

**PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING
KEAMANAN JARINGAN MENGGUNAKAN SNORT
(Studi Kasus: Asrama Bogani Yogyakarta)**

SKRIPSI



disusun oleh

Reza Arfion Tri Putra Fimbay

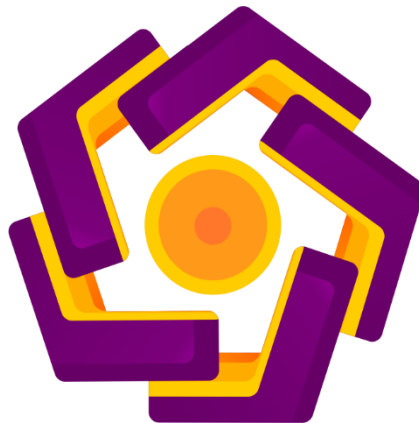
14.11.7996

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

**PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING
KEAMANAN JARINGAN MENGGUNAKAN SNORT
(Studi Kasus: Asrama Bogani Yogyakarta)**

SKRIPSI

untuk memenuhi sebagai persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Reza Arfion Tri Putra Fimbay

14.11.7996

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020**

PERSETUJUAN

SKRIPSI

PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING KEAMANAN JARINGAN MENGGUNAKAN SNORT

(Studi Kasus: Asrama Bogani Yogyakarta)

yang dipersiapkan dan disusun oleh

Reza Arfion Tri Putra Fimbay

14.11.7996

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 16 April 2018

Dosen Pembimbing,

Andika Agus Slameto, M.Kom.

NIK. 190302109

PENGESAHAN

SKRIPSI

PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING KEAMANAN JARINGAN MENGGUNAKAN SNORT (Studi Kasus: Asrama Bogani Yogyakarta)

yang dipersiapkan dan disusun oleh

Reza Arfion Tri Putra Fimbay

14.11.7996

telah dipertahankan di depan Dewan Penguji
pada tanggal 16 Oktober 2020

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Lukman, M.Kom.
NIK. 190302151

Theopilus Bayu Sasongko, S.Kom., M.Eng.
NIK. 190302375

Andika Agus Slameto, M.Kom.
NIK. 190302109

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 November 2020

DEKAN FAKULTAS ILMU KOMPUTER

Krisnawati, S.Si, M.T.
NIK. 190302038

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 12 November 2020



Reza Arfion Tri Putra Fimbay

NIM. 14.11.7996

MOTTO

- ❖ “Karena sesungguhnya sesudah kesulitan itu ada kemudahan, sesungguhnya sesudah kesulitan itu ada kemudahan.” (Al-Insyirah: 5-6)
- ❖ “Namun, bila apa yang kau diskusikan disetiap sujud belum terwujud. Percayalah, tak ada satupun dari doa-doamu yang Tuhan lewatkan. Ia maha mendengar hanya saja Ia ingin melihatmu lebih bersabar”
- ❖ “Belajar tidak selalu dari buku, lingkungan juga bisa membuat kita mengambil pelajaran”
- ❖ “Jangan biarkan orang-orang membuatmu terburu-buru dengan garis waktu mereka”



PERSEMBAHAN

Puji Syukur penulis panjatkan kepada Allah SWT atas segala limpahan Rahmat dan Hidayah-NYA sehingga penulis dapat menyelesaikan skripsi ini dengan baik.

Dengan mengucapkan syukur Alhamdulillah, karya sederhana ini saya persembahkan kepada :

- ❖ Kedua Orang Tua tercinta (Bapak Suyono dan Ibu Fimawati Fimbay, S.Pd), Kakak tercinta (Rizky Arfion Putra Prathama, S.Pd.,Gr. dan Sumarni, S.Pd.,Gr.), Keponakan tercinta (Zafira Syauqia Arfion dan Zahra Elshanum Arfion) yang selalu memberikan doa dan kasih sayang serta tak henti-hentinya memberikan dukungan dan semangat moral, spiritual serta material yang tak ternilai harganya.
- ❖ Teman serasa saudara Moh Fikri Thalani alias Acel, yang selalu bersama-sama merasakan pahit dan manis nya kehidupan rantau di Kota Istimewa Yogyakarta.
- ❖ Teman-teman dan saudaraku yang ada di “HYDRA dan KOPASSUS” terutama Bilex (D-Law), Dimas (Kawahara), dan Aru (Iceland) yang memberikan dukungan semangat, dan canda tawa, dalam proses pengerjaan skripsi ini.
- ❖ Partner tercinta Thyno, yang selalu memberikan dorongan dan dukungan semangat dalam proses pengerjaan skripsi dari awal hingga akhir.

- ❖ Teman terbaik satu kontrakan sampai pindah juga masih satu kos-kosan yaitu Hendrik-San, yang telah membantu banyak dalam proses pengerjaan skripsi ini.
- ❖ Bapak Andika Agus Slameto yang sangat banyak memberikan ilmu dan pengetahuan sebagai pembimbing, dalam mengerjakan skripsi ini.
- ❖ Asrama Bogani Yogyakarta yang sudah memberikan izin pengerjaan skripsi disana.
- ❖ Serta seluruh pihak yang telah banyak membantu yang tidak bisa saya sebutkan satu persatu, saya ucapkan terima kasih atas doa, bantuan, semangat dukungan dan kerjasamanya.

KATA PENGANTAR

Segala puji bagi Allah SWT yang telah memberikan rahmat dan karuniaNya kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini dengan baik dan tepat waktu sesuai yang diharapkan. Shalawat dan salam senantiasa tercurah kepada Rasulullah SAW yang mengantarkan manusia dari zaman kegelapan ke zaman yang terang benderang ini. Penyusunan skripsi ini dimaksudkan untuk memenuhi syarat guna mencapai gelar Sarjana Komputer di Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa penulisan ini tidak akan dapat terselesaikan tanpa bantuan dan dukungan dari berbagai pihak. Oleh sebab itu, penulis ingin menyampaikan rasa terima kasih sedalam-dalamnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Krisnawati, S.Si., M.T selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Sudarmawan, M.T selaku Ketua Program Studi Strata-1 Informatika Universitas AMIKOM Yogyakarta.
4. Bapak Andika Agus Slameto, M.Kom selaku Dosen Pembimbing yang telah memberikan arahan, bimbingan, dan masukan selama proses penyusunan Laporan Skripsi ini hingga selesai.
5. Bapak, Ibu, serta segenap Keluarga Besar tercinta.
6. Tim Penguji, Seluruh Dosen, Staf Pengajar dan Karyawan Universitas AMIKOM Yogyakarta.

7. Asrama Bogani Yogyakarta yang telah memberikan izin untuk melakukan penelitian skripsi disana.
8. Sahabat serta teman-teman yang selalu mendukung Penulis.
9. Serta semua pihak yang telah membantu dalam penyelesaian penyusunan laporan skripsi ini. Penyusun berharap semoga amal baik semuanya dapat menjadi amal ibadah yang diridhoi oleh ALLAH SWT.

Penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang bersifat membangun untuk membuat karya ini lebih baik tentunya.

Penulis juga memohon maaf kepada semua pihak jika dalam pelaksanaan penelitian dan penyusunan laporan skripsi ini terdapat kesalahan atau hal yang kurang berkenan. Semoga skripsi ini dapat bermanfaat bagi para pembaca dan semua pihak khususnya dalam bidang ilmu komputer.

Penulis

Reza Arfion Tri Putra Fimbay

DAFTAR ISI

| | |
|--|-------|
| JUDUL | i |
| PERSETUJUAN | ii |
| PENGESAHAN | iii |
| PERNYATAAN..... | iv |
| MOTTO | v |
| PERSEMBAHAN | vi |
| KATA PENGANTAR | viii |
| DAFTAR ISI..... | x |
| DAFTAR TABEL..... | xiv |
| DAFTAR GAMBAR | xv |
| INTISARI..... | xviii |
| <i>ABSTRACT</i> | xix |
| BAB I | 1 |
| PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 4 |
| 1.3 Batasan Masalah..... | 4 |
| 1.4 Maksud dan Tujuan Penelitian | 5 |
| 1.5 Manfaat Penelitian..... | 5 |
| 1.6 Metode Penelitian..... | 6 |
| 1.6.1 Metode Pengumpulan Data | 6 |
| 1.6.2 Metode Pengembangan Sistem | 7 |
| 1.6.3 Metode Analisis PIECES | 8 |
| 1.7 Sistematika Penulisan..... | 8 |
| BAB II | 10 |
| LANDASAN TEORI | 10 |
| 2.1 Tinjauan Pustaka | 10 |
| 2.2 Dasar Teori | 14 |
| 2.2.1 Jaringan Komputer | 14 |

| | | |
|--------------------------------|--|----|
| 2.2.1.1 | Jenis-Jenis Jaringan Komputer | 14 |
| 2.2.1.2 | Topologi Jaringan | 16 |
| 2.2.1.3 | Keamanan Jaringan | 18 |
| 2.2.1.4 | Penyusup (Intruder) | 19 |
| 2.2.2 | IDS (<i>Intrusion Detection System</i>) | 19 |
| 2.2.2.1 | Jenis-Jenis IDS | 20 |
| 2.2.3 | Jenis Serangan | 21 |
| 2.2.3.1 | Distributed Denial of Service (DDoS) | 21 |
| 2.2.3.2 | Port Scanning | 22 |
| 2.2.3.3 | Paket Sniffing | 23 |
| 2.2.3.4 | IP-Spoofing | 23 |
| 2.2.3.5 | DHCP Snooping | 23 |
| 2.2.3.6 | DNS Forgery | 24 |
| 2.2.3.7 | DNS Cache Poisoning | 24 |
| 2.2.4 | Sistem Operasi (<i>Operating System</i>) | 25 |
| 2.2.4.1 | Linux | 25 |
| 2.2.4.2 | Ubuntu | 26 |
| 2.2.5 | SNORT | 27 |
| 2.2.6 | MySQL | 29 |
| 2.2.7 | Barnyard2 | 30 |
| 2.2.8 | BASE (<i>Basic Analysis and Security Engine</i>) | 31 |
| 2.2.9 | Telegram Bot | 31 |
| BAB III | | 34 |
| ANALISIS DAN PERANCANGAN | | 34 |
| 3.1 | Tinjauan Umum | 34 |
| 3.1.1 | Profil Asrama Bogani | 34 |
| 3.2 | Tahap Analisis | 34 |
| 3.2.1 | Interview | 35 |
| 3.2.2 | Analisis PIECES | 36 |
| 3.2.2.1 | Kinerja (Performance) | 36 |
| 3.2.2.2 | Informasi (Information) | 39 |
| 3.2.2.3 | Ekonomi (Economic) | 42 |

| | | |
|-----------------------------|--|----|
| 3.2.2.4 | Pengendalian (Control)..... | 42 |
| 3.2.2.5 | Efisiensi (Efficiency)..... | 45 |
| 3.2.2.6 | Pelayanan (Services) | 46 |
| 3.2.3 | Analisis Kondisi Lingkungan Fisik..... | 46 |
| 3.2.3.1 | Asrama Bogani Yogyakarta | 46 |
| 3.2.3.2 | Denah Asrama | 47 |
| 3.2.4 | Solusi Terhadap Masalah | 47 |
| 3.2.5 | Analisis Kebutuhan Fungsional | 48 |
| 3.2.6 | Analisis Kebutuhan Non-Fungsional | 48 |
| 3.2.6.1 | Kebutuhan Perangkat Keras | 49 |
| 3.2.6.2 | Kebutuhan Perangkat Lunak | 49 |
| 3.2.7 | Analisis Kebutuhan SDM | 50 |
| 3.2.8 | Analisis Biaya | 51 |
| 3.3 | Tahap Design..... | 51 |
| 3.3.1 | Rancangan Topologi Sistem | 52 |
| 3.3.2 | Rancangan Sistem | 54 |
| 3.3.2.1 | Alur Kerja Sistem | 54 |
| 3.3.2.2 | Alur Deteksi Serangan..... | 57 |
| 3.3.2.3 | Telegram Bot Token dan ID Pengguna..... | 58 |
| 3.3.2.4 | Alur Kirim Notifikasi | 59 |
| 3.3.2.5 | Desain Antarmuka..... | 60 |
| BAB IV | | 63 |
| IMPLEMENTASI DAN PEMBAHASAN | | 63 |
| 4.1 | Tahap Implementasi | 63 |
| 4.1.1 | Konfigurasi IP Address IDS | 63 |
| 4.1.2 | Instalasi dan Konfigurasi Snort..... | 64 |
| 4.1.2.1 | Install Snort | 64 |
| 4.1.2.2 | Konfigurasi Snort | 66 |
| 4.1.2.3 | Uji Coba File Konfigurasi Snort | 69 |
| 4.1.2.4 | Membuat Uji Coba Rules Snort | 69 |
| 4.1.2.5 | Membuat File Rules Serangan..... | 71 |
| 4.1.3 | Instalasi dan Konfigurasi Barnyard2..... | 73 |

| | | |
|----------------------|---|-----|
| 4.1.3.1 | Install Barnyard2 | 73 |
| 4.1.3.2 | Konfigurasi Barnyard2 | 76 |
| 4.1.4 | Konfigurasi SystemD Startup | 78 |
| 4.1.5 | Instalasi dan Konfigurasi BASE | 80 |
| 4.1.5.1 | Install BASE (Basic Analysis and Security Engine)..... | 81 |
| 4.1.5.2 | Konfigurasi BASE (Basic Analysis and Security Engine)..... | 82 |
| 4.1.6 | Konfigurasi Telegram Bot | 85 |
| 4.2 | Pengujian Serangan | 89 |
| 4.2.1 | Hasil Pengujian Port Scanning..... | 89 |
| 4.2.2 | Hasil Pengujian FTP Akses..... | 91 |
| 4.2.3 | Hasil Pengujian SSH Attack | 93 |
| 4.2.4 | Hasil Pengujian DDoS Attack..... | 94 |
| 4.2.5 | Hasil Tampilan BASE (<i>Basic Analysis and Security Engine</i>) | 96 |
| 4.3 | Evaluasi Sistem | 96 |
| BAB V..... | | 100 |
| PENUTUP..... | | 100 |
| 5.1 | Kesimpulan..... | 100 |
| 5.2 | Saran..... | 101 |
| DAFTAR PUSTAKA | | 102 |

DAFTAR TABEL

| | |
|---|----|
| Tabel 3.1 Daftar Port dan Fungsinya | 40 |
| Tabel 3.2 Biaya Langganan Perbulan | 42 |
| Tabel 3.3 Spesifikasi Komputer Server (IDS) | 49 |
| Tabel 3.4 Kebutuhan Perangkat Lunak | 49 |
| Tabel 3.5 Tabel Biaya | 51 |
| Tabel 3.6 Rancangan IP Address | 53 |
| Tabel 4.1 IP Address IDS | 63 |
| Tabel 4.2 Informasi Data Telegram Bot | 88 |
| Tabel 4.3 Tingkat Akurasi Waktu | 97 |
| Tabel 4.4 Selisih Waktu Serangan | 97 |
| Tabel 4.5 Informasi Serangan Terdeteksi | 98 |
| Tabel 4.6 Hasil Pengujian Sistem | 98 |

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2.1 Logo Linux [12] | 26 |
| Gambar 2.2 Logo Ubuntu [13]..... | 27 |
| Gambar 2.3 Logo Snort [15] | 29 |
| Gambar 2.4 Logo MySQL [17]..... | 30 |
| Gambar 2.5 Logo Telegram [21] | 33 |
| Gambar 3.1 Topologi Jaringan Asrama | 35 |
| Gambar 3.2 Keamanan Jaringan WPA2 | 36 |
| Gambar 3.3 Sistem Keamanan Jaringan Asrama..... | 37 |
| Gambar 3.4 Port Scanning | 38 |
| Gambar 3.5 FTP Akses | 38 |
| Gambar 3.6 SSH <i>Brute Force</i> | 39 |
| Gambar 3.7 DDoS <i>Attack</i> | 39 |
| Gambar 3.8 Nmap..... | 40 |
| Gambar 3.9 Paket Data Port Scanning | 43 |
| Gambar 3.10 Paket Data FTP Akses..... | 44 |
| Gambar 3.11 Paket Data <i>SSH Attack</i> | 44 |
| Gambar 3.12 Paket Data DDoS <i>Attack</i> | 45 |
| Gambar 3.13 Asrama Bogani | 46 |
| Gambar 3.14 Denah Asrama | 47 |
| Gambar 3.15 Rancangan Topologi Sistem..... | 52 |
| Gambar 3.16 Flowchart Kerja Sistem | 54 |
| Gambar 3.17 Flowchart Deteksi Serangan | 57 |

| | |
|--|----|
| Gambar 3.18 Flowchart Set Telegram Bot Token | 58 |
| Gambar 3.19 Flowchart Kirim Notifikasi | 59 |
| Gambar 3.20 Antarmuka Notifikasi Telegram..... | 61 |
| Gambar 3.21 Antarmuka BASE..... | 62 |
| Gambar 4.1 Network Interfaces | 64 |
| Gambar 4.2 Snort Version 2.9.9.0..... | 65 |
| Gambar 4.3 Uji Coba File Konfigurasi Snort | 69 |
| Gambar 4.4 Output Rules Snort | 70 |
| Gambar 4.5 Test Ping..... | 71 |
| Gambar 4.6 Alert ICMP Ping..... | 71 |
| Gambar 4.7 File sid-msg.map | 73 |
| Gambar 4.8 Konfigurasi MySQL..... | 74 |
| Gambar 4.9 Tampilan Baris 521-522..... | 74 |
| Gambar 4.10 Barnyard2 Version 2.1.14 | 76 |
| Gambar 4.11 Uji Coba Barnyard2 | 78 |
| Gambar 4.12 Snort Status | 79 |
| Gambar 4.13 Barnyard2 Status | 80 |
| Gambar 4.14 Tampilan Awal BASE..... | 83 |
| Gambar 4.15 Tampilan Create BASE AG | 84 |
| Gambar 4.16 Tampilan BASE AG..... | 84 |
| Gambar 4.17 Tampilan Antarmuka BASE | 85 |
| Gambar 4.18 Request Telegram Bot..... | 86 |
| Gambar 4.19 Membuat Telegram Bot | 86 |

| | |
|---|----|
| Gambar 4.20 Mencari ID Chat Telegram | 87 |
| Gambar 4.21 Data Telegram Bot | 88 |
| Gambar 4.22 Data Profil Telegram Bot | 88 |
| Gambar 4.23 Coding Send API..... | 89 |
| Gambar 4.24 Pengujian Port Scanning | 90 |
| Gambar 4.25 Deteksi Port Scanning | 90 |
| Gambar 4.26 Notifikasi Port Scanning | 91 |
| Gambar 4.27 Pengujian FTP Akses | 91 |
| Gambar 4.28 Deteksi FTP Akses | 92 |
| Gambar 4.29 Notifikasi FTP Akses | 92 |
| Gambar 4.30 Pengujian SSH Brute Force..... | 93 |
| Gambar 4.31 Deteksi SSH Brute Force | 93 |
| Gambar 4.32 Notifikasi SSH Brute Force..... | 94 |
| Gambar 4.33 Pengujian DDoS Attack | 94 |
| Gambar 4.34 Deteksi DDoS Attack..... | 95 |
| Gambar 4.35 Notifikasi DDoS Attack | 95 |
| Gambar 4.36 Tampilan Antarmuka BASE | 96 |

INTISARI

Asrama Mahasiswa Bogani Yogyakarta telah memanfaatkan layanan internet fiber optik untuk menunjang kegiatan belajar mahasiswa dan sebagai sarana mengakses berbagai informasi. Namun layanan jaringan internet yang mengcover kawasan Asrama Bogani masih mengalami berbagai kendala, diantaranya adalah lemahnya sistem keamanan jaringan yang dapat berdampak pada masuknya serangan atau spam pada jaringan yang tidak dapat diketahui oleh administrator.

Untuk menangani masalah tersebut dilakukan penelitian menggunakan metode *NDLC* dengan menggabungkan IDS (*Intrusion Detection System*) Snort dan aplikasi *instant messaging* Telegram. Snort berfungsi sebagai sistem pendeteksi penyusupan IDS (*Intrusion Detection System*), dan bisa sangat berguna dalam merespon insiden-insiden penyerangan terhadap *host-host* jaringan. Penggunaan aplikasi *instant messaging* Telegram berfungsi sebagai media notifikasi terhadap serangan yang terjadi pada jaringan.

Dari hasil pengujian snort dan aplikasi *instant messaging* Telegram pada sistem operasi berbasis Linux dengan contoh kasus pada Ubuntu 16.04 LTS dapat berjalan dengan lancar. Snort yang diterapkan akan melakukan pemeriksaan dan menganalisa paket data yang masuk ke dalam jaringan, jika paket data tersebut terdeteksi sebagai sebuah intrusi maka akan mengirimkan notifikasi *alert* menuju aplikasi *instant messaging* Telegram milik administrator secara *real time*. Sehingga memudahkan administrator dalam memonitoring jaringan.

Kata Kunci : IDS (*Intrusion Detection System*), Snort, Telegram, Linux, Ubuntu.

ABSTRACT

The Yogyakarta Bogani Student Dormitory has utilized fiber optic internet services to support student learning activities and as a means of accessing various information. However, internet network services that cover the Bogani dormitory area still have various problems, including the weak network security system which can have an impact on the entry of attacks or spams on the network that cannot be known by the administrator.

To deal with this problem, a study was conducted using the NDLC method by combining the IDS (Intrusion Detection System) Snort and the Telegram instant messaging application. Snort functions as an IDS (Intrusion Detection System) intrusion detection system, and can be very useful in responding to attack incidents against network hosts. The use of the Telegram instant messaging application serves as a notification medium against attacks that occur on the network.

From the results of testing snort and Telegram instant messaging applications on Linux-based operating systems with an example of cases on Ubuntu 16.04 LTS can run smoothly. The snort that is applied will check and analyze data packets that enter the network, if the data packet is detected as an intrusion it will send an alert notification to the administrator's Telegram instant messaging application in real time. Making it easier for administrators to monitor the network.

Keywords : *IDS (Intrusion Detection System), Snort, Telegram, Linux, Ubuntu.*