PENERAPAN SISTEM PENGAMANAN PORT PADA LAYANAN JARINGAN MENGGUNAKAN PORT KNOCKING

Devie Ryana Suchendra[1], Alfian Fitra Rahman[2], Setia Juli Irzal Ismail[3]
[12]Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
Jl. Telekomunikasi No. 01 Terusan Buah Batu, Bandung 40257, Indonesia
Email: deviersuchendra@tass.telkomuniversity.ac.id[1],
alfian.fitra.rahman@gmail.com[2], jul@tass.telkomuniversity.ac.id[3]

Abstrak

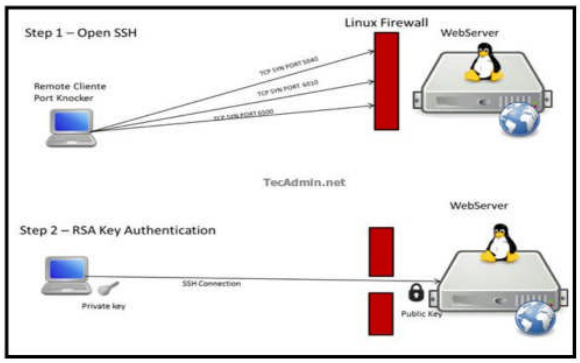
Hal yang terpenting dalam layanan jaringan adalah keamanan akses dan port, hal tersebut merupakan satu kesatuan didalam sebuah layanan. Namun permasalahan yang terjadi adalah port yang terbuka atau akses yang tidak disertai dengan autentikasi dan otorisasi dapat mengakibatkan mudahnya user yang tidak berkepentingan dapat mengakses sistem tersebut. Hal inilah yang menjadi dasar untuk mengamankan hak akses terhadap sebuah sistem yang dibangun tanpa harus menutup port yang dipakai oleh user. Layanan jaringan tersebut akan dibangun di sistem operasi Linux Ubuntu 14.04. Pengamanan port layanan jaringan yang terbuka menggunakan metode port knocking untuk melakukan autentikasi sebelum mengakses server dan dikombinasikan dengan fitur firewall IP filter dan packet timeout pada sebuah router. Dimana metode tersebut akan memilih IP yang diijinkan untuk mengakses server.

Kata kunci : Layanan jaringan, Port knocking, IP filter, Packet timeout.

1. Pendahuluan

Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari pengguna yang disebut "penyusup" untuk mengakses setiap bagian dari sistem jaringan komputer [1]. Pada penelitian ini metode yang digunakan adalah metode IP filter dan port knocking yang di dalamnya menggunakan fitur *packet time out*. *IP filter* adalah suatu mekanisme yang menentukan datagram IP yang akan diproses dengan normal dan IP yang akan *diblock*, dengan diblocknya IP tersebut akan dihapus dan diabaikan. P*acket timeout* merupakan nilai waktu yang ditentukan bagi router CPU untuk menunggu jawaban dari router target sebelum mengasumsikan bahwa paket tidak sampai.[2]

Port knocking adalah metode yang dilakukan untuk membuka akses ke port tertentu yang telah diblock oleh Firewall pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu[3]. Koneksi bisa berupa protocol ICMP, TCP, dan UDP [4]. Jika koneksi yang dikirimkan oleh host tersebut sudah sesuai dengan rule autentikasi yang diterapkan, maka secara dinamis firewall akan memberikan akses ke port yang sudah *diblock* [3].
Dengan cara ini, perangkat jaringan seperti router akan lebih aman, sebab admin jaringan dapat melakukan *filtering* terhadap port-port yang rentan terhadap serangan. Jika dilakukan port scanning port-port tersebut terlihat tertutup. Dari sisi admin jaringan tetap bisa melakukan konfigurasi dan monitoring akan tetapi dengan langkah-langkah khusus (autentikasi) agar bisa diijinkan oleh firewall untuk akses port [4]. Sebagai contoh port knocking dapat dilihat pada Gambar 1.



Gambar 1 Konsep Kerja Port Knocking

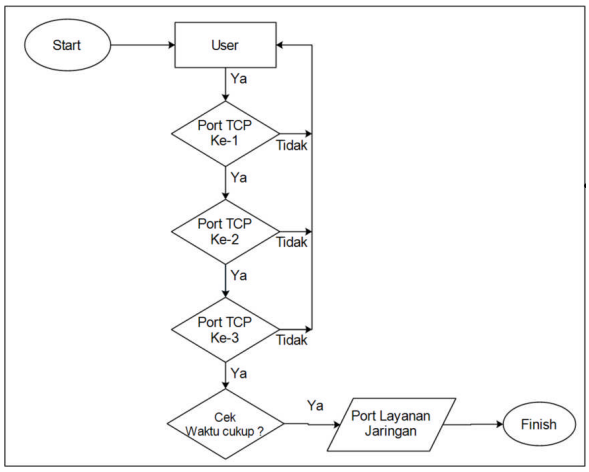
Pada port knocking terdapat istilah *knocking* atau disebut juga autentikasi yaitu usaha untuk membuka port yang tertutup dengan cara mengakses beberapa port komunikasi ketika beberapa port komunikasi tadi diakses dengan kombinasi tertentu, maka akan terbuka sebuah port[5]. Dalam port knocking terdapat program *knock.exe* yaitu suatu program atau *tools* keluaran dari linux untuk melakukan *knocking*.

2. Metode Penelitian

Pada tahap ini ditentukan spesifikasi mengenai sistem yang akan dirancang untuk memenuhi tujuan dari penelitian ini.

A. Perancangan Sistem

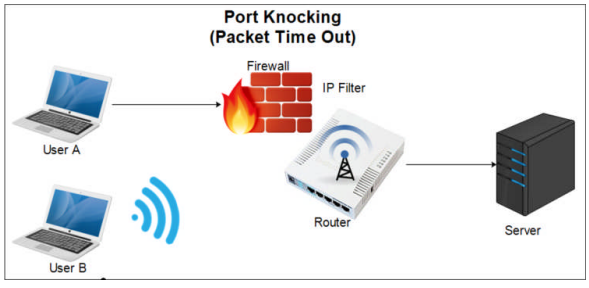
Sistem yang akan digunakan pada penelitian ini adalah mulai dari perancangan, software dan hardware sampai dengan konektivitas ke server.
Metode port knocking pada perancangan sistem usulan ini menggunakan protocol TCP untuk melakukan autentikasi. Sebelumnya port layanan yang terdapat pada server dikondisikan dalam keadaan *closed*/ tertutup sehingga layanan yang terdapat pada server tidak dapat diakses oleh siapapun. Ketika ingin mengakses layanan jaringan yang terdapat pada server harus melakukan autentikasi terlebih dahulu. Hal tersebut bertujuan untuk membuka port yang tertutup. Proses autentikasi port knocking dapat dilihat pada gambar 2



Gambar 2. Flowchart Pengecekan Port

Pada gambar 2 pada pengecekan port, user harus melakukan autentikasi yaitu melakukan knocking sebanyak 3 kali secara berurutan dan dalam waktu yang sudah ditentukan. jika pada proses knocking ternyata melebihi waktu yang ditentukan, maka user harus melakukan autentikasi dari awal.

Selain itu terlihat pada gambar 3 adalah topologi sistem usulan port knocking



Gambar 3. Topologi sistem usulan Port Knocking

Di dalam topologi sistem gambar 3 ini terdapat 2 PC client serta 1 PC server. Di dalam server tersebut terdapat beberapa layanan jaringan diantaranya FTP, email, dan DNS yang terdiri dari Web Server, VirtualHost, CMS, HTTPS. Sedangkan User A menjadi client yang dapat mengakses server yang sudah diamankan menggunakan port knocking dan User B menjadi attacker untuk menguji keamanan server. Sebelumnya server sudah diamankan dengan menggunakan firewall di routerboard Mikrotik yaitu menggunakan IP filter yang bertujuan untuk mengijinkan IP yang dikenal untuk mengakses layanan yang terdapat pada server. Dengan metode tersebut User A (client) maupun User B (attacker) harus melakukan port knocking terlebih dahulu untuk mengakses layanan jaringan yang ada pada server. Dalam metode port knocking ini dikombinasikan dengan fitur *packet timeout*. *Packet* tersebut akan memberi kesempatan waktu dalam proses autentikasi port knocking dan pada saat mengakses layanan jaringan yang ada pada server setelah client melakukan autentikasi atau knocking.
Di dalam perancangan dan implementasi port knocking ini memiliki waktu autentikasi masing-masing sesuai dengan port yang akan digunakan, dapat dilihat pada tabel 1

tabel 1 Implementasi waktu knocking port

No	Keterangan	Name Layanan	Protokol	Port	Knock (TCP)		Waktu Akses yang diberikan
1	Mikrotik	Telnet	SSH	22	Ke-1	1	5 detik
2	Layanan Jaringan		Telnet	23	Ke-2	2	5 detik
			Webfig	80	Ke-3	3	30 menit
		DNS	DNS	53	Ke-1	10	5 detik
			HTTPS	443			
			CMS	80	Ke-2	20	5 detik
			Virtual Host				
			Web Server		Ke-3	30	30 menit
		Email	SMTP	25	Ke-1	100	5 detik
			POP3	110			
			IMAP	143			
			SMTPS	465	Ke-2	200	30 menit
			SMTP	587			
			IMAPS	993	Ke-3	300	5 detik
			POP3S	995			
		File Sharing	FTP	21	Ke-1	1000	5 detik
			Samba	445	Ke-2	2000	5 detik
					Ke-3	3000	30 menit

Berdasarkan tabel 1 implementasi keamanan port knocking dibagi menjadi 2 yaitu, port knocking pada service layanan jaringan dan pada router Mikrotik. Port knocking yang diimplementasikan pada router Mikrotik akan mengamankan port SSH, Telnet, dan Webfig dengan alur autentikasi 1-2-3 yang masing-masing autentikasi memiliki waktu timeout yang sudah ditentukan. Sedangkan pada server layanan jaringan service yang diamankan yaitu DNS, email, dan File Sharing yang masing-masing service memiliki alur autentikasi yang berbeda dan memiliki ratarata waktu timeout 5 detik pada autentikasi pertama dan kedua sedangkan autentikasi yang ketiga akan diberi waktu timeout selama 30 menit, dengan metode tersebut client harus melakukan 3 autentikasi terlebih dahulu sebelum waktu timeout habis untuk bisa mengakses server layanan jaringan dan client hanya bisa mengakses server layanan jaringan dalam waktu 30 menit saja. Jika client mengakses layanan jaringan lebih dari 30 menit service akan menutup dengan sendirinya.

3. Hasil Penelitian

Implementasi port knocking pada Layanan Jaringan

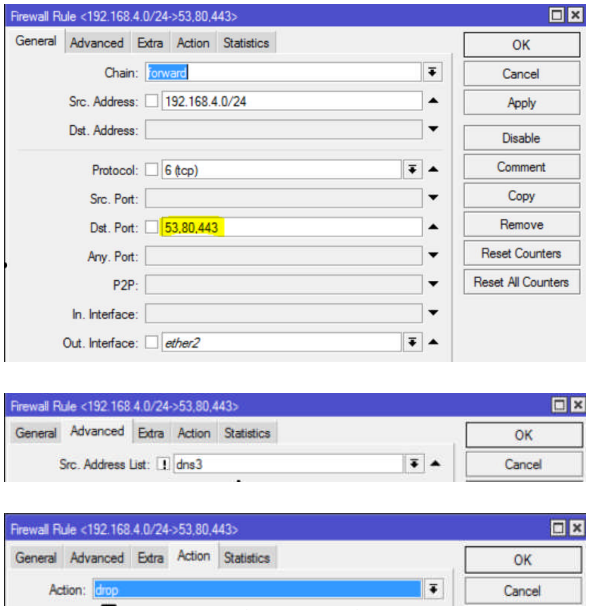
Konfigurasi port knocking akan dibagi menjadi 2 yaitu port knocking untuk client dan untuk attacker.

Implementasi Port knocking pada Router

Implementasi konfigurasi untuk client adalah sebagai berikut

1. Konfigurasi Port knocking DNS

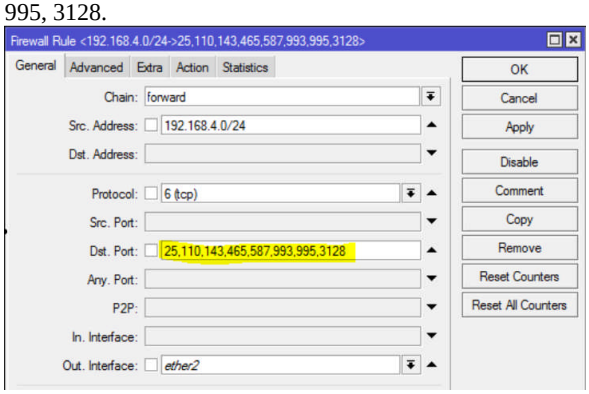
a. Isikan "Chain: forward" kemudian source address isikan IP client yaitu "192.168.4.0/24" kemudian Port yang diamankan untuk DNS yaitu 53, 80, dan 443 Seperti pada Gambar 4.



Gambar 4. Konfigurasi port forwarding dns

2. Konfigurasi Port Knocking untuk Email

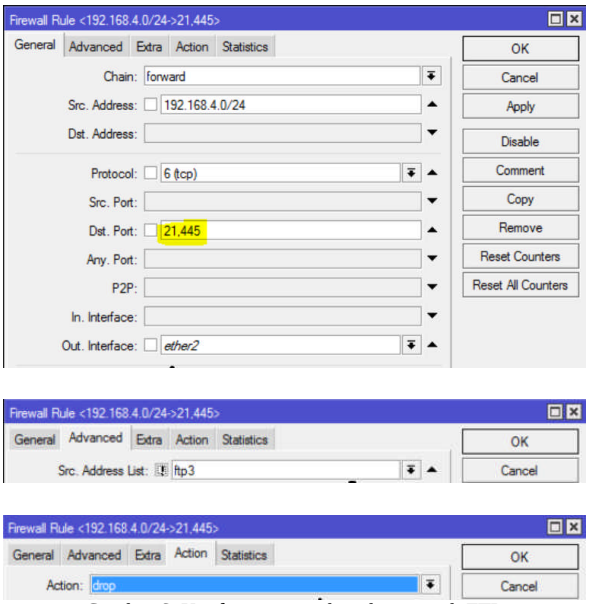
a. Isikan "Chain: forward" kemudian source address isikan IP client yaitu "192.168.4.0/24" kemudian Port yang diamankan untuk email yaitu 25, 110, 143, 465, 587, 993, 995, 3128.



Gambar 5. Konfigurasi port knocking pada email

3. Konfigurasi Port knocking Untuk FTP.

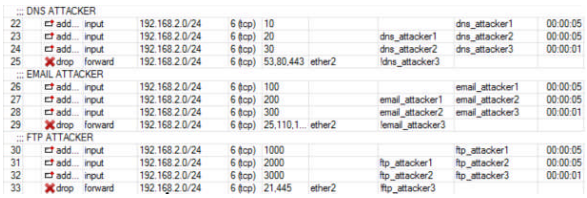
a. Isi "Chain: forward" kemudian source address diisi dengan IP client yaitu "192.168.4.0/24" lalu port yang diamankan untuk FTP yaitu 21 dan 445, seperti pada Gambar 6



Gambar 6. Konfigurasi port knocking untuk FTP

Setelah semua sudah dikonfigurasikan maka hasil dari konfigurasi port knocking dapat dilihat pada gambar 7 dan 8

Gambar 7. Hasil Konfigurasi port knocking untuk client



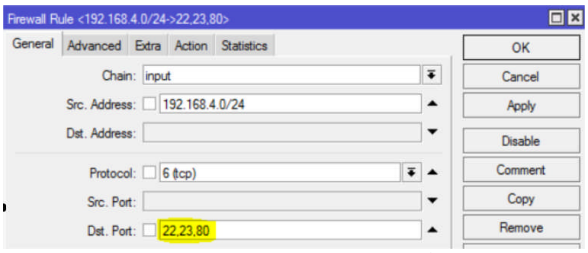
Gambar 8. Hasil Konfigurasi port knocking untuk attacker

Pada gambar 7 dan 8, terdapat layanan jaringan DNS, FTP, dan email yang sudah diimplementasikan dengan metode port knocking.

Implementasi Port knocking pada Router

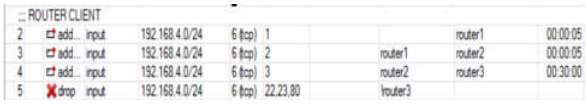
Port router yang diamankan menggunakan metode port knocking yaitu SSH (22), Telnet (23), dan Webfig (80).

Buat rules firewall untuk menutup port SSH (22), Telnet (23), dan Webfig (80). Seperti pada Gambar 4-22

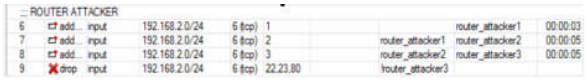


Gambar 9 Port SSH, Telnet, Webfig

Konfigurasi port knocking untuk client dapat dilihat pada gambar di bawah ini.



Gambar 10. Port knocking Untuk Client Router



Gambar 11. Port knocking Untuk Attacker Router

4. Pembahasan

A. *Pengujian*

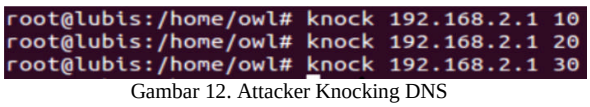
Pengujian sistem adalah proses atau kegiatan yang dilakukan untuk menilai apakah sistem utama yang dirancang telah sesuai dengan apa yang diharapkan. Pengujian ini juga sebagai langkah untuk proses pengembangan sistem berikutnya. Ada pun penjelasan masing-masing pengujian sebagai berikut:

Pada tahap ini dilakukan beberapa pengujian untuk memastikan sistem dibangun dengan baik.
Pengujian keamanan sistem akan dilakukan sebanyak 3 kali uji coba serangan diantaranya,

1. Pengujian terhadap Firewall.
2. Pengujian serangan menggunakan Hydra.
3. Pengujian serangan DoS
4. Pengujian serangan menggunakan metode Brute-Force dan Telnet

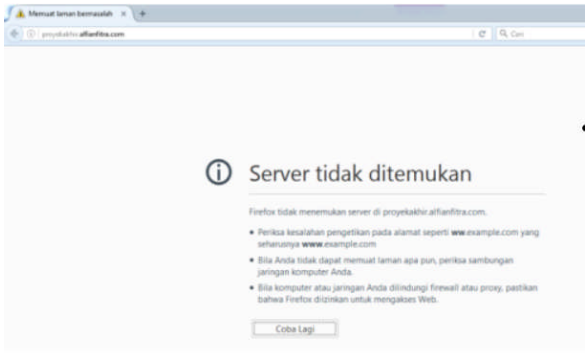
1. Pengujian Terhadap Firewall

Dalam percobaan ini attacker akan mencoba mengakses layanan jaringan DNS, email, dan FTP yang terdapat pada server, dengan kondisi attacker mengetahui alur knocking kemudian attacker melakukan autentikasi sebelum mengakses layanan jaringan. Pengujian ini bertujuan untuk mengantisipasi attacker yang mengetahui alur autentikasi untuk mengkses server.
1. Attacker yang memiliki IP “192.168.2.0/24” melakukan autentikasi
terlebih dahulu menggunakan terminal ubuntu.



Gambar 12. Attacker Knocking DNS

Kemudian attacker akan melakukan percobaan untuk mengakses DNS menggunakan browser.



Gambar 13. Percobaan mengakses DNS menggunakanWebbrowser

Dari gambar 13 dapat diketahui bahwa attacker tidak dapat mengakses DNS meskipun dalam kondisi attacker mengetahui alur autentikasi dan kemudian melakukan autentikasi sebelum mengakses DNS.

2. Pengujian Serangan Hydra

Pada tahap ini dilakukan 2 uji coba yaitu serangan sebelum diamankan dan sesudah diamankan menggunakan Hydra ke server email, FTP, dan SSH (router) untuk mengetahui user dan password.
Attacker menggunakan Hydra di Linux Ubuntu untuk mendapatkan user dan password email. Yaitu dengan cara ketikkan perintah di terminal.

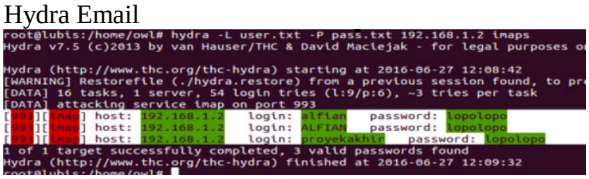
```
Hydra -L user.txt -P pass.txt pop3 postgres
```

```
Hydra -L user.txt -P pass.txt FTP
```

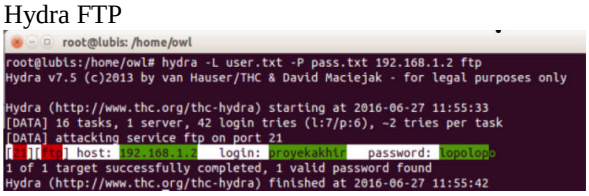
```
Hydra -L user.txt -P pass.txt ssh
```

Gambar 14. Perintah pengujian serangan hydra

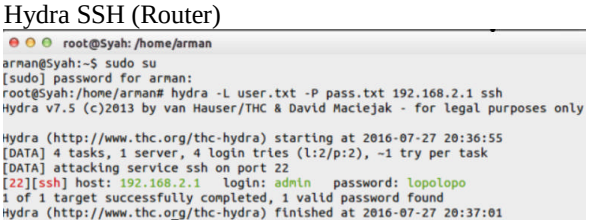
Hasil serangan Hydra sebelum diamankan
Hydra Email



Hydra FTP



Hydra SSH (Router)



Gambar 15. Hydra FTP dan SSH sebelum diamankan

Dari gambar 15 menunjukan bahwa serangan Hydra berhasil mendapatkan user dan password email, FTP, dan SSH/

Pengujian selanjutnya dengan mengamankan sistem yang sudah diamankan terlebih dahulu sebelum dilakukan serangan menggunakan tool Hydra.

Hydra Email

```
root@lubis:/home/owl# hydra -L user.txt -P pass.txt pop3 postgres
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2016-06-27 12:01:21
[DATA] 16 tasks, 1 server, 42 login tries (l:7/p:6), ~2 tries per task
[DATA] attacking service postgres on port 5432
[ERROR] could not resolve address: pop3
0 of 1 target completed, 0 valid passwords found
[ERROR] 1 target did not resolve or could not be connected
Hydra (http://www.thc.org/thc-hydra) finished at 2016-06-27 12:01:21
root@lubis:/home/owl#
```

Hydra FTP

```
root@lubis: /home/owl
root@lubis:/home/owl# hydra -L user.txt -P pass.txt 192.168.1.2 ftp
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2016-06-27 11:49:54
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent
overwriting, you have 10 seconds to abort...
[DATA] 16 tasks, 1 server, 42 login tries (l:7/p:6), ~2 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 16.00 tries/min, 16 tries in 00:01h, 26 todo in 00:02h, 2 active
[ERROR] Too many connect errors to target, disabling ftp://192.168.1.2:21
0 of 1 target completed, 0 valid passwords found
[ERROR] 1 target did not resolve or could not be connected
Hydra (http://www.thc.org/thc-hydra) finished at 2016-06-27 11:51:09
root@lubis:/home/owl#
```

Hydra SSH (Router)

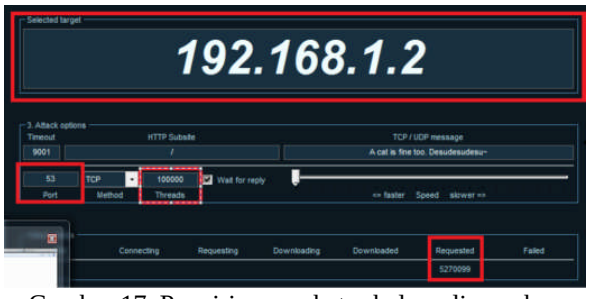
```
root@Syah:/home/arman# hydra -L user.txt -P pass.txt 192.168.2.1 ssh
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2016-07-27 20:39:09
[DATA] 4 tasks, 1 server, 4 login tries (l:2/p:2), ~1 try per task
[DATA] attacking service ssh on port 22
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ERROR] ssh protocol error
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2016-07-27 20:39:20
```

Gambar 16 Hydra FTP dan SSH setelah diamankan

Dari gambar di atas dapat disimpulkan bahwa metode port knocking dapat mengamankan dari serangan Hydra

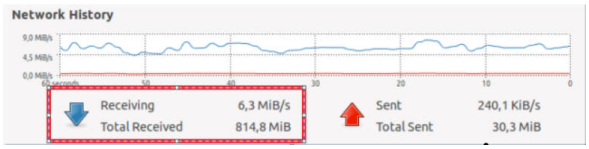
Pengujian Serangan Denial Of Service

Pada tahap ini pengujian dilakukan dengan serangan DoS pada server menggunakan software LOIC dimana percobaan ini dilakukan sebanyak 2 kali, yaitu sebelum diamankan menggunakan port knocking dan sesudah diamankan.



Gambar 17. Pengiriman paket sebelum diamankan

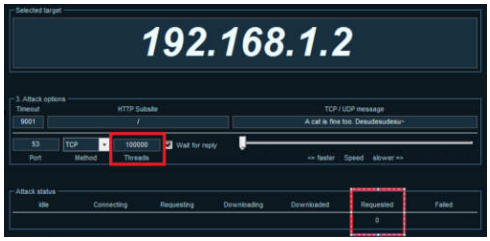
Dapat dilihat pada gambar 17, paket telah terkirim ke server dengan ditandai nilai “requested : 527009”. Kemudian untuk memastikan server terkena serangan DoS yaitu dengan cara melihat system monitor pada server.



Gambar 18.
Monitoring paket yang diterima sebelum diamankan

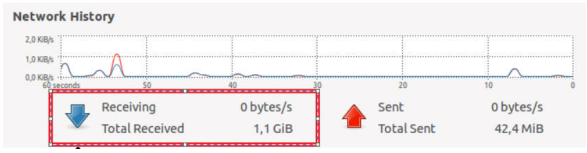
Pada Gambar 18 menandakan server terkena serangan DoS dikarenakan nilai paket yang diterima sebesar 6,3 MiB.

Pengujian setelah Diamankan
Pengujian DoS dilakukan dengan mengirim paket sebanyak 100000.



Gambar 18. Pengiriman paket setelah diamankan

Pada gambar 18 di atas paket DoS tidak terkirim karena nilai “requested : 0”. Kemudian lihat pada server menggunakan system monitor.



Gambar 18.
Monitoring paket yang diterima setelah diamankan

Pada Gambar 18, paket DoS tidak terkirim karena nilai “requested : 0”. Kemudian lihat pada server menggunakan system monitor.

Tabel 2 Pengujian Bloking Serangan

NO	Pengujian	Parameter	Skenario	Hasil yang diharapkan	Tujuan	Hasil
1	Firewall ip filter, port knocking, dan packet timeout	Server layanan DNS, FTP, dan Email tidak dapat diakses meskipun attacker mengetahui dan melakukan knocking terlebih dahulu	Attacker melakukan knocking terlebih dahulu kemudian attacker mengakses server layanan (DNS, FTP, dan Email)	Layanan DNS, FTP, dan Email tetap tidak dapat diakses meskipun attacker melakukan knocking.	Untuk mengantisipasi attacker mengetahui alur knocking	OK
2	Hydra	Firewall harus dapat memblokir serangan Hydra	Attacker akan mencoba mendapatkan user dan password ftp dan email menggunakan Hydra di Linux	Attacker tidak berhasil mendapatkan user dan password FTP dan email	Untuk membuktikan bahwa firewall dapat menahan serangan dari Hydra	OK
3	DOS	Firewall harus dapat memblokir serangan DOS	Attacker akan melakukan DOS dengan cara mengirimkan 10000 paket per detik ke server dengan menggunakan software LOIC	Server dapat menahan serangan DOS	Untuk mengantisipasi dari serangan DOS	OK
4	Brute-Force dan Telnet	Firewall harus memblokir serangan Brute-Force	Attacker mengetahui user dan password untuk akses ke router, kemudian attacker melakukan telnet ke router untuk mendisable rule firewall yang ada	Attacker tidak dapat masuk ke sistem router	Untuk membuktikan bahwa firewall dapat menahan serangan dari brute-force	OK

Pada tabel 2 dapat diketahui metode port knocking juga dapat memblok 3 serangan dari attacker yaitu Brute-Force yang menggunakan Hydra, telnet, dan DoS.

5. Penutup

A. *Kesimpulan*

1. Layanan jaringan dapat saling terintegrasi diantaranya DNS, FTP, dan email, dapat dibangun pada sistem operasi Linux Ubuntu 14.0 2.
2. Dari hasil pengujian yang telah dilakukan menggunakan metode port knocking yang dikombinasikan dengan firewall di Mikrotik, dapat memberikan sistem keamanan autentikasi pada server layanan jaringan dan dapat mengamankan server dari 3 serangan yaitu Hydra, DoS, dan Telnet yang menggunakan ptotocol TCP.

B. *Saran*

1. Server menggunakan IP public atau tersambung dengan internet.
2. TCP yang digunakan untuk autentikasi sebaiknya menggunakan metode acak, tidak berurutan agar tidak mudah untuk ditebak.
3. Membuat metode port knocking dalam satu atau lebih jaringan

DAFTAR PUSTAKA

[1] Z. Ahmad, "Keamanan Jaringan Komputer," Jaringan Komputer,2011.[Online].Available:HTTP://jaringankomputer.org/keamanan-jaringan-komputer. [Accessed 02 Februari 2016].

[2] B. Benardi, Membangun Firewall dengan Cisco Router, Jakarta: Media Komputindo, 2004.

[3] R. Michael, Linux Firewalla, San Fransisco: No Strach Press Inc., 2007.

[4] Admin, "World Ebook Library," ebooklibrary, 2002. [Online].Available:HTTP://www.ebooklibrary.org/articles/networkservice. [Accessed 06 Maret 2016].

[Admin, "Port knocking," Mikrotik.co.id, 2005. [Online]. Available:HTTP://www.Mikrotik.co.id/artikel_lihat.php?id=105. [Accessed 02 Februari 2016]