BAB II
TINJAUAN PUSTAKA

2.1. Penelitian Terkait

Tabel 2.1 Penelitian Terkait

Jurnal	Penulis	Deskripsi	Perbedaan
Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVAS (2023)	Afif Saktiansyah	Implementasi OpenVAS pada jaringan PT. Dutakom Wibawa Putra. Dengan hasil analisis menunjukkan kelemahan kritis di jaringan perusahaan, dan dilanjutkan dengan eksploitasi menggunakan *Metasploit*.	Pada penelitian ini OpenVAS tidak digunakan pada jaringan tetapi di Ubuntu *Server*. Serta dijelaskan cara instalasinya
On the Review and Setup of Security Audit Using Kali Linux (2018)	Teddy Surya Gunawan, Muhammad Kassim Lim, Nurul Zulkurnain,	Membahas uji penetrasi dan analisis keamanan kali linux, akan tetapi lebih berfokus kedalam pengujian penetrasi *server* yang rentan.	Pada penelitian ini melakukan implementasi Lynis diplatform Ubuntu *Server*, serta

	Mira Kartiwi		dijelaskan bagaimana cara penggunaan dan instalasi Lynis
Performance Evaluation of Snort and Suricata Intrusion Detection Systems on Ubuntu Server (2020)	Alka Gupta, Lalitsen Sharma	Membahas pengujian dan perbandingan kinerja antara dua sistem deteksi intrusi, yaitu Snort dan Suricata pada Ubuntu *Server*. Pengujian mencakup beberapa parameter seperti jumlah paket yang berhasil dianalisis, jumlah paket yang terlewatkan oleh IDS, penggunaan CPU, dan penggunaan memori.	Pada penelitian ini membahas deteksi kerentanan pada Ubuntu *Server* menggunakan OpenVAS dan Lynis
VULNERABILITY ASSESSMENT PADA SITUS WWW.HATSEHAT.COM MENGGUNAKAN OPENVAS (2020)	Dewi Laksmiati	Berfokus pada uji coba fungsional alat Penilaian Kerentanan (*Vulnerability Assessment*)	Pada penelitian ini melakukan uji coba OpenVAS terhadap

		OpenVAS dengan melakukan pemindaian kerentanan terhadap situs www.hatsehat.com.	sistem operasi Ubuntu *Server*

2.2. Teknologi Komputer

Teknologi komputer adalah teknologi yang berhubungan dengan komputer, termasuk peralatan-peralatan yang berhubungan dengan komputer seperti printer, pembaca sidik jari, dan bahkan *CD-ROM*. Komputer adalah mesin serba guna yang dapat dikontrol oleh program, digunakan untuk mengolah data menjadi informasi. Program adalah deretan instruksi yang digunakan untuk mengendalikan komputer sehinggaa komputer dapat melakukan tindakan sesuai yang dikehendaki pembuatnya. Data adalah bahan mentah bagi komputer yang dapat berupa angka maupun gambar, sedangkan informasi adalah bentuk data yang telah diolah sehingga dapat menjadi bahan yang berguna untuk pengambilan keputusan.(Elisabeth, 2019)

2.3. Sistem Operasi

Sistem Operasi merupakan hal yang penting untuk dipahami karena merupakan salah satu *software* atau program yang sangat fundamental dalam pengoperasian komputer. Sistem operasi berperan sebagai pengelola sumber daya komputer dan menyediakan lingkungan untuk menjalankan aplikasi atau program. Dalam menjelaskan definisi sistem operasi, dapat merujuk pada berbagai sumber yang dianggap sebagai otoritas di bidang ilmu komputer.(Heryana *et al.*, 2023)

Berdasarkan sumber lain juga menjelaskan bahwa sistem operasi merupakan program pengolah piranti lunak dasar (*essential component*) yang tersimpan sebagai pengelola sumber daya perangkat keras komputer (*hardware*) atau program yang berkomunikasi atau berinterkasi langsung dengan perangkat keras (manajemen *hardware*) danmenyediakan layanan umum untuk aplikasi perangkat lunak (menajalankan aplikasi).(Wahid, 2019)

Gambar 2.1 Sistem Operasi

Sumber (https://pasarind.id/blog/Apa-itu-Sistem-Operasi-OS-berikut-penjelasan-Fungsi-dan-Contohnya)

2.4. Mesin Virtual

Mesin Virtual merupakan sebuah sistem operasi atau aplikasi yang diinstall pada hypervisor dan memiliki fungsi layaknya perangkat fisik (*hardware*) atau bisa juga disebut sebagai duplikat dari komputer asli. Virtualisasi, sebagai konsep yang mendasarinya, adalah suatu proses transformasi dari bentuk fisik menjadi bentuk *software* atau virtual. Proses ini melibatkan penggunaan *hypervisor*, sebuah *software* yang bertanggung jawab untuk menciptakan dan mengelola virtual machine. Dengan kata lain, mesin virtual adalah hasil dari penerapan teknologi virtualisasi yang memungkinkan sistem operasi, *server*, alat penyimpanan, dan perangkat jaringan untuk eksis dalam bentuk virtual, bekerja efisien di atas *hypervisor* tanpa harus terkait langsung dengan perangkat keras fisik.(Yudha, Wing and Eko, 2019)

2.5. VMware

VMware merupakan salah satu solusi untuk menjalankan beberapa sistem operasi agar dapat bekerja secara simultan pada sebuah komputer. VMware adalah suatu perangkat lunak yang dapat menciptakan atau menyimulasikan PC baru, yang disebut mesin virtual. Perangkat keras yang terdapat di dalam mesin virtual sama seperti perangkat yang dipakai *PC*, misalnya *CPU*, *RAM*, *hard disk*, *keyboard*, *mouse*, *CD/DVD Rom*, *soundcard*, dan sebagainya. Dengan kata lain, ada *PC* di dalam *PC*. Sistem operasi yang diinstal melalui VMware disebut *guest operating system*.(Indratno, 2022)

Gambar 2.2 VMware

Sumber (https://www.jetorbit.com/blog/apa-itu-vmware-pengertian-fungsi-keunggulan-dan-fitur/0029

2.6. Ubuntu Server

Ubuntu Server adalah sistem operasi yang dikembangkan oleh Canonical dan sejumlah besar pengembang sumber terbuka di seluruh dunia. Dirancang untuk menggerakkan server modern yang melayani halaman web statis dan dinamis, aplikasi, file, kontainer, dan banyak lagi. Kemampuannya untuk berjalan pada berbagai platform membuatnya menjadi pilihan yang sesuai baik untuk perusahaan maupun hobi.(Hasan,2024)

2.7. Keamanan Siber

Keamanan siber merupakan tindakan untuk melindungi informasi di dunia maya dari aneka serangan. Keamanan siber makin populer berhubung makin banyaknya penggunaan komputer seperti *desktop*, *laptop*, *smartphone*, *server*, dan perangkat *IoT (internet of things*) serta penggunaan jaringan komputer seperti internet dalam kehidupan umat manusia sehari-hari.(Budi, Wira and Infantono, 2021)

Gambar 2.3 Ilustrasi Keamanan Siber

Sumber (https://r17.co.id/insight/article/tetaplah-waspada-ancaman-serangan-siber-pada-dunia-pendidikan)

2.8. Docker

Docker adalah sebuah aplikasi yang berbasiskan teknologi *open source* yang memungkinkan *developer* atau siapapun untuk membuat, menjalankan, melakukan percobaan dan meluncurkan aplikasi di dalam sebuah *container*. Docker membuat proses pemaketan aplikasi bersama komponennya secara cepat dalam sebuah *container* yang terisolasi, sehingga dapat dijalankan dalam infrastruktur lokal tanpa melakukan perbuahan konfigurasi pada *container*.(Dwiyatno *et al.*, 2020)

Kontainer terisolasi satu sama lain dan berisi semua perangkat lunak yang diperlukan, termasuk *API* sistem operasi, perpustakaan, dan file konfigurasi. Kontainer dapat berkomunikasi satu sama lain melalui saluran yang terdefinisi dengan baik. Semua kontainer dijalankan oleh satu kernel sistem operasi sehingga lebih ringan daripada mesin virtual. Perangkat lunak yang meng-host kontainer disebut Docker *Engine* dan saat ini diinstal pada platform Linux, MS Windows, dan Apple MacOS.(Zaitsev and Luszczek, 2020)

2.9. OpenVAS

Open Vulnerability Assessment System (OpenVAS) adalah pemindai kerentanan yang dikelola dan didistribusikan oleh Greenbone Network. Alat ini dirancang sebagai pemindai kerentanan lengkap dengan berbagai tes bawaan dan antarmuka *web* yang memudahkan pengaturan dan menjalankan pemindaian kerentanan. Selain itu, OpenVAS juga menawarkan tingkat konfigurasi pengguna yang tinggi. Secara keseluruhan, OpenVAS merupakan alat yang kuat dan fleksibel untuk melakukan penilaian kerentanan, menyediakan informasi penting untuk meningkatkan keamanan sistem dan melindungi organisasi dari ancaman keamanan.(Muharrom and Saktiansyah, 2023)

Gambar 2 4 OpenVAS

Sumber (https://forum.greenbone.net/t/new-OpenVAS-logo/2795)

2.10. Lynis

Lynis adalah sebuah perangkat lunak sumber terbuka berupa skrip *shell* yang berfungsi berbasis *host*, dirancang untuk sistem operasi seperti Unix, Linux, Solaris 10, MAC, dan lainnya. Perangkat ini mendukung berbagai *plugin* dan pemeriksaan kepatuhan, menjadikannya alat yang efektif untuk memantau dan meningkatkan keamanan sistem operasi host.(Seth *et al.*, 2021)

Lynis melakukan pemindaian kesehatan dan keamanan pada PC atau server untuk meningkatkan penguatan keamanan dan pengujian kepatuhan. Semua audit Lynis bersifat khusus, artinya, setiap audit unik tergantung pada konfigurasi sistem, perangkat lunak yang diinstal, dan faktor lainnya. Semakin banyak komponen yang tersedia di sistem, semakin luas laporan auditnya.

Lynis juga menyediakan beberapa informasi terkait sistem operasi, seperti memori, pengguna, konektivitas jarinagan, *firewall*, dukungan *SNMP*, informasi audit pada *usb* dan perangkat penyimpanan pada sistem operasi

BAB III
RANCANGAN DAN REALISASI ATAU RANCANG BANGUN

3.1. Rancangan Penelitian

Penelitian ini menggunakan pendekatan kualitatif untuk mendapatkan pemahaman yang mendalam tentang keamanan pada sistem operasi Ubuntu *Server* dengan memanfaatkan alat keamanan seperti OpenVAS dan Lynis. Pendekatan kualitatif memungkinkan peneliti untuk mengeksplorasi secara holistik aspek keamanan pada Ubuntu Server melalui analisis terperinci dan pemahaman mendalam terhadap temuan dari alat keamanan tersebut.

3.2. Tahapan Penelitian

Berikut adalah tahapan penelitian yang akan dilakukan dalam penelitian ini:

3.2.1 Pengumpulan Data

a. Analisis Literatur: Melibatkan studi mendalam terhadap literatur terkait sistem operasi, Ubuntu *Server*, dan alat keamanan seperti OpenVAS dan Lynis.
b. Pemahaman Alat Keamanan: Mempelajari dan memahami cara OpenVAS dan Lynis bekerja serta kemampuan deteksi dan analisis keamanan yang mereka tawarkan.

3.2.2 Implementasi

a. Pemasangan Alat Keamanan: Melibatkan langkah-langkah instalasi OpenVAS dan Lynis pada lingkungan Ubuntu *Server* yang sesuai.
b. Konfigurasi Alat Keamanan: Menyesuaikan pengaturan dan konfigurasi agar sesuai dengan kebutuhan penelitian.

3.2.3 Pelaksanaan Pemindaian

a. Pemindaian dengan OpenVAS: Menjalankan pemindaian kerentanan menggunakan OpenVAS untuk mengidentifikasi potensi risiko keamanan.
b. Pemindaian dengan Lynis: Melakukan pemindaian dengan Lynis untuk mengevaluasi keamanan Ubuntu *Server* dari perspektif host-based.

3.2.4 Analisis Data

a. Interpretasi Hasil: Menganalisis hasil pemindaian dari OpenVAS dan Lynis untuk mengidentifikasi kerentanan keamanan dan rekomendasi perbaikan.

3.3. Objek Penelitian

Objek penelitian dalam penelitian ini adalah sistem operasi Ubuntu *Server* yang akan dievaluasi keamanannya menggunakan alat keamanan OpenVAS dan Lynis. Fokus penelitian akan ditempatkan pada pemahaman mendalam tentang kerentanan keamanan dan rekomendasi perbaikan yang diberikan oleh kedua alat tersebut.

Penelitian ini dilakukan pada server yang berada di Politeknik Negeri Jakarta. Tujuan penelitian ini adalah untuk mendapatkan pemahaman yang lebih mendalam tentang seberapa baik alat keamanan mendeteksi dan menangani kerentanan pada sistem operasi Ubuntu Server dan membandingkan kedua alat tersebut pada sistem operasi Ubuntu.

3.4. Model/ Framework/Teknik yang Digunakan

Vulnerability Assessment adalah proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi kerentanan keamanan dalam sistem komputer atau jaringan. Tujuan utamanya adalah untuk memahami dan mengurangi risiko keamanan dengan cara mendeteksi dan menangani kerentanan sebelum dimanfaatkan oleh pihak yang tidak berwenang. Berikut adalah penjelasan lebih rinci tentang tahapan *Vulnerability Assessment*:

a. Identifikasi Kerentanan:

   Tahap ini melibatkan penggunaan alat keamanan seperti OpenVAS untuk melakukan pemindaian sistem secara menyeluruh. Alat ini otomatis menemukan titik-titik rentan dalam keamanan sistem operasi Ubuntu *Server*, baik itu berada di jaringan, sistem operasi, maupun aplikasi yang berjalan di atasnya.

b. Menganalisis Kerentanan:

   Setelah kerentanan teridentifikasi, tahap ini melibatkan analisis mendalam terhadap sifat dan konteks dari setiap kerentanan yang ditemukan. Analisis mencakup penilaian terhadap tingkat keparahan, metode eksploitasi yang potensial, serta dampak yang dapat ditimbulkan terhadap keamanan system.

c. Penilaian Risiko:

Pada tahap ini, dilakukan penilaian risiko terhadap setiap kerentanan yang teridentifikasi. Evaluasi meliputi faktor-faktor seperti keparahan kerentanan, probabilitas eksploitasi oleh penyerang, dan dampak potensial terhadap sistem dan organisasi. Tujuan dari penilaian risiko ini adalah untuk memberikan prioritas kepada kerentanan yang paling mengancam keamanan sistem.

d. Remediasi:

Tahap terakhir dari proses *Vulnerability Assessment* adalah remediasi atau perbaikan. Langkah-langkah remediasi ini dirancang untuk mengurangi atau menghilangkan risiko yang terkait dengan kerentanan yang telah diidentifikasi. Tindakan remediasi dapat berupa penerapan *patch* keamanan, konfigurasi ulang sistem, atau tindakan lain yang direkomendasikan untuk meningkatkan keamanan sistem operasi Ubuntu *Server*.

3.5. Teknik Pengumpulan dan Analisis Data

3.5.1 Teknik Pengumpulan Data

Pada penelitian ini, pengumpulan data dilakukan melalui dua teknik utama:

a. Studi Literatur: Melibatkan analisis mendalam terhadap literatur terkait dengan sistem operasi, Ubuntu *Server*, dan alat keamanan seperti OpenVAS dan Lynis. Studi literatur membantu peneliti memahami konsep, teori, dan prinsip dasar yang menjadi dasar penelitian ini. Informasi yang diperoleh dari literatur akan digunakan sebagai landasan untuk memahami aspek keamanan pada sistem operasi Ubuntu *Server*.

b. Implementasi Alat Keamanan: Melibatkan pemasangan dan konfigurasi alat keamanan, yaitu OpenVAS dan Lynis, pada lingkungan Ubuntu *Server* yang sesuai. Selama implementasi, peneliti akan memahami cara kerja masing-masing alat, konfigurasi yang dapat disesuaikan, dan kemampuan deteksi keamanan yang dimiliki. Proses ini juga termasuk memastikan bahwa alat keamanan telah diaktifkan dan siap digunakan untuk pemindaian.

3.5.2 Analisis Data

Analisis data pada penelitian ini melibatkan beberapa tahap sebagai berikut:

a. Interpretasi Hasil Pemindaian: Setelah pemindaian dilakukan menggunakan OpenVAS dan Lynis, hasilnya akan diinterpretasi secara rinci. Peneliti akan

memahami kerentanan keamanan yang terdeteksi, tingkat risiko yang terkait, dan rekomendasi perbaikan yang diberikan oleh masing-masing alat keamanan. Interpretasi ini penting untuk mendapatkan gambaran yang komprehensif tentang keadaan keamanan Ubuntu *Server*.

b. Analisis Mendalam: Dilakukan analisis mendalam terhadap temuan dari pemindaian, termasuk pemahaman tentang sifat kerentanan dan potensi risiko yang mungkin timbul. Peneliti akan mengevaluasi keparahan kerentanan dan signifikansinya terhadap keamanan sistem operasi Ubuntu *Server*.

BAB IV
HASIL ANALISA DAN PEMBAHASAN

4.1 Analisis Kebutuhan

Analisis Pada tahap ini, analisis kebutuhan dilakukan untuk memastikan bahwa pengujian keamanan dilakukan dengan cakupan yang memadai dan sesuai dengan kebutuhan spesifik dari dua skenario yang diuji. Kebutuhan ini mencakup perangkat lunak yang digunakan, serta metode pengujian yang relevan untuk mengidentifikasi kerentanan dalam sistem.

Dalam implementasi ini, terdapat dua skenario pengujian utama:

1. Skenario 1: Mail Server

Postfix sebagai Mail Transfer Agent (MTA): Digunakan untuk mengelola pengiriman dan penerimaan email pada server.

Thunderbird sebagai Mail Client: Digunakan untuk menguji kemampuan server dalam menangani klien email.

2. Skenario 2: Web Server

Laravel sebagai framework aplikasi web: Digunakan untuk menjalankan aplikasi berbasis web yang diakses oleh pengguna.

MySQL sebagai database server: Berfungsi untuk menyimpan data aplikasi web.

PHP dan Apache sebagai platform: Digunakan untuk mengelola permintaan web dan menjalankan aplikasi Laravel.

4.1.1 Analisis Kebutuhan Perangkat Lunak

Analisis kebutuhan perangkat lunak melibatkan identifikasi perangkat lunak yang diperlukan untuk mendukung operasi dan fungsi dari sistem yang diimplementasikan. Berikut adalah perangkat lunak yang dibutuhkan:

1. Ubuntu Server 22.04

Ubuntu Server 22.04 adalah sistem operasi berbasis Linux yang terkenal karena stabilitas, keamanan, dan dukungan jangka panjang (*LTS*). Versi ini menawarkan pembaruan dan dukungan keamanan selama beberapa tahun, sehingga ideal untuk penggunaan jangka panjang di lingkungan *server*.

2. Lynis

   Lynis merupakan alat audit dan keamanan sistem *open-source* yang dirancang untuk sistem operasi berbasis Unix dan Linux. Lynis melakukan pemeriksaan menyeluruh terhadap konfigurasi sistem untuk mengidentifikasi potensi kerentanan dan memberikan rekomendasi perbaikan. Lynis digunakan untuk melakukan audit keamanan pada sistem Ubuntu Server 22.04, membantu dalam mengidentifikasi konfigurasi yang lemah, komponen yang usang, dan potensi titik masuk bagi penyerang.

3. Docker

   Docker adalah platform *open-source* yang memungkinkan pengembang untuk mengemas aplikasi dan semua dependensinya ke dalam unit yang disebut kontainer. Kontainer ini membungkus sebuah perangkat lunak dalam lingkungan yang lengkap untuk menjalankan aplikasi dengan cara yang terisolasi dari lingkungan lainnya. Docker menyederhanakan proses pengembangan, pengujian, dan penyebaran aplikasi dengan memastikan aplikasi tetap konsisten dalam berbagai lingkungan. Docker digunakan untuk menginstal dan menjalankan OpenVAS dalam kontainer. Penggunaan Docker memudahkan proses instalasi dan memastikan bahwa OpenVAS berjalan dalam lingkungan yang konsisten dan terisolasi.

4. OpenVAS

   OpenVAS atau *Open Vulnerability Assessment System* adalah sistem penilaian kerentanan *open-source* yang menyediakan layanan pemindaian kerentanan jaringan. Alat ini efektif dalam mendeteksi berbagai kerentanan keamanan dalam sistem jaringan. OpenVAS digunakan untuk melakukan pemindaian dan penilaian kerentanan pada jaringan yang diuji. OpenVAS membantu mengidentifikasi dan menganalisis kerentanan, memberikan informasi rinci tentang ancaman yang ditemukan, dan memberikan rekomendasi perbaikan.

5. Postfix

   Postfix adalah mail transfer agent (MTA) yang digunakan untuk mengirim dan menerima email pada server, menggantikan sendmail untuk menangani email dengan cara yang lebih efisien dan aman.

6. Thunderbird

   Thunderbird adalah aplikasi klien email yang digunakan untuk mengakses, mengelola, dan mengirim email melalui server email yang dikonfigurasi, menyediakan antarmuka pengguna yang intuitif.

7. Laravel

   Laravel adalah framework PHP yang mempermudah pengembangan aplikasi web dengan menyediakan berbagai alat dan pustaka untuk pengembangan yang cepat, aman, dan terstruktur.

8. PHP (Hypertext Preprocessor)

   PHP (Hypertext Preprocessor) adalah bahasa pemrograman server-side yang digunakan untuk membangun aplikasi web dinamis dan berinteraksi dengan basis data.

9. MySQL

   MySQL adalah sistem manajemen basis data relasional yang digunakan untuk menyimpan, mengelola, dan mengakses data aplikasi secara efisien.

10. Apache

    Apache adalah web server open-source yang menyajikan konten web dan aplikasi kepada pengguna dengan menangani permintaan HTTP dan menyajikan halaman web serta aplikasi berbasis PHP.

4.1.2 Analisis Kebutuhan Perangkat Keras

Analisis kebutuhan perangkat keras mencakup identifikasi spesifikasi perangkat keras yang diperlukan untuk mendukung operasi sistem secara efisien dan efektif. Berikut adalah perangkat keras yang dibutuhkan:

1. Ubuntu Server

   Sebagai sistem operasi yang dipilih, Ubuntu Server 22.04 harus diinstal pada perangkat keras yang memadai untuk menjalankan semua aplikasi yang dibutuhkan. Spesifikasi minimal perangkat keras yang dibutuhkan untuk Ubuntu Server 22.04 mencakup:

a. RAM

Memori dengan kapasitas 4 *GB* cukup untuk menjalankan Ubuntu Server 22.04 beserta aplikasi-aplikasi pendukung seperti Docker, Lynis, dan OpenVAS.

b. Storage

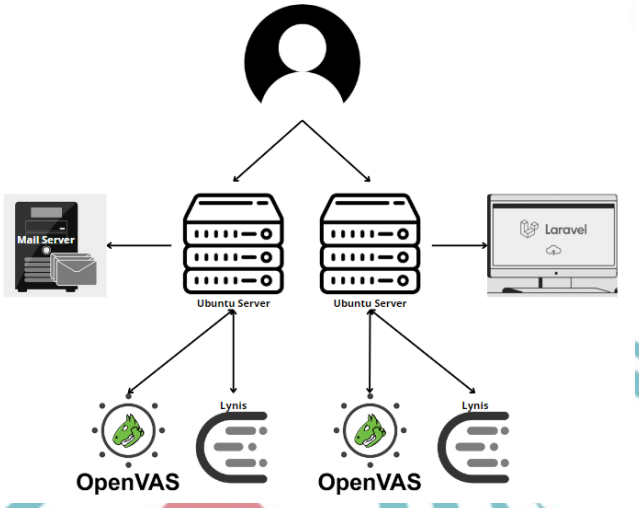
Kapasitas penyimpanan sebesar 50 *GB* cukup untuk menginstal sistem operasi, aplikasi pendukung, dan menyimpan hasil audit serta pemindaian kerentanan.

2. Jaringan

Konektivitas jaringan yang handal dan aman diperlukan untuk tahap implementasi dan operasional sistem. Jaringan ini berfungsi untuk menghubungkan sistem dengan perangkat lain dan memungkinkan pemindaian jaringan yang efektif oleh OpenVAS. Jaringan berperan penting dalam memastikan sistem dapat terhubung dengan lingkungan eksternal dan internal, memungkinkan komunikasi yang lancar antara berbagai komponen sistem. Dalam konteks ini, jaringan yang digunakan berada di lingkungan Politeknik Negeri Jakarta.

4.2 Implementasi Sistem

Setelah perancangan sistem selesai, langkah berikutnya adalah melaksanakan rencana yang telah dirancang dalam lingkungan operasional yang sebenarnya. Bagian implementasi sistem ini fokus pada menjalankan rencana secara konkret dan memastikan sistem beroperasi dengan baik. Berikut adalah detail untuk bagian implementasi sistem:



Gambar 4.1 Alur Implementasi

4.2.1 Instalasi dan Konfigurasi

1. Instalasi Ubuntu *Server*: Melaksanakan instalasi Ubuntu *Server* sesuai dengan konfigurasi yang telah direncanakan dalam tahap perancangan.
2. Instalasi Lynis: Setelah Ubuntu *Server* terpasang, instal dan konfigurasi Lynis untuk melakukan pemindaian awal terhadap sistem. Lynis akan membantu dalam mengevaluasi konfigurasi keamanan yang telah diimplementasikan.

```
ubuntu@ubunt:~$ sudo apt-get install lynis
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Gambar 4.2 Instalasi Lynis

4 Instalasi Docker untuk OpenVAS: Menggunakan Docker, instal dan konfigurasi OpenVAS sebagai alat utama untuk melakukan pemindaian kerentanan yang lebih mendalam.

```
ubuntu@ubunt:~$ sudo apt-get install docker
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

Gambar 4.3 Instalasi Docker

5 Instalasi OpenVAS: Melakukan instalasi OpenVAS di dalam lingkungan Docker yang telah disiapkan, termasuk konfigurasi tambahan yang diperlukan seperti *setting SSL* dan konfigurasi *port*.

```
sudo docker run -d -p 443:443 --name openvas mikesplain/openvas
ikesplain/openvas:latest' locally
```

Gambar 4.4 Instalasi OpenVAS

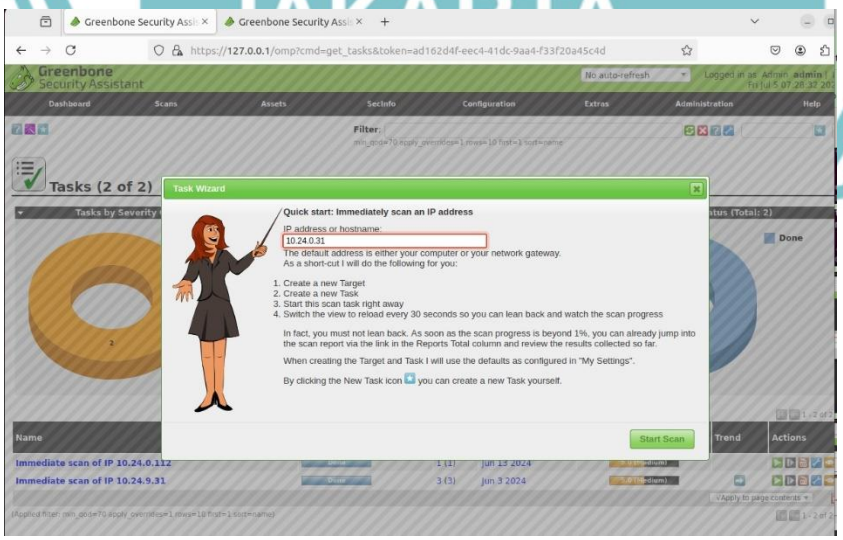
6. Instalasi dan konfigurasi Postfix: Postfix digunakan sebagai mail transfer agent (MTA) untuk mengirim dan menerima email di server. Konfigurasi Postfix dilakukan untuk memastikan server dapat mengelola email secara efektif, termasuk pengaturan domain, alias email, dan kebijakan keamanan.

7 Instalasi Thunderbird: Thunderbird adalah klien email yang digunakan untuk menguji apakah mail server yang dibangun dengan Postfix berfungsi dengan baik. Dengan menggunakan Thunderbird, kita dapat mengirim dan menerima email melalui server Postfix yang telah dikonfigurasi.

8 Instalasi dan konfigurasi Laravel , PHP, MySQL, dan Apache: Laravel dipilih sebagai framework PHP untuk pengembangan aplikasi yang lebih efisien. PHP diinstal untuk mendukung Laravel, dengan versi yang sesuai dengan kebutuhan framework ini. MySQL digunakan sebagai sistem manajemen basis data untuk menyimpan data aplikasi, mencakup pengaturan pengguna, hak akses, dan struktur database. Apache berfungsi sebagai web server yang menyajikan aplikasi Laravel, dengan konfigurasi virtual host dan modul-modul yang diperlukan agar aplikasi dapat diakses melalui IP atau domain yang ditentukan.

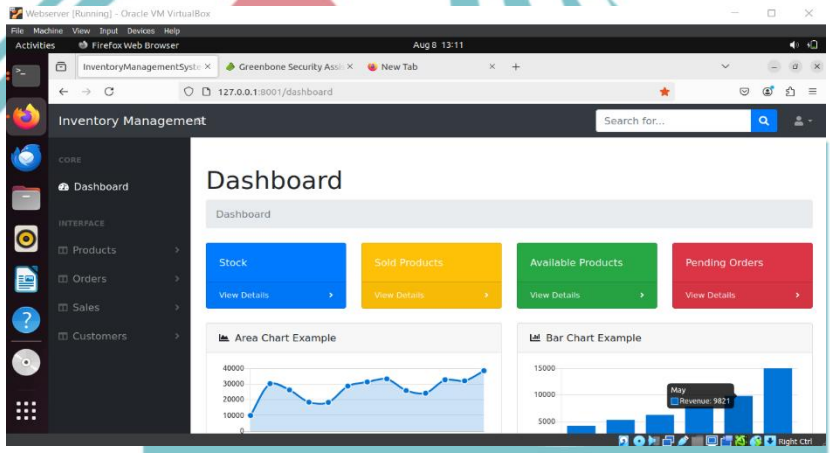
4.2.2 Pelaksanaan Pemindaian dan Monitoring

1. Setelah instalasi selesai, jalankan pemindaian kerentanan menggunakan OpenVAS dan Lynis sesuai dengan pengaturan yang telah ditentukan sebelumnya dalam tahap perancangan.

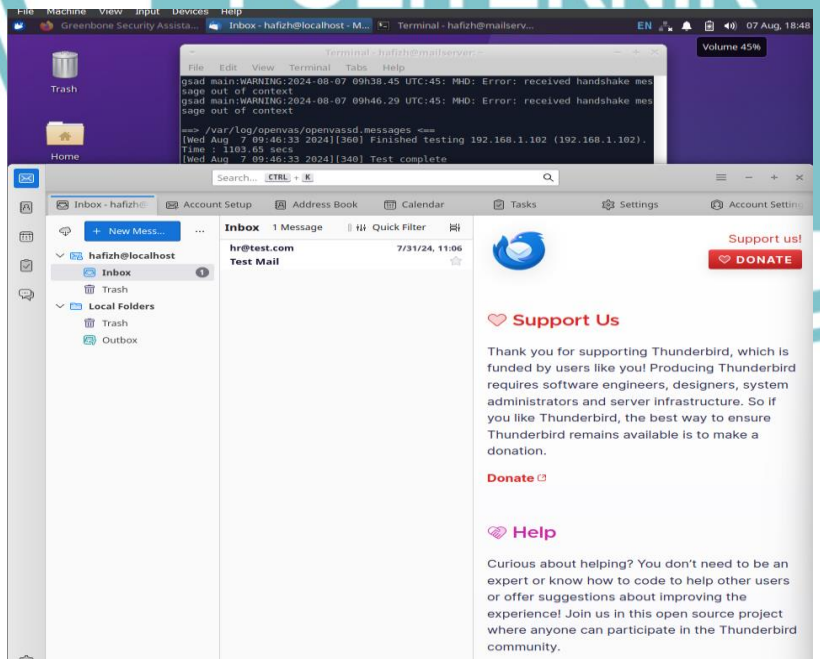


Gambar 4.5 Pemindaian menggunakan OpenVAS

Gambar 4.6 Pemindaian menggunakan Lynis



Gambar 4.7 Tampilan Web Server

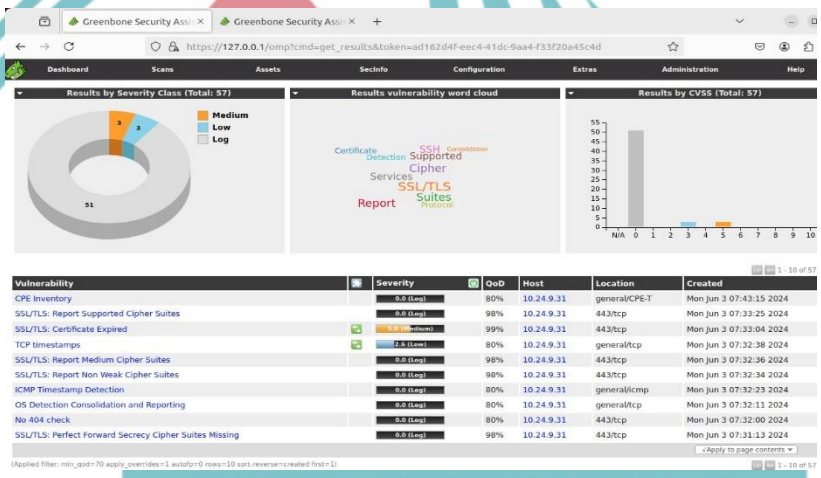


Gambar 4.8 Tampilan Mail Server

2. Monitor proses pemindaian untuk memastikan bahwa semua langkah berjalan dengan baik dan tanpa masalah. Pantau hasil pemindaian untuk mengidentifikasi potensi kerentanan keamanan yang ada dan memulai langkah-langkah perbaikan yang sesuai.

4.2.3 Analisis

Setelah pemindaian selesai, hasilnya dievaluasi untuk mengidentifikasi area yang memerlukan peningkatan keamanan atau penyesuaian tambahan dalam konfigurasi sistem. Kerentanan yang ditemukan dianalisis berdasarkan tingkat keparahan dan potensi dampaknya.



Gambar 4.9 Hasil pemindaian OpenVAS

Gambar 4.10 Hasil pemindaian Lynis

4.3 Pengujian

4.3.1 Deskripsi Pengujian

Pengujian kali ini menyajikan hasil analisis dari implementasi alat keamanan Lynis dan OpenVAS pada sistem operasi Ubuntu Server. Pengujian ini melibatkan dua skenario utama: pengujian pada server email dan server web. Pada Skenario 1, sistem diuji dengan menggunakan Postfix sebagai mail transfer agent dan Thunderbird sebagai aplikasi klien email. Pada Skenario 2, sistem diuji dengan Apache sebagai server web, Laravel sebagai framework aplikasi, PHP sebagai bahasa pemrograman, dan MySQL sebagai sistem manajemen basis data.

Pembahasan meliputi pemindaian kerentanan yang dilakukan dengan OpenVAS dan Lynis, hasil yang diperoleh, serta interpretasi dan rekomendasi perbaikan untuk meningkatkan keamanan Ubuntu Server. OpenVAS digunakan untuk mengidentifikasi potensi kerentanan dalam konfigurasi server dan aplikasi, sementara Lynis menilai kepatuhan terhadap praktik keamanan terbaik dan konfigurasi sistem secara menyeluruh.

4.3.2 Data Hasil Pengujian

4.3.2.1. Identifikasi Kerentanan

1. Skenario 1 Mail Server

a. Pemindaian Kerentanan dengan OpenVAS

Tabel 4.1 Hasil pemindaian OpenVAS

Alat	Klasifikasi	Hasil Pemindaian
OpenVAS	*Medium*	*SSL/TLS Certificate Expired*
	Low	*TCP Timestamp*

b. Pemindaian Kerentanan dengan Lynis

Tabel 4.2 Hasil Pemindaian Lynis

No	Alat	Klasifikasi	Hasil Pemindaian
1	Lynis	*High*	libpam-tmpdir Not Installed
2		*High*	Apport.service, Unsafe
3		*High*	Avahi-daemon.service, Unsafe

4		*Low*	NetworkManager. Service, Exposed
5		*Low*	Colord.servic, Exposed
6		*Low*	Permissions of home directories (WARNING – High)
7		*Medium*	Query unpurged packages (FOUND-Medium)
8		*Medium*	Query unpurged packages FOUND
9		*Low*	Checking Apache NOT FOUND
10		*low*	Checking nginx NOT FOUND

2. Skenario 2 Web Server

a. Pemindaian Menggunakan OpenVAS

Tabel 4.3 Hasil Pemindaian OpenVAS

No	Alat	Klasifikasi	Hasil Pemindaian
1	OpenVAS	Medium	SSL/TLS Certificate Expired
2		Medium	Missing 'httpOnly' Cookie Atribute
3		Low	TCP Timestamp

b. Pemindaian Menggunakan Lynis

Tabel 4.4 Hasil Pemindaian Lynis

No	Alat	Klasifikasi	Hasil Pemindaian
1	Lynis	High	libpam-tmpdir Not Installed
2		High	Apport.service, Unsafe
3		High	Avahi-daemon.service, Unsafe
4		High	NetworkManager.service, colord.service, Exposed
5		High	openvas-scanner.service, Unsafe
6		High	ospd-openvas.service, Unsafe
7		High	gvmd.service, Unsafe

8		High	php8.2-fpm.service, Unsafe
9		High	packagekit.service, Unsafe
10		High	Exceptions found, some exceptional events or information was found
11		Medium	SW prng, NO
12		Low	Searching DNS domain name, unknown

4.3.2.2. Interpretasi Hasil Pemindaian

Setelah melakukan pemindaian menggunakan OpenVAS dan Lynis, berbagai kerentanan telah teridentifikasi yang perlu dianalisis secara menyeluruh untuk memahami dampaknya terhadap keamanan sistem operasi Ubuntu *Server*.

1. Skenario 1 Mail Server

   a. Berdasarkan table 4.1 berikut adalah penjelasan dari hasil pemindaian menggunakan OpenVAS

Tabel 4.5 Penjelasan hasil pemindaian OpenVAS

Klasifikasi	Hasil Pemindaian	Penjelasan Hasil
Medium	*SSL/TLS Certificate Expired*	Kerentanan ini menunjukkan bahwa sertifikat *SSL/TLS* yang digunakan pada sistem telah kedaluwarsa. Hal ini dapat menyebabkan komunikasi yang tidak aman karena sertifikat yang kedaluwarsa tidak lagi dapat dipercaya oleh browser atau klien lain yang mengakses *server*.
Low	*TCP Timestamp*	Kerentanan ini menunjukkan bahwa server mengungkapkan

		informasi waktu yang dapat digunakan oleh penyerang untuk memprediksi urutan paket *TCP*, sehingga memungkinkan kemungkinan serangan *time-based* seperti *Time-based Blind SQL Injection.*

b. Berdasarkan table 4.2 berikut adalah penjelasan dari hasil pemindaian menggunakan Lynis:

Tabel 4.6 Penjelasan hasil pemindaian Lynis

No	Klasifikasi	Hasil Pemindaian	Penjelasan Hasil
1	*High*	*libpam-tmpdir Not Installed*	Modul PAM (Pluggable Authentication Module) yang dirancang untuk mengelola direktori sementara secara aman. Jika modul ini tidak terinstal, direktori sementara seperti /tmp dan /var/tmp mungkin tidak dilindungi dengan baik, berpotensi menimbulkan risiko serangan berbasis direktori sementara.
2	*High*	*Apport.service, Unsafe*	Layanan yang digunakan untuk mengumpulkan dan melaporkan crash dan masalah perangkat lunak. Jika diaktifkan dalam lingkungan server produksi, layanan ini dapat menjadi vektor eksploitasi

			potensial karena dapat mengungkapkan informasi sistem yang sensitif. Disarankan untuk menonaktifkan layanan ini jika tidak diperlukan.
3	*High*	*Avahi-daemon.service, Unsafe*	Layanan yang menyediakan layanan penemuan jaringan di lingkungan lokal. Layanan ini dapat memperkenalkan risiko keamanan karena dapat memungkinkan perangkat di jaringan lokal untuk menemukan server dan layanan secara otomatis. Jika tidak digunakan, sebaiknya dinonaktifkan atau dihapus.
4	*High*	*NetworkManager. Service, Exposed*	Layanan yang mengelola koneksi jaringan dan konfigurasi pada desktop. Pada server, penggunaan NetworkManager bisa menyebabkan risiko jika server tidak memerlukan manajemen jaringan dinamis. Disarankan untuk menonaktifkan layanan ini dan menggunakan alat konfigurasi jaringan seperti netplan atau systemd-networkd.
5	*High*	*Colord.servic, Exposed*	Layanan yang mengelola profil warna perangkat keras. Pada server, layanan ini mungkin

			tidak diperlukan karena lebih relevan untuk lingkungan desktop. Menonaktifkan layanan ini jika tidak digunakan dapat mengurangi potensi risiko keamanan.
6	*High*	*Permissions of home directories (WARNING – High)*	Izin yang tidak tepat pada direktori home pengguna dapat memungkinkan akses tidak sah oleh pengguna lain. Direktori home harus memiliki izin yang ketat (biasanya 700) untuk mencegah akses oleh pengguna lain dan melindungi data pribadi.
7	*Medium*	*Query unpurged packages (FOUND-Medium)*	Paket yang tidak dibersihkan dari sistem dapat mengandung file konfigurasi lama atau paket yang tidak lagi didukung. Paket yang tidak diperlukan atau usang dapat menjadi celah keamanan karena bisa menyisakan komponen yang rentan.
8	*Medium*	*Query unpurged packages FOUND*	Mengindikasikan adanya paket yang tidak dibersihkan yang mungkin berisi konfigurasi atau komponen yang dapat menimbulkan risiko keamanan. Penghapusan paket yang tidak diperlukan dapat mengurangi risiko ini.

9	*Low*	*Checking Apache NOT FOUND*	Apache tidak ditemukan
10	*Low*	*Checking nginx NOT FOUND*	Nginx tidak ditemukan

2. Skenario 2 Web Server

a. Berdasarkan table 4.3 berikut adalah penjelasan dari hasil pemindaian menggunakan OpenVAS

Tabel 4.7 Penjelasan hasil pemindaian OpenVAS

Klasifikasi	Hasil Pemindaian	Penjelasan Hasil
Medium	*SSL/TLS Certificate Expired*	Kerentanan ini menunjukkan bahwa sertifikat *SSL/TLS* yang digunakan pada sistem telah kedaluwarsa. Hal ini dapat menyebabkan komunikasi yang tidak aman karena sertifikat yang kedaluwarsa tidak lagi dapat dipercaya oleh browser atau klien lain yang mengakses *server*.
Medium	Missing 'httpOnly' Cookie Atribute	Cookie yang tidak memiliki atribut HttpOnly dapat menimbulkan risiko keamanan karena atribut ini penting untuk melindungi cookie dari akses yang tidak sah melalui JavaScript di sisi klien. Atribut HttpOnly dirancang untuk mencegah akses cookie oleh skrip yang berjalan di
Low	*TCP Timestamp*	Kerentanan ini menunjukkan bahwa server mengungkapkan

		informasi waktu yang dapat digunakan oleh penyerang untuk memprediksi urutan paket *TCP*, sehingga memungkinkan kemungkinan serangan *time-based* seperti *Time-based Blind SQL Injection.*

b. Berdasarkan table 4.4 berikut adalah penjelasan dari hasil pemindaian menggunakan Lynis

Tabel 4.8 Penjelasan hasil pemindaian Lynis

No	Klasifikasi	Hasil Pemindaian	Penjelasan Hasil
1	*High*	*libpam-tmpdir Not Installed*	Direktori /tmp dan /var/tmp tidak dikelola dengan aman, yang dapat meningkatkan risiko serangan berbasis direktori sementara. Penerapan libpam-tmpdir membantu mengurangi risiko tersebut dengan mengelola akses dan izin lebih baik.
2	*High*	*Apport.service, Unsafe*	Layanan pelaporan bug di Ubuntu. Jika tidak dikonfigurasi dengan benar, layanan ini dapat mengekspos informasi sensitif tentang sistem. Menonaktifkan layanan ini atau

			mengkonfigurasinya dengan hati-hati dapat mengurangi risiko eksposur data yang tidak diinginkan.
3	*High*	*Avahi-daemon.service, Unsafe*	Layanan yang memungkinkan pencarian dan pengenalan layanan di jaringan lokal. Jika tidak digunakan, layanan ini bisa menjadi risiko keamanan karena membuka port dan mengizinkan layanan jaringan lokal yang tidak perlu. Menonaktifkan atau menghapus layanan ini jika tidak diperlukan dapat memperbaiki keamanan.
4	*High*	*NetworkManager.service, colord.service, Exposed*	*NetworkManager.service* mengelola konfigurasi jaringan, dan colord.service mengelola profil warna pada desktop
5	*High*	*openvas-scanner.service, Unsafe*	Layanan pemindaian kerentanan dari OpenVAS. Jika tidak dikonfigurasi dengan benar atau jika eksposur layanan tidak dikendalikan, ini dapat menjadi risiko keamanan. Pastikan layanan ini hanya dapat diakses oleh

			pengguna yang sah dan terkonfigurasi dengan benar.
6	*High*	*ospd-openvas.service, Unsafe*	Bagian dari OpenVAS yang menjalankan pengelolaan proses. Sama seperti openvas-scanner.service, jika layanan ini tidak dikonfigurasi dengan benar, ini bisa membuka risiko. Pengaturan akses yang ketat pada layanan ini adalah penting untuk mencegah akses yang tidak sah.
7	*High*	*gvmd.service, Unsafe*	Layanan utama untuk OpenVAS yang mengelola database dan tugas pemindaian. Layanan ini harus dikonfigurasi dengan sangat hati-hati dan dilindungi dengan kontrol akses yang ketat untuk menghindari potensi risiko keamanan.
8	*High*	*php8.2-fpm.service, Unsafe*	*php8.2-fpm.service* adalah FastCGI Process Manager untuk PHP. Konfigurasi yang tidak aman pada layanan ini dapat membuka celah keamanan

			seperti serangan PHP Remote Code Execution. Pastikan bahwa konfigurasi PHP-FPM sudah aman dan akses ke layanan ini dilindungi dengan baik.
9	*High*	*packagekit.service, Unsafe*	*packagekit.service* digunakan untuk mengelola pembaruan paket di sistem. Jika tidak dikonfigurasi dengan benar, layanan ini dapat menjadi target untuk serangan. Nonaktifkan layanan ini jika tidak diperlukan atau pastikan konfigurasi dan kontrol aksesnya aman.
10	*High*	*Exceptions found, some exceptional events or information was found*	Ada beberapa peristiwa atau informasi yang tidak biasa ditemukan selama pemindaian. Ini dapat menunjukkan masalah konfigurasi atau potensi celah keamanan yang perlu diteliti lebih lanjut untuk memastikan sistem dalam keadaan aman.
11	*Medium*	*SW prng, NO*	*SW prng* (Secure Random Number Generator) tidak ditemukan atau tidak diaktifkan. PRNG yang tidak aman dapat mempengaruhi keamanan

			sistem jika digunakan untuk tujuan kriptografi atau pembuatan token. Pastikan bahwa PRNG yang kuat dan aman digunakan di sistem.
12	*Low*	*Searching DNS domain name, unknown*	Pencarian nama domain DNS menunjukkan status "unknown," yang berarti informasi tentang pencarian DNS mungkin tidak lengkap atau tidak dapat dipastikan. Ini tidak menunjukkan risiko keamanan langsung tetapi dapat memerlukan pemeriksaan lebih lanjut untuk memastikan konfigurasi DNS yang benar dan aman.

4.3.2.3. Penilaian Risiko atau Risk Assessment

Setelah identifikasi dan analisis kerentanan menggunakan OpenVAS dan Lynis, selanjutnya dilakukan penilaian risiko terhadap setiap kerentanan yang ditemukan. Penilaian ini memberikan gambaran mengenai tingkat keparahan kerentanan serta potensi dampak yang dapat ditimbulkan terhadap keamanan sistem dan organisasi secara keseluruhan. Hasil kerentanan dapat diklasifikasin menjadi 3 klasifikasi risiko:

a. *Low*: Kerentanan dengan risiko rendah umumnya mencakup kerentanan yang memiliki dampak yang terbatas atau memerlukan akses yang lebih tinggi untuk dieksploitasi. Meskipun risikonya relatif

rendah, tetap diperlukan tindakan pencegahan untuk mengurangi kemungkinan eksploitasi di masa depan.

b. *Medium*: Kerentanan dengan risiko menengah dapat memiliki dampak yang lebih signifikan jika dieksploitasi. Meskipun tidak segera mengancam keamanan sistem secara keseluruhan, kerentanan ini memerlukan tindakan perbaikan yang lebih serius untuk mengurangi kemungkinan eksploitasi oleh penyerang.

c. *High*: Kerentanan dengan risiko tinggi merupakan yang paling mendesak untuk ditangani. Kerentanan ini memiliki potensi dampak yang besar terhadap keamanan sistem dan organisasi, mungkin memungkinkan akses tidak sah atau manipulasi yang signifikan jika dieksploitasi oleh penyerang. Tindakan perbaikan harus segera dilakukan untuk mengurangi atau menghilangkan risiko ini.

4.3.2.4. Remediasi

Tahap terakhir dari proses *Vulnerability Assessment* adalah remediasi atau perbaikan. Langkah-langkah remediasi ini dirancang untuk mengurangi atau menghilangkan risiko yang terkait dengan kerentanan yang telah diidentifikasi. Berikut adalah rekomendasi perbaikan berdasarkan hasil pemindaian dan analisis yang dapat diambil untuk meningkatkan keamanan Ubuntu *Server*:

1. Skenario 1 Mail Server
   a. Rekomendasi hasil pemindaian menggunkan OpenVAS

Tabel 4.9 Rekomendasi Hasil OpenVAS

Klasifikasi	Hasil Pemindaian	Rekomendasi Perbaikan
Medium	*SSL/TLS Certificate Expired*	Segera memperbarui sertifikat *SSL/TLS* yang kedaluwarsa untuk memastikan komunikasi yang aman.

Low	*TCP Timestamp*	Mengonfigurasi parameter *TCP* untuk mengurangi risiko serangan *time-based*.

b. Rekomendasi hasil pemindaian menggunkan Lynis

Tabel 4.10 Rekomendasi Hasil Lynis

No	Klasifikasi	Hasil Pemindaian	Rekomendasi Pemindaian
1	High	libpam-tmpdir Not Installed	Instal libpam-tmpdir untuk memastikan bahwa direktori sementara (/tmp dan /var/tmp) digunakan secara aman oleh proses sistem. Ini akan membantu mengurangi risiko serangan berbasis direktori sementara.
2	High	Apport.service, Unsafe	Nonaktifkan apport.service jika tidak diperlukan, karena ini bisa membuka risiko jika ada eksploitasi pada sistem.
3	High	Avahi-daemon.service, Unsafe	Nonaktifkan atau hapus avahi-daemon jika tidak digunakan, karena layanan ini memungkinkan pencarian jaringan dan bisa membuka celah keamanan.
4	High	NetworkManager. Service, Exposed	Jika server tidak digunakan sebagai desktop, pertimbangkan untuk menonaktifkan NetworkManager.service dan menggunakan netplan atau systemd-networkd untuk konfigurasi jaringan.

5	High	Colord.servic, Exposed	Nonaktifkan colord.service jika server tidak memerlukan manajemen warna, yang lebih relevan pada lingkungan desktop.
6	High	Permissions of home directories (WARNING – High)	Pastikan direktori home pengguna memiliki izin yang ketat (biasanya 700) untuk mencegah akses oleh pengguna lain.
7	Medium	Query unpurged packages (FOUND-Medium)	Identifikasi dan hapus paket yang tidak dibersihkan dari sistem untuk mengurangi potensi risiko keamanan.
8	Medium	Query unpurged packages FOUND	Hapus paket yang tidak diperlukan dari sistem untuk mengurangi potensi risiko keamanan. Paket yang tidak dibersihkan bisa menjadi celah keamanan karena mungkin mengandung file konfigurasi lama atau paket yang tidak lagi didukung.
9	Low	Checking Apache NOT FOUND	Jika Apache seharusnya terpasang, pastikan layanan berjalan dengan benar. Jika tidak digunakan, pastikan untuk menghapus paket terkait.
10	Low	Checking nginx NOT FOUND	Sama seperti Apache, jika nginx diharapkan ada, instal dan konfigurasikan sesuai kebutuhan. Jika tidak, pastikan tidak ada instalasi yang tersisa

2. Skenario 2 Web Server

a. Rekomendasi hasil pemindaian menggunkan OpenVAS

Tabel 4.11 Rekomendasi Hasil OpenVAS

No	Klasifikasi	Hasil Pemindaian	Rekomendasi Perbaikan
1	Medium	SSL/TLS Certificate Expired	Segera perbarui sertifikat SSL/TLS yang sudah kedaluwarsa.
2	Medium	Missing 'httpOnly' Cookie Atribute	Pastikan cookie yang dikirim oleh aplikasi memiliki atribut HttpOnly untuk melindungi dari pencurian cookie melalui skrip.
3	Low	TCP Timestamp	Nonaktifkan fitur TCP Timestamping untuk mencegah kebocoran informasi mengenai waktu sistem melalui jaringan.

b. Rekomendasi hasil pemindaian menggunkan Lynis

Tabel 4.12 Rekomendasi Hasil Lynis

No	Klasifikasi	Hasil Pemindaian	Rekomendasi Perbaikan
1	High	libpam-tmpdir Not Installed	Sama seperti pada Mail Server, instal libpam-tmpdir.
2	High	Apport.service, Unsafe	Nonaktifkan apport.service.
3	High	Avahi-daemon.service, Unsafe	Nonaktifkan atau hapus avahi-daemon.
4	High	NetworkManager.service, colord.service, Exposed	Nonaktifkan NetworkManager.service dan colord.service jika tidak diperlukan.
5	High	openvas-scanner.service, Unsafe	Periksa dan perbarui konfigurasi openvas-scanner untuk memastikan layanan ini aman, atau nonaktifkan jika tidak diperlukan.

6	High	ospd-openvas.service, Unsafe	Sama seperti openvas-scanner, pastikan ospd-openvas dikonfigurasi dengan benar atau dinonaktifkan jika tidak diperlukan.
7	High	gvmd.service, Unsafe	Periksa konfigurasi dan pastikan gvmd.service berjalan dengan aman.
8	High	php8.2-fpm.service, Unsafe	Periksa konfigurasi PHP-FPM untuk memastikan aman dari eksploitasi. Pastikan konfigurasi file php-fpm.conf dan pool diatur dengan aman.
9	High	packagekit.service, Unsafe	Nonaktifkan packagekit.service jika tidak diperlukan atau pastikan hanya berjalan saat dibutuhkan untuk pembaruan otomatis.
10	High	Exceptions found, some exceptional events or information was found	Tinjau log keamanan untuk mencari tahu apa yang menyebabkan pengecualian dan perbaiki masalah yang terdeteksi.
11	Medium	SW prng, NO	Rekomendasi Perbaikan: Instal haveged atau rng-tools untuk memastikan ketersediaan entropi yang cukup untuk operasi kriptografi.

14	Low	Searching DNS domain name, unknown	Tentukan DNS domain name yang valid atau perbarui konfigurasi jaringan agar domain name bisa dikenali dengan benar.

4.4 Analisis Data

1. Pembahasan

Hasil pemindaian menggunakan OpenVAS dan Lynis pada dua skenario—Mail Server (Postfix dan Thunderbird) dan Web Server (Laravel)—menunjukkan perbedaan dalam pendekatan deteksi dan analisis kerentanan. OpenVAS, dengan fokus pada kerentanan berbasis IP, menghasilkan laporan yang terfokus pada aspek jaringan, seperti sertifikat SSL/TLS yang kedaluwarsa dan pengaturan timestamp TCP. Sementara itu, Lynis melakukan pemindaian langsung di dalam sistem operasi, memberikan gambaran yang lebih komprehensif tentang keamanan sistem dengan menyoroti aspek konfigurasi dan pengaturan yang mempengaruhi keamanan sistem, seperti izin file yang tidak aman, keberadaan paket-paket yang rentan, dan konfigurasi layanan seperti Postfix, Apache, dan layanan sistem lainnya. Untuk skenario Mail Server, analisis ini menunjukkan kebutuhan untuk memperbaiki konfigurasi layanan email dan memperhatikan keamanan jaringan. Sedangkan untuk skenario Web Server, hasilnya menekankan pentingnya konfigurasi PHP dan layanan web secara aman. Kombinasi dari kedua alat ini memberikan pemahaman yang lebih menyeluruh tentang keamanan infrastruktur, dari tingkat jaringan hingga konfigurasi internal sistem operasi.

2. Rekomendasi

Dari hasil analisis menggunakan OpenVAS dan Lynis pada Ubuntu Server dengan dua skenario—Mail Server dan Web Server—teridentifikasi beberapa kerentanan dengan tingkat risiko yang bervariasi. OpenVAS menyoroti masalah seperti sertifikat SSL/TLS yang kedaluwarsa dan parameter TCP yang perlu dikonfigurasi ulang. Lynis menekankan perlunya pemindai malware, penyesuaian hak akses, dan aktivasi logging jarak jauh untuk meningkatkan keamanan sistem. Untuk Mail Server, disarankan untuk

memperbaiki konfigurasi Postfix, memastikan bahwa layanan tidak memiliki celah keamanan yang dapat dieksploitasi. Sedangkan untuk Web Server, penting untuk memastikan konfigurasi PHP dan Apache yang aman, serta penerapan pembaruan rutin. Rekomendasi lanjutan mencakup penerapan pembaruan rutin, monitoring aktif, dan pendidikan keamanan bagi pengguna guna menjaga tingkat keamanan yang optimal pada server Politeknik Negeri Jakarta.