RANCANG BANGUN *INTRUSION PREVENTION SYSTEM* DAN *RECOVERY* PADA *SNORT* DENGAN NOTIFIKASI *WHATSAPP*

SKRIPSI

Dibuat Untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

SEPTIAN HADI FAJAR - 1807422018

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2022

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : SEPTIAN HADI FAJAR

NIM : 1807422018

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : RANCANG BANGUN *INTRUSION PREVENTION SYSTEM DAN RECOVERY* PADA *SNORT* DENGAN NOTIFIKASI *WHATSAPP*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 10, Bulan Agustus, Tahun 2022 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I (Ayu Rosyida Zain, S.ST., M.T.) ( )

Penguji I : (Nur Fauzi Soelaiman, S.T., M.Kom.) ( )

Penguji II : (Maria Agustin, S.Kom., M.Kom.) ( )

Penguji III : (Fachroni Arbi Murad, S.Kom., M.Kom.) ( )

Mengetahui
Jurusan Teknik Informatika dan Komputer
Ketua

Mauldy Laya, S.Kom.,M.Kom.
NIP.197802112009121003

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : SEPTIAN HADI FAJAR

NIM : 1807422018

Jurusan/ProgramStudi dan Jaringan : T.Informatika dan Komputer / Teknik Multimedia

Judul skripsi : RANCANG BANGUN *INTRUSION PREVENTION SYSTEM* DAN *RECOVERY* PADA *SNORT* DENGAN NOTIFIKASI *WHATSAPP*

Menyatakan dengan sebenarnya bahwa skripsiini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatantersebut.

Depok, 15 Juli 2022

Yang membuat pernyataan

(SEPTIAN HADI FAJAR)
NIM. 1807422018

KATA PENGANTAR

Puji serta syukur penulis ucapkan kepada Tuhan Yang Maha Esa, karena atas rahmat dan kahrunia-Nya penulis dapat menyelesaikan laporan skripsi ini dengan baik. Adapun tujuan penulis dari pembuatan laporan skripsi ini adalah untuk memenuhi syarat menyandang gelar Sarjana Terapan (Diploma 4) .Banyak kesulitan yang penulis temui dalam prosess pembuatan laporan skripsi ini namun banyaknya support yang yang didapatkan oleh penulis dalam pembuatan laporan ini sehinnga penulis dapat menyelesaikan lpaoran ini tepat waktu. Maka dari itu penulis ingin mengucapkan terima kasih kepada :

1. Ibu Ayu Rosyida Zain, S.ST., M.T. selaku pembimbing, yang telah memebrikan saran-saran dan motivasi untuk pengambilan judul serta koreksi kesalahan di setiap konsultasi laporan skripsi ini.
2. Waladi Tri Nur Pamungkas, selaku rekan yang telah memberikan saya support dari segi material yang saya gunakan dalam pembuatan laporan skripsi ini.
3. Terkhususnya Orang Tua yang telah memberikan dukungan secara material dan spiritual yang menjadi salah satu pemacu semangat terbaik.

Penulis tahu bahwa laporan ini masih jauh dari kata sempurna, namun penulis berharap laporan ini dapat berguna dalam inovasi-inovasi teknologi khususnya seputar keamanan jaringan. Sekiranya cukup kata-kata prantara dari penulis, semoga laporan ini dapat berguna bagi pembaca, terima kasih.

RANCANG BANGUN *INTRUSION PREVENTION SYSTEM* DAN *RECOVERY* PADA *SNORT* DENGAN NOTIFIKASI *WHATSAPP*

Abstrak

Keamanan jaringan pada sebuah server merupakan hal mutlak pada suatu arsitektur jaringan atau topology jaringan. aksesnya perlu dijaga dari pihak-pihak yang tidak berkepentingan. Mekanisme recovery dan notifikasi juga merupakan hal penting dalam keamanan jaringan server. Proposal skripsi dengan judul *"RANCANG BANGUN INTRUSION PREVENTION SYSTEM DAN RECOVERY PADA SNORT DENGAN NOTIFIKASI WHATSAPP"* memiliki rumusan masalah terkait pembuatan sistem *IPS* pada snort di jaringan server , implementasi mekanisme *recovery* dan notifikasi terkait keamanan server. Tujuan dari proposal skripsi adalah untuk membuat sistem keamanan jaringan yang dapat melakukan filter terhadap *source-source* yang masuk kedalam jaringan server, melakukan otomatisasi dalam mekanisme notfikasi terkait ancaman yang terjadi dan mekanisme recovery.Metode pengumpulan data yang digunakan adalah kuantitatif menggunakan skenario uji experimental, dari skenario uji yang dibuat didapatkanlah data-data yang sesuai dengan realitas pada penggunaan sistem. Data yang telah didapat dibuatkan kesimpulan-kesimpulan yang dapat dimasukan kedalam instrument analisis data secara quantitatif. Agar data-data yang ada dapat dipertanggung jawabkan keilmiahannya maka diambilah tijauan pustakan dari beberapa jurnal ilmiah internasional/nasional sebagai data pendukung.Berdasarkan pengujian yang dilakuan didapatkan beberapa kesimpulan seperti kefektifan kinerja sistem berbanding terbalik dengan banyaknya jumlah deteksi yang terjadi, kecepatan prosess *recovery* terpengaruh oleh jumlah data, sistem dapat melakukan seluruh fungsinya dengan tepat mulai dari deteksi, bloking, *recovery* dan notifikasi ke aplikasi whatsapp namun memiliki delay pada dua jenis ancaman yaitu DOS ICMP traceroute dan DOS SYN flood.

Kata Kunci: Keamanan Jaringan, *IPS*, Server, *Otomatisasi, Snort, Notifikasi, Recovery, whatsapp*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan dalam infrastruktur jaringan adalah hal yang prioritas untuk melindungin sistem dari tindakan-tindakan merusak, memodifikasi dan hal-hal yang bersifat membocorkan data ke pihak lain (Rizal Fauzi and Made Suartana 2018) dari (Binanto, 2007). kategori aliran data dari yang bersifat umum hingga rahasia pasti menggunakan infrastruktur jaringan sebagai media komunikasi dan penyebarannya, terutama pada jaringan server penyimpanan. Salah satu upaya untuk meningkatkan keamanan jaringan pada server adalah dengan *Intrusion Prevention System (IPS)* dan snort sebagai *Intrusion Detection System (IDS). IPS dan IDS* merupakan fasilitas sistem keamanan jaringan yang memiliki fungsi yang berbeda. *IPS* merupakan peningkatan dari *IDS* yang memiliki kamampuan tidak hanya dapat mendeteksi, namun juga dapat melakukan tindakan preventif terkait ancaman yang terdeteksi, *IPS* bekerja dengan melakukan inspeksi pada paket data yang lewat, dan melakukan tindakan terhadap sumber dari paket tersebut ataupun paket itu sendiri bila terdetksi sebagai *threat* (Widya Pradipta 2017). *Threat* sendiri adalah hasil deteksi dari sebuah percobaan penetrasi seorang hacker untuk mendapatkan informasi dari korban, hal tersebut dapat disalahgunakan untuk tindakan kriminal ataupun tindakakan negative lain, salah satu contoh threat yang sering dilakukan salah satunya adalah, port scanning, Nmap dan DOS.

Dalam sistem keamanan server mekanisme *recovery* juga dibutuhkan, dalam upaya mengurangi potensi data rusak bila sistem *IPS* tidak mampu mencegah serangan pada server, backup merupakan mekanisme *recovery* yang efektif guna menghindari kerusakan data pasca indikasi serangan yang terjadi “Operasi Backup / Recovery penting untuk diwujudkan untuk keandalan data yang tinggi. Diperlukan dua server cadangan atau lebih, mengingat risiko data cadangan rusak” (Satoshi, Mutsuo, and Katsuo 2009).

Fakta dari seorang administrator jaringan tidaklah setiap saat berada didepan layar komputer , maka perlulah suatu metode pemberitahuan kepada administrator

jaringan bahwa server atau jaringannya sedang menadapatkan penetrasi. Penelitian Chriss Messina menyatakan “Jejaring sosial paling populer "Ok.ru" di dalam kategori usia memiliki 22% dari semua pengguna, sedangkan di messenger "WhatsApp" angka ini adalah 40%” (Vorontsov and Radmir 2021), berdasarkan uraian tersebut notifikasi deteksi threat melalui applikasi WhatsApp dipilih.

Dengan mengkaloborasikan IPS dengan snort yang telah teruji sebagai IDS dengan kapabilitas deteksi yang tinggi dengan penggunaan resource yang optimal”(Albin and Rowe 2012) dan Bash Program yang akan menjalankan recovery dan notifikasi melalui WhatsApp. Serta didukung juga dengan adanya data-data penelitian sebelumnya yang juga menggunakan WhatsApp sebagai media notifikasi. Seperti “*Implementasi Intrussion Detection System (IDS) Dengan Menggunakan Jejaring Sosial Sebagai Media Notifikasi”* (Iswahyudi 2017) dan “*NOTIFIKASI AGENDA HARIAN MENGGUNAKAN APPLICATION PROGRAMMING INTERFACE (API) DAN SMS GATEWAY”*(Imam Prasetyo, Joko Triyono 2016) memeprkuat latar belakang dalam pembangunan sistem ini.

1.2 Rumusan Masalah

Rumusan masalah yang Penulis dapatkan dari latar belakang diatas antara lain:

1. Bagaimana membuat dan mengimplementasikan sistem IPS pada snort dalam pengamanan server di sisi jaringan ?
2. Bagaimana implementasi sistem notifikasi WhatsApp pada sistem keamanan IDS IPS snort di server ?
3. Bagaimana mengimplementasikan mekanisme *recovery* secara otomatis menggunakan Rsync pada sistem keamanan IDS IPS snort di server ?

1.3 Batasan Masalah

Agar tidak terlampau luas dalam pembahasan ini, maka diterapkan batasan-batasan masalah sehingga tujuan dari pembuatan dari proposal dapat tercapai.

Batasan – batasan masalah tersebut adalah sebagai berikut :

a Sistem ini dilakukan dalam jaringan area lokal(LAN/WLAN)

b Sistem dijalankan dengan lima user pada jaringan, rinciannya sebagai berikut : pada mesin virtual (lubuntu 18.04, 2x Ubuntu Server 20.4, 2x kali linux) dan juga perangkat fisik (BOLT HOME-ROUTER BL201).

c Server yang digunakan bersifat server penyimpanan data 2x Ubuntu Server 20.4 dan satu server utama ubuntu (18.04).

d Deteksi ancaman yang diterapkan ada tiga jenis ancaman (Nmap Scanning port, DOS icmp traceroute, SYN flood).

1.4 Tujuan dan Manfaat

Adapun Tujuan dari Perancangan Sistem Keamanan ini adalah :

1.4.1 Tujuan

a. Membuat sistem keamanan IPS dan recovery pada snort dengan notifikasi WhatsApp guna dapat melakukan tindakan pencegahan yang tepat pada prosess deteksi, filter, dan back up.
b. Melakukan recovery data pada server menggunakan tehnik Rsync.
c. Membuat mekanisme notifikasi *threat* ke WhatsApp serta log-management lokal dengan pengujian DOS (ICMP traceroute dan SYN flood), SQL maping dan Nmap scanning port.

1.4.2 Manfaat

a. Mempersempit celah keamanan yang terbuka untuk penetrasi.
b. Memberikan mitigasi bencana terhadap data dengan tehnik yang efektif dan juga aman.
c. Mempercepat prosess troubleshoot bila terjadi serangan pada server.

1.5 Sistematika Penulisan

Penelitian ini dilakukan dengan metode sebagai berikut:

1. BAB I PENDAHULUAN

Pada tahap ini Penulis menuliskan latar belakang dalam pembuatan proposal skripsi ini, membuat batasan-batasan masalah terkait dengan judul proposal, mebuat rumusan masalah, memberikan tujuan serta kegunaan dalam pembuatan proposal skripsi ini.

2. BAB II TINJAUAN PUSTAKA

Pada tahap ini Penulis melakukan studi pustaka tentang data dan informasi yang berkaitan dengan masalah yang sudah ditentukan pada jurnal – jurnal yang berkaitan dengan masalah proyek tersebut.

3. BAB III METODE PENELITIAN

Pada bab ini akan menjelaskan tentang metodologi penelitian yang digunakan, kemudian menjelaskan. Kemudia menjelaskan Teknik pengumpulan data yang digunakan dalam penelitian mulai dari thapan studi Pustaka hingga Analisa secara umum yang nantinya akan dibahas pada bab selanjutnya. Lalu menjelaskan tentang objek penelitian yang dilakukan

4. BAB IV HASIL DAN PEMBAHASAN

Pada tahap ini, dilakukan pembahasan mulai dari proses persiapan kebutuhan hingga proses uji dengan cara percobaan penetrasi terhadap server yang telah dipasangkan system RANCANG BANGUN INTRUSION PREVENTION SYSTEM DAN RECOVERY PADA SNORT DENGAN NOTIFIKASI WhatsApp apakah threat yang ada pada daftar dapat terdeteksi, terblok dan juga ternotif ke applikasi WhatsApp. Pengujian ini dilakukan untuk mengetahui apakah aplikasi ini berjalan sesuai yang diharapkan Penulis atau tidak. Serta dilakukan pnegumpulan data serta Analisa terkait data yang telah didapat gunakan mendapatkan jawaban atas tujuan—tujuan pada bab 1.

5. BAB V PENUTUP

Pada bab ini akan dibuatlah kesimpulan atas pengujian dan analisis yang telah dilakukan guna mendapatkan hasil akhir dari implementasi rancng bangun sistem ini. Serta penambahan saran oleh penulis untuk pengembangan sistem serupa dimasa yang akan datang agar lebih baik lagi.

6. DAFTARPUSTAKA

Pada bab ini terdapat list-list sumber informasi berupa jurnal , website sebagai bukti atau sumber informasi proposal.

7. DAFTAR RIWAYAT HIDUP

Pada bab ini akan dilampirkan biodata serta urutan riwayat pendidkan Penulis.

8. LAMPIRAN

Pada bab ini akan akan di isi dengan lampiran-lampiran yang terkait kepentingan pembuatan skripsi ini dapat berupa foto, berkas penting, dll.

BAB V
PENUTUP

5.1 Kesimpulan

Adapun kesimpulan-kesimpulan yang didapat dari pengujian sistem terhadap seluruh jenis serangan dalam waktu 360 detik adalah sebagai berikut :

a sistem IPS yang dibuat menggunakan batch script terbukti dapat memblokir serangan snort IDS secara realtime(waktu proses <=1 detik) dengan tingkat keberhasilan Nmpa scanning port 100%, SYN flood 88,79% dan DOS ICMP traceroute 0,04%.

b Notifikasi log management serangan terhadap server dapat terkirimkan melalui mobile apps WhatsApp secara real-time(waktu proses <=1 detik) pada dua jenis serangan. kecepatan kirim notifikasi ada pada angka 1 detik untuk jenis serangan SYN flood, 2 detik untuk serangan DOS ICMP trace route dan 1 detik untuk Nmap scanning port.

c Sistem recovery berjalan dengan semestinya namun belum dapat dikatakan real-time(waktu proses <=1 detik). Kecepatan prosess *backup* pada saat recovery berada pada angka 42 detik untuk SYN flood attack, 23 detik untuk DOS ICMP traceroute, dan 17 detik untuk Nmap scanning port.

5.2 Saran

Adapun saran dari hasil penelitian ini denga adanya beberapa jenis serangan yang disimpulkan terdeteksi dengan tidak *realtime* dan penggunaan *resource* perangkat yang cukup besar maka untuk pengembangkan sistem ini oleh para pengembang / peneliti selanjutnya, untuk menggunakan mekanisme deteksi yang lebih efisien dan efektif guna mendapatkan waktu deteksi yang lebih cepat dan juga tepat serta rendah dalam penggunaan resource seperti CPU dan RAM pada perangkat dengan begitu sistem dapat bekerja dengan lebih baik.

DAFTAR PUSTAKA

Albin, E. and Rowe, N.C. (2012) 'A Realistic Experimental Comparison of the Suricata and Snort Intrusion-Detection Systems'. *Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012* 122–127

Azahari Mohd Yusof, M., Hani Mohd Ali, F., and Yusof Darus, M. (2018) 'Detection and Defense Algorithms of Different Types of DDoS Attacks'. *International Journal of Engineering and Technology* 9 (5), 410–444

Bhatnagar, D., Som, S., and Khatri, S.K. (2019) 'Advance Persistant Threat and Cyber Spying - The Big Picture, Its Tools, Attack Vectors and Countermeasures'. *Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019* 828–839

Cheng, Y.P. and Lin, J.M.C. (2008) 'Awk-Linux: A Lightweight Operating Systems Courseware'. *IEEE Transactions on Education* 51 (4), 461–467

Faiz, M. and Shanker, U. (2016) 'Data Synchronization in Distributed Client-Server Applications'. *Proceedings of 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016* (March), 611–616

Hakim, A.R., Rinaldi, J., and Setiadji, M.Y.B. (2020) 'Design and Implementation of NIDS Notification System Using WhatsApp and Telegram'. *2020 8th International Conference on Information and Communication Technology, ICoICT 2020* 3–6

Hawari Syarif, M. and Kurniawan Febry, I. (2016) 'PENERAPAN IPTABLES FIREWALL PADA LINUX DENGAN MENGGUNAKAN FEDORA Mizan Syarif Hawari Ibnu Febry Kurniawan Abstrak'. *Jurnal Manajemen Informatika. Volume 6 Nomor 1 Tahun 2016 198-207 PENERAPAN* 6, 198–207

Imam Prasetyo, Joko Triyono, D.A. (2016) *Jurnal JARKOM Vol . 4 No . 2 Desember 2016 ISSN : 2338-6313 SISTEM NOTIFIKASI AGENDA HARIAN MENGGUNAKAN APPLICATION PROGRAMMING INTERFACE (API) DAN SMS GATEWAY Jurnal JARKOM Vol . 4 No . 2 Desember 2016 ISSN : 2338-6313*. 4 (2), 38–47

ISO 707:2008 (2003) 'International Standard International Standard'. *61010-1 © Iec:2001* 2003, 13

Iswahyudi, C. (2017) *Implementasi Intrussion Detection System (IDS) Dengan Menggunakan Jejaring Sosial Sebagai Media Notifikasi*. (May)

MODUL AJAR ETHICAL HACKING (n.d.)

Nandi, S.K. (2018) 'MPTCP Performance with Various Configurations, Path Failures and Recovery'. *2018 3rd International Conference for Convergence in Technology, I2CT 2018* 1–6

NMAP (2022) *NMAP* [online] available from <https://nmap.org/>

Purbo, O.W. (n.d.) *Keamanan Jaringan Oleh*.

Rao, V. and Prema, K. V. (2020) 'Performing Real-Time Network Attacks on Smart Weather Monitoring Device Using Kali Linux'. *Proceedings of B-HTC 2020 - 1st IEEE Bangalore Humanitarian Technology Conference*

Rizal Fauzi, A. and Made Suartana, I. (2018) 'Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids'. *Jurnal Manajemen Informatika* 8 (2), 7

Rossheim, R.J. (1963) 'Report on Proposed American Standard Flowchart Symbols for Information Processing'. *Communications of the ACM* 6 (10), 599–604

Sahasrabudhe, S.S. and Sonawani, S.S. (2015) 'Comparing Openstack and VMware'. *2014 International Conference on Advances in Electronics, Computers and Communications, ICAECC 2014*

Sala, F., Schoeny, C., Bitouze, N., and Dolecek, L. (2016) 'Synchronizing Files from a Large Number of Insertions and Deletions'. *IEEE Transactions on Communications* 64 (6), 2258–2273

Satoshi, N., Mutsuo, S., and Katsuo, I. (2009) 'Realtime Network Backup to Existing Servers Based on Stackable Filesystem'. *Proceedings of the International Conference on Complex, Intelligent and Software Intensive Systems, CISIS 2009* (Figure 2), 415–420

Slameto, A.A. and Lukman, L. (2017) 'Penerapan Openssh Dan Bash Script Untuk Simultaneos Remote Access Client Pada Laboratorium Stmik Amikom Yogyakarta'. *Respati* 9 (27), 23–32

Stenberg, D. (2015) *Everything Curl Introduction*.

Sun, L., Du, H., and Hou, T. (2022) 'FR-DETR: End-to-End Flowchart Recognition With Precision and Robustness'. *IEEE Access* 10, 64292–64301

Suwanto, R., Ruslianto, I., and Diponegoro, M. (2019) 'Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website'. *Jurnal Komputer Dan Aplikasi* 07 (1), 97–107

Tabassum, M. and Mathew, K. (2014) 'Software Evolution Analysis of Linux (Ubuntu) OS'. *2014 International Conference on Computational Science and Technology, ICCST 2014* 2014

Vasconcelos, G., Carrijo, G., Miani, R., Souza, J., and Guizilini, V. (2016) 'The Impact of DoS Attacks on the AR.Drone 2.0'. *Proceedings - 13th Latin American Robotics Symposium and 4th Brazilian Symposium on Robotics, LARS/SBR 2016* (December), 127–132

Vishwakarma, A., Kumar, A., and Singh, G.K. (2016) 'Transmultiplexer Filter Bank Systems: A Research Overview'. *International Journal of Signal and Imaging Systems Engineering* 9 (3), 146–155

Vojnak, D.T., Eordevic, B.S., Timcenko, V. V., and Strbac, S.M. (2019) 'Performance Comparison of the Type-2 Hypervisor VirtualBox and VMWare Workstation'. *27th Telecommunications Forum, TELFOR 2019* 27–30

Vorontsov, M. and Radmir, S.I. (2021) 'Automation of Message Sending Processes Using Specialized Software'. *Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2021* 746–748

web Developer (n.d.) *Legion Sparta* [online] available from <https://www.kali.org/tools/legion/>

Widya Pradipta, Y. (2017) 'Implementasi Intrusion Prevention System (Ips) Menggunakan Snort Dan Ip Tables Berbasis Linux'. *Jurnal Manajemen Informatika. Volume 7 Nomor 1 Tahun 2017 21-28 IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX* 7 (1), 21–28

Www.Allitebooks.Com (n.d.)

Xi, J. (2011) 'A Design and Implement of IPS Based on Snort'. *Proceedings - 2011 7th International Conference on Computational Intelligence and Security, CIS 2011* 771–773

Yang, C., Tian, Y., Ma, D., Shen, S., and Mao, W. (2013) 'A Server Friendly File Synchronization Mechanism for Cloud Storage'. *Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCom 2013* (4), 314–316

Yasir, S.A. (2012) *Overhead Evaluation in Real-Time Network Intrusion Detection System Using Snort*. 1–12

LAMPIRAN

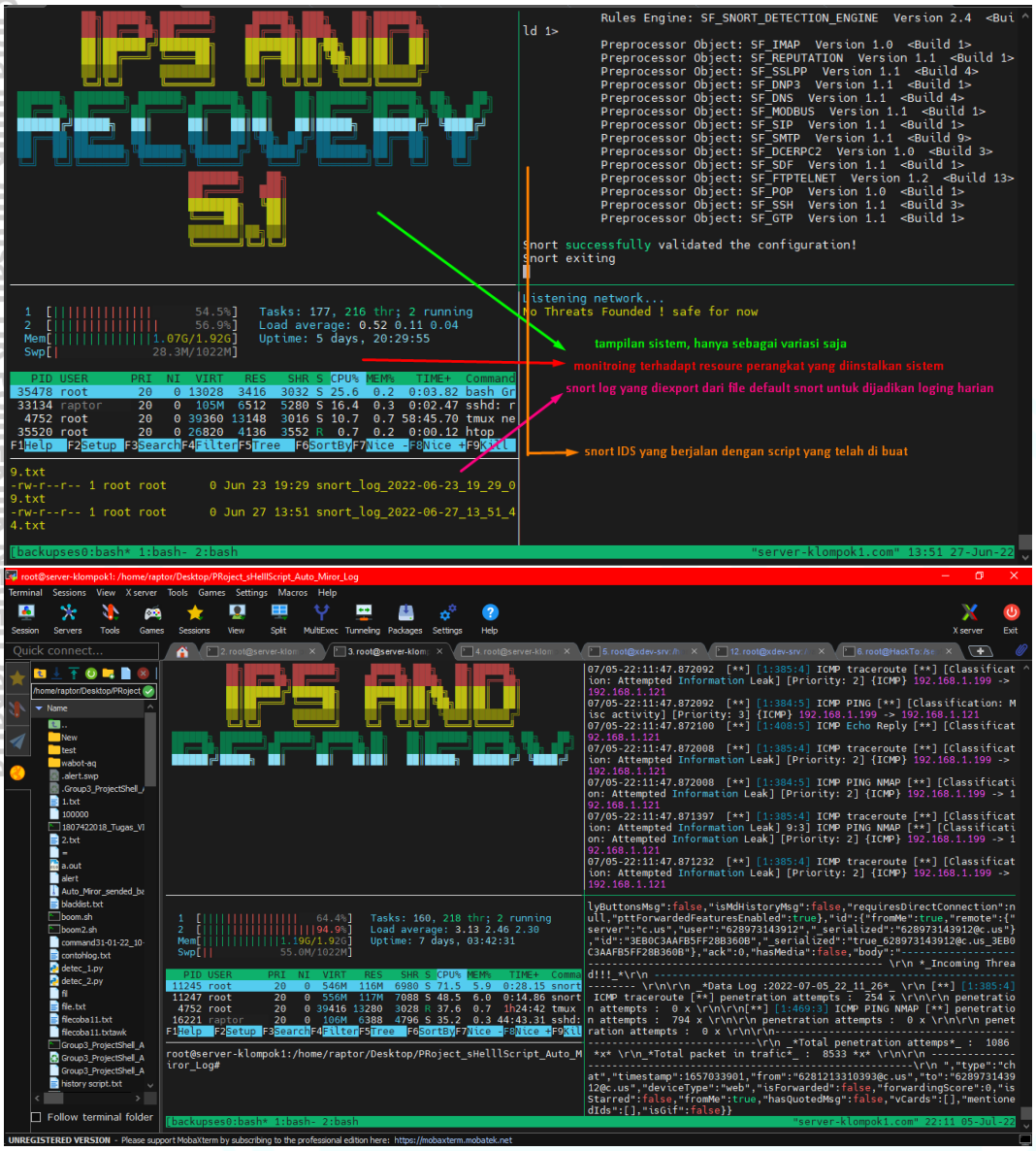
Lampiran- 1 Daftar Riwayat Hidup

DAFTAR RIWAYAT HIDUP

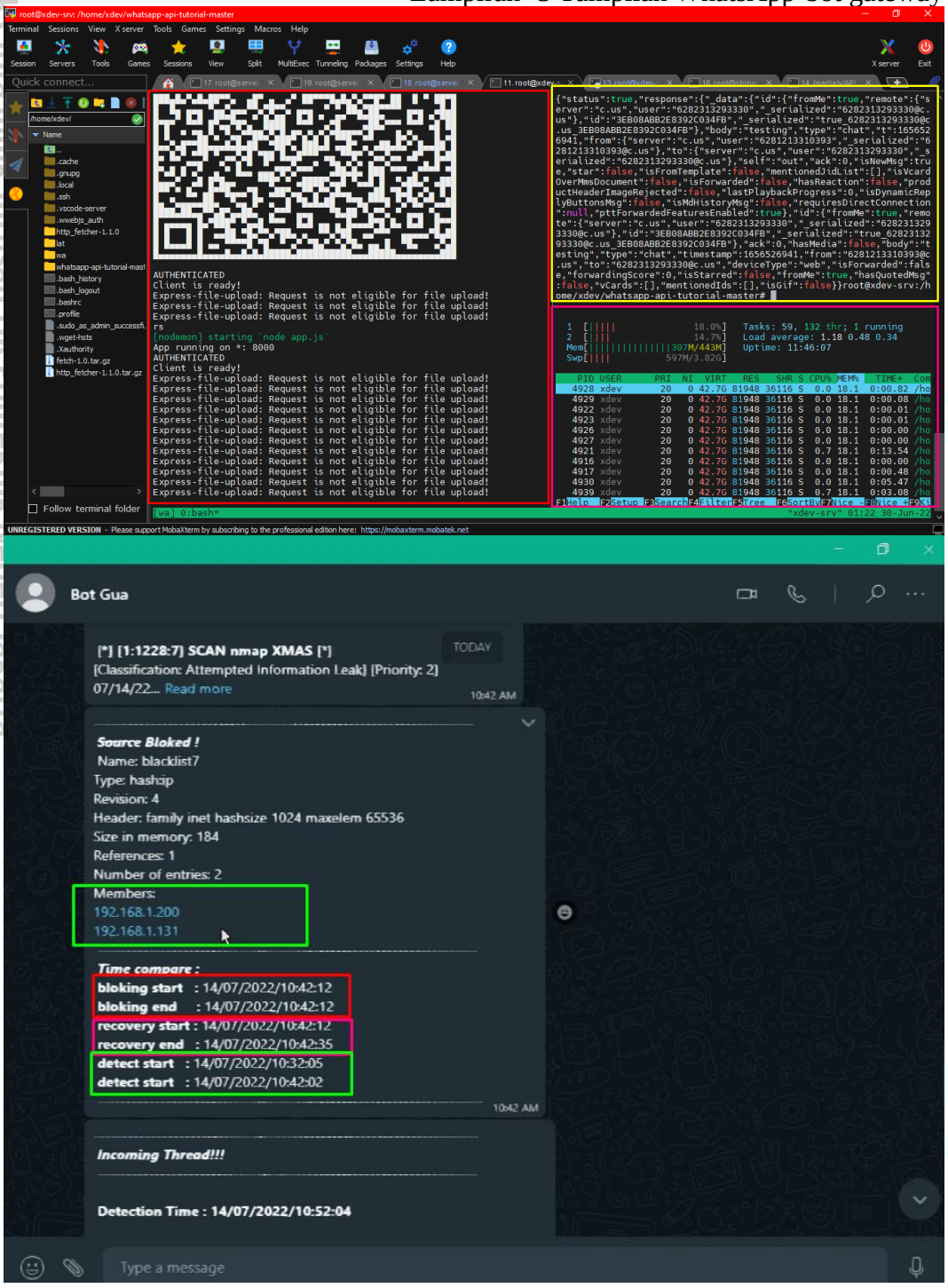
SEPTIAN HADI FAJAR , Depok 09-09-1999.

Menyelesaikan Pendidikan dari sekolah dasar 2011, SDN Sr.Sawah 07 Pagi. Lulus SMP 2014, SMPN 242 Jakarta Selatan. Melanjutkan Pendidikan ke SMAN 97 Jakarta Selatan lulus 2017. Mengikuti program *computer education* di *Continuing Education Program–Center for Computing and Information Technology Fakultas Teknik Universitas Indonesia* Lulus tahun 2019.

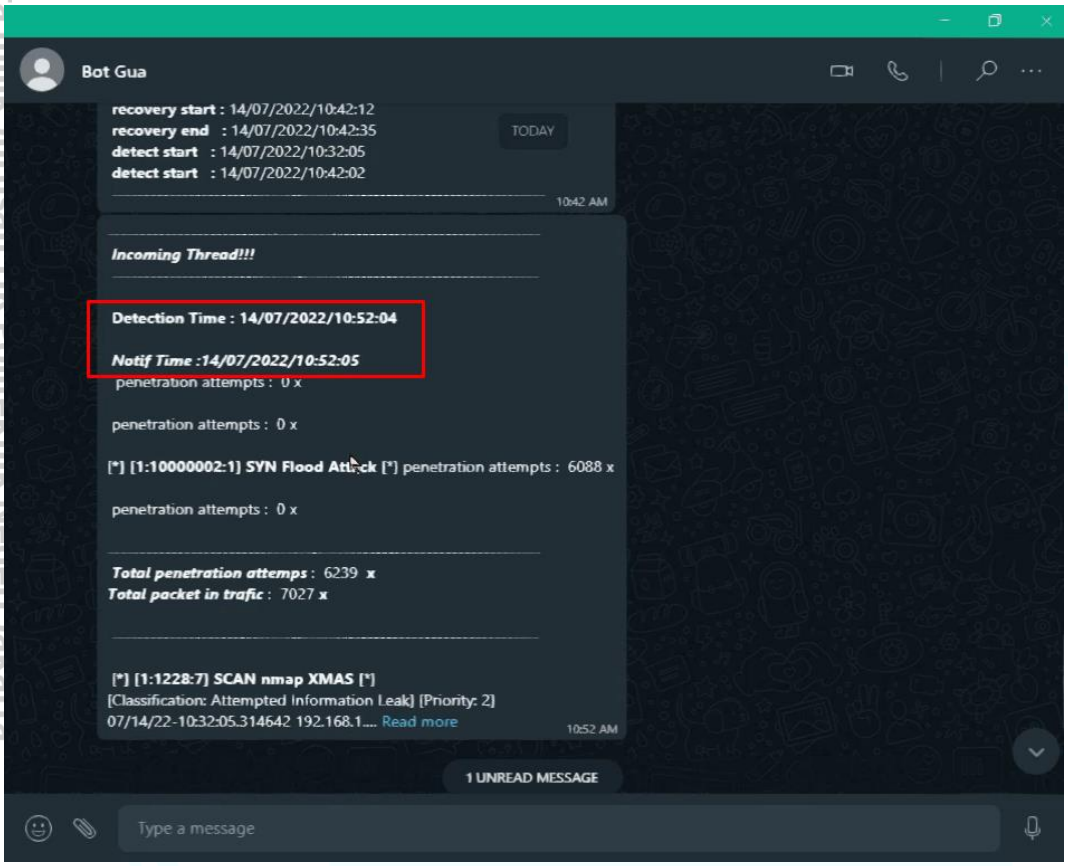
Lampiran- 2 Tampilan Sistem



Lampiran- 3 Tampilan WhatsApp-bot gateway



Lampiran- 4 Tampilan WhatsApp-bot gateway (Lanjutan)



```
#!/bin/bash

#prepare directory and initiation
> alert
> blacklist.txt
ipset restore -f ./ipset.conf
iptables-restore < ./iptables.rules
rm -f snort.log.* && rm -f alert.*
rm -f /var/log/snort/snort.log.*
#============================================
SESSION="IPS"

#create session
tmux -2 new-session -d -s $SESSION

#split pane
tmux split-window -h
tmux select-pane -t 1
tmux split-window -v
tmux select-pane -t 0
tmux split-window -v
tmux select-pane -t 1
tmux split-window -v
tmux resize-pane -t 0 -D 2
tmux resize-pane -t 1 -D 2

#send prosess
tmux send-key -t 3 C-z 'bash Group3_ProjectShell_Auto_Miror_Log.sh
snort_IDS' Enter
tmux send-key -t 4 C-z 'bash Group3_ProjectShell_Auto_Miror_Log.sh
search_' Enter
tmux send-key -t 0 C-z 'bash testNew.sh banner' Enter
tmux send-key -t 2 C-z 'bash Group3_ProjectShell_Auto_Miror_Log.sh
log_' Enter
tmux send-key -t 1 C-z htop Enter
#attach session
tmux -2 attach-session -t $SESSION
```

Lampiran- 6 Source code : Group3_ProjectShell_Auto_Miror_Log.sh

```
#!/bin/bash
#font collor
collorRed()
{(echo -en "\033[31;5;25;2m$string\033[0m\n")}
collorDefault()
{(echo -en "\033[0;0;0;0m$string\033[0m\n")}
collorYellowB()
{(echo -en "\033[33;5;25;1m$string\033[0m\n")}
collorBiruMuda()
{(echo -en "\033[36m$string\033[0m\n")}
collorPink()
{(echo -en "\033[31;5;25;1m$string\033[0m\n")}

#-----------------------------------------------------------------
Initiation-------------------------------------------------------------
--------
ipsetter="blacklist7"

#filter catagory
filter_catagory=("traceroute" "scan nmap xmas" "syn flood attack"
"OR sql injection")

#comparing file
comparing_file="alert"

#destination server
destination_server=("172.17.10.3" "172.17.10.2") # "192.168.87.225")

#host
conlink=("20.243.146.1" "192.168.1.100")

#destination user
destination_user=("xdev" "xdev") #"underscore")

#destination path
destination_path=("/var/RSYNC" "/var/RSYNC2")
#"/home/underscore/Desktop/backup"

#internet adapther
inet_adapter="eth0"

#backup data path
backup_data_path=("/home/raptor/Desktop/PRoject_sHelllScript_Auto_Mi
ror_Log")

#server sendiri
our_server="192.168.1.121"
```

Lampiran- 7 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
#wabot gateway
protocol=("http://")
number=("+628973143912" "+6281213310393")
data=("number" "message" "name" "fileUrl" "media")
port=("8007" "9999" "8005" "8000")
method=("-X POST")
target=("send-message" "send-group-message")

#wa number
wano="+62895379210030"

#bandwith Limit
limit="200m"

##fileCompress
j=0

#-----------------------------------------------------------------
function-------------------------------------------------------------
------
#Run Snort
snort_IDS()
{
    > $(pwd)/alert
    sudo snort -T -c /etc/snort/snort.conf -i $inet_adapter
    sudo snort -A full -l $(pwd) -y -q -c /etc/snort/snort.conf -i
$inet_adapter | sudo snort -A console -q -u snort -g snort -c
/etc/snort/snort.conf -i $inet_adapter
}

#notification
notif_()
{
detectime="Detection Time : $(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
grepoutput=""
localoutput=""
localpayload=""
totalthreat=0
if (( $(grep -i -c --ignore-case "classification" alert) < 500 ));
then

##localpayload
localpayload+=$(<$comparing_file)
   awk 'BEGIN { ORS="%0D%0A"; IFS="" } { print $0  } END { print
"\n"} ' $comparing_file > filecoba11.txt && value=`readarray -t
ARRAY < filecoba11.txt; IFS=''; echo "${ARRAY[*]}"`
```

Lampiran- 8 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
#=====================================================================
=====================================================================
for jk in "${filter_catagory[@]}";do localoutput+="$(grep --ignore-
case "$jk" $comparing_file | sort --unique)"" penetration attempts
:  ""$(grep --only-match -c --ignore-case "$jk" $comparing_file)"" x
\n\n" && ((totalthreat+=$(grep --only-match -c --ignore-case "$jk"
$comparing_file))); done
#=====================================================================
=====================================================================
   for jk in "${filter_catagory[@]}";do grepoutput+="$(grep --
ignore-case "$jk" $comparing_file | sort --unique)"" penetration
attempts :  ""$(grep --only-match -c --ignore-case "$jk"
$comparing_file)"" x %0D%0A%0D%0A" && ((totalthreat+=$(grep --only-
match -c --ignore-case "$jk" $comparing_file))); done
#=====================================================================
=====================================================================
localoutput+="-----------------------------------------------------
-------------\nTotal penetration attemps : "$totalthreat" x \nTotal
packet in trafic :  ""$(grep -c --ignore-case "classification"
$comparing_file)"" x \n\n"
#=====================================================================
=====================================================================


   grepoutput+="-----------------------------------------------------
---------------%0D%0A+_*Total penetration attemps*_ :
+"$totalthreat"+ *x* %0D%0A_*Total packet in trafic*_ :  ""$(grep -c
--ignore-case "classification" $comparing_file)"" *x* %0D%0A%0D%0A"
else
#=====================================================================
=====================================================================
for jk in "${filter_catagory[@]}";do localoutput+="$(grep --ignore-
case "$jk" $comparing_file | sort --unique)"" penetration attempts
:  ""$(grep --only-match -c --ignore-case "$jk" $comparing_file)"" x
\n\n" && ((totalthreat+=$(grep --only-match -c --ignore-case "$jk"
$comparing_file))); done
#=====================================================================
=====================================================================
   for jk in "${filter_catagory[@]}";do grepoutput+="$(grep --
ignore-case "$jk" $comparing_file | sort --unique)"" penetration
attempts :  ""$(grep --only-match -c --ignore-case "$jk"
$comparing_file)"" x %0D%0A%0D%0A" && ((totalthreat+=$(grep --only-
match -c --ignore-case "$jk" $comparing_file))); done
#=====================================================================
=====================================================================
localoutput+="-----------------------------------------------------
-------------\nTotal penetration attemps : "$totalthreat" x \nTotal
```

Lampiran- 9 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
packet in trafic :  ""$(grep -c --ignore-case "classification"
$comparing_file)"" x \n\n"
#=====================================================================
=====================================================================
   grepoutput+="-------------------------------------------------------
----------------%0D%0A+_*Total penetration attemps*_ :
+"$totalthreat"+ *x* %0D%0A_*Total packet in trafic*_ :  ""$(grep -c
--ignore-case "classification" $comparing_file)"" *x* %0D%0A%0D%0A"
fi

#---------------------------------------------------------------------
---------------------------------------------------------------------
## untuk loging ke curl wa
#awk 'BEGIN { ORS="%0D%0A"; IFS="" } { print $0  } END { print "\n"}
' $comparing_file > filecoba11.txt && value=`readarray -t ARRAY <
filecoba11.txt; IFS=''; echo "${ARRAY[*]}"`
######backup-Original#greping untuk value wa-main
######for jk in "${filter_catagory[@]}";do grepoutput+="$(grep --
ignore-case "$jk" alert | sort --unique)"" penetration attempts
:  ""$(grep -i -c --ignore-case "$jk" alert)""x%0D%0A%0D%0A"; done
#new#Greping untuk value wa-main
#for jk in "${filter_catagory[@]}";do grepoutput+="$(grep --ignore-
case "$jk" alert | sort --unique)"" penetration attempts :  ""$(grep
-i -c --ignore-case "$jk" alert)"" x %0D%0A%0D%0A"; done
#grepoutput+="-------------------------------------------------------
-------------%0D%0A_*Total penetration attempts*_ :  ""$(grep -i -c
--ignore-case "classification" alert)"" *x* %0D%0A%0D%0A"
#---------------------------------------------------------------------
---------------------------------------------------------------------
##greping untuk vallue wa-backup
#for i in "${filter_catagory[@]}";do
#grepoutput+="$(grep --ignore-case "${filter_catagory[$k]}"
$omparing_file | sort --unique)"" _*$i*_ penetration attempts
:  ""$(grep -ic --ignore-case "${filter_catagory[$k]}"
$comparing_file)""x%0D%0A"
#((k++))
#done
##greping untuk value wa-main
##for jk in "${filter_catagory[@]}";do grepoutput+="$(grep --ignore-
case "$jk" alert | sort --unique)"" penetration attempts :  ""$(grep
-i -c --ignore-case "$jk" alert)""x%0D%0A%0D%0A"; done
#curl -d "${data[0]}=${number[0]}&${data[1]}=----------------------
-----------------------------------------+%0D%0A+*_Incoming
Thread!!!_*%0D%0A+-----------------------------------------------------
-----------------+%0D%0A%0D%0A+*$detectime*+%0D%0A%0D%0A+_*Notif
Time :$(date +"%d/%m/%Y-[%H:%M:%S:%N]")*_+%0D%0A+$grepoutput+-------
-------------------------------------------------------------
```

Lampiran- 10 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
%0D%0A%0D%0A+$value" ${method[0]}
${protocol[0]}${conlink[0]}:${port[1]}/${target[0]}

##curl untuk wa
notifcontent="----------------------------------------------------------
--------------+%0D%0A+*_Incoming Thread!!!_*%0D%0A+-----------------
-------------------------------------------------
+%0D%0A%0D%0A+*$detectime*+%0D%0A%0D%0A+_*Notif Time :$(date
+"%d/%m/%Y-[%H:%M:%S:%N]")*_+%0D%0A+$grepoutput+--------------------
-----------------------------------------------%0D%0A%0D%0A+$value"
#=========================================================================
=========================================================================
localcontent="----------------------------------------------------------
--------------\nIncoming Thread!!!\n--------------------------------
-----------------------------------\n\n$detectime\n\nNotif Time
:$(date +"%d/%m/%Y-[%H:%M:%S:%N]")\n$localoutput--------------------
-----------------------------------------------\n\n$localpayload"

curl -d "${data[0]}=${number[0]}&${data[1]}=$notifcontent"
${method[0]} ${protocol[0]}${conlink[0]}:${port[1]}/${target[0]}
> ./filecoba11.txt

##local log
if (ls snort_log_\[$(date +"%F")\].txt 2>/dev/null); then echo "log
file for $(date +"%F") already exist !" ; else touch
./snort_log_[$(date +"%F")].txt ; fi
#touch ./snort_log_$(date +"%F").txt
#cat ./alert ./snort_log_$(date +"%F").txt &&
echo -e $localcontent"\n\n" >> ./snort_log_\[$(date +"%F")\].txt

##curl untuk tele
curl -g
"https://api.telegram.org/bot5194540635:AAHrrxlVOzF9T65KF3hB4BSdmfst
NT35fQk/sendMessage?chat_id=1140376054&text="+"_*Data Log :$(date
+"%F_%T" | tr ":" "_")*_%0D%0A$grepoutput+$value"
string="Notif terkirim... [$(date +"%F_%T" | tr ":" "_")] waktu
server"; collorPink
sleep 3s
clear
}
#bloking
blok_()
{
blokstart="$(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
#string="Trafic Sourece :";collorPink
#ipset create $ipsetter hash:ip
```

Lampiran- 11 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
#awk '!x[$4]++ {FS=" "} { if ( match($0,/[0-9]+\.[0-9]+\.[0-9]+\.[0-
9]+/)) { split(substr($0,RSTART,RLENGTH),map,".");if ( ( map[4] >
241 && map[4] < 243 ) ){ print substr($0,RSTART,RLENGTH) } } }'
snort_log_2021-12-24_09_44_15.txt



##string="Trafic Sourece :";collorPink
##ipset create $ipsetter hash:ip
##awk '!x[$4]++ {FS=" "} {
##if ( match($0,/[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+/))
##{
##  split(substr($0,RSTART,RLENGTH),map,".");
##  if (( map[4] > 121 && map[4] < 256 ))
##  {
##    print substr($0,RSTART,RLENGTH) > "blacklist.txt"
##  }
##}
##}' $comparing_file


##while read line ;do
###ipset add "$ipsetter" "$line"
##if ipset test $ipsetter $blackline;then echo "ipset entry already
exist! skip entry";else ipset add $ipsetter $line; fi
##clear
##string="Source : $line Listed";collorYellowB
##done < "blacklist.txt"

if iptables -C INPUT -m set --match-set $ipsetter src -j DROP;then
iptables -D INPUT -m set --match-set $ipsetter src -j DROP;iptables
-I INPUT -m set --match-set $ipsetter src -j DROP; blokend="$(date
+"%d/%m/%Y-[%H:%M:%S:%N]")"; bloked=$(ipset list $ipsetter);
scriptingSCP_;string="already bloked";collorPink;else iptables -I
INPUT -m set --match-set $ipsetter src -j DROP; blokend="$(date
+"%d/%m/%Y-[%H:%M:%S:%N]")"; bloked=$(ipset list $ipsetter);
scriptingSCP_; fi
#iptables -I INPUT -m set --match-set $ipsetter src -j DROP
ipset save > ./ipset.conf
iptables-save -c > ./iptables.rules
#clear
string="-----------------------------------------------------------
-"; collorPink
string="Source Bloked";collorYellowB
cat $(pwd)/blacklist.txt | sort --unique
> $(pwd)/blacklist.txt
sleep 1s
```

Lampiran- 12 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
#done < $comparing_file
#done
}

#log
log_()
{
while true; do
#cp $(pwd)/alert  $(pwd)/snort_log_$(date +"%F_%T" | tr ":" "_").txt
for i in {1..7};do find  . -name "snort_log_[2022-$(date '+%m')-
$(date '+%d' -d "$i day ago")].txt" -exec rm {} \;; done
string="$(ls -l snort_log_\[*\].txt)"; collorYellowB
sleep 5m
clear
done
}


##tamplian networrk safe
display_()
{
clear
string="Listening network..."; collorBiruMuda
string="No Threats Founded ! safe for now"; collorYellowB
}

#Detetcting
search_()
{
#sleep 10
detecstart="$(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
ipset create $ipsetter hash:ip
n=0
while true; do
display_
while read line ; do

if [[ $n -gt 3 ]];then
n=0
fi

#string="Trafic Sourece :";collorPink
#ipset create $ipsetter hash:ip
awk '!x[$4]++ {FS=" "} {
if ( match($0,/[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+/))
{
  split(substr($0,RSTART,RLENGTH),map,".");
```

Lampiran- 13 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
  if (( map[4] > 121 && map[4] < 256 ))
  {
    print substr($0,RSTART,RLENGTH) > "blacklist.txt"
  }
}
}' $comparing_file

while read ipline ; do
if ipset test $ipsetter $ipline;then
        clear
#> $(pwd)/blacklist.txt
#> $(pwd)/$comparing_file
    string="ipset entry already exist! skip entry"; collorPink
    display_
else
   display_
   #> $(pwd)/$comparing_file
   if grep -q --ignore-case --only-match "${filter_catagory[$n]}"
$comparing_file;then
    clear
    string="-------------------------------------------------------
--------"; collorRed
    string="Incoming threats !"; collorPink
    string="Trafic Sourece :";collorPink
    rm -f snort.log.* && rm -f alert.*
    ipset create $ipsetter hash:ip
    ipset add "$ipsetter" "$ipline"
    detecend="$(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
    notif_
    blok_

    string="-------------------------------------------------------
--------"; collorRed
   else
    string="not filter found"; collorPink
#> $(pwd)/blacklist.txt
rm -f snort.log.* && rm -f alert.*
#> $(pwd)/$comparing_file
   fi
fi
((n++))
done < "blacklist.txt"
((n++))
done < $comparing_file
search_
done
}
```

Lampiran- 14 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
#Backup adn compress

Backup()

{
#fileCompress
#com_data="Auto_Miror_sended_backup_from_$our_server_$(date +"%F_%T"
| tr ":" "_").tar.gz"
com_data="Auto_Miror_sended_backup_from_$our_server""$(date +"%F_%T"
| tr ":" "_").tar.gz"
#pwd
#ls
#read
    backup_temp="tempBack"
    rm -r $backup_temp
    mkdir $backup_temp && chmod a+r+w+x $backup_temp
    cd $backup_temp
#pwd
#ls
#read

    loop1=0
    for i in "${backup_data_path[@]}"; do
        #cp "${backup_data_path[$loop1]}" $(pwd)
        cp -r "${backup_data_path[$loop1]}" $(pwd)
        ((loop1++))
    done
#pwd
#ls
#read
    cd ..
#pwd
#ls
#read
    tar -czvf "$com_data" "$backup_temp" >&- 2>&-
#pwd
#ls
#read
}

#tranfer file
scriptingSCP_()
{
recoverystart="$(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
> $(pwd)/alert
string="-------------------------------------------------------------
----"; collorYellowB
```

Lampiran- 15 Source code : Group3_ProjectShell_Auto_Miror_Log.sh (Lanjutan)

```
string="Backuping $(du -sh) data..."; collorYellowB

Backup
loop=0
for i in "${destination_server[@]}";do
    #scp "$com_data"
${destination_user[$loop]}@$i:"${destination_path[$loop]}"

    rsync -e ssh -av -P --bwlimit=$limit --max-size=15360m --size-
only -zcu "$com_data"
${destination_user[$loop]}@$i:"${destination_path[$loop]}"
    ((loop++))
done
rm -f $com_data
rm -r $backup_temp
string="Backuping complete to..."; collorPink
string="-----------------------scp----------------------------------
-------"; collorYellowB
sleep 2s
clear
recoveryEnd="$(date +"%d/%m/%Y-[%H:%M:%S:%N]")"
timecomper="-------------------------------------------------------------
-----------+%0D%0A+*_~Source~ Bloked !_*+%0D%0A+$bloked+%0D%0A+-----
-------------------------------------------------------------
+%0D%0A+*_Time compare :_*+%0D%0A+*bloking start   :*
$blokstart+%0D%0A+*bloking end     :* $blokend+%0D%0A+*recovery
start :* $recoverystart+%0D%0A+*recovery end   :*
$recoveryEnd+%0D%0A+*detect start   :* $detecstart+%0D%0A+*detect
end   :* $detecend+%0D%0A+-----------------------------------------
-------------------------"

##local compare
localcomper="-------------------------------------------------------------
------------\nSource Bloked !\n$bloked\n-----------------------------
-------------------------------------\nTime compare :\nbloking
start   : $blokstart\nbloking end     : $blokend\nrecovery start :
$recoverystart\nrecovery end   : $recoveryEnd\ndetect start   :
$detecstart\ndetect end   : $detecend\n-----------------------------
-------------------------------------"

curl -d "${data[0]}=${number[0]}&${data[1]}=$timecomper"
${method[0]} ${protocol[0]}${conlink[0]}:${port[1]}/${target[0]}
echo -e $localcomper >> ./snort_log_\[$(date +"%F")\].txt
}

"$@"
```

Lampiran- 16 snort.conf : rules yang diaktifkan

```
##include $RULE_PATH/malware-other.rules
##include $RULE_PATH/malware-tools.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/local.rules
include $RULE_PATH/info.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/icmp-info.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/multimedia.rules
include $RULE_PATH/mysql.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/nntp.rules
include $RULE_PATH/pop2.rules
include $RULE_PATH/pop3.rules
include $RULE_PATH/other-ids.rules
include $RULE_PATH/p2p.rules
include $RULE_PATH/policy.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/telnet.rules
#------#include $RULE_PATH/oracle.rules
#include $RULE_PATH/os-linux.rules
##include $RULE_PATH/os-other.rules
##include $RULE_PATH/os-solaris.rules
```