketika men-*scanning* alamat IP publik dari luar yang melakukan *request ping* dan belum melakukan *request ping* serta akses ke *port* ssh yang sudah melakukan *request ping* ke *server router* dan belum melakukan *request ping* ke *server router*.

e. Hasil

1) DMZ (*De- Militarized Zone*)

Hasil yang diperoleh dari hasil pengujian yang telah dilakukan yaitu berupa data perbandingan *loging server* saat terjadi DDoS *attack* dari tiga jenis pengujian DoS *attack* sebelum dan sesudah server diimplementasi teknik DMZ, hasil perbandingan tersebut dapat dilihat pada tabel berikut:

Tabel 3. Trafik Jaringan Tanpa DMZ

Metode/ Pengujian	0	1	2	3	4	5	6	7
UDP Flooding	64471	63454	66158	58749	59388	64080	64387	65532
ICMP Flooding	945696	979059	954148	951498	972169	971084	97226	961774
TCP Flooding	65991	63709	64180	64729	66218	64868	64941	64777

Tabel 4. Trafik Jaringan Dengan DMZ

Metode/ Pengujian	0	1	2	3	4	5	6	7
UDP Flooding	892	895	884	875	879	654	789	952
ICMP Flooding	1024	1652	1236	1254	1481	1521	1254	1231
TCP Flooding	621	526	669	656	639	652	568	592

Tabel 3 dan 4 diatas menggunakan satuan kbit/s.

2) Port Knocking

Pengujian pertama dilakukan *port scanning* ke alamat IP *server router* untuk melihat *port - port* yang terbuka. Sedangkan pada pengujian kedua diperoleh data hasil koneksi ke *server router* dengan menggunakan SSH Linux yang disajikan pada tabel 5. Dari data tersebut terjadi 3 kegagalan dalam koneksi ke *server router* dari 10 kali pengujian. 1 - 3 pengujian mengalami kegagalan secara berturut-turut.

Tabel 5. Pengujian Port Knocking

Pengujian	Hasil	Keterangan
1	X	Gagal
2	X	Gagal
3	X	Gagal
4	V	Berhasil
5	V	Berhasil
6	V	Berhasil
7	V	Berhasil
8	V	Berhasil
9	V	Berhasil
10	V	Berhasil

5. PENUTUP

a. Kesimpulan

Berdasarkan penelitian yang telah dilakukan maka dapat disimpulkan sebagai berikut:

1) Dapat mengkombinasikan 2 metode yaitu DMZ dan *Port knocking* sekaligus untuk keamanan jaringan.
2) Perbedaan *resource* baik dari segi *software* maupun *hardware* dapat mempengaruhi trafik jaringan di server.
3) DMZ (*De-Militarized Zone*) mempengaruhi trafik jaringan di server.
4) Penurunan trafik jaringan dengan menggunakan DMZ dikarenakan request yang bersifat *flooding* ditangani dibagian *server router*.
5) Penggunaan *Port Knocking* sangat bermanfaat pada kondisi jaringan yang menengah kebawah, karena dapat membantu *administrator* dalam mengkonfigurasi *server router* dan tetap menjaga keamanan *server router*.

b. Saran

Untuk saran dari penelitian yang sudah dilakukan adalah sebagai berikut:

1) Agar trafik jaringan pada server ujian tidak terlalu tinggi, maka disarankan menggunakan server virtual. Yang mana jenis dari server tersebut sangatlah berpengaruh pada waktu *response* setiap *request* dari client.
2) Selain jenis dari server agar *request* dari *client* dapat di *handle* dengan baik oleh server utama, maka disarankan menggunakan sistem operasi Linux (khusus pada penggunaan server). Jika pada penelitian ini server menggunakan sistem operasi Windows, yang mana sangat berpengaruh terhadap waktu *response* dan *handle request* dari client.
3) Untuk menghasilkan formula keamanan jaringan yang baik maka diperlukan *hardware* yang mumpuni dan dengan sistem operasi khusus untuk server.
4) Metode ini diharapkan dapat dikembangkan lagi sehingga menghasilkan formula atau kombinasi model jaringan yang lebih baik dan lengkap.

6. REFERENSI

[1] Saputro, Saputro, Wijayanto, "*Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer", 3*(2), 22–27, Informatika 2020.

[2] Lestari, Permana, "Analisis Sistem Jaringan Komputer di Sekolah Menengah Kejuruan Al-Madani Pontianak", *International Journal of Natural Science and Engineering*, *2*(3), 99. 2019

[3] Ridho, Arman, "Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan", *Jurnal Sisfokom (Sistem Informasi Dan Komputer)*, *9*(3), 373–379. 2020.

[4] Purba, Efendi, "Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT", *Aiti*, *17*(2), 143–158, 2021.

[5] Anugrah, Rahmanto, "Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone", *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic, 5*(2), 91–106. 2018.

[6] Fitri, Nathasia, Wilman, "*Port Knocking Dan Honeypot", 3*(1), 27–33. 2017.