PENGGUNAAN *SNORT* SEBAGAI SISTEM PENDETEKSI SERANGAN PADA JARINGAN MENGGUNAKAN NOTIFIKASI TELEGRAM (STUDI KASUS: DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN SUKABUMI)

SKRIPSI

SULTAN ALIF NUR IKHSAN
20200040046

FAKULTAS TEKNIK DAN DESAIN
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS NUSA PUTRA
2024

PENGGUNAAN *SNORT* SEBAGAI SISTEM PENDETEKSI SERANGAN PADA JARINGAN MENGGUNAKAN NOTIFIKASI TELEGRAM (STUDI KASUS: DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN SUKABUMI)

SKRIPSI

Ditujukan Untuk Memenuhi Salah Satu Syarat Dalam Menempuh
Gelar Sarjana Teknik Informatika

SULTAN ALIF NUR IKHSAN

20200040046

FAKULTAS TEKNIK DAN DESAIN
PROGRAM STUDI TEKNIK INFORMATIKA
UNIVERSITAS NUSA PUTRA

2024

PERNYATAAN PENULIS

JUDUL : PENGGUNAAN *SNORT* SEBAGAI SISTEM PENDETEKSI SERANGAN PADA JARINGAN MENGGUNAKAN NOTIFIKASI TELEGRAM (STUDI KASUS: DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN SUKABUMI)

NAMA : SULTAN ALIF NUR IKHSAN

NIM : 20200040046

"Saya menyatakan dan bertanggungjawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya saya sendiri kecuali cuplikan dan ringkasan yang masing masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain yang mengklaim bahwa Skripsi ini sebagai karyanya, yang disertai dengan bukti bukti yang cukup, maka saya bersedia untuk dibatalkan gelar Sarjana Komputer/Sarjana Teknik saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut".

Sukabumi, Juni 2024

Sultan Alif Nur Ikhsan

PENGESAHAN SKRIPSI

JUDUL : PENGGUNAAN *SNORT* SEBAGAI SISTEM PENDETEKSI SERANGAN PADA JARINGAN MENGGUNAKAN NOTIFIKASI TELEGRAM (STUDI KASUS: DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN SUKABUMI)

NAMA : SULTAN ALIF NUR IKHSAN

NIM : 20200040046

Skripsi ini telah diujikan dan dipertahankan di depan Dewan Penguji pada Sidang Skripsi tanggal 19 Juni 2024. Menurut pandangan kami, Skripsi ini memadai dari segi kualitas untuk tujuan penganugerahan gelar Sarjana Komputer (S.Kom)

Sukabumi, 19 Juni 2024

Pembimbing I

Anggun Fergina, M.Kom
NIDN. 0407029301

Pembimbing II

Zaenal Alamsyah, M.Kom
NIDN. 0409069602

Ketua Penguji

Muhammad Ikhsan Thohir, M.Kom
NIDN. 0415049302

Ketua Program Studi

Ir. Sonatri, S.T,M.Kom
NIDN. 0419128801

Plh. Dekan Fakultas Teknik, Komputer dan Desain

Ir. Paikun, ST., MT., IPM, ASEAN Eng
NIDN. 0402037401

Skripsi ini kutunjukan kepada

Ayahanda dan Ibunda tercinta,

dan Adiku tersayang

ABSTRAK

Keamanan jaringan menjadi sangat penting untuk melindungi individu, perusahaan, dan instansi dari ancaman seperti serangan siber, dan pencurian data. Oleh karena itu, memahami pentingnya keamanan jaringan sangat penting. Berdasarkan hasil wawancara, terdapat *server* di *Command Center* Kabupaten Sukabumi yang dikelola oleh DISKOMINFOSAN Kabupaten Sukabumi, *server* tersebut digunakan sebagai *server* aplikasi. Pada *server* tersebut belum memiliki sistem *monitoring* keamanan jaringan yang memberikan *alert* ketika terjadi percobaan penyerangan di *server* tersebut secara *realtime*. Salah satu cara untuk meningkatkan keamanan pada *server* tersebut adalah dengan menggunakan *Intrusion Detection System* (IDS). IDS adalah sistem yang dimaksudkan untuk mendeteksi aktivitas mencurigakan atau serangan pada jaringan. Salah satu tujuan utama IDS adalah untuk memberikan peringatan terhadap ancaman keamanan yang mungkin terjadi. *Snort* adalah salah satu *tools* IDS bersifat *open-source*. *Snort* dibuat untuk mengidentifikasi serangan jaringan dan memberikan peringatan secara *realtime* kepada *administrator* ketika mengidentifikasi perilaku atau pola serangan tertentu. Dalam penelitian ini penulis menggunakan metode pengembangan SPDLC . *Security Policy Development Life Cycle* (SPDLC) adalah sebuah metode pengembangan sistem yang berfokus pada keamanan jaringan. Setelah melakukan pengujian, dapat disimpulkan bahwa *Snort* dapat digunakan sebagai *IDS* yang dipasang di ubuntu *server* 22.04, dengan *rules* yang telah dibuat *Snort* dapat mendeteksi ketika ada yang mencoba *port scanning* ke *server* menggunakan *masscan* dan dapat mendeteksi *ping attack* yang ditujukan ke *server* secara *realtime*. Dengan *script* yang telah dibuat, *Snort* dapat mengirimkan *alert* kepada *network administrator* menggunakan telegram secara *realtime* agar *alert* tersebut dapat langsung ditinjaklanjuti.

Kata Kunci: Command Center, DISKOMINFOSAN Kab.Sukabumi, Intrusion Detection System *(IDS), Security Policy Development Life Cycles (SPDLC), Server, Snort, Telegram*

ABSTRACT

Network security has become very important to protect individuals, companies, and agencies from threats such as cyberattacks, and data theft. Therefore, understanding the importance of network security is essential. Based on the interview results, there is a server in the Sukabumi District Command Center managed by DISKOMINFOSAN Sukabumi District, the server is used as an application server. There is no network security monitoring system on the server to notify users in real time of attempted server attacks. Using an intrusion detection system is one method of strengthening server security (IDS). IDS is a system designed to identify potentially harmful behavior or network attacks. One of the main goals of IDS is to provide warnings against security threats that may occur. Snort is one of the open-source IDS tools. Snort was created to identify network attacks and provide realtime alerts to administrators when identifying certain behaviors or attack patterns. In this study the authors used the SPDLC development method. Security Policy Development Life Cycle (SPDLC) is a system development method that focuses on network security. After testing, it can be concluded that Snort can be used as an IDS installed on ubuntu server 22.04, with the rules that have been made Snort can detect when someone tries port scanning to the server using masscan and can detect ping attacks aimed at the server in real time. With the script that has been created, Snort can send alerts to network administrators using telegram in realtime so that these alerts can be followed up immediately.

***Key*words:** *Command Center, DISKOMINFOSAN Kab.Sukabumi, Intrusion Detection System (IDS), Security Policy Development Life Cycles (SPDLC), Server, Snort, Telegram*

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, berkat rahmat dan karunia-Nya penulis dapat menyelesaikan penulisan skripsi dengan judul "Penggunaan *Snort* Sebagai Sistem Pendeteksi Serangan Pada Jaringan Menggunakan Notifikasi Telegram (Studi Kasus: DISKOMINFOSAN Kab.Sukabumi) ". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana Komputer di Program Studi Teknik Informatika Universitas Nusa Putra. Penyusunan skripsi ini dilakukan dengan tujuan untuk meningkatkan keamanan jaringan *server* di *Command Center* Kab. Sukabumi yang dikelola oleh DISKOMINFOSAN Kab. Sukabumi. Sehubungan dengan itu penulis menyampaikan penghargaan dan ucapan terima kasih yang sebesar-besarnya kepada :

1. Orang tua dan keluarga yang selalu memberikan doa, semangat dan perhatian atas apapun yang sedang penulis lakukan.
2. Bapak Dr. Kurniawan.,ST, M. Si, MM Rektor Universitas Nusa Putra Sukabumi
3. Kepala Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi Bapak Somantri, S.T., M.Kom.
4. Dosen Pembimbing I Ibu Anggun Fergina, M. Kom yang telah memberikan dorongan, saran dan bimbingan yang sangat berharga bagi penulis.
5. Dosen Pembimbing II Bapak Zaenal Alamsyah, M. Kom atas bimbingan, arahan dan pengajarannya yang luar biasa selama proses penulisan skripsi ini.
6. DISKOMINFOSAN Kab. Sukabumi yang telah membantu penulis dalam proses pengumpulan data.
7. Lulu Ayu Indriani seabagai *support system* yang telah membersamai selama masa penulisan skripsi.
8. Rekan –rekan mahasiswa Teknik Informatika 2020 yang selalu memberikan dukungan kepada penulis agar dapat menyelesaikan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu kritik dan saran yang membangun dari berbagai pihak sangat kami harapakan demi perbaikan. *Aamin Yaa Rabbal 'Alamiin*.

Sukabumi, Juni 2024

Sultan Alif Nur Ikhsan

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik UNIVERSITAS NUSA PUTRA, saya yang bertanda tangan di bawah ini:

Nama	: Sultan Alif Nur Ikhsan
NIM	: 20200040046
Program Studi	: Teknik Informatika
Jenis Karya	: Tugas Akhir

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Nusa Putra **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

"PENGGUNAAN *SNORT* SEBAGAI SISTEM PENDETEKSI SERANGAN PADA JARINGAN MENGGUNAKAN NOTIFIKASI TELEGRAM (STUDI KASUS: DISKOMINFOSAN KAB. SUKABUMI)"

beserta perangkat yang ada (jika diperlukan). Dengan hak bebas royalti noneksklusif ini Universitas Nusa Putra berhak menyimpan, mengalih media/format- kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Sukabumi
Pada tanggal : Juni 2024

Yang menyatakan

Sultan Alif Nur Ikhsan

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dinas Komunikasi Informatika dan Persandian (DISKOMINFOSAN) Kab. Sukabumi adalah salah satu lembaga ditingkat pemerintahan daerah yang bertugas untukmengelola infrastruktur tekno*log*i informasi pemerintah daerah, yang mencakup pengembangan sistem informasi, manajemen data, dan keamanan data. Adapun bagian dari Dinas Komunikasi Informatika dan Persandian yakni *Command Center* Kab. Sukabumi. *Command Center* merupakan pusat pengendalian atau pemantauan yang mengkoordinasikan berbagai kegiatan atau informasi dari berbagai sumber.

Kemajuan tekno*log*i telah menimbulkan tantangan keamanan yang signifikan. Keamanan jaringan menjadi sangat penting untuk melindungi individu, perusahaan, dan instansi dari ancaman seperti serangan siber, dan pencurian data. Oleh karena itu, memahami pentingnya keamanan jaringan sangat penting. Menurut Laporan Tahunan *Monitoring* Keamanan Siber 2021, Badan Siber dan Sandi Negara (BSSN) mencatat 1.637.973.022 trafik anomali dengan 242.066.168 anomali tertinggi pada bulan Desember, 264 kasus phishing, 5.940 kasus web defacement dengan 727 kasus tertinggi pada bulan Maret di Indonesia [1]. Berdasarkan hasil wawancara, terdapat *server* di *Command Center* Kabupaten Sukabumi yang dikelola oleh DISKOMINFOSAN Kabupaten Sukabumi, *server* tersebut digunakan sebagai *server* aplikasi. Pada *server* tersebut belum memiliki sistem *monitoring* keamanan jaringan yang memberikan *alert* ketika terjadi percobaan penyerangan di *server* tersebut secara *realtime*.

Salah satu cara untuk meningkatkan keamanan pada *server* tersebut adalah dengan menggunakan *Intrusion Detection System* (IDS). IDS adalah sistem yang dimaksudkan untuk mendeteksi aktivitas mencurigakan atau serangan pada jaringan atau sistem komputer [2]. Salah satu tujuan IDS adalah untuk memberikan peringatan terhadap ancaman keamanan yang mungkin terjadi. *Snort* adalah salah satu *tools* IDS bersifat *open-source*. *Snort* dibuat untuk

mengidentifikasi serangan jaringan dan memberikan peringatan secara *realtime* kepada *administrator* atau sistem keamanan ketika mengidentifikasi perilaku atau pola serangan tertentu [3].

Berdasarkan latar belakang tersebut penulis ingin melakukan penelitian dengan judul **"Penggunaan *Snort* Sebagai Sistem Pendeteksi Serangan pada Jaringan Menggunakan Notifikasi Telegram (Studi Kasus: DISKOMINFOSAN Kab. Sukabumi)"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, masalah penelitian ini dapat dirumuskan sebagai berikut:

a. Bagaimana penggunaan *Snort* sebagai *Intrusion Detection System* (IDS) untuk mendeteksi serangan?
b. Bagaimana Telegram dapat mengirimkan notifikasi pada saat terjadi serangan?
c. Bagaimana melakukan penyerangan menggunakan *port scanning* dan *ping attack* terhadap *server*?

1.3 Batasan Masalah

Adapun batasan-batasan pada penelitian ini yaitu :

a. Menggunakan *tools Snort* sebagai *Intrusion Detection System* (IDS).
b. *Intrusion Detection System* (IDS) akan diterapkan di *virtual private server*.
c. *Virtual private server* hanya memberikan dua layanan, yaitu SSH *Server* dan Web *Server*.
d. Serangan yang digunakan pada penelitian ini adalah *port scanning* dan *ping attack.*
e. Ruang lingkup pengujian terbatas hanya pada jaringan di *Command Center* yangdikelola oleh Dinas Komunikasi Informatika dan Persandian Kab. Sukabumi.
f. Menggunakan metode *Security Policy Development Life Cyle* (SPDLC).
g. Menggunakan telegram sebagai media notifikasi.

1.4 Tujuan Penelitan

Adapun tujuan penelitian ini adalah untuk menggunakan *Snort* sebagai *Intrusion Detection System* (IDS) dalam mendeteksi serangan pada jaringan server di *Command Center* yang dikelola oleh DISKOMINFOSAN Kabupaten Sukabumi dan mengirimkan notifikasi atau *alert* kepada *administrator* melalui telegram.

1.5 Manfaat Penelitian

Adapun manfaat yang penulis harapkan dari penelitian ini adalah sebagai berikut:

1. Bagi Penulis
   a. Mengaplikasikan ilmu mengenai kemanan jaringan yang telah dipelajari Universitas Nusa Putra Sukabumi.
   b. Menambah wawasan baru terkait kemanan jaringan.
2. Bagi Tempat Penelitian

   Diharapkan mampu meningkatkan kemanan jaringan di *Command Center* yang dikelola oleh DISKOMINFOSAN Kabupaten Sukabumi.

1.6 Sistematika Penelitian

Untuk membuat analisis dan pemahaman yang lebih mudah bagi pembaca, penulis membagi penulisan ke dalam 5 (lima) bab dengan sistematika sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini akan membahas serta menguraikan latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini akan membahas dan menjelaskan penelitian yang relevan, gagasan-gagasan yang menjadi landasan teori, dan kerangka pemikiran.

BAB III : METODO*LOG*I PENELITIAN

Pada bab ini akan membahas tentang metode penelitian, metode pengumpulan data, dan metode pengembangan sistem.

BAB IV : HASIL DAN PEMBASAHAN

Pada bab ini akan membahas mengenai hasil dan pembahasaan yang dilakukan selama penelitian.

BAB V : PENUTUP

Pada bab ini akan membahas mengenai kesimpulan dan saran terkait hasil penelitian.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, maka diambil kesimpulan sebagai berikut :

1. Pengujian telah menunjukkan bahwa *Snort*, ketika di*install* pada *server* Ubuntu, dapat digunakan sebagai *Intrusion Detection System*. Dengan *rules* yang telah dibuat. *Snort* dapat mendeteksi ketika ada yang mencoba *port scanning* ke *server* menggunakan *masscan* dan dapat mendeteksi *ping attack yang* ditujukan ke *server* secara *realtime*.
2. Telegram dapat mengirimkan notifikasi dengan *script bash shell* yang telah dibuat. *Script bash shell* akan digunakan agar telegram bot dapat terhubung dengan *Snort*, kemudian membaca *log* serangan yang berjalan di IDS *Snort* dan mengirimkan pemberitahuan ketika terjadi serangan kepada *Network Administrator* melalui telegram.
3. Penyerangan menggunakan *port scanning* dan *ping attack* dilakukan pada terminal yang ada di sistem operasi kali linux, dengan perintah "*masscan* -p0-500 –rate 100 *ip address*", maka *masscan* akan melakukan pemindaian pada port 0 – 500 dengan kecepatan 100 paket/detik *ke ip address server*. Dengan perintah "*ping ip address*", akan mengirim ping atau paket ICMP tanpa henti ke alamat *ip address server*.

5.2 Saran

Setelah kesimpulan diuraikan, kelebihan dan kekurangan di atas dapat digunakan sebagai pelajaran dan referensi untuk ke depannya. Adapaun saran dari penelitian ini yaitu, perlu menambahkan *rules-rules* yang lain agar *Snort* dapat mendeteksi lebih banyak jenis serangan dan juga menggunakan *ip table* pada *firewall* agar serangan tersebut dapat dihentikan.

DAFTAR PUSTAKA

[1] M. Y. Samad and Pratama Dahlian Persadha, "Memahami Perang Siber dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Siber," *J. IPTEKKOM J. Ilmu Pengetah. Teknol. Inf.*, vol. 24, no. 2, pp. 135–146, 2022, doi: 10.17933/iptekkom.24.2.2022.135-146.

[2] I. A. S. Dewi Paramitha, G. M. A. Sasmita, and I. M. S. Raharja, "Analisis Data *Log* IDS *Snort* dengan Algoritma Clustering Fuzzy C-Means," *Maj. Ilm. Teknol. Elektro*, vol. 19, no. 1, p. 95, 2020, doi: 10.24843/mite.2020.v19i01.p14.

[3] H. Awal, "Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan *Snort* Dan Iptables Berbasis Linux," *J. Sains Inform. Terap.*, vol. 2, no. 1, pp. 38–44, 2023, doi: 10.62357/jsit.v2i1.184.

[4] P. H. Putra, "Implementasi *Log* Management Server Menggunakan Elk (Elastic Implementasi *Log* Management Server Menggunakan Elk (Elastic Search , *Log*stash Dan *Kibana*) Stack Pada Server Web *Snort* Di Pt . Xyz," *J. Inform. Sunan Kalijaga*, vol. 4, no. April, pp. 1–8, 2020.

[5] M. Z. Pratama and A. Putra, "Penerapan Sistem Keamanan Intrusion Detection System *Snort* Pada Jaringan Diskominfo Kabupaten Oki," *Pros. Semin. Has. ...*, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/semhavok/article/view/2452%0Ahttps://conference.binadarma.ac.id/index.php/semhavok/article/download/2452/983

[6] D. Yuliandari, B. K. Raja, R. Ningsih, and A. J. Wahidin, "Simulasi Penerapan Sistem Monitoring Jaringan *Snort* NIDS Pada Web Server Menggunakan Metode SPDLC," vol. 5, no. 2, pp. 133–138, 2023.

[7] T. Purnama, Y. Muhyidin, and D. Singasatia, "Implementasi Intrusion Detection System (Ids) *Snort* Sebagai Sistem Keamanan Menggunakan Whatsapp Dan Telegram Sebagai Media Notifikasi," *J. Teknol. Inf. Dan Komun.*, vol. 14, no. 2, pp. 358–369, 2023, doi: 10.51903/jtikp.v14i2.726.

[8] I. C. Utomo, P. S. Informatika, and U. M. Surakarta, "Implementation of IDS Using *Snort* with Barnyard2 Visualization for *Network* Monitoring in The Informatics Engineering Computer Lab at Muhammadiyah University Surakarta," vol. 04, no. 04, pp. 165–171, 2023.

[9] F. Riza, "Sistem Deteksi Intrusi pada Server secara Realtime Menggunakan Seleksi Fitur dan Firebase Cloud Messaging," *J. Sistim Inf. dan Teknol.*, vol. 5, pp. 7–9, 2022, doi: 10.37034/jsisfotek.v5i1.161.

[10] A. Nugraha and D. A. Gustian, "Deteksi Malware Dridex Menggunakan Signature-based *Snort*," *Indones. J. Comput. Sci.*, vol. 10, no. 1, pp. 54–64, 2022, doi: 10.33022/ijcs.v10i1.3068.

[11] G. Tambunan and M. IGN, "Implementasi Keamanan Ids / Ips Dengan *Snort*

Dan IP Tables pada Server," *Semin. Nas. Mhs. Ilmu Komput. dan Apl. Jakarta-Indonesia, 28 Januari 2020 IMPLEMENTASI*, pp. 10–16, 2020.

[12] L. Shuai and S. Li, "Performance optimization of *Snort* based on DPDK and Hyperscan," *Procedia Comput. Sci.*, vol. 183, no. 2018, pp. 837–843, 2021, doi: 10.1016/j.procs.2021.03.007.

[13] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, "Implementasi Keamanan Jaringan Menggunakan Port Knocking," *J. Janitra Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 90–95, 2022, doi: 10.25008/janitra.v2i2.156.

[14] M. A. Husna and P. Rosyani, "Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix yang Terintegrasi dengan Grafana dan Telegram," *JURIKOM (Jurnal Ris. Komputer)*, vol. 8, no. 6, p. 247, 2021, doi: 10.30865/jurikom.v8i6.3631.

[15] A. Yudhistira and Y. Fitrisia, "Monitoring *Log* Server Dengan *Elasticsearch*, *Log*stash Dan *Kibana* (Elk)," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 124–134, 2023, doi: 10.36341/rabit.v8i1.2975.

[16] H. Khotimah, F. Bimantoro, and R. S. Kabanga, "Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat," *J. Begawe Teknol. Inf.*, vol. 3, no. 2, pp. 213–219, 2022, doi: 10.29303/jbegati.v3i2.752.

[17] A. Setiyawan, A. Pinandito, and W. Purnomo, "Pengembangan Sistem Informasi *Log* Management Server Monitoring Menggunakan ELK (Elastic Search, *Log*stash dan *Kibana*) Stack pada Aplikasi Padichain di PT. Bank Rakyat Indonesia," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 5, pp. 2142–2151, 2023, [Online]. Available: http://j-ptiik.ub.ac.id

[18] M. K. Anam, D. Sudyana, A. Noviciatie, and N. Lizarti, "Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru J-PEMAS STMIK Amik Riau," *http//jurnal.sar.ac.id/index.php/J-PEMAS Optim.*, vol. vol 1, no. 2, pp. 37–44, 2020.

[19] S. Informasi, U. Merdeka, M. Jalan, T. Dieng, and N. Klojen, "Implementasi Honeypot Dionaea Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan," no. September, pp. 3807–3817, 2023.

[20] A. Fergina, M. I. Setia, M. Yusuf, and ..., "Analisis Monitoring Sistem Keamanan Jaringan Komputer menggunakan *Software* NMAP (Studi Kasus Jaringan di Universitas Nusa Putra)," *... Ilmu Komput. ...*, 2023, [Online]. Available: http://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/view/45%0Ahttp://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/download/45/41

[21] I. K. K. A. Marta, I. N. B. Hartawan, and I. K. S. Satwika, "Analisis Sistem Monitoring Keamanan Server Dengan Sms Alert Berbasis *Snort*," *Inser. Inf. Syst. Emerg. Technol. J.*, vol. 1, no. 1, p. 25, 2020, doi: 10.23887/insert.v1i1.25874.

[22] D. K. Hakim and S. A. Nugroho, “Implementasi Telegram Bot untuk Monitoring Mikrotik Router,” *Sainteks*, vol. 16, no. 2, pp. 151–157, 2020, doi: 10.30595/st.v16i2.7132.

[23] M. Waruwu, “Pendekatan Penelitian Pendidikan: Metode Penelitian Kualitatif, Metode Penelitian Kuantitatif dan Metode Penelitian Kombinasi (Mixed Method),” *J. Pendidik. Tambusai* , vol. 7, no. 1, pp. 2896–2910, 2023.

[24] M. Mukmin, P. Purnawansyah, and M. Hasnawi, “Notifikasi Bot Telegram Untuk Monitoring Jaringan Pada Kementrian Kelautan Dan Perikanan Untia,” *Bul. Sist. Inf. dan Teknol. Islam*, vol. 3, no. 2, pp. 127–133, 2022, doi: 10.33096/busiti.v3i2.1162.

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS