Implementasi OpenVAS dan Lynis pada Kerentanan Sistem Operasi Ubuntu Server

Muhammad Hafizh Rizqullah
Teknik Multimedia dan Jaringan, Teknik Informatika dan Komputer, Politeknik Negeri Jakarta
Depok, Jawa Barat
Muhammad.hafizhrizqullah.tik20@mhsw.pnj.ac.id

ABSTRAK

Berbagai aspek kehidupan telah diubah oleh kemajuan teknologi informasi dan transformasi digital, terutama di dunia teknologi dan bisnis. Penelitian ini berfokus pada penggunaan alat evaluasi keamanan Lynis dan OpenVAS untuk mendeteksi dan mengidentifikasi kerentanan keamanan pada sistem operasi Ubuntu Server. Selain itu, penelitian ini akan memberikan rekomendasi perbaikan yang tepat untuk meningkatkan keamanan infrastruktur IT. Metode evaluasi kerentanan digunakan dalam penelitian ini untuk menemukan kerentanan pada sistem. Metode ini mencakup instalasi dan konfigurasi Ubuntu Server, instalasi dan konfigurasi Lynis dan OpenVAS, serta pemindaian kerentanan menggunakan kedua alat tersebut. Lynis melakukan pemindaian langsung di dalam sistem operasi untuk memberikan gambaran menyeluruh tentang keamanan internal, sementara OpenVAS berkonsentrasi pada analisis berbasis IP address untuk mendeteksi kerentanan. 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.

Kata kunci: *Ubuntu Server, Vulnerability, Vulnerability Scanning, Lynis, Openvas*

I. PENDAHULUAN

Perkembangan teknologi informasi dan transformasi digital telah menciptakan revolusi dalams berbagai aspek kehidupan, terutama di dunia bisnis dan teknologi. Dalam konteks ini, sistem operasi Ubuntu Server telah muncul sebagai elemen kunci dalam upaya menjaga keamanan digital. Ubuntu Server, yang dikembangkan oleh Offensive Security, dirancang khusus untuk keperluan uji penetrasi, analisis keamanan, dan aktivitas forensik.

Sistem operasi (OS) menjadi pondasi utama dalam menjalankan dan mengelola perangkat keras dan perangkat lunak pada suatu sistem. OS tidak hanya bertanggung jawab atas alokasi sumber daya, tetapi juga menyediakan lingkungan eksekusi untuk aplikasi dan menyediakan kontrol terhadap akses ke sistem. Pilihan OS dapat memiliki dampak signifikan terhadap performa, keamanan, dan kestabilan sistem. Sebagai bagian penting dari infrastruktur IT, OS memainkan peran sentral dalam upaya untuk memastikan keamanan dan keandalan.

Dalam konteks sistem operasi Linux, Ubuntu Server telah menjadi pilihan yang populer untuk menyediakan layanan server. Dengan berlandaskan kernel Linux, Ubuntu Server menawarkan keandalan dan fleksibilitas yang tinggi. Kelebihan dalam manajemen paket, kompatibilitas, dan dukungan komunitas menjadikan Ubuntu Server sebagai pilihan yang menonjol. Dalam evolusinya, Ubuntu Server terus beradaptasi dengan perubahan kebutuhan teknologi, menghadirkan berbagai fitur dan perbaikan keamanan yang mendukung pengguna di seluruh dunia.

Keamanan Ubuntu Server memegang peran sentral dalam pertimbangan penggunaannya sebagai distribusi Menurut Distrowatch.com Linux yang sangat populer untuk server. Dengan nilai rating mencapai 7.54 dan jumlah review sebanyak 465, Ubuntu Server menjadi pilihan yang sangat direkomendasikan, terutama bagi mereka yang ingin mempelajari administrasi server. Keandalan dan fleksibilitas Ubuntu Server telah menarik perhatian komunitas IT di seluruh dunia. Dalam persaingan dengan distribusi Linux lainnya, seperti Debian Server dengan rating lebih tinggi, yakni 8.84 dan jumlah review 547, serta Fedora yang dikembangkan oleh Red Hat dengan rating 8.27 dan 427 review, Ubuntu Server tetap menjadi pilihan favorit. Dengan jumlah pengguna yang signifikan, tantangan keamanan semakin muncul, mendorong perhatian serius terhadap pemindaian kerentanan, identifikasi potensi risiko, dan penerapan praktik keamanan terbaik. Dengan demikian, popularitas Ubuntu Server sebagai pilihan utama untuk administrasi server menempatkannya di garis depan perlindungan keamanan dalam infrastruktur server.(Tenaya et al., 2022)

Saat ini, beberapa solusi digunakan untuk mendeteksi dan mengidentifikasi kerentanan keamanan pada sistem operasi Ubuntu Server, termasuk alat pemindaian seperti OpenVAS dan Lynis. OpenVAS (Open Vulnerability Assessment System) merupakan alat pemindaian kerentanan yang sangat komprehensif, menawarkan

berbagai tes keamanan dan pemindaian menyeluruh yang mampu mendeteksi berbagai jenis kerentanan. OpenVAS dilengkapi dengan antarmuka web yang memudahkan pengaturan dan pemantauan pemindaian. Namun, OpenVAS dapat menjadi rumit untuk dikonfigurasi dan digunakan, terutama bagi pengguna yang kurang berpengalaman. Pemindaian oleh OpenVAS juga bisa memakan waktu cukup lama dan membutuhkan sumber daya sistem yang signifikan, yang dapat menjadi masalah dalam lingkungan produksi. Di sisi lain, Lynis adalah alat pemindaian keamanan host-based yang ringan dan mudah digunakan. Lynis mampu melakukan audit keamanan pada berbagai sistem Unix dan Linux, termasuk Ubuntu Server, dan memberikan laporan rinci tentang temuan dan rekomendasi perbaikan. Alat ini juga mendukung berbagai plugin dan pemeriksaan kepatuhan. Namun, Lynis memiliki cakupan pemindaian yang lebih terbatas dibandingkan dengan OpenVAS, terutama dalam hal deteksi kerentanan jaringan, dan kurang efektif dalam mengidentifikasi beberapa jenis kerentanan yang lebih kompleks.

Untuk mengatasi kekurangan dari solusi-solusi yang ada, pendekatan komprehensif dengan mengimplementasikan dan menganalisis penggunaan OpenVAS dan Lynis secara bersamaan diusulkan dalam penelitian ini. Integrasi OpenVAS dan Lynis dapat memberikan cakupan pemindaian yang lebih luas dan mendalam. OpenVAS dapat digunakan untuk pemindaian kerentanan jaringan yang komprehensif, sementara Lynis dapat fokus pada audit keamanan host-based. Dengan menggunakan kedua alat ini secara bersamaan, pengguna dapat memperoleh gambaran yang lebih lengkap tentang kondisi keamanan Ubuntu Server mereka. Konfigurasi dan optimasi penggunaan OpenVAS dan Lynis akan dilakukan untuk memastikan bahwa alat-alat ini dapat digunakan secara efektif dan efisien, termasuk pengaturan parameter pemindaian yang tepat, penjadwalan pemindaian yang optimal, dan pemanfaatan sumber daya sistem secara efisien. Setelah pemindaian dilakukan, hasil dari kedua alat ini akan dianalisis untuk mengidentifikasi kerentanan keamanan yang ditemukan. Berdasarkan hasil analisis ini, rekomendasi perbaikan yang konkret dan dapat diimplementasikan akan diberikan untuk meningkatkan keamanan Ubuntu Server. Dengan pendekatan ini, penelitian ini bertujuan untuk meningkatkan efektivitas deteksi kerentanan keamanan pada Ubuntu Server dan memberikan solusi yang lebih holistik dan praktis untuk mengatasi berbagai ancaman keamanan yang mungkin dihadapi.

II. Data dan Metodologi

2.1 Data dan Lokasi

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.

2.2 Metodologi

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:

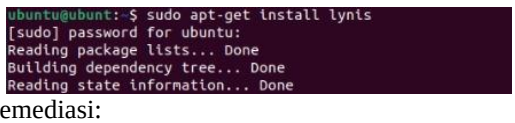
Tahap ini melibatkan penggunaan alat keamanan seperti OpenVAS untuk melakukan pemindaian sistem secara menyeluruh. Alat ini otomatis menemukan titik-titik rentan dalam keamanan sistem operasi Ubuntu Server, baik itu berada di jaringan, sistem operasi, maupun aplikasi yang berjalan di atasnya.

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.



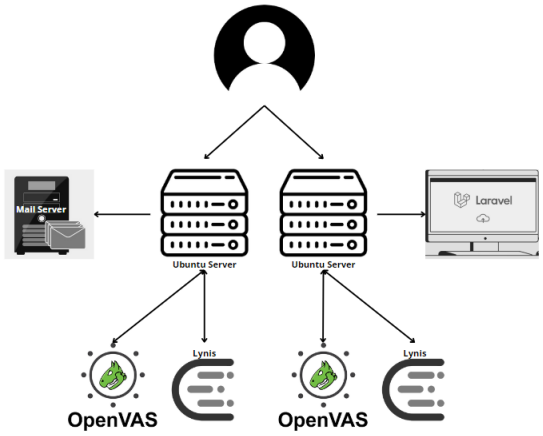
d. Remediasi:

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.

III. Hasil dan Pembahasan

3.1 Alur Implementasi Sistem

Bagian implementasi sistem ini fokus pada menjalankan rencana secara konkret dan memastikan sistem beroperasi dengan baik. Berikut adalah detail untuk bagian implementasi sistem:



3.2 Implementasi Sistem

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.

3. 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:
```

4. 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
```

5. 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.

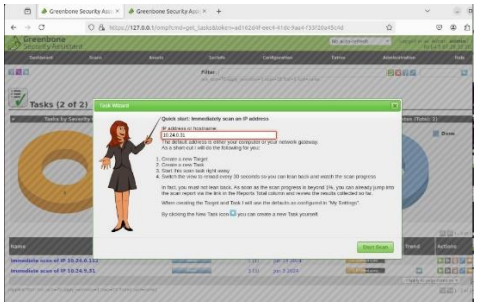
6. Instalasi Thunderbird: Thunderbird adalah klien email yang digunakan untuk menguji apakah mail server yang dibangun dengan Postfix berfungsi dengan baik. Dengan menggunakan Thunderbird, kita dapat mengirim dan menerima email melalui server Postfix yang telah dikonfigurasi.

7. 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.

3.3 Pelaksanaan Pemindaian dan Monitoring

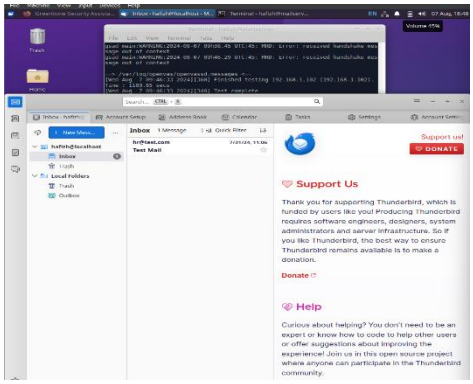
1. Setelah instalasi selesai, jalankan pemindaian kerentanan menggunakan OpenVAS dan Lynis sesuai dengan pengaturan yang telah ditentukan sebelumnya dalam tahap perancangan.



Pemindaian ke Ubuntu *Server* menggunakan OpenVAS

Pemindaian ke Ubuntu *Server* menggunakan Lynis

Tampilan Web Server



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.

3.4 Pengujian

3.4.1. Identifikasi Kerentanan

1. Skenario 1 Mail Server

a. Pemindaian Kerentanan dengan OpenVAS

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

.

b. Pemindaian Kerentanan dengan 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

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

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

3.4.2 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

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. Berikut adalah penjelasan dari hasil pemindaian menggunakan 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

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

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
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.

3.4.3 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 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

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

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

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

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.
12	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.

1. 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.

IV. Simpulan dan Saran

4.1 Simpulan

Dari hasil penelitian ini, bahwa analisis kebutuhan sistem dan evaluasi keamanan dari hasil implementasi kedua alat ini menghasilkan laporan yang mendeteksi kerentanan OpenVAS dan Lynis, Analisis kerentanan pada mail server dan web server di lingkungan Politeknik Negeri Jakarta menunjukkan bahwa kedua jenis server memiliki karakteristik kerentanan yang berbeda namun saling berkaitan. Mail server cenderung memiliki masalah pada konfigurasi layanan dan keamanan jaringan, sedangkan web server memiliki kerentanan yang lebih beragam, mulai dari konfigurasi aplikasi hingga sistem operasi. Meskipun demikian, keduanya sama-sama rentan terhadap kesalahan konfigurasi dan membutuhkan pembaruan yang rutin. Untuk meningkatkan keamanan secara keseluruhan, perlu dilakukan konfigurasi yang tepat, pembaruan sistem yang teratur, dan penerapan praktik keamanan terbaik. Dengan demikian, risiko serangan siber dapat diminimalisir dan integritas data serta layanan dapat terjaga. Ini mencakup masalah konfigurasi sistem dan masalah keamanan. Tingkat kerentanan (low, medium, dan high) ditetapkan berdasarkan tingkat keparahan dan dampak potensial dari masing-masing kerentanan terhadap sistem. Kerentanan dengan dampak rendah (low) biasanya tidak memerlukan tindakan segera tetapi tetap perlu diperhatikan, sementara kerentanan dengan dampak menengah (medium) memerlukan perhatian dan penanganan lebih lanjut. Kerentanan dengan dampak tinggi (high) harus segera diperbaiki karena dapat menimbulkan risiko keamanan sistem yang signifikan.

OpenVAS menggunakan analisis berbasis IP address untuk menunjukkan masalah jaringan tertentu, seperti sertifikat SSL/TLS yang kedaluwarsa dan konfigurasi timestamp TCP yang rawan. Sebaliknya, Lynis menunjukkan berbagai elemen konfigurasi internal, seperti tersedianya paket-paket yang rentan

dan izin file yang tidak aman, serta pengaturan layanan seperti SSH dan Apache yang membutuhkan perbaikan keamanan. Dengan kombinasi kedua alat ini, administrator memiliki pemahaman yang luas tentang keamanan infrastruktur, mulai dari tingkat jaringan hingga konfigurasi internal sistem operasi.

.2 Saran

Penelitian berikutnya disarankan mengusulkan inovasi dalam teknologi analisis keamanan sistem guna memberikan pemahaman yang lebih mendalam. Contoh inovasi termasuk eksplorasi penggunaan alat-alat keamanan terbaru atau teknik pemindaian yang lebih canggih untuk mendeteksi kerentanan yang lebih kompleks. Di samping itu, pertimbangkan juga integrasi tambahan dengan tools keamanan lainnya yang dapat meningkatkan kemampuan dalam mengidentifikasi dan menanggulangi ancaman keamanan secara efektif.

V. Referensi

Budi, E., Wira, D. and Infantono, A. (2021) 'Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0', Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO), 3(November), pp. 223–234. Available at: https://doi.org/10.54706/senastindo.v3.2021.141.

Dwiyatno, S. et al. (2020) 'Implementasi Virtualisasi Server Berbasis Docker Container', PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 7(2), pp. 165–175. Available at: https://doi.org/10.30656/prosisko.v7i2.2520.

Elisabeth, D.M. (2019) 'Kajian Terhadap Peranan Teknologi Informasi Dalam Perkembangan Audit Komputerisasi (Studi Kajian Teoritis)', METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 3(1), pp. 40–53.

Heryana, N. et al. (2023) Prinsip Sistem Operasi.

Indratno, S. (2022) 'Implementasi Load Balancing Mikrotik Menggunakan Metode ECMP Pada STIE Gentiaras Bandar Lampung', Jurnal Teknologi Pintar, 2(6), pp. 1–11. Available at: http://teknologipintar.org/index.php/teknologipintar/article/view/184%0Ahttp://teknologipintar.org/index.php/teknologipintar/article/download/184/180.

Muharrom, M. and Saktiansyah, A. (2023) 'Analysis of Vulnerability Assessment Technique Implementation on Network Using OpenVAS', International Journal of Engineering and Computer Science Applications (IJECSA), 2(2), pp. 51–58. Available at: https://doi.org/10.30812/ijecsa.v2i2.3297.

Seth, B. et al. (2021) 'Secure Cloud Data Storage System Using Hybrid Paillier – Blowfish Algorithm'. Available at: https://doi.org/10.32604/cmc.2021.014466.

Tenaya, G.A.P. et al. (2022) 'Analisis Performansi Dua Sistem Operasi Server CentOS 8 dan Oracle Linux 8 Menggunakan Metode Levene Dengan SysBench', INFORMAL: Informatics Journal, 7(1), p. 31. Available at: https://doi.org/10.19184/isj.v7i1.30172.

Wahid, A.A. (2019) 'Analisis Sistem Keamanan Pada Sistem Operasi Microsoft Windows, Linux Dan Macintosh', Teknik Informatika, 1(3), p. 2.

Yudha, C.F., Wing, W.W. and Eko, P. (2019) 'Analisis Teknologi Virtual Mesin Proxmox Dalam Rangka Persiapan Infrastruktur Server (Studi Kasus:Universitas Nahdlatul Ulama Yogyakarta)', Jurnal INFORMA Politeknik Indonusa Surakarta, 5, pp. 2442–7942.

Zaitsev, D. and Luszczek, P. (2020) 'Docker Container based PaaS cloud computing comprehensive Benchmarks using LAPACK', CEUR Workshop Proceedings, 2608, pp. 323–337. Available at: https://doi.org/10.32782/cmis/2608-25.