WAZUH PORTOFOLIO

IMPLEMENTASI MONITORING LOG MENGGUNAKAN WAZUH

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan sistem informasi merupakan aspek krusial dalam pengelolaan infrastruktur teknologi. Setiap aktivitas yang terjadi di dalam sistem akan menghasilkan log, baik berupa aktivitas login, perubahan konfigurasi, akses file, maupun aktivitas jaringan. Log tersebut menjadi sumber informasi penting dalam mendeteksi ancaman keamanan.

Salah satu solusi untuk melakukan monitoring log secara terpusat adalah dengan menggunakan sistem Security Information and Event Management (SIEM). Wazuh merupakan platform open-source SIEM yang mampu melakukan pengumpulan log, analisis keamanan, deteksi ancaman, serta integrasi dengan framework MITRE ATT&CK.

Dalam proyek ini dilakukan implementasi Wazuh untuk memahami bagaimana sistem monitoring log bekerja serta bagaimana serangan dapat terdeteksi berdasarkan analisis log sistem.

1.2 Rumusan Masalah

Rumusan masalah dalam proyek ini adalah:

1. Bagaimana cara mengimplementasikan Wazuh sebagai sistem monitoring log?
2. Bagaimana Wazuh membaca dan menganalisis log sistem?
3. Bagaimana sistem mendeteksi serangan brute force berbasis log?
4. Bagaimana alert ditampilkan dan dianalisis melalui dashboard?

1.3 Tujuan Proyek

Tujuan dari proyek ini adalah:

1. Memahami konsep dasar SIEM.
2. Mempelajari proses pengumpulan log pada sistem Linux.
3. Memahami mekanisme analisis log oleh Wazuh.
4. Menguji kemampuan deteksi serangan brute force SSH.
5. Menganalisis hasil deteksi berdasarkan rule dan MITRE ATT&CK.

BAB II

LANDASAN TEORI

2.1 Konsep Monitoring Log

Monitoring log adalah proses pengumpulan, penyimpanan, dan analisis data aktivitas sistem untuk mendeteksi kejadian abnormal atau mencurigakan. Log sistem dapat digunakan untuk:

- Audit keamanan
- Deteksi intrusi
- Investigasi insiden
- Analisis forensik

2.2 Security Information and Event Management (SIEM)

SIEM adalah sistem yang menggabungkan fungsi:

- Security Information Management (SIM)
- Security Event Management (SEM)

SIEM memungkinkan organisasi untuk mengumpulkan log dari berbagai sumber, melakukan korelasi, dan menghasilkan alert keamanan secara real-time.

2.3 Wazuh

Wazuh adalah platform keamanan open-source yang menyediakan fitur:

- Log monitoring
- Intrusion Detection System (IDS)
- File Integrity Monitoring (FIM)
- Vulnerability detection
- Active response
- Integrasi dengan MITRE ATT&CK

Komponen utama Wazuh:

1. Wazuh Manager
2. Wazuh Indexer
3. Wazuh Dashboard

BAB III

METODOLOGI DAN PERANCANGAN SISTEM

3.1 Lingkungan Pengujian

Proyek ini menggunakan dua virtual machine yang dijalankan pada Oracle VirtualBox.

1. Server Monitoring (Wazuh Server)

- Sistem Operasi: Ubuntu Server
- RAM: 4 GB
- Storage: 40 GB
- Versi Wazuh: 4.7.5-1

Fungsi server:

- Menjalankan Wazuh Manager
- Menjalankan Wazuh Indexer
- Menjalankan Wazuh Dashboard
- Menjadi target serangan SSH
- Menghasilkan log sistem

2. Mesin Attacker

- Sistem Operasi: Kali Linux
- Tools: Hydra

Fungsi:

- Melakukan simulasi brute force SSH
- Menghasilkan log autentikasi gagal pada server target

3.2 Topologi Sistem

Alur sistem dalam pengujian ini adalah:

Kali Linux (Attacker)
↓
SSH Brute Force
↓
Ubuntu Server (Target)
↓
Log tersimpan di /var/log/auth.log
↓
Wazuh membaca log

↓
Wazuh menganalisis dan mencocokkan rule
↓
Alert muncul di Wazuh Dashboard

BAB IV

IMPLEMENTASI SISTEM

4.1 Instalasi Wazuh

Instalasi dilakukan menggunakan script resmi Wazuh dengan metode all-in-one.

Perintah instalasi:

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

sudo bash wazuh-install.sh -a --ignore-check

Penjelasan parameter:

- -a : Menginstal seluruh komponen (Manager, Indexer, Dashboard).
- --ignore-check : Digunakan jika terjadi error pengecekan versi sistem.

```
kenevan@Wazuh:~$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
kenevan@Wazuh:~$ sudo bash wazuh-install.sh -a --ignore-check
```

4.2 Verifikasi Service

Setelah instalasi selesai, dilakukan pengecekan service:

sudo systemctl status wazuh-manager

sudo systemctl status wazuh-indexer

sudo systemctl status wazuh-dashboard

Jika seluruh service aktif (running), maka instalasi berhasil.

4.3 Akses Dashboard

1. Buka browser.
2. Masukkan IP server Wazuh.
3. Login menggunakan:
    - Username: admin
    - Password: diberikan saat instalasi selesai. Apabila ingin mengganti passwordnya bisa menggunakan

    sudo /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-password-tool.sh -u admin -p Admin123?

    Jangan lupa di restart

    Sudo systemctl restart wazuh-dashboard

```
kenevan@Wazuh:~$ sudo /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh -u admin -p Admin123?
20/02/2026 08:53:19 INFO: Generating password hash
20/02/2026 08:53:57 WARNING: Password changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
kenevan@Wazuh:~$ ^C
kenevan@Wazuh:~$ sudo systemctl restart wazuh-dashboard
```

Dashboard digunakan untuk melihat alert, event, dan hasil analisis log.

BAB V

PENGUJIAN DAN ANALISIS

5.1 Skenario Pengujian

Pengujian dilakukan dengan melakukan serangan brute force SSH menggunakan Hydra dari Kali Linux.

Target:
Layanan SSH pada Ubuntu Server.

Serangan menghasilkan banyak percobaan login gagal yang tercatat pada:

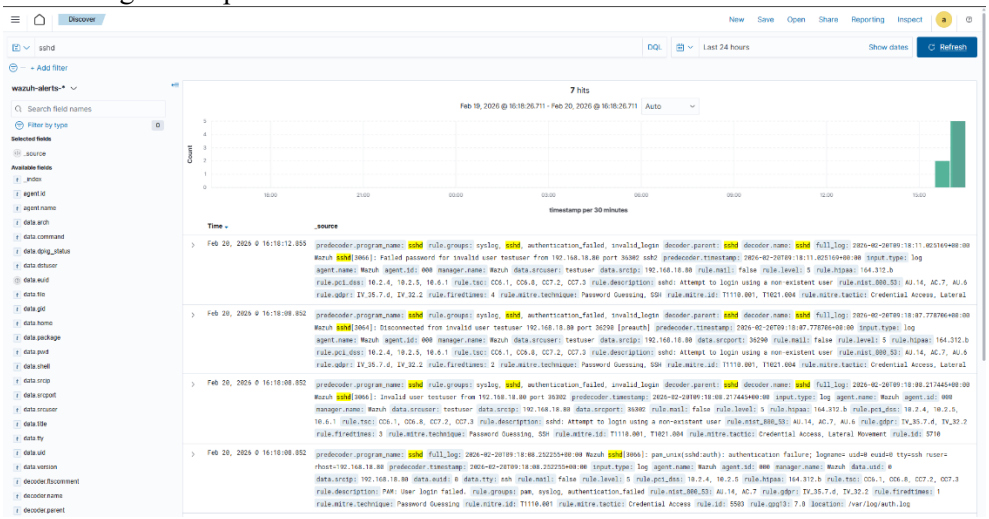
/var/log/auth.log

5.2 Hasil Deteksi

Setelah serangan dilakukan, Wazuh mendeteksi aktivitas mencurigakan dengan detail sebagai berikut:

- Rule ID: 5710
- Rule Level: 5
- Description: sshd: Attempt to login using a non-existent user
- MITRE ATT&CK ID: T1110.001
- Technique: Password Guessing
- Log Source: sshd
- Log Location: /var/log/auth.log

Contoh log:Failed password for invalid user



5.3 Analisis

Proses deteksi terjadi sebagai berikut:

1. SSH mencatat login gagal.
2. Log masuk ke file auth.log.
3. Wazuh membaca log tersebut.
4. Decoder SSH memproses format log.
5. Rule 5710 dicocokkan.
6. Alert level 5 dihasilkan.
7. Alert muncul di dashboard.

Mapping ke MITRE ATT&CK menunjukkan teknik Credential Access melalui Password Guessing (T1110.001).

Hal ini membuktikan bahwa sistem monitoring bekerja secara real-time dalam mendeteksi aktivitas brute force.

BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan implementasi dan pengujian yang dilakukan, dapat disimpulkan bahwa:

1. Wazuh berhasil diinstal dan berjalan dengan baik pada Ubuntu Server.
2. Sistem mampu membaca dan menganalisis log SSH.
3. Serangan brute force berhasil terdeteksi.
4. Alert ditampilkan secara real-time pada dashboard.
5. Deteksi dapat dipetakan ke MITRE ATT&CK framework.

Proyek ini memberikan pemahaman yang jelas mengenai cara kerja SIEM dan pentingnya monitoring log dalam keamanan sistem.

6.2 Saran Pengembangan

Beberapa pengembangan yang dapat dilakukan:

1. Menambahkan agent pada beberapa endpoint.
2. Mengaktifkan fitur Active Response untuk memblokir IP attacker otomatis.
3. Mengaktifkan File Integrity Monitoring (FIM).
4. Mengintegrasikan notifikasi email.
5. Menguji serangan lain seperti privilege escalation atau web attack.

Dengan pengembangan tersebut, sistem monitoring dapat lebih menyerupai implementasi Security Operations Center (SOC) di lingkungan nyata.

Jika Anda mau, saya bisa:

- Mengubah ini ke format skripsi lengkap (Bab I–V dengan daftar isi).
- Menambahkan bagian screenshot placeholder untuk laporan.
- Menambahkan bagian konfigurasi Hydra dan contoh perintahnya.
- Membuat versi yang siap langsung dimasukkan ke file .docx yang lebih rapi dan formal.