# Implementasi Dan Analisis *Vulnerability Management* Pada Tiga Versi Ubuntu Menggunakan *Open Source Vulnerability Scanner* Berdasarkan Cis *Security Metrics*

1st Fauzan Khairy Pulungan
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
fauzankhairypulungan@student.telkomuniversity.ac.id

2nd Umar Yunan Kurnia Septo Hediyanto
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

3rd Adityas Widjajarto
*Fakultas Rekayasa Industri*
*Universitas Telkom*
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

***Abstrak*— Penelitian ini menganalisis vulnerability management pada Ubuntu 18.04, 20.04, dan 22.04 berdasarkan standar CIS Security Metrics. Tools scanning yang digunakan untuk mendapatkan data kerentanan yaitu OpenSCAP. Skenario pengujian pada penelitian ini dijalankan dengan melakukan scanning kerentanan pada tiga versi Ubuntu . Berdasarkan CIS Security Metrics, pada aspek mean time to mitigate vulnerabilities, number of known vulnerabilities, mean time to patch, percentage of configuration, dan configuration management coverage sudah bisa mementukan dalam melakukan upgrade versi Ubuntu yang akan digunakan, yaitu melakukan upgrade versi Ubuntu secara langsung ke Ubuntu 22.04 dari Ubuntu 18.04. Kesimpulan penelitian ini merekomendasikan menggunakan Ubuntu versi 22.04 secara langsung dari versi 18.04 karena vulnerability lebih sedikit pada versi 22.04. Saran dari penelitian ini yaitu meningkatkan spesifikasi dari hardware perangkat yang digunakan untuk melakukan penelitian serta mencari standar dan juga vulnerability scanner yang lebih kompleks agar vulnerability lebih terperinci.**

***Kata kunci : vulnerability, CIS security metrics, Ubuntu, management***

## I. PENDAHULUAN

Perkembangan teknologi di era industri saat ini, sangat menunjukkan peningkatan trafik jaringan internet yang dipakai oleh masyarakat secara signifikan (Putri&Rachmawati, 2019. Pertumbuhan Internet dan kemudahan kepada pengguna komputer untuk dapat berbagi sumber daya dan informasi (Hakim et,al, 2015). Pelanggaran keamanan dapat berdampak sedang hingga parah pada organisasi tertentu, tergantung pada sifat organisasi dan cara sistem informasi yang digunakan (Amit, 2014). Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi saat ini. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang komprehensif dan terstruktur untuk memberikan perlindungan dari risiko organisasi yang munkgin dihadapi. Dalam upaya memecahkan masalah keamanan, dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi dan komunikasi (W, Riadi, & Yudhana, 2016).

Kerentanan sebuah Sistem Operasi sangat penting dipertimbangkan, agar dapat mencegah atau bahkan mengurangi akibat yang ditimbulkan seperti kerusakan karena adanya serangan dari pihak yang tidak bertanggung jawab. Peningkatan kesadaran akan penggunanya, menjadi dasar untuk melakukan langkah awal untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu Sistem Operasi. Faktor-faktor internal dan eksternal yang menjadi kelemahan tersebut adalah kurangnya kesadaran pemilik Sistem Operasi dan kurangnya maintenance serta pembaruan untuk Sistem Operasi tersebut.

Analisis *vulnerability* merupakan tahap penting dalam pengelolaan keamanan Sistem Operasi, termasuk Ubuntu, yang tersedia dalam versi 18.04 (*Bionic Beaver*), 20.04 (*Focal Fossa*), dan 22.04 (*Jammy Jellyfish*). Ubuntu adalah salah satu distribusi populer dari Sistem Operasi GNU/Linux yang digunakan secara luas oleh organisasi dan pengguna individu. Versi Ubuntu mencerminkan tahun rilisnya. Misalkan Ubuntu versi 18.04 menunjukan tahun rilis 2018, dan 04 merupakan versi pembaharuan pada tahun tersebut. Pemilihan Ubuntu versi 18.04, 20.04, dan 22.04 menjadi Sistem Operasi untuk dilakukan analisis *vulnerability* karena pada versi dengan tahun genap ini menunjukkan dukungan LTE (*Long Term Evolution*).

Dalam pengelolaan keamanan, penting untuk secara teratur menganalisis kerentanan yang ada dalam sistem dan mengambil tindakan yang sesuai untuk menutup celah keamanan. Analisis *vulnerability* membantu dalam mengidentifikasi kerentanan yang ada, mengevaluasi tingkat risiko yang terkait, dan memberikan wawasan yang diperlukan untuk mengambil tindakan yang diperlukan.

Dalam konteks analisis *vulnerability* pada Ubuntu, *Open*SCAP menjadi salah satu solusi yang dapat digunakan. *Open*SCAP adalah alat audit yang menggunakan *Extensible Configuration Checklist Description Format* (XCCDF) dan dapat memanfaatkan CIS *Security Metrics*. CIS *Security Metrics* menyediakan seperangkat metrik dan definisi data standar yang digunakan untuk mengumpulkan dan menganalisis informasi tentang kinerja dan hasil proses keamanan.

Dalam rangka mengatasi kerentanan yang ada, diperlukan penelitian, pengembangan, dan pemahaman yang baik tentang penggunaan *Open*SCAP berdasarkan CIS *Security Metrics* dalam analisis *vulnerability* pada Ubuntu versi 18.04, 20.04, dan 22.04. Solusi yang efektif akan memungkinkan organisasi untuk secara efisien mengidentifikasi dan mengevaluasi kerentanan dalam sistem Ubuntu, serta mengambil tindakan yang tepat untuk meningkatkan keamanan dan melindungi sistem dari serangan yang berpotensi merugikan.

## II. KAJIAN TEORI

Menyajikan dan menjelaskan teori-teori yang berkaitan dengan variable-variabel penelitian. Poin subjudul ditulis dalam abjad.

### A. *Vulnarebility*

Menurut Arianto (2016) Vulnerability adalah kelemahan dalam sistem atau infrastruktur yang dapat memungkinkan akses tanpa izin dengan memanfaatkan kelemahan tersebut. Kelemahan ini menjadi dasar bagi para peretas (hacker) untuk menciptakan eksploitasi sebagai cara untuk masuk ke dalam sistem secara ilegal. Hacker seringkali membuat eksploitasi yang sesuai dengan vulnerability yang telah mereka temukan.

### B. Sistem Operasi

Sistem Operasi adalah suatu perangkat lunak yang terdiri dari serangkaian perintah dan bertugas sebagai penghubung antara pengguna (manusia) dengan komputer, memungkinkan komputer untuk beroperasi sesuai dengan keinginan pengguna. (Pangera, 2005). Sistem Operasi yang digunakan pada penelitian ini adalah Windows dan Ubuntu, di mana Windows sebagai *Main*OS dan Ubuntu pada *virtual machine* yang akan dilakukan *vulnerability scan*.

#### 1. Ubuntu

Ubuntu merupakan sebuah distribusi dan Sistem Operasi berbasis GNU/Linux yang tersedia secara gratis dan bersifat open source. (Helmke, Joseph & Rey, 2017). Pada penelitian ini, Versi yang dipakai adalah Ubuntu versi 18.04, 20.04, dan 22.04. Pada penelitian ini, Ubuntu digunakan sebagai objek penelitian yang akan dilakukan *vulnerability scanning* menggunakan *tools Open*SCAP, karena *tools* ini dapat melakukan pemindaian menyeluruh terhadap OS.

### C. Virtualiasi

Virtualisasi adalah suatu proses berbasis perangkat lunak yang digunakan untuk menciptakan representasi dari suatu entitas, seperti *server* virtual, ruang penyimpanan virtual, dan koneksi virtual. Virtualisasi merupakan salah satu metode yang sangat efektif untuk mengurangi anggaran IT dan meningkatkan efisiensi dalam berbagai jenis bisnis. (Vyanza, 2023). Pada penelitian ini menggunakan VMWare sebagai *software* dalam melakukan virtualisasi dan akan dilakukan instalasi OS di dalamnya.

### D. *Vulnerability Scanner*

*Vulnerability scanner* adalah perangkat lunak yang mampu melakukan diagnosa dan analisis kerentanan, juga dikenal sebagai penilaian kerentanan. *Vulnerability scanner* bergantung pada sebuah *database* yang berisi informasi yang diperlukan untuk melakukan pemeriksaan sistem. *Database* kerentanan ini terus diperbarui untuk memastikan mencakup perkembangan terbaru dalam sebuah teknologi. Informasi dalam *database vulnerability scanner* ini digunakan untuk memeriksa dan mengidentifikasi kerentanan dalam Sistem Operasi, *port*, serta kelemahan dalam program atau skrip yang mungkin dapat dieksploitasi. *Scanner* ini kemudian mencoba untuk memanfaatkan setiap kerentanan yang ditemukan. Proses ini sering disebut sebagai *ethical hacking*. (Scarfone, Souppaya, Cody, & Orebaugh, 2008).

#### 1. OpenSCAP (Open Security Content Automation Protocol)

*Open*SCAP adalah sebuah alat audit yang menggunakan *Extensible Configuration Checklist Description Format* (XCCDF). XCCDF adalah sebuah standar yang digunakan untuk menyampaikan konten *checklist* dan menentukan daftar *checklist* keamanan. XCCDF juga digabungkan dengan spesifikasi lain seperti CPE, CCE, dan OVAL, untuk membuat daftar *checklist* SCAP yang dapat diproses oleh produk yang telah divalidasi SCAP.

### E. *Common Vulnerabilities and Exposures* (CVE)

*Common Vulnerabilities and Exposures* (CVE) adalah sebuah katalog yang berisi informasi tentang ancaman keamanan yang diketahui. Katalog ini didukung oleh Departemen Keamanan Dalam Negeri Amerika Serikat (DHS), dan ancaman tersebut dikelompokkan menjadi dua kategori: kerentanan (*vulnerabilities*) dan paparan (*exposures*). Menurut situs *web* CVE yaitu https://www.cve.org, kerentanan merujuk pada kesalahan dalam kode perangkat lunak yang memungkinkan penyerang untuk mendapatkan akses langsung ke sistem atau jaringan. Sebagai contoh, kerentanan dapat memungkinkan penyerang untuk menyamar sebagai *superuser* atau *administrator* sistem yang memiliki hak akses penuh. Di sisi lain, eksposur didefinisikan sebagai kesalahan dalam kode perangkat lunak atau konfigurasi yang memberikan penyerang akses tidak langsung ke sistem atau jaringan. Sebagai contoh, eksposur dapat memungkinkan penyerang untuk secara diam-diam mengumpulkan informasi pelanggan yang dapat dijual (Komputer, Kamus Komputer, 2017).

### F. *Common Vulnerability Scoring System* (CVSS)

*Common Vulnerability Scoring System* (CVSS) adalah sebuah metode pengukuran yang digunakan oleh individu atau organisasi untuk menilai tingkat kerentanan suatu sistem. CVSS saat ini dikelola oleh *forum of incident response and security teams* (FIRST). Tujuan dan sejarah CVSS berasal dari kebutuhan untuk menilai tingkat keparahan kerentanan dengan cara yang ditentukan dan terstruktur. Terdapat masalah ketika laporan kerentanan menyatakan dampak tertentu sebagai "*High*", sementara laporan lain mengklasifikasikan dampak sebagai "*medium*". Hal ini menunjukkan bahwa tidak ada sistem yang terlibat dalam penilaian tersebut, sehingga peringkatnya besifat subjektif.

Untuk mengatasi masalah ini, CVSS hadir dengan berbagai metrik yang telah ditentukan sehingga membuatnya lebih mudah untuk memahami komposisi skor akhir. CVSS pertama kali diperkenalkan dengan versi 1.0 pada tahun 2005, sebagai pendekatan yang kebanyakan berorientasi akademis dalam menilai tingkat keparahan kerentanan. Namun, ketika organisasi mencoba mengimplentasikan CVSS 1.0, mereka menghadapi masalah signifikasn.

Untuk mengatasi kendala tersebut, *forum of incident response and security teams* (FIRST) mengambil peran sebagai pemelihara CVSS. Ini menyebabkan perkembangan cepat CVSS versi 2.0, yang dirilis pada tahun 2007. Setelah delapan tahun berlalu dan mendapatkan umpan balik lebih lanjut dari organisasi dan pengguna, akhirnya dihasilkan rilis CVSS versi 3.0. Rilis ini mencakup perbaikan dan penyempurnaan untuk membuat sistem penilaian kerentanan menjadi lebih efektif dan relevan (FIRST, 2019). CVSS memberikan penilaian kerentanan dalam rentang skor 0.0 hingga 10.0, yang dibagi menjadi empat tingkatan: *Low* (0.0 - 3.9), *Medium* (4.0 - 6.9), *High* (7.0 - 8.9), dan *Critical* (9.0 - 10.0). CVSS menilai kerentanan berdasarkan delapan aspek utama, yaitu: *Attack Vector, Attack Complexity, Privilege Required, User Interaction, Scope, Confidentiality, Integrity, dan Availability* (Muliono, 2018). Pada penelitian ini menggunakan CVSS V3 dikarenakan versi ini adalah versi yang sedang dipakai oleh banyak organisasi dalam melakukan penilaian terhadap tingkat keparahan dari suatu *vulnerability*.

### G. CIS *Security Metrics*

CIS *security metrics* adalah seperangkat standar metrik dan definisi data yang digunakan oleh organisasi untuk

mengumpulkan dan menganalisis informasi tentang kinerja dan hasil dari proses keamanan. Dokumen ini mencakup 28 definisi metrik yang terkait dengan 7 fungsi bisnis utama. Penelitian ini hanya berfokus pada *vulnerability management*, *patch management, configuration management,* dan *change management*.

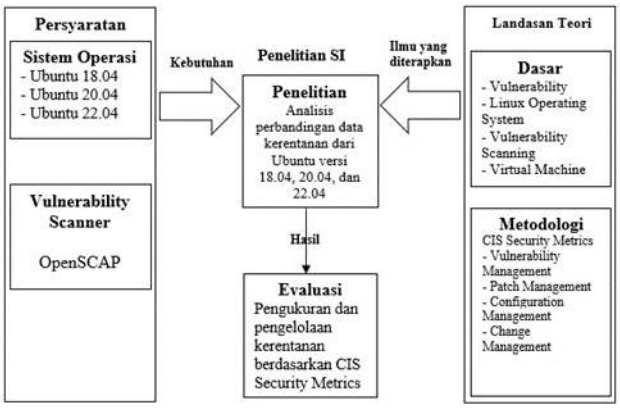
## III. METODOLOGI PENELITIAN

### A. Konseptual Model

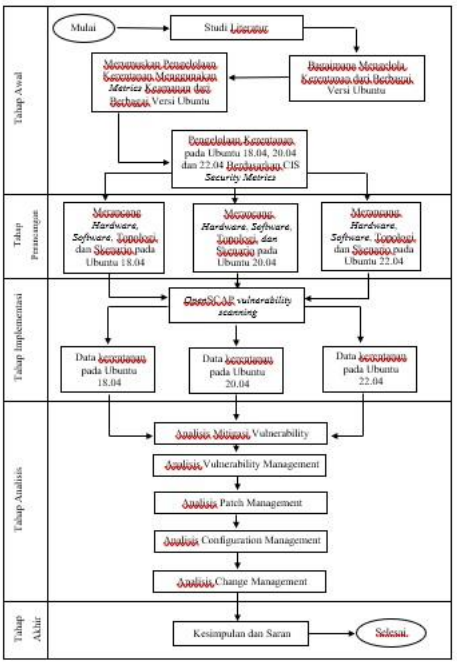
Model konseptual atau kerangka konseptual merupakan model atau kerangka yang menunjukkan hubungan logis antara faktor/variable yang telah diidentifikasi penting untuk menganalisis masalah penelitian. Kerangka konseptual dibangun berdasarkan teori yang sudah ada maupun dokumen-dokumen penelitian terdahulu sehingga terintegrasi sebagai satu kesatuan. Model konseptual yang ada dalam penelitian ini adalah sebagai berikut.

### B. Sistematika Penyelesaian Masalah

Sistematika pemecahan masalah merupakan urutan proses terencana yang perlu dilakukan untuk memcahkan masalah penelitian dengan baik. Sistematika pemecahan masalah dibagi 5 tahap yaitu : tahap awal, tahap perancangan, tahap implementasi, tahap analisis, dan tahap akhir. Berikut sistematika penelitian yang dijelaskan dalam bentuk bagan pada Gambar 2.




GAMBAR 1
Konseptual Model




GAMBAR 2
Sistematika Penyelesaian Masalah

## IV. PERANCANGAN DAN IMPLEMENTASI

### A. Perancangan Sistem

Untuk mencapai tujuan penelitian yang telah dijelaskan sebelumnya, diperlukan suatu struktur yang melibatkan perangkat keras (*hardware*) dan perangkat lunak (*software*) sebagai langkah awal dalam melakukan analisis dan pengujian data dari Ubuntu 18.04, 20.04, dan 22.04.

#### 1. Hardware

TABEL 1
Hardware

| Komponen | Informasi | |
|---|---|---|
| Spesifikasi *hardware* Inti (Laptop) | *Processor* | Intel Core i7 6700HQ Processor |
| | Memori | 8GB RAM |
| | *Hard Disk* | 1TB HDD |
| | Sistem Operasi | Windows 10 Pro 64-bit |
| | Tipe Sistem | 64-bit *Operating System,* x64-*based processor* |

TABEL 2 *Hardware Virtual Machine*

| Komponen | Informasi | |
|---|---|---|
| Spesifikasi Mesin Virtual 1 | *Processor* | 1 *processor core* |
| | Memori | 2048MB |
| | *Hard Disk* | 20GB |
| | Sistem Operasi | Ubuntu 18.04 (64-bit) |
| | Tipe Sistem | 64-bit *operating system* |
| Spesifikasi Mesin Virtual 2 | *Processor* | 1 *processor core* |
| | Memori | 2048MB |
| | *Hard Disk* | 20GB |
| | Sistem Operasi | Ubuntu 20.04 (64-bit) |
| | Tipe Sistem | 64-bit *operating system* |
| Spesifikasi Mesin Virtual 3 | *Processor* | 1 *processor core* |
| | Memori | 2048MB |
| | *Hard Disk* | 20GB |
| | Sistem Operasi | Ubuntu 22.04 (64-bit) |
| | Tipe Sistem | 64-bit *operating system* |

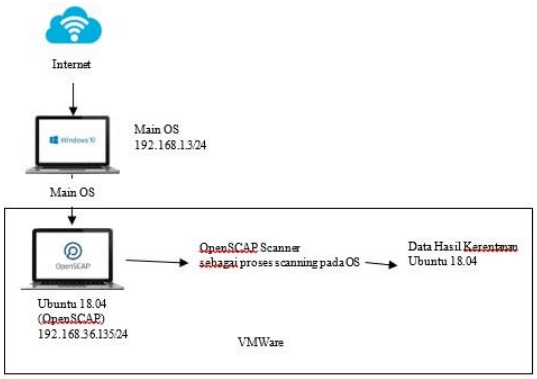
2. Software

*software* yang digunakan pada penelitian ini adalah :

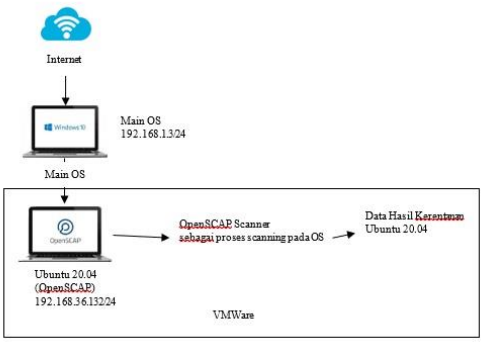
a. *Main* OS, penelitian ini menggunakan Windows 10 sebagai *Main* OS dengan versi 10 pro
b. *Operating system* yang digunakan pada masing-masing *virtual machine* adalah Ubuntu dengan versi 18.04-dekstop-amd64. 20.04-dekstop-amd64, dan 22.04-dekstop-amd64.
c. Pada penelitian ini *virtual machine* yang digunakan adalah VMWare. VMware merupakan perangkat lunak virtualisasi untuk melakukan instalasi *vulnerability scanning tools* dan *operating system*. Versi VMWare yang digunakan adalah versi 12.5.7 *build*-5813279.
d. *Tools* yang digunakan untuk melakukan *vulnerability scanning* pada masing-masing versi Ubuntu adalah *Open*SCAP dengan versi 1.2.15

B. Topologi

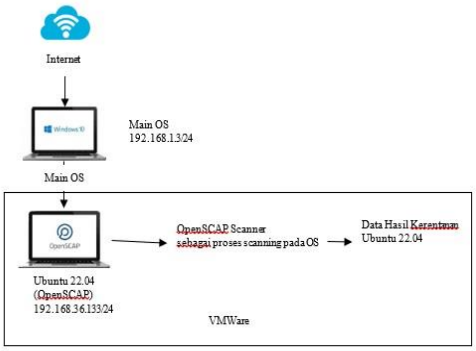
Berikut topologi yang ada dalam penelitian ini.




GAMBAR 3 Topologi pada Ubuntu 18.04




GAMBAR 4 Topologi pada Ubuntu 20.04

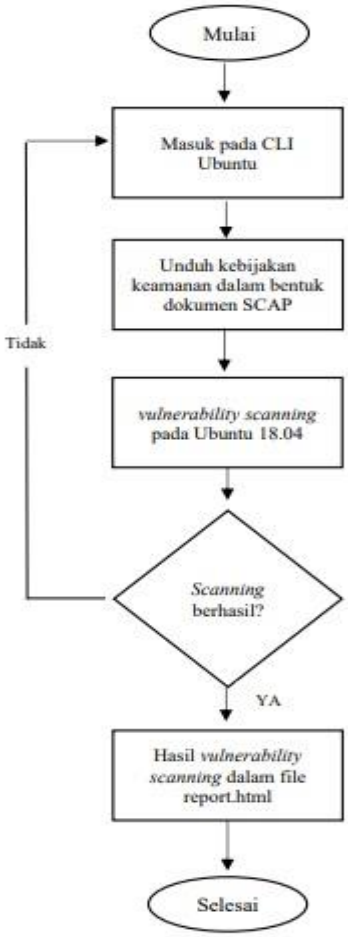



GAMBAR 5 Topologi pada Ubuntu 22.04

C. Skenario Pengujian

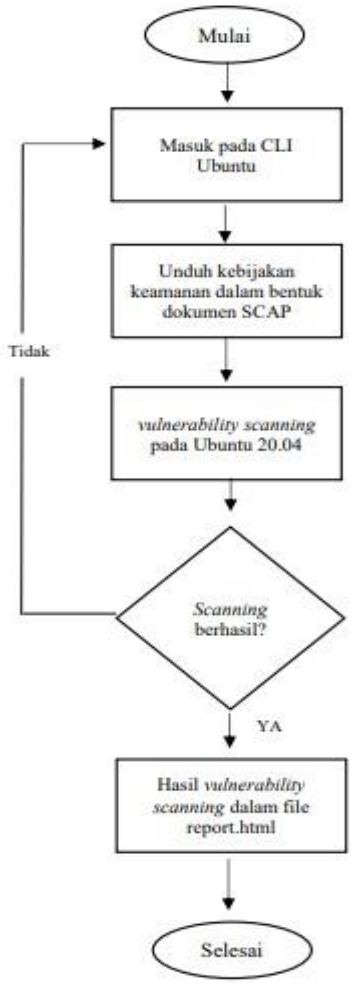
Diagram tersebut mewakili proses deteksi kerentanan secara keseluruhan pada Ubuntu 18.04, 20.04, dan 22.04.

1. Ubuntu 18.04



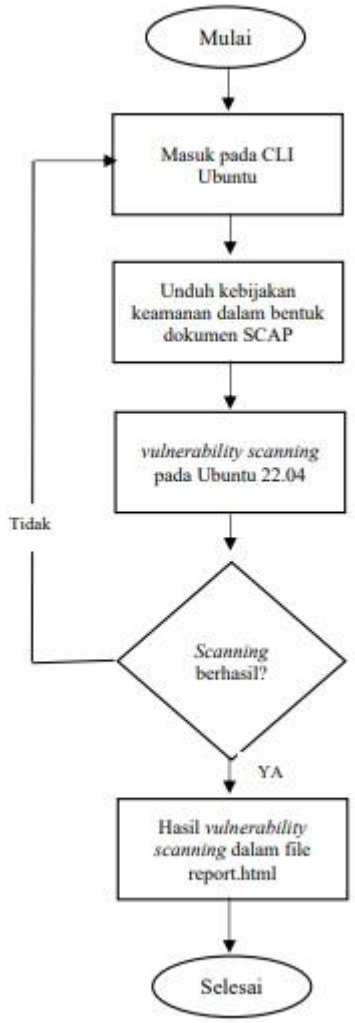

GAMBAR 6
Skenario Pengujian pada Ubuntu 18.04

2. Ubuntu 20.04




GAMBAR 7
Skenario Pengujian pada Ubuntu 20.04

3. Ubuntu 22.04




GAMBAR 8
Skenario Pengujian pada Ubuntu 22.04

D. Implementasi

1. Data Hasil Kerentanan

Berikut data hasil kerentanan pada penelitian ini :

TABEL 3
Data Hasil Kerentanan

| Host | Persentase *vulnerability* |
|---|---|
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 20.04 | 45 % |
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 22.04 | 15 % |
| *Vulnerability* pada Ubuntu 20.04 yang muncul kembali pada Ubuntu 22.04 | 24 % |
| *Vulnerability* pada Ubuntu 18.04 dan 20.04 yang muncul kembali pada Ubuntu 22.04 | 82 % |
| *Vulnerability* terbaru pada Ubuntu 22.04 | 6 % |

## V. ANALISIS

1. Analisis Mitigasi Vulnerability

Berikut tabel analisis mitigasi dari sampel *vulnerability* yang nilai persentasenya paling kecil

TABEL 4 Mitigasi pada Sampel *Vulnerability* Persentase Terkecil

| No | Vulnerability Name | Vulnerability ID | CVSS V3 | Severity Level | Mitigation | Mitigation Time |
|---|---|---|---|---|---|---|
| 1. | Vim *vulnerabilities* | CVE-2022-0943 | 7.8 | High | Update to vim 8.2 from previous version | 19 months |
| 2. | Wayland *vulnerability* | CVE-2021-3782 | 9.8 | Critical | update to wayland 1.20.91 from previous version | 16 months |
| 3. | Exempi *vulnerabilities* | CVE-2018-12648 | 7.5 | High | Update to exempi 2.5.1 from previous version | 16 months |
| 4. | GnuTLS *vulnerabilities* | CVE-2021-4209 | 6.5 | Medium | Update to gnutls 3.7.3 from previous version | 8 months |
| 5. | GnuPG *vulnerability* | CVE-2022-34903 | 6.5 | Medium | Update to GnuPG 2.3.7 from previous version | 3 months |
| 6. | Curl *vulnerability* | CVE-2022-35252 | 3.7 | Low | Update to curl 7.85.0 from previous version previous version | 2 months |
| 7. | Poppler *vulnerability* | CVE-2022-34903 | 7.8 | High | Update to poppler 22.09 from previous version | 1 month |
| 8. | Python *vulnerability* | CVE-2015-20107 | 7.6 | High | Update to python 3.10.8 from previous version | 1 month |
| 9. | NSS *vulnerabilities* | CVE-2022-22747 | 6.5 | Medium | Update to firefox 96.0 and thunderbird 91.5 from previous version | 1 month |
| 10. | OpenSSL *vulnerability* | CVE-2022-2097 | 5.3 | Medium | Update to openssl 1.1.1q from previous version | 1 month |

2. Analisis Vulnerability Scanning Coverage

Pada aspek ini akan dilakukan perbandingan data persentase *vulnerability* pada lingkup aplikasi dan sistem yang ada pada Ubuntu 18.04, Ubuntu 20.04, dan Ubuntu 22.04.

TABEL 5
Analisis *Vulnerability Scanning Coverage*

| Versi OS | Persentase Kerentanan | |
|---|---|---|
| | Aplikasi | Sistem |
| Ubuntu 18.04 | 56% | 44% |
| Ubuntu 20.04 | 57% | 43% |
| Ubuntu 22.04 | 57% | 43% |

3. Analisis Percent of System No Known Severe Vulnerabilities

Pada aspek ini dilakukan identifikasi *vulnerability* yang tidak diketahui baik dari *vulnerability* ID, nilai, atau levelnya pada semua data yang didapatkan dari *vulnerability* yang ada pada Ubuntu 18.04, 20.04, dan 22.04. Berikut daftar kerentanannya.

TABEL 6
Analisis *Percent of System No Known Severe Vulnerabilities*

| Vulnerability Name | Vulnerability ID | CVSS V3 | Severity Level |
|---|---|---|---|
| CUPS *vulnerability* | CVE-2018-4700 | N/A | N/A |
| Babel *vulnerability* | N/A | N/A | N/A |
| GPSd *vulnerability* | N/A | N/A | N/A |
| Caribou vulnerability | N/A | N/A | N/A |
| LTSP Display Manager *vulnerabilities* | N/A | N/A | N/A |
| GNOME Settings *vulnerability* | CVE-2022-1736 | N/A | N/A |

4. Analisis Number of Known Vulnerabilities

Pada aspek ini akan dilakukan perbandingan data jumlah *vulnerability* pada lingkup aplikasi dan sistem yang ada pada Ubuntu 18.04, Ubuntu 20.04, dan Ubuntu 22.04.

TABEL 7 Analisis *Number of Known Vulnerabilities*

| No | Versi OS | Jumlah Kerentanan | |
|---|---|---|---|
| | | Aplikasi | Sistem |
| 1 | Ubuntu 18.04 | 290 | 227 |
| 2 | Ubuntu 20.04 | 202 | 153 |
| 3 | Ubuntu 22.04 | 53 | 40 |

5. Analisis Mean Time to Patch

Pada aspek ini dilakukan perbandingan data waktu *vulnerability* dalam melakukan mitigasi pada Ubuntu versi 18.04, 20.04, dan 22.04.

TABEL 8
Analisis *Mean Time to Patch*

| No | Versi OS | Waktu Mitigasi Kerentanan (bulan) |
|---|---|---|
| 1. | Ubuntu 18.04 | 8 bulan |
| 2. | Ubuntu 20.04 | 6,6 bulan |
| 3. | Ubuntu 22.04 | 5,1 bulan |

6. Analisis Percentage of Configuration Compliance

Pada aspek ini dilakukan perbandingan data persentase *vulnerability* yang muncul dari versi Ubuntu yang paling bawah namun tidak ditangani atau muncul kembali pada versi Ubuntu yang lebih tinggi dan sudah dilakukan mitigasi, misalnya *vulnerability* pada Ubuntu 18.04 yang tidak ditangani atau muncul kembali pada Ubuntu 20.04.

TABEL 9 Analisis *Percentage of Configuration Compliance*

| Host | Persentase *vulnerability* |
|---|---|
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 20.04 | 45 % |
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 22.04 | 15 % |
| *Vulnerability* pada Ubuntu 20.04 yang muncul kembali pada Ubuntu 22.04 | 24 % |
| *Vulnerability* pada Ubuntu 18.04 dan 20.04 yang muncul kembali pada Ubuntu 22.04 | 82 % |
| *Vulnerability* terbaru pada Ubuntu 22.04 | 6 % |

7. Analisis Configuration Management Coverage

Pada aspek ini dilakukan perbandingan data jumlah *vulnerability* yang muncul dari versi Ubuntu yang paling bawah namun tidak ditangani atau muncul kembali pada versi Ubuntu yang lebih tinggi dan sudah dilakukan mitigasi pada lingkup aplikasi dan sistem, misalnya *vulnerability* pada Ubuntu 18.04 yang tidak ditangani atau muncul kembali pada Ubuntu 20.04.

TABEL 10
Analisis *Configuration Management Coverage*

| Host | Aplikasi | Sistem |
|---|---|---|
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 20.04 | 135 | 98 |
| *Vulnerability* pada Ubuntu 18.04 yang muncul kembali pada Ubuntu 22.04 | 46 | 30 |
| *Vulnerability* pada Ubuntu 20.04 yang muncul kembali pada Ubuntu 22.04 | 52 | 35 |
| *Vulnerability* pada Ubuntu 18.04 dan 20.04 yang muncul kembali pada Ubuntu 22.04 | 46 | 30 |
| *Vulnerability* terbaru pada Ubuntu 22.04 | 2 | 3 |

8. Analisis Mean Time to Complete Change

Pada aspek ini memberikan informasi terkait waktu rata-rata dari rilisnya Ubuntu versi 18.04, 20.04, dan 22.04.

TABEL 11
Analisis *Mean Time to Complete Change*

| Host | Rilis |
|---|---|
| Ubuntu 18.04 | 26 April 2018 |
| Ubuntu 20.04 | 23 April 2020 |
| Ubuntu 22.04 | 21 April 2022 |

Pada Tabel 11 menjelaskan tentang waktu rilis dari Ubuntu 18.04, 20.04, dan 22.04 yang berisi tanggal, bulan, dan tahun rilisnya. Setelah dilakukan analisis didapatkan rata-rata waktu rilis dari Ubuntu 18.04, 20.04, dan 22.04 adalah 32 bulan.

## VI. KESIMPULAN

Berdasarkan hasil analisis ada beberapa kesimpulan yang dapat diambil yaitu data yang didapatkan, hasil *vulnerability scanning* terbanyak terdapat pada platform Ubuntu 18.04 yang kerentanannya tidak ditangani pada Ubuntu 20.04 berjumlah 233 *vulnerability* dari total 517 *vulnerability* pada Ubuntu 18.04 dan didapatkan persentase tersebut sebesar 45 persen. Sedangkan hasil *vulnerability scanning* terendah terdapat pada platform Ubuntu 18.04 yang kerentanannya tidak ditangani atau muncul kembali pada Ubuntu 22.04 yang berjumlah 76 *vulnerability* dari total 517 *vulnerability* pada Ubuntu 18.04 dan didapatkan persentase tersebut sebesar 15 persen. Aspek *vulnerability scanning coverage* belum bisa dalam menentukan *upgrade* versi Ubuntu yang akan digunakan. Kemudian pada aspek *mean time to mitigate vulnerabilities*, *number of known vulnerabilities*, *mean time to patch*, *percentage of configuration*, dan *configuration management coverage* sudah bisa mementukan dalam melakukan *upgrade* versi Ubuntu yang akan

digunakan, yaitu melakukan *upgrade* versi Ubuntu secara langsung ke Ubuntu 22.04 dari Ubuntu 18.04. Analisa aspek *percent of systems no known severe vulnerabilities* didapatkan data 6 kerentanan yang tidak diketahui baik dari *vulnerability* ID, nilai, dan levelnya, pada aspek ini tidak berpengaruh dalam menentukan keputusan dalam *upgrade* versi Ubuntu karena *vulnerability* tersebut telah dihapus dari *database* kerentanan. Analisa aspek *mean time to complete change* tidak bisa memberikan saran tentang *upgrade* versi Ubuntu karena tidak membahas tentang *vulnerability* dan hanya memberikan acuan rilisnya Ubuntu versi 18.04, 20.04, dan 22.04. Berdasarkan semua data temuan dari hasil analisis menggunakan CIS *security metrics* disarankan melakukan mitigasi atau *upgrade* secara langsung ke Ubuntu 22.04 dari Ubuntu 18.04.

## REFERENSI


Amit, N. (2014). Linux Server & Hardening Security.

Arianto. (2016). Pengertian Vulnerability dan Cara Pencegahan. Diambil dari https://www.tembolok.id/pengertian-vulnerability-contoh-dan-pencegahan/

FIRST. (2019). Dicari kembali pada 2023, dari https://www.first.org/cvss/

Hakim, L., Murtiyasa, B., & Handaga, B. (2015). Analisis Perbandingan Intrusion Detection System Snort Dan Suricata. 6-14.

Helmke, Joseph, & Rey. (2017). The Official Ubuntu Book.

Hidayah, F. N., Almaarif, A., & Widjajarto, A. (2023). ANALISIS VULNERABILITY MANAGEMENT PADA VULNERABLE DOCKER DAN DOCKER IMAGES MENGGUNAKAN DOCKER SCAN DAN OPENSCAP BERDASARKAN STANDAR NIST CSF .

Komputer, K. (2017). Kamus Komputer. Dicari kembali 2023, dari Kamus Komputer: https://www.kamuskomputer.com/definisi/vulnerability-scanner/

Muliono, Y. (2018). Dicari kembali 2023, dari https://socs.binus.ac.id/2018/12/13/mengenal-istilah-common-vulnerability-scoring-system/

National Vulnerability Database. (n.d.). Dicari kembali pada 2023, dari nvd.nist.gov: https://nvd.nist.gov/

Pangera. (2005). Sistem Operasi.

Putri, D., & Rachmawati, A. (2019). Honeypot cowrie implementation to protect ssh protocol in ubuntu server with visualisation using kippo-graph. International Journal of Advanced Trends in Computer Science and Engineering, 8(6), 3200–3207. doi:https://doi.org/10.30534/ijatcse/2019/86862019

Ramadhan, H. W., Kurniawan, M. T., & Widjajarto, A. (2021). IMPLEMENTASI DAN ANALISIS SECURITY AUDITING MENGGUNAKAN OPEN SOURCE VULNERABILITY SCANNER SOFTWARE PADA SERVER KONTROLER ANSIBLE.

Ramadhan, R. S., Almaarif, A., & Widjajarto, A. (2023). ANALISIS VULNERABILITY MANAGEMENT PADA VULNERABLE DOCKER IMAGES DAN APLIKASI DOCKER IMAGES MENGGUNAKAN CLAIR SCANNER DAN JOOMSCAN BERDASARKAN STANDAR GSA CIO-IT SECURITY-17-80.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment.

Security, T. C. (2010). The CIS Security Metrics.

Teimouri, D. (2018). what is OpenSCAP. Dicari kembali pada 2023, dari teimouri.net: https://www.teimouri.net/what-is-openscap/

Ubuntu wiki : Release. (n.d.). Dicari kembali pada 2023, dari Ubuntu Web site: https://wiki.ubuntu.com/Releases

VMWare. (n.d.). About us: VMWare. Dicari kembali pada 2023, dari VMware Web Site: https://www.vmware.com/sg/company.html

Vyanza. (2023). Membangun Server Berbasis Debian Menggunakan Aplikasi VirtualBox.

W, Y., Riadi, I., & Yudhana, A. (2016). Analisis Keamanan WebserverMenggunakan Metode Penetrasi Testing ( PENTEST ).