31/S/TEKKOM-KCBR/PK.03.08/16/AGUSTUS/2024

IMPLEMENTASI APLIKASI SNORT PADA SISTEM KEAMANAN *SERVER* DENGAN NOTIFIKASI TELEGRAM

SKRIPSI

diajukan untuk memenuhi sebagian syarat
untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

oleh
Muhamad Hisyam Nugraha Solihin
NIM 2009397

PROGRAM STUDI TEKNIK KOMPUTER
KAMPUS UPI DI CIBIRU
UNIVERSITAS PENDIDIKAN INDONESIA

2024

HALAMAN HAK CIPTA

IMPLEMENTASI APLIKASI SNORT PADA SISTEM KEAMANAN *SERVER* DENGAN NOTIFIKASI TELEGRAM.

oleh
Muhamad Hisyam Nugraha Solihin
NIM 2009397

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Komputer

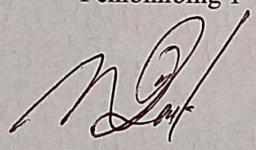
HALAMAN PENGESAHAN SKRIPSI

MUHAMAD HISYAM NUGRAHA SOLIHIN

IMPLEMENTASI APLIKASI SNORT PADA SISTEM KEAMANAN *SERVER* DENGAN NOTIFIKASI TELEGRAM

Disetujui dan Disahkan Oleh Pembimbing,

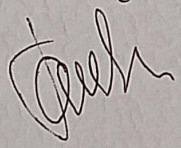
Pembimbing 1



Wirmanto Suteddy, S.T., M.T.

NIP. 920200819830521101

Pembimbing 2

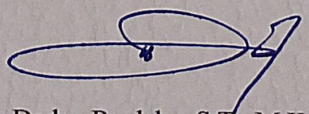


Muhammad Taufik Dwi Putra, S.Tr.Kom., M.T.I.

NIP. 920200819940117101

Mengetahui,

Ketua Program Studi Teknik Komputer



Deden Pradeka, S.T., M.Kom.

NIP. 920200419890816101

HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi dengan judul "Implementasi Aplikasi Snort Pada Sistem Keamanan *Server* dengan Notifikasi Telegram" ini beserta seluruh isinya adalah benar benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung risiko/sanksi apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Agustus 2024

Yang membuat pernyataan

Muhamad Hisyam Nugraha Solihin

NIM. 2009397

HALAMAN UCAPAN TERIMAKASIH

Puji dan syukur penulis panjatkan kehadirat Allah SWT, karena berkat rahmat dan karunia-Nyalah penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Aplikasi Snort Pada Sistem Keamanan *Server* dengan Notifikasi Telegram". Adapun maksud dan tujuan dari penulisan ini adalah untuk memenuhi salah satu syarat untuk mengikuti sidang skripsi, Jurusan Teknik Komputer, Universitas Pendidikan Indonesia Kampus UPI di Cibiru.

Selama penelitian dan penulisan skripsi ini banyak sekali hambatan yang penulis alami, namun berkat bantuan, dorongan serta bimbingan dari berbagai pihak, akhirnya skripsi ini dapat terselesaikan dengan baik. Oleh sebab itu, dengan segala kerendahan hati dan penuh rasa hormat, penulis bermaksud menyampaikan terima kasih kepada:

1. Kedua Orang Tua dirumah yang senantiasa memberikan dukungan baik moral maupun material, serta selalu memberikan do'a setiap harinya untuk penulis sehingga dapat menyelesaikan tugas akhir skripsi ini.
2. Bapak Deden Pradeka, S.T., M.Kom., selaku Ketua Program Studi Teknik Komputer. Saya sangat menghargai waktu dan perhatian yang bapak berikan dalam membantu saya mengembangkan pengetahuan dan keterampilan di bidang Teknik Komputer. Terima kasih atas semua nasihat dan dorongan yang bapak berikan, yang telah berperan besar dalam perkembangan diri saya.
3. Bapak Wirmanto Suteddy, S.T., M.T., selaku dosen pembimbing pertama atas bimbingan, dukungan, dan ilmu yang telah Bapak berikan selama proses penyusunan tugas akhir ini, karena tanpa arahan dan nasihat bapak, saya tidak akan dapat menyelesaikan penelitian ini dengan baik. Saya sangat menghargai kesabaran dan dedikasi bapak dalam membimbing saya, serta semua masukan berharga yang telah membantu saya tumbuh sebagai seorang akademisi.

4. Bapak Muhammad Taufik, S.Tr.Kom., M.T.I., selaku dosen pembimbing kedua atas segala bimbingan dan dukungan yang telah diberikan selama proses penelitian ini. Bapak telah memberikan banyak wawasan yang sangat berharga, yang membantu saya menyelesaikan tugas akhir ini dengan baik. Saya sangat menghargai kesabaran Bapak dalam menjawab setiap pertanyaan saya. Terima kasih atas semua dukungan dan kepercayaan yang bapak berikan, yang telah memotivasi saya untuk terus belajar dan berkembang.
5. Bapak dan Ibu Dosen Program Studi Teknik Komputer serta seluruh civitas akademika Universitas Pendidikan Indonesia yang telah memberikan segala kebaikan dan jasa selama masa perkuliahan. Semoga segala kebaikan dan jasa yang telah berikan mendapatkan balasan yang setimpal.
6. Teman-teman dari aceng team yang beranggotakan, Aceng, Uda lemon, Aldi, Ajay, Ardi, Aduy, Dondi, Jarwo, Tengku, Aca, Cei, Mang Hek dan Wira yang telah menjadi sahabat seperjuangan dalam menjalani perkuliahan di Teknik Komputer.
7. Kepada teman-teman, seluruh mahasiswa Teknik Komputer angkatan 2020, yang telah menjadi sahabat dan saudara selama masa perkuliahan ini. Terima kasih atas segala dukungan, kebersamaan, dan kenangan yang telah kita ciptakan bersama. Tanpa kalian, perjalanan ini tidak akan sama. Kalian adalah keluarga pilihan yang selalu ada dalam suka dan duka. Semoga persahabatan kita terus erat dan membawa kita ke masa depan yang gemilang. Terima kasih atas segalanya.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan, sehingga sangat diharapkan masukan dan kritik dari berbagai pihak untuk perbaikan di masa mendatang. Sekali lagi, saya mengucapkan terima kasih dan mohon maaf yang sebesar-besarnya jika terdapat kesalahan. Semoga penelitian ini memberikan manfaat bagi para pembaca.

IMPLEMENTASI APLIKASI SNORT PADA SISTEM KEAMANAN *SERVER* DENGAN NOTIFIKASI TELEGRAM

Muhamad Hisyam Nugraha Solihin
2009397

ABSTRAK

Perkembangan zaman saat ini telah memasuki era digitalisasi. kegiatan industri maupun instansi pemerintahan berubah dari cara konvensional ke sistem digital. Perkembangan ini mempermudah pekerjaan dan pelayanan yang diberikan pun semakin baik dan cepat, namun dari banyaknya manfaat yang didapat terdapat juga ancaman yang bisa terjadi apabila sistem digital ini diterapkan diberbagai sektor terutama ancaman serangan siber yang akan mengancam *server*. Oleh karena itu perlu dibuat sistem keamanan yang bisa mendetsksi dan mencegah serangan siber tersebut sebelum menghabiskan sumber daya *server*. Beberapa penelitian dilakukan dengan berbagai macam teknik dan *tools* yang digunakan sebagai keamanan *server*. Dalam penelitian ini snort digunakan sebagai sistem keamanan *server* untuk mendeteksi dan mencegah serangan yang masuk ke *server*. Pada penelitian ini menggunakan metodologi *Network Development Life Cycle* (NDLC), metode tersebut dipilih dengan tujuan mengimplementasikan snort dan melakukan evaluasi terhadap kinerja snort dalam mendeteksi serangan siber. Pesan serangan di integrasikan dengan notifikasi telegram lalu akan dikirimkan ke administrator jaringan dengan tujuan mempercepat penanganan serangan siber. Hasil penelitian yang dilakukan adalah snort dapat mendeteksi serangan siber yang terjadi lalu mengirimkan notifikasi serangan tersebut melalui telegram agar penanganan serangan bisa cepat dilakukan. Selain itu, snort berhasil mendeteksi dan memblokir ip dari penyerang sesuai dengan *rules* yang telah dibuat. Percobaan dilakukan sebanyak 30 kali dan menghasilkan waktu pendeteksian serangan rata-rata 1 detik serta akurasi pendeteksian sebesar 100%.

Kata Kunci: Snort, Telegram, Serangan Siber, *Server*

SNORT APPLICATION IMPLEMENTATION ON SERVER SECURITY SYSTEM WITH TELEGRAM NOTIFICATION

Muhamad Hisyam Nugraha Solihin

2009397

ABSTRACT

The current era has entered a phase of digitalization, where industrial activities and government institutions are shifting from conventional methods to digital systems. industrial activities and government agencies are changing from conventional methods to digital systems. This development makes work easier and the services provided are getting better and faster, but of the many benefits obtained there are also threats that can occur if this digital system is implemented in various sectors, especially the threat of cyber attacks that will threaten the server. Therefore, it is necessary to create a security system that can detect and prevent these cyber attacks before consuming server resources. Several studies have been conducted with various techniques and tools used as server security. In this study, snort is used as a server security system to detect and prevent attacks that enter the server. In this study using the Network Development Life Cycle (NDLC) methodology, the method was chosen with the aim of implementing snort and evaluating snort's performance in detecting cyber attacks. Attack messages are integrated with telegram notifications and then sent to network administrators with the aim of speeding up the handling of cyber attacks. The results of the research conducted are snort can detect cyber attacks that occur and then send notifications of the attack via telegram so that handling of attacks can be done quickly. In addition, snort successfully detects and blocks the ip of the attacker according to the rules that have been made. The experiment was conducted 30 times and resulted in an average attack detection time of 1 second and detection accuracy of 100%.

Keywords: Snort, Telegram, Cyber Attack, Server

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Adam Zukhruf, Bagus Fatkhurrozi, & Andriyatna Agung Kurniawan. (2023). Comparative Study Of Distributed Denial Of Service (DDOS) Attack Detection In Computer Network. *Jurnal Teknik Informatika (Jutif)*, *4*(5), 1033–1039. https://doi.org/10.52436/1.jutif.2023.4.5.756

Agus Eka Pratama, I. P., & Mega Handayani, N. K. (2019). Implementasi IDS Menggunakan Snort Pada Sistem Operasi Ubuntu. *Jurnal Mantik Penusa*, *3*(1), 176–181. www.snort.org

Akbar Wisnu Nadyanto, M., & Varriel Avenazh Nizar, M. (2021). Membangun Mail Server Berbasis Linux Menggunakan iRedMail. *JUITIK*, *1*(1), 1–8. http://journal.sinov.id/index.php/juitik/indexHalamanUtamaJurnal:https://journal.sinov.id/index.php

Akis, M., & Pebriyanto, E. (2019). Penerapan Server Web Hosting Berbasis Linux Ubuntu pada Jaringan Komputer SD Negeri 15 Pangkalpinang. *Jurnal SISFOKOM*, *2*(2), 40–46.

Alfazry, M. R., Fadilah, F., Putra, A. P., & Setiawan, A. (2024). Perlindungan Keamanan Website NextCloud: Mengatasi Serangan DoS dengan Konfigurasi Firewall pada Ubuntu. *Journal of Internet and Software Engineering*, *1*(3), 1–11. https://doi.org/10.47134/pjise.v1i3.2639

Aprilyano Ekklesia Tangkowit, Verry Ronny Palilingan, & Olivia Eunike Selvie Liando. (2021). Analisis dan Perancangan Jaringan Komputer Di Sekolah Menengah Pertama. *Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, *1*, 69–82.

Ardi, N., Putra Pratama, S., & Servanda, Y. (2024). Analisis Serangan Forensik Terhadap Serangan Ddos Ping Of Death Menggunakan Tools Nmap Dan Hping3. *Jurnal Jurnal Sains Dan Teknologi (JSIT)*, *4*(2), 2807–7393. http://jurnal.minartis.com/index.php/jsit

Ariyadi, T., Saputra, E., Tio Farizky, M., & Artikel, R. (2023). Analisis Paket ICMP Website Universitas Binadarma Menggunakan Wireshark. *Jurnal Ilmiah Teknik dan Ilmu Komputer*, *2*(2), 55–60. https://doi.org/10.55123

Arlinta Christy Barus, Johannes Harungguan, & Efren Manulu. (2021). Pengujian API Website Untuk Performansi Aplikasi DITENUN. *Journal of Applied Technology and Informatics*, *1*(3), 14–21.

Auliafitri, D., RizkiSuro, E., Malik, M. R. M., & Setiawan, A. (2024). Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit. *Journal of Internet and Software Engineering*, *1*(3), 12. https://doi.org/10.47134/pjise.v1i3.2620

Bayu Rendro, D., Ngatono, & Nugroho Aji, W. (2020). Analisi Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP (Studi Kasus Di SMK Negri 1 Kota Serang). *PROSISKO*, *7*(2), 108–115.

Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review. *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK)*, *7*(2), 60–70.

CNN Indonesia. (2024, Juni 3). *Indonesia Digempur 6 Juta Ancaman Siber di Awal 2024 Modusnya*. CNN Indonesia. Diakses pada 20 Agustus 2024 https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya

Damar, A. M. (2020, Maret 13). *Kata Pengamat Soal Serangan DDoS ke Situs Pemantauan Virus Corona Pemprov Jakarta - Tekno Liputan6.com*. liputan 6. https://www.liputan6.com/tekno/read/4200786/kata-pengamat-soal-serangan-ddos-ke-situs-pemantauan-virus-corona-pemprov-jakarta

Desma Mahendra, D., & Sisilia Mukti, F. (2022). Sistem Deteksi dan Pengendalian Serangan Denial of Service pada Server Berbasis Snort dan Telegram-API Detection and Control System of Denial of Service Attack on Server Based on Snort and Telegram-API. *Techno*, *21*(3), 511–522.

Fernando, N., Humaira, & Asri, E. (2020). Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. *Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4), 121–126. http://jurnal-itsi.org

Gilang Citra Lenardo, Yuda Irawan, & Herianto. (2020). Pemanfaatan Bot Telegram Sebagai Media Informasi Akademik di STMIK Hang Tuah Pekanbaru (Utilization of Telegram Bot as Academic Information Media at STMIK Hang Tuah Pekanbaru). *Jurnal Teknologi Informasi dan Multimedia*, *1*(4), 351–357.

Hanipah, R., & Dhika, H. (2020). Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark. *Journal of Computer and Information Technology*, *4*(1), 11–23. http://e-journal.unipma.ac.id/index.php/doubleclickTelepon:

Harsono, H. (2022). Faktor-Faktor Yang Mempengaruhi Sistem Berbasis Komputer: Sistem Operasi, Server, dan Programer. *Jurnal Manajemen Pendidikan dan Ilmu Solsial*, *3*(2). https://doi.org/10.38035/jmpis.v3i2

Heri Yanto, & Febrihadi. (2020). Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Berbasis Sms Alert. *Jurnal KomtekInfo*, *7*(2), 159–170. https://doi.org/10.35134/komtekinfo.v7i2

Indra Borman, R., Syahputra, K., & Prasetyawan, P. (2019). Implementasi Internet Of Things pada Aplikasi Monitoring Kereta Api dengan Geolocation Information System. *teknik elektro*, *2*, 322–327.

Lukman, & Melati Suci. (2020). Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache. *Jurnal Teknologi Informasi*, *15*(2), 6–15.

Nanda Hasyim. (2019). Network Security Threatscape-Introduction: Lesson 2: DoS Attacks, Spoofing, Smurf Attacks, and Phishing. *Jurnal Sains dan Teknologi*, *3*(2), 1–5.

Natanael Christianto, & Wiwin Sulistyo. (2021). Model Pemantauan Keamanan Jaringan Melalui Aplikasi Telegram Dengan Snort. *Jurnal Teknik Informatika dan Sistem Informasi*, *7*(3), 2443–2229. https://doi.org/10.28932/jutisi.v7i1.4088

Oluwatosin, H. S. (2019). Client-Server Model. *IOSR Journal of Computer Engineering*, *16*(1), 57–71. https://doi.org/10.9790/0661-16195771

Pitriyanti, M., Khairani Daulay, N., & Agus Syamsul Arifin, M. (2023). Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort. *Kajian Ilmiah Informatika dan Komputer*, *3*(4), 323–329. https://djournals.com/klik

Riska, P., Sugiartawan, P., & Wiratama, I. (2019). Sistem Keamanan Jaringan Komputer Dan Data Dengan Menggunakan Metode Port Knocking. *Jurnal Sistem Informasi dan Komputer Terapan Indonesia (JSIKTI)*, *1*(2), 53–64. https://doi.org/10.33173/jsikti.12

Risky, M. A. Z., & Yuhandri, Y. (2021). Optimalisasi dalam Penetrasi Testing Keamanan Website Menggunakan Teknik SQL Injection dan XSS. *Jurnal Sistim Informasi dan Teknologi*, *3*(4), 215–220. https://doi.org/10.37034/jsisfotek.v3i4.68

Sanjaya, T., & Setiyadi, D. (2019). Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. *JURNAL MAHASISWA BINA INSANI*, *4*(1), 1–10.

Shafiyyah, A., Nama, G. F., & Pradipta, R. A. (2024). Implementasi Wazuh Menggunakan Metode PPDIOO Di Sistem Keamanan Jaringan PSDKU Universitas LAmpung Waykanan Sebagai Deteksi dan Respon Serangan Siber. *Jurnal Informatika dan Teknik Elektro Terapan*, *12*(2), 970–982. https://doi.org/10.23960/jitet.v12i2.4074

TEMPO. (2023, Mei 17). *7 Fakta Dugaan Serangan Ransomware oleh LockBit ke BSI - Berita Utama - koran.tempo.co*. Diakses pada 21

Agustus 2024. https://koran.tempo.co/read/berita-utama/482085/7-fakta-dugaan-serangan-ransomware-oleh-lockbit-ke-bsi

Ubaidillah, U., Taryo, T., & Hindasyah, A. (2023). Analisis dan Implementasi Honeypot Honeyd Sebagai Low Interaction Terhadap Serangan Distributed Denial Of Service (DDOS) dan Malware. *JTIM : Jurnal Teknologi Informasi dan Multimedia*, *5*(3), 208–217. https://doi.org/10.35746/jtim.v5i3.405

Widya Astuti, A., Sayudin, & Muharam, A. (2023). Perkembangan Bisnis Di Era Digital. *Jurnal Multidisiplin Indonesia*, *2*(9), 2787–2792. https://jmi.rivierapublishing.id/index.php/rp

Yusup, M., Affandi, A., Riyanto, D., Pratomo, I., & Kusrahardjo, G. (2022). *Review Paper Design and Implementation Fast Response System Monitoring Server Using Simple Network Management Protocol (SNMP)*.

A. Affandi, D. Riyanto, I. Pratomo and G. Kusrahardjo, (2015). Design and implementation fast response system monitoring server using Simple Network Management Protocol (SNMP). International Seminar on Intelligent Technology and Its Applications (ISITIA), 2(3), 385-390, doi: 10.1109/ISITIA.2015.7220011.