ANALISIS DAN IMPLEMENTASI *OPEN-SOURCE HOST INTRUSION DETECTION SYSTEM SECURITY* (OSSEC) PADA SMK NEGERI 2 SUKOHARJO

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Syarat Memperoleh Gelar
Sarjana Strata Satu (S1) Program Studi Informatika

Disusun Oleh:

Muhamad Nashiruddin Zaki

NIM. 19106050027

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2023

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-2938/Un.02/DST/PP.00.9/12/2023

Tugas Akhir dengan judul : Analisis dan Implementasi Open Source Host Intrusion Detection System Security (OSSEC) pada SMK Negeri 2 Sukoharjo

yang dipersiapkan dan disusun oleh:

Nama : MUHAMAD NASHIRUDDIN ZAKI
Nomor Induk Mahasiswa : 19106050027
Telah diujikan pada : Jumat, 15 Desember 2023
Nilai ujian Tugas Akhir : A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Mandahadi Kusuma, M.Eng.
SIGNED

Valid ID: 65825af7df97f

Penguji I

Ir. Sumarsono, S.T., M.Kom.
SIGNED

Valid ID: 658406ccda2bf

Penguji II

Muhammad Galih Wonoseto, M.T.
SIGNED

Valid ID: 6583c84206bc3

Yogyakarta, 15 Desember 2023
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED

Valid ID: 6584e3dbae9af

SURAT PERNYATAAN KEASLIAN / BEBAS PLAGIASI

SURAT PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	: Muhamad Nashiruddin Zaki
NIM	: 19106050027
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

menyatakan bahwa dalam skripsi saya yang berjudul **"Analisis dan Implementasi *Open-Source Host Intrusion Detection System Security* (OSSEC) pada SMK Negeri 2 Sukoharjo"** merupakan hasil penelitian saya sendiri dan tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 20 Desember 2023
Yang menyatakan,

Muhamad Nashiruddin Zaki
NIM. 19106050027

NOTA DINAS PENGUJI I

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

NOTA DINAS KONSULTASI

Hal : Persetujuan Skripsi / Tugas Akhir

Lampiran : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhamad Nashiruddin Zaki
NIM : 19106050027
Judul Skripsi : Analisis dan Implementasi Open-Source Host Intrusion Detection System Security (OSSEC) pada SMK Negeri 2 Sukoharjo

sudah benar dan sesuai ketentuan sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Demikian kami sampaikan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 21 December 2023
Konsultan I,

Ir. Sumarsono, S.T., M.Kom.
NIP. 19710209 200501 1 003

NOTA DINAS PENGUJI II

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

NOTA DINAS KONSULTASI

Hal : Persetujuan Skripsi / Tugas Akhir

Lampiran : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhamad Nashiruddin Zaki
NIM : 19106050027
Judul Skripsi : Analisis dan Implementasi Open-Source Host Intrusion Detection System Security (OSSEC) pada SMK Negeri 2 Sukoharjo

sudah benar dan sesuai ketentuan sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

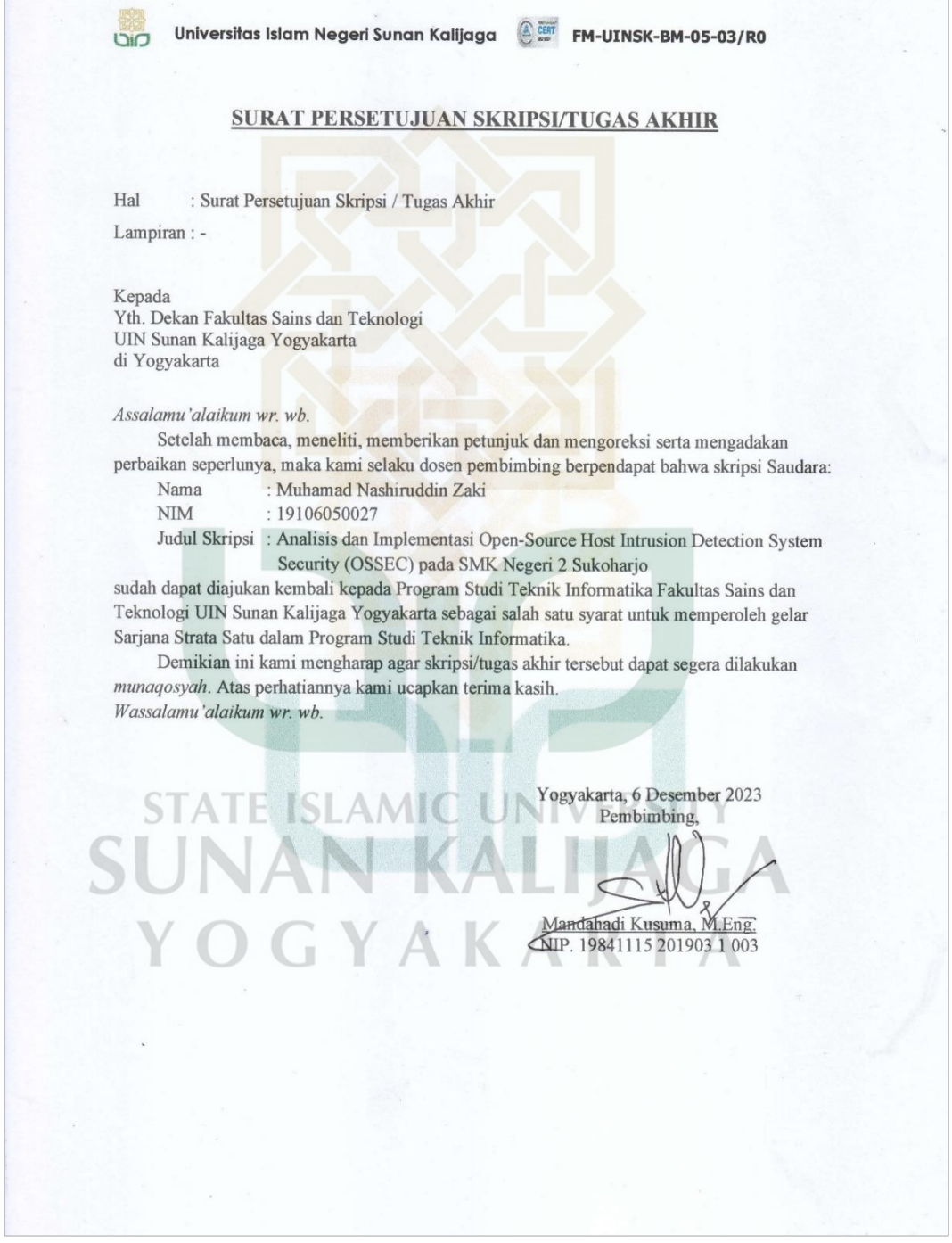
Demikian kami sampaikan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 21 Desember 2023
Konsultan II,

Muhammad Galih Wonoseto, M.T.
NIP. 19901113 201903 1 012

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR



Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Surat Persetujuan Skripsi / Tugas Akhir

Lampiran : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku dosen pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhamad Nashiruddin Zaki
NIM : 19106050027
Judul Skripsi : Analisis dan Implementasi Open-Source Host Intrusion Detection System Security (OSSEC) pada SMK Negeri 2 Sukoharjo

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Teknik Informatika.

Demikian ini kami mengharap agar skripsi/tugas akhir tersebut dapat segera dilakukan *munaqosyah*. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 6 Desember 2023
Pembimbing,

Mandahadi Kusuma, M.Eng.
NIP. 19841115 201903 1 003

ANALISIS DAN IMPLEMENTASI
OPEN-SOURCE HOST INTRUSION DETECTION SYSTEM SECURITY
(OSSEC) PADA SMK NEGERI 2 SUKOHARJO

Muhamad Nashiruddin Zaki

NIM. 19106050027

ABSTRAK

.

Jaringan komputer sebagai basis utama dalam sistem komunikasi dan informasi memerlukan perencanaan keamanan yang efektif untuk mencegah ancaman keamanan jaringan, seperti serangan *Distributed Denial of Service* (DDoS), *Port Scanning*, *Brute Force Attack*, *Malware*, dan sebagainya. Penelitian ini membahas tentang implementasi sistem keamanan komputer berupa *Intrusion Detection System* (IDS) untuk melindungi jaringan komputer dari potensi serangan keamanan. OSSEC *(Open Source Host-based Intrusion Detection System Security)* merupakan salah satu *software* IDS yang digunakan untuk mendeteksi serangan pada perangkat jaringan, mencatat log, dan memberikan peringatan kepada administrator. Studi kasus di SMK Negeri 2 Sukoharjo menunjukkan kekurangan dalam sistem keamanan jaringan, mendorong peneliti untuk melakukan penelitian berjudul "Analisis dan Implementasi Open Source Host Intrusion Detection System Security (OSSEC) pada SMK Negeri 2 Sukoharjo." Penelitian ini bertujuan untuk mengevaluasi keamanan sistem jaringan sekolah terhadap ancaman internal maupun eksternal dengan menerapkan OSSEC sebagai alat monitoring jaringan. Hasil dari penelitian ini adalah sistem OSSEC dapat mendeteksi dan mencatat berbagai jenis serangan terhadap perangkat komputer yang terhubung serta mampu menjalankan *active response* untuk mencegah serangan.

Kata Kunci:

IDS, OSSEC, Pengujian Penetrasi

ANALYSIS AND IMPLEMENTATION OF OPEN-SOURCE HOST INTRUSION DETECTION SYSTEM SECURITY (OSSEC) AT SMK NEGERI 2 SUKOHARJO

Muhamad Nashiruddin Zaki

NIM. 19106050027

ABSTRACT

Computer networks, as systems of communication and information exchange, require effective security planning to prevent network security threats, such as Distributed Denial of Service (DDoS) attacks, port scanning, brute force attacks, malware, and so on. This study discusses the implementation of a computer security system in the form of an Intrusion Detection System (IDS) to protect computer networks from potential security attacks. OSSEC (Open Source Host-based Intrusion Detection System Security) is one of the IDS software used to detect attacks on network devices, log them, and notify administrators. A case study at SMK Negeri 2 Sukoharjo showed deficiencies in the network security system, motivating us to conduct a study entitled "Analysis and Implementation of Open Source Host Intrusion Detection System Security (OSSEC) at SMK Negeri 2 Sukoharjo." This study aims to evaluate the security of the school's network system against internal and external threats by implementing OSSEC as a network monitoring tool. The results of this study are that the OSSEC system can detect and record various types of attacks against connected computer devices and is capable of running active response to prevent attacks.

Keywords:

IDS, OSSEC, Penetration Test

MOTTO

"You don't need to be great to start, but you need to start to be great."

~ *Someone Wise*

HALAMAN PERSEMBAHAN

Skripsi ini penulis persembahkan kepada:

- Allah SWT
- Kedua Orang Tua Tercinta
- Pembaca yang budiman

KATA PENGANTAR

بِسْـــــــــــــــمِ اللهِ الرَّحْمَنِ الرَّحِيْم

Assalamu'alaikum wr. wb.

Puji syukur *Alhamdulillah,* penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul **"Analisis dan Implementasi *Open-Source Host Intrusion Detection System Security* (OSSEC) pada SMK Negeri 2 Sukoharjo"**. **S**holawat serta salam semoga senantiasa tercurah kepada junjungan kita, Baginda Rasulullah Muhammad SAW yang telah menuntun umat manusia dari jalan kegelapan menuju jalan yang terang benderang.

Penulisan skripsi ini dimaksudkan untuk memenuhi sebagian persyaratan untuk mendapatkan gelar sarjana komputer pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Sunan Kalijaga Yogyakarta. Dengan segala kerendahan hati, sudah selayaknya penulis mengucapkan terima kasih kepada pihak-pihak berikut yang telah membantu dalam penulisan skripsi ini.

1. Rektor UIN Sunan Kalijaga Yogyakarta, Bapak Prof. Dr. Phil. Al Makin, S.Ag., M.A.
2. Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta, Ibu Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
3. Kepala Program Studi S1 Teknik Informatika, Ibu Maria Ulfah Siregar, S.Kom., MIT., Ph.D.
4. Bapak Ir. Aulia Faqih Rifa'i, M.Kom. selaku Dosen Pembimbing Akademik.
5. Bapak Mandahadi Kusuma, M.Eng. selaku Dosen Pembimbing Skripsi yang telah memberikan saran dan masukan dalam penulisan skripsi.
6. Ayah, Ibu, Kakak, Adik, dan seluruh keluarga besar yang selalu memberikan semangat dan dukungan kepada penulis.
7. Segenap rekan Asrama Ibadurrahman dan JogjaJE

8. Segenap Dosen Program Studi Teknik Informatika yang telah membimbing dan mencurahkan ilmu kepada penulis.
9. Semua pihak yang berperan membantu penyusunan skripsi ini hingga akhir.

Segala daya dan upaya yang telah dicurahkan dalam penyusunan skripsi ini belum tentu akan menjamin kesempurnaannya, mengingat akan keterbatasan kemampuan yang dimiliki oleh penulis. Oleh sebab itu, saran maupun kritik yang membangun sangat penulis harapkan demi perbaikan dan kebaikan bersama.

Akhir kata, semoga skripsi ini dapat memberikan manfaat keilmuan kepada kita semua. *Aamiin ya rabbal 'alamiin*.

Wassalamu'alaikum wr. wb.

Yogyakarta, 20 Desember 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1. LATAR BELAKANG

Jaringan komputer merupakan suatu sistem yang saling terhubung sebagai perantara dalam proses pertukaran data dan informasi. Sistem ini terdiri atas dua komputer atau lebih yang dihubungkan melalui media transmisi baik secara fisik *(physical)* maupun logis *(logical)* dengan tujuan agar data yang dibawa oleh pengirim dapat diterima oleh penerima (Smith, 2003).

Perencanaan terhadap desain jaringan dan prosedur keamanannya penting dilakukan agar tidak terjadi kebocoran akses atau serangan dari pihak yang tidak bertanggung jawab. Dengan manajemen yang baik akan meningkatkan performa dan reliabilitas sistem jaringan serta meminimalisir terjadinya ancaman keamanan. Setiap organisasi yang mengoperasikan perangkat jaringan merupakan target potensial dari ancaman keamanan. Menurut Stallings & Brown (2015), untuk menerapkan sistem keamanan komputer perlu melakukan manajemen konfigurasi sistem keamanan meliputi *hardware*, *software*, *firmware*, dan dokumentasi. Jika ada kelemahan dalam komponen tersebut, penyerang atau *hacker* dapat mengambil kesempatan untuk melakukan serangan terhadap jaringan komputer seperti serangan *Distributed Denial of Service* (DDoS), *port scanning*, *brute force*, serangan *malware* dan sebagainya. Apabila gagal dalam menangani serangan maka akan berakibat fatal terhadap proses bisnis yang berjalan seperti terganggunya koneksi, kebocoran database, yang dapat mengakibatkan hilangnya reputasi organisasi tersebut akibat serangan yang ditimbulkan.

Untuk mencegah dampak yang ditimbulkan, suatu organisasi perlu menerapkan sistem keamanan komputer yang dapat mencegah terjadinya serangan. Beberapa sistem yang dapat diterapkan seperti *firewall*, *Demilitarized Zone* (DMZ), *Intrusion Detection / Prevention System* (IDS/IPS), IPSec, VPN, dan lain sebagainya (Tanenbaum & Wetherall, 2011). Sistem tersebut memiliki fungsi yang berbeda-beda tetapi memiliki tujuan yang sama yaitu memberikan perlindungan

yang lebih kuat terhadap serangan yang terkait dengan infrastruktur dan melindungi informasi sensitif.

Monitoring jaringan dilakukan untuk menjaga keamanan jaringan dari serangan dari pihak yang tidak bertanggungjawab. Dalam hal monitoring jaringan seorang administrator jaringan atau petugas tidak dapat bekerja penuh untuk melakukan pemantauan di depan layar komputer sehingga dapat mengetahui setiap gangguan pada server dan jaringan. Maka dari itu diperlukan sebuah alat yaitu IDS untuk dapat mendeteksi gangguan secara otomatis dan mencatat log terhadap setiap kegiatan (Stallings & Brown, 2015, chap. 8). IDS akan memberi peringatan kepada administrator tentang serangan yang terjadi agar dapat ditindaklanjuti secara cepat.

OSSEC *(Open Source Host-based Intrusion Detection System Security)* merupakan salah satu alat yang dapat diterapkan untuk melakukan monitoring jaringan berbasis *host*. OSSEC bersifat *open source* dan mendukung beberapa sistem operasi seperti Linux, FreeBSD, OS X, Solaris dan Windows. OSSEC memberikan fungsi yang sama seperti SIEM *(Security Information and Event Management)* dan STRM *(Security Threat Response Management).* Aplikasi ini menggunakan arsitektur client-server. Fitur-fitur yang terdapat pada OSSEC antara lain pencatatan dan analisis log, mengecek integritas, monitoring Windows *registry*, deteksi *rootkit*, respon aktif, dan sistem notifikasi berbasis waktu *(time-based alerting)* melalui email (Lhotsky, 2013).

ELK Stack adalah seperangkat perangkat lunak yang terdiri dari tiga komponen utama: Elasticsearch, Logstash, dan Kibana. Menurut Chhajed, S. (2015) Elasticsearch berfungsi sebagai mesin pencarian dan analitik yang dapat menyimpan dan mengelola data terstruktur dengan cepat, sementara Logstash digunakan untuk pengumpulan, pengolahan, dan pengiriman data log dari berbagai sumber ke Elasticsearch. Kibana menyediakan antarmuka pengguna web untuk membuat visualisasi interaktif dan dashboard berdasarkan data yang tersimpan di Elasticsearch, memungkinkan pengguna untuk melakukan pemantauan dan analisis data log dengan efisien. ELK Stack digunakan untuk keperluan analisis log dan visualisasi data yang dapat diterapkan di berbagai bidang seperti pemantauan jaringan, analisis keamanan, pemantauan aplikasi.

SMK Negeri 2 Sukoharjo adalah instansi pendidikan yang memanfaatkan internet sebagai penunjang dalam pembelajaran dan administrasi sekolah, baik untuk guru, karyawan, maupun para siswa. Beberapa perangkat komputer terhubung ke jaringan internet sekolah meliputi komputer instansi yang menjalankan sistem tata usaha sekolah, komputer guru yang digunakan dalam pembelajaran, serta komputer milik para siswa merupakan aktivitas yang dilakukan dalam jaringan. Dengan banyaknya jumlah pengguna yang mengakses jaringan tersebut, terlebih dengan diterapkannya jaringan Wi-Fi terbuka di SMK Negeri 2 Sukoharjo, membuka celah bagi pihak yang tidak bertanggungjawab untuk melakukan intrusi atau serangan terhadap perangkat komputer dan jaringan di sekolah. Hal tersebut menyebabkan aktivitas internet menjadi terganggu.

Berdasarkan observasi yang penulis lakukan terhadap jaringan komputer SMK Negeri 2 Sukoharjo, terdapat sebuah masalah yaitu dengan terbukanya akses jaringan internet, beberapa komputer rawan dijadikan target seperti serangan *bruteforce*, *port scanning*, DDoS, maupun serangan *malware* terhadap perangkat komputer tersebut. Selain itu juga belum terdapat sistem yang diterapkan untuk mendeteksi dan menangani adanya intrusi pada perangkat komputer yang terhubung ke jaringan. Penerapan IDS *(Intrusion Detection System)* sebagai alat untuk melakukan monitoring aktivitas perangkat pada jaringan komputer diperlukan dalam melindungi komputer-komputer yang menjadi aset internal sekolah dari gangguan keamanan sehingga pengelola jaringan atau administrator dapat melakukan tindakan pencegahan.

Berdasarkan uraian latar belakang masalah tersebut, penulis tertarik untuk melakukan penelitian yang berjudul "Analisis dan Implementasi *Open Source Host Intrusion Detection System Security* (OSSEC) pada SMK Negeri 2 Sukoharjo". Penelitian ini bertujuan untuk mengetahui efektifitas sistem deteksi intrusi berbasis host (HIDS) OSSEC yang diterapkan pada jaringan komputer SMK Negeri 2 Sukoharjo terhadap beberapa jenis gangguan keamanan.

1.2. RUMUSAN MASALAH

Rumusan masalah pada penelitian ini adalah:

1. Bagaimana kemampuan OSSEC sebagai alat monitoring keamanan jaringan yang diterapkan pada jaringan SMK Negeri 2 Sukoharjo?
2. Apa saja jenis serangan yang dapat dideteksi oleh OSSEC?
3. Bagaimanakah hasil penerapan IDS OSSEC dan ELK Stack dalam melakukan monitoring jaringan?

1.3. BATASAN MASALAH

Agar penelitian ini dapat terarah dan tidak keluar dari permasalahan yang ada, maka penulis membatasi ruang lingkup masalah sebagai berikut:

1. Mengimplementasikan sistem OSSEC sebagai alat untuk monitoring jaringan.
2. Melakukan pengujian keamanan jaringan dengan menjalankan beberapa skenario penyerangan, yaitu port scanning, brute force attack, DDoS, dan rootkit.
3. Melakukan analisis hasil pengujian sistem terhadap serangan yang dilakukan.
4. Batas cakupan pengujian yang dilakukan adalah dalam jaringan lokal SMK Negeri 2 Sukoharjo.

1.4. TUJUAN PENELITIAN

Penelitian ini memiliki tujuan yaitu mengimplementasikan sistem deteksi intrusi berbasis *host* (HIDS) OSSEC pada jaringan komputer pada SMK Negeri 2 Sukoharjo dan mengetahui efektifitas sistem HIDS OSSEC yang diterapkan terhadap beberapa jenis gangguan keamanan.

1.5. MANFAAT PENELITIAN

Melalui penelitian ini, diharapkan dapat memberikan manfaat sebagai berikut:

1. Manfaat Teoritis
   a. Memberikan wawasan dalam dunia akademik pada bidang keamanan jaringan komputer.
   b. Sebagai referensi pada penelitian-penelitian selanjutnya yang berhubungan dengan keamanan jaringan komputer.
2. Manfaat Praktis
   a. Bagi penulis

Menambah wawasan penulis dan mengembangkan teori yang telah dipelajari untuk diterapkan ke dalam dunia nyata.

b. Bagi instansi

Hasil dari penelitian ini diharapkan dapat meningkatkan keamanan jaringan komputer pada SMK Negeri 2 Sukoharjo.

BAB V
PENUTUP

5.1. KESIMPULAN

Berdasarkan hasil penelitian dan melakukan analisis hasil pengujian, maka dapat diambil kesimpulan sebagai berikut:

1. OSSEC memiliki kemampuan sebagai alat monitoring keamanan jaringan dengan cara mengumpulkan log untuk melakukan deteksi terjadinya serangan pada perangkat komputer di SMK Negeri 2 Sukoharjo. Jenis serangan yang dideteksi oleh OSSEC ditentukan oleh aturan *(rules)* dan pola serangan *(signature)* yang dikonfigurasi.
2. OSSEC dapat mendeteksi beberapa serangan seperti *port scanning, bruteforce, rootkit* dan DDoS. Selain itu kita dapat memperluas cakupan deteksi dengan menambahkan sensor OSSEC *localfile* untuk melakukan monitoring beberapa program di komputer agent atau dapat juga memasukkan *custom command* untuk dijalankan oleh OSSEC Agent. OSSEC dapat mendeteksi adanya masalah keamanan karena menerapkan logging dari Windows Firewall dan antivirus.
3. Penerapan OSSEC dan ELK Stack sebagai alat monitoring jaringan mempermudah dalam melakukan analisis log seperti pencarian data berdasarkan level *alert,* waktu, maupun deskripsi log. Selain itu kita juga dapat membuat visualisasi data dari log yang disimpan untuk menampilkan ringkasan data yang mudah dipahami.

5.2. SARAN

Untuk meningkatkan efektifitas OSSEC sebagai IDS, ada beberapa saran sebagai berikut:

1. Menerapkan *custom rules* untuk mendeteksi berbagai serangan yang tidak termasuk ke dalam konfigurasi *default* OSSEC.
2. Melakukan implementasi OSSEC ke perangkat komputer yang perlu dilakukan monitoring keamanan.

3. OSSEC tidak bisa mendeteksi serangan secara menyeluruh khususnya serangan pada perangkat jaringan seperti router, printer, dan sebagainya karena tidak ada kompatibilitas dengan OSSEC agent. Saran kedepannya adalah menerapkan sistem keamanan tambahan dengan menggunakan alat monitoring yang sesuai perangkat tersebut.

DAFTAR PUSTAKA

Lhotsky, Brad, (2013), *Instant OSSEC Host-based Intrusion Detection System – A hands-on guide exploring OSSEC HIDS for operational and security awareness*, Packt Publishing

Teixeira, Diogo, Assunção, L., Pereira, Malta, S., Pinto, P., (2019*), OSSEC IDS Extension to Improve Log Analysis and Override False Positive or Negative Detections,* Journal of Sensor and Actuator Networks Vol. 8 No. 46,, MDPI

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,* Pusat Operasi Keamanan Siber Nasional, BSSN, Jakarta.

Chhajed, Saurabh, (2015), *Learning ELK Stack,* Packt Publishing

Eri, Risa Susanti, Arif W., Wahyu A., (2020), *Implementasi Intrusion Prevention System (IPS) OSSEC dan Honeypot Cowrie,* Jurnal SISFOKOM Vol. 11 No. 1 Hal. 73-78, Institut Teknologi Telkom Purwokerto

Tanenbaum, Andrew S. & Wetherall, David J., (2011), *Computer Networks (Fifth Edition*), Pearson Education, Inc., Publishing as Prentice Hall

Yuliana, Yarmis, Hanriyawan A., Ronal H., (2022), *Deteksi Ancaman Keamanan pada Server dan Jaringan Menggunakan OSSEC,* (JITSI) Jurnal Ilmiah Teknologi Sistem Informasi Vol. 3 No. 1 Hal. 8-15

Sinambela, Eka S., (2020), *Evaluasi Performansi Deteksi Serangan pada HIDS OSSEC,* Jurnal Ilmiah KOHESI Vol. 4 No. 1 Januari 2020

Alamsyah, H., Riska, and Akbar, A., (2020), *Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System,* (JOINTECS) Journal of Information Technology and Computer Science Vol . 5 No. 1 (2020) 17 – 24

Sakti, Essy M.S., (2020) *Keamanan Informasi Lanjut Materi Ke 4,* Fakultas Teknik Universitas Persada Indonesia

Kizza, Joseph M., (2005), *Computer Network Security*, Springer Science & Business Media

Stallings, William, & Brown, L., (2015), *Computer Security Principles and Practice 3rd Edition*, Pearson Education, Inc.

Understanding the Five Phases of the Penetration Testing Process (2022, March 28). Retrieved November 20, 2023 from EC-Council

Adikara, Diksi Kalis (2013), *Implementasi Keamanan Sistem Komputer Menggunakan IPS (Intrusion Prevention System Berbasis OSSEC HIDS)*, Fakultas Ilmu Terapan, Teknik Komputer, Telkom University