Implementasi Sistem Keamanan Jaringan Komputer Dengan *Iptables* Sebagai *Firewall* Menggunakan Metode *Port Knocking*

Muhammad Surya Kadafi[1], Mursyidah[2*], Amri[3]

[1,2,3] *Jurusan Tekniknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]kkadafi385@gmail.com
[2*]mursyidah@pnl.ac.id
[3]amri@pnl.ac.id

Abstrak*—Sangat penting untuk memperhatikan keamanan jaringan komputer. *Iptables* berfungsi sebagai *firewall* pada sistem keamanan jaringan yang dapat mengatur dan mengontrol lalu lintas data yang diizinkan untuk mengakses data server. Metode *port knocking* melakukan akses *SSH* server dengan tiga ketukan port yaitu 3000, 4000, 5000. Hal ini dapat memberi lapisan keamanan pada server untuk menghalangi akses dari serangan luar. Pada hasil penelitian ini attacker mengakses server dengan melakukan tiga serangan berupa *port scanning, brute force dan DDoS Attack*. Pada port scanning ada 2 port yang terbuka dan 3 port yang tertutup. Pada pengujian serangan brute force mendapatkan kombinasi nama pengguna dan sandi yang cocok, yang dapat membuka akses server. Pada pengujian *DDoS*, Berhasil mengirimkan *UDP* flood, *ICMP* flood dan *TCP* flood terdapat paket yang ditangkap pada log system berukuran 74 byte, 8 byte, dan 512 byte. Dampak dari serangan *DDoS* dapat menyebabkan kinerja server menurun akibat data yang masuk terus menerus dalam waktu singkat. Hal ini dapat berbahaya jika membiarkan port penting terbuka akan menjadi masalah yang dapat mengakibatkan serangan terhadap server. Port merupakan pintu masuk dan keluar dari jaringan komputer, maka perlu adanya *firewall* agar kerentanan jaringan dapat dibatasi, dengan menutup port dari serangan attacker. Oleh karena itu, penelitian ini dilakukan dengan menggunakan metode *port knocking* dan *Iptables* untuk mengontrol lalu lintas jaringan masuk dan keluar, *Iptables* akan membatasi akses serangan dari luar. Penelitian ini menunjukkan perlu adanya perlindungan informasi port pada server dengan menutup semua informasi port yang terbuka dari attacker, sehingga kerentanan pada jaringan dapat diminimalisir.

Kata kunci— Keamanan Jaringan Komputer, *Firewall, IPTables, Port Knocking.*

Abstract—It is very important to pay attention to computer network security. Iptables functions as a firewall in a network security system that can regulate and control data traffic that is permitted to access server data. The port knocking method accesses the SSH server with three port knocks, namely 3000, 4000, 5000. This can provide a layer of security on the server to block access from outside attacks. In the results of this research, the attacker accessed the server by carrying out three attacks in the form of port scanning, brute force and DDoS attack. In port scanning there are 2 open ports and 3 closed ports. In testing, brute force attacks obtain a matching username and password combination, which can open server access. In the DDoS test, successfully sending UDP flood, ICMP flood and TCP flood, there were packets captured in the system log measuring 74 bytes, 8 bytes and 512 bytes. The impact of a DDoS attack can cause server performance to decrease due to continuous incoming data in a short time. This can be dangerous if leaving important ports open will become a problem that could result in an attack on the server. Ports are the entry and exit points for a computer network, so there is a need for a firewall so that network vulnerabilities can be limited, by closing the ports from attacks by attackers. Therefore, this research was carried out using the port knocking method and Iptables to control incoming and outgoing network traffic, Iptables will limit access to attacks from outside. This research shows the need to protect port information on servers by closing all open port information from attackers, so that network vulnerabilities can be minimized.

Keywords— *Computer Network Security, Firewall, Iptables, Port Knocking.*

I. Pendahuluan

Keamanan jaringan komputer sangat penting untuk menjaga kerahasiaan data dan informasi pada server. Perkembangan teknologi yang terus berkembang pada jaman sekarang, yang akan membawa dampak positif dan risiko pada keamanan informasi. Meskipun banyak memberi dampak yang positif dalam mendapatkan dan menyediakan informasi. Namun dampak negatif juga dapat menjadi ancaman, pencurian, dan perusakan data yang dilakukan oleh penyerang pada sebuah computer [1].

Berdasarkan jurnal yang telah diteliti sebelumnya yang membahas tentang metode sederhana pada *Port Knocking* menggunakan model random. Dalam penelitian tersebut menjelaskan bahwa meskipun *Port Knocking* merupakan metode yang mudah digunakan untuk meningkatkan keamanan jaringan, Namun metode ini masih memiliki kerentanan terhadap serangan menggunakan *TCP Replay* dan *Port Scaning*. Pada penelitian tersebut mengusulkan pendekatan baru atas *Port Knocking* yang menggunakan urutan Port Sumber yang akan digunakan untuk menyederhanakan teknik untuk port sistem *Knocking*. Port sumber secara otomatis dihasilkan oleh sistem operasi dan

telah ditetapkan sebelumnya untuk menghasilkan urutan. Port sumber sendiri adalah nomor port yang digunakan oleh komputer pengirim untuk mengirimkan paket data melalui jaringan. Suatu teknik untuk mengontrol mulai dan berhentinya layanan tertentu mulai dan berhenti untuk mengurangi masalah terhadap serangan ulangan *TCP* dan pemindaian port [2].

Masalah yang akan diselesaikan nantinya menggunakan metode *port knocking* untuk mengamankan layanan pada server. Dengan mengurutkan *port knocking* yang telah ditentukan dan di identifikasi apakah permintaan tersebut merupakan permintaan sah atau tidak untuk server. Cara kerja port knoking dengan mengurutkan beberapa port, dan hanya user tertentu yang dapat mengakses sebuah port yang telah ditentukan, dengan cara mengetuk port terlebih dahulu, cara kerja *Firewall* adalah menutup semua akses serangan dari luar sehingga dapat mengurangi kerentanan terhadap serangan *port scanning, brute force* dan *DDoS*.

A. Keamanan Jaringan

Keamanan jaringan komputer harus menjadi perhatian utama ketika membangun sebuah infrastruktur jaringan. Penggunaan router dengan sistem *firewall* terintegrasi dan dukungan *software* jaringan adalah langkah penting yang dapat membantu mencegah serangan dari luar dan memperkuat keamanan jaringan. Router dengan sistem *firewall* terintegrasi dapat membantu memblokir akses yang tidak diinginkan ke jaringan, sedangkan *software* jaringan seperti *intrusion detection system (IDS)* dan *intrusion prevention system (IPS)* dapat membantu memantau lalu lintas jaringan dan mendeteksi serangan potensial [3].

B. Jaringan komputer

Jaringan komputer merupakan sekumpulan atau kelompok dari beberapa komputer yang saling terhubung satu sama lain dengan menggunakan protokol komunikasi yang telah ditetapkan. Dengan jaringan komputer, pengguna dapat saling berbagi data, aplikasi, dan perangkat keras sehingga dapat meningkatkan efisiensi dan produktivitas kerja. Media komunikasi yang dapat digunakan untuk jaringan komputer antara lain kabel *LAN, wireless,* dan *fiber optic.* Jaringan komputer dapat dibagi menjadi beberapa jenis, seperti jaringan lokal *(Local Area Network/LAN),* jaringan metropolitan *(Metropolitan Area Network/MAN),* dan jaringan luas *(Wide Area Network/WAN).* Selain itu, ada juga jaringan komputer yang dibangun untuk tujuan khusus, seperti jaringan sensor, jaringan industri, dan jaringan nirkabel [3].

C. *Iptables*

Iptables merupakan suatu *firewall* bawaan dari linux yang berfungsi untuk menganalisis dan menyaring paket data yang masuk kedalam *firewall*, apakah paket data tersebut akan di-drop (membiarkan paket tersebut seolah-olah tidak pernah diterima), di-*accept* (menerima paket tersebut untuk diproses lebih lanjut), atau di *reject* (menolak dan memberitahu pengirim bahwa paket data tidak bisa diterima). *Iptables* juga sebagai alat untuk menyaring paket-paket yang masuk, keluar dan sedang berlalu lintas didalam *Firewall* melalui server. Indikator yang digunakan dalam *iptables firewall* adalah *Packet filtering, Accounting, Connection tracking, Packet mangling, Network address translation (NAT), Masquerading, Port Forwarding* dan *Loadbalancing* [4].

D. *Firewall*

Firewall adalah pembatas akses terhadap jaringan yang diproteksi agar terhubung ke internet, atau kumpulan-kumpulan jaringan lainnya. Tujuannya adalah untuk meminimalkan risiko serangan dari luar dan melindungi jaringan dari ancaman keamanan seperti virus, *malware, hacker,* dan serangan *DDoS. Firewall* berfungsi sebagai filter yang memeriksa semua lalu lintas jaringan yang masuk dan keluar dari jaringan yang diproteksi. Dengan mengkonfigurasi *firewall* dengan tepat, administrator jaringan dapat mengatur aturan untuk membatasi akses ke jaringan dari luar dan membatasi akses dari jaringan internal ke internet atau ke jaringan lain yang diproteksi [5].

E. *Port knocking*

Port knocking adalah metode keamanan yang digunakan untuk mengamankan jaringan dan sistem dari serangan luar dengan mengizinkan koneksi hanya melalui port-port tertentu yang sudah diatur sebelumnya. Metode ini memungkinkan koneksi masuk ke dalam sistem hanya setelah pengguna melakukan urutan *knocking* pada port yang telah ditentukan sebelumnya [6].

F. *Port Scanning*

Port Scanning adalah tahapan awal untuk mendeteksi port-port yang terbuka dan mendapatkan informasi dari port yang terbuka pada *host,* versi server dan sebagainya. Serangan terhadap jaringan yang berawal dari port scanning tidak dapat dihindari, karena *port mapping* atau *port scanning* sering teridentifikasi sebagai lalu-lintas rutin pada sebuah jaringan, *DPI (Deep Packet Inspection)* berfungsi sebagai inspector yang dapat digunakan pada setiap lapisan (layer) pada komponen jaringan, sehingga dimungkinkan untuk melakukan analisa dan inspeksi lebih mendalam terhadap trafik data. Proses inspeksi data dalam keadaan Real-time lebih akurat daripada dalam keadaan offline [7].

G. *Brute Force Attack*

Brute force adalah teknik serangan atau tindakan *hacker* secara paksa pada sistem keamanan web dengan menggunakan percobaan menebak *username* dan *password.* Peretas menggunakan serangan *brute force* untuk mendapatkan kerentanan kode dan halaman web tersembunyi yang dapat dieksploitasi, setelah teridentifikasi penyerang menggunakan informasi itu untuk menyusup kedalam sistem dan membahayakan data, tujuan akhir mereka adalah menyebabkan beberapa penolakan layanan pada halaman web dan mengeluarkan data dari system untuk ditujukan ke pihak ketiga [8].

H. *DDoS Attack*

Distributed denial-of-service (DDoS) disebut sebagai senjata pilihan hacker karena telah terbukti menjadi ancaman permanen bagi pengguna, organisasi dan infrastruktur di Internet. Di sisi lain, serangan jaringan merupakan risiko untuk integritas, kerahasiaan dan ketersediaan sumber daya yang disediakan oleh organisasi. Deteksi dini serangan *DDoS* adalah proses fundamental yang dilakukan secara otomatis oleh *Intrusion Detection System (IDS)*. *IDS* yang ada sekarang ini pada umumnya menggunakan teknik deteksi yang jauh dari sempurna jika dibandingkan dengan teknik serangan cyber yang semakin modern. Sistem *IDS* pada umumnya hanya memantau dan memberikan penanda terhadap aktivitas jaringan yang mencurigakan dan langsung dilaporkan sebagai alert, sehingga memberikan dampak adanya volume alert yang terlalu besar dengan tingkat rata-rata *false-positive* yang tinggi. Hal itu disebabkan karena lalu lintas data jaringan merupakan sesuatu yang bersifat *non-stasioner* [9].

II. Metodologi Penelitian

A. Data

Pada bagian ini peneliti menggunakan data sekunder. Yaitu data yang diperoleh dari hasil penelitian sebelumnya.

B. Pengumpulan Data

Pada penelitian ini penulis menggunakan beberapa tahap dan metode dalam menyusun proposal skripsi, yaitu:

1. Observasi langsung: Penulis melakukan observasi langsung terhadap jaringan yang akan diuji dengan menggunakan metode *port knocking*. Observasi ini dilakukan untuk memperoleh data seperti ketukan port yang benar agar bisa terkoneksi ke server, topologi jaringan dan jenis perangkat jaringan yang digunakan.
2. Pengumpulan data sekunder: Pengumpulan data juga dilakukan dengan meninjau sumber data sekunder seperti jurnal penelitian dan artikel terpercaya, terkait dengan masalah yang akan diuji.

C. Spesifikasi *Software* dan *Hardware*

Untuk memudahkan penulis dalam penelitian ini ada beberapa spesifikasi yang digunakan berupa spesifikasi *software* dan spesifikasi *hardware.*

Berikut ini adalah spesifikasi *software:*

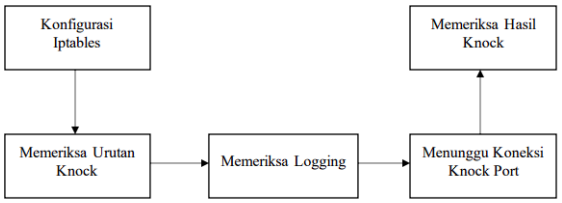
a) Virtual Box: Perangkat lunak virtualisasi untuk menjalankan beberapa sistem operasi di satu perangkat keras.
b) Linux Ubuntu: Untuk menjalankan berbagai layanan dan aplikasi di server.
c) Kali Linux: Untuk melakukan serangan terhadap layanan server meakukan pengujian serangan pada server.
d) *LOIC (Low Orbit Ion Cannon):* Digunakan untuk melakukan serangan terhadap layanan server dan membanjiri server target dengan lalu lintas yang tinggi.
e) Wireshark: Untuk memantau dan merekam lalu lintas jaringan yang masuk dalam bentuk paket data.

Berikut ini adalah spesifikasi *Hardware:*

a) Processor AMD Athlon
b) RAM 8
c) SSD 295 GB

D. Rancangan Blok Diagram

Gambar 1 merupakan blok diagram *Iptables* untuk memonitoring *port knocking* pada port *SSH* server: Ada beberapa langkah-langkah yang akan dilakukan untuk menyelesaikan masalah pada penyusunan penelitian ini. Kerangka kerja *(frame work)* Dapat dilihat pada gambar berikut.



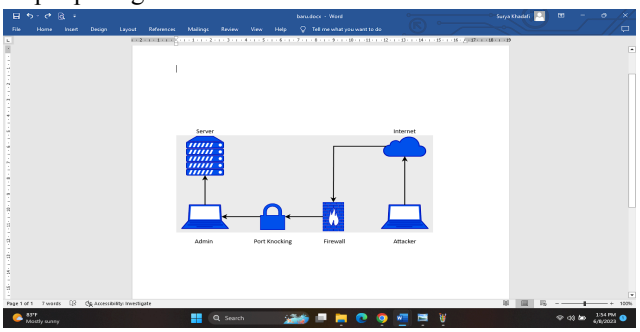
Gambar 1. Rancangan Blok Diagram

Gambar 1 rancangan blok diagram Iptables dapat di jelaskan sebagai berikut.

a) Mengkonfigurasi *iptables* dengan aturan untuk menolak semua koneksi ke port *SSH* yang masuk.
b) Membuat pengaturan *iptables* untuk memeriksa apakah urutan knocking dilakukan dengan benar atau tidak. Jika dilakukan knocking dengan benar maka port *SSH* akan terbuka, Jika tidak maka port akan di tutup.
c) Memeriksa *(logging)* untuk merekam aktivitas akses yang mencurigakan pada jaringan server.
d) Menunggu hingga klien mengetuk urutan port yang benar. Ketika knocking dilakukan dengan benar, aturan *iptables* akan mengizinkan koneksi ke port *SSH*. Jika ketukan port salah maka aturan *iptables* akan menutup akses ke port *SSH.*
e) Memeriksa hasil knock yang dilakukan oleh klien *log* untuk melihat apakah knocking dilakukan dengan benar atau tidak.

E. Topologi Jaringan

Rancangan topologi untuk implementasi *port knocking* terdapat pada gambar 3.



Gambar 2 Topologi jaringan

Berdasarkan gambar 2 Topologi jaringan dapat di jelaskan sebagai berikut:

a) Klient melakukan serangan pada server dengan menginputkan knock pada Port terlebih dahulu.
b) *Firewall* akan mengontrol aliran akses di lingkungan jaringan dan bertujuan untuk memungkinkan konektivitas terkontrol antara klien dan server.
c) *Port knocking* metode yang digunakan untuk mengamankan jaringan dan sistem dari serangan luar dengan mengizinkan koneksi hanya melalui port port yang telah ditentukan dan telah dikonfigurasi sebelumnya.
d) Admin bertanggung jawab untuk menginstal dan mengkonfigurasi sistem operasi, perangkat lunak, dan aplikasi yang diperlukan di server. dan memastikan semua komponen sistem berjalan dengan benar dan terhubung dengan baik.
e) Server berperan dalam mengautentikasi pengguna. Dan mengelola basis data pengguna, izin akses, serta mengautentikasi penyerang saat mencoba mengakses sumber daya sistem yang terdeteksi.

F. Metode penelitian

Metode yang digunakan pada port knocking adalah teknik keamanan jaringan yang memerlukan serangkaian koneksi ke port yang ditentukan sebelum akses ke jaringan atau server. Cara kerja dari metode port knocking dapat dijelaskan seperti berikut.

a) Membuat koneksi ke serangkaian port yang telah ditentukan sebelumnya oleh server.
b) Melakukan urutan koneksi yang telah ditentukan. Urutan tersebut biasanya hanya diketahui oleh pengguna yang telah diberikan akses oleh server.
c) Mengidentifikasi pengguna setelah urutan koneksi yang benar dilakukan, Maka server akan mengidentifikasi terhadap penyerang dengan adanya pemberitahuan pada *logging* server.
d) Membatasi akses masuk pada *SSH* server, sehingga penyerang tidak dapat mengakses port *SSH* server untuk mencegah akses yang tidak sah.

G. Teknik Pengujian

Pada penelitian ini menggunakan Teknik pengujian ketukan *(Knock)* yang digunakan untuk mengamankan akses ke jaringan atau sistem komputer. Teknik ketukan *(Knock)* ini akan memberi tiga lapisan untuk mengakses server. Sehingga server dapat memberikan akses terhadap ketukan port tersebut.

Kemudian membuat batasan akses untuk memblokir terhadap serangan attacker, Attacker akan mencoba melakukan *scanning port* agar celah kerentanan dapat diakses kemudian menyerang keamanan server dengan mengirim serangan kombinasi kata sandi secara berulang-ulang dan menebak kata sandi dan mengirim fake traffic atau lalu lintas palsu yang membuat kinerja server menurun

III. Hasil dan Pembahasan

A. Pengujian *Port Knocking* pada server

Hasil implementasi metode *port knocking* untuk akses *SSH* dengan urutan knocking port 3000, 4000, dan 5000. Metode ini bertujuan untuk meningkatkan keamanan akses ke layanan *SSH* dengan memerlukan urutan knocking port yang benar sebelum akses *SSH* dapat diberikan.

Terdapat empat tahap dalam proses knocking sebelum akses *SSH* diberikan dengan pesan *"OPEN SESAME."* Setiap tahap mewakili koneksi yang dikirim ke alamat IP 192.168.137.3 dengan urutan port 3000, 4000, 5000. Ini merupakan bentuk untuk mengamankan layanan *SSH* dengan menambahkan lapisan keamanan tambahan melalui penggunaan *port knocking.*

Pada gambar 3 dapat dijelaskan bahwa 192.168.137.3 (IP address attacker) telah diizinkan masuk pada ssh server.

```
root@davi-VirtualBox:/home/davi# ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       192.168.137.3

root@davi-VirtualBox:/home/davi#
```

Gambar 3. Akses knock diterima

B. Membatasi akses pada *SSH* server

Untuk membatasi akses server terhadap serangan untuk mengantisipasi kerentanan keamanan pada sistem jaringan, perlu adanya *firewall* untuk menutup kembali hak akses dengan melakukan enable pada *firewall* agar attacker tidak dapat melakukan akses kembali, karena akses telah diblokir terhadap serangan attacker.

Pada gambar 4 dapat dilihat pada keterangan *(UFW BLOCK)* yaitu firewall telah memblokir 192.168.137.3 (IP address attacker) terhadap 192.168.137.2 (IP address server).

```
Aug  3 00:25:39 davi-VirtualBox kernel: [22130.881138] [UFW BLOCK] IN=enp0s3 OUT= MAC=08:00:27:75:02:b0:08:00:27:b1:86:f1:08:00 SRC=
192.168.137.3 DST=192.168.137.2 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15670 DF PROTO=TCP SPT=60548 DPT=22 WINDOW=64240 RES=0x00 SYN UR
GP=0
```

Gambar 4. Koneksi *firewall* diaktifkan

C. Pengujian *Port Scanning*

Pada pengujian *port scanning* attacker akan melakukan *scanning* terhadap port-port yang ada pada suatu perangkat atau jaringan komputer untuk menentukan status dan ketersediaan akses port tersebut. Pengujian ini dilakukan untuk mendapatkan informasi mengenai port-port apa saja yang terbuka pada server.

Ada 2 port yang tetutup dan 3 port yang terbuka dapat dilihat pada table II.

TABEL II
HASIL *SCANNING PORT*

No	Port	State	Service
1	21/tcp	Close	ftp
2	22/tcp	Open	ssh
3	23/tcp	Close	telnet
4	25/tcp	Close	smpt
5	80/tcp	Open	http

Pada tabel II dapat dijelaskan bahwa attacker mencoba menghubungi berbagai port diantaranya port 21,22,23,25,80. Ada dua port yang terbuka yaitu port *SSH* dan *HTTP* dan tiga port yang tertutup yaitu *FTP TELNET SMTP,* attacker melakukan serangan brute force dan DDoS melalui port *SSH* dan *HTTP.*

D. Pengujian *Brute Force Attack*

Pengujian serangan akan dilakukan oleh attacker dengan ip address attacker (192.168.137.3). Saat melakukan *brute force attack,* attacker akan mencoba beberapa nama pengguna dan kata sandi, Kemudian menguji berbagai kombinasi nama dan kata sandi tersebut hingga menemukan informasi login yang benar. Serangan *brute force* bisa memakan lebih banyak waktu jika nama pengguna dan kata sandi yang akan diretas memiliki jumlah karakter yang banyak.

Dapat dilihat pada gambar 5. menunjukkan attacker telah melakukan serangan kombinasi nama pengguna dan kata sandi, sehingga menemukan kecocokan nama pengguna dan kata sandi yang tepat untuk masuk ke dalam server.

Gambar 5. Attacker (192.168.137.3) berhasil masuk ke dalam server

Pada gambar 5 terlihat port 22 *SSH* telah terbuka dan attacker telah berhasil menemukan kecocokan kombinasi nama pengguna dan kata sandi yang benar. Dapat dilihat nama pengguna dan kata sandi yang cocok pada tabel III.

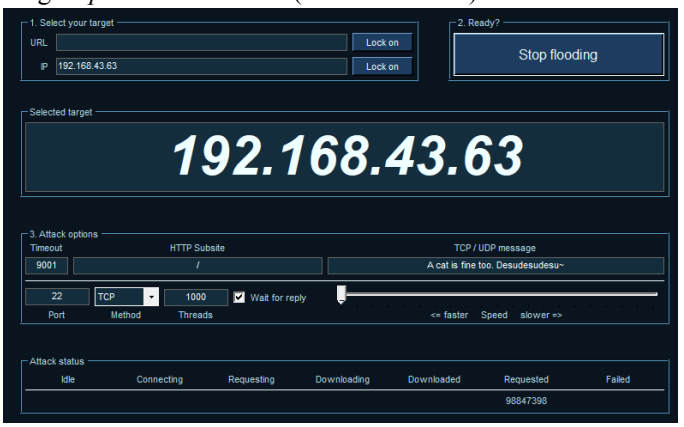
TABEL III
HASIL KECOCOKAN NAMA PENGGUNA DAN KATA SANDI

No	Nama Pengguna	Kata Sandi	Kecocokan
1	root	root	Tidak Cocok
2	admin	admin	Tidak Cocok
3	user	admin123	Tidak Cocok
4	webserver	12345	Tidak Cocok
5	server	password	Tidak Cocok
6	surya	12345678	Tidak Cocok
7	pass	pass12345678910	Tidak Cocok
8	web	password123	Tidak Cocok
9	superadmin	user	Tidak Cocok
10	sys	sys	Tidak Cocok
11	system	system	Tidak Cocok
12	davi	211200	Cocok
13	systemadmin	system123	Tidak Cocok
14	mail	guest	Tidak Cocok
15	mailadmin	security	Tidak Cocok
16	msfadmin	ftp12345678	Tidak Cocok
17	mysql	pass	Tidak Cocok
18	public	Ubuntu1234	Tidak Cocok

Berdasarkan tabel III hasil kecocokan nama pengguna dan kata sandi yang benar terdapat pada urutan ke dua belas dengan nama pengguna: (davi) dan kata sandi: (211200).

E. Pengujian *DDoS (Distributed Denial of Service)*

Pada gambar 6 attacker melakukan serangan *DDoS* pada server dengan mengirimkan *TCP flood*, yang bertujuan untuk membanjiri server target dengan banyak lalu lintas *TCP* palsu, dengan *ip address attacker* (192.168.43.100).



Gambar 6. Attacker melakukan serangan *TCP flood* menggunakan *LOIC*

Dalam serangan *TCP flood*, attacker mengirimkan datagram *TCP* palsu ke server dalam waktu singkat, *log system* menerima paket data yang masuk dari serangan *TCP flood.* Hasil tangkapan paket yang masuk pada *log system* dari serangan *TCP flood* dapat dilihat pada gambar 7

Gambar 7. Serangan *TCP flood* yang masuk pada *log system*

Hasil tangkapan paket *TCP flood* yang diterima oleh server. Dapat dilihat pada tabel IV.

TABEL IV
HASIL SERANGAN *TCP FLOOD* YANG DITERIMA OLEH SERVER.

No	IP Attacker	IP Server	Protokol	Paket yang Masuk
1	192.168.43.100	192.168.43.63	TCP	1694453851.4852

Berdasarkan tabel IV dapat dijelaskan bahwa paket yang ditangkap pada *log system* terdapat (1694453851.4852) paket yang masuk. Serangan *TCP flood* yang dilakukan oleh attacker menyebabkan kinerja sistem server menurun akibat paket yang masuk terus menerus dengan waktu yang singkat.

IV. Kesimpulan

Berdasarkan hasil penelitian ini penulis dapat mengambil kesimpulan bahwa hasil dari tiga ketukan port yaitu 3000, 4000, 5000 dapat membuka akses ke server, ini dapat memberi lapisan keamanan bagi server untuk menghalangi akses dari serangan luar. Hasil pengujian secara virtual menunjukkan bahwa ada 2 port yang tetutup dan 3 port yang terbuka, Port terbuka yaitu layanan *SSH* dan *HTTP,* attacker melakukan serangan terhadap port tersebut, dengan mengirimkan serangkaian kombinasi nama pengguna dan kata sandi yang cocok, yang dapat membuka akses ke server melalui *SSH* server. Hasil pengujian serangan *DDoS* terdapat paket yang ditangkap pada wireshark berukuran 74 *byte* dan panjang paket 32 *byte* dengan port sumber 63665 yang menuju ke port 80 yaitu *HTTP* yang menyebabkan kinerja server menurun akibat data yang masuk terus menerus dalam waktu singkat. Kemudian serangan dari Attacker 2 berhasil mengirimkan *ICMP flood,* hasil yang ditangkap pada log system terdapat *Request id* sebanyak 60163, dengan urutan paket yaitu 3931, 4187, 4443, 4699, 4955, 5211, 5467, 5723 dan ukuran total paket 8 *byte*. Selanjutnya serangan dari attacker 3 berhasil mengirimkan *TCP flood,* hasil yang ditangkap pada *log system* terdapat 5 paket yang masuk dengan ukuran paket 512 dan panjang paket 1460. Hasil pengujian secara langsung attacker membuka celah pada port 22, dengan mengirimkan serangkaian kombinasi nama pengguna dan kata sandi yang cocok, yang dapat membuka akses ke server. Hasil serangan *TCP flood* yang dikirimkan oleh attacker pada server, dengan hasil paket (1694453851.4852) yang terdeteksi pada *log system.*

Referensi

[1] Ernawati, R., Ruslianto, I., Bahri, S., Rekayasa, J., Komputer, S., Mipa, F., Tanjungpura, U., Prof, J., Hadari, H., & Pontianak, N. (2022). Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring. In Coding : Jurnal Komputer Dan Aplikasi (Vol. 10, Issue 01).

[2] Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router Os Menggunakan Metode Port Knocking. In Jurnal Teknoinfo (Vol. 12, Issue 2).

[3] Sugiyono. (2016). Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox Pada Pt Guna Karya Indonesia. Jurnal Cki On Spot, 9(1).

[4] Realize, U. H. (2017). Pengaruh Penggunaan Iptables Firewall Dan Acid Terhadap Keamanan Jaringan. Jurnal Edikinformatika Penelitian Bidang Komputer Sains Dan Pendidikan Informatika, 3(2). Https://Doi.Org/10.22202/Jei.2017.V3i2.1896

[5] Adhi Purwaningrum, F., Purwanto, A., Agus Darmadi, E., Tri Mitra Karya Mandiri Blok Semper Jomin Baru, P., & -Karawang, C. (N.D.). Optimalisasi Jaringan Menggunakan Firewall.

[6] Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server. In Jurnal Ilmiah Nero (Vol. 4, Issue 3).

[7] Analar Valianta Tasmi Deris Stiawan, S. (2016). Identifikasi Serangan Port Scanning Dengan Metode String Matching (Vol. 2, Issue 1). Http://Ars.Ilkom.Unsri.Ac.Id466

[8] Fachri, F. (2023). Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing. 10(1), 51–58. Https://Doi.Org/10.25126/Jtiik.2023105872

[9] Wirawan Muhammad, A., & Riadi, I. (2016). Analisis Statistik Log Jaringan Untuk Deteksi Serangan Ddos Berbasis Neural Network. Ilkom Jurnal Ilmiah, 8(3).