IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* MENGGUNAKAN *TOOLS* ELASTIC SERTA SURICATA SEBAGAI SISTEM PENDETEKSI INTRUSI PADA SISTEM OPERASI LINUX UBUNTU DI PERUSAHAAN PT. ITSEC ASIA

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Gelar Sarjana Terapan

Aldi Alpauji
4817050033

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK NEGERI JAKARTA
2021

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Aldi Alpauji

NIM : 4817050033

Tanggal : 31 Agustus 2021

Tanda Tangan :

HALAMAN PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Aldi Alpauji
NIM	:	4817050033
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	IMPLEMENTASI *SECURITY INFORMATION AND EVENT MANAGEMENT* MENGGUNAKAN *TOOLS* ELASTIC SERTA SURICATA SEBAGAI SISTEM PENDETEKSI INTRUSI PADA SISTEM OPERASI LINUX UBUNTU DI PERUSAHAAN PT. ITSEC ASIA

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 24, Bulan Agustus Tahun 2021 Dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Fachroni Arbi Murad, S.Kom., M.Kom. ( )

Penguji I : Maria Agustin, S.Kom., M.Kom. ( )

Penguji II : Indra Hermawan, S.Kom., M.Kom. ( )

Penguji III : Asep Kurniawan, S.Pd., M.Kom. ( )

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Tuhan Yang Maha Esa, atas berkat dan rahmat-Nya, penulis dapat menyelesaikan laporan skripsi ini. Penulisan laporan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan laporan skripsi, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

a. Bapak Fachroni Arbi Murad, S.Kom., M.Kom. selaku Dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;
b. Orang tua dan keluarga penulis yang sudah memberikan bantuan dukungan penuh secara moral dan material;
c. Fazrin Alfiansyah, selaku teman satu tim, satu perjuangan dalam penyusunan laporan skripsi ini yang telah memberikan bantuan dukungan secara moral; dan
d. Sahabat-sahabat saya, teman-teman “Bismillah”, teman kelas satu perjuangan dari awal hingga akhir masa perkuliahan yang tidak pernah putus memberi semangat.

Akhir kata, penulis berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga laporan skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 01 September 2021

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini :

Nama	: Aldi Alpauji
NIM	: 4817050033
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

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

Implementasi *Security Information and Event Management* Menggunakan *Tools* Elastic Serta Suricata Sebagai Sistem Pendeteksi Intrusi Pada Sistem Operasi Linux Ubuntu di Perusahaan PT. ITSEC ASIA.

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok, Pada tanggal : 01 September 2021

Yang Menyatakan

(Aldi Alpauji)

IMPLEMENTASI SECURITY INFORMATION AND EVENT MANAGEMENT MENGGUNAKAN TOOLS ELASTIC SERTA SURICATA SEBAGAI SISTEM PENDETEKSI INTRUSI PADA SISTEM OPERASI LINUX UBUNTU DI PERUSAHAAN PT. ITSEC ASIA

Abstrak

Jaringan divisi SOC hanya memiliki *firewall* yang terpasang pada router yang diberikan oleh *provider*. Oleh karena itu, perlu adanya perangkat keamanan jaringan tambahan dan perangkat monitoring untuk mengamankan jaringan. Implementasi Suricata sebagai *Intrusion Detection System* (IDS) serta Elastic sebagai *Security Infomation and Event Management* (SIEM) bisa untuk mendeteksi dan mengelola log dalam sebuah jaringan. Log dalam IDS Suricata akan dikelola oleh Elastic yaitu perangkat lunak untuk membentuk SIEM. Tujuan dari penelitian ini adalah untuk mendeteksi serangan *denial of service* dan memonitoring serangan DOS yang masuk pada pada perangkat keamanan jaringan serta mempermudah memonitoring pada Elastic SIEM. pengujian pada penelitian ini adalah pada port 80 yang tebuka setelah di lakukan *scanning* terlebih dahulu. Membanjiri port 80 dengan *denial of service* (DoS), hasil dari serangan yang terbaca oleh perangkat keamanan dimonitoring pada Elastic. Semua serangan yang dilakukan dapat terbaca oleh suricata meskipun suricata tidak bisa membaca semua paket dalah jumlah yang besar, terbukti dengan serangan yang dilakukan oleh Hping3 dengan mengirim 299.979 paket, suricata hanya bisa menagkap 64.730 paket. Elastic SIEM bisa mempermudah dalam memonitoring serangan yan masuk pada perangkat keamanan.

Kata Kunci: *Intrusion Detection System*, *Security Information and Event Management*, dan *denial of service.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet telah menjadi kebutuhan primer bagi masyarakat luas. Kemudahan mengakses internet bisa menjadi solusi praktis bagi masyarakat untuk mendapatkan informasi apapun yang dibutuhkan. Layanan internet menyediakan kebebasan masyarakat untuk mengunduh berbagai hal tanpa mengetahui file tersebut berbahaya atau tidak. Penggunaan internet tidak lepas dari tindak kejahatan atau *cybercrime* yang memanfaatkan internet sebagai sarana untuk masuk ke sebuah sistem dengan tujuan tertentu tanpa sepengetahuan pengguna.

Sistem keamanan jaringan semakin berkembang dengan pesat. Hal ini juga berlaku pada keamanan jaringan komputer yang telah menjadi salah satu bagian yang sangat penting untuk menjaga ketersediaan layanan bagi penggunanya. Sebuah jaringan harus selalu dilindungi dari berbagai serangan. Sistem pendeteksi jaringan yang sudah ada pada saat ini mampu mendeteksi beberapa jenis serangan tetapi hanya pada aturan yang telah dibuat. Sebuah sistem dibutuhkan untuk mampu menanggulangi ancaman yang mungkin terjadi dalam waktu yang cepat serta melindungi jaringan tersebut.

Pada jaringan divisi *Security Operation Center* (SOC) PT. ITSEC ASIA memiliki sebuah jaringan yang digunakan untuk terkoneksi dengan pelanganya di berbagai daerah dan melakukan analisis serangan yang ada pada jaringan pelanggan. jaringan divisi SOC hanya memiliki *firewall* yang terpasang pada router yang diberikan oleh *provider*. Oleh karena itu, perlu adanya perangkat keamanan jaringan tambahan dan perangkat monitoring untuk mengamankan jaringan. penulis ngusulkan untuk membuat prototipe untuk melakukan perlindungan terhadap jaringan yang nantinya bisa di terapkan pada jaringan divisi SOC. Pembuatan prototipe ini di buat agar tidak mengganggu lalu lintas data pada jaringan divisi SOC. Kemanan jaringan yang digunakan yaitu jenis *Intrusion Detection System* (IDS) serta Elastic sebagai SIEM yang akan diterapkan. *Intrusion Detection System* (IDS) adalah perangkat keamanan jaringan yang

memonitor kegiatan jaringan dari aktivitas yang berbahaya. Elastic sendiri adalah *tools* untuk menyimpan data log yang nantinya akan divisualisasikan agar mempermudah dalam monitoring jika ada log yang masuk pada perangakat keaman jaringan Suricata.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, dapat uraikan rumusan masalah untuk dibahas dalam penelitian ini yaitu:

Bagaimana perangkat keamanan jaringan suricata mendeteksi serangan ?

Bagaimana memonitoring serangan yang masuk pada perangkat keamanan jaringan Suricata menggunakan Elastic SIEM ?

Apakah menggunakan Elastic SIEM mempermudah memonitoring serangan yang masuk pada perangkat keamanan jaringan Suricata?

1.3 Batasan Masalah

Berdasarkan latar belakang tersebut, dapat diuraikan batasan masalah untuk dibahas dalam penelitian ini yaitu :

1. Ruang lingkup hanya meliputi pada jaringan prototipe dari jaringan divisi SOC.
2. Log yang masuk pada Elastic SIEM hanya berasal dari IDS suricata.
3. Penggunaan Elastic SIEM hanya pada bagian *discover, visualize* dan *dashboard* Kibana.
4. Pengujian sistem sendiri hanya pada rule DOS untuk memastikan suricata mendeteksinya dan mengirim log pada elastic untuk dapat dimonitoring pada kibana.
5. Serangan dilakukan pada pada jaringan internal yang sama dengan server.
6. Serangan dilakukan dengan perangkat lunak Metasploit, Hping3, dan Slowris pada kali linux serta perangkat lunak Loic pada OS Windows.
7. Pengimplementasian menggunakan sistem operasi Linux Ubuntu yang dioperasikan secara virtual.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini yaitu:

1. Mendeteksi serangan *denial of service* pada perangkat keamanan jaringan Suricata.
2. Memonitoring serangan DOS yang masuk pada pada perangkat keamanan jaringan menggunakan Elastic SIEM.
3. Mempermudah memonitoring serangan yang masuk pada perangkat keamanan jaringan menggunakan Elastic SIEM.

1.4.2 Manfaat

1. Dapat mendeteksi serangan *denial of service* menggunakan perangkat keamanan Suricata.
2. Dapat memonitoring serangan DOS yang masuk pada perangkat keamanan jaringan yang di visualisasikan pada Elastic SIEM.
3. Mempermudah dalam pembacaan serangan menggunakan Elastic SIEM.

1.5 Metode Penyeselaian Masalah

Untuk menyeselaikan masalah ini, metode yang digunakan yaitu bersifat eksperimental dengan membuat sebuah prototipe untuk menguji perangkat keamanan jaringan bisa membaca serangan *Denial of Service* (DOS) pada port 80 yang terbuka, serangan dilakukan menggunakan perangkat lunak Metasploit, Loic, Haping3, dan Slowris. Serta log dari suricata bisa di visualisasikan pada Kibana. Menggunakan Elastic SIEM diharapkan bisa mempermudah dalam memonitor serangan yang masuk pada perangkat keamanan jaringan.

BAB V
PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil dari penelitian yang telah dilakukan oleh penulis, maka dapat ditarik kesimpulan sebagai berikut:

1. Semua serangan DOS yang dilakukan oleh perangkat lunak Metasploit, LOIC. Hping3, dan slowris bisa di deteksi oleh perangkat keamannan jaringan suricata.
2. Semua log yang masuk pada suricata dapat divisualisasikan pada kibana pada bagian *discover, visualize,* dan *dashboard*.
3. Elastic SIEM Mempermudah dalam memonitor perangkat keamanan jaringan.

5.2 SARAN

Saran yang dapat diusulkan pada penelitian ini adalah :

1. Menggunakan lebih dari 2 jenis serangan yang digunakan untuk melihat deteksi suricata dan visualisasi pada kibana.
2. Menggunakan lebih dari 2 tipe log untuk melihat beberapa log yang masuk pada Elastic SIEM.

DAFTAR PUSTAKA

Adesty, Istiana. Prabowo, Adi Wahyu, Sidiq, M Fazar. 2020. Implementation of Intrusion Prevention System (IPS) as a Security from DDOS (Distributed Denial of Service) Attacks.

Admi, A., & Maulana, A. H. N. 2020. Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia. JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia), 5(2), 69-77.

Agrawal, Kavita, and Hemant Makwana. 2015. "Review of Different Log Management Tools Used for Data Analysis." Data Mining and Knowledge Engineering 7.4. 161-163.

Agus Tedyyana Rezki Kurniati. 2016. Membuat Web Server Menggunakan Dinamic Domain. Jurnal Teknologi Informasi & Komunikasi Digital Zone, 7, 1–10.

Ariyus, Dony M. Kom. 2007. "Intrusion detection system." Yogyakarta: Andi.

Bajer, M. 2017. Building an IoT Data Hub with Elasticsearch, Logstash and Kibana.

Borges, Esteban. 2021. “SecurityTrails | Top 16 Nmap Commands to Scan Remote Hosts - Tutorial Guide.” Securitytrails.com, securitytrails.com/blog/nmap-commands. [05 Agutus 2021]

Chapple, Mike. 2013. “The Three Elements of Defense against Denial-of-Service Attacks.” Technology Solutions That Drive Business, biztechmagazine.com/article/2013/02/three-elements-defense-against-denial-service-attacks. [03 Agustus 2021]

Chelara, G., & Hermanto, D. 2014. Analisis Site to Site Virtual Private Network (VPN) pada PT. In Excel Utama Indonesia Palembang. Seminar Perkembangan dan Hasil Penelitian Ilmu Komputer (SPHP-ILKOM) 2 (1): 35 (Vol. 44).

Dewanto, Adetya Putra. 2018. PENETRATION TESTING PADA DOMAIN UII. AC. ID MENGGUNAKAN OWASP 10.

Fauzi, R. A. 2017. Sistem Informasi Akuntansi (Berbasis Akuntansi). Deepublish.

Fridayanthie, E., & Charter, J. 2016. Rancang Bangun Sistem Informasi Simpan Pinjam Karyawan Menggunakan Metode Object Oriented Programming. Jurnal Techno Nusa Mandiri, XIII(2), 63–71.

Handika, Vian. 2020. PERANCANGAN SISTEM MONITORING MULTIPLE NETWORK MENGGUNAKAN PLATFORM ELASTIC STACK (STUDI KASUS: PT. JEDI GLOBAL TEKNOLOGI).

Harjono, E. B. 2016. Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. Sinkron: jurnal dan penelitian teknik informatika, 1(1).

J. Turnbull, 2017. The Logstash Book. James Turnbull.

Jalinus, N., & Ambiyar, A. 2016. Media dan sumber pembelajaran.

Lukman, N. 2016. Studi Implementasi Aplikasi Manajemen Ruang Kelas" Netop School" Berbasiskan Local Area Network (LAN). Studi Implementasi Aplikasi Manajemen Ruang kelas, 11, 1-14.

Malhotra, Aman. Rawat, Lakshya. Kumar, Lokesh. 2020. MINI SECURITY OPERATIONS CENTER USING ELK.

Manuaba, I. B. V. H., Hidayat, R., & Kusumawardani, S. S. 2012. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada). J. Nas. Tek. Elektro Dan Teknol. Inf. JNTETI, 1(1), 13-17.

MS, Divya. SK, Goyal. 2013. An advanced and quick search technique to handle voluminous data.

MUHARTIN, A. 2017. IMPLEMENTASI SISTEM MONITORING JARINGAN WIRELESS DENGAN METODE NETWORKSECURITYMONITORING (NSM)(STUDI KASUS: PUSAT TEKNOLOGI INFORMASI DAN PANGKALAN DATA UIN SYARIF KASIM RIAU) (Doctoral dissertation, Universitas Islam Negeri Sultan Syarif Kasim Riau).

Norrby, Elias. 2018. Investigation and Implementation of a Log Management and Analysis Framework for the Treatment Planning System RayStation.

Nurdin, N. 2015. Analisis Adopsi dan Pemanfaatan Internet di Kalangan Mahasiswa Perguruan Tinggi di Kota Palu. Jurnal Elektronik Sistem Informasi dan Komputer, 1(1), 49-52.

Open Source Search: The Creators of Elasticsearch, ELK Stack & Kibana | Elastic. Elastic.co, Elastic, 2019, www.elastic.co. [15 Agustus 2021]

Patrick, Kleindienst. 2016. Building a real-world logging infrastructure with Logstash, Elasticsearch and Kibana.

Pratiwi, Nurul Hanifah. 2020. IMPLEMENTASI SURICATA SEBAGAI IDS DAN ELASTIC STACK SEBAGAI SIEM PADA LAB DEVELOPMENT BPPT.

Sahoo, P. K., et al. 2021. "Syslog a Promising Solution to Log Management." International Journal of Advanced Research in Computer Science 3.3.

Setiawan, Thomas. 2004."Analisis Keamanan Jaringan Internet Menggunakan Hping, Nmap, Nessus, dan Ethereal." Jurnal Institut Teknologi Bandung 11.6.

Singh, Krishan Kumar, et al. "Elastic search." Int. J. Mod. Trends Eng. Res 5.5 (2018).

Supriadi, Andi. & Gartina, Ghani. 2007. MEMILIH TOPOLOGI JARINGAN DAN HARDWARE DALAM DESAIN SEBUAH JARINGAN KOMPUTER. Informatika Pertanian Volume 16 No. 2

Syani, Mamay. 2020. IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN SURICATA PADA LINUX DEBIAN 9 BERBASIS CLOUD VIRTUAL PRIVATE SERVERS (VPS).

Taware, U. & Shaikh, N. 2018. "Heterogeneous Database System for Faster Data Querying Using Elasticsearch," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 1-4.

Tedyyana, A., & Kurniati, R. 2016. Membuat Web Server Menggunakan Dinamic Domain Name System Pada IP Dinamis. Jurnal Teknologi Informasi & Komunikasi Digital Zone, 7(1), 1–10.

Teguh, T. Saputra, and B. Irawan. Ilhamsyah, 2014,“Aplikasi Antrian Nasabah Bank Menggunakan Teks Dan Suara Berbasis Jaringan Wireless Lokal Area Network (WLAN)”." Jurnal Coding Sistem Komputer Universitas Tanjungpura 2.2: 1-7.

Their, Tomas. 2006. Beginning Ubuntu Linux: From Novice to Professional.

Vanney, Ivan. 2019. “Hping3 Flood Ddos – Linux Hint.” linuxhint.com/hping3/. [05 Agustus 2021]

Varianto, E., & Badrul, M. 2015. Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt. Valdo International. Jurnal Teknik Komputer, 1(1), 54-65.

DAFTAR RIWAYAT HIDUP PENULIS

Lahir di Kuningan, 30 Desember 1997. Lulus dari SDN 2 Baok pada tahun 2010, SMPN 1 Luragung pada tahun 2013, SMAN 1 Luragung pada tahun 2016 dan Diploma II program studi *Network Administrator Professional* di CCIT-FTUI pada tahun 2018. Saat ini sedang menempuh Pendidikan Diploma IV Program Studi Teknik Informatika Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.