IMPLIKASI R-WALL UNTUK PENDETEKSIAN DAN PENGAMANAN SERANGAN SIBER PADA SERVER (STUDI KASUS PADA SERVER INFORMATION COMMUNICATION & TECHNOLOGY AKADEMI ILMU KOMPUTER TERNATE)

Abdul Djalil Djayali[1], Rifaldi Nurdin[2] dan Rachmat Saleh Sukur[3]

[1]Manajemen Informatika, Akademi Ilmu Komputer, Jalan. Sultan Babullah. Kota Ternate, Maluku Utara, Indonesia, 97727
Email: add@aikomternate.ac.id
[2]Information Communication & Technology, Akademi Ilmu Komputer, Jalan. Sultan Babullah. Kota Ternate, Maluku Utara, Indonesia, 97727
Email: af8.gunange@gmail.com
[3]Manajemen Informatika, Akademi Ilmu Komputer, Jalan. Sultan Babullah. Kota Ternate, Maluku Utara, Indonesia, 97727
Email: rss@aikomternate.ac.id

ABSTRAK

Keamanan berbanding terbalik dengan kenyamanan, semakin nyaman dalam penerapan teknologi maka akan berdampak pada sisi keamanan sistem. Server merupakan salah satu infratruktur yang penting dalam mengelolah data. Mencegah serangan pada Server penting untuk dilakukan. Penerapan *firewall* dapat meminimalisir serangan yang membahayakan Server. Salah satunya dengan menerapkan aplikasi *Intrusion Detection System* (IDS) seperti Snort yang memiliki kemampuan untuk mendeteksi serangan yang terjadi pada sistem Server. Pada penelitian ini, penulis melakukan pengembangan sistem yang diberi nama R-Wall. Penerapan R-Wall bertujuan untuk mampu memonitor dan mengamankan server terhadap beberapa metode serangan, antara lain yaitu *distribution denial of service* (DDoS) *ping of death*, *port scanning*, *brute force* pada layanan *file transfer protocol* (FTP) dan *brute force* pada layanan *secure shell* (SSH). Hasil penerapan ini mampu memberikan notifikasi serangan yang dikirimkan melalui robot Telegram dengan total 247 serangan *DDoS ping of death*, 8 serangan *port scanning*, 247 serangan *brute force* pada layanan *FTP* dan 208 serangan pada layanan *brute force SSH*. R-Wall juga mampu melakukan pembatasan akses terhadap penyerang.
Kata kunci: kejahatan siber, *monitoring*, keamanan sistem, server, R-Wall

ABSTRACT

Security is inversely proportional to comfort, the more comfortable the application of technology will have an impact on the security side of the system. The Server is an important infrastructure in managing data. It is important to prevent attacks on Servers. Firewall implementation can minimize attacks that harm the Server. One of them is by implementing an Intrusion Detection System (IDS) application such as Snort which has the ability to detect attacks that occur on Server systems. In this study, the authors developed a system called R-Wall. The implementation of R-Wall aims to be able to monitor and secure Servers against several attack methods, including port scanning, DDoS ping of death SSH brute force, and FTP brute force type. The results of this implementation are able to provide attack notifications sent via Telegram robot with a total of 247 DDoS pings of deadly attacks, 8 port scanning attacks, 247 FTP brute force attacks, and 208 SSH brute force attacks. R-Wall is also able to restrict access to attackers.
Keywords: cybercrime, monitoring, system security, Server, R-Wall

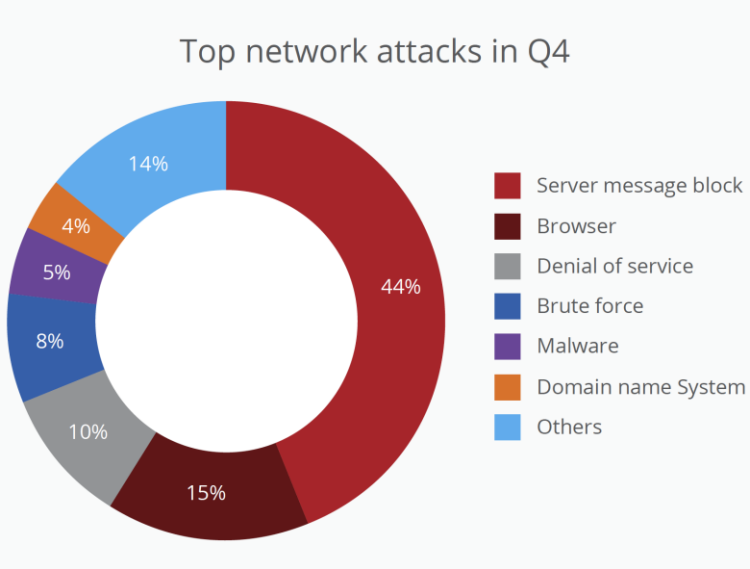
1. PENDAHULUAN

Kejahatan komputer (*cybercrime*) di dunia maya semakin marak terjadi, targetnya tidak hanya perusahaan, namun dapat juga perorangan. Kejahatan komputer mengalami peningkatan dari tahun ke tahun, menyerang infrastruktur baik jaringan, perangkat lunak maupun keras yang bersifat *Internet of Things* (IoT). Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan [1].

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

Desain pengamanan sistem perlu dilakukan guna mencegah serangan yang sangat membahayakan data dan informasi yang terdapat pada sistem. Potensi serangan begitu besar membuat admin sistem merasa kewalahan dan sering kali kehabisan akal dalam mendesain sistem yang lebih aman.

Laporan yang diberikan oleh McAfee Labs pada tahun 2018 menunjukkan potensi serangan yang cukup besar selain pada *SMB* atau *Browser* adalah *denial of service* (DoS) dan *brute force* seperti yang ditunjukkan pada gambar 1. Serangan DoS dan *brute force* merupakan serangan yang umum terjadi pada server. [2]



Gambar 1. Top serangan jaringan oleh McAfee Labs tahun 2018

Pengembangan *firewall* memungkinkan Server bisa terlindungi dari anomali yang dapat memanipulasi data. Dalam penelitian ini dilakukan pengembangan *firewall* yang diberi nama R-Wall. R-Wall merupakan sebuah sistem pengamanan yang dikembangkan pada tahun 2019 oleh Rifaldi N., yang merupakan *framework security* dengan kolaborasi Iptables, Snort dan robot Telegram yang mampu memonitor server, mendeteksi serangan dan memblokir akses serangan. R-Wall juga mampu memberikan notifikasi melalui Telegram secara *real-time* terjadi serangan pengelola server tidak berada di tempat.

2. MATERI DAN METODE

Server

Server merupakan sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer [3]. Sebuah Server dibangun dengan prosesor yang *scalable* juga *random access memory* (RAM) yang besar, berserta sistem operasi yang dirancang sedemikian rupa. Server juga bertugas untuk menjalankan perangkat lunak yang bersifat administratif [4].

Sistem Keamanan Informasi

Sistem keamanan informasi adalah usaha yang dilakukan untuk menjaga integritas (*integrity*) data, kerahasiaan (*confidentiality*) informasi, dan ketersediaan (*available*) akses [5].

Menurut John D. Howard dalam bukunya "*An Analysis of Security Incidents on the Internet*" menyatakan bahwa: "Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab" [6].

Menurut Direktorat Jenderal Aplikasi Informatika Kemeterian Komunikasi dan Informatika Republik Indonesia dalam [1] terdapat 4 tipe serangan yang sering dilakukan yaitu:

1. *Interception* yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi [1],[7].
2. *Interruption* yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login [1],[7].
3. *Fabrication* yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target [1],[7].
4. *Modification* yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan [1],[7].

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

Menurut David Icove, dilihat dari celah keamanan, sistem dapat diklasifikasikan menjadi empat macam [8],[9]:

1. Keamanan fisik (*physical security*) [8],[9].
2. Keamanan data dan media [8],[9].
3. Keamanan dari pihak luar [8],[9].
4. Keamanan dalam operasi [8],[9].

IDS (Intrusion Detection System)

IDS merupakan sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan [10]. Terdapat 2 jenis IDS, antara lain:

1. *Network intrusion detection system* (NIDS), merupakan jenis IDS berbasis jaringan yang ditempatkan pada suatu titik strategis dalam jaringan untuk melakukan pengawasan jalur lalulintas dan menganalisis apakah ada percobaan penyerangan atau penyusupan ke dalam sistem jaringan [10],[11].
2. *Host intrusion detection system* (HIDS), merupakan jenis IDS yang menganalisis aktivitas sebuah *host* jaringan individual untuk mengetahui apakah terdapat percobaan penyerangan atau pengusupan ke dalam jaringan dan melakukan pengawasan terhadap paket yang berasal dari dalam maupun luar hanya pada satu alat saja dan kemudian memberikan peringatan terhadap sistem atau administrator jaringan [10],[11].

Snort

Snort merupakan salah satu jenis IDS jaringan berbasis *open-source* yang mampu menjalankan analisis secara *real-time*, analisis paket *logging* pada *IP network*, analisis *protocol*, *content searching* atau *matching*, dan mendeteksi berbagai serangan dan penyusupan [12].

Iptables

Iptables merupakan suatu sebuah alat dalam sistem operasi *GNU/Linux* yang berfungsi untuk melakukan penyaringan (*filter*) terhadap lalulintas data. Secara sederhana digambarkan sebagai pengatur lalulintas data. Iptables dapat mencakup banyak hal, seperti besar data yang boleh lewat, jenis paket atau *datagram* yang dapat diterima, mengatur lalulintas berdasar asal dan tujuan data [13].

R-Wall

R-Wall merupakan sebuah *tool* yang dibangun menggunakan bahasa pemrograman *bash shell scripting*. R-Wall dibuat pada tahun 2019 oleh mahasiswa Akademi Ilmu Komputer (AIKOM) Ternate yang berfungsi sebagai pengontrol Snort dan Iptables. R-Wall bisa juga dikatakan sebagai *cloning* dari administrator sistem. Ketika ada serangan yang dideteksi dari Snort maka R-Wall secra otomatis akan mengumpulkan informasi tersebut kemudian mengarahkan Iptables untuk memblokir akses dari penyerang dan menyampaikan informasi penyerangan melalui Telegram kepada admin.

Metode Penelitian

Penelitian ini menerapkan metode observatif, implementatif serta metode pengujian secara *blackbox*. Penjelasan dari penerapan metode adalah sebagai berikut [14][15]:

1. Metode secara observatif dilakukan untuk mengumpulkan informasi yang berkaitan sebanyak mungkin guna mendukung penerapan sistem.
2. Metode implementatif dilakukan guna menerapkan pengembangan *firewall* yang sesuai dengan tujuan yang diharapkan. Metode implementatif dimulai dengan menerapkan NIDS dan HIDS dalam menganalisis dan memberikan notifikasi serangan, selanjutnya menerapkan aturan tambahan pada *Iptables* untuk memblokir anomali yang terjadi pada server dan menulis *syntax* untuk pengiriman notifikasi menggunakan robot Telegram pada server.
3. Pengujian *blackbox* dilakukan guna mengetahui sistem berfungsi dengan benar berdasarkan spesifikasi yang telah diterapkan pada server.

Adapun komponen dari metode yang diterapkan seperti pada tabel 1.

Komponen enumerasi *service* diuji dengan metode *blackbox* dengan melakukan pengujian terhadap *service* yang terdapat pada server. Adapun *service* yang diterapkan pada server adalah *service* pada protokol *Internet Control Message Protocol* (ICMP). ICMP diujikan untuk memastikan server memiliki respon terhadap *request*. Selanjutnya adalah pengujian *service* SSH untuk memastikan *port* SSH yang diterapkan pada server berjalan sebagimana yang diharapkan, serta *service* lainnya seperti FTP. Pengujian enumerasi *service* yang dilakukan adalah untuk memastikan setiap *service* yang dibutuhkan berjalan sebagimana yang diharapkan.

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

Tabel.1. Komponen penerapan metode

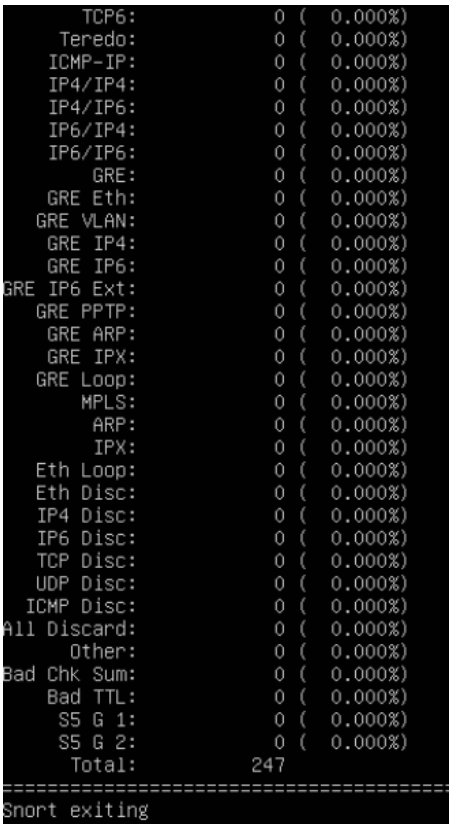
Nama Komponen	Metode
Studi Pustaka	Observatif
Instalasi IDS Snort	Implementatif
Aturan *Iptables*	Implementatif
Syntax notifikasi	Implementatif
Enumerasi *service*	*Blackbox*
Pengujian *DDos ping of death*	*Blackbox*
Port scanning	*Blackbox*
Brute force pada FTP	*BlackBox*
Brute force pada SSH	*BlackBox*
Analisa notifikasi robot Telegram	*BlackBox*

3. HASIL DAN PEMBAHASAN

Telah dilakukan pengujian sistem penggunakan empat metode penyerangan terhadap sistem, yaitu DDoS dengan skala kecil yaitu DDos *Ping of Death*, *port scanning* dan *brute force* pada layanan FTP dan *brute force* pada layanan SSH.

DDos Ping of Death

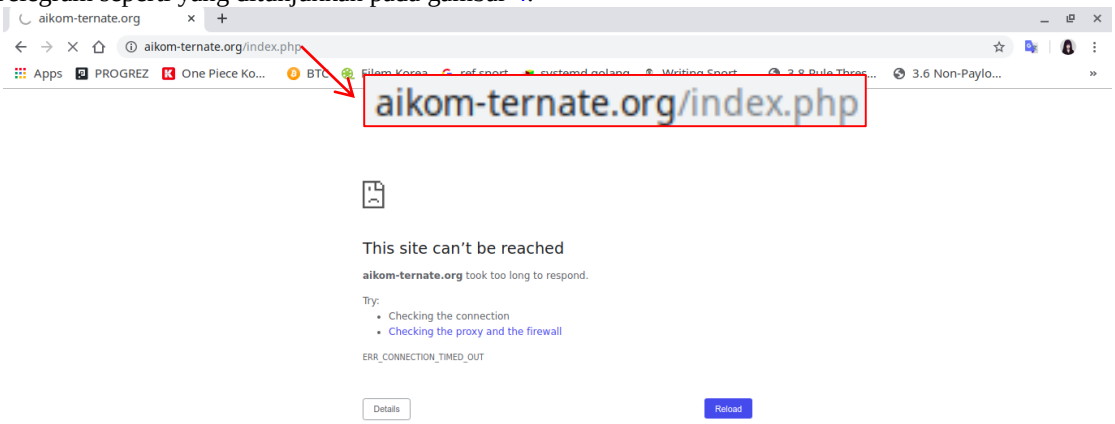
Pengujian *ping of death* dilakukan guna mendapatkan anomali yang dapat dianalisis oleh IDS. *DDos ping of death* pada protokol ICMP dilakukan untuk memeriksa induktivitas jaringan berbasis teknologi *transmission control protocol/internet protocol* (TCP/IP) pada server. Proses yang terjadi selama 1 (satu) kali permintaan menunjukan lebih kecil dari 0,600 per detik dan lebih dari 247 (dua ratus empat puluh tujuh) kali *request* pada protokol ICMP yang berhasil terdeteksi oleh sistem, seperti pada gambar 2.



Gambar 2. Serangan *Traffic ICMP* terdeteksi sebanyak 247 kali

Dalam penelitian ini digunakan pengaturan jumlah batas *request ping* yang diatur R-Wall ke server sebesar 20. Pengaturan batas sebesar 20 untuk memastikan anomali yang terjadi karena *request* di bawah 20 masih tidak berpotensi memberatkan server. Ketika Snort mendeteksi adanya permintaan ICMP yang melebihi 20 maka sistem akan menyaring IP penyerang kemudian melakukan pemblokiran akses

menggunakan Iptables seperti pada gambar 3 dan mengirimkan notifikasi serangan menggunakan robot Telegram seperti yang ditunjukkan pada gambar 4.



Gambar 3. Akses penyerang ke *website* diblokir

Gambar 4. Notifikasi R-Wall adanya serangan lalulintas ICMP ke Telegram

Scanning Port

Pengujian *scanning port* dilakukan dengan cara memasukan perintah `nmap` pada terminal.

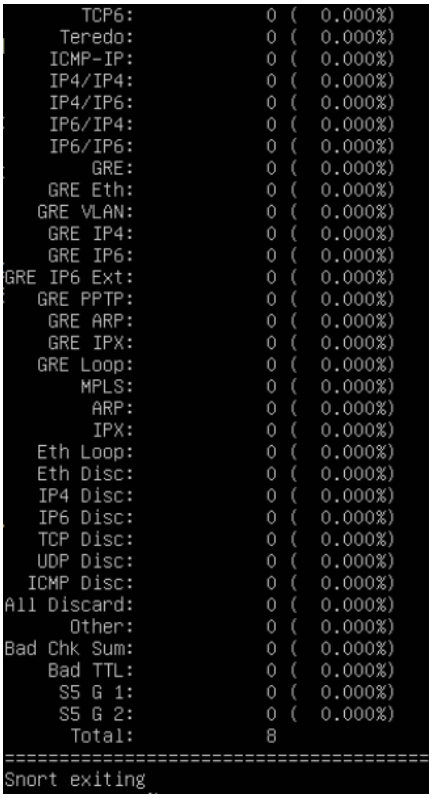
```
# nmap -p 20-500 -v xxx.xx.xx.xxx
```

Hasil dari perintah tersebut adalah adanya 8 kali serangan *scanning port* pada server yang berisi IP dan *port* seperti yang terlihat pada gambar 5. Hasil dari serangan tersimpan dalam *log* R-Wall seperti yang diperlihatkan pada gambar 6. Dari *log* yang berhasil dideteksi oleh Snort, selanjutnya R-Wall akan mengaktifkan aturan Iptables untuk memblokir dan mengirimkan notifikasi serangan melalui robot Telegram seperti pada gambar 7.

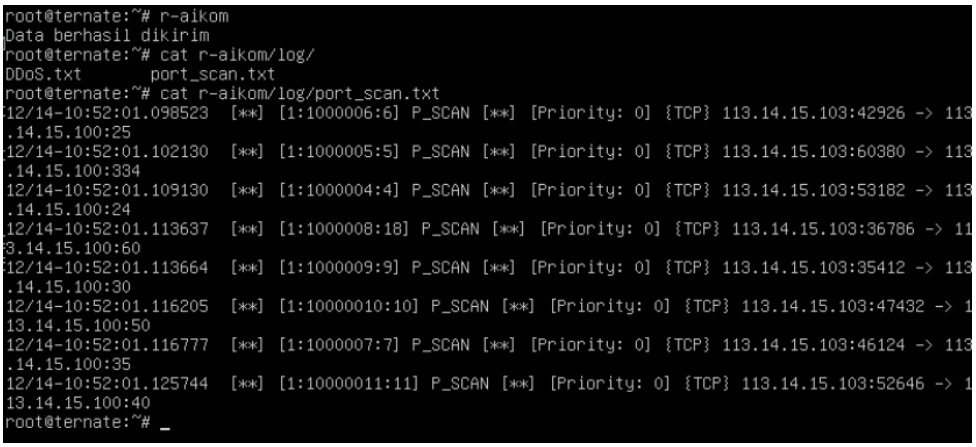
***Brute Force* pada Layanan *File Transfer Protocol* (FTP)**

Pengujian *brute force* pada layanan FTP ini dilakukan menggunakan *tool* sek-kunci yang dibangun secara mandiri untuk mempermudah pengujian, sek-kunci memiliki fitur untuk melakukan *brute force* pada layanan FTP maupun SSH dengan menggunakan *wordlist* yang telah dipersiapkan. Hasil yang diterima seperti pada gambar 8 yang menunjukan penyerang tidak bisa lagi berkomunikasi dengan server karena R-Wall yang diterapkan di server mampu mengatasi serangaan tersebut.

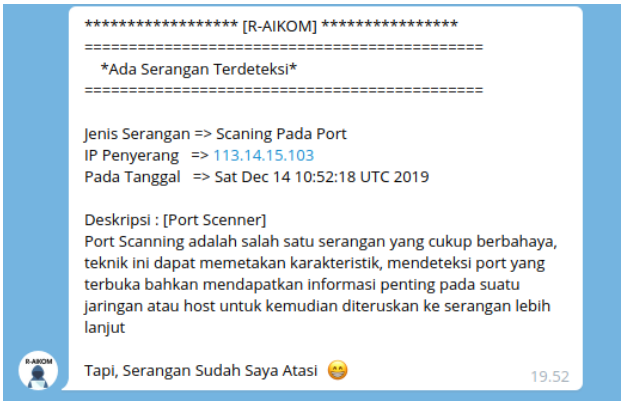
ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)



Gambar 5. Hasil deteksi serangan *port scanning*

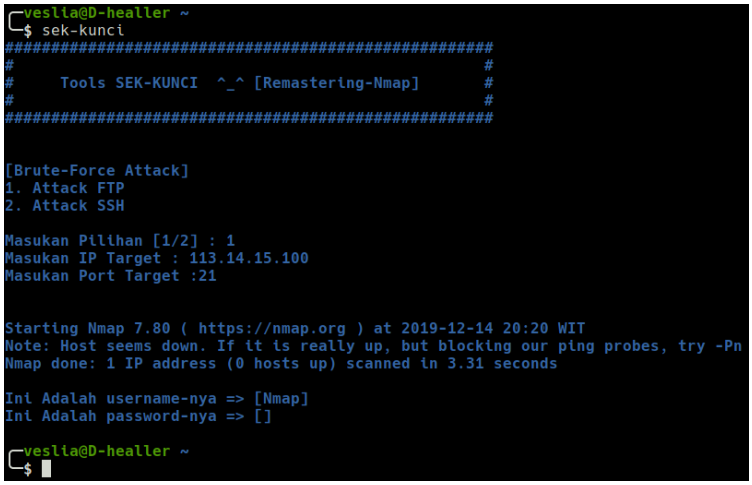


Gambar 6. *Log* serangan *port scanning* yang tersimpan pada R-Wall



Gambar 7. Notifikasi R-Wall adanya serangan *port scanning* ke Telegram

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)



Gambar 8. *Output* yang diterima penyerang menggunakan sek-kunci

Gambar 8 menunjukan bahwa server tidak dalam keadaan aktif lagi dari sisi penyerang. Kondisi ini memungkinkan pengyerang berpikir bahwa sistem yang ditargetkan dalam keadaan tidak aktif namun sebenarnya server telah berhasil memblokir penyerang dengan memanfaatkan R-Wall yang diterapkan ke sistem. Gambar 9 menunjukan serangan dapat dideteksi Snort dan pada blok warna merah merupakan total percobaan *brute force* pada layanan FTP sebanyak 247 kali. Gambar 10 menunjukan *log* R-Wall untuk serangan *brute force* pada layanan FTP. Dari *log* tersebut, R-Wall kemudian mengirimkan notifikasi melalui Telegram, seperti yang terlihat pada gambar 11.

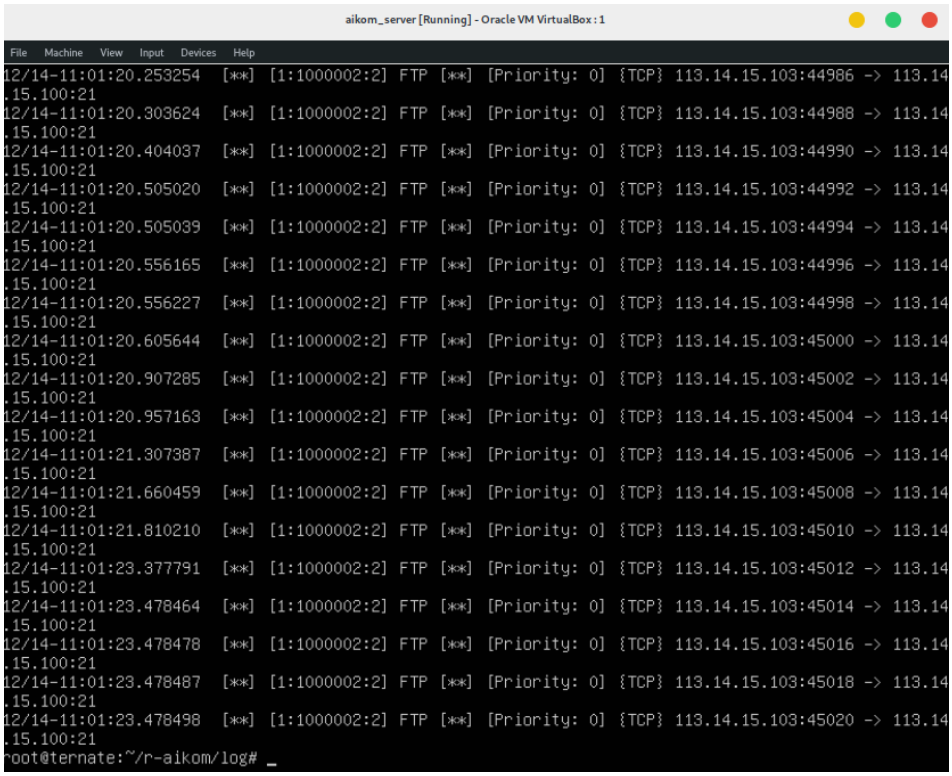
Gambar 9. Deteksi Snort terhadap serangan *brute force* pada layanan FTP

Brute Force* pada Layanan *Secure Shell (SSH)

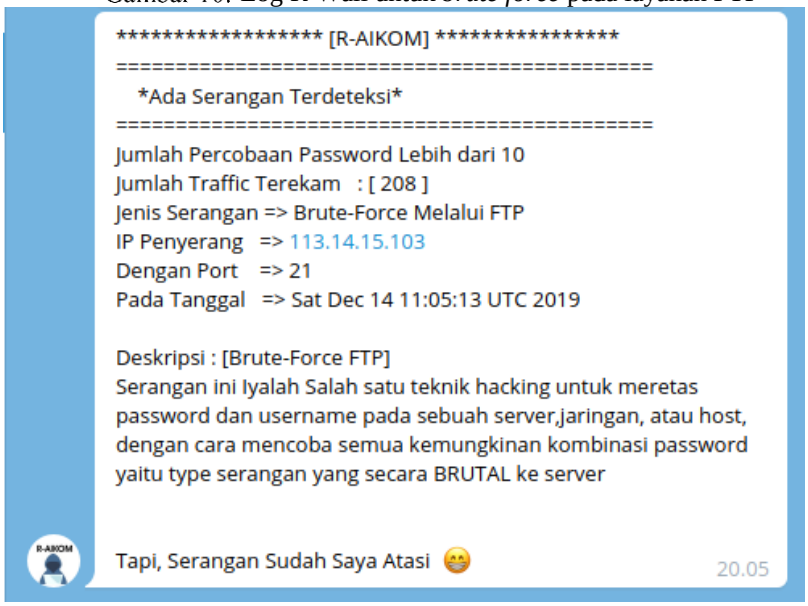
Ketika penyerang gagal dalam melakukan beberapa serangan sebelumnya maka penyerang akan coba melakukan serangan pada layanan SSH dengan berasumsi bahwa kemungkinan serangan ini akan berhasil. Namun serangan tersebut juga mampu diatasi R-Wall sebagai hasil deteksi oleh Snort. Gambar 12 menunjukkan hasil deteksi percobaan serangan sebanyak 208 kali. Dari deteksi Snort ini dilakukan

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

pemblokiran dari IP penyerang yang berhasil masuk dalam *log* R-Wall, seperti yang ditunjukkan pada gambar 13.

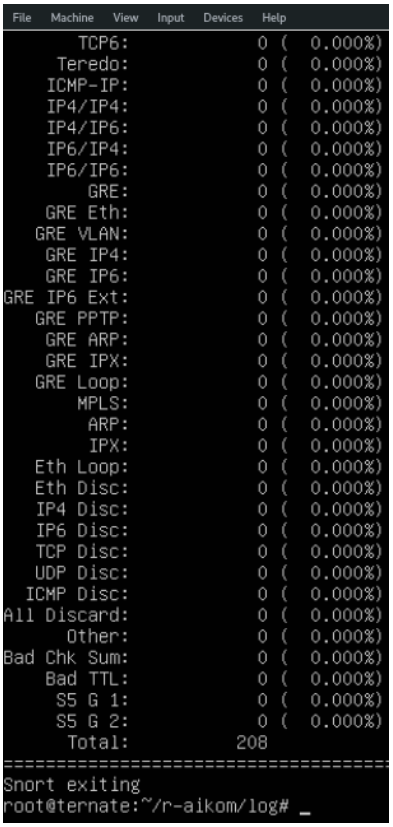


Gambar 10. Log R-Wall untuk *brute force* pada layanan FTP

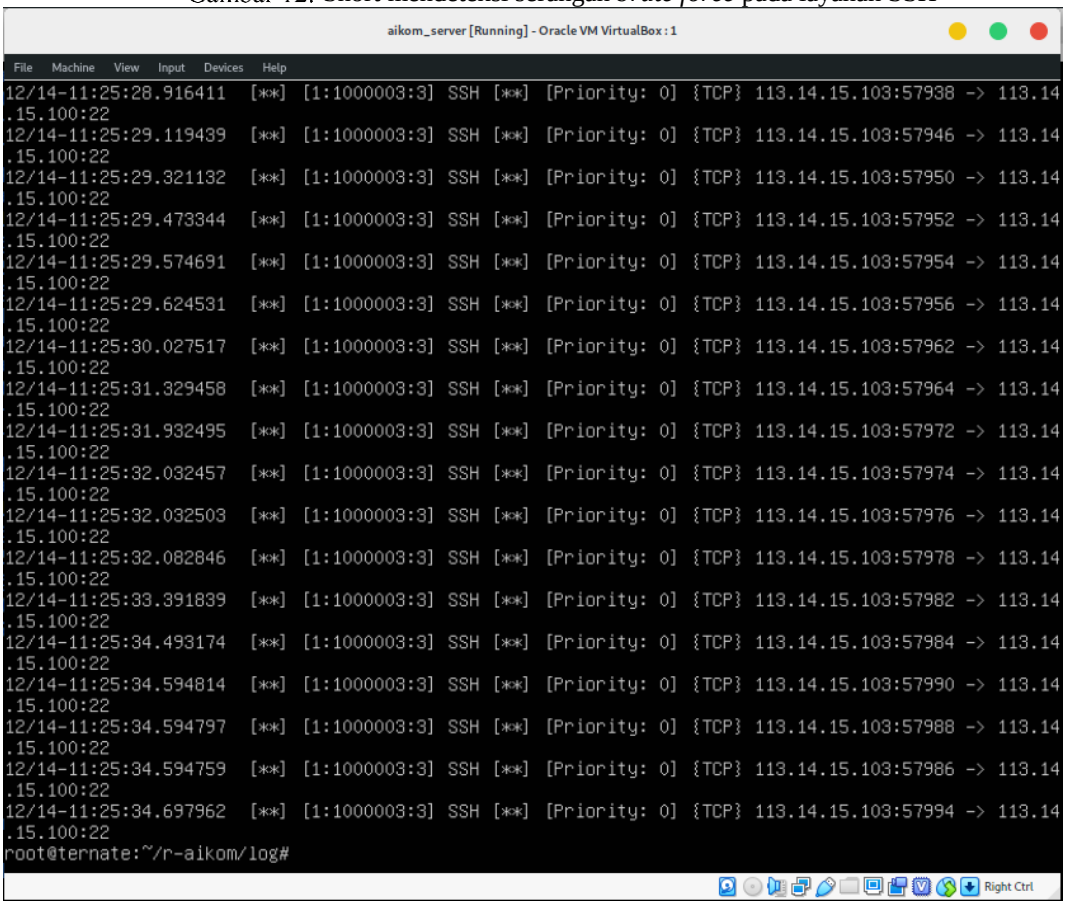


Gambar 11. Notifikasi serangan *brute force* ke layanan FTP

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)



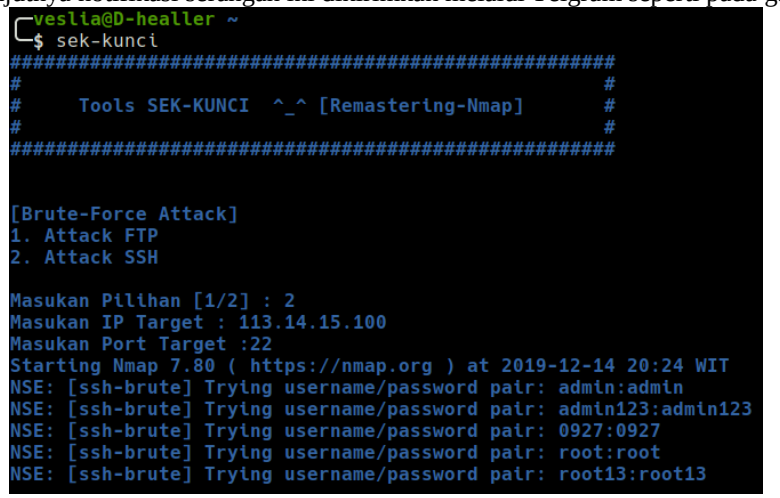
Gambar 12. Snort mendeteksi serangan *brute force* pada layanan SSH



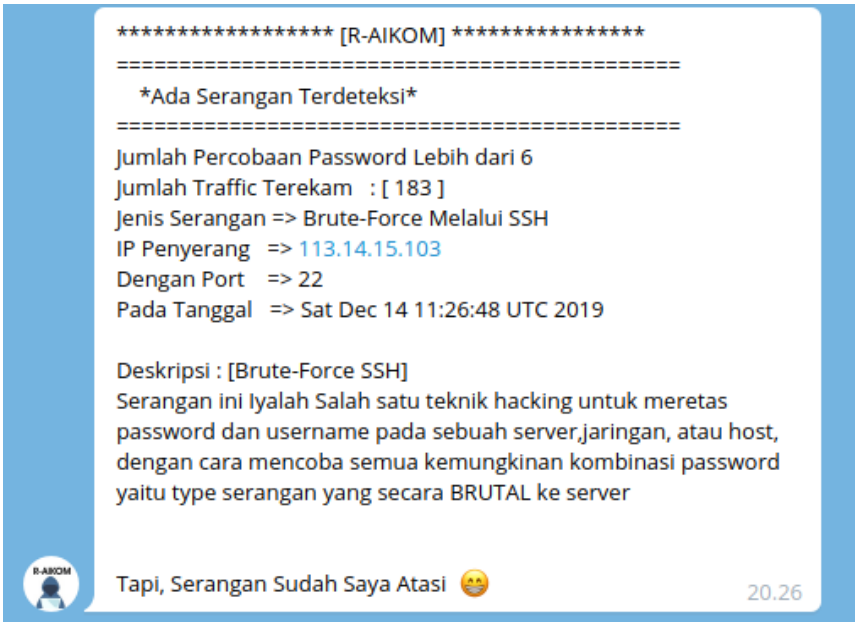
Gambar 13. *Log* R-Wall untuk *brute force* pada layanan SSH

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

Serangan yang dilakukan oleh penyerang akan tidak mendapatkan respon lagi seperti yang terlihat pada gambar 14. Selanjutnya notifikasi serangan ini dikirimkan melalui Telgram seperti pada gambar 15.



Gambar 14. Serangan *brute force* pada layanan SSH pada komputer penyerang terhenti



Gambar 15. Notifikasi serangan Brute-Force SSH

Tabel 2 menunjukan rangkuman hasil pemantauan dan pengamanan serangan pada server untuk empat tipe serangan.

Tabel.2. Hasil analisis pemantauan dan pengamanan serangan pada server

Nama Komponen	Hasil Pengujian		
	Dideteksi	Diblokir	Notifikasi Terkirim
DDos ping of death	247	Ya	Ya
Scanning Port	8	Ya	Ya
Brute Force pada *layanan* FTP	247	Ya	Ya
Brute Force pada SSH	208	Ya	Ya

4. KESIMPULAN DAN SARAN

Pengembangan R-Wall sebagai *firewall* pada Server dengan mengkolaborasikan IDS Snort, Iptables dan robot Telegram membuat membuat pemantauan aktivitas anomali di server lebih mudah dipantau dan pengamanan serangan pada jaringan secara otomatis dapat dilakukan. R-Wall dengan Snort berhasil mendeteksi 247 serangan *DDos ping of death*, 8 serangan *port scanning*, 247 serangan *brute force* pada layanan FTP, 208 serangan *brute force* pada layanan SSH yang terjadi pada server. R-Wall dengan

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)

Iptables berhasil membuat *log* serangan dan memblokir serangan yang terjadi pada server. R-Wall dengan robot Telegram *berhasi*l mengirimkan notifikasi serangan kepada admin server.

Penerapan konsep R-Wall yang dilakukan pada penelitian ini sangat disarankan untuk diterapkan pada server sehingga keamanan jaringan menjadi lebih baik Sistem dapat dikembangkan dengan kemampuan pendeteksian malware misalnya menggunakan MalTrail.

DAFTAR PUSTAKA

[1] Tashia, "Keamanan Jaringan Internet dan Firewall," *Direktorat Jenderal Aplikasi Informatika*, 2017. .

[2] S. Andrews, "Statistical software for teaching: relevant, appropiate and affordable," 2010. [Online]. Available: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-nov-2015.pdf.

[3] Abdurrahman, Soni, and A. Hafid, "Keyword : Proxmox , Virtualization , Resources , Server , Operating System Sistem Operasi," vol. 9, no. 2, pp. 369–376, 2019.

[4] O. Suryana, "Server dan Web Server," no. August, pp. 14–23, 2018.

[5] R. Jumardi, "Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan XYZ," *KajianKebijakanKeamananSistem InformasiSebagaiBentuk PerlindunganKerahasiaanPribadi KaryawanPerusahaanXYZ*, p. 6, 2016.

[6] J. D. Howard, *An Analysis of security incidents on the internet*. 1997.

[7] H. A. Erwin Gunadhi, "KEAMANAN KOMUNIKASI DATA SMS PADA ANDROID DENGAN MENGGUNAKAN APLIKASI KRIPTOGRAPI ADVANCE ENCRYPTION STANDARD (AES)," *STT-Garut*, vol. 12, no. 2, pp. 296–300, 2015, [Online]. Available: http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf.

[8] K. Anom and B. Utama, "Keamanan Komputer & Sistem Informasi." .

[9] Y. P. PHS, "KEAMANAN SISTEM INFORMASI," *STMIK El Rahma – Yogyakarta*, pp. 1–14, 2016.

[10] D. N. Awangga, H. Sajati, and Y. Astuti, "Pemanfaatan Intrusion Detection System (Ids) Sebagai Otomatisasi Konfigurasi Firewall Berbasis Web Service Menggunakan Arsitektur Representational State Transfer (Rest)," *Compiler*, vol. 2, no. 2, pp. 79–88, 2013, doi: 10.28989/compiler.v2i2.49

[11] M. Ulfa, J. Jenderal, A. Yani, and N. Palembang, "Di Jaringan Internet Universitas Bina Darma," no. 12, pp. 105–118.

[12] B. Sudradjat, "Sistem Pendeteksian dan Pencegahan Penyusup Pada Jaringan Komputer Dengan Menggunakan Snort dan Firewall," *JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Res.*, vol. 1, no. 1, pp. 10–24, 2017.

[13] G. Sondakh, M. E. I. Najoan, and A. S. Lumenta, "Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat," *J. Tek. Elektro dan Komput.*, vol. 3, no. 4, pp. 19–27, 2018.

[14] G. W. Setiawan, "Pengujian Perangkat Lunak Menggunakan Metode Black Box Studi Kasus Exelsa Universitas Sanata Dharma," p. 286, 2011.

[15] K. Joesyiana, "Penerapan Metode Pembelajaran Observasi Lapangan Pada Mata Kuliah Manajemen Operasional," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

ISSN: 2337-7631 (printed)
ISSN: 2654-4091 (Online)