IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER

(Skripsi)

Oleh

AZZAH SHAFIYYAH

PROGRAM STUDI S1 TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS LAMPUNG
BANDARLAMPUNG
2024

IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER

Oleh

AZZAH SHAFIYYAH

Skripsi

Sebagai Salah Satu Syarat untuk Mencapai Gelar
SARJANA TEKNIK

Pada

Program Studi S1 Teknik Informatika
Fakultas Teknik

PROGRAM STUDI S1 TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS LAMPUNG
BANDARLAMPUNG
2024

ABSTRAK

IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER

Oleh

Azzah Shafiyyah

PSDKU Universitas Lampung Way Kanan membutuhkan sistem keamanan jaringan yang efektif untuk melindungi jaringan komputer server lab komputer dari serangan siber yaitu *brute force* dan *Denial of Service* (DoS) Untuk meningkatkan keamanan jaringan, diperlukan implementasi sistem keamanan jaringan dengan menggunakan *platform* wazuh sebagai server monitoring dan wazuh *agent* yang diinstal pada komputer server jaringan lab komputer PSDKU menggunakan Server Utama PSDKU. Metode pengembangan sistem keamanan yang digunakan yaitu PPDIOO (*prepare, plan, design, implement, operate, optimize*) cisco. Dalam sistem ini, semua aktivitas dari wazuh agent akan dikirimkan ke wazuh server untuk dilakukan pemantauan dan deteksi serangan siber. Kemudian dilakukan simulasi serangan *brute force* dan *Denial of Service* (DoS) terhadap wazuh *agent* yang terinstal pada server jaringan lab komputer. Respon dari serangan bruteforce yang akan dilakukan adalah dengan memblokir alamat IP penyerang menggunakan *software* fail2ban dan serangan DoS dengan Active Response Wazuh sehingga penyerang tidak dapat mengakses dan tidak dapat terhubung ke komputer server jaringan lab komputer PSDKU. Sistem keamanan jaringan tidak dapat mendeteksi serangan DoS dengan jumlah rata-rata koneksi dibawah 4000 koneksi http, dan Serangan DoS berhasil dilakukan dengan hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan dalam menerima dan melayani koneksi HTTP dibawah 3.522.013 koneksi. Sehingga sistem keamanan jaringan dapat ditingkatkan dan respon terhadap serangan siber dapat dilakukan secara cepat dan efektif.

Kata kunci : *Keamanan Jaringan, Brute Force, DoS,* PSDKU, *PPDIOO*

ABSTRACT

IMPLEMENTATION OF THE NETWORK SECURITY SYSTEM AT PSDKU LAMPUNG WAYKANAN UNIVERSITY USING WAZUH SERVERS FOR CYBER ATTACK DETECTION AND RESPONSE

By

Azzah Shafiyyah

To improve network security, it is necessary to implement a network security system using the wazuh platform as a monitoring server and wazuh agent installed on the PSDKU computer network server using PSDKU Main Server. The method of development of the security system used is PPDIOO (prepare, plan, design, implement, operate, optimize) cisco. In this system, all the activities of the agent will be sent to the server for monitoring and detection of cyber attacks, then simulated brute force and Denial of Service (DoS) attacks against the agent installed on the computer lab network server. The response to a bruteforce attack is to block the attacker's IP address using file2ban software and DoS attacks with Active Response Wazuh so that the attackers can't access and connect to the computer server of the PSDKU computer's lab network. The network security system could not detect a DoS attack with an average number of connections below 4000 http connections, and the DoS Attack was successfully carried out with results showing that PSDKU's Main Server has resilience in receiving and serving HTTP connections under 3.522.013 connections. So the network security system can be improved and the response to cyber attacks can be carried out quickly and effectively.

Keywords: Network Security, Brute Force, DoS, PSDKU, PPDIOO

Judul Skripsi	:	**IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER**
Nama Mahasiswa	:	**Azzah Shafiyyah**
Nomor Pokok Mahasiswa	:	2065061001
Program Studi	:	S1 Teknik Informatika
Fakultas	:	Teknik

MENYETUJUI

1. Komisi Pembimbing

Pembimbing Utama	Pembimbing Pendamping
Ir. Gigih Forda Nama, S.T., M.T.I, IPM.	**Rio Ariestia Pradipta, S.Kom., M.T.I.**
NIP. 198307122008121003	NIP. 198603232019031013

2. Mengetahui

Ketua Jurusan Teknik Elektro	Ketua Program Studi Informatika
Herlinawati, S.T., M.T.	**Yessi Mulyani, S.T., M.T.**
NIP. 197103141999032001	NIP 197312262000122001

MENGESAHKAN

1. Tim Penguji

Ketua : **Ir. Gigih Forda Nama, S.T., M.T.I, I.P.** .....

Sekretaris : **Rio Ariestia Pradipta, S.Kom., M.T.I.** .....

Penguji : **Ir. M. Komarudin, S.T., M.T.** .....

2. Dekan Fakultas Teknik

Dr. Eng. Ir. Helmy Fitriawan, S.T., M.Sc.

NIP 197509282001121002

Tanggal Lulus Ujian Skripsi : 15 Januari 2024

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini, menyatakan bahwa skripsi saya dengan judul "Implementasi Sistem Keamanan Jaringan Di PSDKU Universitas Lampung Waykanan Menggunakan Server Wazuh Untuk Deteksi Dan Respon Serangan Siber" dibuat oleh saya sendiri. Semua hasil yang tertuang dalam skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti bahwa skripsi ini merupakan salinan atau dibuat oleh orang lain, maka saya bersedia menerima sanksi sesuai dengan ketentuan hukum atau akademik yang berlaku.

Bandar Lampung, 20 Januari 2024

Pembuat pernyataan,

Azzah Shafiyyah

NPM 2065061001

RIWAYAT HIDUP

Penulis dilahirkan di Kotabumi Lampung Utara, pada tanggal 28 Februari 2002. Penulis merupakan anak kedua dari pasangan Bapak Juliarsyah Harahab S.Ag dan Ibu Nani Sriwijayanti S.E.

Penulis menyelesaikan pendidikannya di SD Negeri 4 Kotabumi pada tahun 2015, SMP Negeri 7 Kotabumi pada tahun 2017, dan SMA Negeri 3 Kotabumi pada tahun 2020. Pada tahun 2020, penulis terdaftar sebagai mahasiswa Program Studi Teknik Informatika, Jurusan Teknik Elektro, Fakultas Teknik Universitas Lampung melalui jalur Prestasi Khusus.

Selama menjalani proses perkuliahan secara aktif, penulis mengikuti Himpunan Mahasiswa Teknik Elektro (HIMATRO) sebagai anggota Divisi Minat dan Bakat pada periode 2020 – 2022. Selain proses perkuliahan, penulis juga pernah menjalankan magang di Balitbang Kementerian Komunikasi dan Informatika Republik Indonesia sebagai *Cyber Security*, PT Sinergi Transformasi Digital sebagai Network Security Operation Center (Cyber Blue Team). Selain itu juga saya mengikuti kegiatan diluar maupun di dalam kampus seperti kegiatan kepanitiaan event-event lainnya.

Prestasi yang pernah dicapai penulis antara lain adalah sebagai Peraih Sertifikasi Global CCNA (Internasional) yang diadakan di Bali serta menjadi delegasi Mahasiswa Universitas Lampung di Acara G20, Bali 2022.

Keahlian penulis adalah dalam *Cyber Security*, *Security Engineer*.

MOTTO

"Work until you don't have to introduce yourself."

(**Penulis**)

"Jangan menjelaskan dirimu kepada siapapun, karena yang menyukaimu tidakbutuh itu dan yang membencimu tidak percaya itu."

(Ali bin Abi Thalib)

"Allah tidak membebani seseorang melainkan sesuai dengan kesanggupannya."

(Q.S Al Baqarah:286)

"*There are so many great things in life, why dwell on negativity?*"

(Zendaya)

Sujud syukur saya persembahkan kepada Allah ....

Tuhan Yang Maha Esa dan Maha Besar. Berkat limpahan rahmat-Nya saya bisamenjadi pribadi yang bertaqwa, beriman, dan berilmu. Semoga dengan keberhasilan yang telah dicapai ini, saya dapat menuju masa depan yang lebih baik dan dapat menggapai cita -cita serta selalu berada di jalan-Nya.

SAYA PERSEMBAHKAN SKRIPSI INI TERUNTUK:

"Mama Nani dan Papa Juli atas dukungan dan kasih sayang yang diberikan mulai dari saya ada di dunia ini sampai saya sudah besar seperti sekarang ini. Terima kasih kepada Mama dan Papa atas doa yang tak henti - hentinya diberikan serta pengorbanan yang tak terhitung nilainya. Semoga dengan ilmu dan cita - cita yang saya dapatkan kelak akan menjadi amal jariyah bagi Mama dan Papa."

"Terima kasih untuk abang dan adik – adik saya M. Naufal Mahdy, Nabila Haniyah, dan M. Fadhil Fitrizky yang selalu menghibur saat di rumah. Semoga kalian kelak menjadi pribadi yang lebih baik dan sukses."

"Diri saya sendiri. Terima Kasih telah berjuang, melewati rintangan dan berbagai zona nyaman, dan bekerja sama selama ini."

"Terima kasih kepada teman-teman Teknik Informatika Kelas A 2020 yang telah menemani dan membantu saya selama perkuliahan di kampus tercinta Universitas Lampung. Semoga kelak kita semua akan menjadi orang-orang yang sukses."

"Terima kasih kepada seseorang yang tidak henti - hentinya memberikan dukungan, menghadapi saya ketika berada di titik terendah di hidup saya, memberikan semangat untuk saya agar bisa menghadapi semua tantangan dan ketidak percayaan diri saya. *Best wishes to you.*"

SANWACANA

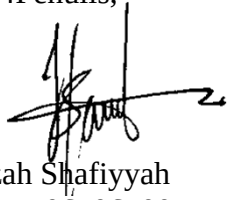
Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayat-Nyasehingga penulis dapat menyelesaikan penyusunan skripsi ini dengan judul "Implementasi Sistem Kramanan Jaringan Di PSDKU Universitas Lampung Way Kanan Menggunakan Server Wazuh Untuk Detekso Dan Respon Serangan Siber. Dalam pelaksanaan dan pembuatan skripsi ini penulis menerima dukungan baik secara moral maupun materil yang sangat berharga dari berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada semua pihak yang telah membantu, khususnya kepada:

1. Allah SWT yang senantiasa memberikan kemudahan dan kelancaran kepada penulis dalam menyelesaikan penelitian dan skripsi ini.
2. Rasulullah SAW yang telah menjadi suri tauladan di sepanjang hidup saya.
3. Mama dan Papa, Abang, Kakak, dan Adek serta keluarga penulis yang selalu memberikan motivasi dan dukungan kepada penulis.
4. Bapak Dr. Eng. Ir. Helmy Fitriawan, S.T., M.Sc., selaku Dekan Fakultas Teknik Universitas Lampung.
5. Ibu Herlinawati, S.T., M.T. selaku Ketua Jurusan Teknik Elektro Universitas Lampung.
6. Ibu Yessi Mulyani, S.T., M.T. selaku Ketua Program Studi Teknik Informatika Universitas Lampung dan telah membantu kelancaran pengerjaan penelitian.
7. Bapak Ir. Gigih Forda Nama, S.T., M.T.I., I.P.M. selaku Pembimbing Utama yang selalu meluangkan waktunya untuk memberikan bimbingan, arahan, dan dukungan.
8. Bapak Rio Ariestia Pradipta, S.Kom, M.T.I. selaku Pembimbing Pendamping yang selalu memberikan motivasi dan memberikan bimbingan kepada penulis untuk menjadi lebih baik.

9. Bapak Ir. M. Komarudin, S.T., M.T. selaku Penguji dalam siding skripsi yang juga turut memberikan bimbingan dan arahan.
10. Bapak Wahyu Eko Sulistiono, S.T., M.SC. selaku Pembimbing Akademik yang telah memberikan bimbingan selama perkuliahan di setiap semester dan selalu memberikan motivasi.
11. Mbak Rika selaku Admin Program Studi Teknik Informatika yang telah banyak membantu penulis dalam segala urusan administrasi selama perkuliahan.
12. Seluruh dosen dan staff Program Studi Teknik Informatika Universitas Lampung yang memberi masukan dan mempermudah proses pembuatan skripsi ini.
13. Teman-teman seperjuangan khususnya M. Aldy Antoro, Naomi Belinda Manurung, teman - teman Magang Kominfo yaitu Kak Gufron, Evnur dan Rizwal, Grup Princezz, dan YHG yang telah banyak memberikan saran, dukungan, dan bantuannya.
14. Tim PSDKU Universitas Lampung Way Kanan terutama Kak Suta, Kak Tomi dan Kak El yang turut serta membantu kelancaran penelitian dan pembuatan skripsi ini.
15. Semua pihak yang turut serta dalam membantu menyelesaikan penelitian dan tidak bisa penulis sebutkan satu persatu.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi pembacanya.

Bandar Lampung, 20 Januari 2024Penulis,



Azzah Shafiyyah
NPM.206506100

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

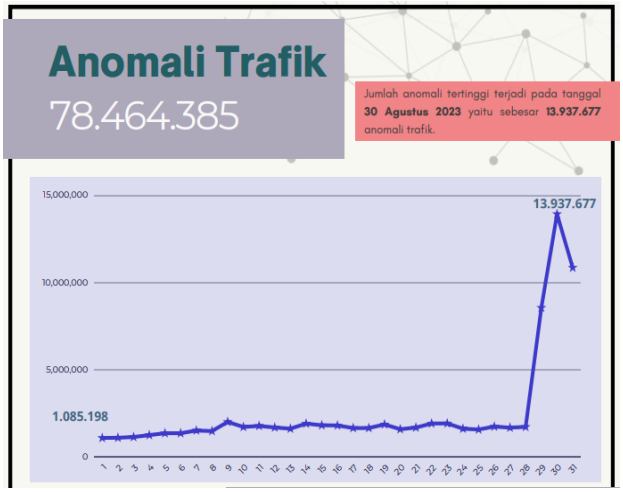
BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan siber merupakan bidang yang berkaitan dengan melindungi sistem komputer, jaringan, dan data dari ancaman dan serangan yang dilakukan secara elektronik. Ancaman-ancaman dalam dunia maya dapat berasal dari berbagai pihak seperti *hacker*, *malware, phishing* dan masih banyak lagi. Maka dari itu, praktik-praktik keamanan siber seperti penggunaan firewall, enkripsi data sensitif, pemantauan aktivitas jaringan secara *real-time*, serta pelatihan kesadaran tentang keamanan bagi pengguna menjadi sangat penting untuk melawan ancaman-ancaman tersebut. [1]

Dalam era digital saat ini, jaringan menjadi bagian yang penting dalam suatu organisasi. [2] Terlebih lagi pada sektor pendidikan, khususnya PSDKU Universitas Lampung di Way Kanan. PSDKU Universitas Lampung Way Kanan adalah salah satu cabang Universitas Lampung yang terletak di Way Kanan atau Program PSDKU adalah salah satu upaya Universitas Lampung untuk meningkatkan peran Universitas Lampung dalam bidang pembangunan nasional dan daerah terutama dalam peningkatan aksesibilitas pendidikan tinggi, dan pembangunan sumberdaya manusia di Kabupaten Way Kanan. PSDKU Universitas Lampung Way Kanan memiliki jaringan yang kompleks. Namun, dengan semakin kompleksnya jaringan, maka semakin besar pula resiko keamanan informasi. Salah satu ancaman yang sering terjadi adalah serangan siber, yang dapat menyebabkan kerugian finansial, pencurian identitas, atau bahkan merusak reputasi sebuah organisasi. Beberapa kasus serangan siber yang pernah terjadi di indonesia (dikutip dari kompas.com) diantaranya adalah Pada tanggal 6 Oktober 2021, situs *Project Multatuli* diserang secara siber menggunakan serangan *Denial of Service (DoS)*, yang mengakibatkan situs tersebut sulit diakses selama beberapa hari. Selain itu Berdasarkan Laporan Bulanan Publik: Hasil

Monitoring Keamanan Siber pada Agustus 2023 mencatat sebanyak 78.464.385 *anomali trafik* yang termasuk serangan siber dan menyebarkan *malware.* [1]



Gambar 1.1 Jumlah Anomali Trafik

Oleh karena itu, sangat penting bagi PSDKU Universitas Lampung Way Kanan untuk menerapkan sistem keamanan jaringan yang efektif.

PSDKU Universitas Lampung Way Kanan merupakan salah satu lembaga pendidikan yang memiliki jaringan komputer. Namun, PSDKU Universitas Lampung Way Kanan menghadapi beberapa masalah dalam menghadapi ancaman serangan siber. Dari hasil wawancara yang te;ah dilakukan di PSDKU, salah satu masalah yang dihadapi adalah tidak adanya sistem keamanan jaringan yang berguna untuk melindungi server jaringan PSDKU Universitas Lampung Way Kanan khususnya Lab Komputer. Tanpa adanya sistem keamanan jaringan yang memadai, jaringan PSDKU di Lab Komputer rentan terhadap ancaman serangan siber. Masalah lain yang dihadapi adalah tidak adanya sistem keamanan jaringan yang berguna untuk memberikan informasi tentang peristiwa keamanan jaringan komputer server di PSDKU Universitas Lampung Way Kanan di Lab Komputer secara *real time*. Informasi tentang peristiwa keamanan server penting untuk mendeteksi dan merespon serangan siber

yang terjadi pada jaringan. Dalam rangka meningkatkan keamanan sistem, diperlukan implementasi sistem keamanan jaringan dengan menggunakan *Security Information and Event Management* (SIEM) sebagai server *monitoring* dan Wazuh *Agent* yang diinstal pada jaringan komputer server di PSDKU. Melalui sistem keamanan yang akan dibangun ini, semua peristiwa keamanan dari Wazuh *Agent* akan dikirimkan ke wazuh server untuk dilakukan pemantauan dan deteksi serangan siber, serta Wazuh menggunakan Aplikasi Telegram untuk mengirimkan notifikasi khusus monitoring aktivitas Log kepada administrator. Selain itu, akan dilakukan pengujian serangan *Brute force* terhadap wazuh agent yang terinstal pada jaringan komputer server di PSDKU di Lab Komputer Jika terjadi serangan, respon yang akan dilakukan adalah dengan memblokir alamat IP penyerang menggunakan perangkat lunak *Fail2ban* sehingga penyerang tidak dapat mengakses dan tidak dapat terhubung ke jaringan komputer server Lab Komputer. Dengan demikian, sistem keamanan dapat ditingkatkan dan respon terhadap serangan siber dapat dilakukan secara cepat dan efektif. Berdasarkan uraian di atas penulis mengambil judul tugas akhir yaitu "**IMPLEMENTASI SISTEM KEAMANAN JARINGAN DI PSDKU UNIVERSITAS LAMPUNG WAYKANAN MENGGUNAKAN SERVER WAZUH UNTUK DETEKSI DAN RESPON SERANGAN SIBER"**

1.2. Rumusan Masalah

Adapun rumusan masalah yang dibahas pada penelitian ini adalah :

1. Bagaimana membangun sistem keamanan jaringan yang dapat mendeteksi dan merespon terhadap serangan siber pada jaringan server komputer di PSDKU Universitas Lampung Way Kanan ?
2. Apakah semua log yang terjadi dapat direkam pada saat serangan terjadi?

1.3. Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah :

1. Ruang lingkup penelitian hanya meliputi jaringan di PSDKU Universitas Lampung Way Kanan khususnya pada jaringan komputer server di Lab Komputer.
2. Serangan siber terhadap server jaringan Lab Komputer PSDKU Universitas Lampung Way Kanan yang dilakukan untuk uji coba yaitu *Brute force attack* dan *Denial of Service* (DoS).
3. *Fail2ban* digunakan untuk merespon serangan *Brute force* dan *Denial of Service* (DoS).

1.4. Tujuan Penelitian

Adapun Tujuan dari penelitian ini adalah:

1. Untuk membangun sistem keamanan jaringan yang dapat mendeteksi dan merespon terhadap serangan siber pada jaringan komputer server di PSDKU Universitas Lampung Way Kanan khususnya di Lab Komputer.
2. Mengintegrasikan sistem Wazuh notifikasi/*alert* dengan menerapkan bahasa pemrograman python dan bash shell melalui Telegram sebagai media notifikasi ketika adanya masalah atau gangguan pada server wazuh,

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Mendeteksi serangan siber dan meningkatkan keamanan jaringan PSDKU Universitas Lampung Way Kanan di Lab Komputer dengan menganalisis peristiwa keamanan wazuh *Agent.*
2. Memberikan informasi kepada *administrator* wazuh server tentang aktivitas wazuh *agent* secara *real time* melalui *dashboard* wazuh *manager*. Hal ini memungkinkan *administrator* wazuh server untuk mengidentifikasi dan mengatasi masalah dengan lebih cepat.
3. Wazuh dapat mengirimkan chat notifikasi Aktivitas *Log Monitoring* wazuh *agent* atau *Security Events* di wazuh server melalui Telegram kepada administrator
4. Melakukan respon terhadap serangan siber guna mengurangi resiko kerusakan jaringan.

1.6. Sistematika Penulisan

Sistematika penulisan laporan akhir bertujuan supaya memberikan suatu gambaran secara sederhana terkait pembahasan yang ada dalam tugas akhir skripsi serta untuk memudahkan dalam memahami isi yang disajikan dalam skripsi ini. Adapun sistematika yang digunakan oleh penulis adalah sebagai berikut :

BAB I: PENDAHULUAN

BAB I merupakan pendahuluan berisi tentang latar belakang, tujuan, rumusan masalah, batasan masalah, manfaat penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

BAB II merupakan tinjauan pustaka berisi definisi mengenai beberapa istilah dalam pengerjaan skripsi yang diambil dari berbagai sumber (buku, jurnal, dan sebagainya). BAB II secara garis besar berisi tentang pengertian PSDKU Universitas Lampung Way Kanan,Keamanan Jaringan, SIEM, Wazuh, *Hydra*, *File2ban*, Jaringan Internet, Serangan Siber (*Cyber Attack), Cyber Security, Bruteforce, Set Top Box*, Sistem Operasi, Ubuntu, Kali Linux, DoS, Slowloris, Telegram, Vmware vSphere, PPDIOO, dan Penelitian Terkait.

BAB III : METODOLOGI PENELITIAN

BAB III merupakan metodologi penelitian berisikan tempat dan waktu penelitan, jadwal penelitian, alat dan bahan penelitian, dan metode yang digunakan dalam penelitian yaitu PPDIOO Cisco yaitu *prepare, plan, design*.

BAB IV : HASIL DAN PEMBAHASAN

BAB IV merupakan Hasil dan Pembahasan tentang metode PPDIOO Cisco *implement, operate, optimize* yaitu implementasi sistem yang sedang berjalan, mengoperasikan sistem keamanan siber, serta optimalisasi terhadapan serangan siber untuk dilakukan guna menghindari kerusakan yang lebih serius.

BAB V : KESIMPULAN DAN SARAN

BAB V merupakan kesimpulan dari hasil dan saran berdasarkan penelitian yang dilakukan serta pengolahan data dan saran yang sesuai dengan hasil penelitian

DAFTAR PUSTAKA

LAMPIRAN

BAB II
TINJAUAN PUSTAKA

2.1 PSDKU Universitas Lampung Way Kanan

Program Studi di Luar Kampus Utama (PSDKU) adalah program studi yang diselenggarakan oleh sebuah perguruan tinggi yang menyediakan pendidikan akademik di luar wilayah kabupaten/kota/kota administratif tempat kampus utama perguruan tinggi tersebut berada. Perguruan tinggi harus mendapatkan izin dari Mendikbud sebelum menjalankan program studi ini. Kampus utama adalah tempat domisili perguruan tinggi yang menyelenggarakan pendidikan akademik di wilayah kabupaten/kota/kota administratif, sesuai dengan keputusan Menteri yang mengatur pendirian perguruan tinggi tersebut.

PSDKU Unila Way Kanan merupakan bagian dari inisiatif Universitas Lampung (Unila) untuk memperkuat pembangunan nasional dan daerah, terutama dalam meningkatkan akses pendidikan tinggi dan pengembangan sumber daya manusia di Kabupaten Waykanan. Program PSDKU Unila Way Kanan adalah bukti nyata komitmen Unila dalam mengurangi kesenjangan akses pendidikan tinggi di wilayah Lampung. Pemilihan Kabupaten Way Kanan sebagai lokasi program PSDKU didasarkan pada letak geografisnya yang strategis, memungkinkan akses dari beberapa kabupaten di Provinsi Lampung. Saat ini, program studi yang tersedia adalah Diploma III Akuntansi, sementara program Sarjana Ilmu Komputer akan segera dibuka. Dalam tahun ajaran baru 2023/2024 ini, terdapat 40 mahasiswa baru prodi D3 Akuntansi yang terdaftar menjadi mahasiswa pada program PSDKU Kab. Way Kanan melalui ujian mandiri. Para mahasiswa baru ini akan mengikuti pendidikan yang telah disesuaikan dengan kebutuhan Kabupaten Way Kanan dan belajar sesuai dengan kurikulum yang sudah disesuaikan dengan diajar oleh dosen yang berkualitas.

2.2 Keamanan Jaringan

Keamanan jaringan atau network security adalah sebuah sistem yang bertugas untuk mengidentifikasi dan mencegah akses tidak sah pada suatu jaringan. Upaya ini bertujuan agar akses penyusup pada sistem jaringan tersebut dapat segera dihentikan. Dengan kata lain, network security mengantisipasi ancaman serangan yang berpotensi merusak sistem keamanan jaringan, baik logic maupun fisik. Keamanan jaringan sendiri mencakup berbagai jaringan perangkat, baik pribadi maupun jaringan yang bersifat publik. Keamanan jaringan melibatkan *access authorization* ke data yang ada di dalam suatu jaringan. Sebagai proteksi sumber daya atau network resource. Keamanan jaringan adalah sistem yang dirancang untuk melindungi jaringan dari ancaman eksternal dan mencegah pencurian data. Tujuannya adalah memberikan perlindungan terhadap berbagai serangan yang dapat merusak integritas dan kerahasiaan jaringan. Dalam konteks ini, keamanan jaringan menggunakan metode dan teknologi untuk mengidentifikasi, mencegah, dan merespons ancaman seperti serangan *brute force*, *malware*, serangan *Denial of Service (DoS)* , peretasan, dan upaya pencurian data. [2]

2.3 *Security Information and Event Management* (SIEM)

SIEM adalah singkatan dari *"Security Information and Event Management"* SIEM diterjemahkan sebagai "Manajemen Informasi dan Keamanan Peristiwa." sistem yang digunakan untuk memantau dan mendeteksi serangan serta merespon keamanan melalui analisis *log* dari berbagai event yang diperoleh dari sumber data secara *real-time*. Teknologi ini memiliki jangkauan pengumpulan data yang luas dan dapat mengaitkan serta menganalisis *event* dari berbagai sumber dan menentukan apakah kejadian tersebut merupakan serangan atau tidak. Analisis SIEM mencakup semua aplikasi yang digunakan perusahaan, perangkat jaringan, perangkat keamanan, dan *server*. Sistem SIEM bekerja dengan mengumpulkan dan menganalisis data dari berbagai sumber dalam suatu infrastruktur IT, seperti log dari perangkat jaringan,

sistem operasi, aplikasi, dan perangkat keamanan. Data ini kemudian diagregasi dan dianalisis untuk mendeteksi aktivitas yang mencurigakan atau ancaman keamanan.

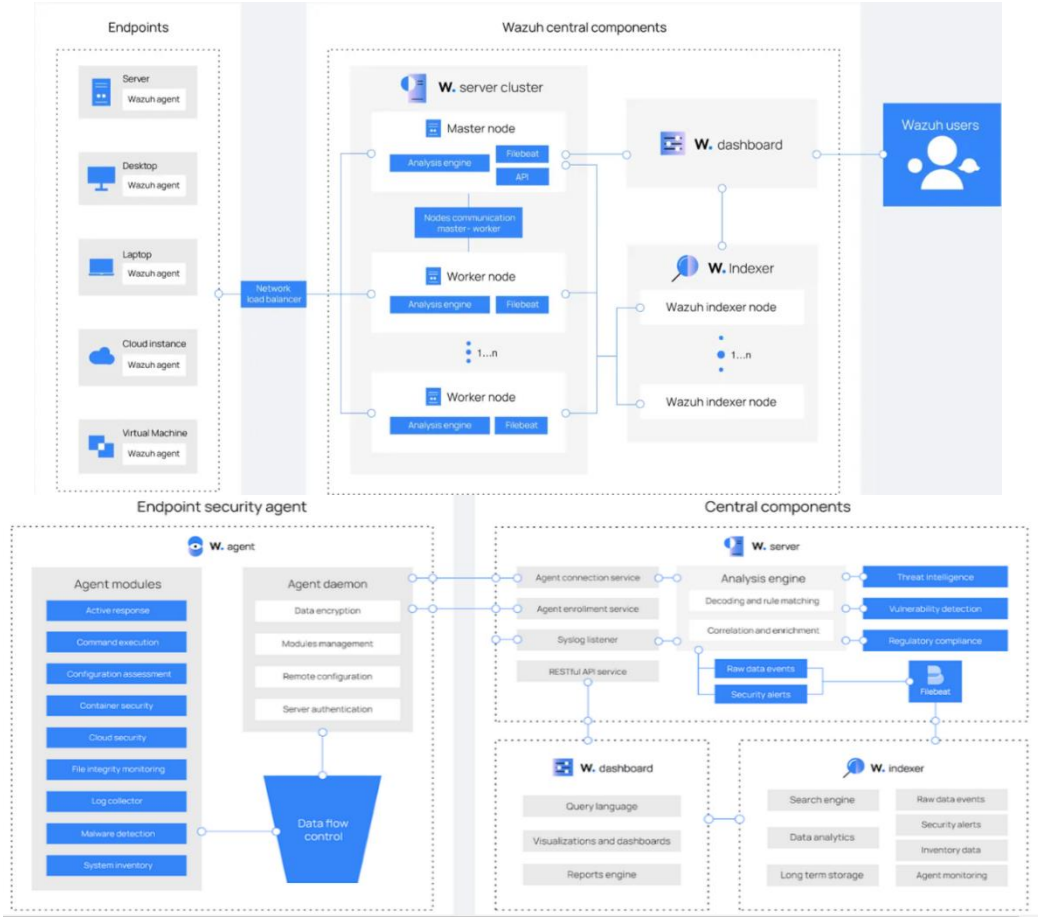
Beberapa fungsi utama dari SIEM meliputi:

1. Pengumpulan Data: SIEM mengumpulkan data keamanan dari berbagai sumber, seperti log perangkat keras, perangkat lunak, dan perangkat keamanan.
2. Pengolahan dan Normalisasi: Data yang dikumpulkan diolah dan dinormalisasi agar dapat diintegrasikan dengan baik dan mudah diolah.
3. Deteksi Ancaman: SIEM menganalisis data untuk mendeteksi pola atau tanda-tanda aktivitas yang mencurigakan atau ancaman keamanan.
4. Manajemen Kejadian: SIEM menciptakan catatan atau peristiwa keamanan dan menyediakan alat untuk menyelidiki dan merespons insiden keamanan.
5. Pelaporan dan Audit: SIEM memberikan laporan keamanan yang terstruktur dan dapat diakses untuk membantu organisasi dalam pemantauan keamanan dan pemenuhan kebutuhan audit.

Dengan menggunakan SIEM, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi, mencegah, dan merespons ancaman keamanan dengan lebih efektif. Sistem ini membantu mengelola kompleksitas keamanan informasi dan memberikan visibilitas yang lebih baik terhadap aktivitas di lingkungan IT suatu organisasi. [3]

2.4 Wazuh

Wazuh adalah perangkat lunak *open source* yang berfungsi sebagai sistem deteksi berbasis host (*endpoint*) yang menyatukan kemampuan XDR *(External Data Representation)* dan SIEM *(Security Information and Event Management)* diantaranya menganalisis *log*, deteksi intrusi dan malware, monitor file integrity, penilaian konfigurasi sesuai standar industri, deteksi kerentanan, dan dukungan kepatuhan terhadap aturan. memberi peringatan berdasarkan waktu, dan merespons secara aktif. Wazuh memberikan fitur visibilitas keamanan yang lebih dalam pada infrastruktur dengan memantau *host* di sistem operasi dan tingkat aplikasi. Arsitektur Wazuh tersusun dari tiga komponen pusat *(Wazuh Indexer, Wazuh Server, Wazuh Dashboard)* dan komponen *endpoint (Wazuh Agent)* yang digambarkan dalam diagram berikut.



Gambar 2. 1 Arsitektur Wazuh

- **Wazuh *Indexer***

  Wazuh *Indexer* merupakan *search engine* untuk mengindeks dan menyimpan *alert* yang dihasilkan oleh Wazuh Server sehingga dapat memudahkan pencarian data dan kebutuhan analisis. Data disimpan dalam JSON document dimana kumpulan dari document yang memiliki korelasi disebut sebagai index. Wazuh menggunakan 4 index yang berbeda untuk masing-masing tipe *alert* sebagai berikut.

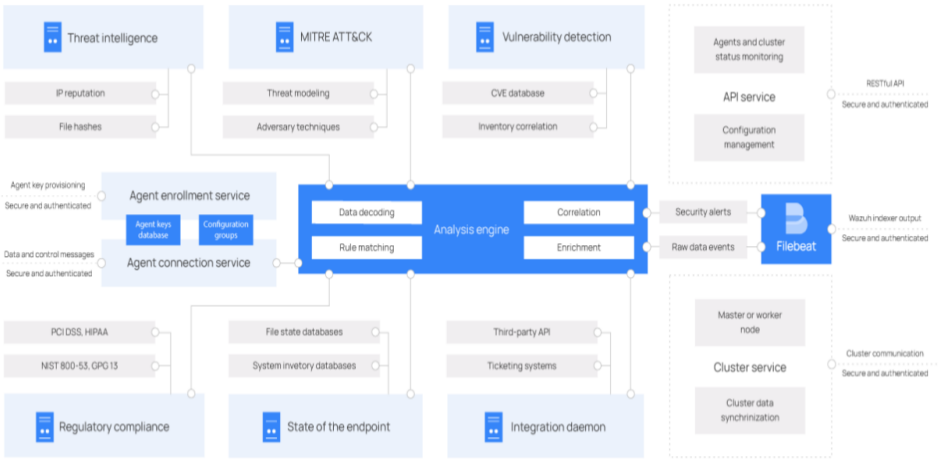
Index	Description
wazuh-alerts	Stores alerts generated by the Wazuh server. These are created each time an event trips a rule with a high enough priority (this threshold is configurable).
wazuh-archives	Stores all events (archive data) received by the Wazuh server, whether or not they trip a rule.
wazuh-monitoring	Stores data related to the Wazuh agent status over time. It is used by the web interface to represent when individual agents are or have been `Active`, `Disconnected`, or `Never connected`.
wazuh-statistics	Stores data related to the Wazuh server performance. It is used by the web interface to represent the performance statistics.

Gambar 2. 2 Komponen Wazuh Indexer

- **Wazuh Server**

  Wazuh Server menganalisis data yang diterima dari Wazuh Agent, memprosesnya melalui *decoders* dan *rules* menggunakan *threat intelligence* untuk mencari ancaman yang populer. Selain itu, Wazuh Server juga digunakan untuk mengelola Wazuh Agent, termasuk kebutuhan konfigurasi dan upgrade.

  Wazuh Server tersusun dari enam komponen dengan fungsinya masing-masing digambarkan dalam diagram berikut.



Gambar 2. 3 Komponen Wazuh Server

1. *Agent enrollment service* untuk mendaftarkan agent baru dengan menyediakan dan mendistribusikan kunci autentikasi yang unik untuk masing-masing agent.
2. *Agent connection service* untuk menerima data dari agent dengan memvalidasi identitas setiap agent dan mengenkripsi komunikasi antara Wazuh Agent dan Wazuh Server.
3. *Analysis engine* untuk analisis data menggunakan decoder untuk mengidentifikasi tipe informasi yang diproses serta mengekstrak data dari pesan log dan menggunakan rules untuk mengidentifikasi pola khusus dari hasil decoder untuk melakukan tindak lanjut.
4. Wazuh RESTful API untuk berinteraksi dengan infrastruktur Wazuh seperti mengelola konfigurasi agent dan server, monitor status infrastruktur, mengelola Wazuh decoder dan rule, dan mendapatkan status dari endpoints.
5. Wazuh *cluster daemon* menyediakan skalabilitas secara horizontal dan digunakan untuk komunikasi antar server dan menjaga sinkronisasi

6. Filebeat untuk mengirimkan event dan alert ke Wazuh Indexer dengan membaca output dari Wazuh analysis engine dan meneruskan evens secara real-time.

- **Wazuh *Dashboard***

  Wazuh *Dashboard* merupakan antarmuka web untuk visualisasi data dan kebutuhan analisis. Wazuh *Dashboard* menampilkan *security events, regulatory compliance*, kerentanan aplikasi yang terdeteksi, data hasil *monitor file integrity*, hasil penilaian konfigurasi, monitoring events pada infrastruktur cloud, dan informasi lainnya yang dapat digunakan untuk mendukung kebutuhan analisis. Selain itu, Wazuh Dashboard juga digunakan untuk mengelola konfigurasi Wazuh dan monitor statusnya.

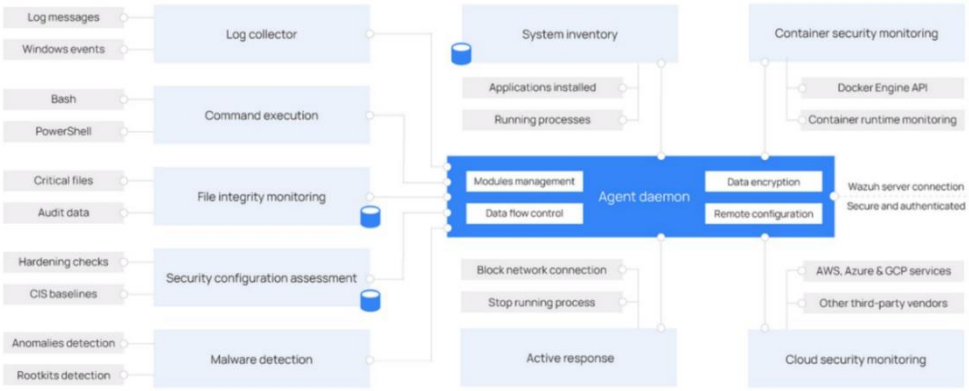
- **Wazuh *Agent***

  Wazuh Agent diimplementasikan pada perangkat endpoint (Linux, Windows, macOS, Solaris, AIX, dan OS lainnya) yang menyediakan kemampuan pencegahan, deteksi, dan respon terhadap ancaman.

  Agen Wazuh bersifat multi-platform dan berjalan pada titik akhir yang ingin dipantau pengguna. Ia berkomunikasi dengan server Wazuh, mengirimkan data hampir secara real-time melalui saluran terenkripsi dan terautentikasi.

  Agen ini dikembangkan dengan mempertimbangkan kebutuhan untuk memantau berbagai titik akhir yang berbeda tanpa memengaruhi kinerjanya. Ini didukung pada sistem operasi terpopuler, dan membutuhkan rata-rata RAM 35 MB.

Agen Wazuh menyediakan fitur fitur utama untuk meningkatkan keamanan sistem Anda. Wazuh Agent tersusun dari beberapa komponen dengan tugas diantaranya monitoring file system, membaca pesan log, mengumpulkan data inventaris, memindai konfigurasi sistem, dan mencari malware sebagaimana digambarkan dalam diagram berikut.



Gambar 2. 4 Komponen Wazuh Agent

Dengan adanya aplikasi Wazuh, aktivitas monitoring dapat dilakukan secara rutin guna mendapat informasi berupa log mengenai aktivitas yang dilakukan oleh agent. Kemudian log tersebut dapat divisualisasikan oleh Wazuh dengan beragam bentuk statistik agar mudah dipahami. Pada menu integrity monitoring menampilkan log dari aktivitas berupa membuat, memodifikasi, dan menghapus file. [4]

2.5 *Hydra*

Hydra adalah alat *cracking login* jaringan paralel yang dapat digunakan sistem operasi seperti *Kali Linux, Parrot*, dan lingkungan pengujian penetrasi utamalainnya. Hydra melakukan serangan *brute force* dengan mencoba kombinasi nama pengguna dan kata sandi yang berbeda. Hydra umumnya digunakan oleh penguji penetrasi bersama dengan alat lain seperti crunch, cupp dll, yang digunakan untuk menghasilkan daftar kata.

Kemudian, Hydra digunakan untuk menguji serangan dengan mencoba kombinasi yang ditentukan oleh daftar kata tersebut. Dalam konteks keamanan siber (cybersecurity), "Hydra" sering merujuk pada perangkat lunak yang disebut "THC-Hydra." Ini adalah alat yang digunakan oleh para profesional keamanan siber dan peneliti keamanan untuk melakukan serangan keamanan terhadap sistem yang dilindungi oleh kata sandi. Alat ini biasanya digunakan untuk menguji keamanan sistem dengan mencoba berbagai kombinasi kata sandi secara otomatis, sehingga disebut sebagai alat brute-force. Berikut adalah beberapa informasi lebih lanjut tentang THC-Hydra:

1. Tujuan: THC-Hydra digunakan untuk mencoba mengakses sistem atau akun yang dilindungi oleh kata sandi dengan mencoba banyak kombinasi kata sandi secara berurutan. Tujuannya adalah untuk menguji seberapa kuat atau lemah sistem keamanan dengan mengidentifikasi kata sandi yang lemah.

2. Serangan Brute-Force: Alat ini mengimplementasikan serangan brute-force, yang berarti mencoba semua kemungkinan kombinasi kata sandi secara berurutan hingga sandi yang benar ditemukan atau sampai daftar kata sandi yang telah ditentukan selesai

3. Protokol Dukungan: THC-Hydra mendukung berbagai protokol, termasuk protokol jaringan seperti SSH (Secure Shell), Telnet, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), dan banyak lainnya. Ini membuatnya berguna untuk menguji keamanan berbagai jenis sistem.

4. Legalitas Penggunaan: Penggunaan THC-Hydra harus dilakukan dengan izin dan hanya pada sistem yang Anda memiliki hak akses atau izin pengujian. Penggunaan alat ini untuk mencoba mengakses sistem tanpa izin adalah ilegal dan dapat mengakibatkan tindakan hukum. Penting untuk diingat bahwa penggunaan alat seperti THC-Hydra harus dilakukan dengan etika dan dalam konteks pengujian

keamanan yang sah, seperti yang dilakukan oleh profesional keamanan siber atau dalam lingkup pengujian keamanan perusahaan untuk mengidentifikasi potensi kerentanannya dalam sistem mereka sendiri. [5]

2.6 *Fail2ban*

Fail2ban adalah perangkat lunak sumber terbuka yang dapat digunakan secara gratis dan bebas, yang dibangun dan dikembangkan menggunakan bahasa pemrograman Python.Fail2ban berfungsi untuk membatasi akses dan menetapkan aturan terhadap akses pada sebuah server. Fail2ban bekerja dengan mengubah aturan konfigurasi *firewall* dengan konfigurasi yang ada pada Fail2ban sendiri. Ketika Fail2ban dijalankan, ia akan mengambil alih fungsi *firewall* yang ada di server. File2ban juga merupakan perangkat lunak keamanan yang digunakan untuk melindungi server atau sistem komputer dari serangan brute-force dan serangan otentikasi yang tidak sah. Fail2ban memonitor log keamanan sistem dan mengambil tindakan otomatis untuk memblokir alamat IP yang mencoba serangan berulang kali. Berikut adalah beberapa informasi lebih lanjut tentang Fail2ban:

1. Deteksi Serangan: Fail2ban bekerja dengan memantau log keamanan sistem untuk mencari tanda-tanda aktivitas yang mencurigakan, seperti upaya login yang gagal atau mencoba masuk ke sistem dengan kata sandi yang salah.

2. Pemblokiran Otomatis: Ketika Fail2ban mendeteksi aktivitas yang mencurigakan, seperti serangan brute-force yang berulang kali dari alamat IP tertentu, ia akan mengambil tindakan otomatis untuk memblokir alamat IP tersebut. Ini bisa dilakukan dengan menambahkan aturan firewall yang sesuai untuk menghentikan lalu lintas dari alamat IP tersebut.

3. Konfigurasi Fleksibel: Fail2ban memungkinkan konfigurasi yang fleksibel, sehingga administrator sistem dapat menentukan

aturan spesifik untuk memantau dan tindakan yang harus diambil dalam respons terhadap aktivitas mencurigakan tertentu. Ini memungkinkan penyesuaian sesuai dengan kebutuhan keamanan sistem

4. Melindungi Layanan Jaringan: Fail2ban dapat digunakan untuk melindungi berbagai layanan jaringan yang rentan terhadap serangan brute-force, seperti SSH, FTP, HTTP, SMTP, dan lainnya.

5. Notifikasi: Fail2ban juga dapat dikonfigurasi untuk mengirim pemberitahuan kepada administrator sistem ketika tindakan pemblokiran dilakukan. Fail2ban adalah alat yang berguna dalam meningkatkan keamanan sistem dengan mengurangi risiko serangan otentikasi yang tidak sah. Namun, penting untuk mengkonfigurasi dan mengelola Fail2ban dengan hati-hati untuk memastikan bahwa tidak ada blokir yang tidak diinginkan terhadap alamat IP yang sah. [6]

2.7 Jaringan Internet

Jaringan internet adalah jaringan global yang terdiri dari banyak ribu jaringan komputer yang saling terhubung secara global menggunakan berbagai teknologi komunikasi. Ini adalah infrastruktur yang memungkinkan komputer dan perangkat lainnya untuk berkomunikasi dan bertukar data di seluruh dunia. Berikut beberapa poin penting tentang jaringan internet:

1. Global dan Terdistribusi: Internet adalah jaringan yang sangat besar dan terdistribusi di seluruh dunia. Ini tidak memiliki satu otoritas pusat yang mengendalikan atau mengelola seluruhnya. Sebaliknya, berbagai penyedia layanan internet, penyedia hosting, dan organisasi lainnya berkontribusi untuk menjalankannya.

2. Protokol Komunikasi: Jaringan internet mengandalkan protokol

komunikasi yang standar, terutama Protokol Kontrol Transmisi/Internet (TCP/IP). Ini adalah set protokol yang memungkinkan perangkat di internet untuk berkomunikasi dan mentransfer data.

3. Akses Publik: Internet menyediakan akses publik yang dapat diakses oleh individu, organisasi, dan perusahaan di seluruh dunia. Ini berarti setiap orang dengan koneksi internet yang sesuai dapat mengakses berbagai layanan, seperti situs web, email, streaming video, dan banyak lagi.

4. Layanan dan Aplikasi: Internet mendukung berbagai layanan dan aplikasi, termasuk World Wide Web (WWW), email, media sosial, panggilan video, transfer file, dan banyak lagi. Ini berarti internet tidak hanya digunakan untuk mengirim dan menerima data, tetapi juga untuk berinteraksi dengan berbagai jenis konten dan layanan

5. Koneksi Beragam: Ada berbagai jenis koneksi internet, termasuk koneksi berbasis kabel (seperti kabel serat optik), koneksi nirkabel (seperti Wi-Fi dan 4G/5G), dan koneksi melalui satelit. Koneksi ini dapat disediakan oleh penyedia layanan internet lokal atau penyedia seluler

6. Keamanan dan Privasi: Keamanan dan privasi menjadi perhatian utama di internet. Untuk melindungi data pribadi dan keamanan, berbagai protokol keamanan seperti SSL/TLS digunakan untuk mengenkripsi komunikasi online, dan berbagai langkah keamanan cyber diterapkan.

Dua unit komputer dikatakan terhubung jika keduanya dapat saling bertukar data dan informasi, serta berbagi sumber daya yang dimilikinya seperti file, printer, media penyimpanan (*hardisk, floppy disk, cd-rom, flashdisk,* dll). [7]

2.8 Serangan Siber (*Cyber Attack*)

Serangan siber adalah bagian dari penggunaan kekuatan bersenjata saat serangan yang dilakukan oleh negara atau subjek hukum internasional lain yang menyebabkan kerusakan padasistem komputer negara yang diserang. Namun hanya dapat dikatakan sebagai perang jika terbukti adanya kerusakan fisik dan kerugian atau korban jiwa. [8] Serangan siber adalah upaya yang dilakukan oleh individu atau kelompok untuk merusak, mengakses, atau mencuri informasi dari sistem komputer atau jaringan melalui internet atau media digital lainnya. Ada berbagai jenis serangan siber yang dapat dilakukan oleh para penyerang, dan seringkali mereka memiliki motif dan tujuan yang berbeda. Berikut adalah beberapa model serangan siber yang umum:

- Malware (Malicious Software): Virus: Menyebar melalui perangkat dan merusak atau menggandakan file.
- Worm: Menyebarkan diri tanpa bantuan manusia dan dapat merusak jaringan atau perangkat.
- Trojan Horse: Mengelabui pengguna dengan menyamar sebagai program yang sah tetapi sebenarnya berisi kode berbahaya.
- Ransomware: Mengenkripsi data dan meminta tebusan untuk mendapatkan kunci dekripsi.

1. Serangan Phishing:
    - Phishing Email: Penyerang mengirim email palsu yang mencoba memancing korban untuk memberikan informasi pribadi atau masuk ke situs web palsu.
    - Spear Phishing: Serangan phishing yang ditargetkan pada individu atau perusahaan tertentu.
    - Whaling: Phishing yang menargetkan pejabat eksekutif atau orang dengan akses tinggi

- Serangan DDoS (Distributed Denial of Service): Menyerang situs web atau server dengan lalu lintas data berlebih untuk membuatnya tidak tersedia bagi pengguna

2. Serangan Man-in-the-Middle (MitM):
    - Penyerang mencoba memasukkan dirinya di antara komunikasi yang berlangsung antara dua pihak untuk mengakses atau memanipulasi data.
3. Serangan Brute Force:
    - Penyerang mencoba semua kombinasi yang mungkin dari kata sandi atau kunci enkripsi hingga mereka berhasil memecahkan kemanan.
4. Serangan Zero-Day:
    - Penyerang menggunakan kerentanan yang belum diketahui
    - di perangkat lunak atau sistem yang diserang.
5. Serangan Social Engineering:
    - Penyerang memanipulasi atau mempengaruhi orang agar memberikan informasi rahasia atau akses ke system
6. Serangan APT (Advanced Persistent Threat):
    - Serangan yang dilakukan oleh penyerang yang sangat terlatih dan bertarget tinggi dengan tujuan mencuri data atau merusak sistem dalam jangka waktu yang lama.
7. Serangan IoT (Internet of Things):
    - Penyerang menyerang perangkat yang terhubung ke internet, seperti kamera keamanan atau perangkat rumah pintar.
8. Serangan Ransomware:
    - Mengenkripsi data atau sistem, kemudian meminta tebusan untuk mengembalikan akses atau data.
9. Serangan Insider Threat:
    - Ancaman dari dalam organisasi, baik disengaja atau tidak, seperti pegawai yang mencuri data atau memberikan akses yang tidak sah.

Penting untuk memiliki lapisan perlindungan yang kuat dan kebijakan keamanan yang ketat untuk melindungi diri dari berbagai jenis serangan siber ini. Selain itu, pemahaman yang baik tentang keamanan siber dan tindakan pencegahan adalah kunci untuk mengurangi risiko serangan siber. [9]

2.9 *Cyber Security*

Dalam beberapa tahun terakhir, para peneliti mulai memasukkan faktor manusia seperti kejahatan dan keahlian dalam model risiko keamanan siber untuk memberikan wawasan tambahan mengenai perilaku manusia yang mendorong atau memitigasi pelanggaran keamanan siber Seiring dengan arus globalisasi dan juga kemajuan dari teknologi memberikan dampak kepada konsep keamanan, pandangan tradisional menyatakan bahwa ancaman kemanan selalu berbentuk fisik namun adanya pergeseran tentang persepsi ancaman pasca perang dingin memungkinkan ancaman kemanan dapat dilakukan secara non fisik, salah satu contohnya melalui dunia maya (cyber). [10] Adanya pergeseran tentang persepsi ancaman kearah non tradisional melalui dunia maya harus mendapatkan perhatian yang serius, negara harus membuat cyber security-nya sebagai upaya dalam mengamankan kemanan nasional. Ancaman serangan cyber tidak saja terjadi pada institusi-institusi publik, melainkan dalam beberapa kasus menyerang institusi pemerintahan. Kemanan cyber mencakup segala sesuatu yang berhubungan dengan pengawasan komputer, monitoring sampai kontrol yang sangat ketat atau perjuangan untuk hak asasi fundamental. Cyber security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap resiko keamanan yang relevan dalam lingkup cyber space. [11]

2.10 *Brute Force*

Bruteforce adalah suatu metode atau teknik yang digunakan dalam keamanan siber untuk mencoba semua kemungkinan kombinasi yang

mungkin dari kata sandi atau kunci enkripsi sampai kombinasi yang benar ditemukan. Ini adalah pendekatan yang sangat kasar dan sering kali memerlukan waktu yang lama, terutama jika kata sandi yang harus dipecahkan sangat panjang atau kompleks. [1] Menurut sebuah penelitian keamanan seperti WPS sangat berpotensi untuk ditembus dengan serangan bruteforce. Bruteforce merupakan salah satu serangan yang banyak digunakan pada jaringan yang menggunakan sistem keamanan password seperti WPA, WPE2K dan WPS. Beberapa poin penting tentang bruteforce:
1. Tujuan Utama: Tujuan dari serangan brute-force adalah untuk mendapatkan akses ke suatu sistem, akun, atau data yang dilindungi dengan menebak kata sandi atau kunci enkripsi yang benar. Ini sering digunakan oleh penyerang untuk mencoba mengakses akun orang lain tanpa izin

2. Cara Kerja: Dalam serangan brute-force, penyerang akan mencoba semua kemungkinan kombinasi kata sandi atau kunci, dimulai dari yang paling sederhana (seperti "123456" atau "password") hingga yang paling rumit. Ini berarti bahwa semua kemungkinan harus diuji, yang bisa memakan waktu lama.

3. Kecepatan dan Keberhasilan: Kecepatan serangan brute-force tergantung pada seberapa cepat penyerang dapat mencoba setiap kombinasi. Semakin panjang dan kompleks kata sandi, semakin lama waktu yang diperlukan. Kunci enkripsi yang lebih kuat juga akan memerlukan waktu lebih lama untuk ditemukan.

4. Pencegahan: Untuk mencegah serangan brute-force, praktik keamanan siber yang umum melibatkan penggunaan kata sandi yang kuat (panjang, kompleks, dan unik), pembatasan percobaan login yang gagal, dan penggunaan metode keamanan tambahan seperti autentikasi dua faktor.

5. Legalitas: Penting untuk diingat bahwa serangan brute-force pada sistem, akun, atau data yang bukan milik Anda tanpa izin adalah ilegal dan melanggar hukum keamanan siber

Serangan brute-force adalah salah satu metode serangan yang paling sederhana dan dapat dilakukan oleh penyerang yang memiliki cukup waktu dan sumber daya. Oleh karena itu, penting bagi individu dan organisasi untuk melindungi sistem mereka dengan menggunakan kata sandi yang kuat dan menerapkan langkah-langkah keamanan tambahan untuk mencegah serangan ini. [12]

2.11 *Set Top Box* (STB)

STB (*Set-Top Box*) adalah perangkat keras berukuran kecil yang umumnya digunakan untuk menghubungkan televisi dengan jaringan atau internet. STB memiliki komponen seperti prosesor, RAM, *port hardware*, dan sistem operasi yang memungkinkan pengguna untuk mengakses berbagai layanan dan konten melalui televisi mereka. STB sering digunakan untuk *streaming* video, televisi digital, video *on demand* aplikasi internet, dan fungsi multimedia lainnya. Salah satu sistem operasi yang umum digunakan pada STB adalah Armbian, yang dirancang untuk berjalan pada perangkat dengan arsitektur ARM dan sering digunakan pada banyak komputer papan tunggal (*single-board computer*). Armbian memberikan fleksibilitas dan kemampuan adaptasi pada perangkat STB dengan berbagai fitur dan aplikasi yang dapat dijalankan melalui antarmuka pengguna yang mudah digunakan. [13]

2.12 Sistem Operasi

Sistem operasi adalah suatu jenis perangkat lunak yang berperan penting dalam pengoperasian sistem komputer. Fungsinya adalah membantu perangkat keras dalam menjalankan berbagai fungsi-fungsinya, termasuk manajemenproses atau kontrol proses. Dengan sistem operasi, perangkat keras dapat diatur dan dikendalikan dengan efisien, memungkinkan penggunaan yang optimal dari sumber daya komputer. Sistem operasi mengelola proses-proses yang berjalandi dalam komputer, mengatur

alokasi memori, mengatur akses ke perangkat keras, serta memfasilitasi komunikasi antara komponen-komponen perangkat keras yang berbeda. Dengan demikian, sistem operasi menjadi fondasi yang penting dalam menjalankan aplikasi dan tugas komputasi dengan lancar dan efektif. [14]

2.13 Ubuntu

Ubuntu adalah sebuah distro Linux yang merupakan pengembangan dari Debian. Ubuntu menyediakan sistem operasi berbasis Debian dengan frekuensi rilis yang teratur, dukungan yang tersedia untuk pengguna perusahaan, dantampilan desktop yang dirancang dengan baik.

Ubuntu melakukan penyebaran dengan pendekatan yang mirip dengan selalu merilis versi terbaru dengan aplikasi-aplikasi *open source* terkini. Dengan pendekatan ini, pengguna Ubuntu dapat menikmati fitur-fitur terbaru dan pembaruan perangkat lunak secara reguler. Ubuntu juga terkenal dengan komunitas yang aktif dan dukungan yang luas, membuatnya menjadi salah satu distro Linux yang populer di kalangan pengguna desktop dan pengguna perusahaan. [15]

2.14 Kali Linux

Kali Linux adalah sebuah distribusi Linux yang didasarkan pada distribusi Debian GNU/Linux dan dikhususkan untuk keperluan forensik digital dan pengujian penetrasi.Distribusi ini dipelihara dan didanai oleh *Offensive Security*, serta merupakan penerus dari *BackTrack* Linux. Kali Linux menyediakan akses yang mudah bagi pengguna ke koleksi alat yang luas dan komprehensif yang berkaitan dengan keamanan. Di antara alat-alat tersebut termasuk *port scanner*, yang digunakan untuk memindai dan mengidentifikasi *port-port* yang terbuka pada sistem target, serta password cracker, yang digunakan untuk memecahkan atau menguji keamanan kata sandi. Dengan fitur-fitur tersebut, Kali Linux menjadi pilihan yang populer

di kalangan profesional keamanan komputer dan peneliti keamanan untuk kegiatan forensik dan pengujianpenetrasi. [16]

2.15 *Denial of Service* (DoS)

Denial of Service (DoS) adalah serangan terhadap suatu sistem atau layanan dengan cara membanjiri sumber daya yang tersedia sehingga sistem atau layanan tersebut tidak dapat memenuhi permintaan yang sah.

Umumnya serangan DoS dan DDoS telah menjadi ancaman besar pada jaringan komputer. Dalam serangan seperti itu, karena menguras sumber daya, beberapa layanan dinonaktifkan, dan kinerja jaringan diturunkan. Serangan ini dianggap berhasil ketika penyerang dengan sengaja menggunakan sumber daya yang mencegah host menggunakan layanan yang ditargetkan.[17] Pendekatan yang berbeda dapat digunakan untuk melakukan serangan DoS/DDoS, termasuk pendekatan berbasis jaringan, seperti membanjiri paket TCP SYN, ICMP, atau UDP, dan pendekatan berbasis host, di mana satu atau beberapa host menargetkan target tertentu. aplikasi untuk mengeksploitasi struktur memorinya, protokol otentikasinya, atau algoritma tertentu. Serangan DoS/DDoS dapat membanjiri bidang kendali, bidang data, atau bandwidth bidang kendali, sementara menyerang bidang kendali SDN dapat mengakibatkan kegagalan seluruh jaringan. Memang benar, pengontrol dianggap sebagai otak dari jaringan, yang mengelola sejumlah besar sakelar/aplikasi. DoS dapat dilakukan menggunakan berbagai metode, termasuk pengiriman lalu lintas yang sangat tinggi, eksploitasi kelemahan dalam perangkat lunak, atau manipulasi protokol jaringan. Untuk melindungi diri dari serangan DoS, organisasi dan penyedia layanan sering kali mengimplementasikan solusi keamanan yang dapat mendeteksi dan merespons terhadap serangan tersebut. [18]

2.16 *Slowloris*

Slowloris adalah jenis serangan *Denial-of-Service* (DoS) yang ditujukan untuk menyebabkan layanan web menjadi tidak responsif atau tidak dapat diakses untuk pengguna yang sah. Serangan ini pertama kali dijelaskan oleh RSnake *(Robert Hansen)* pada tahun 2009. Nama *"Slowloris"* diambil dari kata *"slow"* dan *"loris,"* yang merupakan nama seekor primata dengan gerakan lambat. Cara kerja *Slowloris* melibatkan pengiriman permintaan HTTP yang tidak lengkap atau tidak selesai secara bertahap ke server target. Daripada mengirimkan permintaan HTTP lengkap sekaligus, serangan ini memanfaatkan fakta bahwa banyak server web tidak akan menutup koneksi sampai permintaan HTTP lengkap diterima. *Slowloris* menjaga koneksi tetap terbuka dengan terus-menerus mengirim bagian-bagian kecil dari permintaan, membuat server sibuk menunggu permintaan tersebut selesai. Efek dari serangan *Slowloris* adalah menghabiskan sumber daya server seperti koneksi, dan akhirnya membuat server tidak mampu melayani permintaan dari pengguna yang sah. Serangan ini bersifat lambat dan sulit terdeteksi karena setiap koneksi terlihat seperti koneksi yang sah. Untuk melindungi diri dari serangan *Slowloris*, administrator sistem dapat mengimplementasikan langkah-langkah keamanan seperti membatasi jumlah koneksi dari satu IP, menggunakan firewall, atau mengoptimalkan konfigurasi server untuk menanggapi serangan semacam ini dengan lebih efisien.[32]

2.17 Telegram

Telegram merupakan aplikasi pesan instan yang bersifat *open source* dengan memanfaatkan sistem cloud sebagai media penyimpanan utama yang digunakan untuk menyampaikan informasi jarak jauh dengan cepat, akurat dan terdokumentasi.

Layanan pesan yang sangat populer, dengan opsi untuk berbicara dengan orang-orang dalam grup atau pribadi di cloud.

1. Fitur aplikasi Telegram

- Obrolan rahasia merupakan fitur rahasia obrolan yang dihadirkan Telegram untuk memastikan privasi dan keamanan komunikasi antar pengguna lebih terjamin.
- Grup Telegram sama seperti aplikasi pesan instan lainnya, Telegram juga memungkinkan pengguna untuk memuat grup. Grup di Telegram dapat menampung hingga 200 ribu anggota.
- Saluran Telegram digunakan untuk penyebaran informasi satu arah (broadcast) berupa tulisan, foto, video, dokumen, serta jenis file lainnya secara cepat dan instan. Fungsinya seperti grup, namun hanya pembuat Channel yang dapat mengirim pesan.
- BOT Telegram adalah akun Telegram yang dioperasikan oleh sebuah program otomatis. Contohnya ketika pengguna berkirim pesan ke Bot dengan perintah yang ditemui Bot maka Bot akan menjawab pesan tersebut secara langsung.

2. Kelebihan aplikasi Telegram

    - Memiliki tingkat keamanan terbaik
    - Penyimpanan file berbasis cloud
    - Batas pengiriman file relatif besar
    - Kapasitas grup lebih besar
    - Bisa multi profil

3. Fungsi utama aplikasi Telegram

    - Sebagai aplikasi pesan instan
    - Media membangun komunitas atau fans
    - Media berbagi file video, musik, dll
    - Media transaksi digital dengan BOT

2.18 VMware Vsphere

VMware vSphere adalah sebuah platform virtualisasi yang dikembangkan oleh perusahaan teknologi VMware. Platform ini memungkinkan organisasi untuk mengelola dan menyatukan sumber daya komputasi, penyimpanan, dan jaringan secara virtual. Dengan menggunakan vSphere, perusahaan dapat menciptakan lingkungan data center virtual yang efisien dan dapat dielastisitas. Beberapa fitur kunci dari VMware vSphere meliputi:

1. Hypervisor: vSphere Hypervisor (sebelumnya dikenal sebagai ESXi) adalah hypervisor bare-metal yang memungkinkan virtualisasi langsung pada perangkat keras tanpa memerlukan sistem operasi host. Ini memberikan kinerja yang tinggi dan keamanan karena mengurangi lapisan software tambahan.

2. Virtual Machine (VM): vSphere memungkinkan pembuatan dan manajemen mesin virtual. VM adalah lingkungan virtual yang dapat berjalan secara independen di atas server fisik dan dapat diinstal dengan sistem operasi yang berbeda.

3. vCenter Server: Ini adalah pusat pengelolaan untuk lingkungan vSphere. Dengan vCenter Server, administrator dapat mengelola beberapa server vSphere dan klaster sebagai satu kesatuan. Ini menyediakan fitur-fitur seperti migrasi VM live, penjadwalan sumber daya, dan manajemen keamanan.

4. VMotion: Fitur ini memungkinkan pemindahan VM secara live dari satu host ke host lainnya tanpa memerlukan waktu henti. Ini membantu dalam pemeliharaan, peningkatan kinerja, dan manajemen beban kerja.

5. Storage vMotion: Mirip dengan VMotion, Storage vMotion memungkinkan pemindahan data penyimpanan virtual mesin virtual dari satu penyimpanan ke penyimpanan lainnya tanpa downtime.

6. vSphere Distributed Switch (VDS): VDS adalah switch jaringan virtual yang menyediakan manajemen jaringan terpusat untuk klaster host vSphere.

7. High Availability (HA) dan Fault Tolerance (FT): HA memberikan kemampuan untuk menghidupkan kembali otomatis VM pada host yang berbeda jika terjadi kegagalan hardware. FT, di sisi lain, menyediakan replika instan dari VM yang berjalan di host cadangan untuk mencapai toleransi kesalahan tanpa waktu henti.

   VMware vSphere digunakan oleh banyak organisasi untuk mengoptimalkan penggunaan sumber daya, meningkatkan ketersediaan aplikasi, dan menyederhanakan manajemen infrastruktur virtual. Platform ini cocok untuk lingkungan data center yang besar dan kompleks.

2.19 PPDIOO *(Prepare, Plan, Design, Implement, Operate, Optimize)*

PPDIOO Cisco merupakan metodologi dari Cisco yang mendefinisikan siklus layanan berkelanjutan yang dibutuhkan oleh jaringan komputer yang dirancang untuk mendukung pengembangan jaringan. Metode PPDIOO dapat menghasilkan sistem yang mapan dan menyelesaikan permasalahan yang ada.

PPDIOO Cisco merupakan singkatan enam tahap yaitu *prepare*, *plan*, *design*, *implement*, *operate*, *optimize* yaitu suatu pendekatan yang digunakan dalam siklus hidup dan manajemen jaringan. Ketika diterapkan pada sistem keamanan jaringan dengan menggunakan server Wazuh, berikut adalah beberapa phase yang akan digunakan:

2.19.1 *Prepare* (Persiapan)

Memahami kebutuhan keamanan yang spesifik dan menilai kemampuan organisasi untuk mengelola risiko keamanan. Ini

membantu dalam menentukan sumber daya dan anggaran yang diperlukan untuk implementasi keamanan.

2.19.2 *Plan* (Perencanaan)

Mengidentifikasi dan merencanakan solusi keamanan jaringan dengan menggunakan Wazuh sesuai dengan kebutuhan organisasi. Ini mencakup perencanaan untuk pelaksanaan, integrasi, dan pengelolaan keamanan.

2.19.3 *Design* (Desain)

Membangun desain sistem keamanan yang efektif dan efisien dengan mempertimbangkan kebutuhan organisasi. Ini mencakup konfigurasi server Wazuh, integrasi dengan infrastruktur yang ada, dan pemilihan strategi keamanan yang sesuai.

2.19.4 *Implement* (Implementasi)

Mengimplementasikan server Wazuh sesuai dengan desain yang telah dibuat. Ini melibatkan konfigurasi, instalasi, dan pengaturan yang sesuai agar Wazuh dapat efektif mendeteksi dan merespons terhadap ancaman keamanan.

2.19.5 *Operate* (Operasi)

Menjamin operasionalitas yang berkelanjutan dari sistem keamanan. Melibatkan pemantauan, pemeliharaan, dan manajemen *day-to-day* server Wazuh untuk memastikan bahwa keamanan jaringan tetap efektif dan responsif terhadap ancaman

2.19.6 *Optimize* (Optimasi)

Melakukan evaluasi reguler terhadap kinerja dan efektivitas sistem keamanan. Ini mencakup penyesuaian konfigurasi, peningkatan keamanan, dan penyesuaian strategi berdasarkan evaluasi dan perubahan lingkungan keamanan.

Dengan menerapkan metode PPDIOO, organisasi dapat memastikan bahwa sistem keamanan jaringan mereka dengan server Wazuh tidak hanya diimplementasikan dengan baik tetapi juga dikelola dan dioptimalkan secara berkelanjutan untuk menghadapi ancaman keamanan yang berkembang. [19]

2.20 Literature Review / Penelitian Terkait

2.20.1 Analysis Of Brute Force Attack Logs Toward Nginx Web Server On Dashboard Improved Log Logging System Using Forensic Investigation Method (Aji, R. P., Prayudi, Y., & Luthfi, A. 2023)

Pada penelitian yang berjudul Analisis *Log* Serangan *Bruteforce*Terhadap Web Server*Nginx* Pada Dashbord Sistem Pencatatan *Log* Terimprovisasi Menggunakan Metode Investigasi Forensik sudah sangat baik dan detail dalam mendeteksi serangan siber yaitu *brute force* namun belum ada respon yang diambil ketika terjadi serangan, Pada tugas akhir ini bermaksud untuk memberikan respon terhadap serangan yang terjadi pada server jaringan Lab Komputer PSDKU (*wazuh agent*). Adapun kelebihannya yaitu : Log serangan sudah di analisis dengan sangat baik dan detail, dapat menemukan lokasi penyerang dari metadata log yang diperoleh, dan identifikasi serangan yang sangat baik dari wazuh.

Adapun kekurangannya yaitu : Identifikasi lokasi penyerang belum benar benar akurat, hanya berfokus hanya pada 2 server web, tidak ada respon terhadap serangan yang terjadi. [2

2.20.2 Wazuh sebagai *Log Event Management* dan Deteksi Celah Keamanan pada Server dari Serangan DoS (Muhammad Dehan Pratama, Fitri Nova, Deddy Prayama 2022)

Pada penelitian yang berjudul Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada server dari Serangan DoS dan sudah memanfaatkan wazuh dengan sangat baik namun, dari beberapa uji coba serangan yang dilakukan tidak memberikan respon pencegahan, sehingga

pada tugas akhir ini akan menambahkan respon terhadap serang yang terdeteksi oleh wazuh. Adapun kelebihannya yaitu : Data berupa log yang ditampilkan sudah menggunakan grafik sehingga lebih mudah dianalisis, wazuh dapat melihat aktivitas semua agent, dapat mengetahui berapa banyak serangan yang masuk, sudah terintegrasi ke website virus total sehingga jika ada file yang mengandung malware maka akan otomatis memberi peringatan, sudah terintegrasi ke email sehingga bisa memberikan informasi kepada administrator jaringan secara real time Adapun kekurangannya yaitu : Tidak ada respon terhadap serangn yang terjadi, terdapat serangan yang tidak terdeteksi oleh wazuh. [4]

2.20.3 Pengukuran Kinerja Set Top Box (STB) Sebagai Penyimpanan Cloud. *Diffusion: Journal of Systems and Information Technology* (Patuke, R., Mulyanto, A., & Takdir, R. 2022)

Penelitian ini bertujuan untuk mengetahui kinerja Set Top Box (STB) digunakan sebagai penyimpanan cloud dan untuk mengetahui proses penggunaan STB sebagai penyimpanan cloud dengan menggunakan dua server yaitu apache dan nginx. Penulis mencari dan mengolah sendiri data-data yang berhubungan dengan objek yang diteliti yaitu pengukuran STB digunakan sebagai penyimpanan cloud, pada penelitian ini juga akan dilakukan beberapa proses pengujian terhadap beberapa aktivitas diantaranya upload, download dan response time. Proses upload, download dan response time dilakukan terhadap beberapa jenis dan ukuran file yang berbeda yakni file Mp4 (100 Mb), file BIN (500 Mb), file ISO (1 Gb) dan file RAR (2 Gb). Selain itu, penelitian ini terdapat perbandingan dari segi penggunaan CPU, RAM dan response time terhadap file mp4, BIN, ISO dan RAR dari kedua server yang digunakan yaitu apache2 dan nginx. hasil penelitian ini memungkinkan penulis untuk mengetahui kinerja STB sebagai media penyimpanan cloud serta penulis dapat mengetahui proses penggunaan STB sebagai penyimpanan cloud. Hasil penelitian yang diperoleh penulis cukup baik karena penulis berhubungan langsung dengan objek penelitian. Penelitian ini diharapakan dapat diterapkan dikalangan

masyarakat banyak sehingga memberikan manfaat bagi orang lain maupun penulis itu sendiri. [13]

2.20.4 Serangan DoS dan DDoS di Software Defined Networks: Sebuah survei terhadap solusi yang ada dan tantangan penelitian. (Lubna Fayez Eliyan , Roberto Di Pietro 2021)

Software Defined Networking (SDN) adalah paradigma jaringan baru di mana penerusan perangkat keras dipisahkan dari keputusan kontrol. Hal ini menjanjikan penyederhanaan manajemen jaringan secara dramatis dan memungkinkan inovasi dan evolusi. Di SDN, kecerdasan jaringan secara logis dipusatkan pada pengontrol berbasis perangkat lunak (bidang kendali), sedangkan perangkat jaringan *(OpenFlow Switches)* menjadi perangkat penerus paket sederhana (bidang data) yang dapat diprogram melalui antarmuka terbuka (protokol *OpenFlow*). Pemisahan bidang kontrol dari bidang data menimbulkan berbagai tantangan yang mencakup keamanan, keandalan, penyeimbangan beban, dan rekayasa lalu lintas. Tantangan keamanan yang mengerikan di SDN adalah serangan penolakan layanan (DoS) dan penolakan layanan terdistribusi (DDoS). Misalnya, di SDN, serangan DoS/DDoS dapat membanjiri bidang kontrol, bidang data, atau saluran komunikasi. Menyerang bidang kendali dapat mengakibatkan kegagalan seluruh jaringan, sementara menyerang bidang data atau saluran komunikasi mengakibatkan hilangnya paket dan tidak tersedianya jaringan. Dalam makalah ini kami menyampaikan beberapa kontribusi yang menjelaskan bidang serangan DoS/DDoS di SDN, memberikan latar belakang lengkap tentang bidang tersebut, termasuk serangan dan analisis solusi yang ada. Secara khusus, kontribusi kami dapat diringkas sebagai berikut: kami meninjau dan mensistematisasikan solusi canggih yang mengatasi serangan DoS dan DDoS di SDN melalui lensa pendekatan intrinsik dan ekstrinsik. Selain itu, tindakan penanggulangan yang dibahas disusun sesuai dengan fokusnya, baik pada deteksi, mitigasi, pencegahan, atau degradasi secara perlahan. Selanjutnya, kami mensurvei berbagai pendekatan dan alat yang digunakan untuk menerapkan solusi yang telah

direvisi. [18]

2.20.5 Optimization problem of computer network using ppdioo. *ICIC Express Lett.* (Purwanto, A, & Soewito, B 2021).

Kualitas pelayanan dalam suatu perusahaan dan institusi merupakan hal yang harus diperhatikan untuk mempertahankan bisnis inti. Untuk mendukung hal tersebut digunakan teknologi informasi dan komunikasi. Hal ini menjadikan jaringan komputer sebagai salah satu indikator keberhasilan dalam menunjang kualitas pelayanan sehingga jaringan komputer yang ada harus selalu dijaga dan dioptimalkan. Dengan topologi jaringan yang terukur, kinerja yang terukur, dan perangkat monitoring jaringan diharapkan dapat membantu menjaga kualitas layanan Untuk mengoptimalkan jaringan komputer digunakan metode PPDIOO dari Cisco sebagai frameworknya. Tahapan kerangka ini adalah Prepare, Plan, Design, Implement, Operate dan Optimize. Pekerjaan ini dimulai dari kebutuhan perusahaan/instansi dalam menggunakan jaringan komputer, mempertimbangkan jaringan yang ada, hingga menghasilkan system. jaringan yang optimal. [19]

2.20.6 Implementasi *Security Information And Event Management* (Siem) Pada Aplikasi Sms *Center* Pemerintah Daerah Provinsi Nusa Tenggara Barat (Husnul Khotimah, Fitri Bimantoro, Robert Silas Kabanga, Ida Bagus Ketut Widiartha 2022)

Pada penelitian yang berjudul Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat belum menyajikan data log dari wazuh maka dari itu pada tugas akhir penelis akan memaparkan log dari wazuh agent yang terinstal di server jaringan lab komputer. Adapun kelebihannya yaitu: Penambahan fitur sistem keamanan komputer menjadi langkah yang sangat baik, pemilihan platform wazuh sebagai alat system keamanan komputer sanga tepat karena wazuh memliki banyak fitur keamanan, dan hemat biaya karena wazuh merupakan aplikasi open cource alias gratis.

Adapun kekurangannya yaitu: Tidak ada *log* wazuh *agent* yang ditampilkan, tidak ada uji coba serangan terhadap sistem keamanan jaringan yang dibuat, hanya sekedar melakukan instalasi wazuh aplikasi sms *center*.[20]

2.20.7 Intrusion Detection And Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang. (Arif Gilang Surya Harahap,Hutrianto 2021)

Pada penelitian yang berjudul Intrusion Detection And Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang (2021) sudah banyak uji coba serangan yang dilakukan dan sudah sebagian besar dapat terdeteksi oleh wazuh, berdasarkan penelitian ini penulis juga bermaksud untuk melakukan uji coba serangan ke komputer server jaringan Lab komputer yang sudah terinstall wazuh *agent* yang berfokus pada serangan *brute force* dan *Denial of Service.* Pada penelitian yang berjudul Deteksi Dini Serangan Pada Website Menggunakan Metode Anomali Based (2022), antisipasi serangan sudah dilakukan secara otomatis sehingga dapat melindungi website secara real- time, hal tersebut juga yang akan dilakukan penulis dalam merespon serangan siber pada server jaringan PSDKU Universitas Lampung Way Kanan yang diharapkan dapat melindungi server secara real time. Adapun kelebihannya yaitu: Wazuh dapat mendeteksi dengan cepat ketika penyerang melakukan port scanning pada wazuh agent, pendeteksian yang cepat dan akurat terhadap serangan brute force, serangan metasploit juga dapat terdeteksi oleh wazuh. Adapun kekurangannya yaitu: Wazuh tidak dapat mendeteksi serangan *DENIAL OF SERVICE* (DOS) dengan skala yang kecil, Wazuh dapat mendeteksi serangan *DENIAL OF SERVICE* (DOS) jika sudah terdapat kerusakan pada sistem seperti terputusnya koneksi antara wazuh agent dan wazuh server hal ini merupakan kekurangan yang harus dicari solusinya. [21]

2.20.8 *A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis*., etran.rs (Stanković, S, Gajin, S, & Petrović, R 2022)

Tulisan ini menyajikan prinsip dasar pengoperasian alat Wazuh berdasarkan sistem agen-manajer. Agen yang diinstal pada host mengirimkan data log untuk diproses ke manajer. Berbagai jenis serangan disajikan dan perhatian khusus diberikan pada detail mengenai beberapa serangan terkenal seperti brute force SSH. Serangan itu berhasil dideteksi dan ditunjukkan dengan segera. Sebagai pekerjaan lebih lanjut, diusulkan pemasangan agen pada semua perangkat infrastruktur, tanpa membatasi jenis perangkat. Sebaiknya alat Wazuh diintegrasikan dengan perangkat lunak antivirus untuk mendapatkan pemeriksaan mendalam terhadap virus, worm, trojan, dan konten berbahaya lainnya. Beberapa masalah keamanan paling berhasil dideteksi dengan memeriksa lalu lintas jaringan server yang sebenarnya, yang biasanya tidak dicatat dalam log. Di sinilah Sistem Deteksi Intrusi Jaringan bisa memberikan wawasan tambahan tentang keamanan. Salah satu sistem tersebut adalah Suricata. Karena Suricata mampu menghasilkan log peristiwa JSON *(JavaScript Object Notation),* ia memiliki opsi integrasi yang sangat baik dengan Wazuh. [24]

2.20.9 Sistem Pencegahan Serangan Bruteforce Pada Ubuntu Server Dengan Menggunakan Fail2ban (Iwan Kurniawan , Ferry Mulyanto, Fuad Nandiasa 2016)

Perkembangan internet yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan webserver. Terutama dengan semakin terbukanya pengetahuan hacking dan cracking, didukung dengan banyaknya tools yang tersedia dengan mudah, semakin mempermudah para attacker untuk melakukan aksi penyusupan ataupun serangan. Masalah timbul ketika administrator sedang tidak berada pada posisi siap sedia, sedangkan serangan terhadap server bisa terjadi kapan saja. Salah satu serangan yang berakibat fatal adalah, serangan bruteforce. Serangan bruteforce pada server memang jarang sekali

terjadi, tetapi akibat yang ditimbulkan dari serangan ini adalah penyerang bisa mendapatkan hak akses administrator dan tentu saja membahayakan server. Administrator membutuhkan suatu sistem yang dapat membantu kerjanya. Sebuah sistem yang dapat memberikan hasil laporan apa yang terjadi pada sistem apakah itu sebuah serangan atau penyusupan. Dengan hasil laporan yang di dapat, administrator akan bertindak lebih jauh untuk mencegah terjadinya serangan di masa yang akan datang. Kesimpulan dari penelitian ini yaitu Implementasi fail2ban pada Ubuntu server terbukti dapat mencegah serangan bruteforce dan memblokir alamat ip dari penyerang tersebut kedalam daftar blacklist serta Fail2ban tidak dapat memberikan report kepada administrator melalui web blocklist.de dan email administrator. [25]

2.20.10 A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis (Stefan Stanković, Slavko Gajin, and Ranko Petrović, Member, IEEE 2022)

Tujuan dari makalah ini adalah untuk menyajikan fungsionalitas alat Wazuh dalam mendeteksi serangan yang ditunjukkan pada server web Server web adalah komponen yang sangat rentan terhadap Internet dan jika tidak terlindungi dengan baik, maka sangat rentan terhadap berbagai jenis serangan. Untuk mencegah serangan, mereka harus dideteksi terlebih dahulu dan itulah sebabnya Host Sistem Deteksi Intrusi digunakan. Salah satu solusi yang dapat membantu adalah Wazuh. Ini adalah alat canggih yang menampilkan semua serangan yang terdeteksi dengan sangat detail dan real-time. Meskipun makalah ini menunjukkan analisis serangan yang terdeteksi pada server web, Wazuh adalah alat yang digunakan untuk menganalisis serangan di seluruh infrastruktur. Tulisan ini menyajikan prinsip dasar pengoperasian alat Wazuh berdasarkan sistem agen-manajer. Agen yang diinstal pada host mengirimkan data log untuk diproses ke manajer. [26]

2.20.11 The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods (Suryantoro, T, Purnomosidi, BDP, & *2022 5th International* …IEEE (2022).

SIEM membantu perusahaan dan petugas keamanan untuk memantau serangan, menemukan kerentanan dan menganalisis serangan. Penelitian ini menerapkan pendekatan forensik jaringan dengan OSCAR dan metode deteksi untuk mengetahui efektivitas kinerja wazuh SIEM terhadap serangan port 80 pada web server. Tahapan pengujian serangan port scanning dan scanning direktori http, service web server masih terlihat normal atau tidak ditemukan pesan error 404 pada browser. Deviasi deteksi serangan pada penelitian ini adalah 1,402 detik. Keberadaan SIEM Wazuh mampu membantu petugas keamanan dalam memantau keamanan data perusahaan dan mengamankan aset IT perusahaan. [27]

2.20.12 *Implementasi File Integrity Monitoring System Menggunakan Wazuh Open Security Platform* (Nisa, AK 2023)

Sistem audit dan monitor pada server merupakan hal yang penting pada suatu kemanan jaringan. Server biasanya digunakan untuk beban kerja yang cukup berat dan volume lalu lintas jaringan yang besar, sehingga dampaknya dapat menyebabkan waktu henti, informasi yang rusak, atau pelanggaran keamanan, yang semuanya dapat berdampak negatif. Dengan kebijakan audit yang telah ditentukan, administrator dapat melacak perubahan atau upaya untuk mengakses informasi penting yang telah terjadi pada server. Modul Wazuh yang bisa digunakan untuk mendukung hal tersebut, salah satunya yaitu modul File Integrity Monitoring (FIM) yang dapat digunakan untuk memonitor direktori ataupun file pada sistem operasi. Pada sistem operasi Linux sendiri juga terdapat sistem audit yaitu Audit Daemon atau Audit yang dapat digunakan untuk merekam peristiwa yang terjadi pada sistem Linux, dengan menggunakan framework ini sistem dapat melacak apa yang terjadi di sistem operasi dengan mendengarkan peristiwa berdasarkan aturan yang telah dikonfirmasi sebelumnya. [28]

2.20.13 Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time (Muhammad Alfian Fahrudi, I Made Suartana 2023)

Perkembangan teknologi mempengaruhi perusahaan atau instansi untuk memaksimalkan kinerjanya. Perusahaan menggunakan media internet untuk memberikan informasi, layanan, dan menyimpan data melalui web server. Mudahnya mendapatkan informasi pada media internet menimbulkan kejahatan siber dalam upaya untuk mengambil data pada web server. Salah satu pihak yang menangani dan melindungi keamanan jaringan sebuah perusahaan yaitu Security Operation Center (SOC). sangat berperan penting dalam kondisi ini. Pada penelitian ini mengusulkan sebuah sistem integrasi antara end-point security dengan bot messenger Telegram. Sistem integrasi akan membantu pengeluaran finansial perusahaan dan membantu kinerja SOC dalam memantau web server. Wazuh sebagai aplikasi end-point security yang diintegrasikan dengan bot Telegram. Wazuh merupakan aplikasi open source yang didirikan pada tahun 2015. Sistem integrasi Wazuh dengan bot Telegram mampu mengirim pesan dengan format penulisan sesuai kondisi aktivitas yang terjadi pada web server. Sistem integrasi juga mampu mengurangi pesan yang terkirim ketika terjadi aktivitas yang sama secara terus-menerus. Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa integrasi sistem monitoring Wazuh dengan bot messenger Telegram berhasil mengirim pesan secara real-time. [29]

2.20.14 Implementasi *Security Information And Event Management* (SIEM) Untuk Mendeteksi Dan Analisa Insiden Keamanan Pada Web Server (Hadi, Muhammad Sofiyan and , Devi Afriyantari Puspa Putri, S.Kom., M.Sc 2023)

Berdasarkan hasil evaluasi dan analisa yang telah dilakukan penulis, dapat ditarik kesimpulan bahwa penerapan sistem SIEM Wazuh yang dikombinasikan dengan Suricata mampu mendeteksi intrusi pada web

server secara real-time dan membantu dalam menganalisis adanya insiden keamanan berdasarkan log sehingga respon terhadap insiden siber dapat menjadi lebih cepat dan efisien. Dalam penelitian ini, terdapat beberapa uji serangan yang berhasil dideteksi berkat penggunaan sistem SIEM. Hal ini menunjukkan bahwa SIEM cukup efektif dalam menjaga keamanan web server dari ancaman siber. Selain itu, sistem SIEM berhasil diintegrasikan dengan aplikasi Telegram dan berjalan dengan baik sehingga mampu memberikan notifikasi kejadian insiden keamanan langsung melalui pesan Telegram. Penulis memberikan saran terhadap penelitian berikutnya yang serupa untuk mengembangkan sistem agar mampu digunakan untuk Threat Intelligence melalui integrasi dengan beberapa Threat Intelligence feeds seperti VirusTotal, Open Threat Exchange (OTX), Shodan, ThreatConnect, dan yang lainnya. Dengan demikian, sistem mampu mengidentifikasi ancaman insiden keamanan lebih awal sehingga tim IT security dapat menyusun rencana respons keamanan yang lebih baik seperti isolasi host yang terinfeksi atau memblokir alamat IP berbahaya. Berdasarkan hasil pengujian beberapa teknik serangan web server, sistem mampu mendeteksi adanya insiden keamanan terhadap web server kemudian meneruskan log insiden keamanan yang terdeteksi menuju ke central engine SIEM Wazuh sehingga dapat memunculkan security alert untuk dianalisa dari Wazuh dashboard. Hasil dari analisa security alert menunjukkan bahwa security alert yang muncul merupakan insiden yang benar terjadi dan bukan merupakan false positive. [30]

BAB III
METODOLOGI PENELITIAN

3.1 Waktu dan Tempat Pelaksanaan

Waktu penelitian dilakukan mulai bulan September 2023 hingga November 2023 di PSDKU Universitas Lampung di Way Kanan dengan jadwal penelitian sebagai berikut.

Tabel 3. 1 Jadwal Penelitian

No	Aktivitas	Bulan Agustus – Desember 2023				
		Agustus	September	Oktober	November	Desember
1	Perumusan Masalah					
2	Studi Literatur					
3	*Prepare*					
4	*Plan*					
5	*Design*					
6	*Implement*					
7	*Operate*					
8	*Optimize*					
9	Penulisan Laporan Akhir					

3.2 Alat Penelitian

Di dalam pelaksanaan penelitian, digunakan perangkat pendukung berupa sebuah komputer dengan spesifikasi yang ditunjukan pada Tabel 3.2 dan Tabel 3.3

3.2.1 Perangkat Lunak (Software)

Perangakat lunak yang akan digunakan dalam menyelesaikan tugas akhir ini adalah:

Tabel 3. 2 Perangkat Lunak (Software)

No	Perangkat Lunak
1	Windows 11
2	Sistem Operasi Ubuntu 20.04 LTS, Ubuntu 23.04
3	Sistem Operasi Armbian
4	Draw.io
5	Microsoft Word 2019
6	Mendeley Desktop
7	Putty 0.78.0.0
8	Telegram
9.	Slowloris
10.	Hydra

3.2.2 Perangkat Keras (Hardware)

Perangakat keras yang akan digunakan dalam menyelesaikan tugas akhir ini adalah:

Tabel 3. 3 Perangkat Keras (Hardware)

Perangkat Keras				
Jenis	Set Top Box HG680P	PC Axioo MyPC One Pro K5 (8N2) /LaptopLenovo IdeaPad 330-14|GM	Access Point Ruijie RG-RAP2200(E)	Server PSDKU Rainer Intel Corporation S2600STB
CPU	Quad Core ARM Cortex-A53@ up to 1.51 Ghz	Intel® CoreTM i5-1135G7 / Intel® Celereon® N400 CPU @1.10Ghz, 1101 Mhz,		32 CPUs x Intel® Xeon ® Silver 4216 CPU @2.10GHz 67GHz
RAM	2 GB	8GB / 4 GB		16 GB
Storage	8 GB	256 GB / 500 GB		2 TB
OS	Android 6.1 Marsmellow	Windows		VMware vSphere Ubuntu 23.04
Interface			802.11ac Wave2, 1267Mbps	
Operating Modes	-	-	2.4G/5G Router, Wireless Router	
Wireless	-	-	IEEE 802.11b/g/n	
Protocols	-	-	IPv4, IPv6	

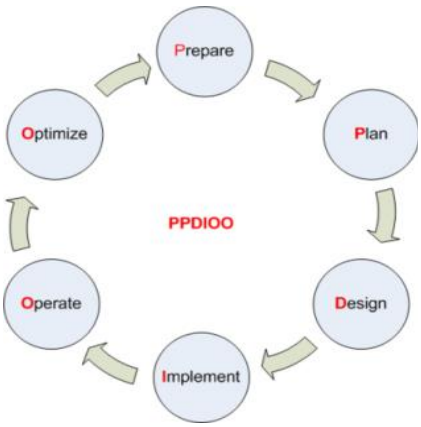
3.2.3 Bahan Penelitian

Adapun bahan penelitian yang digunakan pada penelitian ini yaitu :

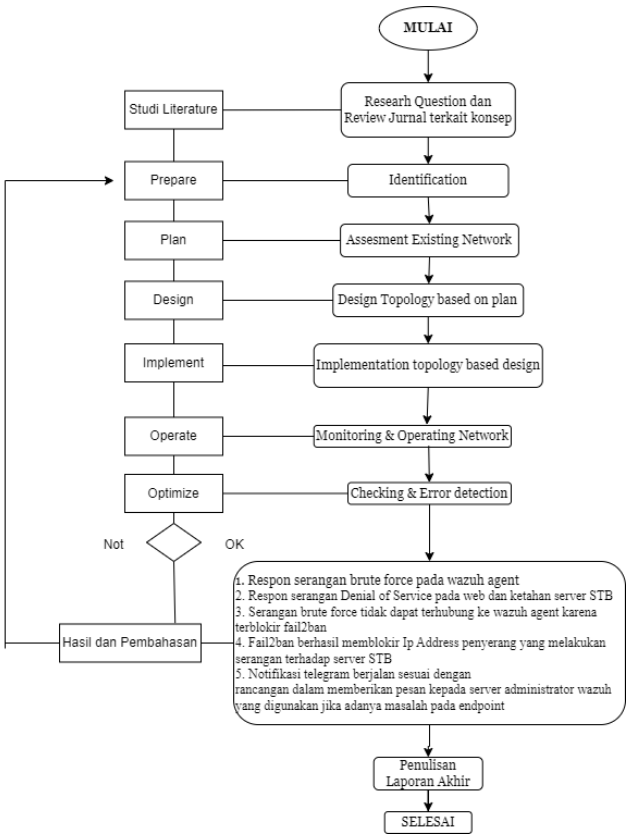
- Bahan penelitian lainnya berupa buku teks, jurnal, skripsi, dan sumber ilmiah lainnya yang didapat dari berbagai situs web

3.3 Tahapan Penelitian

Konsep Tahapan metodologi yang dilakukan pada penelitian ini adalah menggunakan Metode PPDIOO Cisco. PPDIOO Cisco dirancang untuk mendukung pengembangan jaringan. PPDIOO memiliki 6 *Phase* (Tahapan) yaitu *prepare, plan, design, implement, operate, optimize.*



Gambar 3. 1 Metode PPDIOO



Gambar 3. 2 Flowchart Tahapan Penelitian

3.4 Persiapan *(Prepare)*

Berdasarkan hasil pemantauan dan hasil wawancara dengan pihak pengelola PSDKU yang dilakukan pada lab PSDKU, server jaringan di lab tersebut belum memiliki sistem keamanan jaringan yang dapat mendeteksi dan merespon serangan siber. Maka dari itu untuk tahap ini yang perlu di persiapkan yaitu sistem keamanan jaringan guna mendeteksi serangan siber yang masuk pada server jaringan lab PSDKU serta melakukan respon awal terhadap serangan tersebut agar dapat menghindari kerusakan yang lebih serius.

Menilai kemampuan untuk mengelola resiko keamanan menggunakan metode PPDIOO, yang dimana untuk tahapannya ialah sebagai berikut:

1. **Persiapan**

   Pada tahap ini mengidentifikasi masalah konsep keamanan jaringan yang belum tersedia di jaringan PSDKU khususnya di lab komputer dengan melakukan pemantauan serta wawancara yang dilakukan untuk mempersiapkan apa saja yang akan dilakukan untuk melakukan penelitian di PSDKU, terdapat beberapa hasil yang telah didapatkan yaitu Server di PSDKU hanya memiliki 1 server saja, memiliki 2 Lab komputer yang dimana untuk penelitian ini hanya menggunakan Lab Komputer 1 , serta terdapat switch serta access point untuk mengakses jaringan dan internet yang berada di Lab Komputer 1. Server PSDKU belum memiliki keamanan untuk mendeteksi aktivitas biasa ataupun ancaman dari serangan siber, maka dari itu setelah melakukan identifikasi, akan melakukan analisis untuk memastikan apakah jaringan PSDKU memang sudah aman walaupun tidak dilakukan alat pendeteksi atau memang belum aman dari ancaman serangan siber. Sebelum melakukan analisis akan mempersiapkan kebutuhan-kebutuhan apa saja yang akan dilakukan untuk menganalasis jaringan tersebut, untuk kebutuhan seperti perangkat keras dan perangkat lunak sudah ada di table 3.2 dan table 3.3.

2. Perencanaan

Untuk analisis pada tugas akhir ini, akan melakukan percobaan simulasi yang dilakukan pada server jaringan PSDKU dengan menggunakan Hardware Set Top Box (STB) yang sudah terinstall menjadi Server Armbian 20.10, dan melakukan uji coba penyerangan Brute Force dan Denial Of Service menggunakan beberapa PC yang sudah terinstall kali linux yang berada di Lab Komputer terdahap server jaringan PSDKU. Setelah dilakukan uji coba terdapat beberapa masalah yang mengakibatkan pembobolan kata sandi pada sistem server STB sehingga administrator sudah tidak dapat masuk kedalam sistem, dan belum ada respon pengamanan yang bisa mengatasi serangan tersebut. Untuk tahap Denial of Service sebelum menggunakan server Wazuh, serangan ini membanjiri serangan di web server STB yang mengakibatkan web server STB menjadi overload yang cukup lama, dan bagi sebagian besar pengguna sistem, gejala serangan DoS sering kali menyerupai masalah konektivitas jaringan dasar, pemeliharaan rutin, atau lonjakan lalu lintas web sehingga membuat banyak orang mengabaikan masalah tersebut karena tidak memiliki log aktivitas yang bisa dipantau secara real time. Maka dari itu dalam tugas akhir ini mempersiapkan perencanaan penggunaan *platform* wazuh, wazuh merupakan aplikasi *open source* gratis yang berfungsi sebagai *security information and event management* yang dapat membantu dalam mendeteksi ancaman keamanan pada server jaringan PSDKU wazuh server yang berfungsi sebagai alat *monitoring* peristiwa keamanan yang akan diinstall di *cloud* serta wazuh *agent* akan diinstall pada server utama jaringan PSDKU di Lab Komputer. Memilih menggunakan *platform* wazuh sebagai alat yang dapat mendeteksi dan merespon serangan siber pada jaringan komputer server PSDKU. Serta untuk mendeteksi serangan Brute Force dan Denial of Service sebagai salah satu uji coba sistem keamanan jaringan yang akan diimplementasikan di Lab Komputer PSDKU Universitas Lampung Way Kanan menggunakan Server PSDKU.

3. **Desain**

   Pada tahap ini mempersiapkan desain topologi sistem keamanan jaringan yang akan di implementasikan pada jaringan PSDKU, topologi tersebut dibuat berdasarkan hasil pengamatan topologi jaringan pada server PSDKU

4. **Implementasi**

   Pada tahap ini melakukan installasi wazuh server di *cloud* pada *platform idcloudhost* guna untuk *monitoring* peristiwa keamanan dari wazuh *agent*. Kemudian melakukan installasi wazuh *agent* pada server jaringan PSDKU di lab komputer menggunakan server utama PSDKU. Installasi kali linux pada beberapa PC Lab juga dilakukan untuk berperan sebagai penyerang wazuh *agent*, hal ini dilakukan untuk uji coba terhadap sistem keamanan jaringan apakah dapat berjalan dengan baik atau tidak.

5. **Operasi**

   Pada tahap ini melakukan aktivasi wazuh *agent* pada server jaringan PSDKU di lab komputer serta melakukan uji coba serangan *bruteforce* dan *Denial of Service* pada komputer server jaringan PSDKU.

6. **Optimisasi**

   Pada tahap ini melakukan respon terhadap serangan siber yang terjadi pada wazuh *agent*, *software* yang digunakan yaitu fail2ban yang akan memblokir *ip address* penyerang selama beberapa waktu. Hal ini dilakukan untuk pencegahan awal untuk menghindari kerusakan yang lebih serius. Serta mengintegrasikan Wazuh ke Telegram untuk mendeteksi adanya segala aktivitas di server. Hal ini digunakan untuk membantu administrator mengetahui masalah yang terjadi pada server ketika tidak sedang berada di ruang monitoring server.

Keperluan sumber daya sistem untuk Wazuh dapat bervariasi tergantung pada beberapa faktor, termasuk ukuran dan kompleksitas jaringan, jumlah

perangkat yang dimonitor, dan tingkat aktivitas log. Berikut ini adalah perkiraan umum untuk persyaratan sumber daya Wazuh:

1. Storage (Penyimpanan): Keperluan penyimpanan akan bergantung pada jumlah log yang dihasilkan dan disimpan oleh Wazuh. Selain itu, konfigurasi untuk File Integrity Monitoring (FIM) juga dapat mempengaruhi kebutuhan penyimpanan.

2. RAM (Random Access Memory): Wazuh membutuhkan RAM yang memadai untuk menjalankan proses-prosesnya, terutama untuk memproses log dan melakukan deteksi ancaman. Semakin besar jaringan dan semakin banyak perangkat yang dimonitor, semakin besar kebutuhan RAM.

3. CPU (Central Processing Unit): Kebutuhan CPU juga akan bervariasi tergantung pada volume log dan kompleksitas aturan yang diterapkan. Semakin banyak aturan yang diaktifkan, semakin besar kebutuhan CPU.

4. Network Bandwidth (Bandwidth Jaringan): Kebutuhan bandwidth jaringan dapat meningkat tergantung pada volume log yang dikirimkan ke server Wazuh. Jika memonitor banyak perangkat atau mengumpulkan log dari banyak sumber, mungkin memerlukan bandwidth jaringan yang lebih besar.

Tentang seberapa kuat Wazuh dalam menghadapi serangan, keefektifan Wazuh tergantung pada konfigurasi dan pengaturan aturan, serta kemampuan untuk mengenali pola perilaku anormal atau indikator serangan. Wazuh dapat memberikan perlindungan yang baik terhadap berbagai jenis serangan, tetapi tidak ada jaminan bahwa itu akan sepenuhnya mencegah semua serangan.

	Minimum		Recommended	
Component	RAM (GB)	CPU (cores)	RAM (GB)	CPU (cores)
Wazuh indexer	4	2	16	8

Monitored endpoints	APS	Storage in Wazuh indexer (GB/90 days)
Servers	0.25	3.7
Workstations	0.1	1.5
Network devices	0.5	7.4

	Minimum		Recommended	
Component	RAM (GB)	CPU (cores)	RAM (GB)	CPU (cores)
Wazuh server	2	2	4	8

Monitored endpoints	APS	Storage in Wazuh Server (GB/90 days)
Servers	0.25	0.1
Workstations	0.1	0.04
Network devices	0.5	0.2

	Minimum		Recommended	
Component	RAM (GB)	CPU (cores)	RAM (GB)	CPU (cores)
Wazuh dashboard	4	2	8	4

Jumlah data bergantung pada peringatan per detik / *alerts per second* (APS) yang dihasilkan. Tabel ini merinci perkiraan ruang disk yang diperlukan per agent untuk menyimpan peringatan selama 90 hari di server Wazuh Indexer, bergantung pada jenis titik akhir yang dipantau. Jadi bisa dikatakan, untuk lingkungan dengan 80 stasiun kerja, 10 server, dan 10 perangkat jaringan, penyimpanan yang diperlukan di server Wazuh Indexer untuk peringatan 90 hari adalah 230 GB. Dan untuk lingkungan dengan 80 stasiun kerja, 10 server, dan 10 perangkat jaringan, penyimpanan yang diperlukan di Wazuh Server untuk peringatan 90 hari adalah 6 GB.

Untuk keperluan perkiraan ruang disk yang akan dilakukan dilingkungan PSDKU Universitas Lampung Way Kanan per agent untuk menyimpan peringatan selama 90 hari di server Wazuh, untuk lingkungan dengan 10

stasiun kerja, 1 server, 2 perangkat jaringan dan penyimpanan yang diperlukan di server Wazuh Indexer untuk peringatan 90 hari adalah 34 GB dan untuk lingkungan dengan 10 stasiun kerja, 1 server, 2 perangkat jaringan serta penyimpanan yang diperlukan di Wazuh Server untuk peringatan 90 hari adalah 1 GB.

Mempersiapkan klasifikasi Aturan (Rule Level) di Wazuh, Aturan tersebut diklasifikasikan dalam beberapa tingkatan, dari yang terendah (0) hingga maksimum (15). Tabel berikut menjelaskan masing-masing peringatan, yang dapat berguna untuk memahami tingkat keparahan setiap pemberitahuan yang dipicu atau pembuatan aturan khusus.

Tabel 3. 4 Rule Level pada Wazuh

Tingkat	Judul	Keterangan
0	Diabaikan	Tidak ada tindakan yang diambil. Digunakan untuk menghindari positif palsu. Aturan-aturan ini dipindai sebelum aturan lainnya.Sertakan peristiwa yang tidak memiliki relevansi keamanan.
2	Pemberitahuan sistem prioritas rendah	Pemberitahuan sistem atau pesan status. Ini tidak memiliki relevansi keamanan.
3	Acara sukses/Resmi	Ini termasuk upaya login yang berhasil, peristiwa yang diizinkan oleh firewall, dll.

4	Kesalahan sistem prioritas rendah	Kesalahan terkait dengan konfigurasi yang buruk atau perangkat/aplikasi yang tidak digunakan. Ini tidak memiliki relevansi keamanan dan biasanya disebabkan oleh instalasi default atau pengujian perangkat lunak.
5	Kesalahan yang dibuat pengguna	Ini termasuk kata sandi yang terlewat, tindakan yang ditolak, dll. Hal ini tidak memiliki relevansi keamanan.
6	Serangan dengan relevansi rendah	Ini menunjukkan adanya worm atau virus yang tidak berpengaruh pada sistem (seperti kode merah untuk server Apache, dll).Ini juga termasuk kejadian IDS yang sering terjadi dan kesalahan yang sering terjadi.
7	"Kata buruk" cocok	Ini termasuk kata-kata seperti "buruk", "kesalahan", dll. Peristiwa ini sering kali tidak dirahasiakan dan mungkin memiliki relevansi keamanan.
8	Pertama kali terlihat	Sertakan peristiwa yang pertama kali dilihat. Pertama kali peristiwa IDS diaktifkan atau pertama kali pengguna masuk. Ini juga mencakup tindakan yang relevan dengan keamanan (seperti memulai sniffer atau semacamnya).

9	Kesalahan dari sumber tidak valid	Sertakan upaya untuk masuk sebagai pengguna yang tidak dikenal atau dari sumber yang tidak valid. Mungkin memiliki relevansi keamanan (khususnya jika diulang). Ini juga termasuk kesalahan terkait "admin" (akar) akun.
10	Beberapa kesalahan yang dibuat pengguna	Ini termasuk beberapa kata sandi yang buruk, beberapa login yang gagal, dll. Ini mungkin mengindikasikan adanya serangan atau mungkin saja pengguna lupa kredensialnya.
11	Peringatan pemeriksaan integritas	Ini termasuk pesan mengenai modifikasi binari atau keberadaan rootkit (oleh Rootcheck). Ini mungkin mengindikasikan serangan berhasil. Juga termasuk kejadian IDS yang akan diabaikan (jumlah pengulangan yang tinggi).
12	Acara yang sangat penting	Ini termasuk pesan kesalahan atau peringatan dari sistem, kernel, dll. Ini mungkin mengindikasikan serangan terhadap aplikasi tertentu.
13	Kesalahan yang tidak biasa (sangat penting)	Seringkali itu cocok dengan pola serangan yang umum.

14	Peristiwa keamanan yang sangat penting	Seringkali dilakukan dengan korelasi dan ini mengindikasikan serangan.
15	Serangan parah	Tidak ada kemungkinan positif palsu. Perhatian segera diperlukan.

Beberapa hal yang harus disiapkan penulis dalam menyelesaikan tugas akhir ini yaitu mempersiapkan kebutuhan Alat Penelitian dan Bahan Penelitian.

3.5 Perencanaan *(Plan)*

Pada phase metode ini merencanakan bahan untuk menganalisa mengapa harus serangan Brute Force dan DoS yang akan digunakan untuk uji coba sistem keamanan jaringan ini. Setelah menganalisa dan membaca beberapa jurnal dan website dapat disimpulkan bahwa serangan brute force dan DoS merupakan serangan yang popular dikalangan cyberattack karena memiliki catatan aktivitas tindakan merusak terhadap sistem atau jaringan di Indonesia maupun diseluruh dunia. Serangan brute force merupakan metode serangan spesifik dan relatif lama namun lebih disukai untuk akses sistem, terutama menargetkan penyedia layanan cloud. Faktanya, 51% peretas lebih suka menggunakan kekerasan karena kerentanan arsitektur cloud seperti perangkat lunak yang salah dikonfigurasi atau nama pengguna admin yang mudah diperoleh. Variasi terjadi pada tempat peretas memulai dan caranya melakukan upaya. Peretas dapat menggunakan proses manual atau perangkat lunak otomatis untuk menyusup ke jaringan pribadi. Selain itu, peretas mungkin sudah memiliki akses ke informasi tertentu sebelum mereka memulai upayanya. 83% orang Amerika membuat kata sandi yang lemah dalam hal panjang (kurang dari 10 karakter) dan kompleksitas karakter (hanya angka dan huruf) dan 53% menggunakan kata sandi yang sama di seluruh akun**.** 5% dari seluruh pelanggaran data disebabkan oleh serangan brute force. Dari pelanggaran yang disebabkan oleh

peretasan, 80% melibatkan kekerasan atau kredensial yang hilang/dicuri . Untuk serangan *Denial of Service* (DoS) jenis serangan dunia maya yang bertujuan mengganggu situs web (dan jenis properti Internet lainnya) agar tidak tersedia bagi pengguna yang sah dengan cara membanjirinya. Serangan ini lebih sering dilakukan dengan membanjiri host atau jaringan yang ditargetkan dengan permintaan layanan yang tidak sah. Ciri khas dari serangan ini adalah penggunaan alamat IP palsu, yang mencegah server mengautentikasi pengguna. DoS *attack* tetap menjadi ancaman nyata bagi lalu lintas jaringan aplikasi, *server*, ataupun *website* hingga saat ini.

Banyak serangan DoS dari segala jenis dan ukuran dan jaringan adalah salah satu yang terbesar di dunia yang mencakup lebih dari 300 kota di lebih dari 100 negara. Melalui jaringan ini dapat melayani lebih dari 63 juta permintaan HTTP per detik pada puncaknya dan lebih dari 2 triliun permintaan DNS setiap hari. Jumlah data yang sangat besar ini memberikan sudut pandang unik untuk memberikan akses kepada komunitas terhadap tren DoS yang mendalam. Peningkatan serangan DNS yang sengaja direkayasa dan ditargetkan bersamaan dengan lonjakan serangan DDoS sebesar 532% yang mengeksploitasi kerentanan Mitel (CVE-2022-26143). Cloudflare berkontribusi dalam mengungkap kerentanan zero-day ini tahun lalu. Bahkan, menurut laporan *Kaspersky*, serangan ini semakin berkembang dan terus memecahkan rekor tertinggi, hanya dalam waktu tiga bulan saja, yakni pada Januari-Maret 2022, serangan DoS meningkat sebesar 46 persen dibanding kuartal akhir 2021. DoS *attack* juga seringkali tak pandang bulu dalam menyerang jaringan. *Website* besar seperti Amazon *Web Services*, *eBay*, *CNN*, *Wikipedia*, serta *GitHub* pernah menjadi sasaran serangan ini.

Kemudian, perencanaan yang dilakukan selanjutnya yaitu melakukan simulasi uji coba serangan Brute Force dan DoS terlebih dahulu sebelum menggunakan Wazuh Server. Pada tahap awal untuk serangan Brute Force sebelum meng- implementasikan sistem keamanan jaringan menggunakan Server Wazuh Peretas (PC) mengalami pembobolan kata sandi pada sistem server STB sehingga administrator sudah tidak dapat masuk kedalam

sistem, dan belum ada respon pengamanan yang bisa mengatasi serangan tersebut. Untuk tahap Denial of Service sebelum menggunakan server Wazuh, serangan ini membanjiri serangan di web server STB yang mengakibatkan web server STB menjadi overload yang cukup lama, dan bagi sebagian besar pengguna sistem, gejala serangan DoS sering kali menyerupai masalah konektivitas jaringan dasar, pemeliharaan rutin, atau lonjakan lalu lintas web sehingga membuat banyak orang mengabaikan masalah tersebut karena tidak memiliki log aktivitas yang bisa dipantau secara real time.

Maka dari itu dalam tugas akhir ini memilih menggunakan Wazuh dan serangan Brute Force serta Denial of Service sebagai salah satu uji coba sistem keamanan jaringan yang akan diimplementasikan di Lab Komputer PSDKU Universitas Lampung Way Kanan menggunakan Server PSDKU.

Hal selanjutnya yaitu mempersiapkan perangkat keras dan perangkat lunak dalam membangun sistem keamanan jaringan, dilanjutkan dengan mendesain topologi jaringan untuk menerapkan sistem tersebut. Lalu, akan melakukan installasi wazuh server di sistem operasi ubuntu 20.04 Lts yang akan terpasang secara *cloud* di website *idcloudhost*. Penginstalan wazuh server ini bertujuan untuk menerima data *log* dari wazuh *agent* yang kemudian diolah oleh wazuh dan ditampilkan pada *dashboard* wazuh server, data-data ini yang kemudian akan dianalisis oleh administrator jaringan.

Setelah wazuh server berhasil diinstal, penulis beralih melakukan installasi Wazuh *Agent* di *Set Top Box* (STB) dengan sistem operasi armbian yang di jadikan sebagai simulasi server pada jaringan PSDKU khususnya Lab Komputer. Dan installasi Wazuh Agent pada server Ubuntu 23.04 yang berada di server PSDKU, penginstallan wazuh *agent* ini dimaksudkan untuk mencatat semua aktivitas server Lab Komputer PSDKU dan mengirimnya ke wazuh server untuk kemudian dianalisis oleh administrator jaringan. Lalu melakukan installasi sistem operasi kali linux di beberapa PC Lab Komputer yang ditujukan untuk menyerang wazuh

agent yaitu jaringan komputer server di PSDKU Lab Komputer. Jika semua persiapan telah berhasil diinstall maka penulis akan melakukan menghubungkan wazuh server ke wazuh *agent* hal ini dilakukan untuk mengirimkan data *log* dari wazuh *agent* ke wazuh server.

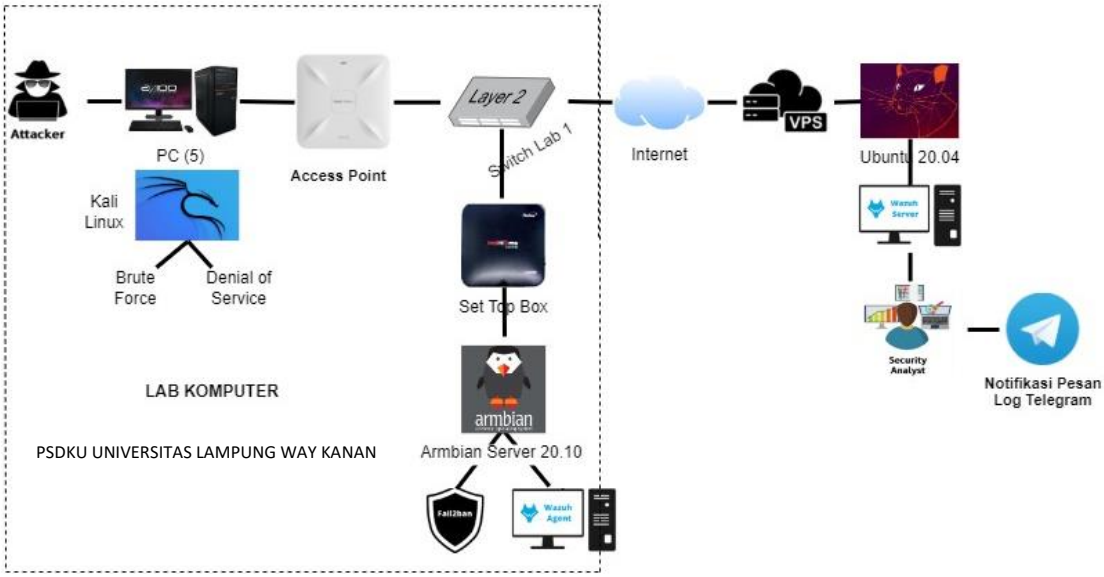
Kemudian merencankan skenario penyerangan yang akan dilakukan terhadap server jaringan Lab Komputer PSDKU, Penyerang akan menggunakan sistem operasi kali linux dan menggunakan perangkat hydra yaitu perangkat lunak yang ditujukan untuk melakukan serangan *bruteforce*. Setelah serangan dilakukan maka wazuh *agent* yang ada di server jaringan Lab Komputer akan merekam aktivitas yaitu percobaan login dari user ke server jaringan, kemudian hasil *log* aktivitas akan dikirimkan ke wazuh server untuk diolah dan akan ditampilkan pada *dashboard* wazuh server.

Untuk mengoptimasi solusi keamanan yang telah dilakukan dalam penelitian ini sistem keamanan jaringan melakukan respon terhadap serangan tersebut dengan bantuan perangkat lunak fail2ban yang akan diinstall pada wazuh *agent*. Fail2ban akan membantu dalam memblokir ip address yang melakukan pelanggaran terhadap aturan keamanan yang telah dikonfigurasi. Sedangkan untuk serangan Denial of Service penyerang menggunakan perangkat lunak slowloris yang ditujukan untuk melakukan serangan untuk menargetkan situs web dan server dengan mengganggu layanan jaringan. Untuk merespons serangan DoS tersebut wazuh akan mendeteksi kejadian serangan kedalam Aktivitas Log dan kemudian Wazuh akan otomatis mengaktifkan command Active Response sebagai tindakan respons otomatis menggunakan Active Responses untuk menanggapi secara cepat pada ancaman yang terdeteksi untuk memblokir IP ketika serangan yang berlangsung.

3.6 Desain *(Design)*

3.6.1 Topologi Simulasi Rancangan Sistem

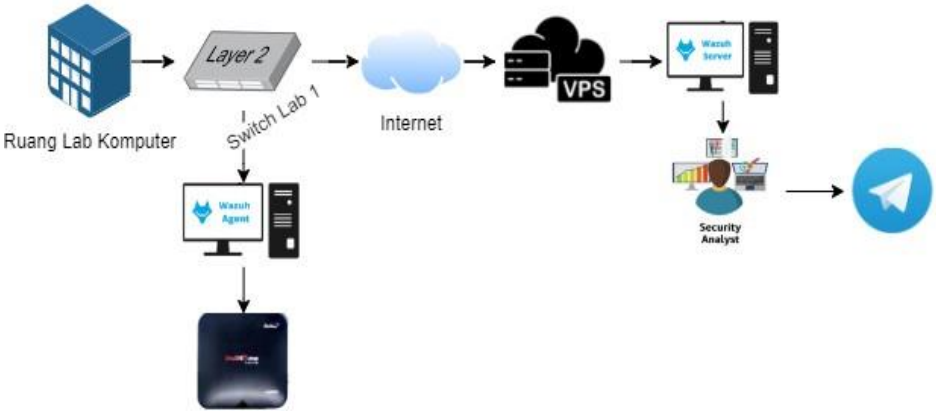
Pada tahapan ini mendesain topologi sistem keamanan jaringan yang akan disimulasikan pada jaringan Lab Komputer PSDKU Universitas Lampung Way Kanan.



Gambar 3. 3 Topologi Simulasi Rancangan Sistem

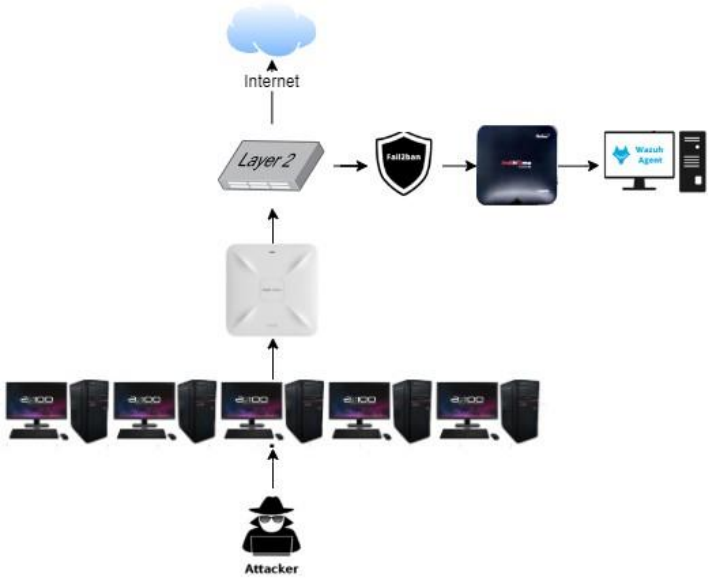
Topologi di atas menunjukkan Rancangan Sistem sebagai simulasi gambaran alur dari sistem keamanan pada jaringan PSDKU. Di Lab Komputer PSDKU sudah terdapat Switch yang akan langsung disambungkan ke server STB menggunakan kabel LAN yang otomatis sudah terhubung ke jaringan PSDKU, STB sudah terinstall Armbian Server Focal Current 20.10, serta sudah terinstall fail2ban serta Wazuh Agent. Jaringan Lab Komputer memiliki internet yang digunakan untuk mengakses Wazuh server menggunakan *IDCloudHost* atau VPS *(Virtual Private Server)* serta didalamnya sudah terdapat *Virtual Machine* OS Ubuntu 20.04 yang dibuat, didalam OS tersebut sudah terinstall Wazuh Server. Kemudian terdapat penyerang *(attacker),* penyerang menggunakan Personal

Computer (PC) yang berjumlah 5-7 PC yang juga sudah terhubung dengan Access Point jaringan PSDKU. Di PC tersebut sudah terinstall Virtual Box yang membuat Virtual Machine yaitu OS Kali Linux, di Kali Linux tersebut penyerang menginstall *software Hydra* untuk mencoba serangan *BruteForce* dan *software Slowloris* untuk serangan *Denial of Service* (DoS) yang akan digunakan untuk menyerang Wazuh Agent. Wazuh Agent yang terinstal pada server lab komputer akan mengirimkan semua *log* termasuk deteksi serangan siber ke wazuh server yang nantinya akan di monitoring oleh administrator jaringan, sekaligus mengirimkan *log* notifikasi ke telegram secara *real time.* Ketika serangan siber terdeteksi maka respon yang diambil yaitu pemblokiran ip address penyerang menggunakan perangkat lunak *file2ban* yang telah diinstal pada wazuh *agent*. Serta menggunakan command Active Response sebagai respon serangan siber yang memang sudah disediakan oleh Wazuh.



Gambar 3. 4 Simulasi Topologi Deteksi Keamanan

Simulasi Topologi Deteksi Keamanan diatas menunjukkan bahwa setiap kegiatan server lab komputer yang dikonekan ke server STB yang sudah menjadi wazuh *agent* akan di kirimkan ke wazuh server yang kemudian akan dimonitoring oleh adiminstrator pada log *security events* yang berada di dashboard wazuh secara *real time* dan otomatis notifikasinya akan masuk ke dalam pesan telegram.

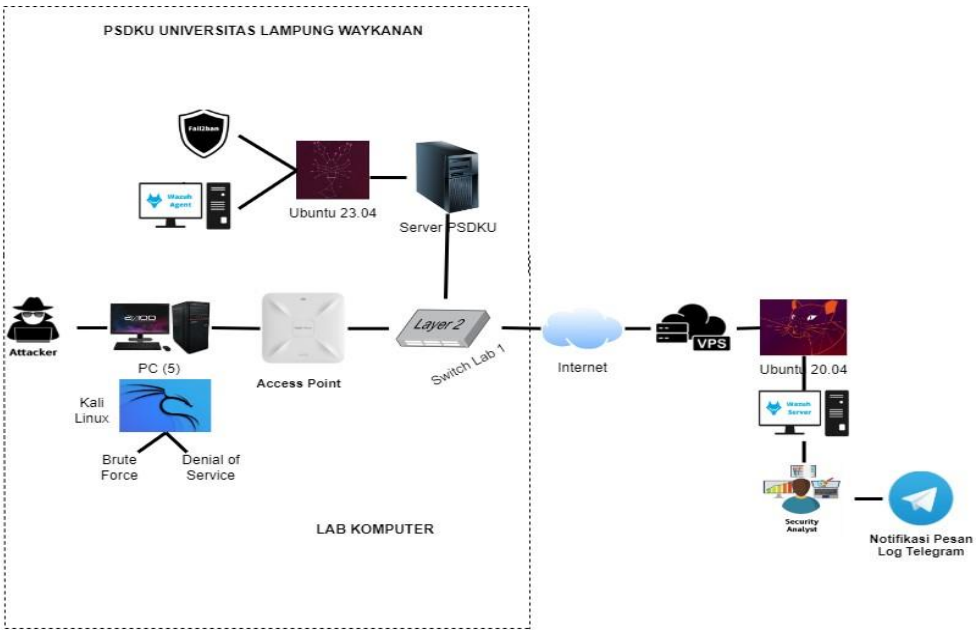


Gambar 3. 5 Topologi Simulasi Response Serangan Siber

Topologi Simulasi Respon Serangan Siber diatas menunjukkan ketika serangan dilancarkan ke server lab komputer maka *fail2ban* akan langsung mendeteksi aktivitas penyerang di server STB, jika aktivitas tersebut melanggar aturan yang telah di konfigurasi *fail2ban*, maka penyerang akan di blokir dengan cara memblokir *IP Adress* penyerang.

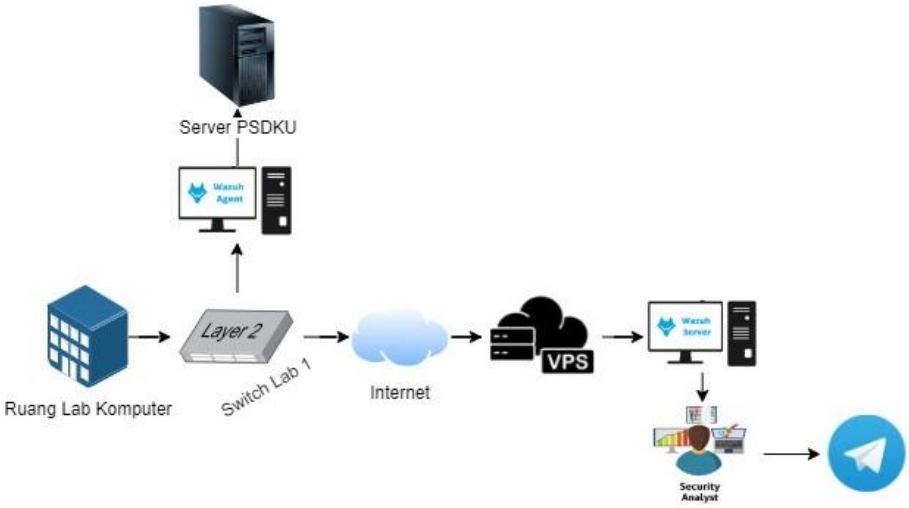
3.6.2 Topologi Rancangan Sistem

Pada tahapan ini setelah melakukan Simulasi terhadap server STB dan berhasil, maka akan dilanjutkan untuk membuat Topologi sistem keamanan jaringan yang akan diimplementasikan pada jaringan Lab Komputer PSDKU Universitas Lampung Way Kanan menggunakan Server Utama PSDKU.



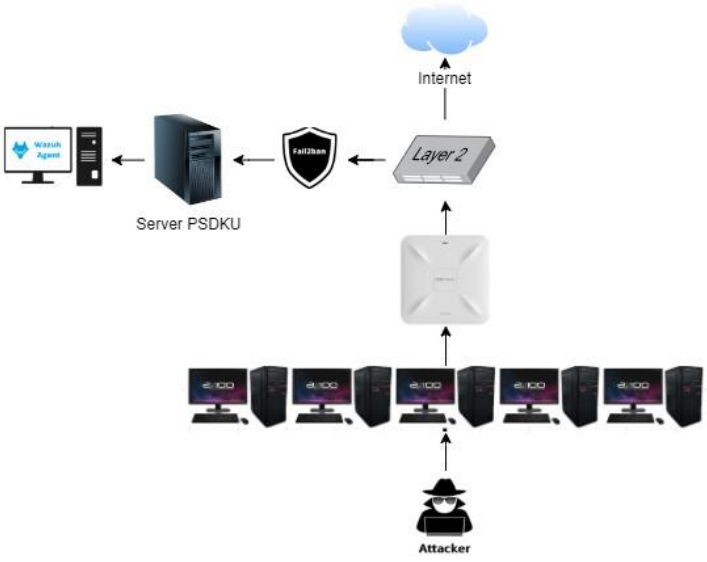
Gambar 3. 6 Topologi Rancangan Sistem

Topologi di atas menunjukkan Rancangan Sistem sebagai gambaran alur Implementasi dari sistem keamanan pada jaringan PSDKU. Di Topologi sebelumnya adalah Simulasi untuk Perancangan Sistem yang akan diimplementasikan dengan menggunakan Server STB, dan untuk rancangan sistem yang sebenarnya akan diimplementasikan menggunakan Server utama PSDKU. Diserver jaringan utama PSDKU sudah terinstall VMware vSphere dan Virtual Machine OS Ubuntu Server 23.04, serta sudah terinstall fail2ban serta Wazuh Agent. Dan untuk alurnya tidak jauh berbeda dengan penjelasan di Topologi Simulasi Rancangan Sistem pada Gambar 3.3.



Gambar 3. 7 Topologi Deteksi Keamanan

Topologi Deteksi Keamanan diatas adalah topologi yang akan direncanakan untuk implementasi di tugas akhir ini. Topologi ini menunjukkan bahwa setiap kegiatan server lab komputer yang dikonekan ke utama PSDKU yang sudah menjadi wazuh *agent* akan di kirimkan ke wazuh server yang kemudian akan dimonitoring oleh adiminstrator pada log *security events* yang berada di dashboard wazuh secara *real time* dan otomatis notifikasinya akan masuk ke dalam pesan telegram.



Gambar 3. 8 Topologi Response Serangan Siber

Topologi Response Serangan Siber diatas adalah topologi yang akan direncanakan untuk implementasi di tugas akhir ini yang menunjukkan ketika serangan dilancarkan ke server utama PSDKU di lab komputer maka *fail2ban* akan langsung mendeteksi aktivitas penyerang, jika aktivitas tersebut melanggar aturan yang telah di konfigurasi di *fail2ban*, maka penyerang akan otomatis di blokir dengan cara memblokir *IP Address* penyerang.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan yang diperoleh berdasarkan hasil dari tugas akhir ini adalah sebagai berikut:

1. Berhasil mengimplementasikan sistem keamanan jaringan yang dapat mendeteksi dan merespon serangan siber menggunakan Wazuh. Administrator dapat memonitoring aktivitas keamanan menggunakan Wazuh.
2. Wazuh berhasil mendeteksi serangan *Brute force* yang dilakukan didalam jaringan.
3. Fail2ban berhasil diterapkan dan dapat mencegah aktivitas serangan bruteforce.
4. Wazuh tidak dapat mendeteksi serangan *Denial of Service* (DoS) apabila serangan dilakukan dengan skala dan intensitas yang kecil dengan jumlah rata-rata koneksi dibawah 4000 koneksi http.
5. Serangan *Denial of Service* berhasil dilakukan dengan hasil yang menunjukkan bahwa Server Utama PSDKU memiliki ketahanan dalam menerima dan melayani koneksi HTTP dibawah 3.522.013 koneksi dari total keseluruhan soket koneksi HTTP.
6. Integrasi Wazuh ke Telegram berhasil dilakukan dengan baik dan mampu mendeteksi adanya segala aktivitas di server. Hal ini membantu administrator mengetahui masalah yang terjadi pada server ketika tidak sedang berada di ruang monitoring server.

5.2 Saran

Adapun saran yang diperoleh berdasarkan hasil dari tugas akhir ini adalah sebagai berikut

1. Penulis menyarankan untuk mengembangkan sistem secara lebih lanjut dengan melakukan jenis serangan yang lainnya tidak hanya berfokus terhadap serangan *Brute Force* dan *Denial of Service* (DoS) dengan tujuan untuk mengetahui kemampuan deteksi dari SIEM.
2. Penulis berharap sistem keamanan jaringan ini dapat diterapkan secara lebih luas pada PSDKU Universitas Lampung Way Kanan, maupun instansi lainnya.

DAFTAR PUSTAKA

[1] Badan Siber dan Sandi Negara, Id-SIRTII/CC 2023. Laporan Bulanan Publik Hasil Monitoring Keamanan Siber 2023.

[2] Aji, R. P., Prayudi, Y., & Luthfi, A. Analysis Of Brute Force Attack Logs Toward Nginx Web Server On Dashboard Improved Log Logging System Using Forensic Investigation Method. *Jurnal Teknik Informatika (Jutif)*, *4*(1), 39-48,2023

[3] Kamal and Setiawan. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Jurnal Informatika Universitas Islam Indonesia* Vol. 2 No. 2, 2021

[4] Fitri Nova, Pratama, M. D., & Prayama, D. Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos, 2022

[5] Sampurna, M. R. Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA: Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA. *Journal of Network and Computer Applications (ISSN: 2964-6669)*, *1*(2), 25-33, 2022

[6] Prasetyo, K. A., Idhom, M., & Wahanani, H. E. (2020). Sistem Pencegahan Serangan Bruteforce Pada Multiple Server Dengan Menggunakan Fail2ban. *Jurnal Informatika dan Sistem Informasi*, *1*(3), 789-796.

[7] Wongkar, S., Sinsuw, A. A., & Najoan, X. (2015). Analisa implementasi jaringan internet dengan menggabungkan jaringan lan dan wlan di desa kawangkoan bawah wilayah amurang ii. *Jurnal Teknik Elektro dan Komputer*, *4*(6), 62-68.

[8] Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). *terAs Law Review: Jurnal Hukum Humaniter dan HAM*, *3*(1), 11-22.

[9] Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi)*, *22*(2), 143-158.

[10] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.

[11] Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2023). Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka). Jurnal Bidang Penelitian Informatika, 1(1), 57-64.

[12] Prayogo, F. A. (2016). *Perancangan Sistem Pencegahan Serangan Bruteforce pada Jaringan Wireless* (Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW).

[13] Patuke, R., Mulyanto, A., & Takdir, R. (2022). Pengukuran Kinerja Set Top Box (STB) Sebagai Penyimpanan Cloud. *Diffusion: Journal of Systems and Information Technology*, *2*(2), 1-12.

[14] Ma, L., & Zhao, D. (2022, September). Research on Setting of Two Firewall Rules Based on Ubuntu Linux System. In *2022 International Conference on Computer Network, Electronic and Automation (ICCNEA)* (pp. 178-182). IEEE.

[15] Siagiaan, E. R. (2023). Pelatihan Pengenalan Dasar Linux Ubuntu 22.04 LTS di Pusat Pendidikan Manajemen Bisnis "Mitra Kreatif Computer" Kisaran. *Jurnal Masyarakat Indonesia (Jumas)*, *2*(02), 109-116.

[16] Singh, G. D. (2022). *The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-ng, and Empire*. Packt Publishing Ltd.

[17] Dandotiya, M., Dandotiya, A. S., Dandotiya, N., & Sahu, A. A Secure Detection Framework for ARP, DHCP, and DoS Attacks on Kali Linux.

[18] Eliyan, LF, & Pietro, R Di (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, Elsevier, https://www.sciencedirect.com/science/article/pii/S0167739X21000911

[19] Purwanto, A, & Soewito, B (2021). Optimization problem of computer network using ppdioo. *ICIC Express Lett*, scholar.archive.org,z

[20] Hidayat, Sutanta and Raharjo (2016). PENGONTROLAN VPS (VIRTUAL PRIVATE SERVER) SEBAGAI SERVER RADIO STREAMING VIA ANDROID

[21] Husnul Khotimah, Fitri Bimantoro, Robert Silas Kabanga, Ida BagusKetut Widiartha (2022). Implementasi *SecurityInformation And Event Management* (Siem) PadaAplikasi Sms *Center*Pemerintah Daerah ProvinsiNusa Tenggara Barat

[22] Arif Gilang Surya Harahap,Hutrianto (2021). *Intrusion Detection And Anomaly* Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang

[23] Fariadi , M RezaRedo Islami (2022). Deteksi Dini Serangan PadaWebsite MenggunakanMetode *Anomali Based*

[24] Stanković, S, Gajin, S, & Petrović, R (2022). *A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis*., etran.rs, https://www.etran.rs/2022/zbornik/ICETRAN-22_radovi/068-RTI2.6.pdf

[25] Iwan Kurniawan , Ferry Mulyanto, Fuad Nandiasa (2016) SISTEM PENCEGAHAN SERANGAN BRUTEFORCE PADA UBUNTU SERVER DENGAN MENGGUNAKAN FAIL2BAN.

[26] Stefan Stanković, Slavko Gajin, and Ranko Petrović, Member, IEEE 2022. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis

[27] Suryantoro, T, Purnomosidi, BDP, & ... (2022). The Analysis of Attacks Against Port 80 Webserver with SIEM Wazuh Using Detection and OSCAR Methods. *2022 5th International …*, ieeexplore.ieee.org, https://ieeexplore.ieee.org/abstract/document/10052950/

[28] Nisa, AK (2023). *Implementasi File Integrity Monitoring System Menggunakan Wazuh Open Security Platform*., etd.repository.ugm.ac.id, https://etd.repository.ugm.ac.id/penelitian/detail/225639

[29] Muhammad Alfian Fahrudi, I Made Suartana (2023). Integrasi End-point Security Berbasis Agent dan Bot Messenger untuk Deteksi dan Monitoring Serangan pada Web Server secara Real-time

[30] Hadi, Muhammad Sofiyan and , Devi Afriyantari Puspa Putri, S.Kom., M.Sc (2023) *Implementasi Security Information And Event Management (SIEM) Untuk Mendeteksi Dan Analisa Insiden Keamanan Pada Web Server*. Skripsi skripsi, Universitas Muhammadiyah Surakarta.

[31] Arif Gilang Surya Harahap , Hutrianto (2021) Intrusion Detection And Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang.

[32] Arman, M. (2020). Metode pertahanan web server terhadap distributed slow HTTP DoS attack. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, *7*(1), 56-70.

[33] Wazuh documentation: https://documentation.wazuh.com/current/getting-started/index.html