Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

Sistem Keamanan Server Linux CentOS Dengan Metode Port Knock dan RST Cookies

***Muh. Adrian Juniarta Hidayat[1], Hadian Mandala Putra[2]**
[1]Program Studi Sistem Informasi, Universitas Hamzanwadi
[2] Program Studi Teknik Komputer, Universitas Hamzanwadi
*adrianjh@hamzanwadi.ac.idi

Abstrak

Meningkatnya layanan berbasis online membuat sistem keamanan untuk komputer server menjadi semakin dibutuhkan. Komputer server merupakan perangkat yang harus selalu tersedia untuk diakses kapan saja dan dimana saja. Beberapa sistem keamanan yang diperlukan untuk komputer server diantaranya yakni keamanan untuk akses port ssh untuk kebutuhan akses server secara jarak jauh dan sistem keamanan untuk menjaga server dari serangan Denial of Service(DoS) yang dapat membuat server menjadi down dan tidak dapat diakses sama sekali. Dalam penelitian ini, diusulkan sistem keamanan untuk komputer server dengan sistem operasi Linux CentOS pada sistem akses port 22 Secure Shell (SSH) dengan menggunakan metode port knock dan sistem keamanan untuk mencegah serangan Denial of Service(DoS) pada komputer server dengan metode RST Cookies. Hasil simulasi dari percobaan akses port 22 ssh untuk komputer server dapat berkerja dengan baik dimana port 22 Secure Shell (SSH) akan tetap tertutup dan tidak dapat diakses secara sembarangan kecuali dengan mengakses beberapa port terlebih dahulu sesuai dengan aturan port knocking yang telah ditetapkan. Begitu pula dengan penerapan sistem keamanan dengan metode RST Cookies bekerja dengan sangat baik untuk mencegah serangan Denial of Service(DoS) dan tetap dapat menjaga server untuk dapat diakses dengan waktu respon yang baik di bawah 1 ms.

Kata kunci: Keamanan Server, Linux CentOS, Port Knock, RST Cookies

Abstract

The increase in online-based services makes a security system for server computers increasingly needed. A server computer is a device that must always be available to be accessed anytime and anywhere. Some of the security systems needed for server computers include security for ssh port access for remote server access needs and a security system to protect servers from Denial of Service (DoS) attacks which can make the server down and completely inaccessible. In this study, a security system is proposed for a server computer with the Linux CentOS operating system on a port 22 secure shell(ssh) access system using the port knock method and a security system to prevent Denial of Service (DoS) attacks on server computers using the RST Cookies method. The simulation results from the port 22 Secure Shell (SSH) access experiment for the server computer can work well where port 22 Secure Shell(SSH) will remain closed and cannot be accessed carelessly except by accessing several ports first according to predefined port knocking rules. Likewise, the implementation of a security system with the RST Cookies method works very well to prevent Denial of Service (DoS) attacks and can still keep the server accessible with a good response time of under 1 ms.

Keywords: *Server Security, Linux CentOS, Port Knock, RST Cookies*

1. Pendahuluan

Keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Menurut G. J.

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik [1].

Keamanan teknologi informasi mengacu pada usaha dalam mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan [2]. Salah satu bagian terpenting dari sebuah infrastruktur sistem informasi ialah server. Aspek keamanan menjadi faktor yang penting untuk diperhatikan pada sebuah komputer server dikarenakan berbagai serangan dari luar sering diluncurkan dengan memanfaatkan kelemahan yang ada pada server. Mengamankan komputer server sama pentingnya dengan mengamankan situs web atau aplikasi web itu sendiri dan jaringan sekitarnya. Seperti pada penelitian yang dilakukan oleh Ramli Ahmad dkk yang berjudul "Penggunaan Metode Backpropagation Pada Jaringan Syaraf Tiruan Untuk Intrusion Detection System" [3]. Pada penelitian tersebut, peneliti merancangan sebuah keamanan jaringan untuk *Intrusion Detection System (IDS)* menggunakan metode Backpropagation pada jaringan syaraf tiruan. Dari penelitian tersebut didapat bahwa sistem keamanan tersebut sangat bermanfaat dalam membantu mendeteksi kegiatan abnormal dalam sebuah jaringan yang mana sangat membantu dalam hal keamanan siber. Pembuatan sistem yang melibatkan suatu server terkadang terjadi kelalaian dalam menambahkan sistem keamanan untuk server yang mana hal tersebut dapat menjadi kerugian apabila terjadi tindakan ilegal terhadap komputer server tersebut. Seperti halnya pada penelitian yang dilakukan oleh Suhartini dkk yang berjudul "Implentasi Aplikasi Ujian Online Berbasis Client Server Studi Kasus di SMA Negeri 3 Selong" [4]. Pada penelitian tersebut, tidak diterapkan suatu sistem keamanan server pada sistem yang dibuat, hal ini tentu dapat membuat komputer server menjadi sangat rentan terhadap serangan yang tidak diinginkan. Apabila kita memiliki aplikasi web yang aman dan komputer server yang tidak aman atau sebaliknya, maka hal tersebut masih sangat beresiko pada sistem. Ada beberapa hal yang perlu diperhatikan sebagai landasan dasar mengamankan sebuah komputer server, diantaranya adalah menghapus layanan yang tidak diperlukan, membuat aturan akses server dengan baik, memisahkan pengaturan pengembangan/pengujian/lingkungan produksi, menghapus modul-modul yang tidak terpakai atau tidak sesuai dengan kebutuhan, memasang beberapa *patch* keamanan yang dibutuhkan dan rajin melakukan pemindaian terhadap layanan yang berjalan pada komputer server tersebut untuk memastikan semua layanan berjalan dengan baik dan sesuai kebutuhan [5].

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

Pada penelitian ini, diusulkan untuk membuat suatu sistem kemanan tambahan untuk sebuah komputer server dengan tujuan untuk mengankan port *Secure Shell (SSH)* yang mana port ini merupakan gerbang utama untuk mengakses suatu komputer server. Selain itu sistem keamanan untuk menjaga server tetap stabil dan berjalan dengan baik juga diterapkan sistem pengaman dengan RST Cookies sebagai teknik untuk mencegah terjadinya serangan skala besar yang bertujuan untuk membuat komputer server menjadi *down* atau tidak dapat diakses secara normal..

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Beberapa penelitian terkait yang memiliki hubungan dengan penelitian yang dilakukan sebagai berikut.

- Khadafi S. dkk, "Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada FTP Server Berbasis Linux Ubuntu Server" [6]. Pada penelitian tersebut, peneliti menerapkan firewall dan metode port knocking untuk mengamankan port 21 yaitu port untuk File Transport (FTP). Peneliti menggunakan firewall untuk menutup semua port dan menggunakan port knocking sebagai tahapan otentikasi untuk dapat mengakses layanan FTP.
- Tito Brades, Irwansyah Irwansyah, "Pemanfaatan Metode Port Knocking dan Blocking Untuk Keamanan Jaringan BPKAD Provinsi Sumsel" [7]. Pada penelitian tersebut, peneliti menggunakan metode port knocking untuk mengamankan akses pada beberapa port seperti winbox, telnet dan webfig. Dari hasil penelitian tersebut bahwa metode port knock dapat menjadi pengamanan ekstra untuk terhubung ke router.
- Andik Saputro dkk, "Metode Demilitarized dan Port Knocking Untuk Keamanan Jaringan Komputer" [8]. Pada penelitian tersebut, peneliti menggunakan metode demilitarized dan port knocking untuk membuat sistem keamanan jaringan server. Dari penelitian tersebut didapatkan bahwa teknik demilitaized zone digunakan untuk mengakses server lokal agar dapat diakses dari luar jaringan dan port knocking digunakan untuk lapisan keamanan sebelum pengguna dapat mengakses server tersebut.
- Fachri Fahmi, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing" [9]. Pada penelitian tersebut, peneliti melakukan optimasi pengamanan server dengan melakukan perbaikan konfigurasi pada *File2ban* untuk mencegah peretasan dengan menkonfigurasi ulang beberapa pengaturan

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

pada file tersebut, sehingga celah kerentanan pada server dapat ditutup dengan baik.

- Molavi Arman, Nur Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan PFSense" [10]. Pada penelitian tersebut, peneliti membuat sistem kemanan untuk suatu webserver dengan menerapkan metode PFSense. Peneliti menggunakan bantuan aplikasi snort sebagai tool untuk mengenali serangan dan memberikan alert terhadap serangan yang terjadi juga dapat melakukan pemblokiran secara otomatis.
- Pada penelitian ini, diusulkan untuk menggunakan metode port knock dan RST Cookies sebagai metode pengamanan jaringan server dari akses port Secure Shell (SSH) dan serangan Denial of Service(DoS). Metode port knocking akan digunakan sebagai pengamanan apabila akan mengakses server dari luar jaringan utama. Sedangkan RST Cookies akan digunakan sebagai pengamana server agar tidak down dan tetap dapat diakses meski sedang mengalami serangan DoS

2.2. Landasan Teori

1. Keamanan Teknologi Informasi

Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap beberapa aspek keamanan komputer, di antaranya ialah sebagai berikut :

- *Authentication* : memastikan bahwa informasi benar-benar asli berasal dari pihak yang dikehendaki.
- *Integrity* : memastikan bahwa informasi yang dikirim benar-benar original (tidak dimodifikasi).
- *Confidentiality* : merupakan usaha untuk menjaga kerahasiaan informasi.
- *Availability* : memastikan ketersediaan informasi.

2. Port Knock

Port Knock adalah metode keamanan yang digunakan untuk mengamankan akses ke sistem komputer atau jaringan [11]. Teknik ini menggunakan permintaan koneksi ke port-port tertentu pada tujuan yang ditentukan. Jika urutan yang tepat diikuti, firewall akan membuka port tertentu untuk akses dari alamat IP yang menginisiasi urutan port knocking tersebut. Port knocking berusaha menyembunyikan layanan yang tersedia dan hanya mengizinkan akses ke port-port tertentu jika urutan port knocking yang benar dilakukan. Hal ini dirancang untuk melindungi sistem dari serangan port scanning, di mana penyerang mencoba mengidentifikasi port-port yang terbuka pada sistem target. Berikut

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

adalah langkah-langkah umum dalam port knocking:

- Penyerang harus mengirimkan serangkaian permintaan koneksi ke port-port tertentu pada sistem target dalam urutan yang ditentukan sebelum port yang dituju terbuka.
- Sistem target akan menggunakan firewall atau perangkat lunak khusus untuk memantau permintaan koneksi yang masuk.
- Jika urutan yang tepat dari permintaan koneksi diterima oleh sistem target, firewall akan membuka port tertentu sehingga akses ke layanan diizinkan dari alamat IP yang melakukan port knocking.

3. Denial of Service (DoS)

Denial of Service (DoS) merupakan jenis serangan terhadap sistem dalam jaringan internet dengan cara menghabiskan sumber daya yang dimiliki oleh suatu sistem komputer server sehingga tidak dapat menjalankan fungsinya dengan benar dan secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan sistem yang diserang tersebut [12]. Serangan DoS memanfaatkan kelemahan sistem pada keterbatasan sumber daya, baik bandwidth, kemampuan menyimpan memori, server dan kelemahan lainnya [13]. Dalam serangan DoS penyerang menggunakan satu komputer dan satu koneksi internet saja ketika meluncurkan serangan. Untuk melancarkan serangan yang berskala lebih besar, penyerang bisa menggunakan banyak komputer dan banyak koneksi internet yang dikontrol secara bersamaan dengan menggunakan botnet. Botnet merupakan sejumlah komputer yang terinfeksi malware tanpa disadari oleh penggunanya [14]. Serangan dengan menggunakan banyak komputer disebut dengan istilah *Distributed Denial of Service (DDoS).*

4. RST Cookies

RST Cookies adalah singkatan dari *"Request Security Token Cookies."* Ini adalah metode yang digunakan dalam keamanan layanan aplikasi web untuk melindungi informasi pengguna dan mencegah serangan peretas yang dapat mengambil alih sesi pengguna [15]. RST Cookies bekerja dengan cara menyematkan informasi keamanan tambahan ke dalam cookie yang dikirimkan ke browser pengguna. Cookie ini berisi token keamanan yang unik dan berubah secara dinamis setiap kali pengguna melakukan permintaan ke server. Token ini digunakan oleh server untuk mengotentikasi dan mengotorisasi permintaan pengguna. Dengan menggunakan RST Cookies, aplikasi web dapat memastikan bahwa setiap permintaan yang diterima berasal dari pengguna yang sah dan memiliki hak akses yang sesuai.

2.3. Tahapan Penelitian

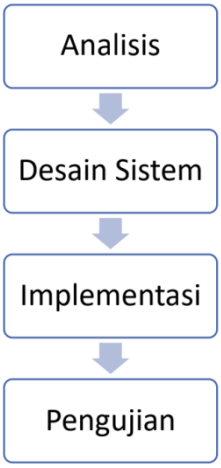
Dalam melaksanakan penelitian ini, ada beberapa tahapan yang akan dilalui. Adapun tahapan

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

penelitian yang akan dilakukan selama proses penelitian adalah sebagai berikut.



Gambar 1. Tahapan penelitian

Gambar 1. menunjukkan tahapan-tahapan yang dilakukan dalam penelitian ini mulai dari analisis kebutuhan penelitian, membuat desain sistem keamanan dan simulasi, implementasi metodologi keamanan dan pengujian dari hasil implementasi metode tersebut.

1. Analisis

   Analisa terbagi menjadi 2 (dua), yaitu analisa sistem dan analisa kebutuhan. Analisis sistem adalah penjabaran dari suatu sistem yang utuh ke berbagai bagian komponennya dengan tujuan agar dapat mengidentifikasi dan mengevaluasi berbagai masalah atau hambatan yang muncul pada sistem sehingga nantinya dapat dilakukan penanggulangan, perbaikan dan pengembangan. Analisis kebutuhan yakni menentukan output atau keluaran yang dihasilkan oleh sistem berdasarkan kebutuhan perangkat lunak (Software) dan kebutuhan perangkat keras (Hardware) dari sistem yang akan dibangun.

2. Desain Sistem

   Desain sistem merupakan tahapan untuk mendefinisikan kebutuhan fungsional, persiapan untuk rancang bangun implementasi, menggambarkan bagaimana suatu sistem dibentuk yang dapat berupa penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi, termasuk menyangkut konfigurasi dari komponen-komponen perangkat lunak dan perangkat keras dari suatu sistem.

3. Implementasi

   Tahap implementasi merupakan tahap penerjemahan desain sistem ke dalam bentuk nyata. Pada tahap inilah wujud sistem yang di buat akan terlihat secara nyata dalam bentuk hasil implementasi konfigurasi sistem keamanan terhadap sebuah komputer server.

4. Pengujian

   Pada tahap proses pengujian merupakan tahap akhir dari penelitian ini di mana sistem yang baru akan diuji bagaimana hasil dari implementasi dari metode keamanan yang diterapkan pada sebuah komputer server

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

3. Metode Penelitian

Pada penelitian ini, metode yang digunakan adalah pendekatan eksperimen atau percobaan langsung dan perbaikan secara langsung untuk melihat kinerja sistem pengamanan server untuk akses root dengan metode port knocking dan sistem pengamanan serangan Denial of Service (DoS) dengan metode RST Cookies pada komputer server dengan sistem operasi linux CentOS versi 7.

3.1. Metode Port Knock

Metode Port Knocking digunakan untuk mengamanakan akses port ssh. Dengan teknik ini, port 22 yang dignakan untuk mengakses root server akan ditutup dan dilindungi mengunakan firewall terlebih dahulu. Port 22 dapat dibuka hanya dengan menggunakan pola port knocking pada beberapa port terlebih dahulu, apabila pola yang digukana benar, maka firewall akan membuka akses ke port tersebut, namun apabila pola yang digunakan salah, maka firewall akan memblokir percobaan akses tersebut.

Jika kita mengonfigurasi port Knocking akses ke port 2, port ini akan terbuka saat kita melakukan request ke port 1000 200 3000 dalam urutan itu, begitu kita menyelesaikan urutannya dengan benar maka firewall akan terbuka. Dengan ini kita menambahkan lagi tingkat keamanan untuk beberapa jenis koneksi ke server kita. Untu mendapatlan akses ke port 22, maka klien/sysadmin dapat melakukan pengetikan port menggunakan Nmap, Telnet, atau alat untuk keperluan ini.

```
[options]
        logfile = /var/log/knockd.log

[openSSH]
        sequence = 5040,6010,6500
        seq_timeout = 30
        tcpflags = syn
        Start_command = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 22 -j ACCEPT

[closeSSH]
        sequence = 4040,5050,8080
        seq_timeout = 30
        command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
        tcpflags = syn
```

Gambar 2. merupakan konfigurasi aturan untuk metode port knocking. Pada konfigurasi tersebut sudah di tambahkan rule untuk port berapa saja yang harus di akses terlebih dahulu sebelum mengakses port ssh 22. Pola yang digunakan untuk membuka akses ialah port 5040, 6010, 6500 dan pola yang digunakan untuk menutup akses ialah port 4040, 5050, 8080.

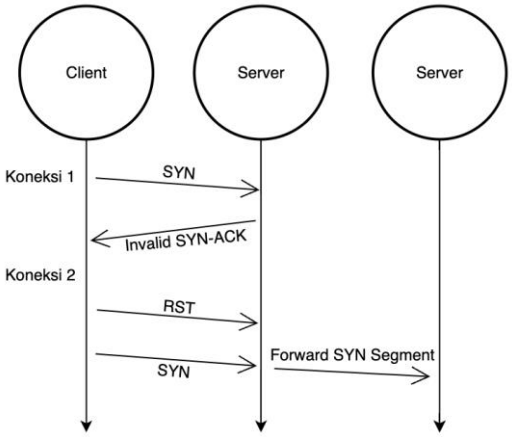
3.2. Metode RST Cookies

Pada bagian keamanan server untuk mengantisipasi serangan DoS, diterapkan metode pengamanan RST Cookies. RST cookies adlah salah satu metode pengamanan yang untuk serangan DoS dimana server mengirim ACK + SYN yang tidak valid dan klien akan melakukan forward untuk memberitahu server bahwa ada error. Adapun bagan kerja metode ini seperti gambar berikut.

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500



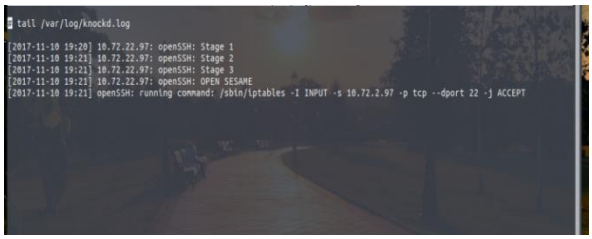
Gambar 3. Alur kerja RST Cookies

Pada Gambar 3. menunjukkan bagaimana sistem kerja RST Cookies dalam mengamankan server. Pada ilustrasi tersebut terlihat server dengan sengaja mengirimkan SYN-ACK yang tidak valid sebagai tanggapan atas koneksi utama dari klien tertentu. Hal ini akan mengakibatkan klien membuat parsel RST, memberi isyarat bahwa ada sesuatu yang tidak beres dari permintaan koneksi tersebut. Jika koneksi ini diterima, server tersebut mengakui bahwa permintaan itu asli kemudia mencatat klien, dan menerima asosiasi koneksi dengan klien tersebut

4. Hasil dan Pembahasan

4.1. Percobaan Akses Root Server

Pada percobaan akses root server pada port ssh dilakukan dengan memanggil susunan port yang telah ditetapkan pada aturan keamanan yang telah dibuat. Adapun respon dari server dalam menyimpan log percobaan akses port ssh remote server terlihat sebagai berikut.



Gambar 4. Log file akses server secara remote dengan metode port knocking

Pada Gambar 4. menunjukkan log percobaan akses yang tersimpan pada server. Pada file log tersebut terlihat bagaimana server merespon untuk membuka akses port ssh kedalam server saat dicoba akses secara jarak jauh. Dengan menerapkan metode port knocking ini dapat menjadi sistem pengaman untuk membuat server tetap menutp port 22 ssh agar tidak dapat diakses secara sembarangan oleh pihak lain. Server hanya akan membuka akses ke port ssh apabila proses knocking port dengan urutan yang telah ditentukan dilakukan dengan benar.

4.2. Percobaan Serangan Denial of Service(DoS)

Pada percobaan serangan *Denial of Service(DoS)* digunakan parameter percobaan sebagai berikut.

Tabel 1. Parameter serangan DoS

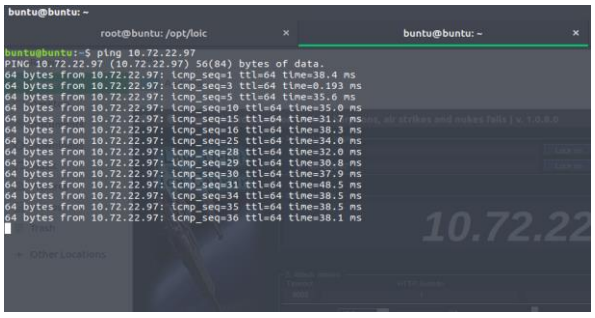
Parameter percobaan DoS	
Port	80
Protocol	TCP
Jumlah Thread	1.000.000

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

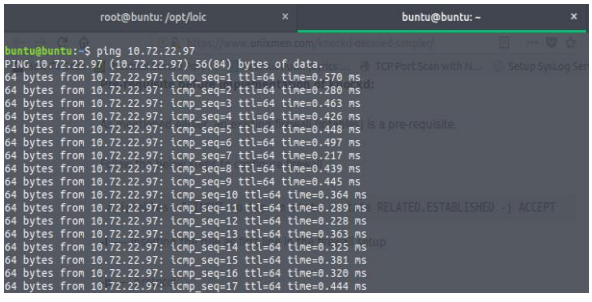
DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

Pada Tabel 1. menunjukkan parameter yang digunakan dalam melakukan simulasi serangan *Denial of Service(DoS)* pada server yang telah di terapkan keamanan dengan metode RST Cookie. Percobaan serangan akan dilakukan pada protokol TCP pada port http dengan jumlah thread yang dikirimkan sebanyak 1 juta thread. Adapun hasil percobaan ditunjukkan sebagai berikut.



Gambar 5. Respon server ketika dilakukan serangan sebelum pengamanan

Pada Gambar 5. menunjukkan bagaimana respon server ketika coba diakses dengan kondisi server sedang menerima serangan *Denial of Service(DoS)*. Server memberikan waktu respon yang rata-rata di atas 30 ms. Adapun respon server ketika diakses setelah diterapkan metode pengamanan RST Cookies adalah sebagai berikut.



Gambar 6. Respon server ketika dilakukan serangan setelah pengamanan

Pada Gambar 6. menunjukkan bagaimana respon server ketika coba diakses dengan kondisi server sedang menerima serangan *Denial of Service(DoS)*. Server dapat memerikan respon yang cepat dan stabil dengan waktu respon di bawah 1 ms. Dengan menerapkan metode pengamanan RST Cookies untuk mencegah serangan *Denial of Service(DoS)* pada server terlihat bahwa metode pengamanan ini dapat bekerja dengan sangat baik dengan menjaga sumber daya tetap aman dan server tetap dapat memerikan respon yang cepat pada setiap permintaan yang masuk. Terlihat cukup berbeda signifikan waktu respon server apabila tidak diterapkan sistem pengaman dimana waktu respon server di atas 30 ms saat dilakukan serangan *Denial of Service(DoS)*

5. Kesimpulan

Berdasarkan hasil perancangan dan implementasi sistem keamanan pada server dengan sistem operasi Linux CentOS versi 7 didapatkan hasil bahwa, penerapan metode port knock untuk mengamankan port 22 *Secure Shell (SSH)* dapat berkerja dengan sangat baik. Server akan menutup akses pada port 22 terlebih dahulu agar tidak dapat diakses secara ilegal oleh sembarangan orang dari jarak jauh. Komputer server kemudian akan membuka port 22 apabila pengguna yang mencoba mengakses port tersebut melakukan akses beberapa port dengan

Infotek : Jurnal Informatika dan Teknologi
Vol. 6 No. 2, Juli 2023
Hal.411-420

e-ISSN 2614-8773

DOI : 10.29408/jit.v6i2.17500 Link : https://dx.doi.org/10.29408/jit.v6i2.17500

urutan tertentu terlebih dahulu sesuai dengan aturan urutan yang telah ditetapkan dalam konfigurasi port knocking Begitu pula dengan penerapan metode RST Cookies untuk sistem keamanan server guna mencegah server down ketika terjadi serangan skala besar *Denial of Service(DoS)* pada server. Dengan menerapkan metode RST Cookies, server tetap dapat bekerja dengan sangat baik membuat server tetap stabil dan tetap dapat diakses walaupun terjadi percobaan serangan skala besar yang bertujuan untuk menghabiskan sumber daya server

6. Daftar Pustaka

[1] G.J Simson, dan gene Spafford, Practical UNIX & Internet Security, O'Reilly & Associates, Inc,2nd edition, 1996.
[2] William Stallings, Network and Internetwork Security, Prentice Hall, 1995.
[3] Ramli Ahmad, Bq Andriska Candra, Amri Muliawan Nur, "Penggunaan Metode Backpropagation Pada Jaringan Syaraf Tiruan Untuk Intrusion Detection System", Infotek : Jurnal Informatika dan Teknologi, Vol. 3 No. 2, Juli 2020.
[4] Suhartini, dkk, "Implentasi Aplikasi Ujian Online Berbasis Client Server Studi Kasus di SMA Negeri 3 Selong", Infotek : Jurnal Informatika dan Teknologi, Vol. 5 No. 1, Januari 2022.
[5] Budi Rahardjo, Keamanan Sistem Informasi: Keamanan di Internet, Seminar Informasi Infrastruktur Nasional, ITB, 1997.
[6] Khadafi S. dkk, "Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada FTP Server Berbasis Linux Ubuntu Server", Jurnal Ilmiah Nero, Vol. 4 No. 3, 2019.
[7] Brades T. dkk, "Prmanfaatan Metode Port Knocking dan Blocking Untuk Keamanan Jaringan BPKAD Provinsi Sumsel", Artikel Ilmu Komputer, Vol. 3 No. 2, 2022.
[8] A, Saputro dkk, "Metode Demilitarized dan Port Knocking Untuk Keamanan Jaringan Komputer", CyberSecurity dan Forensik Digital, Vol. 3, No. 2, h. 22-27, 2020.
[9] Fahmi Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing", Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), Vol. 10, No. 1, Februari 2023.
[10] Molavi Arman, Nur Rachmat, "Implementasi Sistem Keamanan Web Server Menggunakan PFSense", Jusikom : Jurnal Sistem Komputer Musirawas, Vol 05 No 01 Juni 2020.
[11] Edy Haryanto, Widyawan, Dani Adhipta, "Meningkatkan Keamanan Port Knocking Dengan Kombinasi Special Features ICMP, Source Port, dan Tunneling", Seminar Riset Teknologi Informasi (SRITI), 2016.
[12] P. Ferguson and D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IPSource Address Spoofing. RFC 2827 (Best Current Practice), May 2000.
[13] Jonathan Lemon et al. Resisting SYN Flood DoS Attackswith a SYN Cache. BSDCon, 2002.
[14] XiaoFeng Wang and Michael K Reiter. Defending against denial-of-service attacks with puzzle auctions. In Security and Privacy. IEEE, 2003
[15] W. Eddy. TCP SYN Flooding Attacks and Common Mitigations. RFC 4987 (Informational), August 2007