Bab I Pendahuluan

I.1 Latar Belakang

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 menunjukkan 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.

I.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka penulis merumuskan permasalahan dalam penelitian ini sebagai berikut :

1. Bagaimana menelusuri kerentanan dari berbagai versi Ubuntu?
2. Bagaimana analisa menggunakan *metrics* keamanan pada kerentanan dari berbagai versi Ubuntu?
3. Bagaimana mitigasi berdasarkan pengelolaan kerentanan dari berbagai versi Ubuntu?

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

1. Melakukan *vulnerability scanning* untuk mendapatkan kondisi *vulnerability* pada Ubuntu versi 18.04, 20.04, dan 22.04.

2. Menerapkan CIS *Security Metrics* untuk melakukan analisis *vulnerability* pada Ubuntu versi 18.04, 20.04, dan 22.04.

3. Menganalisa bagaimana mitigasi dari hasil *vulnerability management* pada Ubuntu versi 18.04, 20.04, dan 22.04.

I.4 Manfaat Penelitian

Manfaat dari penelitian ini sebagai berikut :

1. Keilmuan
   - Memberikan pengetahuan terkait aspek pengelolaan kerentanan pada berbagai versi Ubuntu.
   - Memberikan pengetahuan terkait peran CIS *Security Metrics* dalam melakukan analisis *vulnerability*.
2. Praktis
   - Memberikan solusi terhadap kerentanan yang ada dalam Ubuntu versi 18.04, 20.04, dan 22.04.
   - Memberikan gambaran dan fungsi *Open*SCAP pada Ubuntu versi 18.04, 20.04, dan 22.04.

I.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini, yaitu :

1. Tahapan eksperimen dari penelitian ini dilakukan sebatas pada level sistem.

2. *Vulnerability scanning* menggunakan *Open*SCAP pada Ubuntu versi 18.04, 20.04, dan 22.04 yang tidak membahas *patching* dan pengelolaannya.

3. Penggunaan CIS *Security Metrics* dibatasi hanya pada *Vulnerability Management, Patch Management, Configuration Management*, dan *change management*.

I.6 Sistematika Penulisan

Sistematika penulisan penelitian ini adalah sebagai berikut :

BAB I Pendahuluan

Bab ini terdiri dari latar belakang berupa cara dalam mengemukakan masalah terkait penelitian. Perumusan masalah berupa hal-hal apa yang menjadi fokus untuk dibahas. Tujuan penelitian berupa tujuan dari penelitian dibuat. Manfaat penelitian berupa manfaat yang didapatkan pada penelitian dan dibagi menjadi manfaat keilmuan dan praktis. Batasan penelitian berupa hal-hal apa saja yang menjadi batasan pada penelitian untuk menghindari penyimpangan maupun pelebaran pokok masalah agar penelitian lebih terarah. Dan sistematika penulisan berupa bab-bab yang ada pada penelitian serta pembahasannya.

BAB II Tinjauan Pustaka

Bab ini berisi tentang teori dasar yang digunakan dalam penyelesaian penelitian ini, khususnya mengenai *Vulnerability, Open*SCAP, dan CIS *Security Metrics* untuk mendukung penelitian terkait penanganan kerentanan, strategi mitigasi, serta analisa.

BAB III Metodologi Penelitian

Bab ini berisi penjelasan mengenai konseptual model untuk merumuskan solusi dari permasalahan yang ada. Model konseptual dalam penelitian ini dibagi menjadi 3 bagian yaitu persyaratan, penelitian SI, dan landasan teori. Pada persyaratan terdapat 2 bagian yaitu Sistem Operasi yang digunakan yaitu Ubuntu versi 18.04, 20.04, dan 22.04. Selanjutnya bagian *vulnerability scanner* menggunakan *Open*SCAP. Kemudian pada penelitian SI terdapat 2 bagian yaitu penelitian yang berisi analisa perbandingan data kerentanan dari Ubuntu versi 18.04, 20.04, dan 22.04 . Selanjutnya bagian evaluasi yang berisi pengukuran dan pengelolaan kerentanan berdasarkan CIS *Security Metrics*. Terakhir pada landasan teori terdapat 2 bagian yaitu dasar berisi teori yang digunakan dan metodologi yang digunakan.. Dan juga berisi sistematika penelitian yang digunakan untuk menjelaskan langkah-langkah penyelesaian masalah.

BAB IV Perancangan dan Implementasi

Bab ini berisi penjelasan mengenai rancangan sistem dan penggunaan *open source vulnerability tools* yaitu *Open*SCAP yang digunakan untuk melakukan *scanning*. Skenario yang dilakukan pada Ubuntu 18.04, 20.04, dan 22.04 dalam bentuk simulasi dan penjelasan mengenai setiap hasil dari skenario pengujian.

BAB V Analisis

Bab ini berisi tentang analisis dari data hasil pengujian yang telah dilakukan pada bab sebelumnya mengenai *vulnerability* yang ditemukan pada Ubuntu 18.04, 20.04, dan 22.04. Analisis ini dilakukan menggunakan CIS *Security Metrics* dengan salah satu tujuan untuk mengelola pembaharuan versi Ubuntu.

BAB VI Kesimpulan dan Saran

Bab ini berisi penjelasan kesimpulan dari penelitian yang telah dilakukan, rancangan sistem, dan skenario pengujian serta saran yang diperlukan agar untuk peluang penelitian selanjutnya.