MODIFIKASI SISTEM MONITORING KEAMANAN LOCAL AREA NETWORK BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SURABAYA

PROYEK AKHIR

Oleh:
INDRA AL-RASYID CANDRAWIMBA
NIT: 30221010

PROGRAM STUDI DIPLOMA 3 TEKNIK NAVIGASI UDARA
POLITEKNIK PENERBANGAN SURABAYA
2024

MODIFIKASI SISTEM MONITORING KEAMANAN LOCAL AREA NETWORK BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SURABAYA

PROYEK AKHIR

Diajukan sebagai Syarat untuk Mendapatkan Gelar Ahli Madya (A.Md.) pada
Program Studi Diploma 3 Teknik Navigasi Udara

Oleh:
INDRA AL-RASYID CANDRAWIMBA
NIT: 30221010

PROGRAM STUDI DIPLOMA 3 TEKNIK NAVIGASI UDARA
POLITEKNIK PENERBANGAN SURABAYA
2024

LEMBAR PERSETUJUAN

MODIFIKASI SISTEM MONITORING KEAMANAN *LOCALAREA NETWORK BERBASIS* NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SIJRABAYA

Oleb:
INDRAAL-RASY ID CANDRAWfMBA
NIT. 30221010

Disetujui untuk diujikan pada :
Surabaya, 04 Juli 2024

Pembimbing I : NYARIS PAMBUDIYATNO, S.SiT., MMTr
NIP . 19820525 200502 I 001

Pembimbing II : BA.MBANG BAGUS.H, S.SiT.. M1, MT
NIP. 19810915 200502 1001

LEMBAR PENGESAHAN

MODIFIKASI SISTEM MONITORING KEAMANAN LOCAL AREA NETWORK BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PE NERBANGAN SURABAYA

Oleb.
INDRA AL-RASYID CANDRAWIMBA
NIT 30221010

Telah dipertahankan dan dinyatakan lulus pada Ujian Proyek Akhir
Program Pendidikan Diploma 3 Teknik Navigasi Udara
Polileknik Penerbangan Surabaya
Pada tanggal: 04 Juli 2024

Pamtia Penguji

I. Ketua · Dr. YUYUN SUPRAPTO, S SiT, Mtvi
NIP. 19820107 200502 2 001

2 Sekretaris ARGO PRAGOLO, ST.
NIK 10011243

3. Anggota · NYARISPAMBUDIYATNO, S.SiT., MMtr
NIP 19820525 200502 I 001

Ketua Program Studi
D3 Teknik Navigasi Udara

NYARI pAMBUDIYATNO. S SIT MMtr
NIP 19820525 200502 I 00 I

MOTTO DAN PERSEMBAHAN

MOTTO :

"Jika Anda berani melihat ke dalam diri Anda sendiri, Anda akan menemukan harta karun yang lebih besar daripada yang lain di luar"
(Maulana Jalaluddin Rumi)

PERSEMBAHAN :

Allah SWT yang telah melimpahkan rahmat dan hidayahNya.
Baginda Nabi Muhammad SAW yang telah memperjuangkan segalanya hingga terasa nikmatnya saat ini.
Orangtua yang tercinta, untuk setiap do'a yang selalu dipanjatkan,serta dukungan di setiap langkah saya, tanpa mereka saya bukanlah siapa-siapa.
Para pembimbing yang telah membimbing saya.
Teman teman saya yang selalu memberikan dukungannya dan menemani selama perkuliahan ini.

PERNYATAAN KEASLIAN DAN HAK CIPTA

Saya yang bertanda tangan di bawah ini :

Nama	: Indra Al-Rasyid Candrawimba
NIT	30221010
Program Studi	: D3 Teknik Navigasi Udara
Judul Proyek Akhir	: Modifikasi Sistem Monitoring Keamanan Local Area Network Berbasi Notifikasi Telegram Dengan Snort dan Honeypot Di Politeknik Penerbangan Surabaya

dengan ini menyatakan bahwa :

1. Proyek Akhir ini merupakan karya asli dan belum pernah diajukan untuk mendapatkan gelar akademik. baik di Politeknik Penerbangan Surabaya maupun di Perguruai1 Tinggi lain, serta dipublikasikan, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengaI1 disebutkan nama pengarang dan dicaI1tumkan dalam daftar pustaka.

2. Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan Hak Bebas Royaliti Non Eksklusif (Non-Exclusive Royalty-Free Right) kepada Politeknik Penerbangan Surabaya beserta pe.rangkat yang ada Gika diperlukan). Dengan hak ini, Politeknik Penerbangan Surabaya berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalaI1 data (database), merawat, dan mempublikasikan proyek akhi.r saya dengan tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pemyataan ini saya buat dengan sebenarnya. Apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran, maka saya bersedia menerima sanksi akademik berupa pencabutan gelaryang telah diperoleh, serta sanksi lainnya sesuai dengan nonna yang berlaku di Politeknik Penerbangan Surabaya

Surabaya, 4 Juli 2024

Yang membuat pemyataan

Indra AlRasyid Candrawimba

NIT. 30221010

KATA PENGANTAR

Puji syukur atas segala rahmat dan karunia Tuhan Yang Maha Esa, proyek Akhir yang berjudul "**MODIFIKASI SISTEM MONITORING KEAMANAN *LOCAL AREA NETWORK* BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SURABAYA**" dapat diselesaikan dengan baik sebagai syarat untuk menyelesaikan program Diploma 3 Teknik Navigas Udara Angkatan 14 di Politeknik Penerbangan Surabaya.

Ucapan terimakasih penulis sampaikan atas bantuan, bimbingan dan pengarahan dari berbagai pihak selama proses penyusunan Proyek Akhir kepada:

1. Bapak Bapak Ahmad Bahrawi, S.E., M.T. Selaku Direktur Politeknik Penerbangan Surabaya.
2. Bapak Nyaris Pambudiyatno, S.SiT., M.MTr. Selaku Ketua Program Studi Diploma 3 Teknik Navigasi Udara dan Dosen Pembimbing Proyek Akhir.
3. Bapak Bambang Bagus Hariyanto, S.SiT., MM., MT. Selaku Dosen Pembimbing Penulisan Proyek Akhir.
4. Segenap dosen, instruktur, dan pegawai Politeknik Penerbangan Surabaya.
5. Bapak Agus Santoso dan Ibu Mia Novianti selaku orang tua saya, yang tak henti-hentinya memberikan doa, ridho, restu serta bantuan secara materi maupun dukungan moral untuk kelancaran Proyek Akhir ini.
6. Rekan-rekan Teknik Navigasi Udara Angkatan 14 dan rekan-rekan dari prodi lainnya yang telah membantu, serta memberi dukungan hingga terselesaikannya Proyek Akhir ini.
7. Seseorang spesial dan tersayang yang telah meluangkan waktu, tenaga, dan pikiran untuk menemani penulisan Proyek Akhir ini.
8. Semua pihak yang telah memberikan dukungan sehingga penulis dapat menyelesaikan pendidikan di Politeknik Penerbangan Surabaya.

Penulis memohon maaf apabila dalam penulisan Proyek Akhir ini masih terdapat kekurangan dan jauh dari kesempurnaan. Penulis juga mengharapkan kritik dan saran yang membangun demi pengembangan Proyek Akhir ini untuk lebih baik lagi.

Surabaya, 2024

Indra AlRasyid Candrawimba
NIT. 30221010

ABSTRAK

MODIFIKASI SISTEM MONITORING KEAMANAN LOCAL AREA NETWORK BERBASIS NOTIFIKASI TELEGRAM DENGAN SNORT DAN HONEYPOT DI POLITEKNIK PENERBANGAN SURABAYA

Berkembangnya teknologi pada era ini menciptakan dampak positif yang signifikan terutama dalam bidang networking, yang ditandai dengan kemajuan tools dan fitur yang semakin kompleks. Perkembangan ini, meskipun memudahkan pengguna untuk mengakses internet, juga membuka peluang luas bagi kejahatan siber atau *cybercrime*. Pada tahun 2015, Indonesia menempati peringkat kedua dalam serangan siber, menunjukkan kerentanan dan kemudahan dieksplotasi oleh para hacker. Ransomware WannaCry menyerang komputer di 150 Negara pada tahun 2017. Pada tahun 2022, tercatat 8.831 kasus terkait kejahatan siber, dengan 12,74 juta akun mengalami kebocoran data. Serangan siber seperti *port scanning, brute force attack, phising, denial of service* (DoS), *malware*, dan lainnya menjadi ancaman yang tidak dapat diabaikan.

Saat ini, sebagian besar pendidikan dilakukan secara online, menunjukkan bahwa teknologi internet memegang peran penting dari operasional instansi. Politeknik Penerbangan Surabaya merupakan salah satu kampus yang menggunakan teknologi cloud computing atau teknologi komputer yang menggunakan internet sebagai medianya. Pada penelitian ini penulis akan membahas desain penelitian yang digunakan dalam eksperimen keamanan jaringan. Penelitian ini menggunakan pendekatan penelitian dan pengembangan (R&D) dengan model ADDIE, dan fokusnya adalah mengembangkan dan menerapkan sistem keamanan jaringan menggunakan metode NIDPS *(Network Intrusion Detection and Prevention System)* yang menggunakan perangkat lunak Snort dan Honeypot.

Hasil dari penelitian yang dilakukan menunjukkan bahwa monitoring dan sistem keamanan jaringan dapat bekerja dalam mendeteksi aktifitas anomali pada jaringan. Selain itu, dapat terintregasi dengan aplikasi Telegram dalam mengirimkan notifikasi alert Snort menggunakan bot Telegram. Dalam penelitian ini juga ada evaluasi untuk penambahan fitur fail2ban untuk memblokir serangan serta performa jaringan yang kurang maksimal dalam mengirimkan notifikasi ke Telegram.

Kata kunci : Kejahatan siber, cloud computing, keamanan jaringan, NIDPS, Snort, Honeypot.

ABSTRACT

MODIFICATION OF THE LOCAL AREA NETWORK SECURITY MONITORING SYSTEM BASED ON TELEGRAM NOTIFICATION WITH SNORT AND HONEYPOT AT AVIATION POLYTECHNIC SURABAYA

The development of technology in this era has created a significant positive impact, especially in the field of networking, which is characterized by the advancement of increasingly complex tools and features. This development, while making it easier for users to access the internet, also opens up vast opportunities for cybercrime. In 2015, Indonesia ranked second in cyberattacks, demonstrating the vulnerability and ease of exploitation by hackers. The WannaCry ransomware attacked computers in 150 countries in 2017. In 2022, 8,831 cases related to cybercrime were recorded, with 12.74 million accounts experiencing data leakage. Cyber attacks such as port scanning, brute force attacks, phishing, denial of service (DoS), malware, and others are threats that cannot be ignored.

Today, most education is conducted online, indicating that internet technology plays an important role in agency operations. Politeknik Penerbangan Surabaya is one of the campuses that uses cloud computing technology or computer technology that uses the internet as a medium. In this study the authors will discuss the research design used in network security experiments. This research uses a research and development (R&D) approach with the ADDIE model, and the focus is on developing and implementing a network security system using the NIDPS (Network Intrusion Detection and Prevention System) method using Snort and Honeypot software.

The results of the research conducted show that the monitoring and network security system can work in detecting anomalous activities on the network. In addition, it can be integrated with the Telegram application in sending Snort alert notifications using Telegram bots. In this research there is also an evaluation for the addition of fail2ban features to block attacks and network performance that is less than optimal in sending notifications to Telegram.

Keywords *: Cybercrime, cloud computing, network security, NIDPS, Snort, Honeypot.*

DAFTAR ISI

Halaman

PROYEK AKHIR i
LEMBAR PERSETUJUAN ii
LEMBAR PENGESAHAN iii
MOTTO DAN PERSEMBAHAN iv
PERNYATAAN KEASLIAN DAN HAK CIPTA v
KATA PENGANTAR vi
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR GAMBAR xi
DAFTAR TABEL xii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Sistematika Penulisan 4
BAB 2 LANDASAN TEORI 5
2.1 Kajian Teori 5
2.1.1 Jaringan internet 5
2.1.2 (Intusion Detection and Prevention System) IDPS 6
2.1.3 Forensik Jaringan 6
2.1.4 Snort 7
2.1.5 Rules Snort 8
2.1.6 Honeypot 8
2.1.7 Linux 9
2.1.8 ADDIE 10
2.1.9 Monitoring Keamanan jaringan 11
2.1.10 Telegram 11
2.1.11 Quality of Service (QoS) 12

2.2 Kajian Penelitian Terdahulu 14
BAB 3 METODE PENELITIAN 17
3.1 Desain Penelitian 17
3.2 Perancangan Sistem 18
3.3 Waktu dan Tempat Penelitian 20
BAB 4 HASIL DAN PEMBAHASAN 21
4.1 Analisis 21
4.2 Design 22
4.3 Development 24
4.4 Impelentation 31
4.5 Evaluation 34
BAB 5 KESIMPULAN DAN SARAN 35
5.1 Kesimpulan 35
5.2 Saran 36
DAFTAR PUSAKA 37

DAFTAR GAMBAR

Gambar 2. 1 Topologi Star 5
Gambar 2. 2 IDPS 6
Gambar 2. 3 Mode Paket Snort 7
Gambar 2. 4 Bagian Rules Snort 8
Gambar 2. 5 Model ADDIE 10
Gambar 2. 6 Logo Aplikasi Telegram 12
Gambar 3. 1 Infrastruktur Jaringan 17
Gambar 4. 1 Setting IP Address server yang dilindungi 23
Gambar 4. 2 Setting IP Address server yang dilindungi 25
Gambar 4. 3 Penyesuaian IP Address 25
Gambar 4. 4 Cek proses snort 26
Gambar 4. 5 Snort telah berjalan 26
Gambar 4. 6 api_id dan api_key dari honeydb 27
Gambar 4. 7 Mengatur log serangan 27
Gambar 4. 8 Mengatur layanan yang dijadikan tiruan 28
Gambar 4. 9 Honeydb telah berjalan 28
Gambar 4. 10 Pembuatan Bot API Telegram 29
Gambar 4. 11 Pembuatan Bot API Telegram 29
Gambar 4. 12 Pembuatan Bot API Telegram 29
Gambar 4. 13 Pembuatan Bot API Telegram 29
Gambar 4. 14 Skrip bot telegram 30
Gambar 4. 15 chat_id dan token bot telegram 30
Gambar 4. 16 bot Telegram terhubung dengan Snort 30
Gambar 4. 17 Log serangan pada Snort 31
Gambar 4. 18 Alert terkirim melalui bot Telegram 31
Gambar 4. 19 Log serangan pada server Honeydb 32
Gambar 4. 20 Alert yang terkirim pada bot Telegram 32

DAFTAR TABEL

Tabel 2. 1 Kategori Throughtput..... 12
Tabel 2. 2 Kategori Delay (Latency) 13
Tabel 2. 3 Kategori Jitter..... 13
Tabel 2. 4 Kategori Packet Loss 14
Tabel 2. 5 Kajian Penelitian Terdahulu 14
Tabel 3. 1 Jadwal Penelitian 20
Tabel 4. 1 Hasil Pengukuran QoS..... 33
Tabel 4. 2 Hasil Pengukuran QoS..... 33
Tabel 4. 3 Hasil Pengukuran QoS..... 33
Tabel 4. 4 Hasil Pengukuran QoS..... 33

DAFTAR PUSAKA

Akshay, A. D., Bhushan, A., Anand, N., Khemka, R., & Devi K.A, S. (2020). HONEYPOT: Intrusion Detection System. *International Journal of Education, Science, Technology, and Engineering*, *3*(1), 13–18. https://doi.org/10.36079/lamintang.ijeste-0301.66

Arfianto, A. Z. (2017). *Penggunaan Bot Telegram Sebagai Announcement System pada Intansi Pendidikan*. https://www.researchgate.net/publication/321845746

Branch, R. M. (2010). Instructional design: The ADDIE approach. In *Instructional Design: The ADDIE Approach*. Springer US. https://doi.org/10.1007/978-0-387-09506-6

Dewi, N. K., & Putra, A. S. (2021). *Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT. ARS Solusi Utama)* (Vol. 22, Issue 1).

Fathin, R., Hamid, A., Pambudiyatno, N., Warsito, T., Politeknik,), & Surabaya, P. (2023). Monitoring sistem keamanan jaringan berbasis telegram pada local area network di politeknik penerbangan surabaya. *Prosiding Seminar Nasional Inovasi Teknologi Penerbangan (SNITP) Tahun*, 2023.

Fernández-Álvarez, P., & Rodríguez, R. J. (2021). *Extraction and Analysis of Retrievable Memory Artifacts from Windows Telegram Desktop Application*.

Hassan Rizky Putra Sailellah. (2023, April 28). *Pengertian OS Linux*. https://it.telkomuniversity.ac.id/pengertian-os-linux/

Khadafi, S., Meilani, D., Arifin, S., Komputer-Institut, S., Adhi, T., Surabaya, T., Rahman, J. A., & 100 Surabaya, H. N. (2017). *SISTEM KEAMANAN OPEN CLOUD COMPUTING MENGGUNAKAN IDS (INTRUSION DETECTION SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM)*.

Komang, I., Marta1, K. A., Nyoman, I., Hartawan2, B., Kadek, I., & Satwika3, S. (2020). ANALISIS SISTEM MONITORING KEAMANAN SERVER DENGAN SMS ALERT BERBASIS SNORT. *INSERT: Information System and Emerging Technology Journal*, *1*(1

Mr. Kartik Chawda, & Mr. Ankit D. Patel. (2014). *Dynamic & Hybrid Honeypot Model for Scalable Network Monitoring*.

Mualfah, D., & Riadi, I. (2017). Network Forensics For Detecting Flooding Attack On Web Server. In *IJCSIS) International Journal of Computer Science and Information Security* (Vol. 15, Issue 2). https://sites.google.com/site/ijcsis/

Muhammad Adri. (2003). *Sejarah Internet*.

Purba, W. W., & Efendi, R. (2020). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi*, *17*(Agustus), 143–158.

Putri, R. U., & Istiyanto, J. E. (2012). Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada. *IJCCS*, *6*(2), 101–112. www.ugm.ac.id.

Rasudin. (2014). *QUALITY OF SERVICE (QOS) PADA JARINGAN INTERNET DENGAN METODE HIERARCHY TOKEN BUCKET Rasudin*.

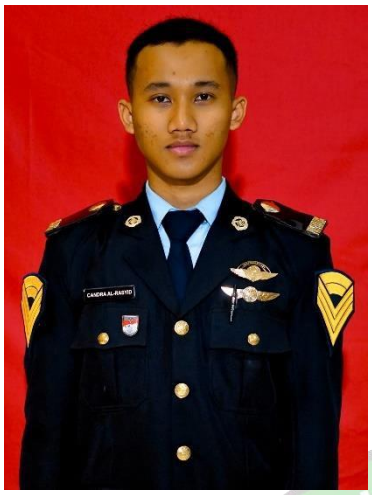
Roesch, M. (1999). *Snort-Lightweight Intrusion Detection for Networks*.

Saut Parsaoran Tamba, M. K., Yonata Laia, M. K., & Saut Dohot Siregar, S. Pd. , M. P. (n.d.). 1974-Article Text-6394-1-10-20211007. *2021*.

Slamet. (2018). *Association for Information Systems-Indonesia chapter (AISINDO)*.

Zenarmor. (2023, December 4). *Snort IDS/IPS Explained*. https://www.zenarmor.com/docs/network-security-tutorials/what-is-snort

DAFTAR RIWAYAT HIDUP



INDRA AL-RASYID CANDRAWIMBA, lahir di Denpasar, Bali pada tanggal 19 April 2003. Merupakan anak pertama dari tiga bersaudara dari pasangan Bapak Agus Santoso dan Ibu Mia Novianti. Bertempat tinggal di Perumahan Pesona Wisata III A/12, Kel. Pemecutan Klod Kec. Denpasar Barat, Denpasar, Bali. Memulai Pendidikan Sekolah Dasar di SD Muhammadiyah 1 Denpasar. Melanjutkan Pendidikan di Pondok Pesantren Salafiyah Syafi'iyah Sukorejo Situbondo dan menempuh pendidikan SMP di SMP Ibrahimy 1 Sukorejo hingga lulus pada tahun 2018. Melanjutkan Pendidikan SMK dengan konsentrasi jurusan Teknik Komputer dan Jaringan di SMK Ibrahimy 1 Sukorejo dan lulus pada tahun 2021. Selanjutnya pada bulan September 2021 diterima sebagai Taruna Politeknik Penerbangan Surabaya pada program Studi Teknik Navigasi Udara sampai dengan saat ini. Selama masa Pendidikan di Politeknik Penerbangan Surabaya telah mengikuti *On the Job Training (*OJT) di Perum LPPNPI Cabang Tanjungpandan serta PT. Angkasa Pura II H.AS. Hananjdoeddin, Belitung.