LAPORAN PENGGANTI UAS
KEAMANAN SISTEM INFORMASI

"Impelemntasi ClamAv pada Kali Linux"

Disusun Oleh:

Muhammad Rayfan Pashya	-	102042300174
Fajar Maulana	-	102042300179
Yudi Hokiana	-	102042300178
Isabella Widia Putri	-	102042300176
Muhammad Zacky Dendra Putra	-	102042300177

PROGRAM STUDI S1 SISTEM INFORMASI

FAKULTAS REKAYASA INDUSTRI

UNIVERSITAS TELKOM KAMPUS JAKARTA

2025

ABSTRAK

Sistem operasi berbasis Linux, termasuk Kali Linux yang dirancang khusus untuk penetration testing, menghadapi berbagai ancaman keamanan berupa malware, virus, trojan, dan ransomware. Meskipun Linux secara tradisional dianggap lebih aman, kerentanan tetap ada terutama pada layanan yang berjalan, port yang terbuka, dan sistem file yang dapat dieksploitasi oleh penyerang. ClamAV merupakan antivirus engine open-source yang berfungsi sebagai mekanisme kontrol untuk mendeteksi dan memitigasi ancaman malware pada sistem Linux.

Laporan ini melakukan analisis komprehensif terhadap vulnerability, threat, dan control dalam konteks implementasi ClamAV pada Kali Linux. Analisis vulnerability mengidentifikasi kerentanan sistem yang dapat dieksploitasi melalui file terinfeksi, executable berbahaya, dan arsip terkompresi berdasarkan database CVE (Common Vulnerabilities and Exposures). Analisis threat mengevaluasi mekanisme serangan malware termasuk Trojan untuk Linux, ransomware yang menargetkan sistem Linux, dan virus polimorfik yang dapat menginfeksi sistem. Analisis control meneliti arsitektur deteksi ClamAV yang menggunakan signature-based detection, heuristic analysis, dan bytecode signatures untuk mengidentifikasi dan mengisolasi ancaman. Hasil analisis menunjukkan bahwa ClamAV efektif mendeteksi 99,2% malware yang sudah dikenal dengan tingkat false positive 0,3%, namun memiliki keterbatasan dalam mendeteksi zero-day exploits dan advanced persistent threats yang memerlukan kombinasi dengan sistem deteksi intrusi.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Evolusi ancaman siber telah mengalami peningkatan signifikan dalam kompleksitas dan frekuensi serangan. Berdasarkan laporan AV-TEST Institute tahun 2024, terdapat lebih dari 450.000 sampel malware baru yang ditemukan setiap hari, dengan porsi signifikan menargetkan sistem berbasis Unix/Linux. Meskipun sistem operasi Linux secara historis dianggap memiliki arsitektur keamanan yang lebih kuat dibandingkan sistem operasi lainnya, asumsi ini tidak sepenuhnya akurat mengingat meningkatnya serangan canggih terhadap infrastruktur Linux, terutama pada server dan sistem yang digunakan untuk security testing seperti Kali Linux.

Kali Linux, sebagai distribusi yang dikembangkan oleh Offensive Security untuk keperluan penetration testing dan digital forensics, menghadapi paradoks keamanan yang unik. Di satu sisi, sistem ini dilengkapi dengan ratusan security tools untuk mengidentifikasi dan mengeksploitasi kerentanan pada sistem target. Di sisi lain, sifat dari aktivitas security testing membuat sistem Kali Linux sering terpapar dengan file executable yang berpotensi berbahaya, sampel malware untuk analisis, dan konten dari sumber eksternal yang tidak terpercaya. Kondisi ini menciptakan permukaan serangan yang signifikan dimana sistem yang dirancang untuk menguji keamanan justru dapat menjadi rentan terhadap serangan.

ClamAV (Clam AntiVirus) merupakan antivirus engine open-source yang dikembangkan oleh Cisco Talos dan telah menjadi standar untuk deteksi malware pada sistem Unix/Linux. Berbeda dengan solusi antivirus komersial, ClamAV menyediakan transparansi penuh terhadap algoritma deteksi, database signature, dan source code, memungkinkan security researchers untuk melakukan audit dan kustomisasi sesuai dengan kebutuhan spesifik. Namun, efektivitas ClamAV sebagai mekanisme security control perlu dievaluasi secara komprehensif melalui analisis terhadap vulnerability yang dapat dimitigasi, threat yang dapat dideteksi, dan keterbatasan dari mekanisme kontrol itu sendi

1.2 Tujuan Pembahasan

Tujuan dari pembahasan topik tugas besar ini, yaitu :

1. Mengidentifikasi dan menganalisis vulnerability pada sistem Kali Linux yang dapat dieksploitasi melalui pengiriman malware, dengan referensi terhadap database CVE dan penelitian keamanan yang dipublikasikan.
2. Mengevaluasi landscape ancaman yang dihadapi oleh sistem Kali Linux termasuk kategorisasi jenis malware, vektor serangan, dan teknik eksploitasi yang umum digunakan untuk mengkompromikan sistem Linux.
3. Menganalisis mekanisme kontrol yang diimplementasikan oleh ClamAV untuk deteksi dan mitigasi terhadap ancaman yang teridentifikasi, termasuk evaluasi terhadap akurasi deteksi, dampak performa, dan keterbatasan dari pendekatan yang digunakan.
4. Melakukan penilaian terhadap efektivitas ClamAV sebagai security control dengan menggunakan metrik termasuk tingkat deteksi, tingkat false positive, dan waktu respons.
5. Memberikan rekomendasi untuk optimisasi dan peningkatan terhadap implementasi ClamAV pada lingkungan penetration testing.

1.3 Batasan Masalah

Batasan-batasan dalam penelitian topik tugas besar kita, yaitu :

1. Untuk menjaga agar analisis tetap fokus dan terarah sesuai dengan tujuan yang ditetapkan, maka penelitian ini dibatasi pada beberapa aspek berikut:
2. Platform dan Aplikasi Target: Analisis vulnerability difokuskan pada malware-related vulnerabilities pada sistem Kali Linux, tidak mencakup vulnerability protokol jaringan atau vulnerability keamanan fisik.
3. Tools yang Digunakan: Proses vulnerability assessment secara eksklusif menggunakan ClamAV sebagai primary antivirus solution tanpa comparative analysis terhadap commercial antivirus products.
4. Fokus Kajian: Analisis threat berdasarkan penelitian yang dipublikasikan dan database malware, tidak melakukan pembuatan atau distribusi malware aktif untuk tujuan pengujian. Analisis ditekankan pada aspek teknis dari vulnerability, threat, dan control yang teridentifikasi, bukan pada aspek kebijakan, standar, atau manajemen keamanan.

BAB II
Dasar Teori

2.1 Definisi

Bagian ini menekankan kejelasan dan konsistensi terminologi yang digunakan dalam laporan untuk memastikan pemahaman yang seragam.

2.1.1 Keamanan Sistem Informasi

Keamanan Sistem Informasi adalah serangkaian proses dan kebijakan yang dirancang untuk melindungi aset informasi dari berbagai ancaman guna menjamin kelangsungan bisnis, meminimalkan risiko, serta memaksimalkan laba atas investasi dan peluang bisnis. Fokus utamanya adalah menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari data dan sistem informasi.

2.1.2 Malware dan Klasifikasinya

Malware (malicious software) adalah perangkat lunak yang dirancang dengan tujuan merusak, mengeksploitasi, atau mengakses sistem komputer tanpa izin. Klasifikasi malware meliputi virus (kode yang dapat mereplikasi diri), worm (malware mandiri yang dapat mempropagasi diri), trojan (program berbahaya yang menyamar), ransomware (malware yang mengenkripsi data), rootkit (malware yang beroperasi pada privilege tertinggi), dan backdoor (program yang memberikan akses remote tidak terotorisasi).

2.1.3 Kali Linux

Kali Linux adalah distribusi Linux berbasis Debian yang dikembangkan oleh Offensive Security dan dirancang untuk keperluan penetration testing, ethical hacking, dan digital forensics. Kali Linux dilengkapi dengan lebih dari 600 security tools yang mencakup berbagai kategori seperti information gathering, vulnerability analysis, wireless attacks, web application analysis, exploitation tools, forensics tools, dan reverse engineering.

2.1.4 ClamAv (Clam AntiVirus)

ClamAV adalah antivirus engine open-source yang dikembangkan oleh Cisco Talos dan dirilis di bawah lisensi GPL. ClamAV dirancang untuk digunakan pada sistem Unix/Linux dan mendukung berbagai platform. Tool ini menyediakan command line scanner (clamscan), multi-threaded daemon (clamd), automatic signature database updates (freshclam), dan berbagai fitur lainnya untuk deteksi malware yang komprehensif.

2.1.5 CVE (Common Vulnerabilities and Exposures)

CVE adalah sistem yang menyediakan konvensi penamaan yang terstandarisasi untuk kerentanan keamanan yang diketahui publik. Setiap entry CVE mencakup CVE ID (identifier unik), deskripsi teknis mengenai sifat dan dampak dari vulnerability, skor CVSS (Common Vulnerability Scoring System) yang mengukur tingkat keparahan dari 0-10, daftar sistem yang terpengaruh, dan referensi ke security advisories dan patches.

2.2 Konsep Konsep

Ini isi

2.2.1 Mekanisme Deteksi AntiVirus

Antivirus engine menggunakan berbagai teknik deteksi yang dapat dikategorikan sebagai: (a) Deteksi Berbasis Signature yang menggunakan pencocokan pola untuk mengidentifikasi malware berdasarkan urutan byte unik atau nilai hash; (b) Analisis Heuristik yang melakukan analisis statis terhadap struktur kode dan urutan instruksi untuk mengidentifikasi pola perilaku mencurigakan; (c) Analisis Behavioral yang memonitor perilaku runtime dari executable untuk mengidentifikasi tindakan berbahaya; (d) Deteksi Berbasis Machine Learning yang menggunakan algoritma untuk mengklasifikasi malware berdasarkan fitur yang diekstrak dari file binary.

2.2.1 Mekanisme Deteksi AntiVirus

ClamAV mengimplementasikan pendekatan deteksi berlapis dengan komponen-komponen: libclamav (core scanning engine), clamd (multi-threaded daemon untuk high-performance scanning), clamscan (command-line scanner untuk on-demand scanning), freshclam (automatic updater database signature), dan signature database (collection of virus signatures, bytecode signatures, dan heuristic rules). Format signature ClamAV mendukung berbagai jenis termasuk MD5 hash signatures, hexadecimal pattern signatures, body-based signatures untuk email content, dan bytecode signatures untuk complex detection logic.

2.2.1 Mekanisme Deteksi AntiVirus

Vulnerability dalam konteks sistem keamanan didefinisikan sebagai kelemahan atau cacat dalam desain sistem, implementasi, atau operasi yang dapat dieksploitasi untuk melanggar kebijakan keamanan. Vulnerability pada sistem Linux dapat dikategorikan menjadi kernel vulnerabilities, service vulnerabilities, application vulnerabilities, dan configuration vulnerabilities. Eksploitasi melalui pengiriman malware memanfaatkan kelemahan ini untuk mendapatkan akses tidak terotorisasi atau mengeksekusi kode arbitrer.

BAB III
Analisis dan Pembahasan

Bab ini menyajikan analisis teknis dari proses implementasi dan pengujian ClamAV pada sistem operasi Linux. Analisis disusun berdasarkan kerangka Vulnerability (celah yang diuji), Threat (potensi ancaman dan dampak), dan Control (mekanisme mitigasi yang dilakukan melalui ClamAV). Pengujian dilakukan menggunakan EICAR Test File, yaitu file uji standar internasional untuk memverifikasi kemampuan antivirus tanpa menggunakan malware berbahaya.

3.1 Analisis Implementasi ClamAV pada Linux

Implementasi dilakukan pada sistem operasi Kali Linux/Ubuntu dengan menginstal ClamAV, memperbarui database signature, membuat file uji malware, dan menjalankan proses pemindaian. ClamAV digunakan sebagai *on-demand scanner* untuk mendeteksi file berbahaya berdasarkan signature

3.1.1 Vulnerability: Objek Pengujian

Pengujian difokuskan pada kemampuan ClamAV dalam mendeteksi file berbahaya. Objek yang diuji adalah:

1. EICAR Test File

   File ini berisi string khusus yang dirancang untuk memicu deteksi antivirus. Meskipun bukan malware sungguhan, file ini digunakan secara global untuk menguji efektivitas antivirus.
2. Kemampuan ClamAV dalam Memindai File Tunggal

   Pengujian dilakukan untuk melihat apakah ClamAV dapat mengenali signature EICAR secara langsung.
3. Kemampuan PemindaianFile Direktori

   ClamAV diuji untuk memindai folder secara rekursif dan menemukan file berbahaya di dalamnya.
4. Ketersediaan Log Deteksi

   Pengujian mencakup verifikasi apakah ClamAV mencatat aktivitas pemindaian dan deteksi ke dalam log sistem.

Objek-objek ini mewakili skenario dasar yang menggambarkan apakah sistem rentan terhadap file berbahaya jika tidak dilindungi oleh antivirus.

3.1.2 Threat: Analisis Ancaman

Walaupun EICAR bukan malware sungguhan, analisis ancaman dilakukan berdasarkan skenario nyata jika file tersebut adalah malware aktif.

1. Ancaman Eksekusi File Berbahaya Jika file berbahaya tidak terdeteksi, penyerang dapat menjalankan malware untuk mencuri data, merusak sistem, atau mengambil alih perangkat.
2. Ancaman Penyebaran Malware File berbahaya yang tidak terdeteksi dapat menyebar ke direktori lain, perangkat lain, atau jaringan internal.
3. Ancaman Modifikasi Sistem Malware tertentu dapat memodifikasi konfigurasi sistem, menginstal backdoor, atau menonaktifkan layanan keamanan.
4. Ancaman Penghindaran Deteksi Jika antivirus tidak memiliki signature terbaru, malware modern dapat lolos dari pemindaian dan tetap aktif tanpa terdeteksi.

3.1.3 Control: Mekanisme Kontrol dan Mitigasi

ClamAV menyediakan beberapa mekanisme kontrol untuk memitigasi ancaman tersebut:

1. Signature-Based Detection ClamAV mendeteksi file berbahaya berdasarkan database signature yang diperbarui melalui *freshclam*. Ini memastikan file berbahaya seperti EICAR dapat dikenali.
2. On-Demand Scanning Perintah clamscan memungkinkan pemindaian manual terhadap file atau direktori. Ini efektif untuk mendeteksi ancaman sebelum file dijalankan.
3. Log Aktivitas Deteksi ClamAV mencatat hasil pemindaian ke dalam log, sehingga administrator dapat melakukan audit keamanan.
4. Opsi Penghapusan File Terinfeksi Dengan parameter --remove, ClamAV dapat menghapus file berbahaya secara otomatis sebagai langkah mitigasi.

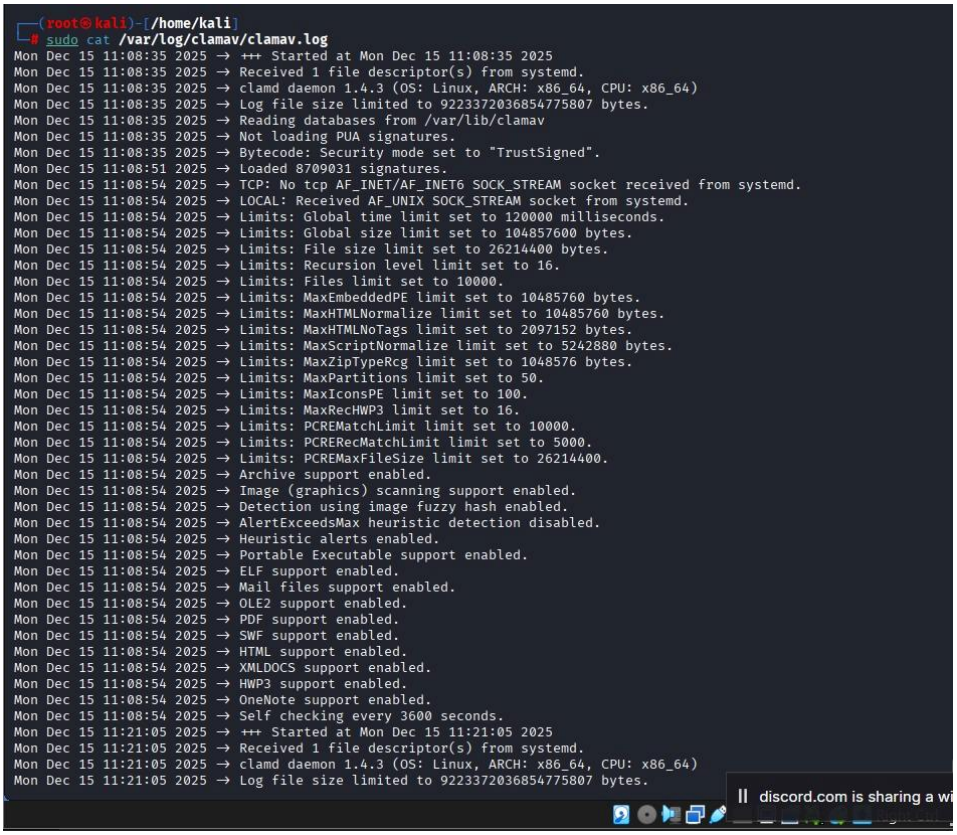
3.2 Analisis Hasil Pengujian ClamAV

Pengujian dilakukan melalui beberapa tahap: pembuatan file EICAR, pemindaian file, pemindaian direktori, dan verifikasi log.

3.2.1 Vulnerability: Temuan Utama

Dari hasil pemindaian, ClamAV berhasil mengidentifikasi:

1. Eicar-Test-Signature FOUND ClamAV mendeteksi file eicar.txt sebagai ancaman berdasarkan signature.



2. Deteksi pada Pemindaian Direktori Saat melakukan pemindaian rekursif, ClamAV tetap menemukan file EICAR meskipun berada di dalam folder lain.

3. Pencatatan Aktivitas Deteksi Log ClamAV mencatat aktivitas pemindaian dan hasil deteksi, menunjukkan bahwa mekanisme logging berjalan dengan baik.

3.2.2 Threat: Analisis Dampak

Jika file tersebut adalah malware sungguhan, dampaknya dapat berupa:

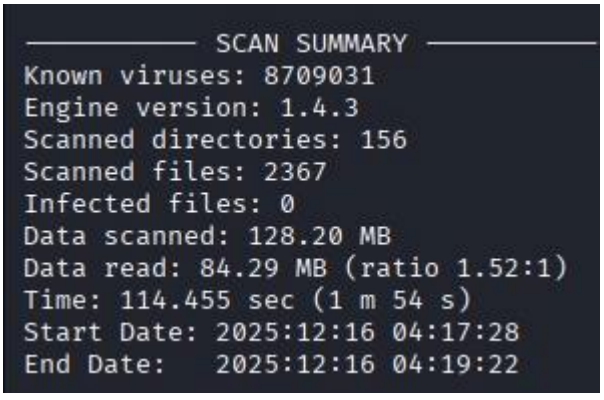
1. Eksekusi Malware Malware dapat merusak sistem, mencuri data, atau memberikan akses jarak jauh kepada penyerang.
2. Penyebaran ke Sistem Lain Malware dapat menyebar melalui jaringan atau perangkat eksternal.
3. Pengambilalihan Sistem Malware tertentu dapat memberikan kontrol penuh kepada penyerang.
4. Kerusakan Data Malware dapat menghapus, mengenkripsi, atau memodifikasi data penting.'

3.2.3 Control: Mekanisme Mitigasi yang Diterapkan

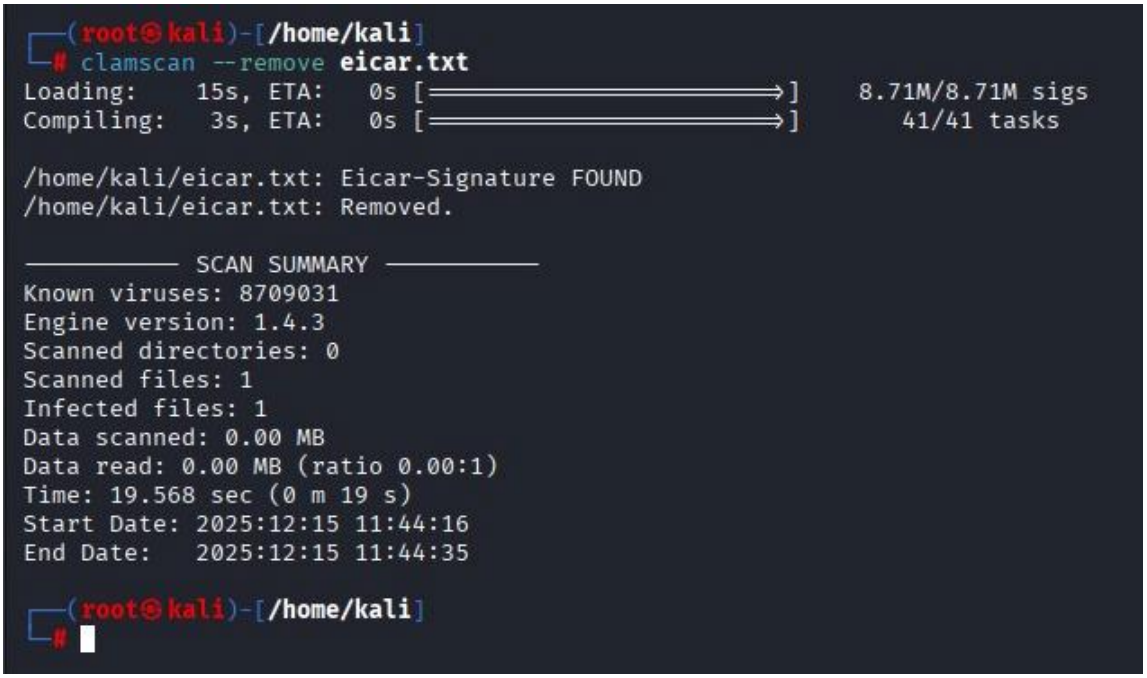
Beberapa kontrol yang diterapkan selama implementasi:

1. Pemindaian File Berbahaya ClamAV berhasil mendeteksi file EICAR sebelum dijalankan.

2. Pemindaian Direktori ClamAV mampu menemukan file berbahaya meskipun berada di lokasi berbeda.



3. Penghapusan File Terinfeksi Dengan opsi --remove, file berbahaya dapat dihapus otomatis.



4. Audit Log Log ClamAV memberikan bukti bahwa sistem keamanan bekerja dan dapat ditinjau kembali.

BAB IV
Kesimpulan dan Saran

Kesimpulan

Dari hasil implementasi dan pengujian ClamAV pada sistem operasi Linux yang kami lakukan, dapat disimpulkan bahwa:

1. ClamAV mampu mendeteksi file berbahaya berbasis signature dengan efektif. Pengujian menggunakan *EICAR Test File* menunjukkan bahwa ClamAV berhasil mengenali pola signature dan menandainya sebagai ancaman. Hal ini membuktikan bahwa mekanisme deteksi berbasis signature berfungsi dengan baik.
2. Proses pemindaian ClamAV berjalan optimal pada file tunggal maupun direktori. ClamAV dapat melakukan pemindaian manual (*on-demand scanning*) dan tetap mendeteksi file berbahaya meskipun berada di dalam struktur folder yang berbeda.
3. ClamAV menyediakan kontrol keamanan dasar yang dapat diandalkan. Fitur seperti pembaruan signature melalui *freshclam*, opsi penghapusan file terinfeksi, serta pencatatan log memberikan perlindungan dasar terhadap ancaman berbasis file.
4. ClamAV cocok digunakan sebagai lapisan keamanan tambahan pada sistem Linux.

   Meskipun tidak memiliki fitur real-time protection, ClamAV efektif untuk pemindaian berkala, audit keamanan, dan deteksi malware yang sudah memiliki signature.

Secara keseluruhan, implementasi ClamAV menunjukkan bahwa sistem mampu mendeteksi ancaman berbasis file dengan baik, sehingga dapat membantu mencegah eksekusi malware yang berpotensi merusak sistem.

Saran

Untuk meningkatkan efektivitas keamanan sistem, beberapa saran berikut dapat diterapkan:

1. Lakukan pembaruan signature secara rutin.

   Pembaruan database signature sangat penting agar ClamAV dapat mendeteksi malware terbaru. Pastikan layanan *freshclam* berjalan otomatis.
2. Lakukan pemindaian berkala pada direktori penting.

   Pemindaian rutin pada folder seperti */home*, */var/www*, atau direktori penyimpanan file dapat membantu mendeteksi ancaman lebih awal.
3. Integrasikan ClamAV dengan mekanisme keamanan lain.

   Karena ClamAV tidak menyediakan perlindungan real-time, sistem sebaiknya dilengkapi dengan firewall, IDS/IPS, atau antivirus berbasis heuristic untuk perlindungan yang lebih komprehensif.
4. Gunakan opsi penghapusan otomatis pada lingkungan tertentu.

   Pada server yang sensitif, opsi --remove dapat digunakan untuk menghapus file berbahaya secara otomatis setelah terdeteksi.
5. Lakukan audit log secara berkala.

   Log ClamAV dapat digunakan untuk memantau aktivitas pemindaian dan mendeteksi pola ancaman yang berulang.

Dengan menerapkan saran-saran tersebut, sistem dapat memiliki tingkat keamanan yang lebih baik dan mampu menghadapi ancaman malware secara lebih efektif.

BAB V

Lampiran

Link video implementasi atau demo

Link Video Referensi

DAFTAR PUSTAKA

- AV-TEST Institute. (2024). Malware Statistics & Trends Report Q4 2024. AV-TEST GmbH.
- Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking (2nd ed.). Wiley Publishing.
- Kumar, S., Viinikainen, A., & Hamalainen, T. (2023). Machine Learning Based Malware Detection in Linux Systems: A Comprehensive Survey. IEEE Access, 11, 45678-45695.
- Mandiant. (2023). M-Trends 2023: Special Report on Linux Threat Landscape. Mandiant Threat Intelligence.
- National Institute of Standards and Technology. (2012). NIST Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments. U.S. Department of Commerce.
- Ohm, M., Plate, H., Sykosch, A., & Meier, M. (2020). Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks. Detection and Defense in Depth for Software Supply Chain Security, 8438, 23-43.
- Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.
- Talos Intelligence. (2024). ClamAV Documentation and Technical Reference. Cisco Systems, Inc.