IMPLEMENTASI INSTRUCTION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA DALAM MENDETEKSI SERANGAN DENIAL OF SERVICE PADA SERVER LINUX DEBIAN 8.0 DI BLPT YOGYAKARTA

TUGAS AKHIR

Disusun oleh:

Ayu Sulistiya Ningrum	**17.01.3917**
Yayan Puji Anggraeni	**17.01.3963**

PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

IMPLEMENTASI INSTRUCTION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA DALAM MENDETEKSI SERANGAN DENIAL OF SERVICE PADA SERVER LINUX DEBIAN 8.0 DI BLPT YOGYAKARTA

TUGAS AKHIR

Diajukan kepada Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta
untuk memenuhi salah satu syarat memperoleh gelar Ahli Madya Komputer
Pada jenjang Program Diploma – Program Studi Teknik Informatika

Disusun oleh:

Ayu Sulistiya Ningrum	**17.01.3917**
Yayan Puji Anggraeni	**17.01.3963**

PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2020

HALAMAN PERSETUJUAN

TUGAS AKHIR

IMPLEMENTASI INSTRUCTION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA DALAM MENDETEKSI SERANGAN DENIAL OF SERVICE PADA SERVER LINUX DEBIAN 8.0 DI BLPT YOGYAKARTA

yang dipersiapkan dan disusun oleh

Ayu Sulistiya Ningrum 17.01.3917

Yayan Puji Anggraeni 17.01.3963

Telah disetujui oleh Dosen Pembimbing Tugas Akhir

pada tanggal 10 Januari 2020

Dosen Pembimbing,

Barka Satya,.M.Kom
NIK. 190302126

HALAMAN PENGESAHAN

TUGAS AKHIR

IMPLEMENTASI INSTRUCTION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA DALAM MENDETEKSI SERANGAN DENIAL OF SERVICE PADA SERVER LINUX DEBIAN 8.0 DI BLPT YOGYAKARTA

yang dipersiapkan dan disusun oleh

Ayu Sulistiya Ningrum 17.01.3917

Yayan Puji Anggraeni 17.01.3963

Telah dipertahankan di depan Dewan Penguji
pada tanggal 15 Januari 2020

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Lukman,M.Kom **NIK. 190302151**	
Agit Amrullah,S.Kom.,M.Kom **NIK. 190302356**	

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
Tanggal 15 Januari 2020

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PENGESAHAN

TUGAS AKHIR

IMPLEMENTASI INSTRUCTION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA DALAM MENDETEKSI SERANGAN DENIAL OF SERVICE PADA SERVER LINUX DEBIAN 8.0 DI BLPT YOGYAKARTA

yang dipersiapkan dan disusun oleh

Ayu Sulistiya Ningrum 17.01.3917

Yayan Puji Anggraeni 17.01.3963

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Januari 2020

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Melwin Syafrizal, S.Kom.,M.Eng **NIK. 190302105**	
Banu Santoso, ST., M.Eng **NIK. 190302327**	

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya Komputer
Tanggal 20 Januari 2020

DEKAN FAKULTAS ILMU KOMPUTER

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

HALAMAN PENGESAHAN
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ayu Sulistiya Ningrum
NIM : 17.01.3917

Menyatakan bahwa Tugas Akhir dengan judul berikut:
Implementasi Instruction Detection System (IDS) Menggunakan Suricata Dalam Mendeteksi Serangan Denial Of Service Pada Server Linux Debian 8.0 Di Blpt Yogyakarta.

Dosen Pembimbing : Barka Satya.,M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 15 Januari 2020
Yang Menyatakan,

Meterai Asli
Rp 6.000

Ayu Sulistiya Ningrum

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Yayan Puji Anggraeni
NIM : 17.01.3963

Menyatakan bahwa Tugas Akhir dengan judul berikut:
Implementasi Instruction Detection System (IDS) Menggunakan Suricata Dalam Mendeteksi Serangan Denial Of Service Pada Server Linux Debian 8.0 Di Blpt Yogyakarta.

Dosen Pembimbing : Barka Satya.,M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 20 Januari 2020
Yang Menyatakan,

Meterai Asli
Rp 6.000

Yayan Puji Anggraeni

HALAMAN MOTTO

Hidup yang tidak dipertaruhkan tidak akan pernah dimenangkan

Ketika anak kecil sedang berjalan dan jatuh, apakah dia berfikir **'ternyata saya tidak berbakat jalan' dan berhenti begitu saja ?**

Samudra yang luas berawal dari sungai yang kecil

.

HALAMAN PERSEMBAHAN

Dengan segala puji dan syukur kepada Tuhan yang Maha Esa dan atas dukungan dan doa dari orang-orang tercinta, akhirnya tugas akhir ini dapat diselesaikan dengan baik. Oleh karena itu, dengan rasa bangga dan bahagia kami haturkan rasa syukur dan terimakasih kami kepada :

1. Allah SWT, karena hanya atas izin dan karunia-Nyalah maka tugas akhir ini dapat dibuat dan selesai pada waktunya. Puji syukur yang tak terhingga pada Tuhan semesta alam yang meridhoi dan mengabulkan segala doa.
2. Orang tua kami, yang tidak pernah lelah memberikan kami dukungan dan doa. Untuk Ibu yang tidak pernah lelah dalam memberikan semangat supaya kami bisa menyelesaikan tugas akhir ini dan untuk Bapak yang telah banyak memberikan begitu banyak pengorbanan yang tidak bisa kami balaskan. Terimakasih banyak kami ucapkan untuk keduanya.
3. Bapak Dosen Pembimbing Barka Satya.M,Kom yang selama ini telah tulus iklas meluangkan waktunya untuk menuntun dan mengarahkan kami, memberikan bimbingan dan pelajaran yang tiada ternilai harganya, agar kami menjadi lebih baik. Terimakasih banyak atas segala jasa yang telah diberikan kepada kami. Semoga ilmu yang telah di ajarkan kepada kami, menjadi lading amal dan semoga menjadi ilmu yang barokah untuk kami.
4. Rekan-rekan kelas 17 D3 Teknik Informatika, yang telah memberikan kami dukungan, semangat serta menemani selama 2 tahun dalam kelas yang penuh dengan segala kondisi dalam hidup. Terimakasih atas kenang-

5. Kenangan yang telah kita ukir bersama-sama. Semoga kita menjadi orang-orang yang bermanfaat dan dikenang menjadi pribadi yang baik.
6. Bapak Langgeng Arie Wira Yudha.,MM selaku pembimbing kami selama melaksanakan kegiatan magang dan kegiatan penelitian selama 4 bulan ini pada BLPT Yogyakarta.
7. Bapak Barno Waluyu,Amd.,Kom selaku salah satu teknisi diunit ELIN (Elektro dan Informatika) yang telah membimbing kami selama kegiatan magang berlangsung.
8. Kami persembahkan pula untuk yang selalu bertanya : “Kapan wisuda cuy”.
9. Serta untuk semua karyawan BLPT Yogyakarta yang kami hormati. Terimakasih atas bantuan, doa, dan motivasi yan telah diberikan. Terimakasih telah menerima kami sebagai keluarga besar BLPT Yogyakarta.

Akhir kata kami persembahakan tugas akhir ini untuk kalian semua, orang-orang yang telah memberikan pengalaman yang sangat berarti dalam hidup kami. Semoga tugas akhir ini dapat bermanfaat dan berguna untuk kemajuan ilmu pengetahuan di masa yang akan datang.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya kepada penulis sehingga dapat menyelesaikan Tugas Akhir dengan judul Implementasi *Instruction Detection System* (IDS) Menggunakan Suricata Dalam Mendeteksi Serangan *Denial Of Service* Pada Server Linux Debian 8.0 Di BLPT Yogyakarta, sesuai yang diharapkan. Dalam penyusunan Tugas Akhir ini, tentu saja masih banyak kekurangan dan hambatan yang terkadang ditemui baik secara teknik maupun non-teknis sehingga dalam melengkapi penyusunan Tugas Akhir ini tidak lepas dari bimbingan, bantuan, dan dorongan dari berbagai pihak.

Tugas akhir ini disusun sebagai salah satu syarat kelulusan Program Diploma III Jurusan Teknik Informatika Universitas Amikom Yogyakarta dan untuk memperoleh gelar Ahli Madya Komputer.

Pada kesempatan ini penulis memberikan ucapan terimakasih kepada :

1. Allah SWT, yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini.
2. Bapak Prof. Dr.M. Suyanto,MM selaku Rektor Universitas Amikom Yogyakarta.
3. Ibu Krisnawati.,S.Si,MT selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Bapak Melwin Syafrizal,.S.Kom.,M.Eng selaku Ketua Program Studi D3 Teknik Informatika.

5. Bapak Barka Satya.,M.Kom selaku dosen pembimbing yang telah memberikan pengarahan dan bimbingan kepada penulis.
6. Kedua orangtua beserta keluarga yang selalu memotivasi, doa dan juga dukungan.
7. Keluarga besar BLPT Yogyakarta atas izin penelitian,bantuan dan kerjasama selama pengerjaan Tugas Akhir.
8. Teman-teman dan pihak lain yang selalu memberikan dukungan selama pengerjaan Tugas Akhir ini.

Penulis tentunya menyadari bahwa dalam penyusunan Tugas Akhir ini masih banyak kekurangan dan kelemahan. Oleh karena itu saran dan masukan dari pembaca sangat kami harapkan sebagai acuan untuk lebih baik di waktu yang akan datang. Semoga Tugas Akhir ini dapat bermanfaat bagi semua belah pihak yang membacanya.

Yogyakarta, 10 Januari 2020

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Balai latihan pendidikan teknik (BLPT) Yogyakarta adalah sebuah tempat latihan terpusat yang menyelenggarakan pendidikan, pelatihan, dan pengembangan keteknikan. Sistem keamanan jaringan menjadi sesuatu hal yang harus diperhatikan dan sangat penting untuk sebuah instansi perusahaan. Terdapat banyak ancaman yang bias kapan saja menyerang yang tentu akan berdampak pada layanan yang dimiliki, sehingga menimbulkan banyak kerugian. Mengantisipasi ancaman tersebut diperlukan sebuah system pendeteksi intrusi serangan yang kemungkinan akan terjadi di server ICT BLPT Yogyakarta.

Pada tugas akhir ini penulis akan Implementasi Instruction Detection System (IDS) Menggunakan Suricata Dalam Mendeteksi Serangan Denial of Service Pada Server Linux Debian 8.0 di BLPT Yogyakarta.Sistem pendeteksi intrusi merupakan salah satu usaha yang dikembangkan untuk tujuan melindungi server, system atau jaringan. IDS yang digunakan dalam usaha membangun system pendeteksi intrusi adalah Suricata. IDS Suricata merupakan sebuah aplikasi open source yang dapat mendeteksi aktivitas yang merugikan dalam sebuah jaringan computer. Tools pembangunan system pendeteksi intrusi tersebut dengan menggunkan serangan DoS (Denial of Service) dari LOIC. Pengujian dilakukan dengan pola serangan untuk menguji kemampuan suricata dalam mendeteksi serangan terhadap system keamanan. Metode yang penulis gunakan yaitu observasi, studi literature, instalasi, konfigurasi,pengujian.

Dari hasil pengetesan didapatkan bahwa IDS Suricata dapat mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan computer dan menghasilkan output yang tersimpan dalam bentuk file log. Dari file log tersebut juga dijelaskan waktu serangan, tanggal, jam, dan penjelasan deskripsi dari serangan tersebut.

Keyword **: IDS, Instruction Detection System, Instruction, Suricata.**

ABSTRACT

Balai Latihan Pendidikan Teknik (BLPT) Yogyakarta is a centralized training center that organizes education, training and engineering development. Network security systems become something that must be considered and is very important for a company agency. There are many threats that can attack at any time which will certainly have an impact on the services they have, resulting in many losses. Anticipating this threat requires an intrusion detection system that is likely to occur on the Yogyakarta BLPT ICT server.

In this thesis the author will Implement Instruction Detection System (IDS) Using Suricata in Detecting Denial of Service Attacks on Debian 8.0 Linux Servers at BLPT Yogyakarta. Intrusion detection systems are an effort developed for the purpose of protecting servers, systems or networks. The IDS used in an effort to build an intrusion detection system is Suricata. IDS Suricata is an open source application that can detect harmful activities in a computer network. The intrusion detection system development tools use the DoS (Denial of Service) attack from LOIC. Testing is done with an attack pattern to test the ability of Suricata to detect attacks on the security system. The method I use is observation, study of literature, installation, configuration, testing.

From the test results found that Suricata IDS can detect suspicious activity in a computer network and produce output that is stored in the form of log files. The log file also describes the attack time, date, time, and description of the attack

Keyword : IDS, Instruction Detection System, Instruction, Suricata.