Skema Pendanaan: Peneliti Madya

LAPORAN PENELITIAN

Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall

Peneliti

Hillman Akhyar Damanik, S. Kom., M. Kom (190016)

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR
AGUSTUS 2024

HALAMAN PENGESAHAN
LAPORAN PENELITIAN

Judul Penelitian	: Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall
Bidang Penelitian	: Teknologi Informasi
Ketua Peneliti	
a. Nama Lengkap	: Hillman Akhyar Damanik
b. NIP/NIDN/ID-SINTA	: 190016/0320038704/6694077
c. Jabatan Fungsional	: Asisten Ahli
d. Program Studi	: Teknik Informatika
e. Nomor HP	: 082299099294
f. Alamat e-mail	: hillman.akhyardamanik@budiluhur.ac.id
Mahasiswa (1)	
a. Nama Lengkap	: Fadhilla Muhammad
b. NIM	: 2111500019
Mahasiswa (2)	
a. Nama Lengkap	: Akbar Nur Wahyudin
b. NIM	: 2011500754
Lama Penelitian	: 6 bulan
Biaya Penelitian	
a. Sumber Universitas Budi Luhur	: Rp. 7500.000
b. Sumber lain (sebutkan jika ada)	: Rp. -

Jakarta, 09-08-2024

Mengetahui,
Dekan/Kepala Pusat Studi

(Dr. Achmad Solichin, S.Kom., M.T.I)
NIP 050023

Ketua Pelaksana

(Hillman Akhyar Damanik, S. Kom., M. Kom)
NIP 190016

Menyetujui,
Direktur Riset dan Pengabdian Kepada Masyarakat

(Ir. Prudensius Maring, M.A.)
NIP 190043

No. Registrasi : 011 01 LPJ 08 24
Tanggal : 12 08 24 Paraf :

RINGKASAN

Kompleksitas ancaman siber terhadap infrastruktur jaringan perusahaan, institusi pendidikan, dan pemerintah menjadikan perlindungan infrastruktur jaringan sebagai prioritas utama. Berbagai perangkat router dan server sangat rentan terhadap berbagai jenis ancaman siber, sehingga memerlukan solusi deteksi dan respons yang komprehensif. Penelitian ini akan mengimplementasikan sistem deteksi intrusi dengan mengintegrasikan teknologi SIEM dan (Extended Detection and Response solutions) XDR Wazuh. Sistem ini menganalisis data index pattern dari perangkat wazuh agent untuk mendeteksi dan merespons serangan menggunakan firewall active response XDR. Pengujian dilakukan pada perangkat MikroTik Router, ubuntu server untuk menguji serangan reconnaissance attack, brute force dan DoS. Hasil penelitian menunjukkan serangan Nmap dan brute force berhasil dideteksi oleh Wazuh Manager dan memblokir IP penyerang melalui active response. Pendeteksian serangan brute force menunjukkan peningkatan traffic hingga 60 Kbps dan penggunaan CPU mencapai 100%, kemudian terjadi penurunan setelah firewall active response diaktifkan. Authentication failure mencapai 2198 kali dalam satu jam pertama serangan brute force. Penggunaan CPU meningkat dari 20% hingga 85% selama serangan dan menurun menjadi 15% setelah firewall active response diaktifkan. Serangan DoS, pada MikroTik mengalami peningkatan penggunaan CPU hingga 89% dan memori 56.32%. Setelah aktivasi firewall active response, penggunaan CPU menurun menjadi 5%. Traffic pada interface MikroTik meningkat hingga 3.3 Mbps selama serangan, kemudian menurun ke 1 Kbps setelah firewall diaktifkan.

Kata Kunci: Suricata, Distributed Denial-of-Service, Agglomerative Hierarchical Clustering, IPTables

PRAKATA

Puji dan syukur kami curahkan ke hadirat Tuhan Yang Maha Esa yang telah mencurahkan semua karunia sehingga diberikan keyakinan dan kemudahan dalam menyusun dan menyiapkan laporan penelitian ini dengan judul Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall. Pada kesempatan ini, peneliti ingin menyampaikan rasa terima kasih kepada:

1. Bapak Dr. Achmad Solichin, S. Kom., M.T.I. sebagai Dekan Fakultas Teknologi Informasi Universitas Budi Luhur.
2. Bapak Dr. Ir. Prudensius Maring, M.A. sebagai Direktur Penelitian dan Pengabdian Masyarakat Universitas Budi Luhur.
3. Semua pihak yang telah membantu penelitian ini, mohon maaf apabila ada kesalahan yang terucap dan terbersit, mohon dibukakan pintu maaf yang selapang-lapangnya.

Akhirnya dengan segala kerendahan hati, peneliti berharap agar penelitian ini dapat memberikan manfaat bagi peneliti, lingkungan kampus dan sekitarnya. Saran dan kritik yang membangun sangat diharapkan guna perbaikan penelitian mendatang.

Jakarta, Agustus 2024

DAFTAR ISI

RINGKASAN ..... **iii**
PRAKATA ..... **iv**
DAFTAR TABEL ..... **viii**
DAFTAR GAMBAR ..... **ix**
DAFTAR LAMPIRAN ..... **xii**
BAB I **12**
PENDAHULUAN **12**
1. Latar Belakang dan Rumusan Masalah 12
2. Pendekatan Pemecahan Masalah 13
3. State of the Art dan Kebaruan 13
4. Peta Jalan Penelitian 15
BAB II **16**
METODE **16**
2. Metode Penelitian 16
2.1. Studi Literature 17
2.1.1. Prepare (Persiapan) 17
2.1.2. Planning (Perencanaan) 18
2.1.3. Design 19
2.1.4. Implementation (Implementasi) 20
2.1.5. Operate (Operasional) 21
2.1.6. Optimize 22
BAB III **24**
HASIL PELAKSANAAN PENELITIAN **24**
3.1. Tahap Prepare (Identifikasi Penelitian) **24**
3.1.1. Jenis Serangan dan Implementasi Mitigasi 25
3.1.2. Evaluasi Hasil 26
3.2. Tahap Planning (Formulasi Arsitektur Jaringan dan Desain Sistem) **26**
3.2.1. Instrumentasi Kebutuhan Perangkat Keras (Hardware) dan Perangkat Lunak (Software) 26
3.2.2. Perancangan Arsitektur Topologi Physic pada lingkungan Infrastruktur Jaringan 29

3.3. Tahap Desain (Pengembangan Arsitektur Teknis) 30

3.3.1. Konfigurasi Topologi 31

3.3.2. Konfigurasi IP Address 32

3.3.3. Node Proxmox *Hypervisor* Wazuh *Agent* 33

3.3.4. Node VMWare Hypervisor Attacker 34

3.3.5. Konfigurasi Node Wazuh Agent 35

3.3.6. Arsitektur Framework Firewall IPTables dan Active Response Wazuh 36

3.4. Tahap Implementasi (Implementasi dan Pengujian Fungsionalitas Sistem) 39

3.4.1. Instalasi dan Konfigurasi Wazuh *Security Information and Event Management* (SIEM) dan Extended Detection and Response (XDR) 40

3.4.2. Konfigurasi *Syslog* dan *Log Index Pattern Archives* pada Wazuh server 52

3.4.3. Konfigurasi Wazuh *Agent* 55

3.4.4. Implementasi dan Konfigurasi Node Agent Router MikroTik 62

3.4.5. Konfigurasi dan Implementasi *Node Attacker* 64

3.4.6. Perancangan dan Implementasi Framework iptables ipset dan Active Responses Firewall Wazuh 67

3.5. Tahap Operasi (Operasi dan Eksekusi Sistem) 73

3.5.1. Pengujian Serangan Network Mapping pada Perangkat Wazuh Agent (Ubuntu Server) 73

3.5.2. Pengujian Serangan *Brute Force* pada Perangkat Wazuh Agent (Ubuntu Server) 77

3.5.3. Pengujian Serangan *Denial of Service* (DoS) pada Perangkat Wazuh Agent (Ubuntu Server) 83

3.5.4. Pengujian Serangan Denial of Service (DoS) pada Perangkat Wazuh Agent (MikroTik RouterOS) 84

3.6. Tahap Optimasi (Evaluasi) 87

3.6.1. Konfigurasi dan Evaluasi Optimasi Firewall Active Responses Wazuh XDR 88

3.6.2. Evaluasi Optimasi Firewall Active Responses Wazuh XDR (Scanning NMAP) 89

3.6.3. Evaluasi Optimasi Firewall Active Responses Wazuh XDR (Serangan Brute Force) 90

BAB IV 104
KESIMPULAN DAN SARAN 104
4.1. Kesimpulan 104
4.2. Saran 104
DAFTAR PUSTAKA 106
LAMPIRAN 108

DAFTAR TABEL

1. Tabel 3.1 Instrumen Kebutuhan Perangkat Keras (Hardware) 27
2. Tabel 3.2 Instrumen Kebutuhan Perangkat Keras (*Software*)..... 29
3. Tabel 3.3 Komponen Konfigurasi IP Address 32
4. Tabel 3.4 Node Proxmox *Hypervisor Wazuh Agent* 33
5. Tabel 3.5 VMWare *Hypervisor* (*Attacker*) 35
6. Tabel 3.6 Konfigurasi dan Penamaan Wazuh *Agent*..... 36
7. Tabel 3.7 Konfigurasi wazuh *agent* pada *hypervisor* proxmox 55
8. Tabel 3.8 Konfigurasi Logical Wazuh Agent Router MikroTik..... 63
9. Tabel 3.9 Hasil log pada wazuh manager pada MikroTik RouterOS. 74

DAFTAR GAMBAR

1. Gambar 2.1 Metode dan Tahapan Penelitian 16
2. Gambar 2.2 Perancangan Sistem Infrastruktur Jaringan Router dan Server 23
3. Gambar 3.1 Perancangan Arsitektur Topologi *Physic* 30
4. Gambar 3.2 Perancangan Arsitektur Topologi *Logic* 31
5. Gambar 3.3 Perancangan Arsitektur Topologi *Logic* 37
6. Gambar 3.4 Arsitektur modul XDR Active Response wazuh..... 37
7. Gambar 3.5 Tahap instalasi Wazuh Manager 41
8. Gambar 3.6 Konfigurasi Node Wazuh Indexer, Manager dan Server 42
9. Gambar 3.7 Konfigurasi Sertifikat Wazuh Indexer 43
10. Gambar 3.8 Konfigurasi file `opensearch.yml` 44
11. Gambar 3.9 Status Wazuh Indexer..... 44
15. Gambar 3.10 Verifikasi Konfigurasi Wazuh *Indexer* 45
16. Gambar 3.11 Verifikasi Operasioan Wazuh Manager 46
17. Gambar 3.12 Instalasi dan Konfigurasi Paket Wazuh Filebeat..... 46
18. Gambar 3.13 Konfigurasi *file script filebeat index.number_of_shards* 47
19. Gambar 3.14 Konfigurasi Filebeat Wazuh *Alert* dan *Archives* 48
20. Gambar 3.15 Sertifikat Filebeat 49
21. Gambar 3.16 Verifikasi status Filebeat 50
22. Gambar 3.17 Pengujian Filebeat dan *Elasticsearch* 50
23. Gambar 3.18 Konfigurasi Wazuh Dashboard dan Sertifikat 51
24. Gambar 3.19 Konfigurasi Wazuh Dashboard 51
25. Gambar 3.20 Konfigurasi Host Wazuh (`wazuh.yml`)..... 52
26. Gambar 3.21 Konfigurasi `ossec_config` Wazuh Server 53
27. Gambar 3.22 Dataset Log Wazuh-Archives 56
28. Gambar 3.23 Konfigurasi Wazuh Agent di VM Proxmox 56
29. Gambar 3.24 Konfigurasi Wazuh Agent Brute Force..... 57
30. Gambar 3.25 *Script* Koneksi (*Brute Force*) ke Wazuh Manager..... 57
31. Gambar 3.26 Konfigurasi agent (Brute Force) 58
32. Gambar 3.27 Konfigurasi Wazuh Agent Hping3..... 59
33. Gambar 3.28 *Script* Koneksi Wazuh Agent (Hping) ke Wazuh Manager. 59

34. Gambar 3.29 Konfigurasi Wazuh Agent Agent_Hping3 60
35. Gambar 3.30 Konfigurasi Wazuh *Agent Network Mapping* 61
36. Gambar 3.31 *Script* Koneksi (*Network Mapping*) ke Wazuh Manager 62
37. Gambar 3.32 Konfigurasi Wazuh Agent Agent_Network_Mapping 62
38. Gambar 3.33 MikroTik Decoder 64
39. Gambar 3.34 VMWare dan Kali Linux OS 65
40. Gambar 3.35 Firewall IPTable IPSet 68
41. Gambar 3.36 Active Response Brute Force 69
42. Gambar 3.37 Active Response Nmap dan DoS 70
43. Gambar 3.38 Konfigurasi *Decoder* Router MikroTik (`decoder.xml`) . 71
44. Gambar 3.39 Konfigurasi MikroTik *Rules* 72
45. Gambar 3.40 Inventory Agent Wazuh 74
46. Gambar 3.41 Serangan Attacker Nmap menuju Wazuh Agent 74
47. Gambar 3.42 Pemindaian Nmap menuju Wazuh Agent 75
48. Gambar 3.43 Deteksi Log Wazuh Agent 75
49. Gambar 3.44 *Alert* serangan yang terdeteksi pada wazuh manager..... 77
50. Gambar 3.45 Grafik Serangan pada Wazuh Dashboard 77
51. Gambar 3.46 *Inventory Agent* Wazuh *Brute Force* 78
52. Gambar 3.47 Serangan Attacker (Brute Force) menuju Wazuh Agent 78
53. Gambar 3.48 Pengujian konektivitas wazuh agent dari Kali Linux 80
55. Gambar 3.49 Serangan Brute Force pada Wazuh Agent 80
56. Gambar 3.50 Upaya Autentikasi Gagal dari Serangan Brute Force 81
57. Gambar 3.51 Monitoring Wazuh Dashboard (Serangan Brute Force) 82
58. Gambar 3.52 Monitoring Events Wazuh Dashboard Brute Force Attack . 83
59. Gambar 3.53 Inventory Agent Wazuh Denial of Service (DoS) 84
60. Gambar 3.54 Serangan *Attacker* (*Brute Force*) menuju Wazuh *Agent*..... 84
61. Gambar 3.55 Log Wazuh Manager *log-prefix=SYN Flood Attempt* 85
62. Gambar 3.56 Statistik SeranganDoS pada Wazuh Manager..... 86
63. Gambar 3.57 Topologi Optimasi *Active Responses* Wazuh XDR 88
64. Gambar 3.58 Active Responses Wazuh Serangan (*Scanning*) Nmap..... 89
65. Gambar 3.59 Active Responses Wazuh Serangan (*Scanning*) Nmap..... 90

66. Gambar 3.60 Hasil Deteksi Serangan *Brute Force* pada Manager 91
67. Gambar 3.61 Peningkatan *Traffic* di *Interface* ens18 pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 92
68. Gambar 3.62 Peningkatan *Traffic* CPU *Jumps* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 93
69. Gambar 3.63 Peningkatan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 93
70. Gambar 3.64 Authentication Failure Serangan Brute Force (1 Hours) 94
71. Gambar 3.65 Hasil Deteksi *Active Response* Firewall 95
72. Gambar 3.66 Monitoring Wazuh Manager Selama 2 Jam 96
73. Gambar 3.67 Penurunan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 96
74. Gambar 3.68 Penurunan *Traffic* CPU *Jumps* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 97
75. Gambar 3.69 Penurunan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force* 98
76. Gambar 3.70 Peningkatan *Traffic* CPU *Utilization* pada Perangkat MikroTik RouterOS (wazuh *agent*) dari serangan *Denial of Service* (DoS)..... 90
77. Gambar 3.71 Peningkatan Interface Network pada Perangkat MikroTik Router OS (wazuh agent) dari serangan Denial of Service) 99
78. Gambar 3.72 ICMP ping loss Serangan DoS 99
79. Gambar 3.73 ICMP ping Drop Serangan DoS 100
80. Gambar 3.74 High Spike Memory Usage Attack DoS 100
81. Gambar 3.75 High Spike CPU Usage Attack DoS 101
82. Gambar 3.75 Reduction in CPU usage traffic on the wazuh agent..... 101
83. Gambar 3.75 Reduction in memory usage traffic on the wazuh agent 102
84. Gambar 3.75 ICMP Ping normal status 102
85. Gambar 3.75 ICMP Ping Loss normal status 102

DAFTAR LAMPIRAN

1. **Lampiran 1.** Realisasi Penggunaan Anggaran..... 104
2. **Lampiran 2.** Biodata Ketua dan Anggota Tim Peneliti..... 106
3. **Lampiran 3.** Surat Perjanjian Kontrak Penelitian..... 111
4. **Lampiran 4.** Catatan Harian 114
5. **Lampiran 5.** Artikel Ilmiah (*Submitted*)..... 116
7. **Lampiran 6.** HKI 118

BAB I

PENDAHULUAN

1. Latar Belakang dan Rumusan Masalah

Perangkat infrastruktur jaringan router dan server saat ini hadir lebih banyak variasi dan jumlah, dengan penempatan perangkat pada *node*, *edge* dan *end point* yang vital dan krusial dalam keberlangsungan operasional jaringan perusahaan, baik dalam skala Small Office Home Office (SOHO), *enterprise, service provider*, pendidikan dan pemerintah (1). Ancaman, kerentanan dan resiko pada perangkat tersebut menjadi celah bagi para peretas untuk melakukan serangan siber (*cyberattacks*) dan kejahatan *cyber* (*cybercrime*), termasuk *reconnaissance attack*, *access attack* dan *DoS attack*. Banyak perusahaan yang mempunyai kantor yang tersebar dan menghubungkan ratusan perangkat berupa router dan server dan seringkali tidak aman dan memiliki kerentanan yang berbeda, yang disebabkan oleh pertumbuhan informasi dan jaringan yang berkembang pesat (2). Serangan DDoS merupakan salah satu ancaman terbesar yang sering terjadi pada layanan pengadaan pemerintah (LPSE) (3). Serangan DDoS masih menjadi ancaman besar, terutama akibat peningkatan konektivitas pada perangkat Edge router ISP, penelitian ini mengidentifikasi dan menganalisis aktivitas DDoS menggunakan *honeynet* berdasarkan paket yang ditangkap dan dianalisis oleh *network protocol sniffer* dan alat analisis serangan berbasis signature (4). Sebanyak 4 juta dengan ukuran 4 TB mengungkap perangkat MikroTik terinfeksi serangan DDoS dan malware (5) (6). Muwardi melakukan percobaan pembuatan prototype sistem keamanan, monitoring dan evaluasi sistem keamanan server menggunakan IDS Snort untuk keamanan infrastruktur perangkat server yang terhubung kejaringan, untuk pengujian brute force (7). Pola serangan brute force pada SSH port pada perangkat router menghasilkan nama pengguna dan kata sandi yang paling banyak dieksploitasi oleh peretas (8). Laporan Badan Siber dan Sandi Negara (BSSN) selama tahun 2023 menemukan banyak upaya serangan DoS yang menargetkan Indonesia dan diprediksi sampai tahun 2024 potensi serangan DoS ini akan terus meningkat. Selama tahun 2023 terdapat sebanyak 403.990.813 anomali. 4.001.905 aktivitas Advanced Persistent Threat (APT) dan aktivitas ransomware sebanyak 1.011.209

(9). Berdasarkan uraian latar belakang dari kompleksitas serangan dan ancaman cybercriminals, perumusan permasalahan untuk penelitian ini yaitu 1) Mengembangkan dan membangun sistem keamanan pada perangkat router dan server yang efektif untuk untuk mendeteksi serangan reconnaissance attack, access attack dan DoS attack. 2) Mengintegrasikan wazuh XDR dan Suricata, untuk mengimplementasikan sistem deteksi intrusi yang holistik dengan memberikan respon terhadap serangan yang terdeteksi. 3) Menguji, mengevaluasi dan memitigasi jenis serangan termasuk pengukuran sumber daya CPU dan memori.

2. Pendekatan Pemecahan Masalah

Pendekatan dan strategi pemecahan masalah dilakukan dengan pendekatan yang meliputi:

1. Identifikasi dan analisis kebutuhan. Langkah ini melibatkan pengetahuan yang komprehensif tentang konfigurasi perangkat keras dan perangkat lunak yang digunakan pada topologi, VMWare dan Proxmox akan digunakan sebagai virtualisasi hypervisor untuk node Apache web server, Ubuntu Server, Kali Linux, dan attacker endpoint Hping3, Hydra Parrot OS dan Network Mapping (Nmap).
2. XDR Wazuh dan SIEM Server dikonfigurasi dan diimplementasikan untuk menganalisis data log dari peristiwa yang dihasilkan dari perangkat node virtualisasi server.
3. Mitigasi serangan dengan Firewall *iptables ipset* dan *active response* (XDR) wazuh, digunakan untuk menambahkan *rule* dan *policy* berdasarkan metode Firewall, untuk membuat *policy drop* berdasarkan *malicious source* IP Address.

3. State of the Art dan Kebaruan

Ancaman serangan siber yang semakin tinggi pada perangkat jaringan router dan server, sampai saat ini telah menjadi perhatian utama bagi perusahaan, instansi Pendidikan dan pemerintahan. Sementara itu, sampai saat ini banyak penelitian yang dilakukan dengan teknik serangan yang beragam dan berkembang pesat

seperti reconnaissance attack, access attack dan DoS attack. Penelitian penggunaan teknologi IPS Honeypot Artillery dan Wazuh SIEM hanya dilakukan untuk memblokir lalu lintas yang anomali dari event log IPS honeypot, dan hanya menggunakan server based (10). Sankar dan Fasila mengintegrasikan ELK stack dan Wazuh untuk mengumpulkan data dan mendeteksi ancaman, intrusi, dan anomali. Namun penelitian ini hanya menghasilkan SOC untuk pemantauan pada sistem monitoring (11). Suryantoro hanya menerapkan pendekatan forensik jaringan dan metode deteksi untuk mengetahui efektivitas kinerja wazuh SIEM untuk serangan port 80 pada web server, penerapan SIEM Wazuh mampu membantu petugas keamanan mengamankan aset IT perusahaan (12). Younus dan Alanezi mengintegrasikan teknik Wazuh dan IDS untuk meningkatkan deteksi terbatas hanya pada serangan DoS. Hasil dari penerapan eksperimental menghasilkan sistem deteksi dan berhasil dalam memitigasi serangan siber (13). Praptodiyono, dkk hanya mengusulkan strategi hybrid dengan menggabungkan Suricata dan pfSense untuk mengatasi serangan DDoS. Hasil penelitian menunjukkan nilai throughput sebesar 1,08 %, jumlah paket yang dikirim sebesar 57,32 %. Nilai delay 10.18 ms, dan nilai jitter menurun sebesar 88.99 %, Penggunaan CPU sebesar 14,7% (14). Pada penelitian yang dilakukan Zebari dkk, hanya fokus pada serangan HTTP pada IIS window server dan apache ubuntu server dengan serangan TCP Syn flood (15). Penelitian yang dilakukan Oktivasari, dkk hanya difokuskan pada layanan web server dengan teknik mitigasi IPTables (16). Pada penelitian ini, dibandingkan dengan penelitian sebelumnya, untuk mengatasi kompleksitas ancaman dan serangan siber, memerlukan pendekatan yang lebih baik dalam meningkatkan ketahanan siber yang lebih holistik dan terintegrasi, peneliti mengembangkan beberapa pendekatan dan teknik, yaitu:

1. Sistem pendekatan hybrid, dengan menggabungkan teknik Wazuh XDR, SIEM, Firewall IPTable dan active response (XDR) wazuh untuk meningkatkan sistem monitoring Security Operation Center (SOC), deteksi dan respon terhadap ancaman.
2. Sistem multiple attack vector, dengan melakukan berbagai jenis serangan pada lingkungan infrastruktur jaringan pada perangkat router dan server.

3. Penelitian difokuskan pada kerentanan perangkat router dan server yang dimodelkan
4. Melakukan evaluasi pengukuran performansi sumber daya Network Capacity, CPU dan memori sebelum dan setelah terjadi serangan yang diemulasikan.

4. Peta Jalan Penelitian

Peta jalan penelitian diuraikan sebagai berikut:

1. Tahapan yang telah dicapai pada penelitian yaitu, peneliti dan tim peneliti, telah melakukan studi literature untuk mengetahui dan memahami, ancaman, kerentanan dan resiko infrastruktur jaringan perangkat router dan server, sistem deteksi intrusi, dan teknologi yang terkait sistem deteksi, orkestrasi keamanan perangkat jaringan, respon, mitigasi dengan teknik Wazuh active response XDR dan iptables ipset firewall.
2. Tahapan yang akan dilakukan dalam jangka waktu penelitian yaitu dengan menggunakan pendekatan PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) Cisco life cycle.
3. Tahapan yang akan direncakan pada hasil akhir penelitian yaitu, melakukan penyusunan laporan akhir dan publikasi penelitian.

Berikut merupakan tabel peta jalan penelitian 5 tahun mendatang

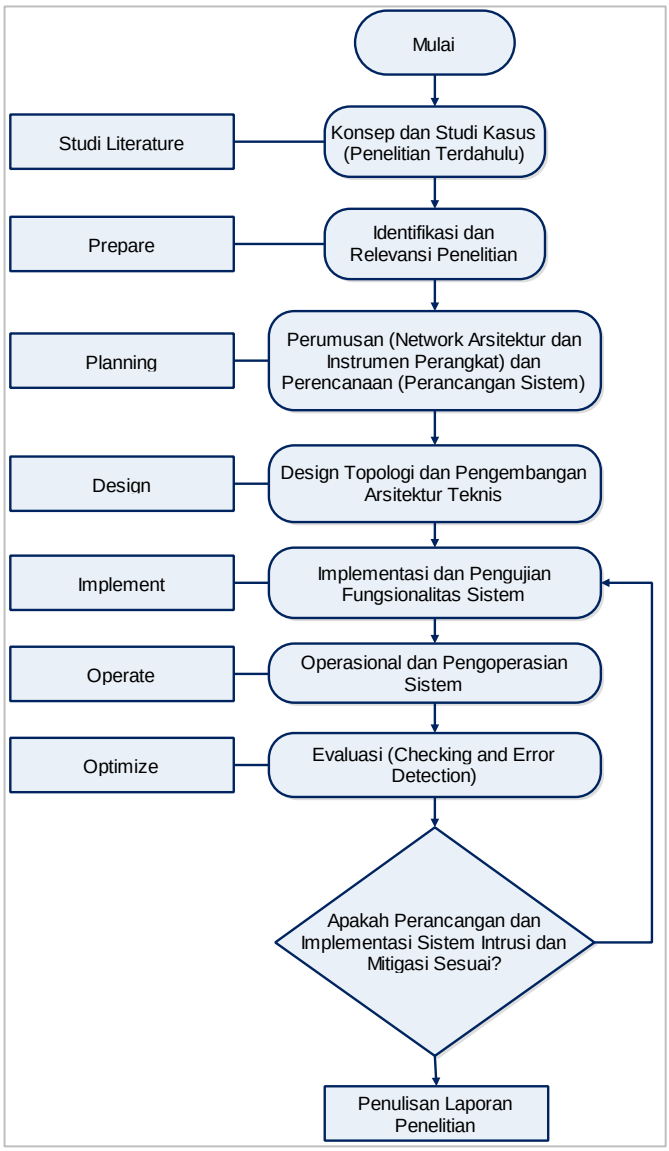
Tahun	Fokus Penelitian	Kegiatan Utama
1	Evaluasi Teknologi yang Digunakan	- Evaluasi efektivitas XDR dan integrasi dengan SIEM
2	Pengembangan Sistem Deteksi Intrusi	- Pengembangan algoritma deteksi serangan
3	Implementasi dan Uji Coba Lanjutan	- Implementasi pada lingkungan jaringan yang lebih kompleks dan coba terhadap serangan yang lebih canggih
4	Optimalisasi dan Skalabilitas	- Optimalisasi performa sistem dan Skalabilitas untuk lingkungan jaringan yang besar
5	Penyebaran dan Adopsi	- Pelatihan Pengguna

BAB II

METODE

2. Metode Penelitian

Metode dan tahapan penelitian yang akan dilakukan menggunakan pendekatan PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) Cisco life cycle yang ditunjukkan seperti pada Gambar 1.



Gambar 2.1 Metode dan Tahapan Penelitian

Studi literature, perumusan masalah penelitian dan tujuan penelitian sudah dilakukan sebagian selama proses penyusunan proposal penelitian ini. Pada penelitian dengan melibatkan penelusuran yang sesuai dan komprehensif tentang topik, relevansi dan poin penting yang akan dilakukan yaitu sistem deteksi intrusi dan metode dari enelitian terkait mengenai Wazuh *active response* XDR, SIEM, kerentanan, serangan, respon dan serangan infrastruktur jaringan perangkat router dan server. Tahapan penelitian dengan menggunakan pendekatan PPDIOO Cisco *life cycle* untuk diuraikan sebagai berikut:

2.1.Studi Literature

A. Proses
    1. Melakukan analisis untuk kerentanan yang ada pada perangkat router dan server.
    2. Melakukan literature untuk serangan reconnaissance attack, access attack dan DoS attack
    3. Meneliti untuk penerapan integrasi yang sudah ada mengenai SIEM, iptables ipset dan active response (XDR) wazuh.
    4. Mempelajari hardware dan software untuk membangun dan mengimplementasikan sistem intrusi dan mitigasi.

B. Luaran
    1. Membuat dokumen untuk merangkum data teknis kerentanan perangkat router dan server, teknik serangan, teknik mitigasi dengan framework firewall iptables ipset dan active response (XDR) wazuh.

C. Indikator Capaian

Indikator capaian pada tahap ini membuat dokumen modul yang siap digunakan untuk mendukung penelitian, dan mengetahui dan memahami untuk kebutuhan perangkat hardware dan software untuk Implementasi siap digunakan.

2.1.1. Prepare (Persiapan)

Tahapan prepare dilakukan dengan menerapkan dan mendata serta meneliti perkembangan pada bidang penelitian yang akan diterapkan. Penelitian ini akan

dilakukan dari Bulan Mei - Agustus 2024 pada Infrastruktur Jaringan di perusahaan AJN yang terdapat virtualisasi perangkat router dan server dengan pemodelan topologi yang akan diterapkan. bagaimana kebutuhan untuk infrastruktur jaringan pada perangkat router dan virtualisasi server yang akan diselidiki, jenis serangan dan penerapan mitigasi dari penelitian: Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall.

A. Proses
    1. Persiapan waktu dan tempat penelitian
    2. Analisis kebutuhan untuk infrastruktur jaringan pada perangkat router dan virtualisasi server yang akan diselidiki, jenis serangan dan penerapan mitigasi.
    3. Membuat rencana untuk RAB, alokasi waktu penelitian
B. Luaran
    1. Penelitian ini akan dilakukan dari Bulan Mei - Agustus 2024 di AJN Solusindo, Pada penelitian ini kami melakukan emulasi dan implementasi dengan melakukan eksperimen dan menguji strategi mitigasi tanpa mengganggu operasi jaringan yang sebenarnya
    2. Cakupan sumber daya untuk kebutuhan penelitian.
C. Indikator Capaian
    1. Dokumen dan modul untuk kegiatan penelitian
    2. Dokumen rencana kerja (jadwal, waktu dan tahapan)

2.1.2. Planning (Perencanaan)

Tahap planning dilakukan untuk mengindentifikasi kebutuhan teknis untuk implementasi (perangkat keras, perangkat lunak dan perangkat VMWare dan proxmox hypervisor, router MikroTik, vServer, VPS Server, Switch, PC/Laptop, Kabel LAN dan konektivitas internet).

A. Proses
    1. Melakukan identifikasi kebutuhan teknis untuk implementasi (perangkat keras, perangkat lunak dan perangkat VMWare dan proxmox hypervisor,

router MikroTik, vServer, VPS Server, Switch, PC/Laptop, Kabel LAN dan konektivitas internet).

2. Melakukan perancangan arsitektur dan topologi (*Physic* dan *logic*) sistem.
3. Menentukan penjadwalan untuk kegiatan implementasi dan pengujian sistem.

B. Luaran

1. Dokumen spesifikasi teknis siap digunakan.
2. Rancangan arsitektur sistem (diagram visual untuk integrasi komponen)
3. Langkah dan tahapan yang dilakukan selama kegiatan implementasi

C. Indikator Capaian

1. Penyelesaian untuk dokumen spesifikasi teknis penelitian.
2. Dokumen perancangan arsitektur sistem
3. Dokumen Draft tahap implementasi

2.1.3. Design

Setelah tahap persiapan (*prepare*) dan perencanaan (*planning*), tahap selanjutnya adalah tahap desain (design) infrastruktur jaringan dan komponen yang dimodelkan. Dalam tahap desain ini, fokus utama adalah merancang arsitektur detail topologi jaringan logis (*logical*), dan konfigurasi teknis untuk implementasi sistem. Tahap desain untuk penerapan sistem melibatkan penyusunan spesifikasi teknis dan arsitektur sistem yang akan digunakan untuk mengimplementasikan solusi deteksi intrusi dan mitigasi kerentanan, termasuk perancangan topologi jaringan secara logis (*logical*) dan pengaturan komunikasi antar komponen dan alokasi IP Address.

A. Proses

1. Mendesain topologi dan konektivitas *physic* jaringan.
2. Mendesain topologi dan konektivitas *logic* jaringan.

B. Luaran

Dokumen desain sistem yang terhubung dan berinteraksi (perangkat keras, perangkat lunak dan perangkat VMWare Desktop hypervisor, router, server,

VPS Server, Switch, Access Point, PC/Laptop, Kabel LAN dan konektivitas internet)

C. Indikator Capaian

Topologi jaringan untuk konektivitas perangkat telah disusun.

2.1.4. Implementation (Implementasi)

Tahap implementasi dalam penelitian ini melibatkan instalasi, konfigurasi dan pembuatan script firewall pada lingkungan pengujian untuk memastikan bahwa sistem firewall dan active responses bekerja sesuai dengan yang diharapkan. Proses ini meliputi instalasi dan konfigurasi perangkat keras, sistem operasi ubuntu server, hypervisor proxmox dan vmware, serta framework active responses menggunakan script python. Pengujian yang dilakukan dengan skenario serangan nyata menggunakan tools di kali linux, untuk menguji serangan reconnaissance attack, access attack dan DoS attack. Peneliti akan mengukur efektivitas sistem dalam mendeteksi, merespons, dan memitigasi serangan pada firewall dengan monitoring pada wazuh dashboard. Hasil dari tahap implementasi ini selanjutnya akan memberikan data empiris yang dapat digunakan peneliti untuk mengevaluasi efektivitas dan kinerja solusi yang diusulkan dalam penelitian.

A. Proses

1. Melakukan konfigurasi infrastruktur (hardware dan software)
2. Mempersiapkan VMWare Desktop Hypervisor, Sistem Operasi, Web Server
3. Menetapkan dan menentukan untuk arsitektur sistem (integrasi Wazuh Agent, Wazuh Manager, SIEM, framework firewall *iptables ipset* dan active response (XDR) wazuh
4. Melakukan konfigurasi VPS Server (Wazuh Manger dan VPS Ubuntu Server)
5. Melakukan konfigurasi integrasi sistem (Wazuh agent, Wazuh Server Manager (*Indexer*, Server dan *Dashboard*).

6. Menentukan jenis serangan yang akan dilakukan pada perangkat router dan server
7. Melakukan dan membuat *policy* dan *rule* mitigasi serangan

B. Luaran
1. Sistem Perangkat hardware dan software terkonfigurasi
2. Perangkat Hardware dan Software siap digunakan
3. Konektivitas physical Wazuh Agent, Wazuh Manager di IDCloudhost, SIEM, dan framework firewall *iptables ipset* dan *active response* (XDR) wazuh
4. VPS Server siap digunakan untuk SOC
5. Pengoperasian sistem konfigurasi *policy* dan *rule* diterapkan
6. Hasil Pengujian serangan attacker end point Hping3, Hydra, Network Mapping (Nmap) dengan serangan DoS, Brute Force, Port scanning

C. Indikator Capaian
3. Pengujian dan Emulasi

2.1.5. Operate (Operasional)

Tahap operasional penelitian ini adalah tahap dimana sistem yang telah diimplementasikan dan dirancang akan digunakan dan diuji dengan kondisi nyata. Fokus pada tahap ini pengujian dilakukan dengan serangan terhadap sistem pada wazuh agent untuk memastikan bahwa semua pemodelah dan mekanisme pertahanan yang telah diimplementasikan pada infrastruktur jariangan dapat berfungsi dan bekerja, termasuk teknik serangan yang akan dilakukan adalah reconnaissance attack (Nmap), access attack (brute force), dan DoS attack.

A. Proses
1. Melakukan pelaksanaan implementasi untuk sistem Sistem Deteksi Intrusi Hybrid Wazuh XDR, SIEM, dan Firewall pada Kerentanan Infrastruktur Jaringan Perangkat Router dan Server
2. Melakukan pengujian sistem jaringan dan monitoring (SOC) secara berkala untuk mendeteksi dan merespon anomali dan serangan

3. Melakukan pengujian teknik mitigasi serangan dengan *active response* (XDR) wazuh

B. Luaran
   1. Sistem yang dibangun dapat beroperasi sesuai rencana dan tujuan yang telah ditetapkan
   2. Pengujian fungsionalitas yang dilakukan berhasil

C. Indikator Capaian
   1. Penilaian terhadap tingkat kesiapan sistem saat dioperasionalkan
   2. Evaluasi hasil pengujian

2.1.6. Optimize

Tahap optimalisasi penelitian ini berfokus pada peningkatan efektivitas dan efisiensi sistem keamanan dari infrastruktur jaringan yang telah diimplementasikan. Adapaun langkah yang dilakukan meliputi dua aspek utama yaitu konfigurasi dan evaluasi optimasi firewall serta *active responses* wazuh XDR, dan evaluasi performa sumber daya CPU dan memory pada perangkat server dan router sebelum dan setelah terjadi serangan.

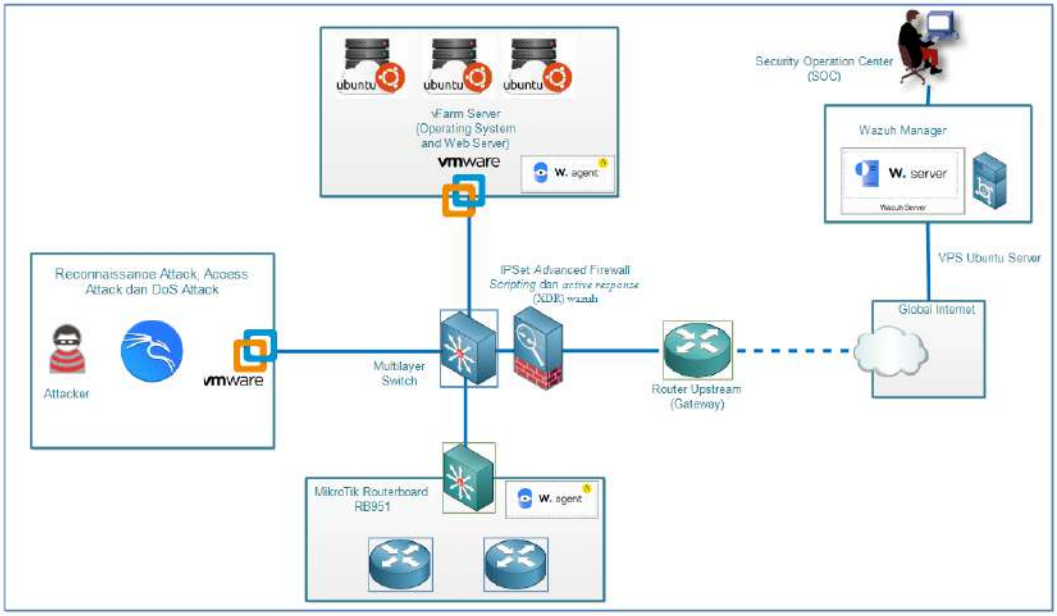
A. Proses
   1. Melakukan evaluasi kinerja sistem hybrid intrusi dan teknik mitigasi (lalu lintas jaringan, sistem deteksi dan respon
   2. Melakukan evaluasi kinerja sistem hybrid intrusi dan teknik mitigasi (lalu lintas jaringan, sistem deteksi dan respon
   3. Melakukan dokumentasi optimasi perancangan sistem dan mitigasi serangan

B. Luaran
   1. Meningkatkan kinerja sistem yang sudah dioptimalkan untuk kinerja sistem yang maksimal
   2. Melakukan perbaikan untuk sistem dan teknik mitigasi yang sudah diimplementasikan
   3. Dokumentasi draft modul optimasi sistem *hybrid* intrusi dan mitigasi serangan.

C. Indikator Capaian

1. Peningkatan kinerja sistem untuk melakukan deteksi, merespon dan memitigasi dari serangan *malicious* source IP Address.

Perancangan Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall, diilustrasikan pada Gambar 2



Gambar 2.2. Perancangan Sistem Infrastruktur Jaringan Perangkat Router dan Server

BAB III

HASIL PELAKSANAAN PENELITIAN

3.1. Tahap Prepare (Identifikasi Penelitian)

Tahapan prepare dilakukan dengan menerapkan dan mendata serta meneliti perkembangan pada bidang penelitian yang akan diterapkan. Penelitian ini akan dilakukan dari Bulan Mei - Agusuts 2024 pada Infrastruktur Jaringan perusahaan AJN yang terdapat virtualisasi perangkat router dan server dengan pemodelan topologi yang akan diterapkan. Kegiatan prepare dilakukan untuk menilai seberapa baik teknologi saat ini dengan terintegrasi dengan seluruh siklus operasi manajemen jaringan, berupa desain, penyebaran, dan pemantauan terkait pendeteksian dan pencegahan system. Dalam tahap persiapan penelitian yang akan dilakukan pada Sistem Deteksi Intrusi Hibrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan iptables ipset, berikut adalah beberapa terkait kebutuhan infrastruktur jaringan: 1.1.1. Kebutuhan Infrastruktur Jaringan

1. Router CCR1036-8G-2S

   Router ini digunakan dan berfungsi sebagai gateway utama yang terhubung langsung ke internet.

2. Router RB951Ui-2HnD

   Router ini digunakan dan berfungsi untuk simulasi serangan dari Kali Linux.

3. Server VM VMWare dan Proxmox Hypervisor

   Berfungsi untuk menyediakan lingkungan virtualisasi, termasuk sebagai korban serangan yang akan dinstall server web Apache, Ubuntu Server, Kali Linux, dan *attacker endpoint* Hping3, Hydra Parrot OS dan Nmap sebagai host untuk agent Wazuh.

4. vServer Cloud Public

   Digunakan dan berfungsi sebagai server tempat meng-host Wazuh Manager, yang bertanggung jawab untuk mengelola dan menganalisis data dari Wazuh Agent yang terdistribusi.

Identifikasi kebutuhan perangkat infrastruktur diatas menentukan kebutuhan spesifik untuk infrastruktur jaringan, seperti router dan perangkat server.

Mengkonfigurasi perangkat keras dan perangkat lunak sesuai dengan peran masing-masing, router difungsikan sebagai gateway internet, Proxmox dan VMware hypervisor untuk lingkungan virtual sebagai *victim* (*agent*), serta vServer IDCloud untuk Wazuh Manager, dengan melakukan pengujian untuk memastikan bahwa setiap komponen infrastruktur berfungsi dengan baik dan sesuai dengan ekspektasi, termasuk pengujian keamanan untuk mengevaluasi keefektifan solusi deteksi intrusi *hybrid* dan mitigasi kerentanan yang diimplementasikan.

3.1.1. Jenis Serangan dan Implementasi Mitigasi

Jenis serangan dibagai menjadi 3 (tiga) kategori yaitu:

1. *Reconnaissance Attack*

   Reconnaissance attack yang dilakukan merupakan tahap pemindaian (scanning) untuk mendeteksi kerentanan sistem operasi Ubuntu Server 20.04.6 LTS yang akan diinstal wazuh agent. Teknik serangan dilakukan dengan pemindaian terhadap victim (wazuh agent) menggunakan Nmap dari Kali Linux untuk mengidentifikasi layanan yang berjalan pada sistem operasi target.

2. *Access Attack*

   Serangan access attack bertujuan untuk mendapatkan akses kredensial tidak sah ke sistem operasi Ubuntu Server 20.04.6 LTS (wazuh agent). Serangan brute force termasuk dalam kategori yang akan diimplementasikan, di mana penyerang mencoba berbagai kombinasi kredensial username dan password untuk mendapatkan akses, menggunakan *wordlist* rockyou.txt. Teknik yang digunakan untuk melakukan attack emulation adalah hydra parrot OS.

3. *Denial of Service* (DoS) *Attack*

   Serangan DoS dimodelkan untuk membuat layanan dan jaringan Web Server Apache pada Ubuntu Server 20.04.6 LTS (*wazuh agent*) tidak dapat diakses dengan membanjiri sistem dengan lalu lintas dengan mengeksploitasi kerentanan tertentu untuk menyebabkan crash. Teknik yang digunakan untuk melakukan *attack emulation* adalah Hping3.

Tahap Mitigasi dilakukan dengan 3 (tiga) Teknik sebagai berikut:

1. Penerapan teknik *Detection and Response solutions* (XDR) – Mengintegrasikan Solusi XDR untuk respon cepat terhadap ancaman yang dimodelkan dari serangan *Brute Force*.
2. Penerapan teknik *Framework* Hydra Parrot OS – mengotomisasi solusi firewall untuk respon cepat terhadap ancaman yang dimodelkan dari serangan Brute Force untuk membuat aturan (*rule*) dari *blocking source* IP Address.
3. Penerapan *iptables ipset* untuk membuat *policy deny* berdasarkan malicious *source* IP *address*.

3.1.2. Evaluasi Hasil

Dengan melakukan evaluasi dari implementasi, melibatkan pengukuran dari performansi sumber daya *network capacity*, CPU dan memori. Penggunaan CPU dan memori akan dilakukan komparasi sebelum dan setelah terjadi serangan. Evaluasi ini juga mencakup analisis efektivitas mitigasi serangan seperti DDoS dan *brute force*, menilai seberapa cepat dan efektif sistem XDR dan firewall dalam mendeteksi dan merespons ancaman. Kesimpulan dari evaluasi ini akan memberikan gambaran tentang kinerja dan keamanan jaringan serta rekomendasi peningkatan lebih lanjut untuk memastikan perlindungan optimal terhadap berbagai ancaman.

3.2. Tahap Planning (Formulasi Arsitektur Jaringan dan Desain Sistem)

Tahap planning dilakukan untuk mengindentifikasi kebutuhan teknis untuk implementasi (perangkat keras, perangkat lunak dan perangkat VMWare dan proxmox hypervisor, router MikroTik, vServer, VPS Server, Switch, PC/Laptop, Kabel LAN dan konektivitas internet).

3.2.1. Instrumentasi Kebutuhan Perangkat Keras (Hardware) dan Perangkat Lunak (Software)

Kebutuhan perangkat keras yang digunakan untuk penelitian melibatkan penggunaan berbagai perangkat keras yang penting untuk infrastruktur jaringan yang akan diimplementasikan dengan kategori yang aman dan efisien. Server HPE ProLiant dengan spesifikasi seperti pada Tabel 3.1. akan digunakan sebagai

platform virtual machine (VM) Proxmox dan VMware *hypervisor* untuk menjalankan berbagai VM Agent Wazuh yang akan menjadi target serangan. Router MikroTik CCR1036-8G-2S berfungsi sebagai *gateway* dan perutean antara perangkat pada infrastruktur jaringan yang dimodelkan. MikroTik RB951Ui-2HND berfungsi untuk emulasi serangan dari Kali Linux, sedangkan switch TL-SG2210P berfungsi untuk menghubungkan semua perangkat dalam infrastruktur jaringan. Server VPS IDCloud berfungsi untuk meng-host wazuh manager atau server yang bertugas memonitoring, menganalisis dan *active response* data dari wazuh agent yang terinstal pada perangkaat virtual machine korban (*victims*). Semua perangkat ini diatur untuk mendukung emulasi serangan dan pengujian sistem deteksi intrusi serta mitigasi kerentanan, memastikan setiap komponen berfungsi secara optimal untuk menciptakan infrastruktur jaringan yang *responsive* dan aman terhadap ancaman. Instrumentasi *hardware* yang digunakan dalam penelitian ini diuraikan pada tabel 3.1 sebagai berikut.

Tabel 3.1. Instrumentasi Kebutuhan Perangkat Keras (*Hardware*)

SPESIFIKASI PERANGKAT KERAS (*HARDWARE*)					
Deskripsi Product Hardware	**RAM**	**Storage**	**CPU**	**Interface**	Operating System
HPE ProLiant DL360 Gen10 Server	64 GB	1 TB	Intel® Xeon® Scalable 8100	Gigabit Ethernet	Proxmox Hypervisor
HPE ProLiant DL360 Gen10 Server	64 GB	1 TB	Intel® Xeon® Scalable 8100	Gigabit Ethernet	VMWare Hypervisor
MikroTik CCR1036	4 GB	1 GB	Tilera Tile-Gx36 1.2GHz 36 Cores	Gigabit Ethernet	MikroTik OS
MikroTik RB951	128 MB	128 MB	AR9344 600MHz	Gigabit Ethernet	MikroTik OS
Switch TL-SG2210P	-	-	-	Gigabit Ethernet	TP-Link OS
STP Cable Cat 6	-	-	-	-	
Server VPS	8 GB	100 GB	KVM	Gigabit Ethernet	Ubuntu Server 20.04

Kebutuhan perangkat lunak yang digunakan untuk penelitian melibatkan penggunaan berbagai perangkat lunak sistem operasi dan framework tool yang penting untuk infrastruktur jaringan. dengan spesifikasi seperti pada Tabel 3.2. Penerapan pada penelitian ini menggunakan berbagai perangkat lunak dan sistem operasi untuk membangun, menguji, dan memonitoring infrastruktur jaringan serta melakukan serangan emulasi dan simulasi. VM proxmox dan vmware *hypervisor* digunakan sebagai platform virtualisasi untuk menjalankan VM yang akan menjadi target serangan. Ubuntu server LTS pada cloud berfungsi sebagai wazuh manager untuk memantau dan menganalisis data dari Wazuh Agent, yang juga berjalan pada Ubuntu Server LTS pada VM yang menjadi korban serangan dengan menggunakan *private address*. Active response (XDR) wazuh dan IPTable berfungsi sebagai pencegahan intrusi malicious IP address dengan memblokir IP berdasarkan log. Router berbasis cloud (CHR) digunakan sebagai Wazuh Agent untuk memantau aktivitas jaringan dan mengirimkan laporan ke wazuh manager yang akan diinstall dan dikonfigurasi pada VMWare hypervisor. Selanjutnya untuk simulasi dan emulasi serangan, beberapa alat digunakan yaitu Slowloris untuk serangan DoS dari Kali Linux, Hydra untuk serangan *brute force*, serta kali linux sebagai platform yang menjadi pengujian penetrasi. Network *mapper* (Nmap) digunakan untuk pemindaian (*scanning*) untuk perangkat ubuntu server yang sudah terinstall sistem operasi dan layanan seperti *apache webserver*, tujuannya adalah untuk mengidentifikasi perangkat dan *services* yang berjalan agar dapat dieksploitasi. Pemodelan untuk semua perangkat lunak ini bekerja untuk menciptakan lingkungan pengujian yang realistis, dengan memastikan penerapan sistem deteksi intrusi dan mitigasi dapat berfungsi dalam menghadapi berbagai jenis serangan.

Tabel 3.2. Instrumentasi Kebutuhan Perangkat Lunak (*Software*)

SPESIFIKASI PERANGKAT LUNAK (SOFTWARE)	
Deskripsi Product Hardware	**Kategori**
Proxmox VE 6.4 ISO	Virtual Machine
VMware Desktop Hypervisors	Virtual Machine

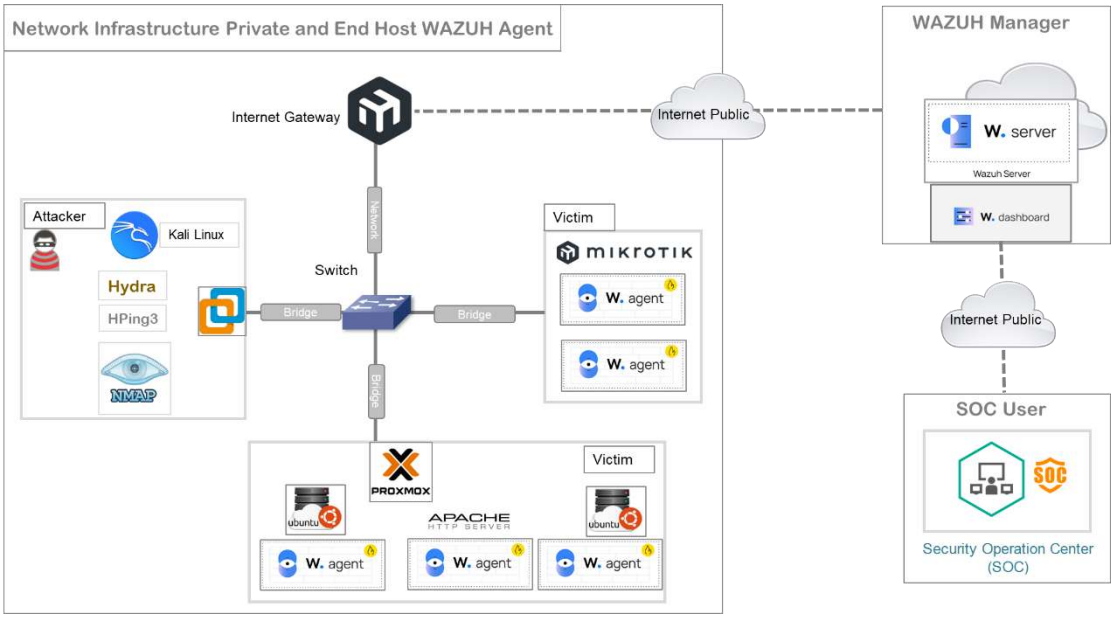
Routers Tile: - System - Routing - DHCP - Advanced Tool - Security	Router Gateway
RouterOS Mipsbe: - System - Routing - DHCP - Advanced Tool - Security	Router Agent (*Victim*)
Ubuntu Server 20.04 LTS	Wazuh Manager
Ubuntu Server 20.04 LTS	Wazuh Agent (*Victim*)
XDR *active response*	Stateless Firewall
IPTable Framework	Firewall
Cloud Host Router	Wazuh Agent (*Victim*)
Slowloris	Attacker
Hydra	Attacker
Kali Linux	Attacker
Network Mapper (NMAP)	Attacker

3.2.2. Perancangan Arsitektur Topologi Physic pada lingkungan Infrastruktur Jaringan

Gambar 3.1 menunjukkan arsitektur topologi jaringan yang digunakan dalam penelitian, topologi yang dimodelkan terdiri dari beberapa komponen utama, baik perangkat dan konektivitas yang bekerjasama untuk menguji dan memantau infrastruktur jaringan yang dimodelkan. Internet gateway router menghubungkan jaringan internal dengan internet public (jaringan internet), untuk interkoneksi wazuh agent dan wazuh manager. Sementara *Firewall* digunakan untuk menambahkan rule dan policy berdasarkan *policy permit, drop* berdasarkan malicious source IP Address. Attacker yang menggunakan kali linux OS dengan Slowloris (DoS), Hydra (*brute force*), dan NMAP (*scanning* jaringan) untuk mengemulasikan serangan terhadap jaringan. Target serangan (*victim*) adalah sistem operasi virtual yang diinstall di VM proxmox, seperti Apache (web server) serta router MikroTik dan CHR. Wazuh agent di install pada semua vServer untuk

memantau aktivitas dan mengirim data ke Wazuh Manager. Wazuh Manager, yang diinstal pada server VPS, mengumpulkan dan menganalisis data dari masing-masing wazuh agent dan pada wazuh manager juga diterapkan framework firewall untuk mengelola respon aktif terhadap serangan yang dimodelkan. Semua dataset serangan dan pencegahan akan dipantau melalui Wazuh dashboard, yang menyediakan antarmuka grafis untuk analisis lebih lanjut.

Seluruh sistem ini diawasi oleh Security Operation Center (SOC), yang menggunakan data dari wazuh manager dan dashboard untuk mendeteksi, menganalisis, dan merespon insiden keamanan secara *real-time*. Penerapan pada penelitian ini memungkinkan simulasi serangan dan pengujian teknik deteksi intrusi serta mitigasi kerentanan, memastikan bahwa infrastruktur jaringan aman dan responsif terhadap berbagai jenis ancaman.



Gambar 3.1. Perancangan Arsitektur Topologi Physic pada lingkungan Infrastruktur Jaringan

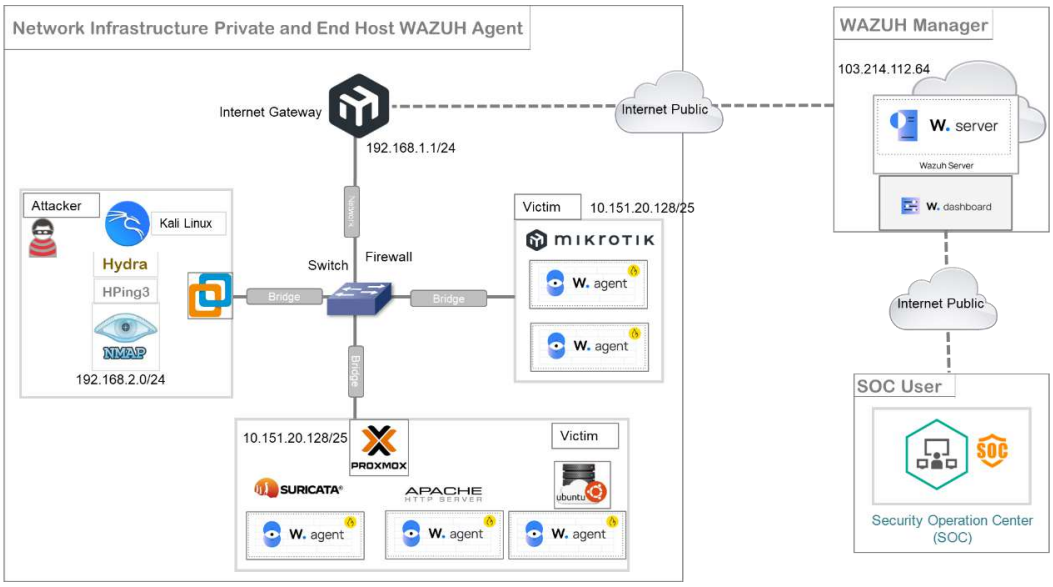
3.3.Tahap Desain (Pengembangan Arsitektur Teknis)

Setelah tahap persiapan (*prepare*) dan perencanaan (planning), tahap selanjutnya adalah tahap desain (*design*) infrastruktur jaringan dan komponen yang dimodelkan. Dalam tahap desain ini, fokus utama adalah merancang arsitektur detail topologi jaringan logis (*logical*), dan konfigurasi teknis untuk implementasi

sistem. Tahap desain untuk penerapan sistem melibatkan penyusunan spesifikasi teknis dan arsitektur sistem yang akan digunakan untuk mengimplementasikan solusi deteksi intrusi dan mitigasi kerentanan, termasuk perancangan topologi jaringan secara logis (*logical*) dan pengaturan komunikasi antar komponen dan alokasi IP Address.

3.3.1. Konfigurasi Topologi

Gambar 3.2 merupakan tahap penyusunan arsitektur dan topologi jaringan. Langkah pertama adalah merancang arsitektur sistem yang mencakup semua komponen utama seperti router, switch, server fisik dan virtual, serta *endpoint* penyerang (*attacker*) sistem operasi, layanan dan wazuh agent yang akan dipantau.



Gambar 3.2 Perancangan Arsitektur Topologi *Logical* pada lingkungan Infrastruktur Jaringan

Visualisasi topologi *logical* jaringan menggambarkan bagaimana komponen perangkat akan terhubung. Pada arsitektur topologi ini, HPE ProLiant digunakan sebagai node VM utama dengan konfigurasi Proxmox dan VMware *Hypervisor* untuk menjalankan berbagai mesin virtual. Router MikroTik CCR1036 berfungsi sebagai gateway internet, sementara MikroTik RB951Ui-2HND digunakan untuk pengujian serangan. Semua perangkat dihubungkan melalui switch TP-Link TL-SG2210P.

3.3.2. Konfigurasi IP Address

Tabel 3.3 merupakan komponen perangkat yang dikonfigurasi dengan IP address yang spesifik untuk memastikan komunikasi yang optimal berdasarkan kebutuhan topologi dengan memastikan bahwa setiap perangkat dapat saling berkomunikasi dengan aman melalui gateway yang sudah ditentukan. Konfigurasi IP address untuk perangkat dalam penelitian ini sangat penting untuk memastikan komunikasi yang efisien dan aman di seluruh jaringan. Gateway router menggunakan alokasi IP Address 192.168.1.2/24 untuk menghubungkan jaringan private infrastruktur yang dimodelkan ke internet. Proxmox Hypervisor, active response (XDR) wazuh, dan VM ubuntu server (wazuh agent) menggunakan subnet 10.151.20.128/25 dan gateway 10.151.20.129. Kali linux (Hydra, Hping3 dan NMAP), yang digunakan untuk emulasi dan simulasi serangan dialokasikan dengan subnet 192.168.2.0/24 untuk menguji respon sistem terhadap ancaman penyerang (attacker). Terdapat dua (2) router MikroTik yang bertindak sebagai perangkat korban berada di subnet (10.151.20.128/29), yang bertujuan untuk menguji berbagai skenario serangan.

Tabel 3.3. Komponen Konfigurasi IP Address

Komponen IP Address Devices vServer dan Router				
Devices	**IP Address**	**Subnet Mask**	**Iface**	**Gateway**
Router Gateway	192.168.1.2	255.255.255.0	Ether3	192.168.1.2
Proxmox Hypervisor	10.151.20.230	255.255.255.128	Ether1	10.151.20.129
IPTables Firewall	10.151.20.171	255.255.255.128	ens18	10.151.20.129
Active response (XDR) wazuh	103.214.112.64	255.255.255.255	ens18	N/A
Hydra Hping3 dan NMAP	192.168.2.39	255.255.255.0		192.168.2.1
Ubuntu Server (Brute Force)	10.151.20.250	255.255.255.128	ens18	10.151.20.129
Ubuntu Server (Hping3)	10.151.20.251	255.255.255.128	ens18	10.151.20.129
Ubuntu Server (NMAP)	10.151.20.252	255.255.255.128	ens18	10.151.20.129
Router MikroTik (Victim)	10.151.20.238	255.255.255.128	Ether2	10.151.20.129

Router MikroTik (Victim)	10.151.20.239	255.255.255.128	Ether2	10.151.20.129

3.3.3. Node Proxmox *Hypervisor* Wazuh *Agent*

Penerapan dan konfigurasi untuk node wazuh agent pada VM proxmox *hypervisor* diuraikan pada tabel 3.4. Berikut adalah konfigurasi VM untuk node wazuh *agent* yang dikonfigurasi dengan ubuntu server:

Table 3.4. Node Proxmox Hypervisor Wazuh Agent

Proxmox Hypervisor Virtual Machine Wazuh Agent			
Node	**AJN Node**		
Name	Wazuh Agent-1	Wazuh Agent-2	Wazuh Agent-3
VM ID	120	121	122
Storage	Local-VM	Local-VM	Local-VM
ISO Image	Ubuntu Live Server 20.04	Ubuntu Live Server 20.04	Ubuntu Live Server 20.04
SCSI Controller	VirtIO SCSI	VirtIO SCSI	VirtIO SCSI
Hard Disk	80 GB	80 GB	80 GB
CPU (Core)	6	6	6
Memory	8192	8192	8192
Bridge	VMBR1	VMBR1	VMBR1

Uraian tabel 3.4 untuk konfigurasi virtual node wazuh agent pada Proxmox Hypervisor

a. **Node** - Node berfungsi untuk host fisik dalam cluster proxmox hypervisor. Setiap wazuh agent ditempatkan pada node yang sama: `AJN Node` untuk keseragaman dalam pengujian dan pengelolaan sumber daya virtual sistem operasi yang akan diinstall.
b. **Name -** `Wazuh Agent-1, Wazuh Agent-2, Wazuh Agent-3` merupakan penamaan untuk mengidentifikasi untuk masing-masing VM yang mengoperasionalkan wazuh agent.
c. **VM ID**: masing-masing wazuh agent akan memiliki ID unik yaitu (120, 121, 122) yang berfungsi dan digunakan untuk mengidentifikasi mesin virtual di dalam proxmox hypervisor.

d. **Storage**: Storage `Local-VM` mengindikasikan bahwa disk (*hard disk*) virtual dari setiap wazuh agent disimpan secara lokal pada node tersebut.
e. **ISO Image**: ISO image Ubuntu Live Server 20.04 akan digunakan untuk instalasi sistem operasi untuk setiap Wazuh Agent dan pemilihan ubuntu server karena memiliki kompatibilitas dan stabilitas dengan wazuh.
f. **SCSI Controller**: VirtIO SCSI akan digunakan untuk controller disk virtual.
g. **Hard Disk**: masing-masing wazuh agent dialokasikan 80 GB hard disk. Kapasitas HD digunakan untuk mengakomodasi sistem operasi dan wazuh Agent serta dataset yang dikumpulkan untuk analisis.
h. **CPU (Core)**: Setiap wazuh agent dialokasikan 6 core vCPU, alokasi vCPU ini untuk memastikan bahwa setiap VM memiliki cukup kekuatan pemrosesan untuk menangani tugas-tugas deteksi intrusi dan pemantauan secara efektif.
i. **Memory**: masing-masing wazuh agent dialokasikan 8 GB. Alokasi memori ini diperlukan untuk menjalankan aplikasi wazuh agent dan proses-proses lain yang dijalankan pada wazuh agent dan sistem operasi.
j. **Bridge**: Interface jaringan `vmbr1` menghubungkan setiap Wazuh *agent* ke jaringan virtual yang disediakan oleh Proxmox, dengan infrastruktur jaringan. Bridge ini memungkinkan mesin virtual untuk berkomunikasi dengan perangkat lain dalam jaringan, termasuk attacker, wazuh manager dan perangkat korban (*victims*).

Konfigurasi node VM wazuh agent yang dimodelkan berguna memastikan bahwa setiap wazuh agent memiliki sumber daya yang cukup untuk beroperasi secara optimal, baik untuk pemrosesan data, penyimpanan, dan konektivitas jaringan.

3.3.4. Node VMWare Hypervisor Attacker

Instalasi dan konfigurasi vmware desktop hypervisor pada penelitian digunakan untuk menginstal dan mengkonfigurasi kali linux, dan menjalankan teknik penyerangan menggunakan Hydra, Hping3, dan Network Mapping (NMAP).

Instalasi dan konfigurasi kali linux di mesin VMware dengan mengatur dan mengalokasikan seperti vCPU, memori, dan hard disk (SCSCI), network interface seperti pada tabel 3.5. ISO image Kali Linux 2023.1 dipilih sebagai media instalasi, yang menyediakan berbagai alat keamanan bawaan yang diperlukan untuk simulasi serangan.

Tabel 3.5. VMWare *Hypervisor* (*Attacker*)

Node	Name	Memory	vProcessor	Hard Disk (SCSCI)	Network Adapter
Node Virtual	Kali Linux OS (Hydra, Hping3 dan NMAP)	4 GB	4	80 GB	Bridge

Setelah proses instalasi dan konfigurasi kali linux OS berhasil diinstal, tahap selanjutnya adalah proses instalasi dan konfigurasi tools penyerang (*attackers*). Pertama, Hydra akan digunakan untuk melakukan serangan brute force pada protokol jaringan serta mencoba berbagai kombinasi kredensial username dan password yang tercantum dalam `wordlist rockyou.txt` yang dimodelkan, bertujuan untuk menguji ketahanan sistem terhadap serangan *brute force*. Kedua, Hping3, pada target serangan MikroTik RouterOS akan digunakan untuk melakukan serangan *denial-of-service* (DoS) dengan membuat MikroTik tidak responsive. Pengujian dengan *tool* Nmap dilakukan untuk pemetaan dan pemindaian jaringan dan identifikasi layanan yang berjalan di wazuh agent, untuk mengidentifikasi perangkat dan layanan (*service*) yang aktif. Node kali linux OS yang terkonfigurasi ini akan digunakan untuk emulasi dan simulasi serangan terhadap infrastruktur jaringan yang diawasi oleh sistem Wazuh, yang memungkinkan evaluasi dan mekanisme deteksi dan respons yang dimodelkan.

3.3.5. Konfigurasi Node Wazuh Agent

Konfigurasi node untuk Wazuh *agent* pada Wazuh Manager merupakan tahapan penting untuk memastikan bahwa sistem wazuh manager dapat memonitor dan merespons ancaman secara efektif dan *real-time* dari wazuh *agent*. Penambahan Wazuh Agent diterapkan pada tiga sistem operasi ubuntu server yang sudah diinstal sesuai tabel 3.6.

Tabel 3.6. Konfigurasi dan Penamaan Wazuh *Agent* di Wazuh Manager

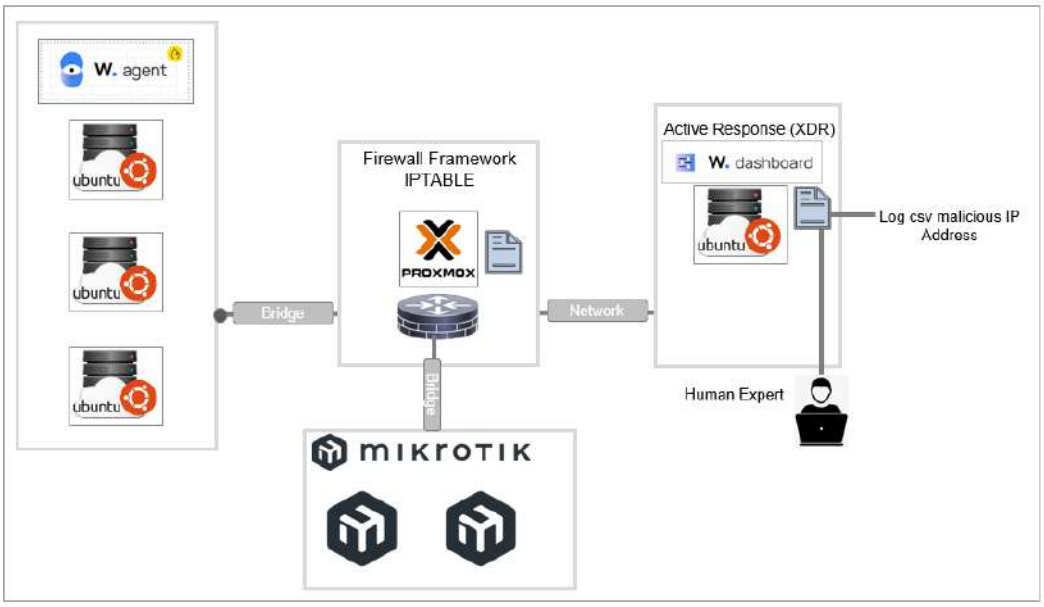
System and Architecture Wazuh Agent				
Operating System	**Server Address (FQDN)**	**Agent Name**	**Groups**	**API Agent**
deb amd 64	103.214.112.64	Agent_Brute_Force	Brute Force	
deb amd 64	103.214.112.64	Agent_Slowloris	Slowloris	
deb amd 64	103.214.112.64	Agent_NMAP	Network Mapping	

Proses instalasi wazuh agent akan ditambahkan secara manual ke sistem wazuh manager (server) dan wazuh agent akan diinstall menggunakan *shell (bash)* untuk mengunduh, menginstal, dan mengkonfigurasi wazuh agent ke wazuh manager. Pada pemodelan di penelitian ini wazuh agent diinstall di sistem controller untuk terhubung ke wazuh manager dengan ip address public 103.214.112.64, dan memberikan nama agent Agent_Brute_Force, Agent_Hping3 dan Agent_NMAP.

3.3.6. Arsitektur Framework Firewall IPTables dan Active Response Wazuh

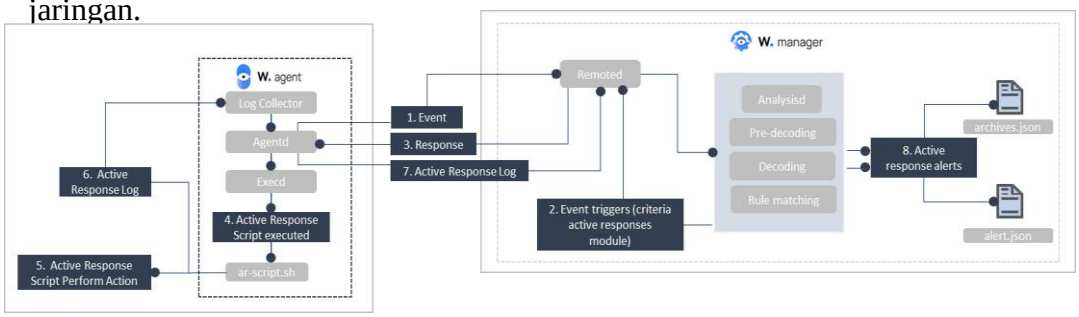
Konfigurasi untuk mitigasi serangan dilakukan dengan double layer framework firewall IPTables dan XDR active response wazuh seperti gambar 3.3. Framework firewall ini berfungsi untuk menambahkan rule secara dinamis untuk merespons aktivitas sumber IP address penyerang. Tindakan dan proses firewall ini dimulai dengan serangan yang dilakukan pada wazuh agent pada sistem operasi ubuntu server dan router mikrotik, berdasarkan IP Address. IP address ini kemudian ditambahkan ke daftar IP berbahaya menggunakan IPSet. Selanjutnya penerapan mitigasi juga dilakukan framework modul active response wazuh untuk memonitor log service SSH untuk mendeteksi *brute force*. Proses monitoring dengan aktivitas log di setiap node agent di wazuh, dengan mendeteksi serangan *brute force*, kemudian mengirimkan data ke wazuh manager. Wazuh manager akan mengidentifikasi IP address yang terlibat dalam aktivitas mencurigakan atau serangan. Konfigurasi *active response* yang dimodelkan pada penelitian ini, digunakan untuk mengatasi serangan *brute force* pada layanan SSH dengan memanfaatkan fitur wazuh active response untuk memblokir alamat IP penyerang secara otomatis. Konfigurasi active response ini melibatkan komponen utama dari

wazuh agent yang diinstall sistem operasi ubuntu server, dan wazuh manager yang bertindak sebagai *controller*.



Gambar 3.3. Arsitektur Umum *Framework* Firewall IPTables dan *Active Response* (XDR) wazuh

Gambar 3.4 Merupakan arsitektur modul *active response* wazuh, bekerja dengan mengeksekusi skrip *response* secara otomatis pada *endpoint* (wazuh agent) yang dimonitor dari *index pattern* yang sudah dikonfigurasi sebelumnya (*wazuh alert.json dan wazuh archives.json*) dengan rule-ID, level, atau *rule group*. Dengan menerapkan modul active response, tim keamanan (SOC) dapat mengotomatisasi tindakan respons terhadap kejadian ataupun insiden pada perangkat infrastruktur jaringan.



Gambar 3.4. Arsitektur modul XDR *Active Response* wazuh

Dengan menggunakan modul *active response* Wazuh, peneliti mengotomisasi framework firewall untuk serangan *brute force*, modul ini akan memicu skrip yang secara otomatis mengambil tindakan untuk mengatasi ancaman *brute force* tersebut. Kebijakan `action` firewall berupa pemblokiran akses dari IP penyerang, dengan aturan yang telah ditentukan.

a. Event

Memonitoring wazuh agent - ketika terdapat event dengan deteksi serangan *brute force* pada Wazuh agent yang dimonitor, event ini dicatat oleh *log collector*.

b. The event trigger criteria configured in the active response module

Wazuh Server (Wazuh Manager) - event akan dikirimkan ke wazuh server untuk dianalisis. Event tersebut memicu script yang dikonfigurasi dalam modul *active response*, seperti *rule* tertentu yang mengidentifikasi ancaman atau jenis serangan dari *brute force*.

c. Response

Pada wazuh agent setelah *event* memenuhi kriteria, respon diaktifkan dan dikirim kembali ke agent di endpoint pada sistem operasi ubuntu server.

d. *Execution of Active Response Script* (4 dan 5)

Wazuh agent akan menjalankan skrip eksekusi dan *active responses* yang sudah dikonfigurasi sebelumnya. Skrip ini merupakan firewall drop untuk memblokir IP penyerang (*brute force*)

e. Active response log created

Pada wazuh agent log dari `action` *active responses* akan dibuat dan dicatat wazuh agent. Log ini berisi informasi tentang tindakan yang diambil sebagai respons terhadap event tersebut.

f. Active response log analysis

Analisis akan dilakukan pada wazuh server untuk log *active responses* dan dianalisis di wazuh server untuk memastikan bahwa `action` yang dilakukan sudah sesuai dan berhasil dalam mengurangi ancaman.

g. Active responses alerts

Wazuh Server akan menampilkan pada wazuh dashboard alert berdasarkan *active responses* yang telah dilakukan dan menyimpannya dalam file JSON (`archives.json` dan `alerts.json`). Masing-masing alert ini akan memberikan informasi kepada tim keamanan tentang tindakan yang diambil dan status *endpoint* pada wazuh dashboard.

3.4. Tahap Implementasi (Implementasi dan Pengujian Fungsionalitas Sistem)

Tahap implementasi dalam penelitian ini melibatkan instalasi, konfigurasi dan pembuatan script firewall pada lingkungan pengujian untuk memastikan bahwa sistem firewall dan active responses bekerja sesuai dengan yang diharapkan. Proses ini meliputi instalasi dan konfigurasi perangkat keras, sistem operasi ubuntu server, hypervisor proxmox dan vmware, serta framework active responses menggunakan script python. Pengujian yang dilakukan dengan skenario serangan nyata menggunakan tools di kali linux, untuk menguji serangan reconnaissance attack, access attack dan DoS attack. Peneliti akan mengukur efektivitas sistem dalam mendeteksi, merespons, dan memitigasi serangan pada *firewall* dengan monitoring pada wazuh dashboard. Hasil dari tahap implementasi ini selanjutnya akan memberikan data empiris yang dapat digunakan peneliti untuk mengevaluasi efektivitas dan kinerja solusi yang diusulkan dalam penelitian.

3.4.1. Instalasi dan Konfigurasi Wazuh *Security Information and Event Management* (SIEM) dan Extended Detection and Response (XDR)

Implementasi untuk tahap instalasi dan konfigurasi wazuh *Security Information and Event Management* (SIEM) dan *Extended Detection and Response* (XDR) merupakan tahap krusial untuk penelitian, bertujuan untuk mendeteksi secara real time dengan wazuh dashboard dan mitigasi ancaman pada infrastruktur jaringan yang dimodelkan. Pada penelitian ini, Wazuh SIEM dan XDR akan berperan penting untuk mengumpulkan, menganalisis, dan merespons wazuh agent atau layanan pada system operasi dan perangkat router MikroTik secara real-time. Proses instalasi ini akan dimulai dengan instalasi node wazuh *indexer*, server dan dashboard pada *Virtual Private Server* (VPS) IDCloud yang dihosting secara public, yang berfungsi dan bertanggung jawab untuk menerima dan memproses log dari berbagai wazuh agent yang tersebar dan terpasang pada perangkat endpoint (vServer ubuntu server dan router MikroTik). Masing-masing wazuh agent akan dikonfigurasi untuk mengirimkan data log secara terus-menerus ke wazuh manager.

1. Langkah Pertama

Langkah pertama ini melakukan pengunduhan dan instalasi *packet* dan *library* wazuh manager. Perintah berikut merupakan tahap menginstal wazuh manager pada sistem operasi ubuntu server pada VPS. Instalasi ini dimulai dengan perintah:

```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

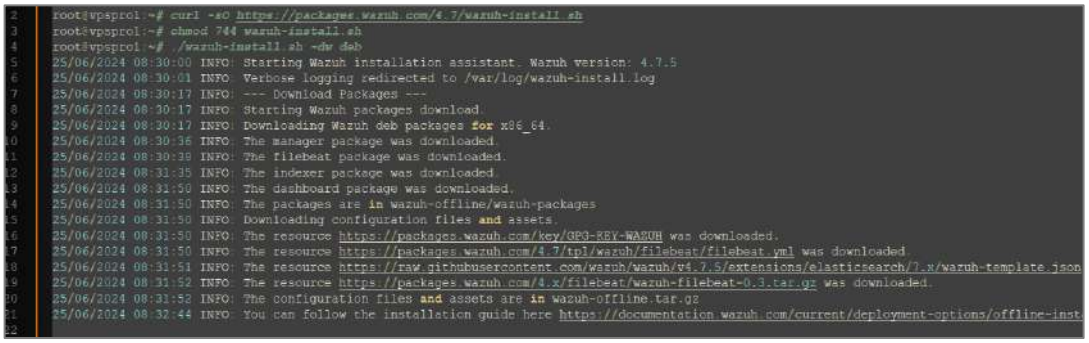
Setelah skrip wazuh manager selesai di *download*, perintah selanjutnya menjalankan perintah:

```
chmod 744 wazuh-install.sh
```

Baris perintah diatas akan memberikan izin kepada file wazuh agera dapat membaca (*read*), menulis (*write*), dan mengeksekusi (*execute*), pada wazuh manager dan memastikan bahwa skrip dapat dieksekusi dengan aman.

```
./wazuh-install.sh -dw deb
```

Baris perintah diatas digunakan untuk mengeksekusi skrip instalasi wazuh manager dengan `-dw deb`, untuk menginstruksikan dan menjalankan baris skrip dalam proses instalasi wazuh manager `(-d)` dan agen `(-w)` pada *hosting* VPS server. Proses tersebut akan mengotomatisasi instalasi dan konfigurasi wazuh manager, seperti pada gambar 3.5.



Gambar 3.5 Tahap instalasi Wazuh Manager

2. Langkah Kedua

Pada langkah kedua ini, melakukan konfigurasi pada wazuh manager untuk pengaturan IP Address wazuh indexer node, wazuh server node dan wazuh dashboard node. Tahap pertama dengan mendownload file konfigurasi `config.yml`.

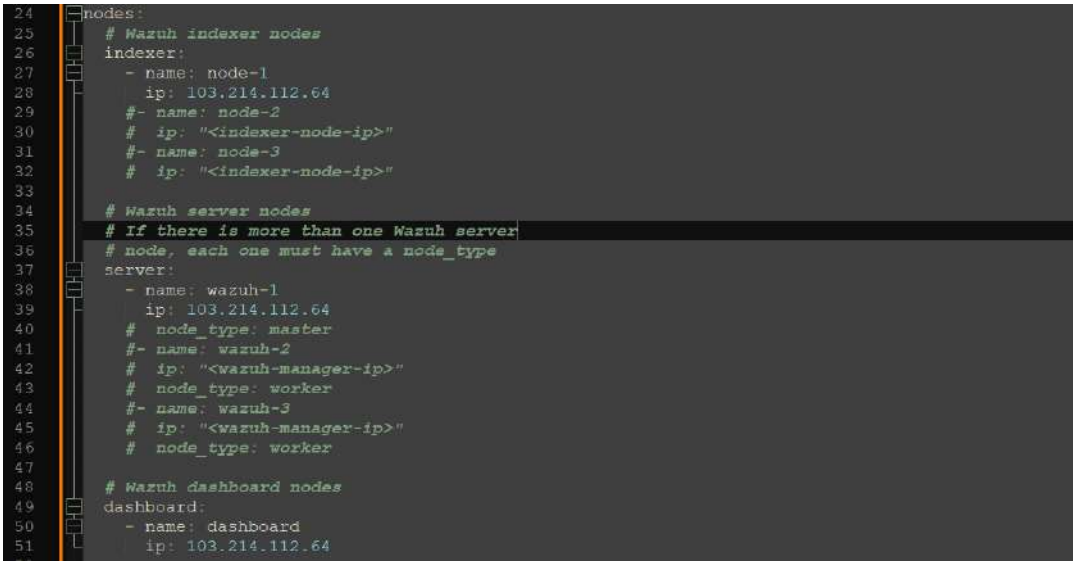
a. *Wazuh indexer node* – konfigurasi IP address 103.214.112.64 yang berfungsi dan bertanggung jawab untuk konektivitas dan komunikasi dengan wazuh agent dan penerapan *active responses*.

b. *Wazuh server node* – IP address pada server node berfungsi mengindeks dataset log yang dikumpulkan untuk proses pencarian dan analisis dengan *elasticsearch.*

c. *Wazuh dashboard node* – konfigurasi IP *address* untuk dashboard node yang berfungsi sebagai antarmuka pengguna berbasis web untuk memantau dan mengelola seluruh sistem wazuh manager.

```
curl -sO https://packages.wazuh.com/4.7/config.yml
```

Konfigurasi config.yml dikonfigurasi pada IP address pada masing-masing node yang dalam arsitektur wazuh manager seperti gambar 3.6.



Gambar 3.6 Konfigurasi node indexer, server dan dashboard wazuh manager

3. Langkah ketiga merupakan instalasi dan konfigurasi sertifikat wazuh manager, dengan perintah:

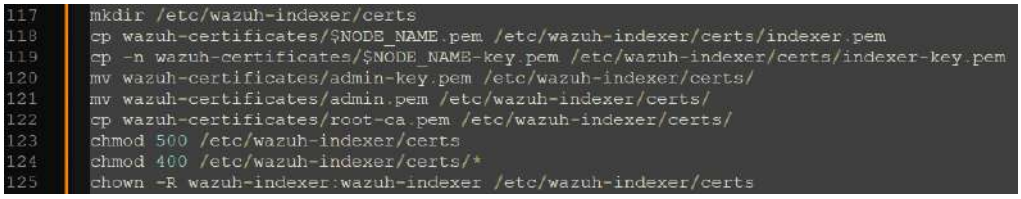
```
curl -sO https://packages.wazuh.com/4.7/wazuh-certs-tool.sh
./wazuh-certs-tool.sh --all
```

Skrip diatas merupakan aktivasi sertifikat wazuh manager, untuk factor keamanan komunikasi antara komponen wazuh manager (*indexer*, *server* dan *dashboard*) dengan wazuh agent.

4. Langkah keempat adalah membuat node untuk menetapkan `node-1` yang sudah dikonfigurasi sebelumnya pada `config.yml`. Baris perintah pada `node-1` akan menyesuaikan dan menyelaraskan konfigurasi node dengan entri yang ada di `config.yml`, `node-1` merupakan node untuk wazuh indexer. Konfigurasi `node-1` ini akan menyesuaikan dengan IP Address 103.214.112.64/32, yang sudah dikonfigurasi dalam `config.yml`. Baris perintahnya adalah `NODE_NAME=node-1` konektivitas dan komunikasi untuk semua node dalam wazuh manager. Node *indexer* akan berperan dan bertanggung jawab untuk

melakukan *index* dan penyimpanan dataset log dari agent wazuh. Kemudian setelah `node-1` selanjutnya akan dilakukan beberapa konfigurasi seperti pada gambar 3.7, dengan langkah-langkah sebagai berikut:

a) Pembuatan sertifikat keamanan wazuh untuk digunakan pada wazuh indexer.
b) Konfigurasi penamaan penamaan sertifikat (`indexer.pem` dan `indexer-key.pem`)
c) Konfigurasi autentikasi cluster wazuh
d) Verifikasi sertifikat Root CA
e) Konfigurasi hak akses dan *privilege* untuk sertifikat pada direktori.



Gambar 3.7 Konfigurasi Sertifikat Wazuh Indexer

5. Langkah kelima melakukan konfigurasi pada *file* `opensearch.yml` bertujuan untuk mengatur identitas dan konfigurasi wazuh *indexer* yang terhubung dengan `opensearch`. Gambar 3.8 merupakan tahap pertama untuk, `node.name: "node-1"` mengidentifikasi *node name* wazuh indexer yang akan berjalan pada wazuh manager, bagaimana node ini akan mengindentifikasi node dalam kluster `OpenSearch`.

```
network.host: "0.0.0.0"
node.name: "node-1"
cluster.initial_master_nodes:
- "103.214.112.64"
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
discovery.seed_hosts:
  - "103.214.112.64"
#  - "node-2-ip"
#  - "node-3-ip"
node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false

plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=node-1,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"
```

Gambar 3.8 Konfigurasi file `opensearch.yml`

Tahap kedua pada proses dan konfigurasi yang dilakukan adalah, `cluster.initial_master_nodes: - "103.214.112.64"` bertujuan untuk menetapkan `node-1`, sebagai node master dalam *cluster* `OpenSearch`. `node-1` yang akan mengelola dan mengatur distribusi data *cluster* dan menggunakan IP Address `103.214.112.64`. `cluster.name: "wazuh-cluster` merupakan penamaan dari *cluster* wazuh *indexer*. Masing-masing node yang akan bergabung *cluster* wazuh *indexer* akan menggunakan dan diindentifikasi dalam cluster yang sama. `discovery.seed_hosts: 103.214.112.64`, merupakan daftar host yang akan berfungsi pada node ketika membentuk cluster. konfigurasi file `opensearch.yml` dilakukan untuk memanstikan node wazuh *indexer* dapat berfungsi pada cluster.

6. Langkah selanjutnya pada wazuh indexer, melakukan pemeriksaan status layanan wazuh indexer, untuk menampilkan status, layanan dan log seperti gambar 3.9.

```
root@manager:/home/manager# systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-06-29 08:19:39 UTC; 1 weeks 1 days ago
       Docs: https://documentation.wazuh.com
   Main PID: 27236 (java)
      Tasks: 114 (limit: 9424)
     Memory: 1.6G
     CGroup: /system.slice/wazuh-indexer.service
             └─27236 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60
```

Gambar 3.9 Status Wazuh Indexer

7. Proses selanjutnya pada wazuh indexer adalah melakukan inisialisasi dengan perintah sebagai berikut:

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

8. Setelah menjalankan baris perintah diatas, langkah selanjutnya adalah melakukan verifikasi pada wazuh indexer, dengan perintah sebagai berikut:

```
curl -XGET https://localhost:9200 -u
```

Baris perintah diatas menggunakan `curl`, untuk mengirimkan request `GET` ke wazuh indexer di `https:// localhost` menggunakan port 9200. Tahapan ini dilakukan untuk verifikasi konfigurasi wazuh indexer agar dapat menerima dataset seperti pada gambar 3.10

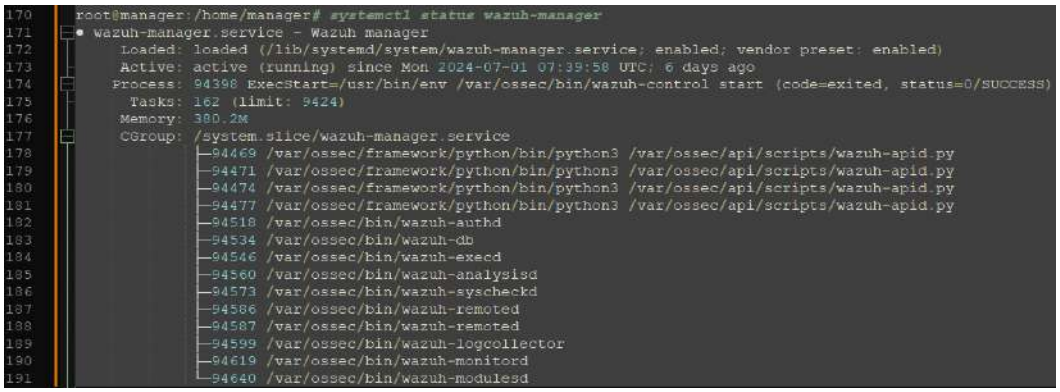
```
root@vpspro1:~# curl -XGET https://localhost:9200 -u admin:admin -k
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "h2a9oCdPRU-vNjbbzsZcGQ",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
}
root@vpspro1:~#
```

Gambar 3.10 Verifikasi Konfigurasi Wazuh *Indexer*

9. Setelah wazuh indexer running dan berfungsi, langkah selanjutnya adalah menginstal wazuh manager dengan perintah sebagai berikut:

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

Baris skrip diatas merupakan paket wazuh manager yang akan diinstal di Hosting VPS, yang merupakan komponen utama untuk mengelola wazuh agent yang terdistribusi, mengumpulkan data dari wazuh agent untuk dianalisa berdasarkan *log*, dan melakukan tindakan (*active responses*) keamanan berdasarkan aturan (*rule*) yang akan ditentukan. Gambar 3.11 merupakan verifikasi wazuh manager setelah proses instalasi dan konfigurasi.



Gambar 3.11 Verifikasi Operasioan Wazuh Manager

10. Langkah selanjutnya melakukan instalasi paket `filebeat` untuk memastikan komponen wazuh `filebeat` dikonfigurasi dengan benar pada wazuh manager. Baris perintah yang digunakan untuk instalasi dan konfigurasi filebeat seperti pada gambar 3.12.

```
dpkg -i ./wazuh-offline/wazuh-packages/filebeat*.deb
cp ./wazuh-offline/wazuh-files/filebeat.yml /etc/filebeat/ &&\
cp ./wazuh-offline/wazuh-files/wazuh-template.json /etc/filebeat/ &&\
chmod go+r /etc/filebeat/wazuh-template.json
```

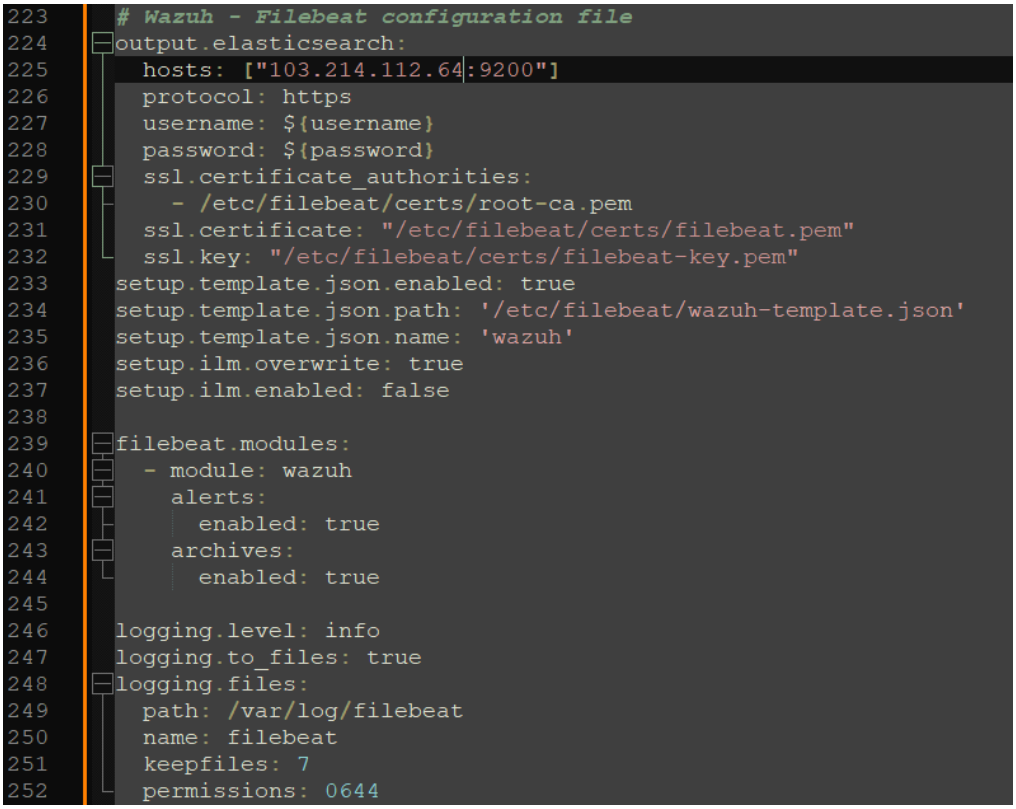
Gambar 3.12 Instalasi dan Konfigurasi Paket Wazuh Filebeat

Penyalinan dan penyesuaian konfigurasi paket `filebeat` diatas merupakan instalasi dan konfigurasi paket spesifik yang akan digunakan wazuh manager untuk fungsi monitoring. Termasuk untuk mengumpulkan dan mengirimkan *log* serta mengatur dataset *log* disimpan dan diindeks pada *Elasticsearch*.

Setelah konfigurasi `filebeat`, langkah selanjutnya melakukan konfigurasi *file script* `index.number_of_shards` bertujuan untuk mengoptimalkan penggunaan sumber daya dan kinerja indeks *elasticsearch*. Nilai shard yang akan dirubah yaitu `index.number_of_shards: 3` menjadi `index.number_of_shards: 1`. Tujuannya adalah untuk mengurangi *overhead* pengelolaan dan penyebaran data dalam cluster, seperti gambar 3.13

Gambar 3.13 Konfigurasi *file script filebeat* index.number_of_shards

11. Langkah selanjutnya merupakan konfigurasi *file script* `filebeat.yml` yang nantinya akan digunakan untuk pengiriman dataset log ke *elasticsearch*, dan mengaktifkan modul `filebeat` wazuh untuk pengumpulan log berdasarkan `alert` dan `archives`.



Gambar 3.14 Konfigurasi Filebeat Wazuh Alert dan Archives

Konfigurasi *file script* `filebeat.yml` pada gambar 3.14, merupakan *key* untuk mengaktifkan dan mengumpulkan dataset log dari wazuh manager ke *elasticsearch* kunci menggunakan `filebeat`. Konfigurasi `output.elasticsearch: hosts: ["103.214.112.64:9200"]` merupakan penyesuaian host dan *elasticsearch* port tempat `filebeat` mengirimkan dataset log. Konfigurasi ini akan relevan dengan *endpoint* tempat *elasticsearch* menerima dataset yang dikirim dari `filebeat` wazuh manager. Semua dataset log yang dikumpulkan wazuh manager, termasuk `alert` dan `archives`, akan dikirim menuju *elasticsearch* pada *host* 103.214.112.64.

Selanjutnya, `filebeat.modules:` akan diubah dari `alert: enable false` menjadi `alert: enable true` dan `archives: enable false` menjadi `archives: enable true` pada konfigurasi wazuh `filebeat.yml`. Tujuan dari konfigurasi file script ini akan mengaktifkan pengumpulan `alert` dan `archives` dari wazuh ke *elasticsearch* melalui `filebeat`, sehingga wazuh manager dapat memonitoring dan menganalisis kejadian yang terdeteksi oleh wazuh secara *realtime*.

12. Pada filebeat yang sudah dikonfigurasi diatas langkah selanjutnya adalah membuat kredensial username dan password pada keystore filebeat dengan baris perintah sebagai berikut:

```
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force
```

Baris perintah diatas digunakan untuk membuat dan menyimpan nilai *username* dan *password* yang akan digunakan untuk mengautentikasi *elasticsearch* pada *keystore* `filebeat`.

13. Langkah selanjutnya melakukan konfigurasi wazuh dengan baris perintah `NODE_NAME=wazuh-1`, merujuk pada pengaturan node wazuh file `config.yml`. Selanjutnya melakukan konfigurasi sertifikat `filebeat` dengan menggunakan sertifikat `wazuh-certificates`, dan mengatur hak akses serta *privilege* seperti pada gambar 3.15.

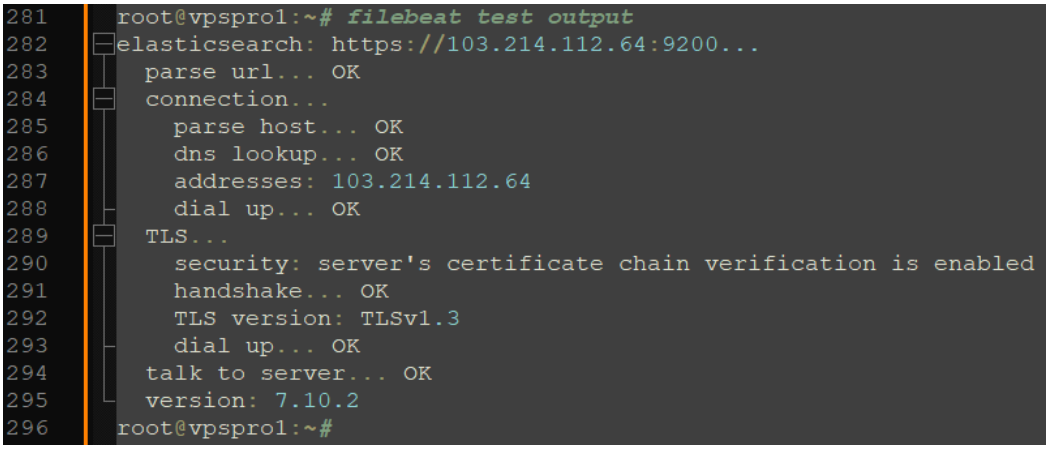
```
256  mkdir /etc/filebeat/certs
257  cp wazuh-certificates/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
258  cp wazuh-certificates/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
259  cp wazuh-certificates/root-ca.pem /etc/filebeat/certs/
260  chmod 500 /etc/filebeat/certs
261  chmod 400 /etc/filebeat/certs/*
262  chown -R root:root /etc/filebeat/certs
```

Gambar 3.15 Sertifikat Filebeat

Langkah diatas merupakan tahap krusial, karena berfungsi untuk memastikan `filebeat` dapat melakukan koneksi menuju *elasticsearch* secara aman. Gambar 3.16 merupakan verifikasi `filebeat` untuk memastikan memastikan konektivitas dan komunikasi antara `filebeat` dan *elasticsearch* berjalan dengan benar dan untuk enripsi dan autentikasi dapat berjalan.

Gambar 3.16 Verifikasi status Filebeat

14. Langkah selanjutnya gunakan *filebeat test output* untuk melakukan pengujian koneksi dari `filebeat` ke *elasticsearch* yang sudah dikonfigurasi pada *host* 103.214.112.64:9200, seperti pada gambar 3.17.



Gambar 3.17 Pengujian Filebeat dan *Elasticsearch*

Dari hasil pengujian diatas hasil dari `elasticsearch: https://103.214.112.64:9200` menunjukkan bahwa `filebeat` telah dikonfigurasi untuk terhubung ke Elasticsearch melalui https://103.214.112.64:9200 dan dapat melakukan parsing dan sudah berhasil me *resolve* ke IP Address host 103.214.112.64. *Transport Layer Security* (TLS)

menunjukkan kalau `filebeat` sudah dapat memverifikasi sertifikat yang diterima dari server *elasticsearch*.

15. Langkah terakhir adalah membuat sertifikat dan konfigurasi untuk wazuh dashboar dengan konfigurasi seperti pada gambar 3.18. Konfigurasi sertifikat yang dilakukan untuk wazuh dashboard menggunakan `wazuh-certificates`, mengatur hak akses dan *privilege*. Langkah pertama adalah membuat node *dashboard* dengan baris perintah `NODE_NAME=dashboard`. Node ini merujuk pada penamaan entitas sebelumnya pada `config.yml`. pada konfigurasi ini, penggunaan `NODE_NAME=dashboard` untuk mengidentifikasi konfigurasi sertifikat untuk wazuh *dashboard* serta menentukan langkah konfigurasi, dari pembuatan direktori, penyalinan sertifikat, dan *privilege* seperti pada Gambar 3.18.

```
299  NODE_NAME=dashboard
300  mkdir /etc/wazuh-dashboard/certs
301  cp wazuh-certificates/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
302  cp wazuh-certificates/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
303  cp wazuh-certificates/root-ca.pem /etc/wazuh-dashboard/certs/
304  chmod 500 /etc/wazuh-dashboard/certs
305  chmod 400 /etc/wazuh-dashboard/certs/*
306  chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Gambar 3.18 Konfigurasi Wazuh Dashboard dan Sertifikat

16. Langkah ini merupakan konfigurasi pada `dashboard.yml` dengan baris perintah: `/etc/wazuh-dashboard/opensearch_dashboards.yml`, untuk mengubah aturan koneksi dan komunikasi wazuh dashboard. Konfigurasi ini akan dihubungkan dengan *opensearch* atau *elasticsearch*.

```
311  server.host: 0.0.0.0
312  server.port: 443
313  opensearch.hosts: https://10.151.20.169:9200
314  opensearch.ssl.verificationMode: certificate
315  #opensearch.username:
316  #opensearch.password:
317  opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
318  opensearch_security.multitenancy.enabled: false
319  opensearch_security.readonly_mode.roles: ["kibana_read_only"]
320  server.ssl.enabled: true
321  server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
322  server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
323  opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
324  uiSettings.overrides.defaultRoute: /app/wazuh
```

Gambar 3.19 Konfigurasi Wazuh Dashboard

File script `opensearch.host` akan digunakan digunakan untuk wazuh dashboard melakukan komunikasi. URL https://103.214.112.64:9200 memperlihatkan wazuh *dashboard* akan terbuhung ke `opesearch` dengan *host* IP *address* 103.214.112.64 dan menggunakan port 9200. Konfigurasi ini memastikan kalau wazuh *dashboard* dapat beroperasi dengan aman saat terkoneksi dengan `OpenSearch`. Selanjutnya gunakan perintah baris dibawah untuk melakukan konfigurasi pada `wazuh.yml`.

```
nano /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml
```

```
328 hosts:
329   - default:
330       url: https://103.214.112.64
331       port: 55000
332       username: wazuh-wui
333       password: wazuh-wui
334       run_as: false
335
```

Gambar 3.20 Konfigurasi Host Wazuh (`wazuh.yml`)

Gambar 3.20 merupakan konfigurasi URL dan kredensial wazuh dashboard agar dapat diakses secara remote untuk monitoring dan pengelolaan *log*, *alert* wazuh agent secara lebih mudah dan terpusat.

3.4.2. Konfigurasi *Syslog* dan *Log Index Pattern Archives* pada Wazuh server

Implementasi dan konfigurasi *syslog* dan *log* module *index pattern*, pada wazuh server merupakan tahap awal untuk memastikan dan memaksimalkan kemampuan wazuh syslog dan log archives untuk active responses XDR wazuh. Pada penelitian ini konfigurasi index pattern ini digunakan untuk mengumpulkan, menganalisis dan menyimpan log dari masing-masing wazuh agent, termasuk perangkat router dan vServer. Sehingga penerapan *active responses* yang diimplementasikan dapat memberikan gambaran yang komprehensif tentang aktivitas pada infrastruktur jaringan dalam mendeteksi potensi ancaman secara lebih efektif. File penyimpanan yang dibuat oleh server wazuh server yang berisi log, peringatan (*alerts*), dan data terkait keamanan lainnya yang dikumpulkan dari endpoint wazuh agent yang dipantau. Index pattern wazuh yang akan diimplementasikan dan dikonfigurasi

adalah *wazuh-archive*. *wazuh-archive* menyimpan semua peristiwa yang diterima oleh wazuh server, untuk meninjau data historis insiden keamanan, menganalisis tren, dan menghasilkan laporan. Berikut langkah yang dilakukan untuk mengkonfigurasi *index pattern: wazuh-archives* pada wazuh server:

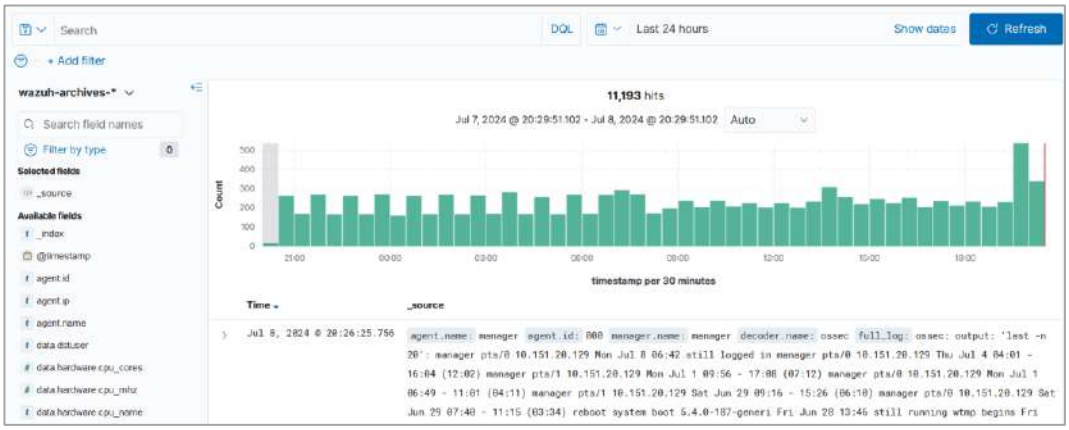
a. Langkah pertama pada file /var/ossec/etc/ossec.conf, akan dikonfigurasi <ossec_config> dengan baris script seperti gambar 3.21. Konfigurasi <alerts_log>yes</alerts_log>: akan berfungsi mencatat semua log dan *alert* yang dihasilkan wazuh ke dalam file log alerts.log dan archive.log. File log ini akan digunakan untuk melacak dan meninjau *alert* yang terdeteksi pada wazuh server. Konfigurasi <logall_json>yes</logall_json>: berfungsi untuk mengaktifkan log dari semua dataset log dalam format JSON. Konfigurasi <jsonout_output>yes</jsonout_output>: akan dikonfigurasi untuk dapat menyimpan seluruh hasil log analysis dalam format JSON.

```
336  <ossec_config>
337    <global>
338      <jsonout_output>yes</jsonout_output>
339      <alerts_log>yes</alerts_log>
340      <logall>no</logall>
341      <logall_json>yes</logall_json>
342      <email_notification>no</email_notification>
343      <smtp_server>smtp.ajn.wazuh.com</smtp_server>
344      <email_from>wazuh@ajn.wazuh.com</email_from>
345      <email_to>recipient@ajn.wazuh.com</email_to>
346      <email_maxperhour>12</email_maxperhour>
347      <email_log_source>alerts.log</email_log_source>
348      <agents_disconnection_time>10m</agents_disconnection_time>
349      <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
350    </global>
351
352    <alerts>
353      <log_alert_level>3</log_alert_level>
354      <email_alert_level>12</email_alert_level>
355    </alerts>
```

Gambar 3.21 Konfigurasi ossec_config Wazuh Server

b. Pada *index pattern* wazuh-archives akan terlihat, wazuh mengindeks dataset log yang disimpan pada wazuh-arhives di *Elasticsearch*. Fungsi utama dari index pattern ini merupakan memformat dan mengatur data *log* termasuk *field* dan menganalisis *timestamp* dan *agent* ID. *Index pattern wazuh-archives-** yang dimodelkan juga menjadi komponen dalam konfigurasi wazuh server untuk dapat mengindeks, memformat, menganalisis, dan memvisualisasikan

data log dengan mudah dan efektif, sehingga meningkatkan kemampuan wazuh dashboard untuk mendeteksi dan merespon ancaman pada infrastruktur jaringan untuk komponen perangkat router dan vServer.



Gambar 3.22 Dataset Log Wazuh-Archives

Pada gambar 3.22, merupakan log yang menunjukkan aktivitas login dari pengguna untuk agent wazuh manager selama beberapa hari terakhir. Wazuh dashboard akan mencatat dan mengumpulkan log informasi ini untuk membantu mendeteksi aktivitas mencurigakan, seperti akses yang tidak sah ke sistem yang dimodelkan pada masing-masing perangkat router dan vServer.

c. Pada ossec.conf wazuh manager akan dikonfigurasi komunikasi antara wazuh agent dan wazuh manager.

```
<ossec_config>
    <remote>
    <connection>syslog</connection>
    <port>514</port>
    <protocol>udp</protocol>
  <allowed-ips>10.151.20.128/25</allowed-ips>
    <local_ip>103.214.112.64</local_ip>
   </remote>

   <remote>
     <connection>secure</connection>
     <port>1514</port>
     <protocol>tcp</protocol>
     <queue_size>131072</queue_size>
   </remote>
</ossec_config>
```

Konfigurasi remote pada `ossec.conf` wazuh manager dikonfigurasi untuk menentukan bagaimana wazuh agent dan wazuh manager berkomunikasi pada distribusinya. Konfigurasi baris *script* komunikasi wazuh agent dan wazuh manager adalah sebagai berikut:

Baris *script* pada konfigurasi diatas merupakan konektivitas *syslog*. `Connection` merupakan jenis koneksu yang digunakan *syslog* untuk wazuh *agent* dapat mengirimkan *log* ke wazuh manager melalui protocol *syslog*. `Port` berfungsi untuk koneksi *syslog* menggunakan *port default* 514 dan dikonfigurasi pada wazuh *agent* untuk proses pengiriman *log syslog*. `Protocol` akan digunakan untuk koneksi *syslog* dengan *protocol* UDP untuk proses pengiriman *log* dari wazuh *agent* ke wazuh *manager*. `Allowed-IPS` merupakan subnet IP Address dengan `rule permit accept` untuk mengirim data log ke wazuh manager (10.151.20.128/25). `Local_IP` akan menentukan IP Address wazuh manager agar wazuh *agent* mengetahui tujuan pengiriman data *log*.

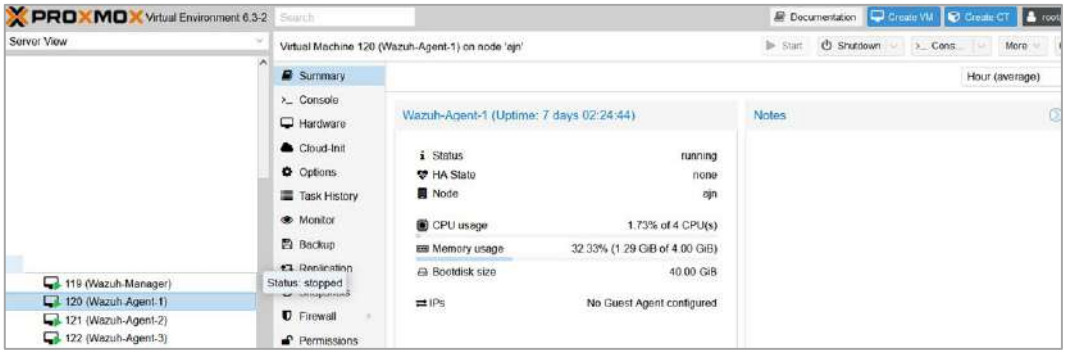
3.4.3. Konfigurasi Wazuh *Agent*

Konfigurasi node untuk wazuh agent dimodelkan dengan penambahan wazuh agent pada *hypervisor proxmox* untuk sistem operasi ubuntu server 20.04 yang sudah diinstal sesuai tabel 3.7.

Tabel 3.7. Konfigurasi wazuh *agent* pada *hypervisor* proxmox

System and Architecture Wazuh Agent				
Hypervisor Node	**Server Address (FQDN)**	**Agent Name**	**Groups**	**API Agent**
Wazuh-Agent-1	103.214.112.64	Agent_Brute_Force	Brute Force	-
Wazuh-Agent-3	103.214.112.64	Agent_Slowloris	Slowloris	-
Wazuh-Agent-3	103.214.112.64	Agent_NMAP	Network Mapping	-

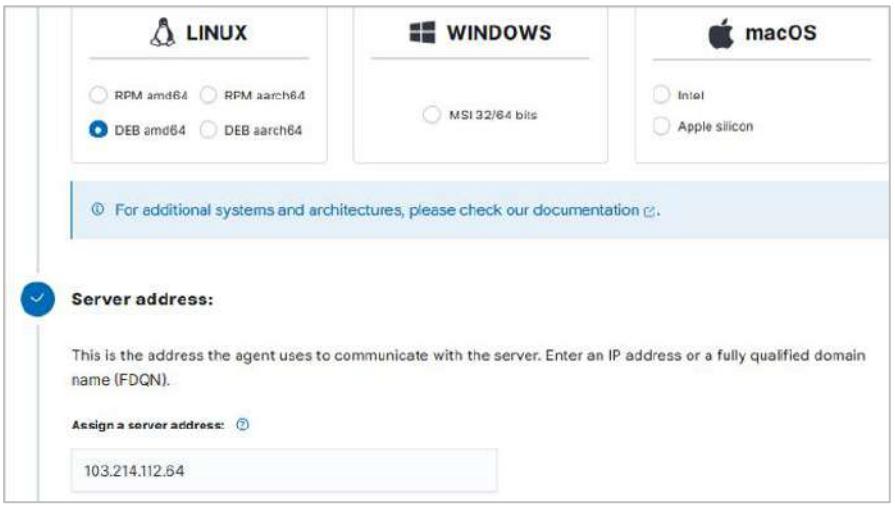
Gambar 3.23 merupakan skenario yang dilakukan pada penelitian, wazuh agent instal pada 3 (tiga) sistem operasi Ubuntu Server, dengan penamaan Wazuh-Agent-1, Wazuh-Agent-2, dan Wazuh-Agent-3.

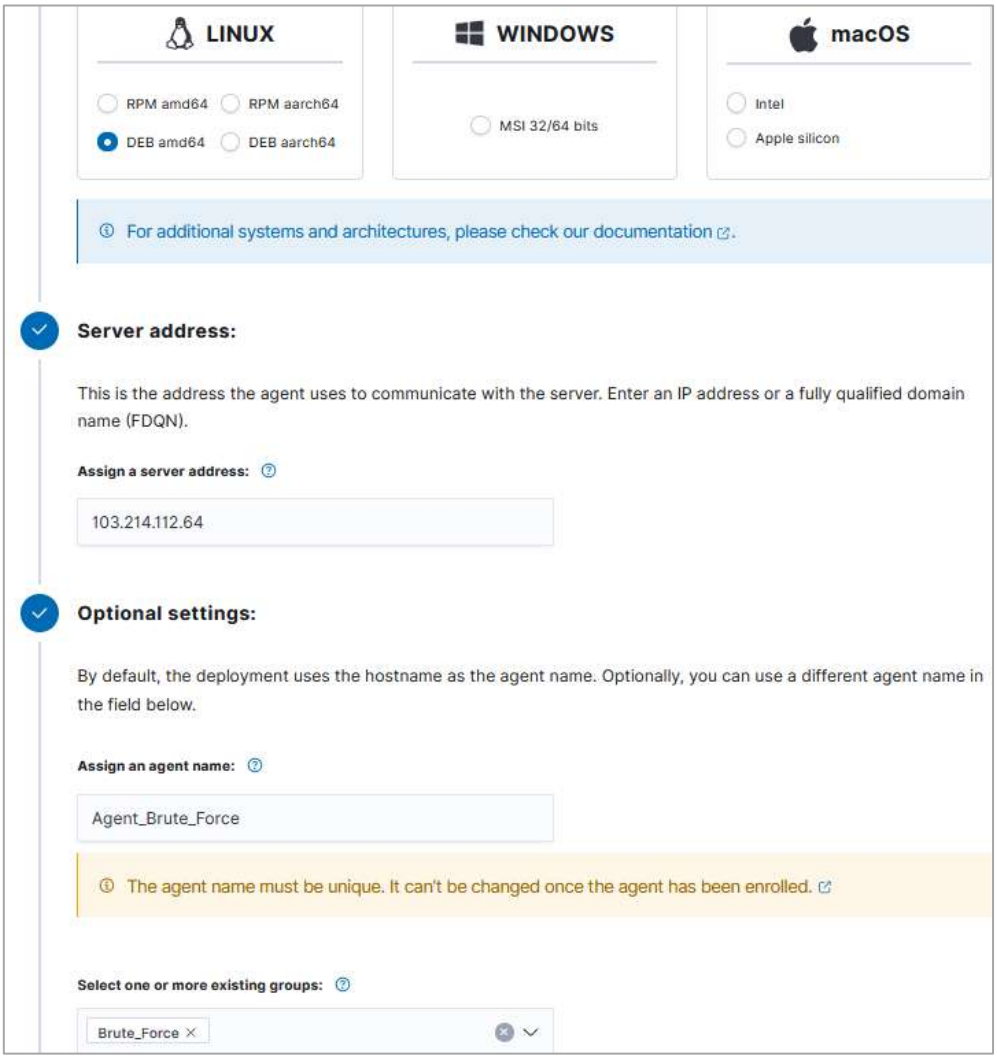


Gambar 3.23 Instalasi dan Konfigurasi Wazuh Agent pada Ubuntu Server di VM Proxmox

Berikut Langkah untuk melakukan instalasi dan konfigurasi wazuh agent:

1) Langkah pertama konfigurasi wazuh agent akan ditambahkan secara manual ke sistem wazuh manager dan wazuh agent akan diinstall menggunakan *shell (bash)* untuk mengunduh, menginstal, dan mengkonfigurasi wazuh agent ke wazuh manager seperti gambar 3.24. Konfigurasi Wazuh-Agent-1: Agent_Brute_Force dengan parameter sebagai berikut:
    - System : Deb AMD64
    - Server FQDN : 103.214.112.64
    - Assign an agent name : Agent_Brute_Force
    - Group : Brute_Force





Gambar 3.24 Konfigurasi Wazuh Agent Brute Force

2) Pada langkah kedua konfigurasi pada sistem operasi ubuntu server (Wazuh-Agent-1) seperti pada gambar 3.25 dibawah ini.

```
382  wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
383  agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER=' 103.214.112.64'
384  WAZUH_AGENT_NAME='Agent_Brute_Force' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
```

Gambar 3.25 *Script* Koneksi Wazuh Agent (*Brute Force*) ke Wazuh Manager

3) Langkah ketiga melakukan konfigurasi pada shell script ossec.conf wazuh agent_brute_force seperti pada gambar 3.26.

Konfigurasi pada gambar 3.26, merupakan *script* wazuh agent (`Agent_Brute_Force`) untuk koneksi dan komunikasi dengan wazuh manager. Konfigurasi pada wazuh *agent* untuk komunikasi ke wazuh manager melibatkan

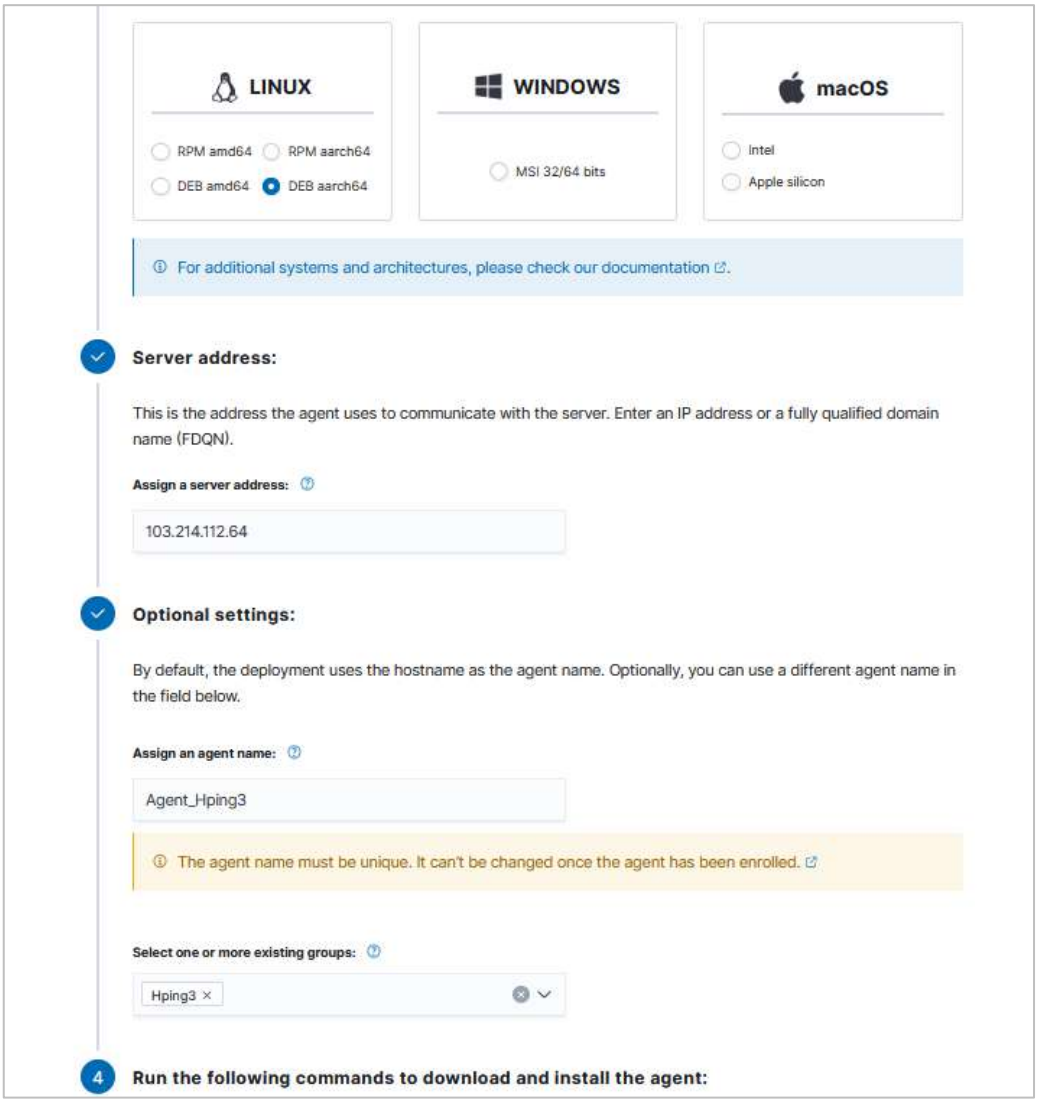
konfigurasi dan pengaturan parameter didalam file `ossec.conf`. Pada bagian `<server>`, IP *address* ditentukan oleh *tag* `<address>`, dengan subnet 103.214.112.64/32. Kemudian untuk port yang digunakan untuk komunikasi dan koneksi wazuh *agent* dan wazuh manager ditentukan oleh tag `<port>`, dengan nilai 1514. Selanjutnya *protocol* yang digunakan untuk transmisi data antara wazuh agent dan wazuh manager adalah protocol TCP, dengan *tag* `<protocol>`. Konfigurasi yang dibuat pada wazuh *agent* ini untuk memastikan wazuh *agent* dapat mengirim data *log* dan menerima perintah dari wazuh manager melalui komunikasi infrastruktur jaringan yang telah dimodelkan.

Gambar 3.26 Konfigurasi Wazuh *Agent* (*Agent_Brute_Force*)

4) Pada langkah keempat merupakan konfigurasi wazuh agent untuk system operasi Ubuntu Server 20.04 dengan node Wazuh-Agent-2: Agent_Slowloris dengan parameter sebagai berikut:
   - System : Deb AMD64
   - Server FQDN : 103.214.112.64
   - Assign an agent name : Agent_Hping3
   - Group : Hping3

Konfigurasi wazuh *agent* ini mengatur bagaimana wazuh *agent* untuk konektivitas dan berkomunikasi dengan wazuh manager dan memastikan *log*, *alerts* dan serangan yang terjadi pada wazuh *agent* dapat mengirimkan dataset *log* dengan menerima perintah dari wazuh manager. Penempatan *endpoint* wazuh agent ini akan dimodelkan pada infrastruktur jaringan *private* dan terkoneksi dengan jaringan

internet untuk wazuh manager. Dengan konfigurasi yang dimodelkan, wazuh *agent* akan secara otomatis terhubung ke wazuh manager menggunakan *shell script* yang telah dikonfigurasi seperti pada gambar 3.27.



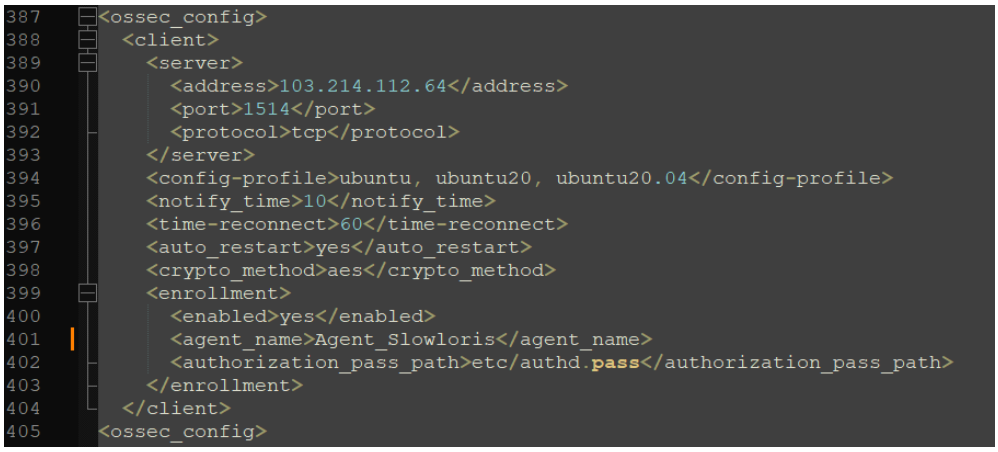
Gambar 3.27 Konfigurasi Wazuh Agent Hping3

5) Pada langkah kelima konfigurasi pada sistem operasi ubuntu server (Wazuh-Agent-2) seperti pada gambar 3.28 dibawah ini.

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent
_4.7.5-1_arm64.deb && sudo WAZUH_MANAGER='103.214.112.64' WAZUH_AGENT_GROUP=
'Hping3' WAZUH_AGENT_NAME='Agent_Hping3' dpkg -i ./wazuh-agent_4.7.5-1_arm64.deb
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Gambar 3.28 *Script* Koneksi Wazuh Agent (Hping) ke Wazuh Manager

6) Langkah keenam melakukan konfigurasi pada *shell script* `ossec.conf` wazuh *agent* untuk agent_Hping3 seperti pada gambar 3.29.



Gambar 3.29 Konfigurasi Wazuh Agent Agent_Hping3

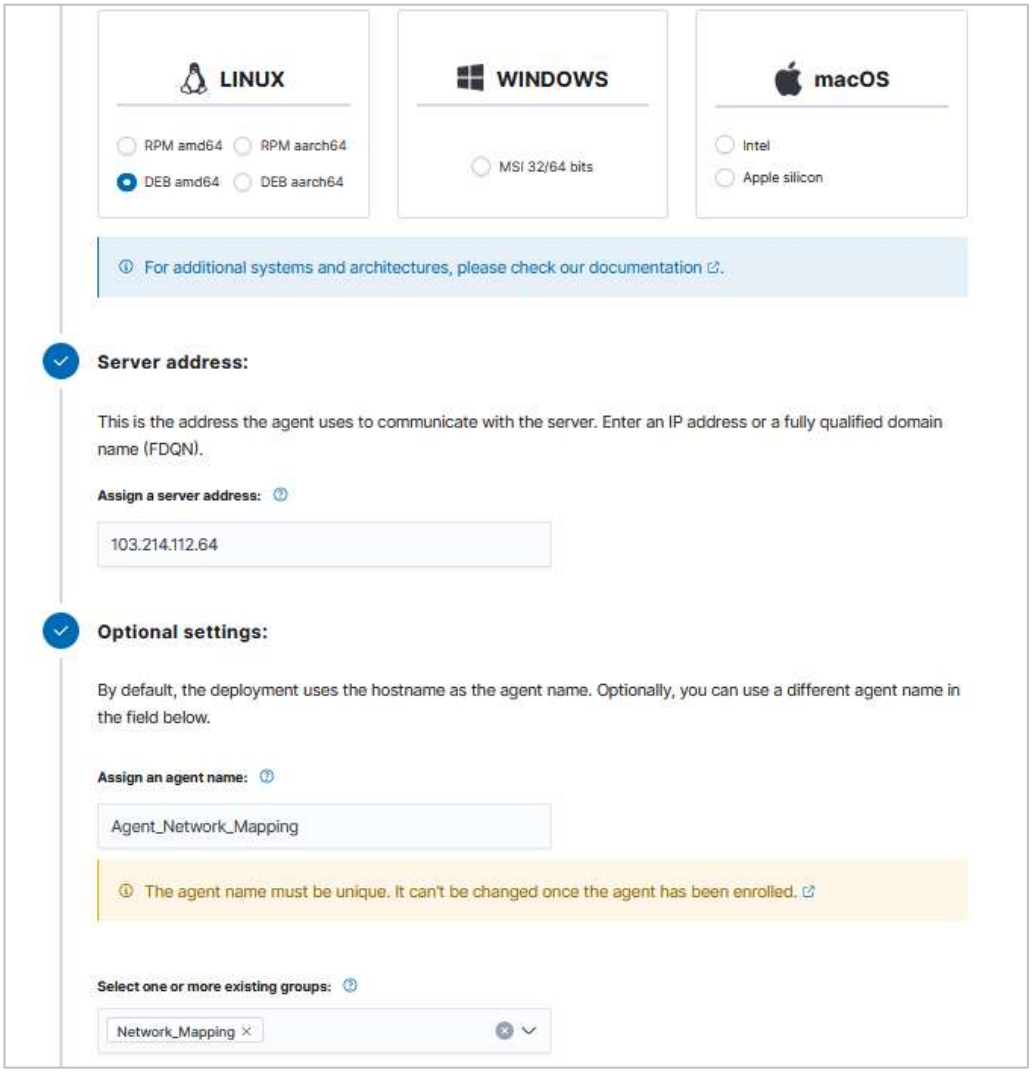
Konfigurasi pada gambar 3.29, merupakan *script* wazuh agent (Agent_Slowloris) untuk koneksi dan komunikasi dengan wazuh manager. Konfigurasi pada wazuh *agent* untuk komunikasi ke wazuh manager melibatkan konfigurasi dan pengaturan parameter didalam file `ossec.conf`. Pada bagian `<server>`, IP *address* ditentukan oleh *tag* `<address>`, dengan subnet 103.214.112.64/32. Kemudian untuk *port* yang digunakan untuk komunikasi dan koneksi wazuh *agent* dan wazuh manager ditentukan oleh *tag* `<port>`, dengan nilai 1514. Selanjutnya *protocol* yang digunakan untuk transmisi data antara wazuh *agent* dan wazuh manager adalah protocol TCP, dengan *tag* `<protocol>`. Konfigurasi yang dibuat pada wazuh *agent* ini untuk memastikan wazuh *agent* dapat mengirim data *log* dan menerima perintah dari wazuh manager melalui komunikasi infrastruktur jaringan.

7) Pada langkah ketujuh merupakan konfigurasi wazuh *agent* untuk system operasi Ubuntu Server 20.04 dengan node Wazuh-Agent-3: Agent_Network_Mapping dengan parameter sebagai berikut:

- System : Deb AMD64
- Server FQDN : 103.214.112.64
- Assign an agent name : Agent_Network_Mapping

- Group : Network_Mapping

Konfigurasi wazuh *agent* (*Agent_Network_Mapping*) ini mengatur bagaimana wazuh agent dapat berkomunikasi dengan wazuh manager dan memastikan dataset *log*, *alerts* dan serangan yang terjadi pada wazuh agent dapat mengirimkan dataset *log* dengan menerima perintah dari wazuh manager. Penempatan *endpoint* wazuh agent ini akan dimodelkan pada infrastruktur jaringan private dan terkoneksi dengan jaringan internet untuk wazuh manager. Dengan konfigurasi yang dimodelkan, wazuh *agent* akan secara otomatis terhubung ke wazuh manager menggunakan *shell script* yang telah dikonfigurasi seperti pada gambar 3.30.



Gambar 3.30 Konfigurasi Wazuh *Agent Network Mapping*

8) Langkah kedelapan konfigurasi pada sistem operasi ubuntu server (Wazuh-Agent-3) seperti pada gambar 3.31 dibawah ini.

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_
4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='103.214.112.64' WAZUH_AGENT_GROUP=
'Network_Mapping' WAZUH_AGENT_NAME='Agent_Network_Mapping' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
```

Gambar 3.31 *Script* Koneksi (*Network Mapping*) ke Wazuh Manager

9) Langkah kesembilan melakukan konfigurasi pada *shell script* `ossec.conf` wazuh *agent* untuk `agent_network_mapping` seperti pada gambar 3.32. Konfigurasi pada wazuh *agent* untuk komunikasi ke wazuh manager melibatkan konfigurasi dan pengaturan parameter didalam file ossec.conf. Pada bagian <server>, IP *address* ditentukan oleh *tag* <address>, dengan subnet 103.214.112.64/32. Kemudian untuk *port* yang digunakan untuk komunikasi dan koneksi wazuh *agent* dan wazuh manager ditentukan oleh *tag* <port>, dengan nilai 1514. Selanjutnya *protocol* yang digunakan untuk transmisi data antara wazuh *agent* dan wazuh manager adalah protocol TCP, dengan *tag* `<protocol>`. Konfigurasi yang dibuat pada wazuh *agent* ini untuk memastikan wazuh *agent* dapat mengirim data *log* dan menerima perintah dari wazuh manager melalui komunikasi infrastruktur jaringan private menuju VPS hosting untuk wazuh manager.

```
<ossec_config>
  <client>
    <server>
      <address>103.214.112.64</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>ubuntu, ubuntu20, ubuntu20.04</config-profile>
    <notify_time>10</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
    <enrollment>
      <enabled>yes</enabled>
      <agent_name>Agent_Network_Mapping</agent_name>
      <authorization_pass_path>etc/authd.pass</authorization_pass_path>
    </enrollment>
  </client>
<ossec_config>
```

Gambar 3.32 Konfigurasi Wazuh Agent Agent_Network_Mapping

3.4.4. Implementasi dan Konfigurasi Node Agent Router MikroTik

Implementasi dan konfigurasi node agent router MikroTik yang dimodelkan pada penelitian ini meliputi instalasi dan konfigurasi wazuh *agent* dengan mengumpulkan log dari router MikroTik dan mengirimkannya ke wazuh manager. Teknik yang digunakan dengan *logging* MikroTik.

Tabel 3.8. Konfigurasi Logical Wazuh Agent Router MikroTik

System and Architecture Wazuh Agent Router MikroTik			
Hostname	**IP Address**	**Agent Name**	**Groups**
MikroTik-R1	10.151.20.238/25	MikroTik (Victim)	Router
MikroTik-R2	10.151.20.239/25	MikroTik (Victim)	Router

Pada tabel 3.8, merupakan parameter konfigurasi yang akan digunakan pada router MikroTik-R1 dan MikroTik-R1. Berikut diuraikan untuk langkah melakukan konfigurasi wazuh agent router MikroTik yang diterapkan:

1. Langkah pertama untuk skenario MikroTik-R1 dan MikroTik-R2, akan dikonfigurasi *logging* pada router MikroTik untuk mengirim log ke wazuh manager menggunakan *port default* 514. Konfigurasi ini dilakukan dengan *rule* baru menambahkan aturan baru pada "`system`" dan Action ke "`remote`". Kebijakan *rule* ini dikonfigurasi untuk memastikan bahwa semua pesan log akan dikirim secara remote ke wazuh manager. Baris perintah router MikroTik-R1 dan MikroTik-R2 dikonfigurasi sebagai berikut:

```
/system logging action
set 3 bsd-syslog=yes remote=103.214.112.64 syslog-
severity=emergency
/system logging
set 0 action=remote
set 1 action=remote
set 2 action=remote
add action=remote topics=!debug
add action=remote topics=system
```

2. Langkah kedua pada wazuh server

   Proses konfigurasi pada wazuh manager dimulai dengan mengkonfigurasi `decoder` untuk format *log* yang dikirim oleh router MikroTik. `Decoder`

ini akan berfungsi untuk mengurai (parse) pesan log dari perangkat router MikroTik untuk data *log time*, *log source*, *event type* dan data lain yang relevan. Dengan konfigurasi decoder yang tepat pada wazuh server, sehingga wazuh server dapat mengelompokkan informasi yang dikirim dari perangkat router MikroTik.

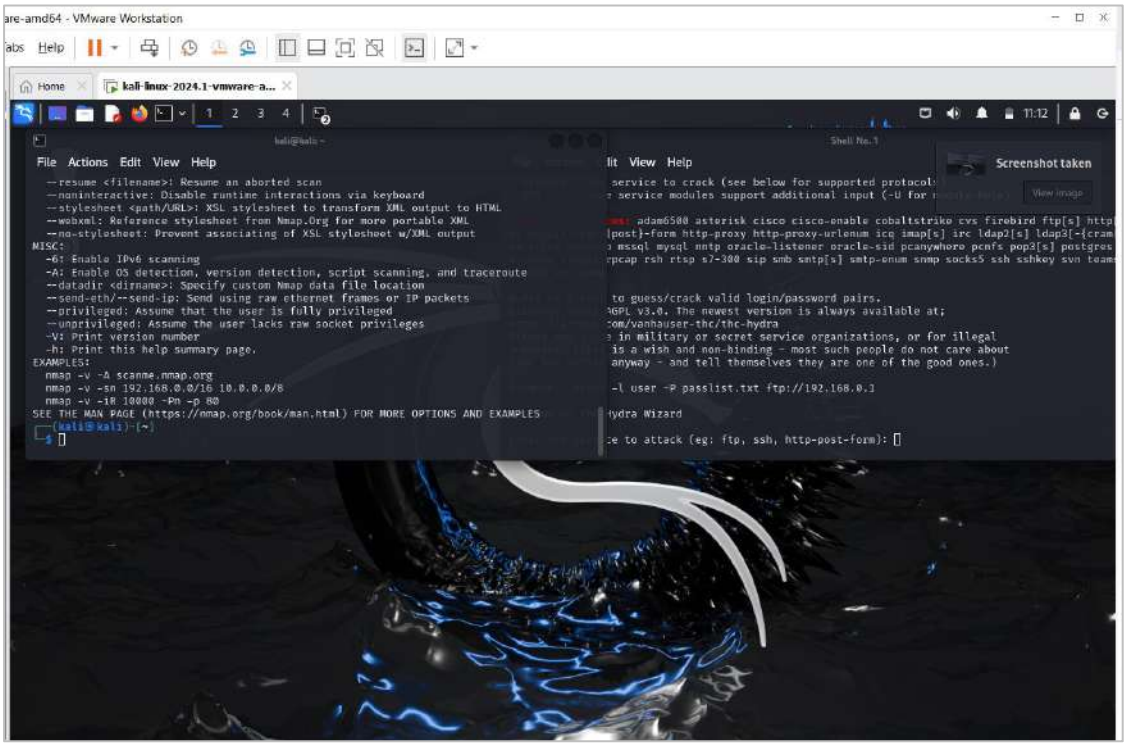
Gambar 3.33 merupakan konfigurasi decoder router MikroTik pada wazuh server untuk mengurai *log* yang diterima dari router MikroTik. Langkah pertama, buat file mikrotik_decoders.xml di direktori /var/ossec/etc/decoders/. File decoder ini mendefinisikan pola untuk mengurai log MikroTik. Decoder (mikrotik) dengan *tag* <prematch> dikonfigurasi untuk memastikan log MikroTik yang dapat diproses, diikuti oleh beberapa child decoder menggunakan pola regex untuk menerima timestamp *log*, *user login*, IP *address*, *interface*, dan *protocol*. Konfigurasi ini secara otomatis wazuh server akan mengekstrak data log dari router MikroTik, dengan aturan (*rule*) untuk mendeteksi dan merespons serangan.

```
<decoder name="mikrotik">
  <prematch>^RouterOS7.1-logs: </prematch>
</decoder>
<decoder name="mikrotik1">
  <parent>mikrotik</parent>
  <regex type="pcre2">\S+ (\w+ \d+ \d+:\d+:\d+) MikroTik user (\S+) (.*?) from (\d+.\d+.\d+.\d+) via (\w+)</regex>
  <order>logtimestamp, logged_user, action, ip_address, protocol</order>
</decoder>
<decoder name="mikrotik1">
  <parent>mikrotik</parent>
  <regex type="pcre2">\S+ (\w+ \d+ \d+:\d+:\d+) MikroTik dhcp-client on (\S+) (.*?) address (\d+.\d+.\d+.\d+)</regex>
  <order>logtimestamp, interface, action, ip_address</order>
</decoder>
<decoder name="mikrotik1">
  <parent>mikrotik</parent>
  <regex type="pcre2">\S+ (\w+ \d+ \d+:\d+:\d+) MikroTik router (\S+)</regex>
  <order>logtimestamp, action</order>
</decoder>
```

Gambar 3.33 MikroTik Decoder

3.4.5. Konfigurasi dan Implementasi *Node Attacker*

Konfigurasi penyerang yang akan dimodelkan dan diimplementasikan, dikonfigurasi pada virtual VMware. Tiga teknik serangan yang akan digunakan adalah *reconnaissance attack* (*Network Mapping*), *access attack* (*Brute Force*), dan DoS *attack* (*Slowloris*). Ketikga Teknik tersebut akan diinstal di Kali Linux OS, seperti gambar 3.34.



Gambar 3.34. VMWare Workstation dan Kali Linux OS

1. *Reconnaissance Attack* (*Network Mapping*)

   Teknik ini digunakan untuk mengidentifikasi wazuh agent pada ubuntu server dan perangkat router MikroTik, untuk menemukan *services* atau layanan yang sedang berjalan pada jaringan target. Fungsi NMAP ini akan mendapatkan informasi pada masing-masing wazuh agent system operasi dan layanan yang sedang berjalan. Kali Linux OS secara *default* sudah dilengkapi dengan Nmap, salah satu teknik serangan yang dilakukan adalah dengan mengirimkan baris perintah `sudo nmap -sS --script=vuln <IP_Address>` untuk melakukan pemindaian (*scanning*) pada masing-masing wazuh *agent* (ubuntu server) dan router MikroTik.

2. *Access Attack* (*Brute Force*)

   Tool yang digunakan untuk teknik serangan access attack adalah hydra, dengan teknik *brute force* untuk *services* autentikasi SSH dan Telnet pada router MikroTik dan service FTP pada wazuh agent (Ubuntu server). Dalam penelitian ini, hydra akan digunakan untuk menyerang *service* autentikasi

pada host target wazuh *agent*, untuk layanan SSH, FTP, dan Telnet menggunakan *wordlist* `rockyou.txt` dan `darkc0de.txt`. baris shell untuk serangan menggunakan hydra untuk wazuh agent adalah sebagai berikut:

- Serangan service SSH wazuh agent pada router MikroTik:

```
hydra -l username -P /usr/share/wordlists/rockyou.txt
ssh:// 10.151.20.252
hydra -l username -P /usr/share/wordlists/darkc0de.txt
ssh:// 10.151.20.252
```

- Service service Telnet wazuh agent pada Ubuntu Server 20.04:

```
hydra -l username -P /usr/share/wordlists/rockyou.txt
telnet:// 10.151.20.252
hydra -l username -P /usr/share/wordlists/darkc0de.txt
telnet:// 10.151.20.252
```

- Serangan service FTP wazuh agent pada Ubuntu Server 20.04:

```
hydra -l username -P /usr/share/wordlists/rockyou.txt
ftp:// 10.151.20.250
hydra -l username -P /usr/share/wordlists/darkc0de.txt
ssh:// 10.151.20.250
```

3. DoS *Attack* (*Hping3*)

Teknik serangan dengan DoSDoS attack bertujuan untuk membuat layanan atau server target tidak dapat diakses. Pemodelan dalam penelitian ini, teknik serangan DoS dilakukan untuk wazuh (Ubuntu Server 20.04) dan router MikroTik. Slowloris digunakan untuk serangan DoS, Hping3 dimodelkan dengan membukan protocol HTTP secara berkelanjutan, sehingga wazuh *agent* tidak merespons akses dan *request* dari user. Teknik untuk menjalankan serangan terhadap wazuh agent menggunakan perintah:

- Serangan service HTTP wazuh agent pada Ubuntu Server 20.04:

```
sudo hping3 -S --flood -p 80 10.151.20.238
sudo hping3 -S --flood -p 23 10.151.20.238
sudo hping3 -S --flood -p 22 10.151.20.238
```

- Serangan terhadap router MikroTik menggunakan perintah:

```
sudo hping3 -S --flood -p 80 10.151.20.238
sudo hping3 -S --flood -p 23 10.151.20.238
sudo hping3 -S --flood -p 22 10.151.20.238
```

Skenario dan ilustrasi serangan dilakukan dilingkungan infrastruktur jaringan private yang dimodelkan menggunakan OS kali linux yang diinstal di virtual hypervisor VMWare. Hasil dari serangan ini selanjutnya akan dideteksi, dianalisis dan dievaluasi pada dashboard wazuh manager yang sudah diterapkan. Dengan melakukan teknik serangan *reconnaissance attack* (*Network Mapping*), *access attack* (*Brute Force*), dan DoS *attack* (*Slowloris*), user (SOC) dapat memantau pada wazuh dashboard untuk semua log pada `alert.json` dan `archives.json` untuk tahap mitigasidari dampak yang ada dari serangan tersebut.

3.4.6. Perancangan dan Implementasi Framework iptables ipset dan Active Responses Firewall Wazuh

Pemodelan untuk infrastruktur *framework* IPTables dan *active responses* wazuh, teknik yang diimplementasikan adalah IPSet dan *firewall scripting* menggunakan *shell script*.

1. Implementasi Framework *iptables ipset*

   IPSet diterapkan dengan penanganan *file list* IP address untuk membuat *rule* `block/deny` IP address yang didata dari wazuh dashboard yang terdeteksi sebagai sumber serangan dari penyerang. Implementasi IPSet ini akan dilakukan dengan membuat *file* yang berisi daftar IP *address* yang akan diblokir. Langkah instalasi dan konfigurasi IPSet adalah sebagai berikut:

   - Instalasi dan konfigurasi ipset dengan perintah: apt install ipset
   - Langkah berikutnya membuat file di direktori: `ip_address_deny.txt` untuk daftar IP address *address* dengan *rule block/deny*. File `ip_address_deny.txt` ini akan didaftarkan source IP address dengan kriteria anomali berdasarkan hasil dari wazuh dashboard.

Kebijakan aturan untuk IPTables ini akan diimplementasikan berdasarkan dataset log wazuh dashboard dari hasil serangan *reconnaissance attack*

(*Network Mapping*), *access attack* (*Brute Force*), dan DoS *attack* (*Slowloris*) berdasarkan *source* IP *address* untuk parameter *protocol source ip address, destination ip address, source port, destination port*. Pengujian dan hasil dilakukan dengan memonitoring selama proses implementasi pada infrastruktur jaringan pada perangkat wazuh agent router MikroTik dan ubuntu server. File konfigurasi *rules* `ipset` file yang diterapkan untuk teknik mitigasi pada penelitian ini ditunjukkan pada sintaks gambar 3.35.

```
#!/bin/bash
echo "## Source-IP-Address-Drop-From-File."
# File that contains the Ips and Nets to block
FILE="ip_address_deny.txt"
ipset -N bad_hosts iphash -exist
# Flushing the set if it exists
ipset -F bad_hosts
echo "Adding Ips from $FILE to bad_hosts set:"
for ip in `cat $FILE`
do
ipset -A bad_hosts $ip
echo -n "$ip "
Done
echo -e "\nDropping with iptables... "
iptables -I INPUT -m set --match-set bad_hosts src -j DROP
echo "Done"
```

Gambar 3.35 Firewall IPTable IPSet

Sintaks *shell script* `ipset` *file* ini, akan melakukan entri secara otomatis pada server firewall iptables untuk memblokir (*deny*) semua *source* IP address yang diinput pada file dari hasil dataset wazuh dashboard.

2. Implementasi Active Responses Wazuh Manager

Pemodelan arsitektur *active response* wazuh merupakan mekanisme untuk mitigasi serangan pada perangkat wazuh agent router MikroTik dan ubuntu server secara otomatis, teknik yang digunakan adalah `firewall-drop` *Stateful Active Response*. Pada wazuh manager *active response* akan digunakan untuk merespons serangan yang diemulasikan dari *brute force*, *network mapping*, dan DoS. Serangan dengan teknik *brute force*, wazuh manager akan dikonfigurasi untuk mendeteksi serangan pada *services* protocol SSH. Penerapan emulasi serangan pada penelitian ini, akan diemulasikan dengan serangan brute force pada agent wazuh untuk perangkat router MikroTik dan ubuntu server dengan *script active response*, dengan membuat *rule* memblokir (*deny*) IP address penyerang. Ketika *rule* yang ditentukan

dengan penamaan –"SSH brute force trying to get access to the system" terdeteksi, maka modul *active response*, akan menjalankan *script* untuk memblokir IP *address* dari penyerang. Selanjutnya, setiap kali wazuh agent mendeteksi upaya serangan *brute force* pada layanan SSH, wazuh akan secara otomatis menjalankan *script* yang memblokir IP address penyerang, sehingga mencegah akses lebih lanjut dan melindungi sistem dari serangan berulang. Gambar 3.36 merupakan potongan baris *script* penerapan *firewall-drop Stateful Active Response*.

```
507  <ossec_config>
508    <global>
509      <jsonout_output>yes</jsonout_output>
510      <alerts_log>yes</alerts_log>
511      <logall>no</logall>
512      <logall_json>yes</logall_json>
513      <email_notification>no</email_notification>
514      <smtp_server>smtp.ajn.wazuh.com</smtp_server>
515      <email_from>wazuh@ajn.wazuh.com</email_from>
516      <email_to>recipient@ajn.wazuh.com</email_to>
517      <email_maxperhour>12</email_maxperhour>
518      <email_log_source>alerts.log</email_log_source>
519      <agents_disconnection_time>10m</agents_disconnection_time>
520      <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
521    </global>
522    <!--
523    <active-response>
524      <command>firewall-drop</command>
525      <location>local</location>
526      <rules_id>100200, 100201</rules_id>
527      <timeout>180</timeout>
528    </active-response>
529    -->
530    <active-response>
531      <command>firewall-drop</command>
532      <location>local</location>
533      <rules_id>5758</rules_id>
534      <timeout>180</timeout>
535    </active-response>
536  <ossec_config>
```

Gambar 3.36 *Firewall-Drop Stateless Active Response* Wazuh Manager (*Brute Force*)

Konfigurasi firewall-drop *Stateful Active Response* diatas merupakan bagian dari konfigurasi wazuh yang dijalankan pada wazuh manager pada file `/var/ossec/etc/ossec.conf`. `<active-response>`: merupakan bagian utama yang mendefenisikan tindakan (*action*) *active response* pada wazuh manager. `<command>firewall-drop</command>`: akan dikonfigurasi untuk menentukan script yang akan dijalankan untuk melakukan instruksi dengan menambahkan IP address penyerang ke daftar *firewall block*. `<location>local</location>`: Menentukan nilai *local* atau agent wazuh

lokal tempat *event alerts* terdeteksi. Artinya nilai wazuh pada wazuh manager akan menunjukkan bahwa perintah harus dijalankan pada server wazuh server. `<rules_id>5758</rules_id>`: Menentukan aturan ID yang akan menjadi *trigger* tindakan *active response* pada wazuh manager. Nilai aturan ID yang dikonfigurasi adalah ID 5758, untuk mendeteksi serangan *brute force*. `<timeout>180</timeout>`: Menentukan durasi waktu dalam detik untuk melakukan tindakan *stateful active response* sebelum dibatalkan secara otomatis. Tindakan yang akan dilakukan oleh `firewall-drop` adalah memblokir IP *address* selama 180 detik (3 *minutes*) dan secara otomatis akan aktif kembali. Konfigurasi `firewall-drop` akan memberikan pendekatan yang proaktif untuk melindungi wazuh *agent* dari penyerang dengan *script active response* wazuh, dengan memastikan bahwa tindakan mitigasi akan diambil secara otomatis saat ancaman terdeteksi pada wazuh *agent*, dan pemodelah ini memungkinkan untuk pemulihan otomatis setelah periode waktu yang ditentukan.

```
539 <group name="custom_active_response_rules,">
540   <rule id="100200" level="12">
541     <if_sid>86600</if_sid>
542     <field name="event_type">^alert$</field>
543     <match>Denial of Services (DoS) attack</match>
544     <description>GoldenEye DoS attack has been detected. </description>
545     <mitre>
546       <id>T1498</id>
547     </mitre>
548   </rule>
549
550   <rule id="100201" level="12">
551     <if_sid>86600</if_sid>
552     <field name="event_type">^alert$</field>
553     <match>Scan NMAP Scripting Engine</match>
554     <description>Nmap scripting engine detected. </description>
555     <mitre>
556       <id>T1595</id>
557     </mitre>
558   </rule>
559 </group>
```

Gambar 3.37 *Firewall-Drop Stateless Active Response* Wazuh Manager (Nmap dan DoS)

Selanjutnya pada wazuh manager, untuk *stateful active response*, digunakan untuk aturan khusus mendeteksi penggunaan Network Mapping (NMAP) *scripting engine* dan serangan DoS dari *event alert* wazuh *agent* (ubuntu server). Aturan ini akan digunakan untuk *trigger* mengeksekusi *script* `firewall-drop` pada agen wazuh yang terdeteksi serangan. Mapping (NMAP) *scripting engine*: merupakan

aturan yang dibuat dengan untuk mendeteksi penggunaan Nmap pada wazuh *agent*, dengan tujuan mengidentifikasi kerentanan *service protocol* pada wazuh *agent*.

Pada gambar 3.37 *script* yang dikonfigurasi untuk `firewall-drop` akan menambahkan IP *address* ke daftar firewall. Ketika sistem wazuh manager mendeteksi aktivitas pemindaian (*scanning*) dari Nmap dan serangan DoS melalui *alert* yang dihasilkan dari wazuh agent, aturan yang telah dikonfigurasi pada wazuh manager akan memicu `firewall-drop` melakukan *active response*. `<group name="custom_active_response_rules">`, akan menentukan group dengan aturan menjadi *trigger active response* berdasarkan serangan yang dideteksi. `<field name="event_type">^alert$</field>`, akan menentukan aturan jika tipe dari *events* merupakan *alert*. `<match>Denial of Services (DoS) attack</match>` aturan ini akan memicu ketika ada pesan yang match dengan "*Denial of Services (DoS) attack*". Selanjutnya aturan yang digunakan pada baris script gambar 3.37, untuk Nmap, komponen utama adalah `<rule id="100201" level="12">`, aturan ini akan menentukan alokasi ID 100201 dan level 12, yang menunjukkan tingkat severity level ancaman dari serangan yang dilakukan. `<field name="event_type">^alert$</field>` adalah aturan jika peristiwa serangan yang terjadi merupakan *alert*. Kemudian untuk aturan `<match>Scan NMAP Scripting Engine</match>`, menentukan bahwa aturan ini match dengan pesan `"Scan NMAP Scripting Engine"`. Aturan yang dikonfigurasi pada wazuh manager, dengan mendeteksi aktivitas yang sesuai dengan aturan yang telah ditentukan, seperti serangan DoS Nmap *scripting engine*, akan memicu *script* dan menghasilkan pemantauan pada wazuh *dashboard*.

```
562
563  <decoder name="mikrotik">
564    <prematch>^RouterOS7.1-logs: </prematch>
565  </decoder>
566
567  <decoder name="mikrotik1">
568    <parent>mikrotik</parent>
569    <regex type="pcre2">\S+ (\w+ \d+ \d+:\d+:\d+) MikroTik user (\S+) (.*?) from (\d+.\d+.\d+.\d+) via (\w+)</regex>
570    <order>logtimestamp, logged_user, action, ip_address, protocol</order>
571  </decoder>
572  <decoder name="mikrotik1">
573    <parent>mikrotik</parent>
574    <regex type="pcre2">\S+ (\w+ \d+ \d+:\d+:\d+) MikroTik router (\S+)</regex>
575    <order>logtimestamp, action</order>
576  </decoder>
```

Gambar 3.38 Konfigurasi *Decoder* Router MikroTik (`decoder.xml`)

Selanjutnya pada penelitian ini wazuh manager juga dikonfigurasi untuk aturan dan `decoder` untuk menangkan dan menampung *log* dari perangkat router MikroTik. Konfigurasi ini termasuk pembuatan *file* aturan `mikrotik_decoders.xml` untuk mendeteksi *events* untuk mengidentifikasi dan mengklasifikasikan peristiwa berdasarkan tingkat keparahan (*severity*). `Decoder` akan berfungsi memecah log menjadi bagian yang dapat dianalisis oleh wazuh. Dengan mengkonfigurasi aturan dan `decoder` wazuh manager dapat memicu peringatan yang relevan dan respons otomatis terhadap aktivitas yang terdeteksi dari *log* router MikroTik, penerapan untuk penelitian ini decoder dan rules router MikroTik akan dikonfigurasi untuk aktivitas *login user account* dan *reboot* perangkat router. Langkah untuk mengkonfigurasi `decoder` router MikroTik, file `mikrotik_decoders.xml` akan dibuat pada di direktori `/var/ossec/etc/decoders/`. Gambar 3.38 merupakan potongan *script* untuk konfigurasi `mikrotik_decoders.xml` pada perangkat router MikroTik.

Langkah selanjutnya membuat MikroTik rule dengan file `mikrotik_rules.xml` di direktori `/var/ossec/etc/rules/` seperti gambar 3.39. File `mikrotik_rules.xml` berisi *rule* untuk mendefenisikan *active responses* wazuh server dari berbagai *events log* yang dikirim oleh perangkat dari MikroTik.

```
<group name="Mikrotik,">
  <rule id="110000" level="0">
    <decoded_as>mikrotik</decoded_as>
    <description>Mikrotik-Event</description>
  </rule>
  <rule id="110001" level="5">
    <if_sid>110000</if_sid>
    <match>dhcp-client on ether</match>
    <description>MikroTik dhcp-client received an IP address $(ip_address)</description>
  </rule>
  <rule id="110002" level="5">
    <if_sid>110000</if_sid>
    <match>rebooted</match>
    <description>MikroTik router rebooted</description>
  </rule>
  <rule id="110003" level="5">
    <if_sid>110000</if_sid>
    <match>logged out from</match>
    <description>MikroTik user logged out via $(protocol)</description>
  </rule>
  <rule id="110004" level="5">
    <if_sid>110000</if_sid>
    <match>logged in from</match>
    <description>MikroTik user logged in from $(ip_address) via $(protocol)</description>
  </rule>
</group>
```

Gambar 3.39 Konfigurasi MikroTik *Rules*

Konfigurasi dilakukan dengan menambahkan `rule` ke file `mikrotik_rules.xml`, dengan beberapa ID sebagai berikut:

1) `Rule ID 110000` akan bertindak sebagai rule dasar sebagai pemicu setiap wazuh server mendeteksi events log diperangkat router MikroTik.
2) `Rule ID 110001` berfungsi untuk mendeteksi dari perangkat router MikroTik untuk IP address yang menggunakan *protocol* DHCP-CLIENT.
3) `Rule ID 110002` akan memicu wazuh server mendeteksi perangkat MikroTik ketika terdapat *events* `system reboot`.
4) `Rule ID 110003` dikonfigurasi untuk dapat mendeteksi ketika user melakukan *logout* dari router MikroTik.

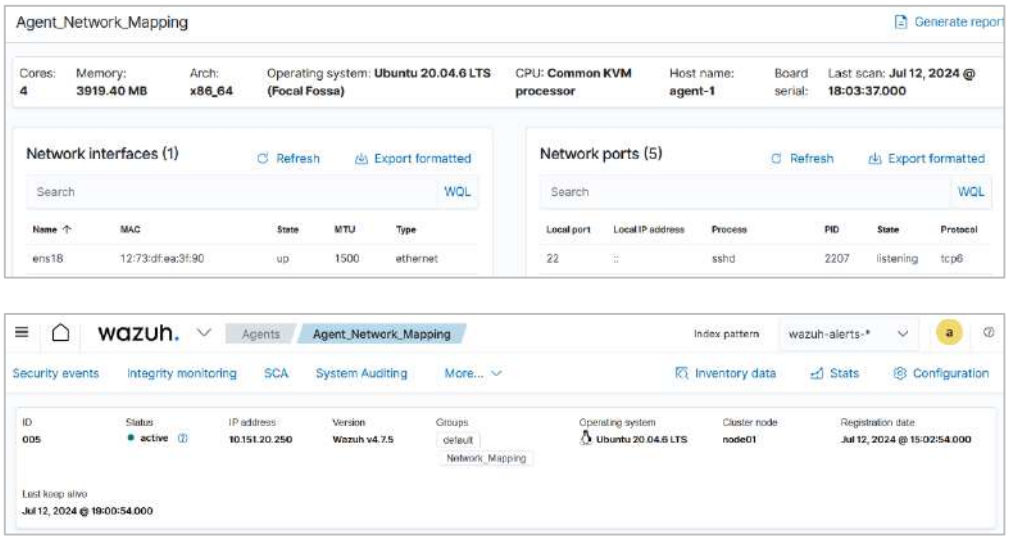
`Rule ID 110004` akan memicu ketika user melakukan *login* pada router MikroTik menggunakan IP *address* dan protocol tertentu.

3.5.Tahap Operasi (Operasi dan Eksekusi Sistem)

Tahap operasional penelitian ini adalah tahap dimana sistem yang telah diimplementasikan dan dirancang akan digunakan dan diuji dengan kondisi nyata. Fokus pada tahap ini pengujian dilakukan dengan serangan terhadap sistem pada wazuh agent untuk memastikan bahwa semua pemodelah dan mekanisme pertahanan yang telah diimplementasikan pada infrastruktur jariangan dapat berfungsi dan bekerja, termasuk teknik serangan yang akan dilakukan adalah *reconnaissance attack* (Nmap), *access attack* (*brute force*), dan DoS *attack*.

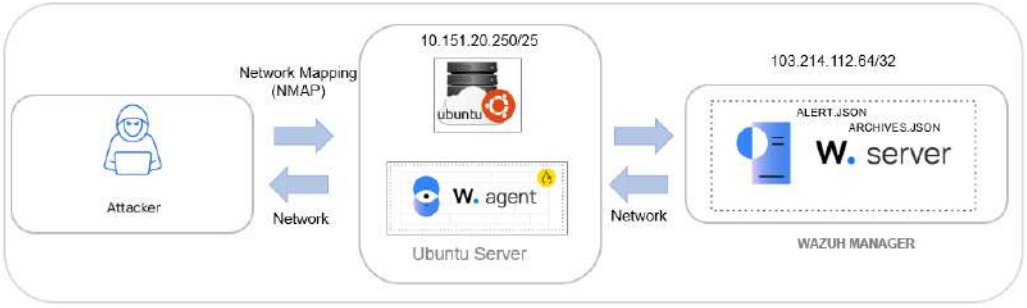
3.5.1. Pengujian Serangan Network Mapping pada Perangkat Wazuh Agent (Ubuntu Server)

Gambar 3.40 merupakan *inventory* untuk wazuh agent yang menggunakan Operating system Ubuntu 20.04.6 LTS (Focal Fossa). *Inventory* ini mencakup berbagai komponen yang terdapat pada agent wazuh, termasuk versi sistem operasi, *hardware, software,* IP *address* yang terinstal, serta konfigurasi jaringan.



Gambar 3.40 Inventory Agent Wazuh

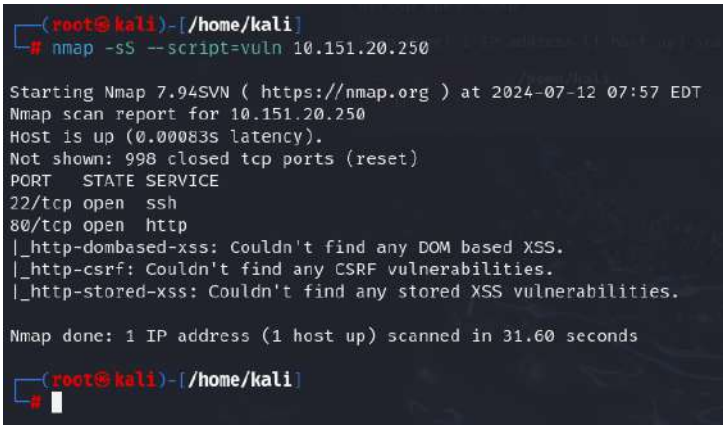
Gambar 3.41 menggambarkan ilustrasi dan skenario pengujian dengan *network_mapping* ke perangkat ubuntu server (wazuh agent).



Gambar 3.41 Ilustrasi Serangan Attacker (*Network Mapping*) menuju Wazuh Agent

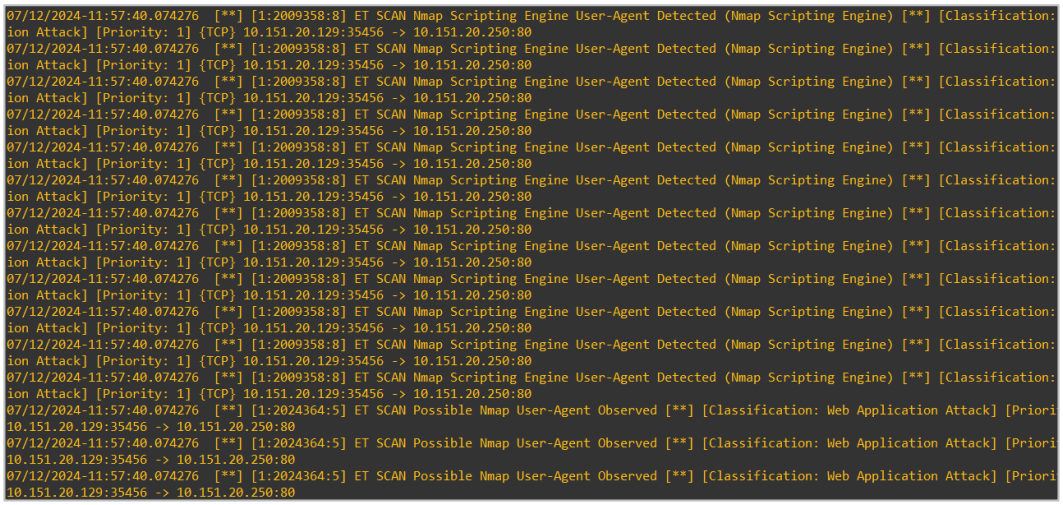
Dalam skenario gambar 3.41, penyerang (*attacker*) menggunakan subnet IP *address* 10.151.20.129/25 menggunakan Nmap, dimodelkan melakukan pemindaian (*scanning*) pada sistem di jaringan target (*agent* wazuh). Agent wazuh terhubung ke sistem wazuh manager dengan alamat IP 103.214.112.64/32. Selanjutnya ketika wazuh agent mendeteksi pemindaian Nmap, wazuh *agent* akan mengirimkan data *log* dan wazuh server pada file `archives.json` dan `alert.json` akan menyimpan dan memproses *log* untuk dianalisis dan menampilkannya pada wazuh *dashboard*. Serangan Nmap akan dilakukan dari kali

linux OS menggunakan perintah `sudo nmap -sS --script=vuln 10.151.20.250` yang ditujukan pada wazuh agent, seperti pada gambar 3.42.



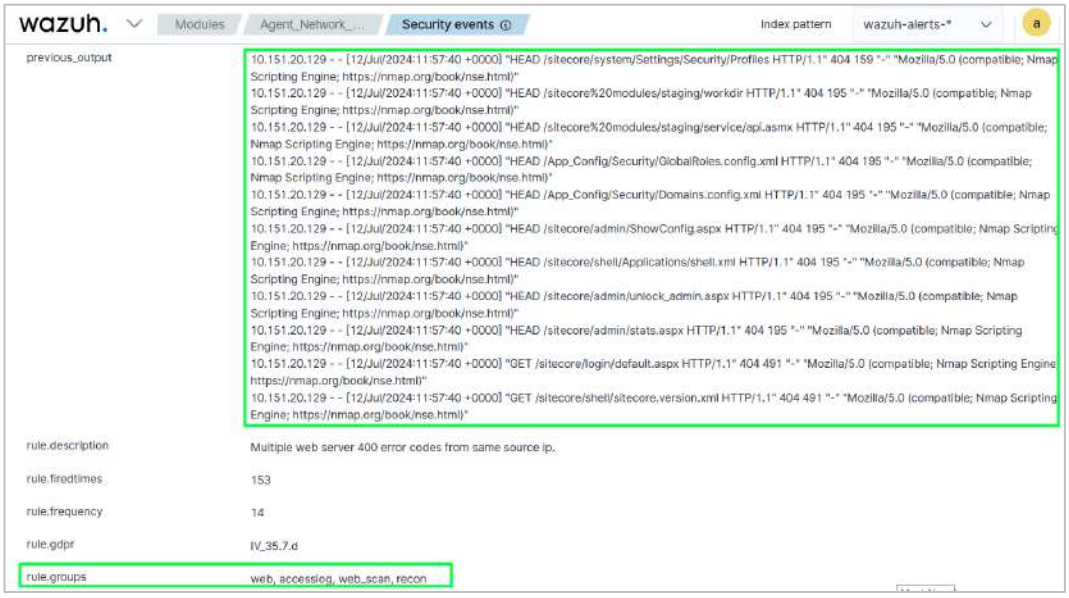
Gambar 3.42 Pemindaian Attacker (Network Mapping) menuju Wazuh Agent

Gambar 3.42 merupakan skenario, yang digunakan penyerang menggunakan Nmap dengan opsi `-sS` dalam melakukan *scanning port* SYN, dan *script* `--script=vuln` untuk mendeteksi kerentanan (*vulnerability*) ke wazuh agent (IP 10.151.20.250). Hasil dari scnning yang dilakukan, menunjukkan terdapat dua port dengan *status open* ditemukan (port 22/tcp untuk *services* ssh dan port 80/tcp untuk *service* http. Dari hasil *scanning* ini terdapat ada dua port dengan status *open*, yang dapat menjadi potensi serangan. Gambar 3.43 merupakan *log* yang dihasilkan dari wazuh agent.



Gambar 3.43 Deteksi Log Wazuh Agent

Terlihat pada tanggal 12 Juli 2024, sejumlah *log* dari wazuh *agent* menunjukkan adanya aktivitas *scanning* menggunakan Nmap dari IP address 10.151.20.129. Berdasarkan *log* `alert.json`. Nmap mendeteksi pemindaian jaringan terhadap IP *address* 10.151.20.250. Entri *log* mencatat deteksi `ET SCAN Nmap Scripting Engine User-Agent`, notifikasi ini mengindikasikan penggunaan Nmap *scripting engine* dalam serangan tersebut. Entri *log* ini akan diklasifikasikan sebagai serangan terhadap aplikasi *web* dengan prioritas tinggi (*Priority*: 1). Dari hasil log ini dapat disimpulkan bahwa penuerang mencoba mengidentifikasi kerentanan (*vulnerability*) pada wazuh agent dengan pemindaian Nmap. Hasil dari deteksi ini sangat penting, untuk mengindikasikan adanya usaha eksploitasi dari penyerang terhadap *service* yang berjalan pada *port* 80 (http). Gambar 3.44 merupakan wazuh manager akan menerima dan menganalisis log yang dikirimkan dari wazuh agent secara otomatis, dan akan mengidentifikasi ancaman yang terjadi dan melakukan *active responses* yang tepat untuk melindungi wazuh *agent* dari potensi serangan lebih lanjut. Setiap aktivitas yang terjadi dengan skema pemindaian yang terdeteksi penggunaan dengan Nmap akan dicatat sebagai peristiwa pemindaian dengan signature ID spesifik yaitu *et scan nmap scripting engine user-agent detected*.



Gambar 3.44 *Alert* serangan yang terdeteksi pada wazuh manager

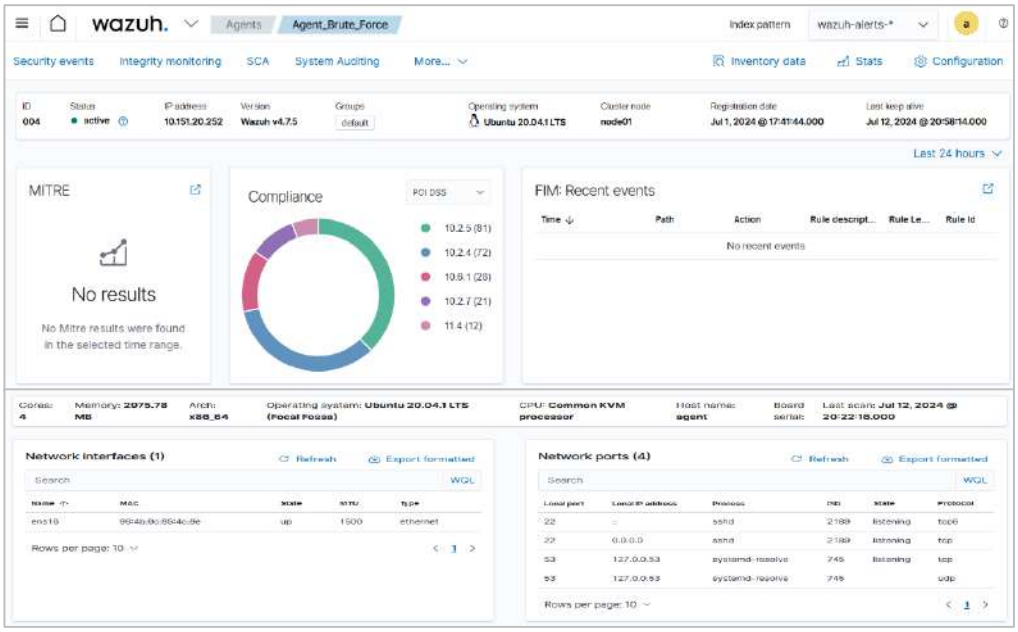
Gambar 3.45 merupakan wazuh dashboard yang menunjukkan hasil serangan Nmap yang terdeteksi oleh *agent* wazuh. Event pada wazuh *dashboard* akan muncul sebagai *events* yang memuat sejumlah informasi untuk aktivitas serangan. Dalam *event* yang ada pada wazuh *dashboard*, informasi seperti *timestamp* menunjukkan waktu tepat ketika aktivitas terdeteksi, sumber IP *address* (IP *address* sumber dari mana serangan berasal), dan IP *destination* (IP *address* tujuan target) akan dicantumkan.

Gambar 3.45 Grafik Serangan pada Wazuh Dashboard

3.5.2. Pengujian Serangan *Brute Force* pada Perangkat Wazuh Agent (Ubuntu Server)

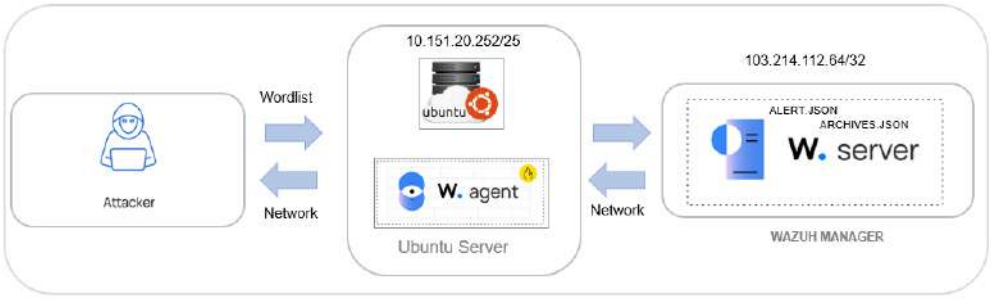
Gambar 3.46 merupakan *inventory* untuk wazuh agent, untuk serangan *brute force* yang menggunakan Operating system Ubuntu 20.04.6 LTS (Focal Fossa).

Inventory ini mencakup berbagai komponen yang terdapat pada agent wazuh, termasuk versi sistem operasi, *hardware*, *software*, IP *address* yang terinstal, serta konfigurasi jaringan.



Gambar 3.46 *Inventory Agent* Wazuh *Brute Force*

Dalam skenario ini, penyerang (*attacker*) menggunakan subnet IP *address* 10.151.20.129/25 menggunakan hydra. Agent wazuh terhubung ke sistem wazuh manager dengan alamat IP 103.214.112.64/32. Selanjutnya ketika wazuh *agent* mendeteksi serangan *brute force* dengan hydra, wazuh *agent* akan mengirimkan data *log* dan wazuh server pada file `archives.json` dan `alert.json` akan menyimpan dan memproses *log* untuk dianalisis dan menampilkannya pada wazuh *dashboard*.

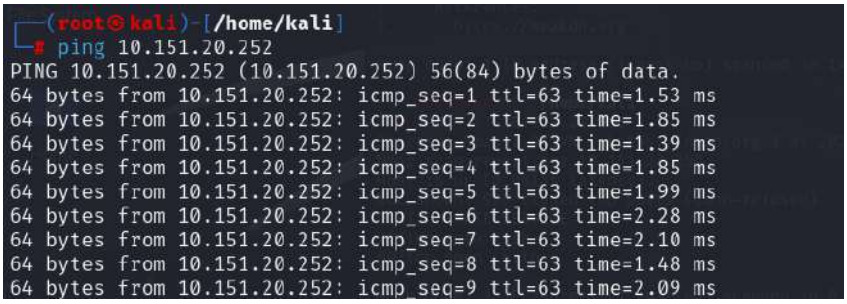


Gambar 3.47 Serangan *Attacker* (*Brute Force*) menuju Wazuh *Agent*

Gambar 3.47 menggambarkan ilustrasi dan scenario pengujian dengan *network_mapping* ke perangkat ubuntu server (wazuh *agent*). Pengujian scenario serangan ini, penyerang (*attacker*) menggunakan *wordlist* `rockyou.txt` dan `darkc0de.txt`, yang merupakan daftar kata yang digunakan untuk uji penetrasi dengan mencoba berbagai kombinasi kredensial *username* dan *password*. Tujuannya adalah mendapatkan akes keperangkat wazuh agent.

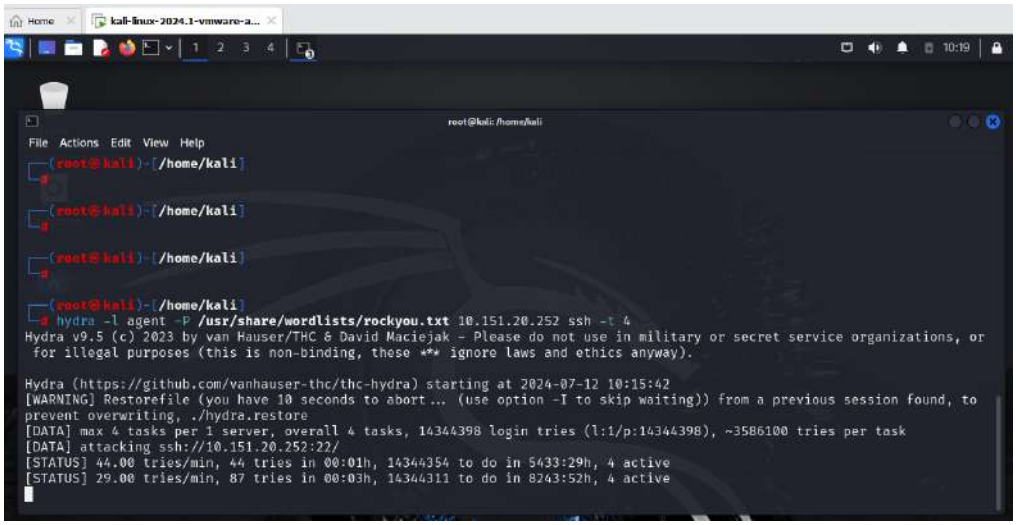
Pengujian serangan ini ditujukan ke wazuh *agent* yang menggunakan ubuntu server dan sudah terdapat kredensial *username* dan *password* dan menggunakan subnet IP *address* 10.151.20.252/25. Wazuh agent ini terhubung secara remote ke jaringan public wazuh server menggunakan IP *address* 103.214.112.64/32. Selanjutnya ketika wazuh agent mendeteksi serangan *brute force*, wazuh agent akan mengirimkan data *log* dan wazuh server pada file `archives.json` dan `alert.json` akan menyimpan log untuk diproses dan dianalisis dan menampilkannya pada wazuh dashboard. Ketika serangan *brute force* dilakukan dengan percobaan login yang berulang-ulang gagal terdeteksi oleh wazuh server, maka aturan dan *active responses* yang sudah dikonfigurasi akan memicu pemblokiran IP address penyerang. Teknik ini dikonfigurasi untuk menghentikan serangan sebelum berhasil mengkases sistem wazuh agent yang menjadi target serangan. Gambar 3.46 merupakan alur dan yang ilustrasi untuk konektivitas dan data yang terjadi selama pengujian, yang mencakup penyerang yang mencoba berbagai kombinasi login, menggunakan *wordlist*, kemudian wazuh akan memonitor aktivitas tersebut, serta melakukan analisis serta mengambil tindakan pencegahan.

Tahap melakukan serangan untuk *protocol* ssh pada wazuh *agent* menggunakan *wordlist*, langkah pertama, serangan akan dilakukan dari virtual kali linux (IP address: 10.151.21.129) menuju wazuh *agent* yang menjadi target (IP: 10.151.21.252). Selanjutnya memastikan adanya konektivitas antara penyerang dan wazuh agent yang menjadi target, dengan menguji koneksi menggunakan perintah seperti `ping` seperti gambar 3.48.



Gambar 3.48. Pengujian konektivitas wazuh agent dari Kali Linux

Tahap melakukan serangan untuk *protocol* ssh pada wazuh *agent* menggunakan *wordlist*, langkah pertama, serangan akan dilakukan dari virtual kali linux (IP address: 10.151.21.129) menuju wazuh *agent* yang menjadi target (IP: 10.151.21.252). Selanjutnya memastikan adanya konektivitas antara penyerang dan wazuh agent yang menjadi target, dengan menguji koneksi menggunakan perintah seperti `ping` seperti gambar 3.47.

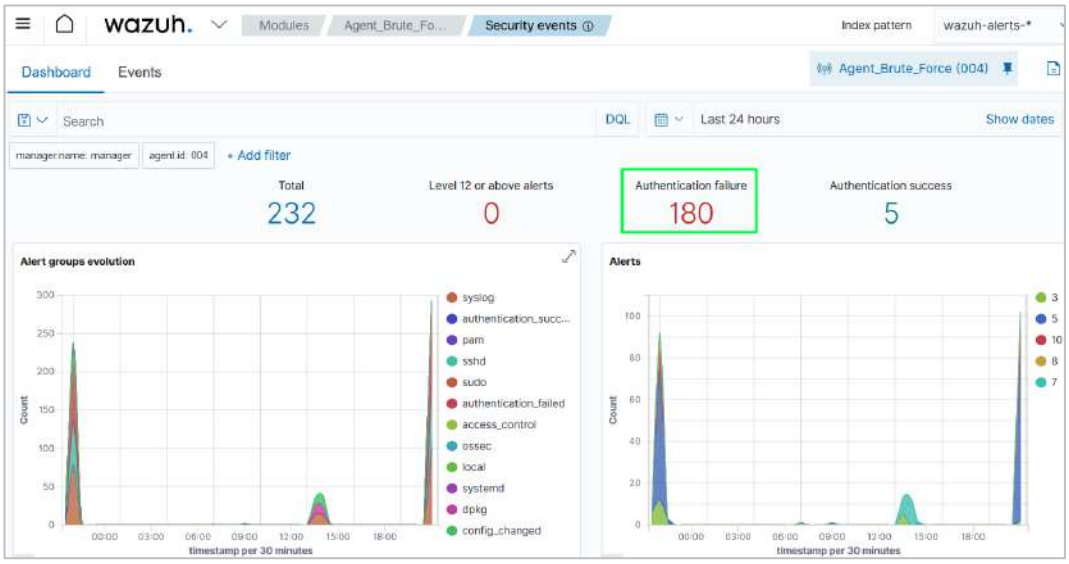


Gambar 3.48 Serangan Brute Force pada Wazuh Agent

Gambar 49 merupakan aktivitas serangan *brute force*, yang dilakukan dari kali linux OS menggunakan hydra untuk mencoba memecahkan kredensial kata sandi login SSH pada alamat IP 10.151.20.252 dengan menggunakan username `"agent"`. pada *wordlist* `"rockyou.txt"`. Hydra memproses serangan pada tanggal 12 Juli 2024, dengan mencoba sebanyak mungkin kombinasi kredensial *username* dan *password* yang tercantum dalam file `rockyou.txt`. Proses serangan dengan menjalankan hingga 4 tugas secara paralel untuk mempercepat

proses, hydra berusaha menemukan kata sandi yang benar untuk username "`agent`" pada wazuh agent (ubuntu server).

Setiap beberapa menit, hydra akan memberitahukan *update* status terbaru untuk jumlah percobaan serangan kredensial yang telah dilakukan dan jumlah percobaan serangan kredensial yang masih tersisa. Dalam beberapa menit *hydra* telah mencoba 87 kombinasi *password* dari total 14.344.398 kombinasi. Update percobaan serangan yang dilaporkan 29-44 percobaan per menit. Gambar 50 merupakan monitoring pada wazuh dashboard. Notifikasi *180 authentication failure* mengindikasikan bahwa terdapat 180 upaya serangan untuk autentikasi yang gagal pada wazuh *agent*. Notifikasi ini menunjukkan bahwa terdapat upaya serangan dan percobaan *brute force* menggunakan *wordlist*, dengan percobaan login yang tidak sah yang mencoba mengakses sistem operasi wazuh *agent* menggunakan kredensial *password* yang salah. Setiap ada percobaan login yang gagal, wazuh manager akan mencatat dan mengumpulkannya sebagai *event*, yang kemudian dianalisis dan dilaporkan pada wazuh *dashboard*.



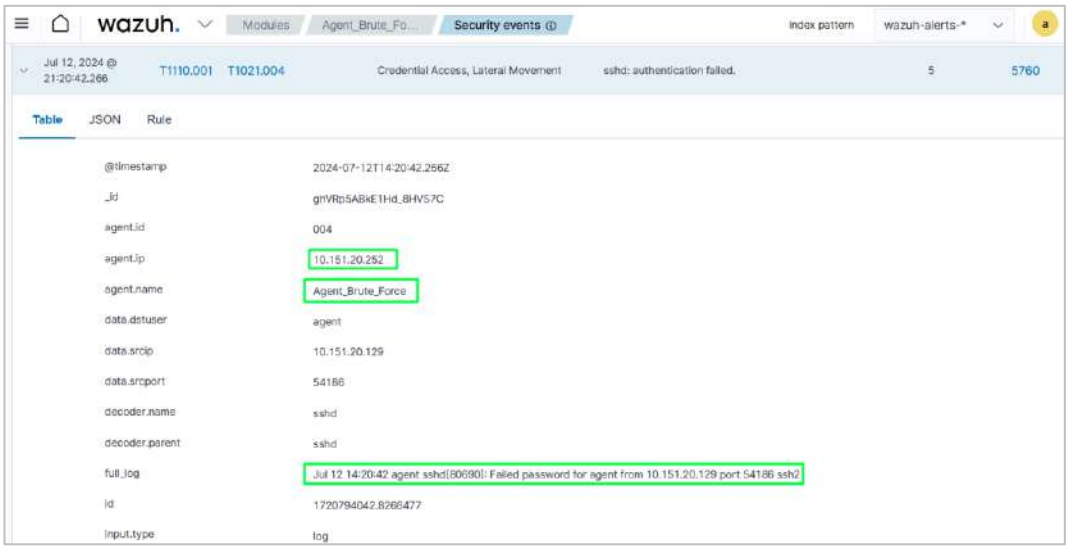
Gambar 3.49 Upaya Autentikasi Gagal dari Serangan Brute Force

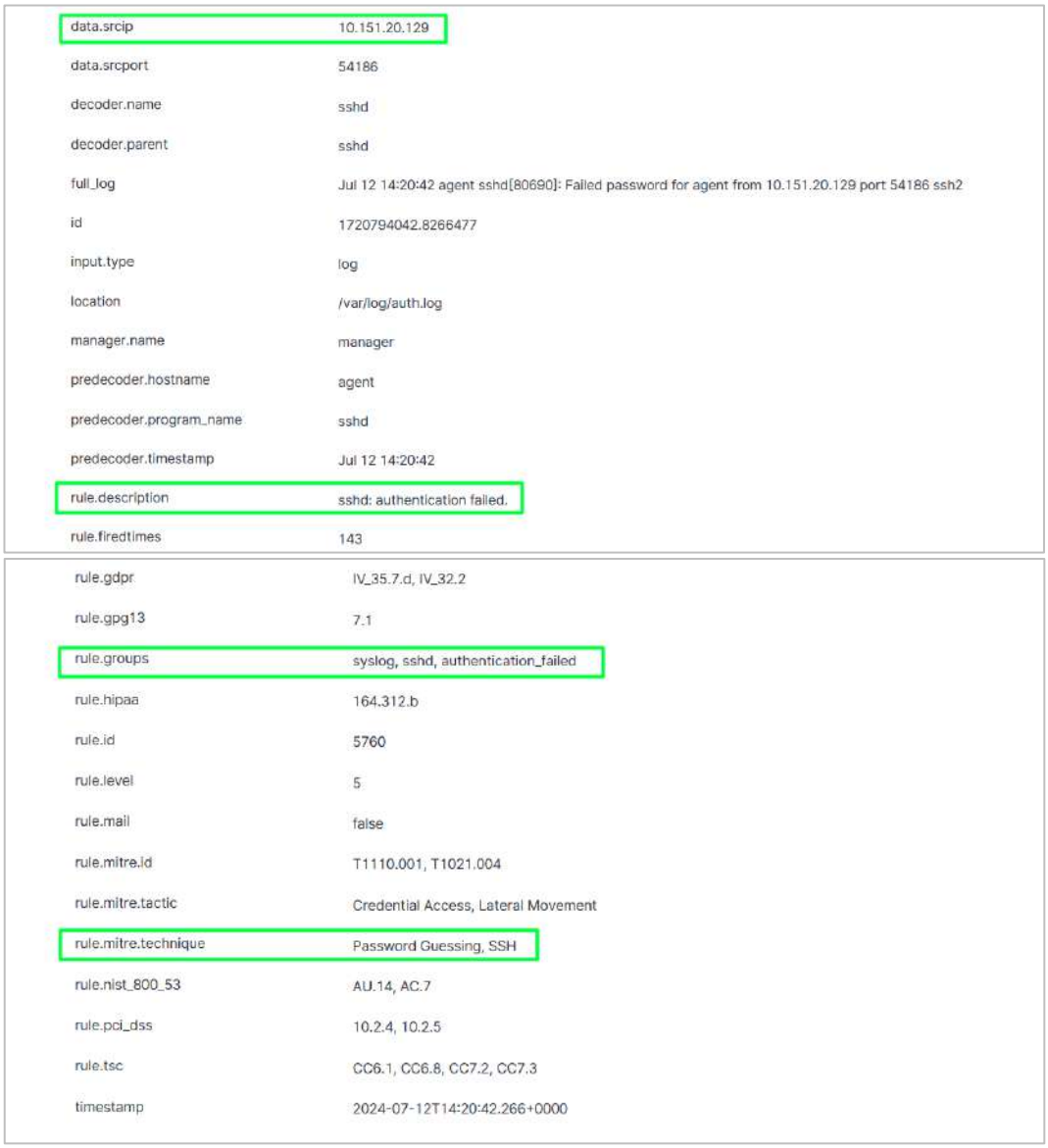
Pada gambar 3.50 menunjukkan pada tanggal 12 Juli 2024 pukul 21:20:42, wazuh dashboard mencatat *events* yang dikategorikan sebagai "*Credential Access, Lateral Movement*" di dashboard monitoring. Kejadian ini menunjukkan karena

adanya percobaan autentikasi yang gagal pada layanan sshd (*secure shell daemon*). Pesan *log* tersebut menunjukkan telah terjadi upaya autentikasi yang tidak sukses, dan mengindikasikan ada *user* yang berupaya untuk masuk ke sistem wazuh dashboard menggunakan kredensial yang tidak sah dan tidak valid.

Gambar 3.50. Monitoring Wazuh Dashboard (Serangan *Brute Force*)

Gambar 3.51 merupakan wazuh *dashboard* yang menunjukkan hasil serangan *brute force* yang terdeteksi oleh agent wazuh. Event pada wazuh *dashboard* akan muncul sebagai events yang memuat sejumlah informasi untuk aktivitas serangan. Dalam *event* yang ada pada wazuh *dashboard*, informasi seperti *timestamp* menunjukkan waktu tepat ketika aktivitas terdeteksi, sumber IP *address* (IP *address* sumber dari mana serangan berasal), dan IP *destination* (IP *address* tujuan target) akan dicantumkan.

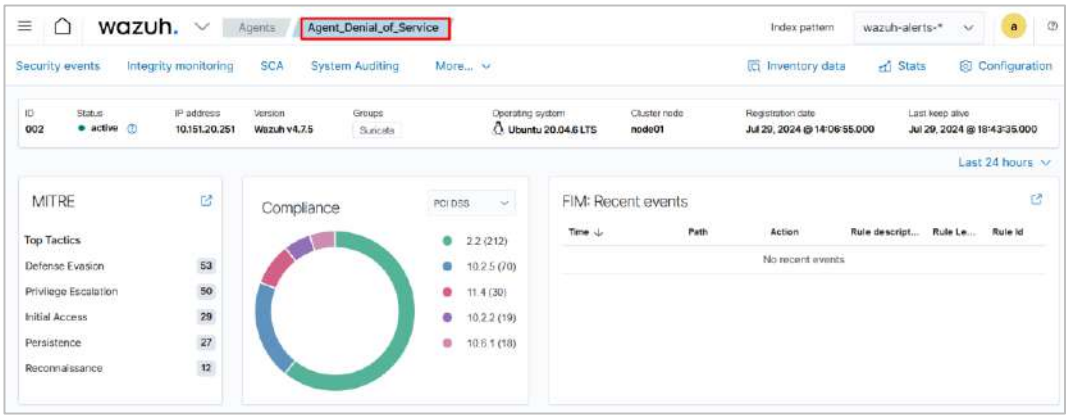




Gambar 3.51. Monitoring *Events* Wazuh Dashboard (Serangan *Brute Force*)

3.5.3. Pengujian Serangan *Denial of Service* (DoS) pada Perangkat Wazuh Agent (Ubuntu Server)

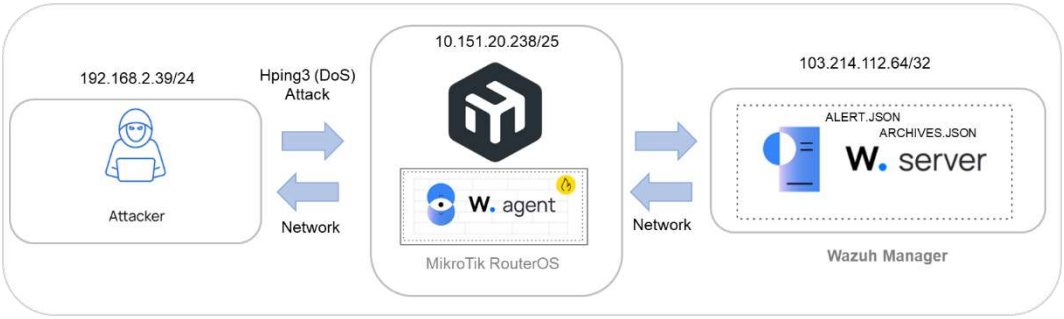
Gambar 3.52 merupakan *inventory* untuk wazuh *agent* (DoS), untuk serangan *Denial of Service* (DoS) menggunakan sistem operasi Ubuntu Server 20.04.6 LTS (Focal Fossa). Inventory ini mencakup berbagai komponen yang terdapat pada *agent* wazuh, termasuk versi sistem operasi, *hardware*, *software*, IP *address* yang terinstal, serta konfigurasi jaringan.



Gambar 3.52 *Inventory Agent* Wazuh *Denial of Service* (DoS)

3.5.4. Pengujian Serangan Denial of Service (DoS) pada Perangkat Wazuh Agent (MikroTik RouterOS)

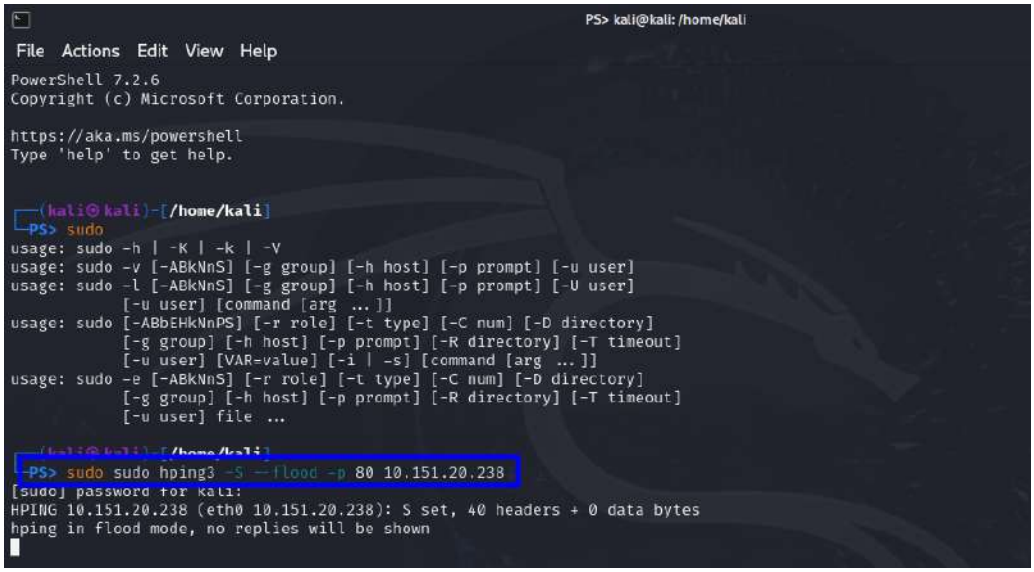
Pengujian serangan Denial of Service (DoS) pada perangkat MikroTik RouterOS (wazuh agent) bertujuan untuk mengevaluasi kemampuan wazuh dalam mendeteksi dan merespons serangan DoS. Dalam pengujian ini, `hping3` digunakan untuk melakukan serangan DoS dari mesin virtual yang diinstal di VMware.Topologi jaringan yang digunakan dalam pengujian ini seperti pada gambar 3.53.



Gambar 3.53 Serangan *Attacker* (*Brute Force*) menuju Wazuh *Agent*

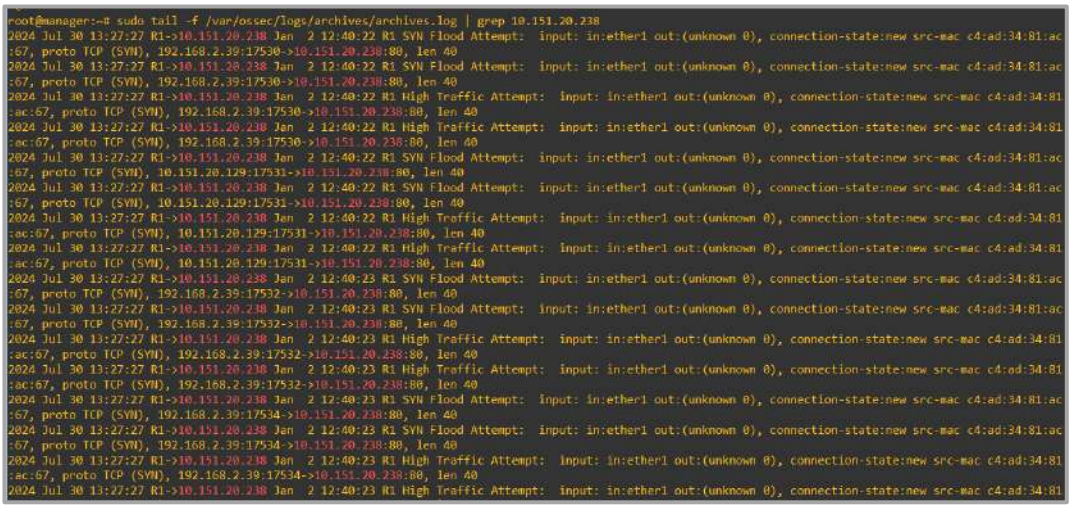
Attacker menggunakan hping3 untuk melakukan serangan DoS. Wazuh agent menggunakan rsyslog pada ubuntu server 20.04 untuk dapat terintegrasi dengan mikrotik. Topologi pengujian menunjukkan skenario serangan Denial of Service (DoS) ke perangkat MikroTik RouterOS yang berfungsi sebagai wazuh agent. Dalam skenario emulasi ini, penyerang menggunakan `hping3` yang diinstal pada

kali linux untuk melakukan serangan DoS. Penyerang terhubung ke network 10.151.20.128/29 dan mengirimkan serangan DoS ke MikroTik RouterOS dan bertujuan membanjiri (*flooding*) perangkat mikrotik dengan lalu lintas yang berlebihan sehingga menyebabkan gangguan service dan perangkat tidak dapat diakses.



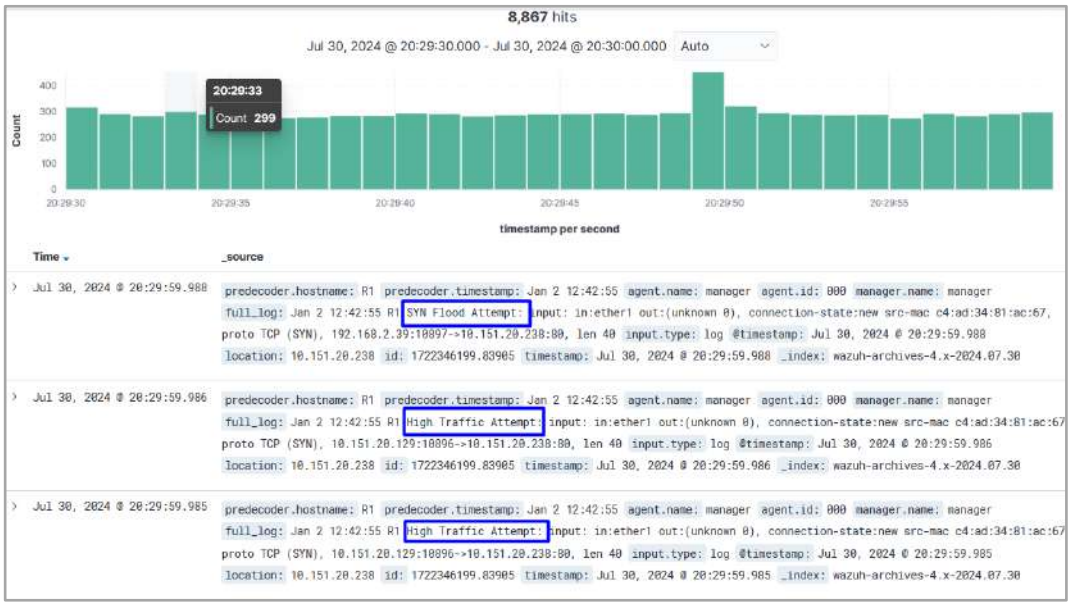
Gambar 3.54 Serangan *Denial of Service* pada Wazuh *Agent* (MikroTik RouterOS)

MikroTik RouterOS sebagai wazuh agent berada di dalam subnet dengan IP address 10.151.20.238/25. Router akan menerima serangan DoS dari penyerang (*attacker*) dan mencatat kejadian `log-prefix="SYN Flood Attempt` sebagai log, kemudian wazuh server akan mendeteksi untuk analisis lebih lanjut. Wazuh server berada di jaringan dengan IP address103.214.112.64/32. Pada konfigurasi wazuh manager, log yang diterima dari perangkat MikroTik RouterOS dikumpulkan dan dianalisis untuk mendeteksi pola serangan. Ketika serangan `log-prefix="SYN Flood Attempt` terdeteksi, wazuh server mencatat detail serangan dalam format JSON pada file `archives.json` dan `alert.json`. Pada Gambar 3.55, pada log wazuh manager berhasil mendeteksi serangan `SYN Flood` dengan menghasilkan log yang menunjukkan adanya upaya `SYN Flood` dan lalu lintas tinggi. Berikut merupakan log output yang dihasilkan wazuh manager.



Gambar 3.55 Log Wazuh Manager Mendeteksi *log-prefix=SYN Flood Attempt*

Pada gambar 3.55 merupakan salah satu *log* yang menunjukkan adanya upaya serangan `SYN Flood` dari IP address penyerang yaitu 192.168.2.39 menuju IP Address target wazuh agent (10.151.20.238) pada *service port* 80, yang dideteksi oleh wazuh sebagai lalu lintas yang tinggi dan upaya serangan `SYN Flood`.



Gambar 3.56 Statistik Serangan Denial of Service (DoS) pada Wazuh Manager

Gambar 3.56 merupakan hasil serangan Denial of Service (DoS) pada wazuh manager, dengan menunjukkan sejumlah log dan statistik dalam rentang waktu tertentu dan mencatat aktivitas serangan pada perangkat MikroTik. Statistik

serangan pada grafik gambar 3.56 menunjukkan jumlah hit per detik yang diterima oleh wazuh manager selama periode waktu tertentu pada tanggal 30 Juli 2024, antara pukul 20:29:30 sampai 20:30:00 sebanyak 8.867, dan dengan jumlah 299 hit per detik. Jumlah ini menunjukkan lonjakan lalu lintas (*traffic*) yang diakibatkan oleh serangan DoS. Log detail serangan terdapat beberapa entri log yang menunjukkan serangan *syn flood* dan traffic yang tinggi.

Tabel 3.9 merupakan detail hasil log serangan pada wazuh manager pada perangkat MikroTik RouterOS.

SYN Flood Attempt dan High Traffic Attempt					
Waktu	Host	MAC Sumber	Protocol	Sumber IP	Target IP
30 Juli 2024 pukul 20:29:59	R1	C4:AD:34:81:AC:67	TCP (SYN)	192.168.2.39:18997	10.151.20.238:80

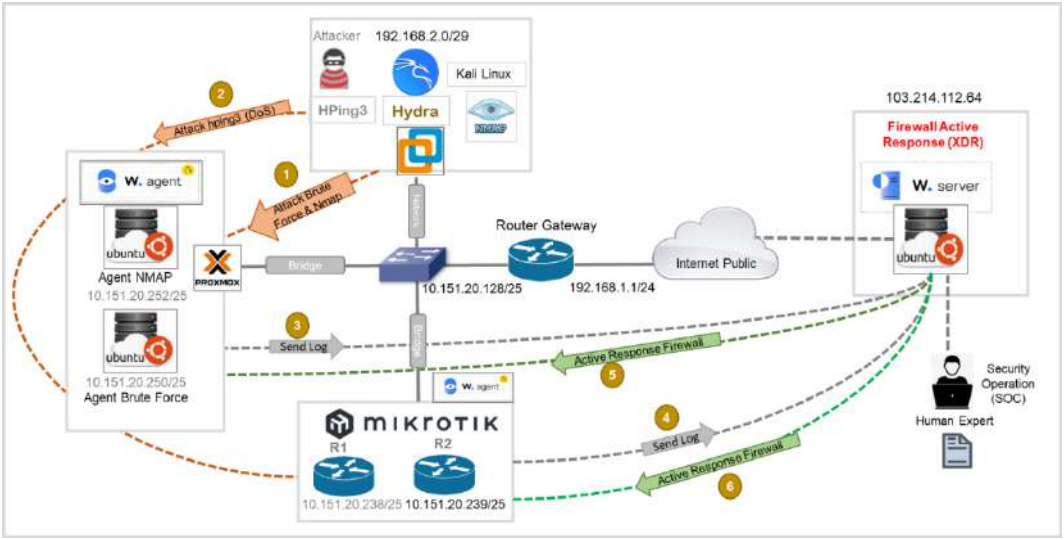
SYN *flood attempt*, merupakan log serangan SYN Flood, di mana penyerang mengirimkan sejumlah besar paket `SYN` dengan tujuan membanjiri sumber daya perangkat MikroTik (wazuh agent) yang bertujuan menghabiskan sumber daya sistem berupa CPU dan memory sehingga layanan menjadi tidak tersedia atau tidak dapat diakses. High traffic attempt, merupakan log yang menunjukkan adanya lalu lintas tinggi (*high traffic*) ke perangkat MikroTik dan dicatat oleh wazuh manager, *high traffic* ini mengindikasikan bahwa perangkat MikroTik sedang dibanjiri dengan lalu lintas yang sangat besar.

3.6. Tahap Optimasi (Evaluasi)

Tahap optimalisasi penelitian ini berfokus pada peningkatan efektivitas dan efisiensi sistem keamanan dari infrastruktur jaringan yang telah diimplementasikan. Adapaun langkah yang dilakukan meliputi dua aspek utama yaitu konfigurasi dan evaluasi optimasi firewall serta *active responses* wazuh XDR, dan evaluasi performa sumber daya CPU dan memory pada perangkat server dan router sebelum dan setelah terjadi serangan.

3.6.1. Konfigurasi dan Evaluasi Optimasi Firewall Active Responses Wazuh XDR

Gambar 3.57 merupakan implementasi infrastruktur topologi pada penelitian ini menunjukkan bagaimana integrasi *active responses* wazuh XDR dengan wazuh agent pada masing-masing perangkat *endpoint* (server dan router), dapat mendeteksi dan merespons serangan dari kali linux (hping3, hydra dan *brute force*) secara efektif. Konfigurasi pada infrastruktur topologi ini memungkinkan untuk mengevaluasi efektivitas dari *firewall active responses* wazuh XDR dalam memitigasi berbagai jenis serangan, serta mengukur performa sistem (router dan server) dalam kondisi normal dan saat terjadi serangan.



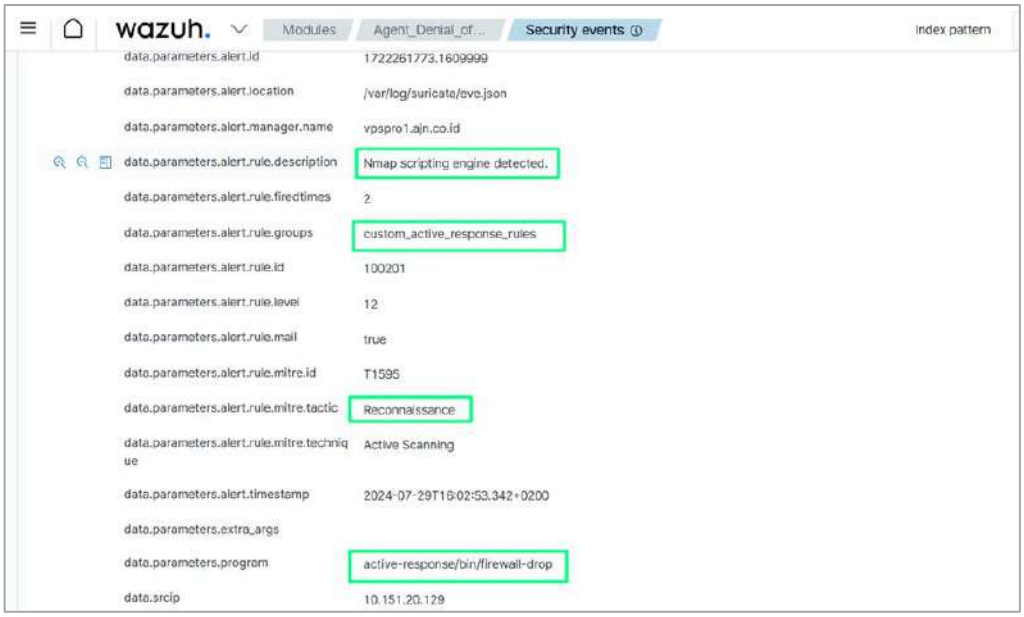
Gambar 3.57 Topologi Optimasi *Firewall Active Responses* Wazuh XDR

Topologi gambar 3.57 menunjukkan implementasi sistem keamanan infrastruktur jaringan menggunakan wazuh XDR (*Extended Detection and Response*) dengan *active responses*. Log yang dihasilkan dari aktivitas scanning Nmap ini akan dikirimkan dari wazuh agent ke wazuh server (103.214.112.64/32). Pengiriman log ini melalui router gateway yang berfungsi sebagai penghubung antara jaringan internal dan wazuh server yang berada di *public cloud*. Wazuh server akan menerima log dan melakukan analisis berdasarkan aturan dan *decoder* yang telah dikonfigurasi. Analisis ini memungkinkan wazuh server untuk mendeteksi pola aktivitas mencurigakan seperti scanning Nmap, serangan *brute*

force dan serangan Denial of Service (DoS). Berdasarkan hasil analisis, wazuh server mendeteksi adanya scanning Nmap dari alamat IP attacker (192.168.2.39).

3.6.2. Evaluasi Optimasi Firewall Active Responses Wazuh XDR (Scanning NMAP)

Berdasarkan gambar 3.58, dapat disimpulkan bahwa wazuh manager berhasil menjalankan fungsinya sebagai sistem deteksi intrusi dan *active response* XDR. *Index pattern* deteksi serangan wazuh Manager berhasil mendeteksi adanya aktivitas scanning pada perangkat server (*wazuh agent*) yang dilakukan dengan *network mapping* (nmap), dengan nilai pada `data.parameters.alert.rule.description : Nmap scripting engine detected`. *Active responses* setelah terdeteksi serangan, wazuh manager secara otomatis menjalankan *active responses*, yang sudah dikonfigurasi sebelumnya untuk memblokir akses dari IP *address* sumber serangan. Hal ini terlihat pada nilai `data.parameters.program` yang menunjukkan eksekusi program `active-response/firewall-drop`.



Gambar 3.58 Active Responses Wazuh Serangan (*Scanning*) Nmap

Setelah mendeteksi serangan, wazuh server akan mengaktifkan modul *active response* yang telah dikonfigurasi. Dalam kasus ini, *active response* firewall

diaktifkan untuk memblokir IP *address attacker* yang scanning Nmap. Gambar 3.59 menunjukkan bahwa *active responses* berhasil memblokir serangan. Hal ini ditandai dengan nilai `rule.description = Host blocked by Firewall Active Response`. Keterangan ini memberikan informasi bahwa tindakan *active responses* yang diinisiasi oleh wazuh manager berhasil dilakukan untuk memblokir akses dari sumber IP address penyerang.

Gambar 3.59 Active Responses Wazuh Serangan (*Scanning*) Nmap

3.6.3. Evaluasi Optimasi Firewall Active Responses Wazuh XDR (Serangan Brute Force)

Penerapan pengujian dan emulasi serangan SSH *brute force* dengan *active response* pada penelitian ini, dimodelkan terhadap endpoint ubuntu server (wazuh agent) dan mengkonfigurasi modul *active response* wazuh untuk memblokir IP address penyerang. Tujuan utama dari konfigurasi ini merupakan pencegahan serangan *brute force* pada service SSH yang aktif pada perangkat wazuh agent. Adapun langkah yang dilakukan untuk mendeteksi serangan dan eksekusi active responses wazuh digunakan opsi

a) *Rule* ID - Respon yang akan dieksekusi dan dijalankan untuk setiap kejadian (*event*) log dengan ID 5758

b) *Rule Group* - Respon yang akan dieksekusi dan dijalankan untuk setiap kejadian (*event*) pada group yang dikonfigurasi

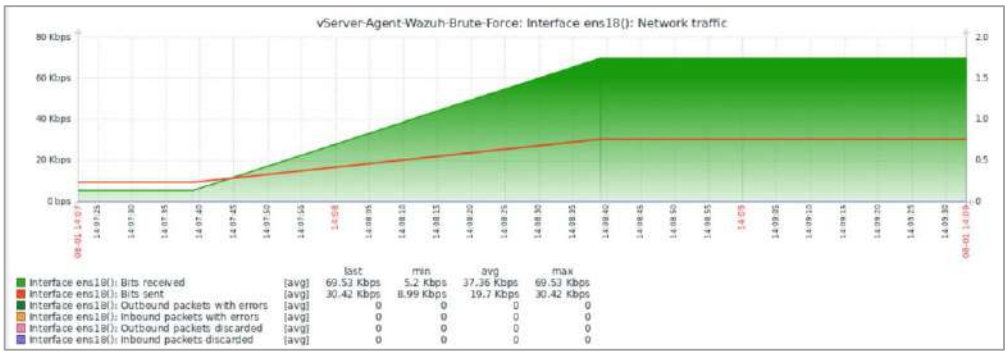
c) *Level* - Respon yang akan dieksekusi dan dijalankan untuk setiap kejadian (*event*) pada level rendah sampai level tinggi.

Pengujian dan emulasi ini *module active responses* dikonfigurasi untuk menjalankan *script*, dengan memblok IP address penyerang ketika aturan `5758 – Maximum authentication attempts exceeded` terjadi. Konfigurasi pendeteksian dilakukan pada ubuntu server (wazuh agent) untuk monitoring autentikasi SSH, terhadap upaya akses login ketika melebihi batas maksimum, dengan rule ID 5758, wazuh agent akan mengirimkan log ke wazuh server untuk dapat dianalisa. Selanjutnya analisis dan deteksi pada wazuh server ketika menerima log dari wazuh agent dengan mendeteksi aturan (*rule*) 5758 akan di *trigger* bahwa telah terjadi serangan *brute force* pada layanan SSH, seperti pada gambar 3.60.

Gambar 3.60 Hasil Deteksi Serangan *Brute Force* pada Wazuh Manager (*Dashboard*)

Pada gambar 3.61, menunjukkan lonjakan trafik pada interface ubuntu server (wazuh agent) dimulai sekitar pukul 14:07. Peningkatan traffic ini merupakan jumlah bit yang diterima oleh `interface ens180` pada wazuh agent, serta jumlah paket yang diterima (*received*). Sebelum pukul 14:07, trafik pada interface relatif stabil dan rendah. Namun, setelah pukul 14:07, terjadi peningkatan yang

signifikan, mencapai puncak sekitar 60 Kbps. Peningkatan traffic ini menunjukkan bahwa serangan *brute force* yang menggunakan *wordlist* `rockyou.txt` mulai memberikan beban yang signifikan pada interface perangkat ubuntu server, dengan mengirimkan sejumlah besar permintaan ke server target. *Bits received* mengalami peningkatan yang konsisten dalam jumlah bit yang diterima, menunjukkan banyaknya data yang dikirim ke perangkat wazuh agent oleh penyerang. *Packets received* merupakan jumlah paket yang diterima juga mengalami peningkatan, peningkatan traffic ini merupakan upaya autentikasi yang dikirimkan oleh penyerang dari upaya *brute force*.

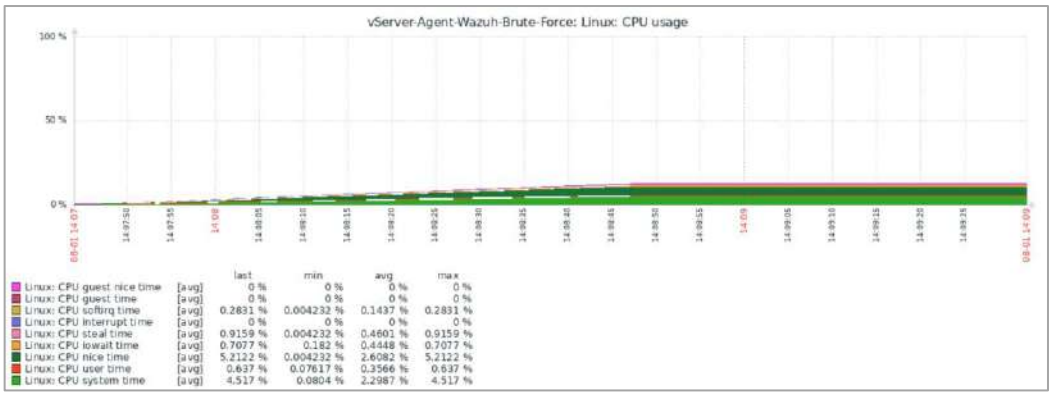


Gambar 3.61 Peningkatan *Traffic* di *Interface* ens18 pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

Pada gambar 3.62, hal yang sama terjadi lonjakan dalam *context switches* dan *interrupts per second* pada CPU *jumps* mulai terjadi sekitar pukul 14:07. Sebelumnya nilai CPU *jumps* berada pada level yang rendah dan normal. Namun, setelah pukul 14:07, nilai ini meningkat, menunjukkan bahwa CPU *jumps* mulai menerima lebih banyak permintaan dan interupsi dari proses yang sedang berjalan. *Context switches* yang tinggi menunjukkan bahwa CPU *jumps* harus sering beralih antara berbagai proses, hal ini disebabkan oleh beban kerja yang tinggi dari serangan *brute force*.

Gambar 3.62 Peningkatan *Traffic* CPU *Jumps* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

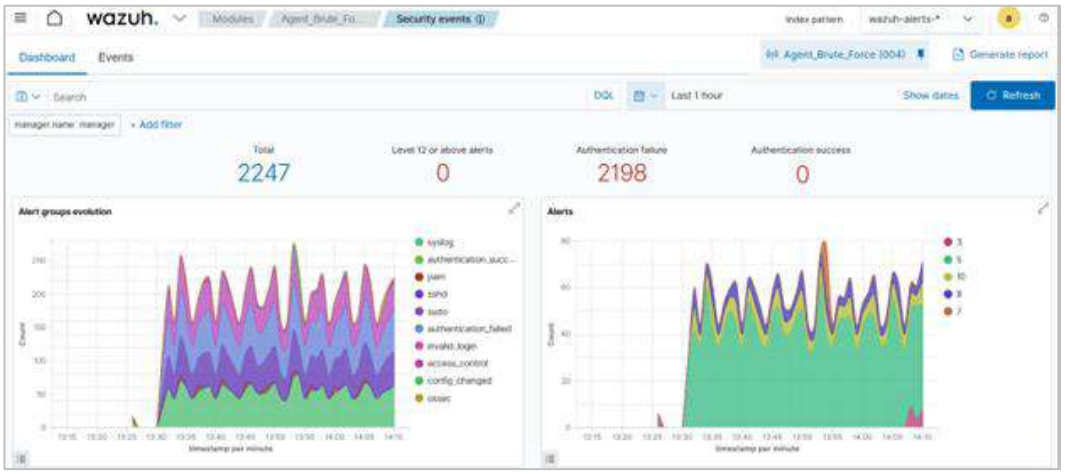
Pada gambar 3.63, terlihat peningkatan penggunaan CPU terlihat sekitar pukul 14:08. Penggunaan CPU yang mencakup *user time* dan *system time* mulai meningkat secara signifikan, sementara *idle time* mulai berkurang. Sebelum pukul 14:07, penggunaan CPU sebagian besar terlihat dalam keadaan *idle*, menunjukkan bahwa server (wazuh agent) tidak sedang terbebani. Namun, setelah pukul 14:07, penggunaan CPU oleh proses *user time* dan oleh kernel meningkat, menunjukkan bahwa server mulai bekerja lebih untuk menangani permintaan yang masuk dari serangan *brute force*.



Gambar 3.63. Peningkatan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

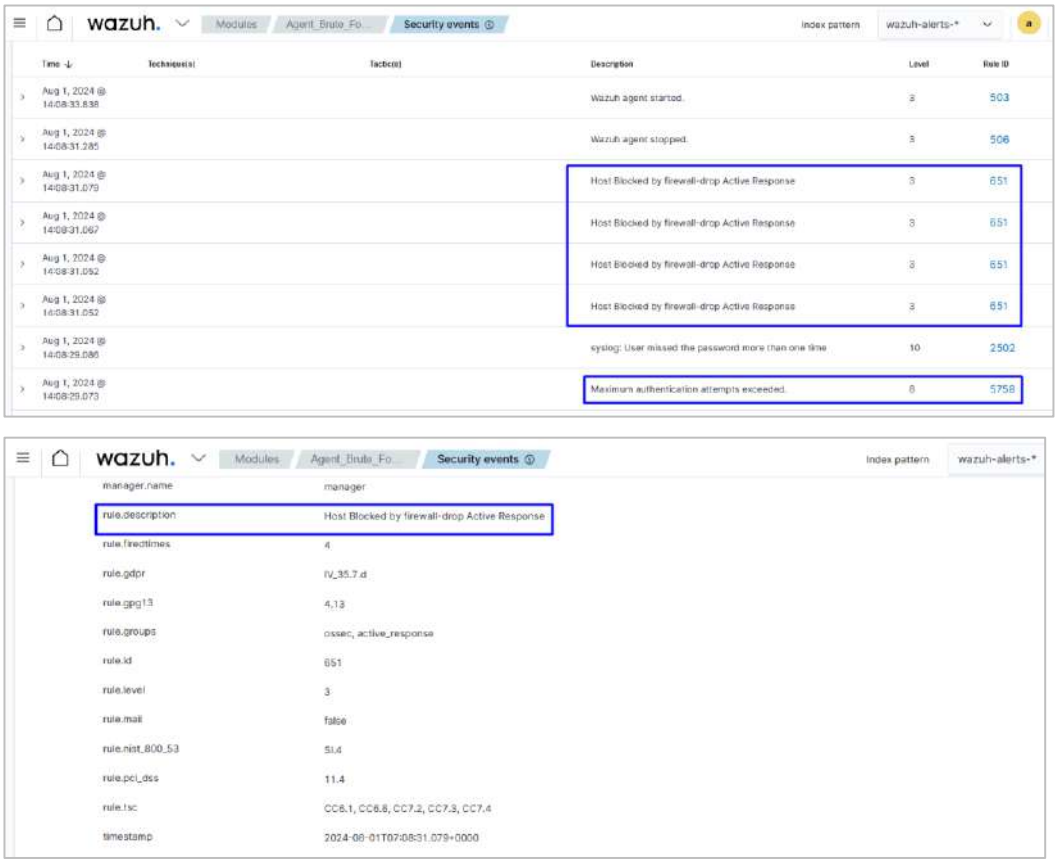
Berdasarkan konfigurasi *active response* yang diterapkan, wazuh server akan mengenali kejadian ini sebagai ancaman pada wazuh agent. Selanjutnya eksekusi *active responses* akan bekerja setelah mendeteksi serangan, wazuh server akan mengaktifkan modul *active response* yang telah dikonfigurasi. Modul ini menjalankan *script* yang dirancang untuk memblokir IP address penyerang secara otomatis. Script tersebut akan berinteraksi dengan firewall `ipset` untuk

memblokir semua lalu lintas dari IP address penyerang. Pada gambar 3.64, Jumlah *authentication failure* 2198, merupakan kegagalan autentikasi dalam waktu 1 jam. Hasil analisa dari wazuh manager menunjukkan adanya serangan *brute force* yang sangat massif ke wazuh agent. Serangan *brute force* ini merupakan upaya sistematis untuk menebak kata sandi dengan mencoba berbagai kombinasi karakter, menggunakan file teks *wordlist* `rockyou.txt`. Target serangan ini secara spesifik menargetkan sistem autentikasi pada perangkat wazuh *agent*.



Gambar 3.64. *Authentication Failure* Serangan Brute Force (1 Hour)

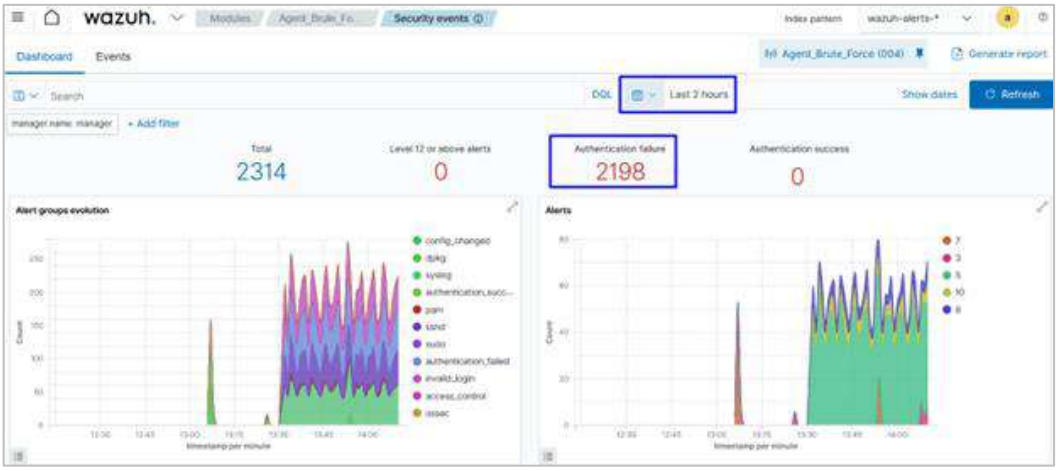
Berdasarkan gambar 3.65, disimpulkan bahwa wazuh manager berhasil menjalankan fungsinya sebagai sistem deteksi intrusi dan *active response* XDR. *Index pattern* deteksi serangan wazuh manager berhasil mendeteksi adanya aktivitas serangan *brute force* pada perangkat server (*wazuh agent*), dengan nilai pada `data.parameters.alert.rule.description : Maximum authentication attempts exceeded`. Wazuh manager secara otomatis menjalankan *active responses*, yang sudah dikonfigurasi sebelumnya untuk memblokir akses dari IP *address* sumber serangan. Gambar 3.65 menunjukkan bahwa active response berhasil memblokir serangan, hal ini terlihat pada nilai `rule.description` yang menunjukkan eksekusi program `Host Blocked by firewall-drop Active Response`.



Gambar 3.65 Hasil Deteksi Serangan *Brute Force* dan *Active Response* Firewall

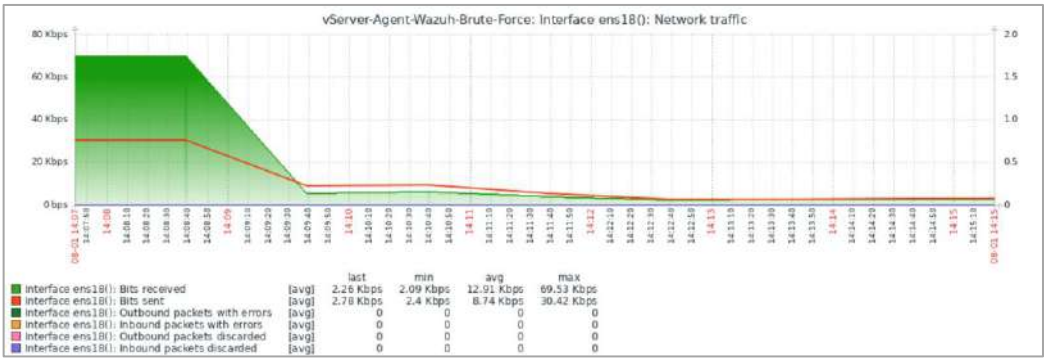
Gambar 3.66 menunjukkan hasil pemantauan dari wazuh manager pada serangan *brute force* menggunakan *wordlist* `rockyou.txt` yang ditargetkan pada autentikasi SSH. Monitoring dilakukan selama 1 jam pertama selanjutnya diteruskan hingga 2 jam. Wazuh manager mendeteksi serangan menggunakan mekanisme *Active Response* untuk memblokir serangan dari sumber serangan. Selama monitoring dilakukan pada 1 jam pertama, terdeteksi 2198 (*authentication failure*) upaya autentikasi yang gagal yang mengindikasikan serangan *brute force*. *Alert* dengan *description*: `Maximum authentication attempts exceeded (5758)` menunjukkan bahwa wazuh manager berhasil mendeteksi serangan dari sumber serangan. Konfigurasi *Active Response* pada wazuh manager mengaktifkan mekanisme `firewall-drop` untuk memblokir IP address yang melakukan serangan. Tabel *Alerts* menunjukkan bahwa beberapa entri `Host Blocked by firewall-drop Active Response (651)`, yang

menandakan bahwa wazuh manager telah memblokir IP address penyerang. Pada gambar 3.66 setelah dimonitoring selama 2 jam, jumlah kegagalan autentikasi tetap sama yaitu 2198 (*authentication failure*), yang menunjukkan bahwa tidak ada serangan tambahan yang berhasil dari penyerang menembus wazuh agent. Indikator ini menunjukkan bahwa mekanisme *active response* bekerja dengan baik dalam memblokir serangan *brute force*.



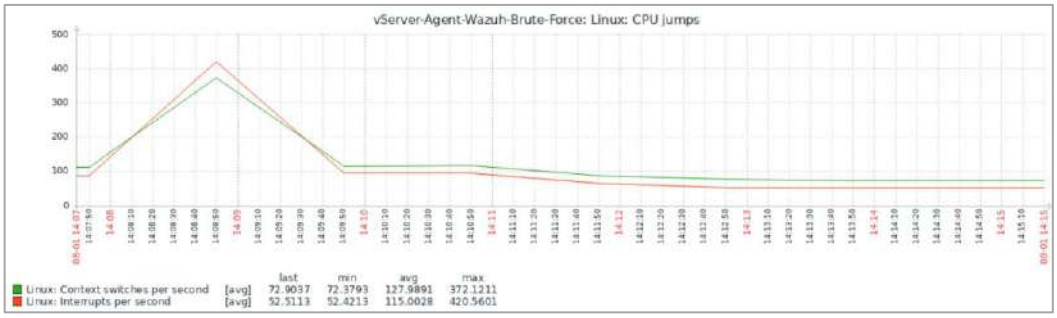
Gambar 3.66 Monitoring Wazuh Manager Selama 2 Jam

Pada gambar 3.67, menunjukkan bahwa setelah firewall *active response* diaktifkan, terjadi penurunan trafik dari pukul 14:09. Sebelum waktu tersebut, kapasitas interface `ens18` terlihat terjadi peningkatan trafik yang signifikan, mencapai 60 Kbps. Namun, setelah pukul 14:09, trafik pada interface `ens18` menurun sampai 0-1 Kbps. Hal ini menunjukkan bahwa firewall *active response* berhasil memblokir serangan *brute force* yang sedang berlangsung pada perangkat ubuntu server (wazuh *agent*), sehingga jumlah permintaan yang diterima oleh server (wazuh *agent*) menurun drastis.



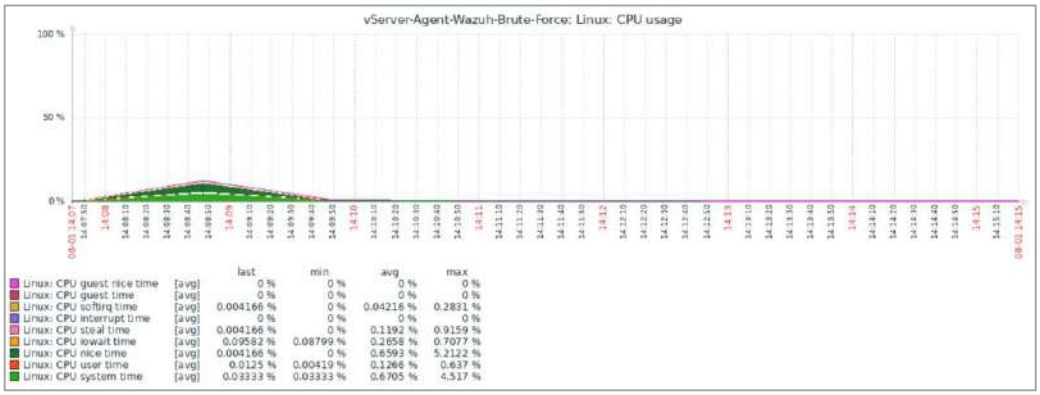
Gambar 3.67 Penurunan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

Pada gambar 3.68, penurunan CPU *jumps context switches* dan *interrupts per second*, mulai terjadi sekitar pukul 14:09. Terlihat sebelum waktu tersebut, nilai CPU *jumps context switches* dan *interrupts per second* mengalami peningkatan mencapai 500 per detik. Namun, setelah pukul 14:09, nilai CPU *jumps context switches* dan *interrupts per second* kembali menurun ke tingkat yang stabil dan lebih rendah. Penurunan nilai ini menunjukkan bahwa setelah *firewall active response* diaktifkan, beban kerja CPU *jumps* akibat interupsi yang tinggi dan permintaan dari serangan *brute force* berkurang secara signifikan, dan CPU *jumps* kembali ke keadaan normal.



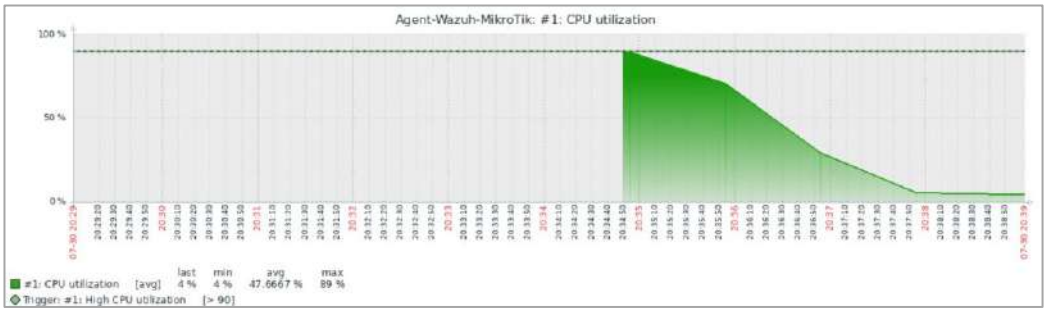
Gambar 3.68 Penurunan *Traffic* CPU *Jumps* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

Pada gambar 3.69, terlihat penggunaan CPU mulai menurun sekitar pukul 14:09. Sebelum waktu penurunan tersebut, penggunaan CPU dari proses pengguna (*user time*) dan oleh kernel (*system time*), menunjukkan nilai yang meningkat signifikan karena serangan *brute force* yang sedang berlangsung pada perangkat ubuntu server (wazuh *agent*). Namun, setelah pukul 14:09, penggunaan CPU terlihat menurun hingga mencapai nilai nol. Penggunaan penurunan ini menunjukkan bahwa firewall *active response* berhasil menghentikan dengan memblokir serangan *brute force*, dengan mengurangi beban kerja CPU yang sebelumnya terjadi peningkatan.



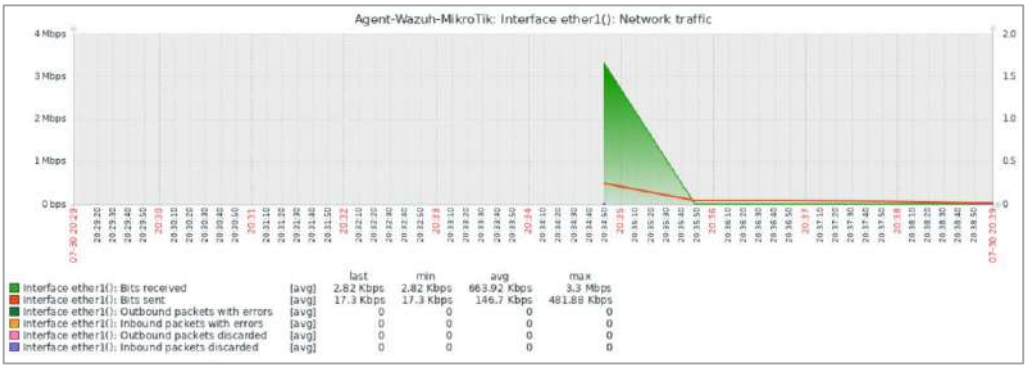
Gambar 3.69 Penurunan *Traffic* CPU *usage* pada Perangkat Ubuntu Server (wazuh *agent*) dari serangan *Brute Force*

Berdasarkan grafik gambar 3.70, pada perangakat ubuntu server (wazuh agent) mengalami serangan Denial of Service (DoS) yang cukup signifikan. Terlihat terdapat peningkatan pada penggunaan dalam waktu yang relatif singkat. Lonjakan ini merupakan aktivitas membanjiri sistem wazuh agent dengan permintaan berlebihan, sehingga mengganggu kinerja normal sistem. Pada grafik terlihat bahwa penggunaan utilitas CPU pada agent wazuh yang terhubung ke perangkat MikroTik RouterOS mengalami peningkatan kapasitas dari pukul 20:34:50. Penggunaan utilitas CPU meningkat hingga mencapai 89% dari kapasitas maksimum. Setelah aktivasi dan firewall *active response* dijalankan, terlihat pada grafik penggunaan utilisasi CPU pada perangkat wazuh agent mulai menurun sekitar pukul 20:38:00, kembali ke tingkat normal sekitar 5%. Peningkatan utilisasi penggunaan CPU menunjukkan bahwa serangan DoS menyebabkan beban kerja yang sangat tinggi pada utilisasi CPU, namun dari aktivasi *active* response wazuh manager firewall berhasil mengurangi beban tersebut secara signifikan, dengan memblokir IP address penyerang.



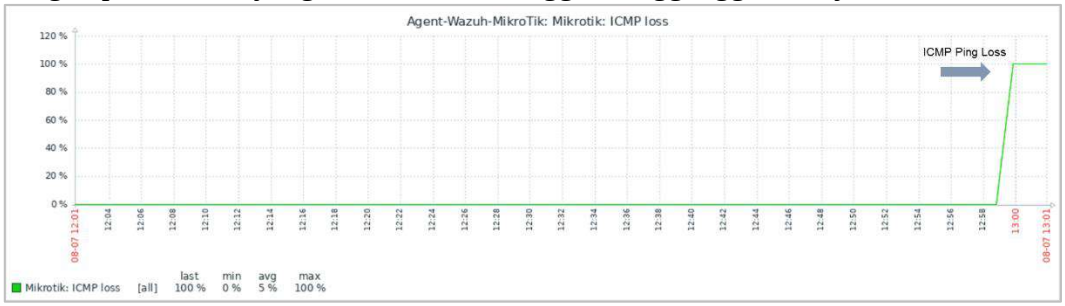
Gambar 3.70 Peningkatan *Traffic* CPU *Utilization* pada Perangkat MikroTik RouterOS (wazuh *agent*) dari serangan *Denial of Service* (DoS)

Pada gambar 3.71, grafik menunjukkan peningkatan lalu lintas pada `interface ether1` perangkat MikroTik RouterOS. Trafik mengalami peningkatan sekitar pukul 20:34:50, mencapai dengan penggunaan bandwidth sebesar 3.3 Mbps.



Gambar 3.71 Peningkatan *Interface Network* pada Perangkat MikroTik RouterOS (wazuh *agent*) dari serangan *Denial of Service* (DoS)

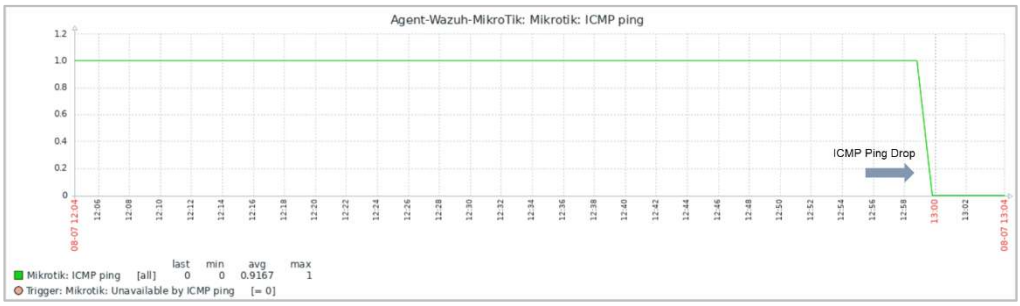
Gambar 3.72 *Agent* wazuh mengalami serangan *Denial of Service* (DoS) yang signifikan. Terjadi peningkatan kapasitas sumber daya dalam waktu yang relatif singkat. Lonjakan ini merupakan aktivitas yang membanjiri sistem agen wazuh dengan permintaan yang berlebihan, sehingga mengganggu kinerja normal sistem.



Gambar 3.72 ICMP ping loss Serangan DoS

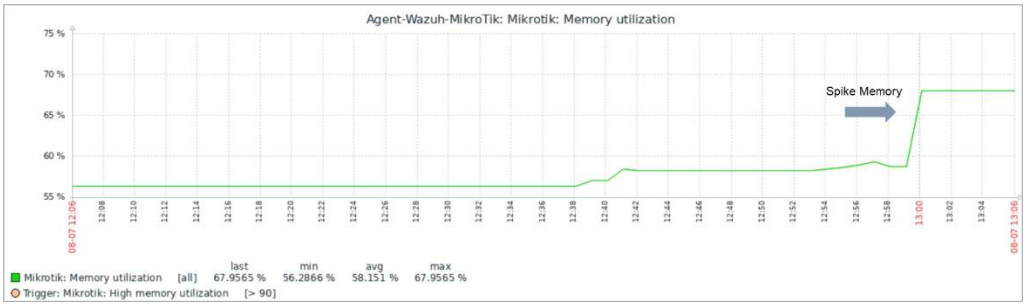
ICMP Ping loss terlihat meningkat secara signifikan pada pukul 13:00, dengan kehilangan ping ICMP mencapai 100%. Kehilangan ping ini menunjukkan bahwa selama serangan DoS, router tidak dapat menanggapi permintaan ping ICMP, yang menunjukkan hilangnya konektivitas secara total.

Gambar 3.73 menunjukkan hasil respon ping ICMP yang turun menjadi 0 pada pukul 13:00. Penurunan ini mengkonfirmasi hilangnya total respon ping ICMP, dari serangan DoS ini dapat dilihat bahwa router tidak dapat memproses permintaan ping karena serangan DoS.



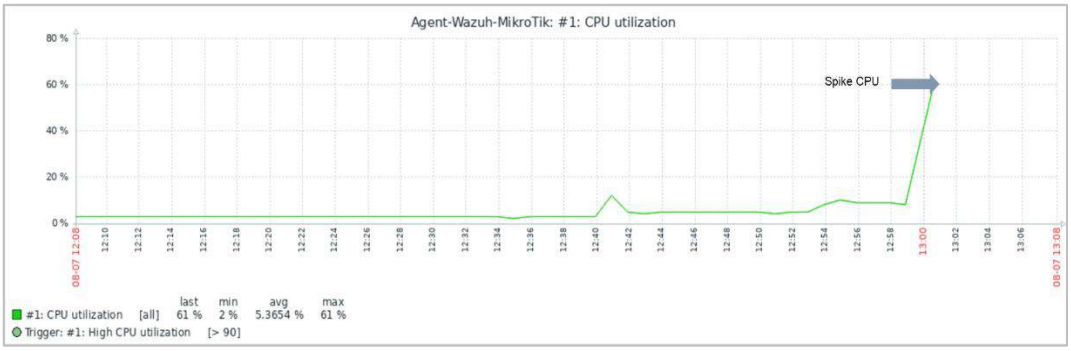
Gambar 3.73 ICMP ping Drop Serangan DoS

Gambar 3.75 memperlihatkan penggunaan kapasitas memori router relatif rendah dan normal sebelum serangan pada pukul 13:00 terjadi lonjakan penggunaan memori yang tinggi, mencapai 67%. Lonjakan ini menandakan bahwa memori router sangat terbebani saat terjadi serangan DoS, hal ini menunjukkan ketidakmampuan router dalam menangani lalu lintas jaringan.



Gambar 3.75 High Spike Memory Usage Attack DoS

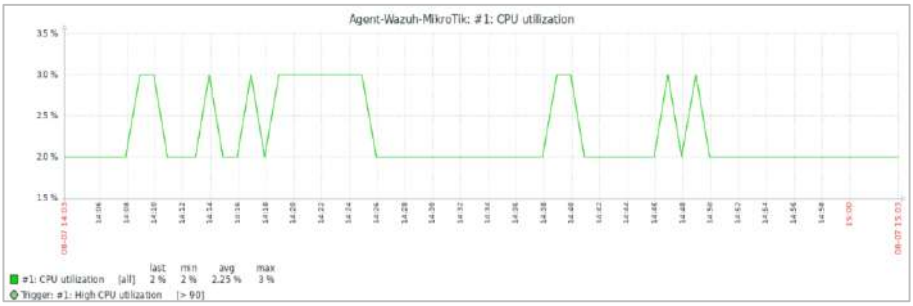
Gambar 3.76 menunjukkan penggunaan kapasitas CPU router relatif rendah dan normal sebelum serangan pada pukul 13:00, terjadi lonjakan penggunaan CPU yang tinggi, mencapai 67%.



Gambar 3.76 High Spike CPU Usage Attack DoS

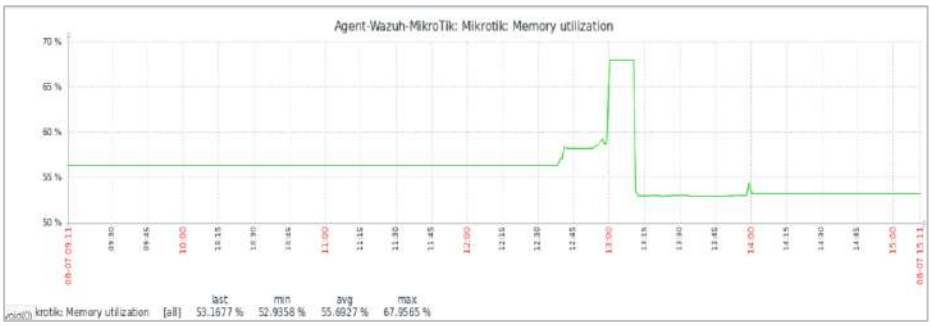
Lonjakan ini menunjukkan bahwa CPU router sangat terbebani selama serangan DoS, menunjukkan ketidakmampuan router dalam menangani lalu lintas jaringan.

Setelah firewall *active response* diaktifkan, terlihat pada grafik bahwa penggunaan CPU pada perangkat wazuh agent sudah mulai menurun, kembali ke penggunaan normal maksimal 3%, terlihat grafik penurunan pada gambar 3.77. Peningkatan penggunaan CPU tersebut menunjukkan bahwa serangan DoS menyebabkan beban kerja yang sangat tinggi pada penggunaan CPU, namun dari pengaktifan firewall wazuh manager *active response* berhasil menurunkan beban secara signifikan, dengan cara memblokir alamat IP penyerang.



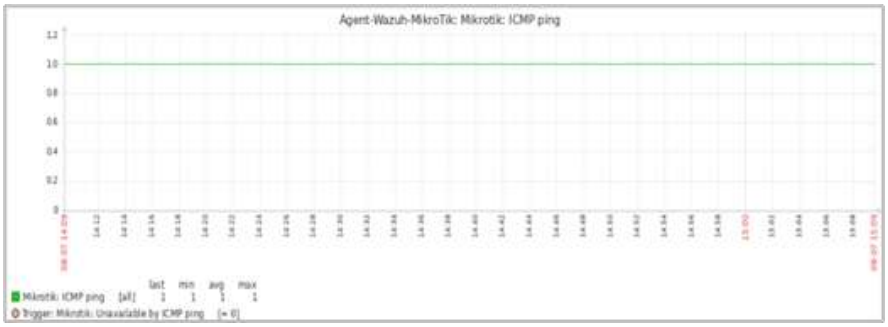
Gambar 3.77 Reduction in CPU usage traffic on the wazuh agent

Selain itu, grafik penggunaan memori pada gambar 3.78 juga menunjukkan normalisasi setelah respons aktif server wazuh diaktifkan.



Gambar 3.78 Reduction in memory usage traffic on the wazuh agent

Selain itu, grafik penggunaan ICMP ping gambar 3.79 dan ICMP ping *loss* gambar 3.80 juga menunjukkan hasil normal setelah respons aktif server wazuh diaktifkan, yang memblokir alamat IP penyerang.



Gambar 3.79 ICMP Ping normal status

Sebelum intervensi serangan DoS menyebabkan peningkatan signifikan dalam penggunaan memori dan menyebabkan penurunan ICMP Ping loss dalam ICMP ping. Namun, setelah sistem mitigasi diterapkan, semua metrik ini kembali normal, yang menunjukkan bahwa serangan telah berhasil diatasi dan jaringan kembali beroperasi dengan stabil.

Gambar 3.80 ICMP Ping Loss normal status

Mitigasi ini membuktikan efektivitas implementasi firewall XDR wazuh dalam menjaga stabilitas dan keamanan jaringan untuk perangkat router terhadap serangan

DoS. Secara keseluruhan, hasil ini menggarisbawahi pentingnya memiliki sistem deteksi dan mitigasi yang responsif untuk memastikan kelangsungan operasi jaringan tanpa gangguan yang signifikan.

BAB IV
KESIMPULAN DAN SARAN

4.1. Kesimpulan

Implementasi sistem deteksi dan mitigasi intrusi dari penelitian ini menunjukkan dan menghasilkan bahwa teknik yang digunakan pada infrastruktur perangkat router dan server sangat efektif dalam mendeteksi dan memitigasi berbagai serangan yang diemulasikan. Wazuh manager yang dikonfigurasi berhasil mendeteksi serangan brute force, *Denial of Service* (DoS) dan pemindaian Nmap, serta mengaktifkan *firewall* respons aktif untuk memblokir serangan berdasarkan alamat IP *malicious* penyerang. Dalam pemindaian menggunakan Nmap, wazuh XDR mampu mendeteksi aktivitas pemindaian dan mengaktifkan *firewall* respons aktif untuk memblokir IP penyerang. Selama serangan *brute force*, peningkatan signifikan dalam penggunaan CPU dan lalu lintas jaringan diamati, tetapi setelah *firewall* diaktifkan, penggunaan CPU dan lalu lintas jaringan kembali normal, yang menunjukkan efektivitas sistem dalam menangani serangan. Dalam kasus serangan DoS pada MikroTik RouterOS, penggunaan CPU dan memori oleh pengguna meningkat, tetapi setelah *firewall active response* diaktifkan, penggunaan CPU turun kembali ke status normal. Hasil pengujian keseluruhan menunjukkan dan menghasilkan bahwa *firewall active response* XDR memberikan perlindungan terhadap berbagai jenis serangan yang dimodelkan, mengurangi beban kerja sistem, dan memastikan stabilitas jaringan.

4.2. Saran

Berdasarkan hasil penelitian, beberapa saran dapat diusulkan untuk pengembangan lebih lanjut dari sistem deteksi dan mitigasi serangan siber yang berbasis Wazuh XDR dan firewall active response. Pertama, perlu dikembangkan algoritma deteksi yang lebih canggih guna menghadapi serangan siber yang lebih kompleks dan tersembunyi. Hal ini penting untuk meningkatkan kemampuan sistem dalam mendeteksi serangan yang lebih sulit diidentifikasi dengan metode deteksi konvensional. Kedua, pengujian ekstensif terhadap berbagai jenis serangan

siber harus dilakukan untuk memastikan kehandalan sistem di berbagai skenario serangan yang berbeda. Pengujian ini akan membantu mengidentifikasi kelemahan yang mungkin ada dan memastikan bahwa sistem dapat berfungsi optimal dalam situasi nyata. Ketiga, perlu dilakukan optimasi kinerja sistem deteksi dan respon aktif, sehingga dampak terhadap performa jaringan dapat diminimalkan selama serangan berlangsung. Optimasi ini akan membantu menjaga stabilitas jaringan dan mengurangi beban kerja sistem saat menghadapi serangan yang intensif. Keempat, pembaruan berkala pada aturan deteksi dan konfigurasi firewall sangat diperlukan untuk menghadapi ancaman siber yang terus berkembang. Pembaruan ini akan memastikan bahwa sistem selalu menggunakan metode terbaru untuk mendeteksi dan memitigasi serangan. Terakhir, pendidikan dan pelatihan bagi staf IT mengenai penggunaan dan konfigurasi sistem Wazuh XDR, serta teknik mitigasi serangan siber, perlu ditingkatkan. Dengan pengetahuan yang memadai, staf IT akan lebih siap dalam menangani serangan siber dan memanfaatkan sistem secara optimal.

DAFTAR PUSTAKA

1. Damanik HA, Anggraeni M, Nusantari FAA. Konsep dan Penerapan Switching dan Routing Implementasi Jaringan Komputer Berbasis Cisco. Riana Kusumawati, editor. Jawa Barat: CV. Mega Press Nusantara; 2023. 244 p.
2. Damanik HA, Anggraeni M. Pola Pengelompokan dan Pencegahan Public Honeypot menggunakan Teknik K-Means dan Automation Shell-Script. 2024;12(1):65–79.
3. Akbar S, Endroyono, Wibawa AD. The impact analysis and mitigation of DDoS attack on local government electronic procurement service (LPSE). Proceeding - 2016 Int Semin Intell Technol Its Appl ISITIA 2016 Recent Trends Intell Comput Technol Sustain Energy. 2017;36:405–10.
4. Triantopoulou S, Papanikas D, Kotzanikolaou P. An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet. 10th Int Conf Information, Intell Syst Appl IISA 2019. 2019;1–5.
5. Ceron M, Scholten C. MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. NOMS 2020 - 2020 IEEE/IFIP Netw Oper Manag Symp. 2020;
6. Howard W, Borowczak M. Detecting DDoS Attacks near the Edge with Router Canaries. IEEE Int Conf Consum Electron - Berlin, ICCE-Berlin. 2020;2020-Novem:18–21.
7. Helmiawan MA, Julian E, Cahyan Y, Saeppani A. Experimental Evaluation of Security Monitoring and Notification on Network Intrusion Detection System for Server Security. 2021 9th Int Conf Cyber IT Serv Manag CITSM 2021. 2021;1–6.
8. Subhan A, Kunang YN, Yadi IZ. Analyzing the Attack Pattern of Brute Force Attack on SSH Port. Proceeding - Int Conf Inf Technol Comput 2023, ICITCOM 2023 [Internet]. 2023;67–72. Available from: https://ieeexplore.ieee.org/document/10441929
9. BSSN. Lanskap Keamanan Siber Indonesia 2022. Badan Siber dan Sandi

Negara. 2022;(70).

10. Suhendi MRA, Alfarizi, Sukmandhani AA, Prabowo YD. Network Anomaly Detection Analysis using Artillery Honeypot and Wazuh SIEM. 2023 IEEE 9th Int Conf Comput Eng Des [Internet]. 2023;1–6. Available from: https://ieeexplore.ieee.org/document/10425009
11. Sankar NA, A FK. Implementation of SOC using ELK with Integration of Wazuh and Dedicated File Integrity Monitoring. 2023 9th Int Conf Smart Comput Commun. 2023;
12. Suryantoro T, Sari DF. Analisa Serangan Terhadap Port 80 Webserver Dengan SIEM Wazuh Menggunakan Metode Deteksi Dan OSCAR. 2022;(September):1–6.
13. Younus ZS, Alanezi M. Detect and Mitigate Cyberattacks Using SIEM. Proc - Int Conf Dev eSystems Eng DeSE. 2023;510–5.
14. Praptodiyono S, Firmansyah T, Anwar MH, Wicaksana CA, Pramudyo AS, Al-Allawee A. Development of Hybrid Intrusion Detection System Based on Suricata With Pfsense Method for High Reduction of Ddos Attacks on Ipv6 Networks. Eastern-European J Enterp Technol. 2023;5(9(125)):75–84.
15. Zebari RR, Zeebaree SRM, Jacksi K. Impact Analysis of HTTP and SYN Flood DDoS Attacks on Apache 2 and IIS 10.0 Web Servers. ICOASE 2018 - Int Conf Adv Sci Eng. 2018;156–61.
16. Oktivasari P, Zain AR, Agustin M, Kurniawan A, Murad F arbi, Anshor M fabian. Analysis of Effectiveness of Iptables on Web Server from Slowloris Attack. 2022 5th Int Conf Comput Informatics Eng [Internet]. 2022; Available from: https://ieeexplore.ieee.org/document/9970143/authors#authors

LAMPIRAN

Lampiran 1. Realisasi Penggunaan Anggaran

Dana Disetujui: Rp 7500.000

Jenis Pembelajaan	Komponen	Item	Kuantitas	Biaya Satuan	Total
Belanja Bahan	ATK	ATK	1	Rp300.000	Rp300.000
Belanja Bahan	Bahan penelitian (habis pakai)	Kabel, RJ45 dan Switch	15	Rp53.500	Rp802.500
Pengumpulan Data	Honor pembantu peneliti	Honorium pembantu peneliti	2	Rp300.000	Rp600.000
Pengumpulan Data	FGD				
Pengumpulan Data	Transport	Transport Dosen dan Mahasiswa ke AJN (3 orang) kali 5	15	Rp60.000	Rp900.000
Pengumpulan Data	Konsumsi	Konsumsi Rapat dan Kordinasi 3 Orang 4 Kali	12	Rp50.000	Rp600.000
Pengumpulan Data	Penginapan				
Analisis Data	Honor pengolah data	Pembuatan sistem, Konfigurasi dan Implementasi Sistem	1	Rp2.000.000	Rp2.000.000
Analisis Data	Honor narasumber				
Sewa Peralatan	Peralatan penelitian	Server, IDCloud dan Router (Paket), Internet (Paket)	1	Rp1.900.000	Rp1.900.000
Pelaporan penelitian	Honor administrasi peneliti				
Lainnya	Biaya pendaftaran HKI	Pencatatan Ciptaan dan Materai	1	Rp400.000	Rp400.000

Lampiran 2. Biodata Ketua dan Anggota Tim Peneliti

A. Identitas Diri Ketua Peneliti

1. Nama Lengkap : Hillman Akhyar Damanik, M. Kom.
2. Jenis Kelamin : Laki-laki
3. Jabatan Fungsional : Assisten Ahli
4. NIP/NIDN : 190016 / 0320038704
5. Tempat, Tanggal Lahir : P. Marihat, 20 Maret 1987
6. E-mail : hillman.akhyardamanik@budiluhur.ac.id
7. No Handphone : 082299099294
8. Alamat : Jl. Ciputat Raya Jl. Amal No.22 Pondok Pinang Keb.Lama-Jaksel

B. Riwayat Pendidikan

	SI	S2	S3
Nama Perguruan Tinggi	Universitas Muhammadiyah Riau	Universitas Budi Luhur	-
Bidang Ilmu	Teknik Informatika	Ilmu Komputer	-
Tahun Masuk-Lulus	2008-2012	2016 - 2018	-

C. Pengalaman Penelitian

No.	**Tahun**	**Judul Penelitian**	**Pendanaan**	
			Sumber	**Jumlah (Rp)**
1	2018	Teknik Pengujian Keamanan Data Text Bertingkat Dengan Metode Steganography LSB dan Teknik Enkripsi	Mandiri	-
2	2020	Implementation Scheme SLA and Network Availability Mechanism for Customer Service Provider	Universitas Budi Luhur	IDR 7,500,000
3	2020	Pemulihan dan Optimalisasi Kegagalan Multipath Link pada Lingkungan Metro-E	DIKTI	IDR 20,000,000

		dengan Policy Subroutines dan Internal Border Gateway Protocol (IBGP)		
4	2021	Implementation of Backoff Algorithm Bidirectional Forwarding Detection (BFD) and MPLS VRF for Fast Recovery Mechanism End-to-End Multi-Circuit (E2E)	Universitas Budi Luhur	IDR 7,500,000
5	2022	Mekanisme Penerapan dan Virtualisasi Honey Mesh pada Lingkungan Network Enterprise Threat Untuk Pendeteksian dan Pencegahan System Attack	Universitas Budi Luhur	IDR 7,500,000
6	2023	Pengenalan Pola Pendeteksian dan Pencegahan System Attack Pada Public Honey Mesh Menggunakan Firewall Automation Shell Script dan Teknik K-Means	Universitas Budi Luhur	IDR 7,500,000

D. Publikasi Artikel Ilmiah dalam Jurnal

No.	Jurnal Artikel Ilmiah	Nama Jurnal	Volume/Nomor/Tahun
1	Analysis Stego-Image Extraction Using ROT13 and Least Significant Bit (LSB) Algorithm Method on Text Security	Jurnal Ilmiah FIFO	9/2/2018
2	Implementation Scheme SLA and Network Availability Mechanism for Customer Service Provider	Jurnal Penelitian Pos dan Informatika	10/2/2020

3	Implementation of Backoff Algorithm Bidirectional Forwarding Detection (BFD) and MPLS VRF for Fast Recovery Mechanism End-to-End Multi-Circuit (E2E)	Jurnal Penelitian Pos dan Informatika	11/2/2020
4	Pola Pengelompokan dan Pencegahan Public Honeypot menggunakan Teknik K-Means dan Automation Shell-Script	Elkomika Itenas	12/01/2023

E. Pemakalah Seminar Ilmiah

No.	Nama Temu Ilmiah	Judul Artikel Ilmiah	Waktu dan Tempat
1	BICAME	Converged Transparent Satellite For LTE A Evaluation State-of-the-Art Layer 2 Method	Institut Teknologi Kalimantan
2	Conference Series 2019-International Conference on Data and Information Science 2018 (ICODIS)	A Satellite-LTE Delay-Tolerant Capabilities Tunneling: Design and Performance Evaluation	Telkom University
3	2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)	Optimization Info Rate Using APSK Modulation Scheme for Delivery GSM ABIS over Satellite Communications	Bandung

4	ICERIA 2020 Journal of Physics: Conference Series	Mechanical Converged Transparent Satellite for LTE: An Evaluation State-of-the-Art Layer 2 Method	Institut Teknologi Kalimantan
5	2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)	Fast-recovery and optimization multipath circuit networks environments using routing policies different administrative distance and internal BGP	Yogyakarta
6	Proceedings of the 1st International Conference on IT, Communication and Technology for Better Life-ICT4BL	Scalable Resilient Internal BGP: Fast Recovery Mechanism Provide Multi-link Environment Carrier Ethernet Backhaul	Jakarta
7	Journal of Physics: Conference Series	Improving Internal BGP Provide Fast Failover in Multihoming Environment Mobile Backhaul	Yogyakarta
8	RSF Conference Series: Engineering and Technology	Securing Data Network for Growing Business VPN architectures Cellular Network Connectivity	Jakarta

F. Karya Buku

No.	Judul Buku	Tahun	Jumlah Halaman	Penerbit
1	Konsep Penerapan Switching dan Routing pada Implementasi Jaringan Komputer Berbasis Cisco	2022	300 Halaman	Mega Press Nusantara

G. Perolehan HKI

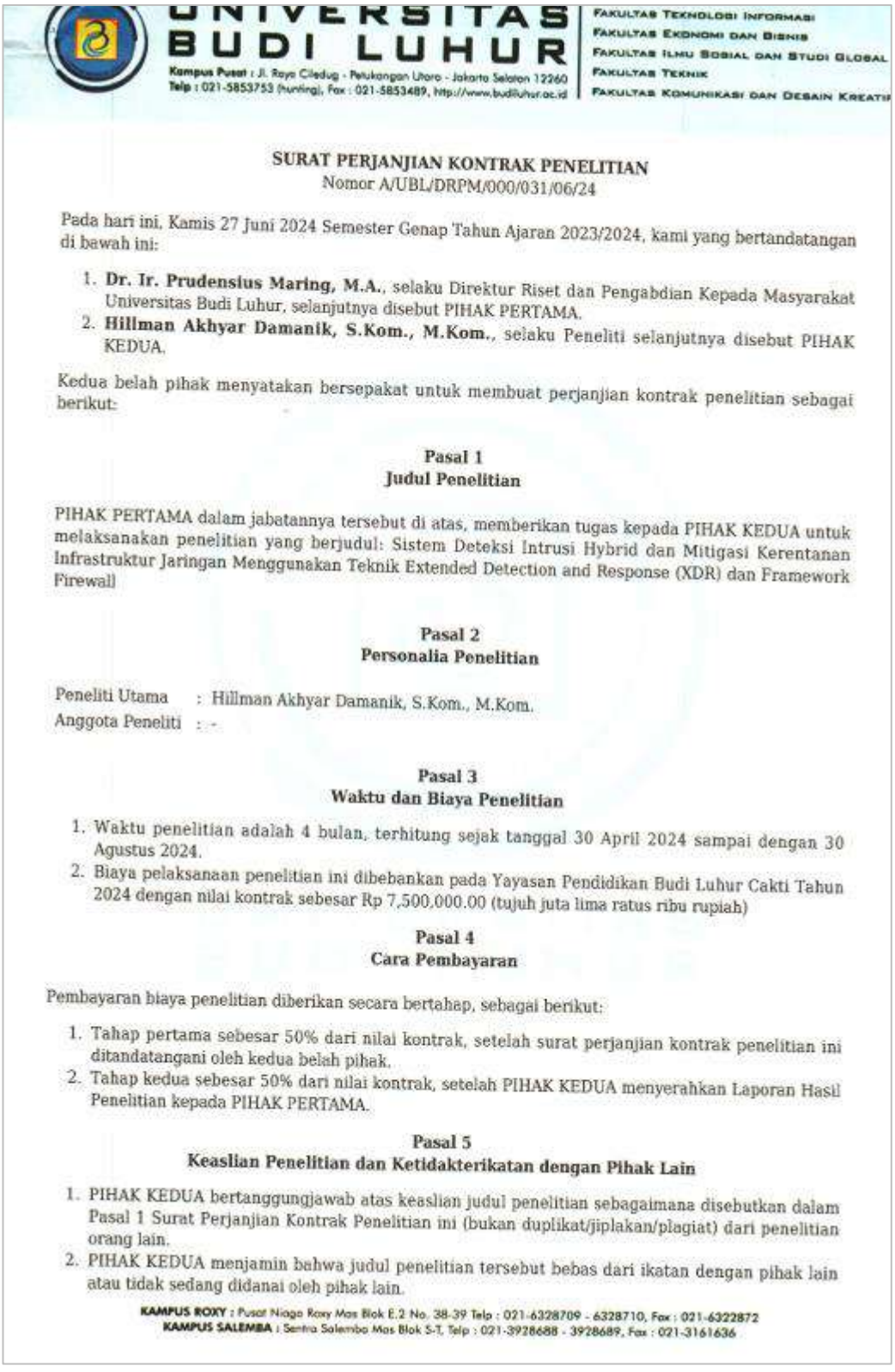
No	Judul/Tema HKI	Tahun	Jenis	Nomor P/ID
1	Peningkatan Kompetensi Guru Dan Siswa SMK Pustek Serpong Melalui Pelatihan Computer Network Dan Network Security	2022	HKI	000390536

2	Fast-Recovery and Optimization Multipath Circuit Networks Environments Using Routing Policies Different Administrative Distance and Internal BGP	2023	HKI	000444041

Jakarta, 09 Agustus 2024

(Hillman Akhyar Damanik)

Lampiran 3. Surat Perjanjian Kontrak Penelitian



UNIVERSITAS BUDI LUHUR

Kampus Pusat : Jl. Raya Ciledug - Petukangan Utara - Jakarta Selatan 12260
Telp : 021-5853753 (hunting), Fax : 021-5853489, http://www.budiluhur.ac.id

FAKULTAS TEKNOLOGI INFORMASI
FAKULTAS EKONOMI DAN BISNIS
FAKULTAS ILMU SOSIAL DAN STUDI GLOBAL
FAKULTAS TEKNIK
FAKULTAS KOMUNIKASI DAN DESAIN KREATIF

SURAT PERJANJIAN KONTRAK PENELITIAN
Nomor A/UBL/DRPM/000/031/06/24

Pada hari ini, Kamis 27 Juni 2024 Semester Genap Tahun Ajaran 2023/2024, kami yang bertandatangan di bawah ini:

1. **Dr. Ir. Prudensius Maring, M.A.**, selaku Direktur Riset dan Pengabdian Kepada Masyarakat Universitas Budi Luhur, selanjutnya disebut PIHAK PERTAMA.
2. **Hillman Akhyar Damanik, S.Kom., M.Kom.**, selaku Peneliti selanjutnya disebut PIHAK KEDUA.

Kedua belah pihak menyatakan bersepakat untuk membuat perjanjian kontrak penelitian sebagai berikut:

Pasal 1
Judul Penelitian

PIHAK PERTAMA dalam jabatannya tersebut di atas, memberikan tugas kepada PIHAK KEDUA untuk melaksanakan penelitian yang berjudul: Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall

Pasal 2
Personalia Penelitian

Peneliti Utama : Hillman Akhyar Damanik, S.Kom., M.Kom.
Anggota Peneliti : -

Pasal 3
Waktu dan Biaya Penelitian

1. Waktu penelitian adalah 4 bulan, terhitung sejak tanggal 30 April 2024 sampai dengan 30 Agustus 2024.
2. Biaya pelaksanaan penelitian ini dibebankan pada Yayasan Pendidikan Budi Luhur Cakti Tahun 2024 dengan nilai kontrak sebesar Rp 7,500,000.00 (tujuh juta lima ratus ribu rupiah)

Pasal 4
Cara Pembayaran

Pembayaran biaya penelitian diberikan secara bertahap, sebagai berikut:

1. Tahap pertama sebesar 50% dari nilai kontrak, setelah surat perjanjian kontrak penelitian ini ditandatangani oleh kedua belah pihak.
2. Tahap kedua sebesar 50% dari nilai kontrak, setelah PIHAK KEDUA menyerahkan Laporan Hasil Penelitian kepada PIHAK PERTAMA.

Pasal 5
Keaslian Penelitian dan Ketidakterikatan dengan Pihak Lain

1. PIHAK KEDUA bertanggungjawab atas keaslian judul penelitian sebagaimana disebutkan dalam Pasal 1 Surat Perjanjian Kontrak Penelitian ini (bukan duplikat/jiplakan/plagiat) dari penelitian orang lain.
2. PIHAK KEDUA menjamin bahwa judul penelitian tersebut bebas dari ikatan dengan pihak lain atau tidak sedang didanai oleh pihak lain.

KAMPUS ROXY : Pusat Niaga Roxy Mas Blok E.2 No. 38-39 Telp : 021-6328709 - 6328710, Fax : 021-6322872
KAMPUS SALEMBA : Sentra Salemba Mas Blok S-T, Telp : 021-3928688 - 3928689, Fax : 021-3161636

3. PIHAK KEDUA menjamin bahwa judul penelitian tersebut bukan merupakan penelitian yang SEDANG ATAU SUDAH selesai dikerjakan, baik didanai oleh pihak lain maupun oleh sendiri.
4. PIHAK PERTAMA tidak bertanggungjawab terhadap tindakan plagiat yang dilakukan oleh PIHAK KEDUA.
5. Apabila dikemudian hari diketahui ketidakbenaran pernyataan ini, maka kontrak penelitian DINYATAKAN BATAL, dan PIHAK KEDUA wajib mengembalikan dana yang telah diterima kepada Yayasan Pendidikan Budi Luhur Cakti sebagai pemberi dana.

Pasal 6
Monitoring Penelitian

1. PIHAK PERTAMA berhak untuk:
   a. Melakukan pengawasan administrasi, monitoring, dan evaluasi terhadap pelaksanaan penelitian.
   b. Memberikan sanksi jika dalam pelaksanaan penelitian terjadi pelanggaran terhadap isi perjanjian oleh peneliti.
   c. Bentuk sanksi disesuaikan dengan tingkat pelanggaran yang dilakukan.
2. Pemantauan kemajuan penelitian dikoordinasikan oleh PIHAK PERTAMA.
3. Pelaksanaan kemajuan penelitian dilaksanakan pada tanggal 12 Juli 2024.
4. Format Laporan Kemajuan dan teknis pelaksanaannya diatur oleh PIHAK PERTAMA.

Pasal 7
Laporan Akhir Penelitian

PIHAK KEDUA wajib menyerahkan laporan akhir dalam bentuk softcopy, paling lambat tanggal 16 Agustus 2024.

Pasal 8
Sanksi

Segala kelalaian baik disengaja maupun tidak, sehingga menyebabkan keterlambatan menyerahkan laporan hasil penelitian dengan batas waktu yang telah ditentukan akan mendapatkan sanksi sebagai berikut:

1. Tidak diperbolehkan mengajukan usulan penelitian pada semester berikutnya bagi ketua dan anggota peneliti.
2. PIHAK KEDUA diberikan kesempatan perpanjangan waktu penelitian selama 2 (dua) minggu sampai dengan tanggal 30 Agustus 2024.
3. Jika setelah masa perpanjangan tersebut PIHAK KEDUA tidak dapat menyelesaikan penelitiannya, PIHAK KEDUA diwajibkan mengembalikan dana yang sudah diterima kepada Yayasan Pendidikan Budi Luhur Cakti dengan cara mengembalikan tunai kepada PIHAK PERTAMA.

Pasal 9
Penutup

Perjanjian ini berlaku sejak ditandatangani dan disetujui oleh PIHAK PERTAMA dan PIHAK KEDUA.

Jakarta, 27 Juni 2024

PIHAK PERTAMA	PIHAK KEDUA
Dr. Ir. Prudensius Maring, M.A.	Hillman Akhyar Damanik, S.Kom., M.Kom.
NIP. 190043	NIP. 190016

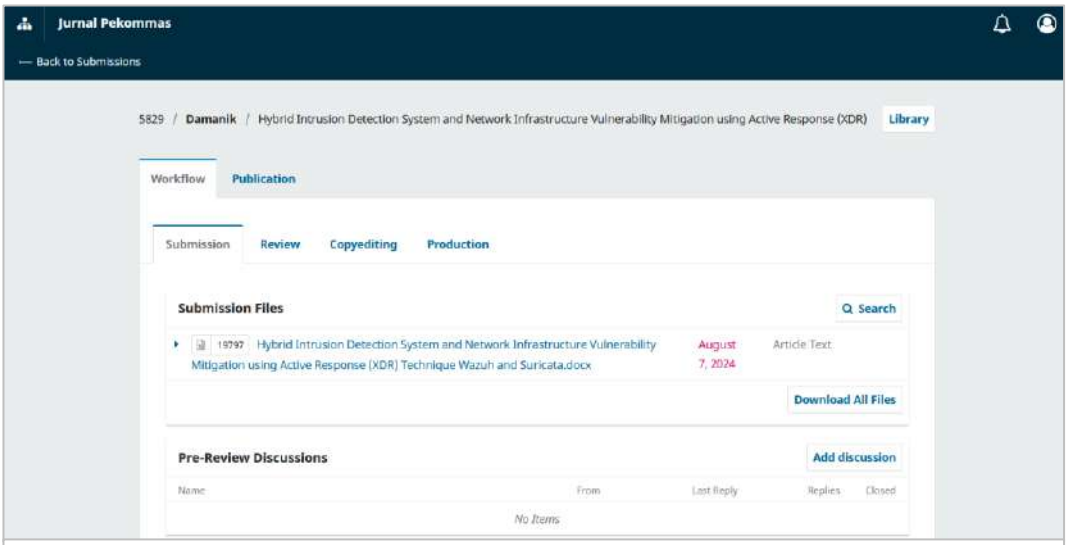
Lampiran 4. Catatan Harian

No	Tanggal	Kegiatan
1	9 Mei 2024	1) Melakukan analisis untuk kerentanan yang ada pada perangkat router dan server. 2) Melakukan literature untuk serangan reconnaissance attack, access attack dan DoS attack 3) Meneliti untuk penerapan integrasi yang sudah ada mengenai SIEM, iptables ipset dan active response (XDR) wazuh. 4) Mempelajari hardware dan software untuk membangun dan mengimplementasikan sistem intrusi dan mitigasi.
2	17 Mei 2024	1) Persiapan waktu dan tempat penelitian 2) Analisis kebutuhan untuk infrastruktur jaringan pada perangkat router dan virtualisasi server yang akan diselidiki, jenis serangan dan penerapan mitigasi. 3) Membuat rencana untuk RAB, alokasi waktu penelitian
3	7 Juni 2024	1) Melakukan identifikasi kebutuhan teknis untuk implementasi (perangkat keras, perangkat lunak dan perangkat VMWare dan proxmox hypervisor, router MikroTik, vServer, VPS Server, Switch, PC/Laptop, Kabel LAN dan konektivitas internet). 2) Melakukan perancangan arsitektur dan topologi (*Physic* dan *logic*) sistem. 3) Menentukan penjadwalan untuk kegiatan implementasi dan pengujian sistem.
4	21 Juni 2024	1. Mendesain topologi dan konektivitas *physic* jaringan. 2. Mendesain topologi dan konektivitas *logic* jaringan.
5	5 Juli 2024	1) Melakukan konfigurasi infrastruktur (hardware dan software) 2) Mengkonfigurasi VMWare Desktop Hypervisor, Sistem Operasi, Web Server 3) Menetapkan dan menentukan untuk arsitektur sistem (integrasi Wazuh Agent, Wazuh Manager, SIEM, framework firewall *iptables ipset* dan active response (XDR) wazuh

		4) Melakukan konfigurasi VPS Server (Wazuh Manger dan VPS Ubuntu Server) 5) Melakukan konfigurasi integrasi sistem (Wazuh agent, Wazuh Server Manager (*Indexer*, Server dan *Dashboard*). 6) Menentukan jenis serangan yang akan dilakukan pada perangkat router dan server 7) Melakukan dan membuat *policy* dan *rule* mitigasi serangan
6	19 Juli 2024	1) Melakukan pelaksanaan implementasi untuk sistem Sistem Deteksi Intrusi Hybrid Wazuh XDR, SIEM, dan Firewall pada Kerentanan Infrastruktur Jaringan Perangkat Router dan Server 2) Melakukan pengujian sistem jaringan dan monitoring (SOC) secara berkala untuk mendeteksi dan merespon anomali dan serangan 3) Melakukan pengujian teknik mitigasi serangan dengan *active response* (XDR) wazuh
7	26 Juli 2024	1) Melakukan evaluasi kinerja sistem hybrid intrusi dan teknik mitigasi (lalu lintas jaringan, sistem deteksi dan respon 2) Melakukan evaluasi kinerja sistem hybrid intrusi dan teknik mitigasi (lalu lintas jaringan, sistem deteksi dan respon 3) Melakukan dokumentasi optimasi perancangan sistem dan mitigasi serangan
8	01 Agustus 2024	Tahap Penyusunan laporan Akhir penelitian

Lampiran 5. Artikel Ilmiah (Submitted)

Disubmit pada Jurnal Pekommas Kominfo (Sinta 2)



Jurnal Pekommas Vol. x No. x, Month Year: Page – Page

Hybrid Intrusion Detection System and Network Infrastructure Vulnerability Mitigation using Active Response (XDR) Technique Wazuh and Suricata

Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Active Response (XDR) Wazuh dan Suricata

Hillman Akhyar Damanik

Fakultas Teknologi Informasi Universitas Budi Luhur

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, Indonesia 1226012
hillman.akhyardamanik@budiluhur.ac.id

Received : 00 Month 202x | | Revised : 00 Month 202x | | Accepted: 00 Month 202x

Abstract – The complexity of cyber threats against the network infrastructure of companies, educational institutions, and government makes protecting network infrastructure a top priority. Router and server devices are highly vulnerable to various types of cyber threats, requiring comprehensive detection and response solutions. This research will implement an intrusion detection system by integrating SIEM technology and wazuh XDR (Extended Detection and Response solutions). This system analyzes index pattern data from wazuh agent devices to detect and respond to attacks using the XDR active response firewall. The testing was conducted MikroTik RouterOS, Ubuntu Server 20.04 as wazuh agent to test reconnaissance attacks, brute force and DoS attacks. The results of the research show Nmap and brute force attacks were successfully detected by wazuh manager and blocked the attacker IP malicious through active response. Detection of brute force attacks showed an increase in traffic of up to 60 Kbps and CPU usage reached 100%, then decreased after the active response firewall was activated. Authentication failure reached 2198 times in the first hour of the brute force attack. CPU usage increased from 20% to 85% during the attack and decreased to 15% after the active response firewall was activated. DoS attacks, on MikroTik experienced an increase in CPU usage of up to 61% and memory of 67%. After activating the active response firewall, CPU usage decreased to 3%. Traffic on the MikroTik interface increased to 3.3 Mbps during the attack, then decreased to 1 Kbps after the firewall was activated.

Keywords: Router, Server, Wazuh XDR, SIEM, Firewall

Lampiran 4. HKI

Peraturan Menteri Kehakiman R.I.

Nomor : M.01-HC.03.01 Tahun 1987

Kepada Yth. :

Direktur Jenderal HKI

melalui Direktur Hak Cipta,

Desain Industri, Desain Tata Letak,

Sirkuit Terpadu dan Rahasia Dagang

di

Jakarta

PERMOHONAN PENDAFTARAN CIPTAAN

I. Pencipta:

1. Nama	: Hillman Akhyar Damanik
2. Kewarganegaraan	: Indonesia
3. Alamat	: Flamboyan Unit No.57 Jl. Mesjid Nurul Iman Cipadu - Tangerang 15155
4. Telepon	:
5. No. HP & E-mail	: 082299099294 & hillman.akhyardamanik@budiluhur.ac.id

II. Pemegang Hak Cipta:

1 Nama	: DRPM Universitas Budi Luhur
2. Kewarganegaraan	: Indonesia
3. Alamat	: Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan Jakarta, 12260
4. Telepon	: 021 - 5853753
5. No. HP & E-mail	: hki@budiluhur.ac.id

III. Kuasa:

1. Nama	:
2. Kewarganegaraan	:
3. Alamat	:
4. Telepon	:
5. No. HP & E-mail	:

IV. Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall

V. Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia:

VI. Uraian ciptaan:

Kompleksitas ancaman siber terhadap infrastruktur jaringan perusahaan, institusi pendidikan, dan pemerintah menjadikan perlindungan infrastruktur jaringan sebagai prioritas utama. Berbagai perangkat router dan server sangat rentan terhadap berbagai jenis ancaman siber, sehingga memerlukan solusi deteksi dan respons yang komprehensif. Penelitian ini akan mengimplementasikan sistem deteksi intrusi dengan mengintegrasikan teknologi SIEM dan (Extended Detection and Response solutions) XDR Wazuh. Sistem ini menganalisis data index pattern dari perangkat wazuh agent untuk mendeteksi dan merespons serangan menggunakan firewall active response XDR. Pengujian dilakukan pada perangkat MikroTik Router, ubuntu server untuk menguji serangan reconnaissance attack, brute force dan DoS. Hasil penelitian menunjukkan serangan Nmap dan brute force berhasil dideteksi oleh Wazuh Manager dan memblokir IP penyerang melalui active response. Pendeteksian serangan brute force menunjukkan peningkatan traffic hingga 60 Kbps dan penggunaan CPU mencapai 100%, kemudian terjadi penurunan setelah firewall active response diaktifkan. Authentication failure mencapai 2198 kali dalam satu jam pertama serangan brute force. Penggunaan CPU meningkat dari 20% hingga 85% selama serangan dan menurun menjadi 15% setelah firewall active response diaktifkan. Serangan DoS, pada MikroTik mengalami peningkatan penggunaan CPU hingga 89% dan memori 56.32%. Setelah aktivasi firewall active response, penggunaan CPU menurun menjadi 5%. Traffic pada interface MikroTik meningkat hingga 3.3 Mbps selama serangan, kemudian menurun ke 1 Kbps setelah firewall diaktifkan.

Jakarta, 09 Agustus 2024

Hillman Akhyar Damanik

SURAT PENGALIHAN HAK CIPTA

Yang bertanda tangan dibawah ini:

1. Nama	: Hillman Akhyar Damanik
2. Kewarganegaraan	: Indonesia
3. Alamat	: Flamboyan Unit No.57 Jl. Mesjid Nurul Iman Cipadu - Tangerang 15155
4. Telepon	:
5. No. HP & E-mail	: 082299099294 & hilladamanik@gmail.com

Adalah Pihak I selaku pencipta, dengan ini menyerahkan karya ciptaan saya kepada:

Nama	: DRPM Universitas Budi Luhur
Alamat	: Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta 1220

Adalah Pihak II selaku Pemegang Hak Cipta berupa Analisis dan Mitigasi Kerentanan DDoS pada Infrastuktur Jaringan dengan Teknik *Hierarchical Clustering* dan Firewall IPTables untuk didaftarkan di Direktorat Hak Cipta, Desain Industri, Desain Tata Letak dan Sirkuit Terpadu dan Rahasia Dagang, Direktorat Jenderal Hak Kekayaan Intelektual, Kementerian Hukum dan Hak Azasi Manusia R.I.

Demikianlah surat pengalihan hak ini kami buat, agar dapat dipergunakan sebagaimana mestinya.

Jakarta, 09 Agustus 2024

Pemegang Hak Cipta	Pencipta
(Dr. Ir. Prudensius Maring, M.A)	(Hillman Akhyar Damanik)

SURAT PERNYATAAN

Yang bertanda tangan dibawah ini:

1. Nama	: Hillman Akhyar Damanik
2. Kewarganegaraan	: Indonesia
3. Alamat	: Flamboyan Unit No.57 Jl. Mesjid Nurul Iman Cipadu - Tangerang 15155
4. Telepon	:
5. No. HP & E-mail	: 082299099294 & hilladamanik@gmail.com

Dengan ini menyatakan bahwa:

1. Karya Cipta yang saya mohonkan:

Berupa	: Penelitian
Berjudul	: Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Extended Detection and Response (XDR) dan Framework Firewall

Tidak meniru dan tidak sama secara esensial dengan Karya Cipta milik pihak lain atau obyek kekayaan intelektual lainnya sebagaimana dimaksud dalam Pasal 68 ayat (2);

- Bukan merupakan Ekspresi Budaya Tradisional sebagaimana dimaksud dalam Pasal 38;
- Bukan merupakan Ciptaan yang tidak diketahui penciptanya sebagaimana dimaksud dalam Pasal 39;

- Bukan merupakan hasil karya yang tidak dilindungi Hak Cipta sebagaimana dimaksud dalam Pasal 41 dan 42;
- Bukan merupakan Ciptaan seni lukis yang berupa logo atau tanda pembeda yang digunakan sebagai merek dalam perdagangan barang/jasa atau digunakan sebagai lambang organisasi, badan usaha, atau badan hukum sebagaimana dimaksud dalam Pasal 65 dan;
- Bukan merupakan Ciptaan yang melanggar norma agama, norma susila, ketertiban umum, pertahanan dan keamanan negara atau melanggar peraturan perundang-undangan sebagaimana dimaksud dalam Pasal 74 ayat (1) huruf d Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

2. Sebagai pemohon mempunyai kewajiban untuk menyimpan asli contoh ciptaan yang dimohonkan dan harus memberikan apabila dibutuhkan untuk kepentingan penyelesaian sengketa perdata maupun pidana sesuai dengan ketentuan perundang-undangan.
3. Karya Cipta yang saya mohonkan pada Angka 1 tersebut di atas tidak pernah dan tidak sedang dalam sengketa pidana dan/atau perdata di Pengadilan.
4. Dalam hal ketentuan sebagaimana dimaksud dalam Angka 1 dan Angka 3 tersebut di atas saya / kami langgar, maka saya / kami bersedia secara sukarela bahwa:

a. Permohonan karya cipta yang saya ajukan dianggap ditarik kembali; Karya Cipta yang telah terdaftar dalam Daftar Umum Ciptaan Direktorat Hak Cipta, Direktorat Jenderal Hak Kekayaan Intelektual, Kementerian Hukum Dan Hak Asasi Manusia R.I dihapuskan sesuai dengan ketentuan perundang-undangan yang berlaku.
b. Dalam hal kepemilikan Hak Cipta yang dimohonkan secara elektronik sedang dalam berperkara dan/atau sedang dalam gugatan di Pengadilan maka status kepemilikan surat pencatatan elektronik tersebut ditangguhkan menunggu putusan Pengadilan yang berkekuatan hukum tetap.

Demikian Surat pernyataan ini saya / kami buat dengan sebenarnya dan untuk dipergunakan sebagimana mestinya.

Jakarta, 09 Agustus 2024

Yang menyatakan,