e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Application Of Wazuh To Conduct Monitoring Network Security System (Case Study Of SMK N 1 Bengkulu City)

Penerapan Wazuh Untuk Melakukan Monitoring Sistem Keamanan Jaringan (Studi Kasus SMK N 1 Kota Bengkulu)

Edwin Aripilahi [1)]; Khairil [2)]; Abdussalam Al Akbar [3)]
[1,2,3)] ***Universitas Dehasen Bengkulu***
Email: [1)] edwinaripilahi@gmail.com

How to Cite :
Aripilahi, E., Khairil, K., Akbar, A, A. (2024). Application Of Wazuh To Conduct Monitoring Network Security System(Case Study of SMK N 1 Bengkulu City). Jurnal Media Computer Science, 3(2).

ARTICLE HISTORY
Received [08 Juni 2024]
Revised [09 Juli 2024]
Accepted [11 Juli 2024]

KEYWORDS
Wazuh, Network Monitoring, Network Security

ABSTRAK

Penerapan Wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu dapat membantu operator jaringan memonitoring sistem keamanan, komputer dan mempermudah melakukan kontrol pada perangkat yang di monitoring, sehingga dapat mengambil tindakan sesegera mungkin jika terjadi gangguan pada sistem dan jaringan berdasarkan hasil monitoring. Wazuh dapat memonitoring file-file yang ada di dalam folder directory. Informasi yang diberikan berupa aktifitas tambah, modifikasi, dan hapus file-file yang terdapat pada folder directory tersebut. Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa Penerapan Wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu berjalan dengan baik dan dapat membantu administrator jaringan dengan memberikan informasi terkait dengan perangkat agent yang di monitoring

ABSTRACT

The application of Wazuh to monitor network security systems at SMK Negeri 1 Bengkulu City can help network operators monitor security systems, computers and make it easier to control the devices being monitored, so that they can take action as soon as possible if there is a disruption to the system and network based on the monitoring results. Wazuh can monitor files in the directory folder. The information provided is in the form of adding, modifying and deleting files contained in the directory folder. Based on the tests carried out, the results showed that the application of Wazuh to monitor the network security system at SMK Negeri 1 Bengkulu City was running well and could help network administrators by providing information related to the agent device being monitored.

PENDAHULUAN

Sesuai dengan tuntutan pekerjaan untuk meningkatkan keamanan, jaringan komputer sebagai salah satu teknologi yang diharapkan dapat membantu terus perkembangan sesuai dengan kebutuhan para pengguna jaringan komputer. Hal ini terlihat dengan munculnya teknologi baru

dibidang jaringan komputer dengan sasaran peningkatan kemampuan yang lebih berorientasi pada keamanan jaringan dan keamanan perangkat komputer. Maka dari itu sangat diperlukan sebuah sistem yang dapat melakukan monitoring setiap saat.

Dalam menjaga kondisi keamanan jaringan ditemukan adanya masalah, seperti sulitnya memantau kondisi jaringan terhadap perubahan-perubahan yang terjadi seperti perubahan status jaringan dari hidup ke mati dan sebaliknya, kondisi yang mengakibatkan terjadinya jaringan mati antara lain kerusakan yang terjadi pada software maupun hardware contohnya pada software mengalami bug yang tidak diketahui dari mana penyebabnya, komunikasi dapat yang lambat dan pada hardware misalnya ethernet mati dan sering terjadinya tegangan listrik yang tidak stabil.

Kondisi tersebut timbul karena jaringan yang tidak terpantau sepenuhnya dikarenakan belum ada sistem yang melakukan monitoring secara real time, serta sistem yang harus mengawasi dengan cara mengecek kondisi server satu per satu. hal ini mengakibatkan penanganan masalah jaringan menjadi lambat. Untuk mengatasi permasalahan tidak terpantaunya kondisi jaringan dapat dilakukan dengan menerapkan sistem yang dapat melakukan monitoring Jaringan secara real time.

Dengan adanya sistem monitoring jaringan komputer pada SMK N 1 Kota Bengkulu dengan menggunakan tool Wazuh di harapkan dapat menciptakan keamanan perangkat dalam mengakses jaringan.Sehingga tidak mengganggu pekerjaan guru, tata usaha dan kegiatan belajar mengajar khususnya pelajaran yang berhubungan dengan penggunaan jaringan komputer.

Salah satu tools sistem monitoring jaringan yaitu Wazuh, merupakan sistem monitoring jaringan bersifat open source sehingga dapat dikonfigurasi sesuai dengan kebutuhan, kegunaannya antara lain untuk memantau kondisi jaringan di lingkungan yang kompleks di beberapa lokasi, Wazuh juga menghasilkan data kinerja dari hasil monitoring untuk pelaporan. Wazuh mampu memonitor segala sesuatu yang terhubung dengan jaringan yang akan ditangani, selain itu dapat mengirimkan notifikasi jika terdapat perubahan status dan Wazuh memungkinkan multi threaded (dapat melakukan monitoring berbagai macam aktifitas yang terjadi dalam jaringan).

Sistem monitoring jaringan yang diimplementasikan dapat diterapkan di SMK N 1 Kota Bengkulu untuk memonitoring jaringan komputer dan mempermudah melakukan kontrol serta perbaikan pada jaringan dan sistem.

LANDASAN TEORI

Implementasi

Menurut Muktar (2018:53), Implementasi merupakan sebuah teknik penerapan suatu sistem atau metode guna mendapatkankan hasil yang diinginkan dan mengurangi sebuah sistem menjadi bagian – bagian komponen dengan tujuan mempelajari seberapa baik bagian – bagian komponen dengan tujuan yang diharapkan. Analisa sistem merupakan tahapan awal dengan proses pengembangan sistem, sehingga tahapan ini menjadi acuan pelaksanaan pada proses pengembangan sistem.

Menurut Jeffrey (2019:24) Implementasi sistem adalah teknik penerapatan suatu metode pada rangkaian sistem dengan tujuan mempelajari komponen tersebut bekerja dan berinteraksi untuk menyelesaikan tujuan dan mendapatkan hasil yang baik.

Perancangan sistem merupakan pelengkap dari analisa sistem ke dalam suatu sistem yang utuh dengan tujuan mendapatkan sistem yang lebih baik. Ada enam tahap analisis sistem:

1. Mengumumkan penelitian sistem. Ketika perusahaan menerapkan sistem baru, manajemen bekerja sama dengan pekerja perihal sistem baru tersebut.
2. Mengorganisasikan tim proyek.
3. Mendefinisikan kebutuhan informasi. Melalui wawancara perorangan, pengamatan, pencarian catatan dan survey.
4. Mendefinisikan kriteria kinerja sistem Setelah kebutuhan informasi manajer didefinisikan, langkah selanjutnya adalah menspesifikasi secara tepat apa yang harus dicapai oleh sistem.

e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

5. Menyiapkan usulan rancangan, Analisa sistem memberikan kesempatan bagi para manajer untuk membuat keputusan terusan atau hentikan untuk kedua kalinya.
6. Menyetujui atau menolak rancangan proyek Manajer dan komite pengarah sistem informasi manajemen mengevaluasi usulan rancangan dan menentukan apakah memberi persetujuan atau tidak.

Tinjauan Linux Ubuntu

Menurut Santoso (2019:57) Linux adalah tiruan (clone) UNIX. Pengembangan Linux pertama kali dilakukan Linus Benedict Torvalds. Seluruh kode sumber Linux termasuk kernel, device drivers, libraries, program dan tool pengembangan disebarkan secara bebas dengan lisensi GPL (General Public License) versi kedua.

Berdasarkan basisnya, distro Linux dibagi antara :

1. Debian seperti Knoppix, Ubuntu, Kuliax, BlankON, dan lain-lain.
2. RPM (RedHat Package Manager) seperti PCLinuxOS, FedoraCore, IGOS, CentOS, EduLinux, dan lain-lain.
3. Slackware seperti Slackware, Kate OS, Truva Linux, ZenCafe Linux, Wolfix dan lain-lain.

Distribusi-distribusi menggunakan kernel Linux yang disetujui Linus Torvalds sehingga menjamin kompatibilitas. Perbedaan antara lain pada :

1. Paket-paket perangkat lunak yang disetakan di distribusi.
2. Struktur direktori.
3. Metode pemaketan perangkat lunak.
4. Inisialisasi sistem.

Ubuntu adalah salah satu distribusi Linux yang berbasiskan Debian GNU/Linux dan memiliki interface desktop (Wikipedia, 2008). Ubuntu adalah sepenuhnya sistem operasi open source yang dibangun berdasarkan kernel Linux. Nama Ubuntu sendiri diambil dari bahasa kuno Afrika Zulu dan Xhosa (oo-boon-too) yang artinya “rasa perikemanusiaan terhadap orang lain”.

Berdasarkan Ubuntu Documentation Project dijelaskan bahwa lingkungan desktop bawaan Ubuntu adalah GNOME, platform pengembangan dan keluarga desktop UNIX dan Linux terdepan. Skema penomoran versi Ubuntu didasarkan pada tanggal rilis sebuah versi dari distribusi. Nomor versi berasal dari tahun dan bulan rilis, bukan mencerminkan versi sebenarnya dari perangkat lunak.

Ubuntu mempunyai filosofi sebagai berikut:

1. Bahwa perangkat lunak harus tersedia dengan bebas biaya
2. Bahwa aplikasi perangkat lunak tersebut harus dapat digunakan dalam bahasa lokal masing-masing dan untuk orang-orang yang mempunyai keterbatasan fisik
3. Bahwa pengguna harus mempunyai kebebasan untuk mendapatkan, mengubah, dan mendistribusikan perangkat lunak sesuai dengan apa yang mereka butuhkan tanpa halangan apapun.

Ubuntu terdiri dari banyak paket, kebanyakan berasal dari distribusi di bawah lisensi lisensi software bebas. Namun, beberapa software khususnya driver menggunakan Proprietary software. Lisensi yang pada umumnya adalah GNU General Public License (GNU GPL) dan GNU Lesser General Public License (GNU LGPL), dengan tegas menyatakan bahwa pengguna dengan bebas dapat menjalankan, menggandakan, mempelajari, memodifikasi, dan mendistribusikan tanpa pembatasan apapun. Namun tetap ada software proprietary yang dapat berjalan di Ubuntu. Ubuntu berfokus pada ketersediaan kegunaan pada orang dengan disabilitas. Ubuntu juga berfokus pada internasionalisasi dan aksesibilitas untuk dapat menjangkau banyak orang. Dalam hal keamanan, perangkat sudo dapat meningkatkan privilage secara sementara untuk melakukan tugas administratif, sehingga akun root dapat terus terkunci, dan mencegah orang tidak terauthorisasi melakukan perubahan sistem atau membuka kelemahan keamanan.

Desktop Ubuntu memakai desktop environment grafis. Sebelum Ubuntu 11.04 interaksi grafis pengguna adalah GNOME versi 2, tetapi setelah versi 11.04, berubah menjadi Unity. Unity adalah lingkungan desktop yang dikembangkan oleh Canonical yang awalnya dirancang untuk edisi Netbook. Tetapi GNOME dipakai kembali mulai versi 17.10.

Jaringan Komputer

Menurut Fahlepi (2018:88) Jaringan komputer adalah kumpulan komputer dan perangkat lain yang saling berhubungan dan membentuk satu kesatuan sistem. Jaringan komputer memungkinkan informasi dan data untuk berpindah dari satu jaringan ke jaringan lain, sehingga memungkinkan pengguna jaringan komputer untuk bertukar dokumen dan data. Tidak hanya itu, jaringan komputer juga memungkinkan pengguna untuk mencetak ke printer yang sama dan menggunakannya bersama-sama.

Secara sederhana, dalam sebuah jaringan komputer, biasanya tersusun dari komputer Server yang berperan sebagai pusat pengaturan dan komputer Host sebagai tempat pengguna beroperasi. Adapun fungsi jaringan komputer yang paling sederhana adalah memudahkan membagi beban kerja perangkat untuk menjalankan sebuah program. Selain itu, fungsi jaringan komputer yang berikutnya adalah menghemat sumber daya.

Menurut Pratama (2019:12) Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat berkomunikasi satu sama lainnya "a network is a interconnection of a set of device capale of communication". Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan autonomous. Dua unit komputer dikatakan terkoneksi apabila keduanya bisa saling bertukar data / informasi.

Sejarah jaringan komputer dimulai pada tahun 1940 di Amerika Serikat melalui proyek pengembangan komputer Model I di laboratorium Bell dan kelompok riset Harvard University yang dipimpin oleh Howard Aiken. Saat itu, proyek tersebut hanya bertujuan untuk memanfaatkan sebuah perangkat komputer sehingga dapat dipakai bersama. Pada tahun 1950, saat komputer mulai berkembang dan superkomputer lahir, muncullah kebutuhan akan sebuah komputer yang mampu melayani banyak terminal. Kemudian ditemukanlah konsep TSS (Time Sharing System) atau sistem antrian. Pada tahun 1969, terbentuklah jaringan komputer pertama yang disebut ARPANET.

Topologi Jaringan

Menurut Muzakir (2019:14) Topologi dapat diartikan sebagai layout atau arsitektur atau diagram jaringan komputer. Topologi meupakan aturan bagai mana menghubungkan komputer secara fisik. Topologi berkaitan dengan cara komponen-komponen jarinagn (seperti: server workstation, router, switch) saling berkomunikasi melalui media tranmisi data. Ketika kita memilih satu topologi maka kita perlu menikuti spesifikasi yang diberlakukan atas topologi tersebut. Ada beberapa topologi utama yang sering di gunakan yaitu: Topologi bus, topologi star, topologi ring, topologi tree, topologi mesh.

Sistem Monitoring Jaringan

Menurut Dasanty (2020:39) Monitoring jaringan merupakan tugas berat dan tersulit bagian dari pekerjaan administrator jaringan secara berkala dalam menjaga kelancaran suatu jaringan. Jika jaringan mengalami masalah yang berhubungan dengan keamanan dan performa dengan waktu yang singkat maka akan berdampak pada kelangsungan suatu instansi yang menggunakan jaringan tersebut akan menurun. Untuk itu diperlukan sebuah fasilitas berupa sistem monitoring agar administrator dapat memonitoring jaringan.

Tinjauan Keamanan Jaringan

Menurut Ferdiansyah (2020:65) Keamanan jaringan adalah sebuah pekerjaan untuk memelihara seluruh sumber jaringan dalam keadaan baik. Sistem Keamanan jaringan adalah sekumpulan perangkat untuk memantau dan mengontrol jaringan. Sistem Keamanan jaringan

terdiri dari tambahan perangkat keras dan piranti lunak yang diimplementasikan di antara komponen–komponen jaringan yang sudah ada.

Konfigurasi keamanan Jaringan sangat penting karena meningkatkan kemampuan untuk skala infrastruktur TI tanpa meningkatkan staf administrasi TI untuk mengelola perangkat / sistem tersebut. Ini membuatnya layak untuk mengimplementasikan keamanan konfigurasi. Keamanan konfigurasi meliputi kegiatan administrasi yang menitikberatkan pada pembuatan, pemeliharaan, perubahan terkendali, dan kendali mutu produk. Pembuatan jaringan dilakukan kajian sesuai dengan kebutuhan seperti berapa alokasi bandwith yang dibutuhkan, sistem pengalamatan IP Address dan kebutuhan lainnya yang diperlukan. Untuk pemeliharaan sebisa mungkin dilakukan secara berkala seperti melakukan pengecekan kabel, melakukan restart server secara teratur dan lainnya agar jaringan computer yang dibangun dapat berfungsi dengan baik.

Tinjauan Kualitas Jaringan

Menurut Ahmad (2019:49) Kualitas jaringan didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan. Pada jaringan berbasis IP, IP QoS mengacu pada performansi dari paket -paket IP yang lewat melalui satu atau lebih jaringan.

Metode pengukuran yang digunakan untuk menentukan kemampuan sebuah jaringan seperti; aplikasi jaringan, host atau router dengan tujuan memberikan network service yang lebih baik dan terencana sehingga dapat memenuhi kebutuhan suatu layanan. Melalui QoS seorang network administrator dapat memberikan prioritas trafik tertentu. QoS menawarkan kemampuan untuk mendefinisikan atribut-atribut layanan yang disediakan, baik secara kualitatif maupun kuantitatif. Tujuan QoS menyediakan kualitas layanan yang berbeda-beda berdasarkan kebutuhan layanan di dalam jaringan. Quality of Service (QoS) merupakan sebuah arsitektur end-to-end dan bukan merupakan sebuah fitur yang dimiliki oleh jaringan. QoS suatu jaringan merujuk pada tingkat kecepatan dan kehandalan penyampaian berbagai jenis data di dalam suatu komunikasi

Parameter QoS adalah latency, jitter, packet loss, throughput, MOS, echo cancellation dan PDD. QoS sangat ditentukan oleh kualitas jaringan yang digunakan. Terdapat beberapa faktor yang dapat menurunkan nilai QoS, seperti : Redaman, Distorsi, dan Noise. QoS didesain untuk membantu end user (klien) menjadi lebih produktif dengan memastikan bahwa user mendapatkan performansi yang handal dari aplikasi-aplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Kemampuan QoS mengacu padae tingkat kecepatan dan kehandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi.

Menurut Alfatah (2019:29) Quality of Service (QoS) atau Kualitas layanan adalah metode pengukuran yang digunakan untuk menentukan kapabilitas jaringan, seperti Aplikasi jaringan, host, atau router untuk menyediakan layanan jaringan yang lebih baik dan lebih terencana yang memenuhi kebutuhan layanan.

Tinjauan Wazuh

Menurut Purbo (2019:67) Wazuh adalah tools untuk memonitor host atau perangkat yang biasanya digunakan oleh seorang SysAdmin dalam melakukan monitoring dan reporting. Wazuh sendiri dapat dikatakan sebagai versi pengembangan dari Nagios karena menggunakan plugin dari Nagios. Wazuh berjalan di hampir semua jenis sistem operasi.

Wazuh adalah perangkat lunak Monitoring Open Source yang memonitor host, aplikasi, dan services. Hasilnya mencakup keadaan dan metrik saat ini, keduanya dapat disimpan untuk jangka panjang. Alih-alih mengkonfigurasi semuanya secara statis, Wazuh memungkinkan Anda untuk membuat aturan berlaku yang menghasilkan objek pemantauan Anda secara dinamis.

METODE PENELITIAN

Dalam Penelitian proposal skripsi ini penulis menggunakan metode penelitian kuantitatif eksperimen. Metode ini bersifat validation atau menguji, yaitu menguji pengaruh satu atau lebih variabel terhadap variabel lain, seperti kinerja linux ubuntu server dalam menjalankan wazuh, kinerja wazuh dalam melakukan monitoring keamanan jaringan komputer di SMK N 1 Kota Bengkulu, dan waktu respon yang dibutuhkan wazuh dalam melakukan monitoring.

HASIL DAN PEMBAHASAN

Penerapan Wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu dapat membantu operator jaringan dalam memantau sistem keamanan setiap perangkat komputer yang terhubung pada jaringan hanya dengan satu unit komputer sebagai server, sehingga dapat mengambil tindakan sesegera mungkin jika terjadi gangguan pada jaringan berdasarkan hasil monitoring.

Untuk membuka tampilan awal wazuh pada web browser pastikan semua elemen wazuh seperti wazuh dashboard, wazuh manager, wazuh indexer, wazuh server dan filebeat semua aktif.

Pada tahap ini dilakukan pengujian terhadap infrastruktur jaringan yang telah diimplementasikan apakah berjalan dengan baik atau tidak. Pengujian Penerapan Wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu seperti Tabel 1.

Tabel 1 Hasil Pengujian

No	Indikator Pengujian	Hasil	Ket
1.	Monitoring Security Event dari agent Windows.	Wazuh dapat membaca log sistem operasi dan log aplikasi untuk selanjutnya diteruskan ke central manager yang selanjutnya di analisis berbasis penyimpanan (storage) dan role	Berhasil
2.	Monitoring Integrity Event dari agent Windows pada folder directory tertentu.	Wazuh dapat memantau file sistem, mengidentifikasi perubahan, dan atribut file yang perlu perhatikan. Selain itu, secara realtime mengidentifikasi pengguna dan aplikasi yang digunakan untuk membuat atau memodifikasi file.	Berhasil
3.	Pngujian respon aktif *security alert* wazuh dengan melakukan serangan brute-force ke komputer agent	Wazuh dapat medeteksi adanya serangan bruter force terhadap semua komputer agent yang termonitor..	Berhasil

Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa Penerapan Wazuh untuk melakukan monitoring dan manajemen jaringan di SMK Negeri 1 Kota Bengkulu berjalan dengan baik dan dapat membantu administrator jaringan dengan memberikan informasi terkait dengan perangkat agent yang di monitoring.

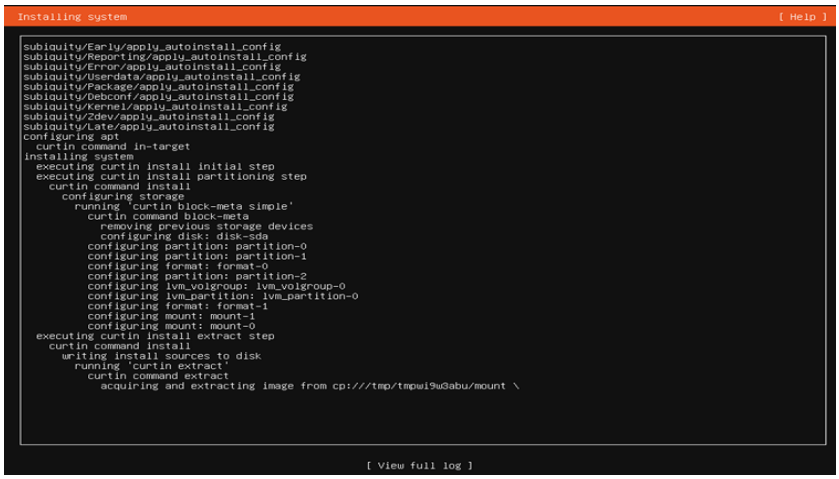
e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Pembahasan

Dalam Penerapan Wazuh untuk melakukan monitoring dan manajemen jaringan di SMK Negeri 1 Kota Bengkulu, terdapat beberapa tahapan yang dilakukan, diantaranya :

1. Menyiapkan Server Wazuh
   Tahap ini server yang digunakan berupa Virtual Machine yang dapat diakses melalui VMWare. Pada virtual machine server tersebut dilakukan instalasi sistem operasi Linux Ubuntu Server, seperti terlihat pada Gambar 1.

Gambar 1 Instalasi Linux Ubuntu Server Untuk Wazuh



2. Setelah instalasi sistem operasi linux ubuntu selesai, langkah selanjutnya melakukan instalasi wazuh pada server, dengan perintah : curl -sO https://packages.wazuh.com/4.5/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

3. Kemudian masuk ke Web UI Wazuh dengan cara ketik url https://IPAddressServer, dan akan tampil halaman login seperti Gambar 2.

Gambar 2 Login Web UI Wazuh

4. Setelah berhasil login, langkah selanjutnya mendaftarkan agent-agent yang akan dimonitoring oleh Wazuh, dimana dalam penelitian ini terdapat 2 perangkat yang akan dimonitoring dengan sistem operasi yaitu Windows dan Linux Ubuntu. Untuk itu, dilakukan proses definisi agent terlebih dahulu dengan klik , sehingga akan menampilkan halaman deploy new agent pada sistem operasi windows, seperti terlihat pada Gambar 3.

Gambar 4 Deploy New Agent

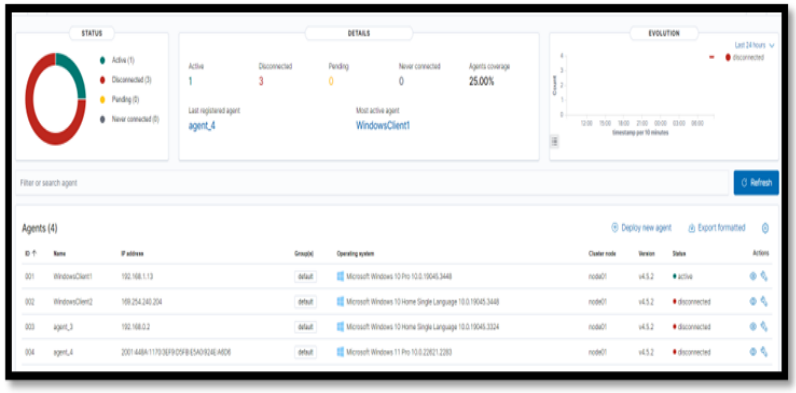
Pada Gambar 4 tersebut, terdapat 6 langkah yang harus dilakukan, antara lain :

a. Memilih sistem operasi yang digunakan oleh agent,
b. Memilih versi dari sistem operasi yang digunakan oleh agent
c. Memilih architecture yang digunakan oleh agent
d. Memasukkan IP Address dari Wazuh Server
e. Mendaftarkan nama agent baru tersebut
f. Melakukan instalasi pada agent agar terdeteksi oleh Wazuh Server, dengan perintah : Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.1.12' WAZUH_REGISTRATION_SERVER='192.168.1.12' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WindowsClient1'
g. Menjalankan agent dengan perintah : NET START Wazuh

5. Masuk ke agent yang akan didaftarkan, dengan masukkan perintah seperti :Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.5.2-1.msi -OutFile ${env:tmp}\wazuh-agent.msi; msiexec.exe /i ${env:tmp}\wazuh-agent.msi /q WAZUH_MANAGER='192.168.1.12' WAZUH_REGISTRATION_SERVER='192.168.1.12' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='WindowsClient1'

6. Kemudian cek dashboard Web UI Wazuh, dan secara otomatis akan menampilkan agent yang baru saja didaftarkan, seperti terlihat pada Gambar 5.

Gambar 5 Agent Yang Sudah Didaftarkan Ke Wazuh

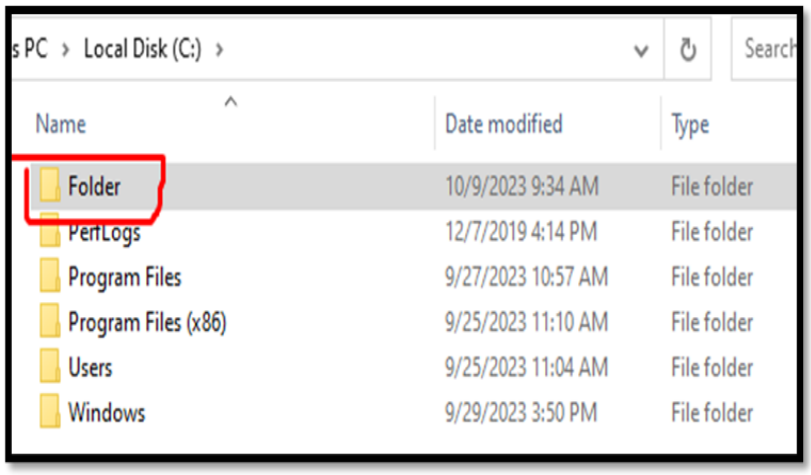


e-ISSN 2828-0490
JURNAL MEDIA COMPUTER SCIENCE

Selain itu, pada wazuh terdapat monitoring integrity event yang dapat memonitoring folder directory pada agent, dalam hal ini peneliti menggunakan sistem operasi Windows sebagai agent. Adapun tahapan yang dilakukan antara lain :

1. Membuat folder baru pada agent Windows, seperti terlihat pada Gambar 6.

Gambar 6 Membuat Folder Directory Baru



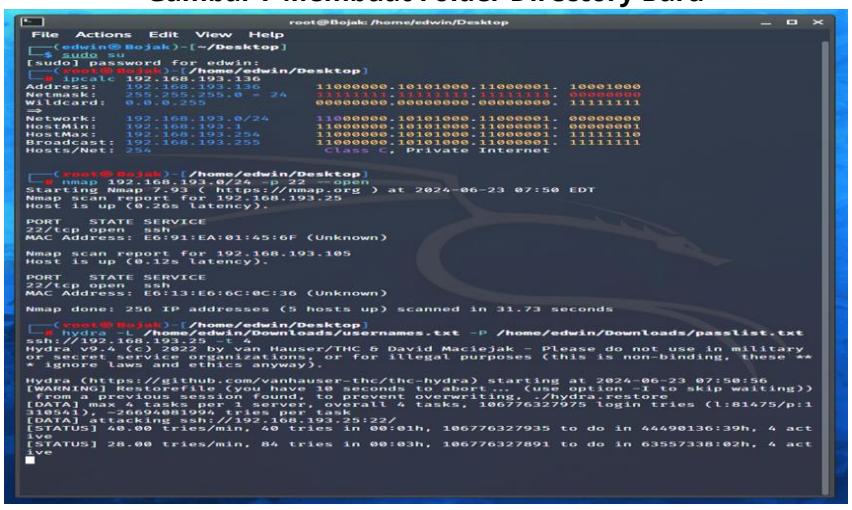
2. Kemudian konfigurasi file ossec.conf dan menambahkan bagian yang akan dimonitoring dengan perintah seperti; <directories check_all="yes" report_changes="yes" realtime="yes">C:\Folder</directories>

   Pada perintah tersebut, semua yang terjadi di dalam folder di drive C akan dilaporkan baik membuat file baru, memodifikasi serta menghapus file yang terdapat di folder directory tersebut.

3. Membuka dashboard Web UI Wazuh dan masuk ke integrity event, secara otomatis akan menampilkan log berupa grafik dan detail deskripsi yang terjadi pada folder directory yang dimonitoring.

Pada tahap akhir pengujian, peneliti melakukan serangan brute-force kepada salah satu komputer agent yang terhubung dan termonitoring oleh server wazuh untuk menguji kemampuan dari respon aktif security alert wazuh dalam memonitoring percobaan login pada SSH komputer agent.

Gambar 7 Membuat Folder Directory Baru

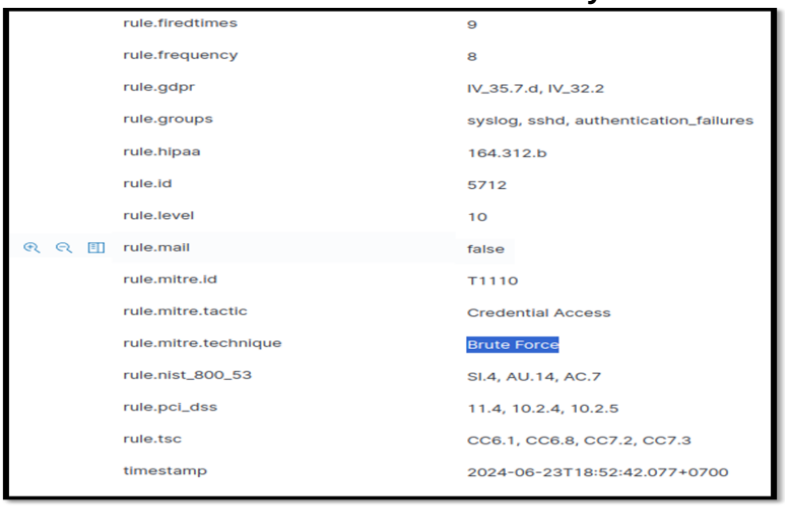


Pada Gambar 7. tersebut, terdapat 5 langkah yang harus dilakukan, antara lain :

1. Membuka terminal linux, pada pengujian ini peneliti menggunakan kali linux sebagai komputer pengirim serangan brute-force.
2. Kemudian masuk sebagai user root dengan perintah sudo su dan memasukan password login.
3. Masukan perintah ipcalc dengan ip komputer yang terhubung pada jaringan untuk memastikan ip network yang akan di lakukan scaning, seperti pada gambar di dapati bahwa ip network yang akan di lakukan scaning adalah 192.168.193.0/24
4. Masukan perintah nmap dengan ip network yang tadi di dapat kemudian tambahkan perintah -p 22 –open untuk melakukan scaning port 22 ssh yang terbuka, pada gambar terdapat ada dua ip yang memiliki port 22 ssh yang terbuka, yang pertama 192.168.193.105 yang merupakan port ssh milik server wazuh, kemudian yang kedua 192.168.193.25 yang merupakan port ssh komputer agent 07 yang telah peneliti lakukan instalasi open ssh untuk di lakukan pengujian serangan brute-force
5. Pada tahap akhir masukan perintah Hydra untuk memanggil tool hydra pada kali linux, yang kemudian tambahkan perintah -L /home/edwin/Downloads/usernames.txt untuk memanggil wordlist username pada directory penyimpanan dan tambahkan lagi perintah -P /home/edwin/Downloads/passlist.txt untuk memanggil wordlist password pada directory penyimpanan dan kemudian masukan perintah ssh://192.168.193.25 -t 4 untuk memulai serangan brute-force.

Kemudian kita kembali pada tampilan dashboard wazuh untuk memastikan bahwa serangan brute-force telah terdeteksi oleh server wazuh seperti pada gambar di bawah.

Gambar 8 Membuat Folder Directory Baru



Dari gambar di atas di dapati bahwa serangan brute-force terhadap ssh komputer agent telah terdeteksi secara rinci oleh server wazuh.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Penerapan Wazuh untuk melakukan monitoring dan manajemen jaringan di SMK Negeri 1 Kota Bengkulu dapat membantu operator jaringan memonitoring jaringan komputer dan mempermudah melakukan kontrol serta perbaikan pada jaringan dan sistem, sehingga dapat mengambil tindakan sesegera mungkin jika terjadi gangguan pada jaringan berdasarkan hasil monitoring.

2. Wazuh dapat memonitoring file-file yang ada di dalam folder directory. Informasi yang diberikan berupa aktifitas tambah, modifikasi, dan hapus file-file yang terdapat pada folder directory tersebut.
3. Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa Penerapan Wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu berjalan dengan baik dan dapat membantu administrator jaringan dengan memberikan informasi terkait dengan perangkat agent yang di monitoring

Saran

Berdasarkan kesimpulan, maka penulis menyarankan agar dapat menerapkan wazuh untuk melakukan monitoring sistem keamanan jaringan di SMK Negeri 1 Kota Bengkulu, sehingga membantu memberikan informasi administrator jaringan terkait dengan perangkat agent yang terdaftar di wazuh server.

DAFTAR PUSTAKA

Ahmad. S Abdullah. 2019. Analisis Quality Of Service (QoS) pada Wireless Local Area Network (WLAN) AD – Hoc dengan menggunakan antena buatan. Program Studi Sistem Informasi Universitas Gajah Mada. Yogyakarta

Alfatah, Dedi Muhammad. 2019. Pengaruh Kualitas Jaringan Internet Terhadap Kepuasan Pelanggan Indihome PT. Telkom. Jurnal Imiah Pendidikan dan Pembelajaran. p-ISSN : 1858-4543 e-ISSN : 2615-6091. Program Studi Magister Teknologi & Kejuruan, Fakultas Teknik, Universitas Negeri Padang

Dasanty, Laras Vriella. 2020. Studi Literatur Monitoring Manajemen Jaringan Internet Dengan Konsep SNMP Terhadap Akses Siswa. Jurnal IT-EDU. Pendidikan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Surabaya

Fahlepi, Roma Doni. 2018. Jaringan Komputer Dari Jarak Jauh Dengan Penerapan Hamachi VPN. Jurnal Evolusi. Universitas Bina Sarana Informatika

Februrian. 2020. Membangun Dan Menguji Web Browser Dan Server Pada Onion Web Server (Deepweb). Jurnal JARKOM. E-ISSN: 2338-6304. Institut Sains & Teknologi AKPRIND. Yogyakarta

Ferdiansyah, Pramudhita. 2020. Analisis Manajemen Bandwidth Menggunakan Hierarchical Token Bucket Pada Router dengan Standar Deviasi. Jurnal Nasional Teknologi dan Sistem Informasi. ISSN 2460-3465. Universitas Amikom Yogyakarta.

Hariyadi, I Putu. 2018. Analisa Penerapan Private Cloud Computing Berbasis Proxmox Virtual Environment Sebagai Media Pembelajaran Praktikum Manajemen Jaringan. Jurnal MATRIK. p-ISSN. 1858-4144. STMIK Bumigora. Nusa Tenggara Barat

Jeffrey, A Denzi. 2017. Handbook of Qualitative Research. Pustaka Pelajar. Yogyakarta

Muktar, Ahmad. 2018. Authentic Assessment: Penilaian Berbasis Kelas dan Kompetensi. Refika Aditama. Bandung

Muzakir, Muhammad. 2019. Optimasi Kinerja Jaringan Menggunakan HSRP (Hot Standbye Router Protocol). Bina Darma Conference on Computer Science. Fakultas Teknik Ilmu Komputer, Universitas Bina Darma

radikta, Jurista Purnama. 2018. Perancangan Sistem Monitoring Konsultasi Bimbingan Akademik Mahasiswa dengan Notifikasi Realtime Berbasis SMS Gateway. Jurnal Media Informatika Budidarma. ISSN 2614-5278. Fakultas Teknologi Komunikasi dan Informasi, Informatika, Universitas Nasional. Jakarta

Pratama, I Putu Agung. 2016. Handbook Jaringan Komputer – Edisi Revisi. Graha Ilmu. Yogyakarta

Purbo, Onno W. 2019. Macam-macam Tool Yang Dapat Digunakan Dalam Melakukan Monitor Jaringan Berbasis Open Source. Mediacom. Bandung

Santoso, Akhmad. 2019. Koneksi Internet Dengan Modem Handphonepada Sistem Operasi Linux

Ubuntu (Studi Kasus Pada SMA N 2 Semarang). Jurnal Ilmiah Fakultas Ilmu Terapan, Universitas Sains dan Teknologi(STEKOM). Semarang