BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Dalam melakukan penelitian terkait analisis resiko kerentanan komunikasi data pada perangkat pendukung industri 4.0, Perlu untuk meninjau penelitian terdahulu yang nantinya digunakan sebagai acuan dan pedoman untuk melakukan penelitian selanjutnya. Dan peneliti memerlukan data untuk mendukung penelitian ini maka diperlukannya penelitian-penelitian terdahulu yang relevan dan akan di bahas dalam tabel 2.1.

2.1.1 Penelitian Terdahulu I

Pada penelitian terdahulu yang ditulis oleh J. Sönnerup, M. Hell (2018) terkait "Evaluating Security of Software Through Vulnerability Metrics" yang menjelaskan tentang bagaimana seseorang memahami dan mengukur keamanan dari sebuah perangkat lunak yang memiliki kerentanan yang berbeda-beda. Dibutuhkannya metrik kerentanan ini sangat penting untuk meninjau dan memutuskan terkait kerentanan apa yang terekspos pada sebuah perangkat lunak. Dari penggunaan metrik kerentanan tersebut menunjukkan bahwa setiap data CVE yang dirilis secara umum memang data yang dapat di pertanggung jawabkan terkait kerentanan-kerentanan yang berada dalam NVD atau *National Vulnerability Database* sehingga acuan dalam mencari

kerentanan sebuah produk perangkat lunak benar-benar direview secara matang dan dengan skor yang relevan.

2.1.2 Penelitian Terdaluhu II

Pada penelitian lain yang ditulis oleh D. De Roure, S. Cannady, R. Mantilla Montalvo, R. Nicolescu, M. Huth, and P. Radanliev (2019) yang berjudul "Analysing IoT cyber risk for estimating IoT cyber insurance." juga membahas tentang industri 4.0 juga menyebutkan bahwa banyak sekali kemungkinan-kemungkinan yang terjadi sehingga pertukaran data yang terjadi bisa bocor atau di ketahui oleh *hacker* ataupun orang lain yang seharusnya tidak boleh tahu atas data tersebut. Karena pada industri 4.0 ini banyak sekali melibatkan sensor-sensor yang saling terhubung dan bagaimana kita bisa mengetahui setiap sensor tersebut sudah aman dalam proses pertukan data, sehingga diperlukannya langkah awal untuk membuat sebuah regulasi untuk memberikan batasan terhadap perangkat-perangkat IoT yang terdapat pada industri 4.0. Pada jurnal tersebut juga telah memberikan pemahaman terkait upaya-upaya untuk mengintegeritaskan standar dan tata kelola ke dalam Industri 4.0 dan menawarkan pemahaman yang lebih baik tentang model penilaian dampak ekonomi untuk industri 4.0 [4].

2.1.3 Penelitian Terdahulu III

Pada penelitian terdahulu lainnya juga yang ditulis oleh A. Fajaryanto, T. Dirgahayu, dan Y. Prayudi (2015) yang berjudul "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web" membahas tentang metode yang nantinya akan saya gunakan pada penelitian ini, yaitu *passive information gatherting*. Metode ini digunakan untuk mengumpulkan informasi-informasi terkait perangkat yang terhubung ke internet melaui jaringan ip public dengan mengambil ip address, merek perangkat, versi perangkat, port yang terbuka, dan beberapa informasi yang sangat diperlukan oleh attacker maupun pentester. Passive information gathering merupakan langkah awal dalam hal *IT Security* untuk menuju fase lainnya jadi diperlukannya untuk mengenali perangkat dan karakteristik dari target adalah langkah awal attacker maupun pentester dalam melakukan serangan terhadap targetnya [5].

Tabel 2. 1 Penelitian Terdahulu

No	Judul/Peneliti/Tahun	Metode	Perumusan Masalah	Hasil Penelitian
1	Evaluating Security of Software Through Vulnerability Metrics/ J. Sönnerup, M. Hell/2018	Vulnerability Metrics	Melakukan evaluasi terhadap perangkat lunak menggunakan vulnerability metrics untuk mendapatkan hasil skoring	
2	Analysing IoT cyber risk for estimating IoT cyber insurance.	Cyber Value-At-Risk	Melakukan analisis terkait perkembangan dunia insdustri di era 4.0 yang nantinya akan memberikan penilaian dampak resiko kuantitatif pada era industri 4.0	
3	Penerapan Metode ISSAF Dan OWASP Versi 4 Untuk Uji Kerentanan Web Server/A. Fajaryanto, T. Dirgahayu, Y. Prayudi/2015	ISSAF dan OWASP versi 4	Menggunakan metode ISSAF dan OWASP versi 4 untuk menguji tingkat keamanan dari web server	

2.2 Teori Dasar Yang Digunakan

2.2.1 Manajemen Resiko

Manajemen risiko adalah suatu pembahasan yang disusun; Suatu rangkaian aktivitas manusia termasuk: Edisi rilis, pengembangan strategi untuk mengelola dan mengelola risiko dengan menggunakan pemberdayaan /

pengelolaan Sumber Daya. Strategi yang dapat diambil antara lain adalah memindahkan risiko ke pihak lain, menghindari risiko, mengurangi efek negatif, dan mengambil sebagian atau semua risiko. Manajemen risiko tradisional berfokus pada risiko-risiko yang diakibatkan oleh sebab fisik atau hukum (seperti bencana alam atau kebakaran, kematian, serta pemulihan hukum. Manajemen risiko dapat diterapkan pada seluruh organisasi, pada seluruh area kegiatan dan pada setiap tingkat, setiap saat, baik pada setiap fungsi khusus, proyek, proses maupun setiap kegiatan. Mengenai sasaran dan tujuan pelaksanaan manajemen risiko adalah untuk mengurangi risiko yang mungkin akan muncul (risiko), mengukur risiko dari potensi ancaman, menentukan seberapa besar kerugian yang diderita akibat meningkatkan potensi bisnis. Ancaman ini dapat disebabkan oleh berbagai elemen seperti teknologi, human error, Lingkungan, politik maupun dari organisasi[6].

2.2.2 Kerentanan Jaringan

Keamanan jaringan saat ini menjadi masalah yang sangat penting dan terus berkembang. Beberapa masalah menyangkut sistem keamanan saat ini menjadi suatu garapan yang membutuhkan biaya dan perlindungan yang besar. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan dan sistem-sistem setingkat itu, membutuhkan tingkat keamanan yang dibutuhkan tinggi. Hal ini lebih penting karena kemajuan bidang komputer dengan konsep

terbuka sistemnya jadi tantangan, di mana saja dan kapanpun, memiliki peluang untuk mengakses kawasan vital tersebut. Keamanan jaringan yang terdefinisi dari sumber daya untuk melawan penyingkapan, modifikasi, utilisasi, pelarangan dan perusakan oleh orang yang tidak dapat diizinkan. Beberapa ahli jaringan mengatakan bahwa hanya ada satu cara mudah dan ampuh untuk membuat sistem jaringan komputer yang aman yaitu dengan menggunakan pemisah antara komputer dengan jaringan selebar satu inci, dengan kata lain, hanya komputer yang tidak terhubung ke jaringanlah yang menyediakan keamanan yang sempurna. Meskipun ini adalah solusi yang buruk, tetapi ini menjadi trade-off antara pertimbangan fungsionalitas dan memasukan kekebalan terhadap gangguan.

Keamanan jaringan komputer sendiri sering dipandang sebagai hasil dari beberapa faktor yang bervariasi tergantung pada bahan dasar, tetapi secara normal setidaknya beberapa hal di bawah ini diikutsertakan: (1) *confidentiality* (kerahasiaan) – ada beberapa jenis informasi yang tersedia di dalam sebuah jaringan komputer. Setiap data yang berbeda pasti mempunyai grup pengguna yang berbeda pula dan data dapat dikelompokkan sehingga beberapa pembatasan kepada penggunaan data harus ditentukan. Pada umumnya data yang terdapat di dalam suatu perusahaan bersifat rahasia dan tidak boleh diketahui oleh pihak ketiga yang bertujuan untuk menjaga rahasia perusahaan dan strategi perusahaan. Backdoor, sebagai contoh, melanggar

kebijakan perusahaan dikarenakan menyediakan akses yang tidak diinginkan ke dalam jaringan komputer perusahaan; (2) *integrity* (integritas) – jaringan komputer yang dapat diandalkan juga berdasar pada fakta bahwa data yang tersedia apa yang sudah seharusnya. Jaringan komputer mau tidak mau harus terlindungi dari serangan yang dapat merubah data selama dalam proses transmisi. Man-in-the-Middle merupakan jenis serangan yang dapat merubah integritas dari sebuah data yang mana penyerang (attacker) dapat membajak session atau memanipulasi data yang terkirim; (3) *availability* (ketersediaan) – ketersediaan data atau layanan dapat dengan mudah dipantau oleh pengguna dari sebuah layanan. Ketidaktersediaan dari sebuah layanan dapat menjadi sebuah halangan untuk maju bagi sebuah perusahaan dan bahkan dapat berdampak lebih buruk lagi, yaitu penghentian proses produksi. Sehingga untuk semua aktifitas jaringan, ketersediaan data sangat penting untuk sebuah sistem agar dapat terus berjalan dengan benar [7].

2.2.3 Era Industri 4.0

Industri 4.0 adalah istilah yang saat ini umum digunakan untuk revolusi industri ke-4. Berbagai studi1-5 menjelaskan bahwa revolusi pertama yang dimulai dengan penemuan mesin uap pada tahun 1780an berkembang hingga pertengahan abad XIX berbasis industri mekanik berdaya air dan uap. Pada akhir abad XIX revolusi kedua ditandai dengan kemampuan produksi massal

dengan tenaga listrik berbasis pembagian kerja (assembly line). Kemudian, pada tahun 1970an dimulai era revolusi ketiga dengan otomasi pekerjaan-pekerjaan kompleks didukung teknologi elektronik dan informasi. Saat ini dikatakan revolusi keempat ditandai dengan kemampuan teknologi sensor, keterhubungan (*interconnectivity*) dan analisis data yang memungkinkan kustomisasi (*customization*) massal, integrasi rantai pasokan dan efisiensi lebih tinggi berbasis sistem *cyber-physical*. Dengan kata lain, Industri 4.0 adalah transformasi yang demikian cepat dalam desain, manufaktur, operasi, sertra layanan produk dan sistem produksi. Studi-studi tersebut juga menyebutkan bahwa Industri 4.0 mengubah banyak hal, termasuk: meningkatnya fleksibilitas produksi, kustomisasi massal, produktivitas, mutu produk, keterlibatan pelanggan dalam proses desain, semakin mendekatnya lokasi produksi ke pelanggan, dan model bisnis [1].

2.2.4 Passive Information Gathering

Ada sejumlah teknik dan proses yang tersedia ketika melakukan latihan Pengumpulan Informasi Pasif. Makalah teknis ini akan merinci teknik yang paling relevan dan berusaha untuk menguraikan baik proses pemikiran yang

diperlukan untuk mengidentifikasi informasi yang bocor, dan untuk mengevaluasi risiko keamanan relatif terkait dengan kebocoran.

Banyak informasi penting dapat dipanen secara pasif dan selanjutnya digunakan dalam serangan langsung atau untuk memperkuat serangan lain yang ditargetkan pada suatu organisasi. Bergantung pada sumbernya, informasi seperti tingkat perbaikan layanan saat ini, tata letak arsitektur jaringan internal dan detail akun dapat dengan mudah diperoleh. Sama pentingnya, dengan sedikit wawasan tentang di mana informasi ini diperoleh dan tingkat rincian informasi, suatu organisasi sering dapat memperbaiki kebocoran informasi ini secara sederhana dan cepat [8].

2.2.5 Shodan

Shodan adalah mesin pencari yang dirancang untuk mencari perangkat dan sistem komputer yang terhubung dengan *World Wide Web*. Situs ini diluncurkan pada tahun 2008 oleh programer komputer John Matherly, yang memiliki ide mencari peralatan-peralatan yang terhubung dengan Internet. Matherly langsung mengetahui fakta tentang perangkat dan sistem komputer di dunia terhubung ke Internet, termasuk lampu lalu lintas, kamera keamanan, sistem penghangat rumah, sistem kontrol taman bermain, SPBU, jaringan listrik, dan PLTN. Sebagian besar sistem ini memiliki keamanan dan perlindungan yang lemah. Kerusakan parah dapat terjadi jika situs ini jatuh ke tangan yang salah. Shodan kini memberikan 10 hasil pencarian untuk

pengguna tanpa akun, 50 untuk pengguna berakun, dan semuanya untuk pengguna yang membayar [9].

2.2.6 Python

Python merupakan bahasa pemrograman dinamis yang mendukung pemrograman berbasis objek. Python Diperoleh dari beberapa versi. Namun pada prinsipnya Python dapat diperoleh dan digunakan secara bebas, bahkan untuk keperluan komersial. Karena lisensi Python tidak bertentangan dengan resolusi *Open Source* maupun *General Public License* (GPL) [10].

2.2.7 CVE (Common Vulnerability and Exposure)

CVE (*Common Vulnerability and Exposure*) merupakan sistem yang menyediakan rujukan atau referensi terkait kerentanan dan paparan informasi keamanan yang bisa diakses and diketahui oleh publik.program CVE ini bisa dijalankan oleh siapapun dan akan diverifikasi oleh Mitre Corporation. CVE sekarang menjadi standar industri untuk pengidentifikasi kerentanan dan paparan. Entri CVE - juga disebut "CVEs," "ID CVE," dan "nomor CVE" oleh komunitas - memberikan poin referensi untuk pertukaran data sehingga produk dan layanan cybersecurity dapat berbicara satu sama lain. Entri CVE juga menyediakan garis dasar untuk mengevaluasi cakupan alat dan layanan sehingga pengguna dapat menentukan alat mana yang paling efektif dan

sesuai untuk kebutuhan organisasi mereka. Singkatnya, produk dan layanan yang kompatibel dengan CVE memberikan cakupan yang lebih baik, interoperabilitas yang lebih mudah, dan keamanan yang ditingkatkan [11].

2.2.8 Nmap

Nmap ("*Network Mapper*") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan [12].

2.2.9 Web Scraping

Web Scraping adalah proses pengambilan informasi dari website yang ada atau teknik penggalian informasi dari sebuah situs. Web Scraping menerapkan pengindeksan dengan cara menelusuri dokumen HTML dari

website yang akan diambil informasinya untuk di tag HTML agar bias mengapit informasi yang diambil untuk ditirukan pada aplikasi web scraping yang akan kita buat . Proses Web scraping dilakukan dengan cara mengambil sebuah dokumen semiterstruktur seperti HTML atau XHTML. Selanjutnya dokumen tersebut di analisis dan kemudian data yang dibutuhkan diambil dari halaman tersebut untuk digunakan bagi kepentingan lain. Web scraping bukanlah data mining karena data mining adalah proses pengambilan informasi untuk memahami pola semantik atau tren dari sejumlah data yang besar (big data). Aplikasi web scraping atau intelligent, automated, or autonomous agent fokus pada cara memperoleh data melalui pengambilan data [13].

2.2.10 Weak Password

Weak Password adalah suatu bentuk dari data otentikasi rahasia yang digunakan untuk mengontrol akses ke dalam suatu sumber informasi. Password akan dirahasiakan dari mereka yang tidak diijinkan untuk mengakses, dan mereka yang ingin mengetahui akses tersebut akan diuji apakah layak atau tidak untuk memperolehnya. Walaupun de mikian, password bukan berarti suatu bentuk kata-kata; tentu saja password yang bukan suatu kata yang mempunyai arti akan lebih sulit untuk ditebak. Sebagai tambahan, password sering digunakan untuk menggambarkan sesuatu yang lebih tepat disebut pass phrase. Password kadang-kadang digunakan juga

dalam suatu bentuk yang hanya berisi angka (*numeric*); salah satu contohnya adalah Personal Identification Number (PIN). Password umumnya cukup pendek sehingga mudah untuk diingat [14].

2.2.11 CVSS (Common Vulnerability Scoring System)

CVSS atau Common Vulnerability Scoring System adalah sebuah sistem skoring untuk menentukan skor dari celah kerentanan pada sebuah aplikasi atau sistem dengan beberapa metrik yaitu Base Metrics, Temporal Metrics, Enviromental Metrics. Dengan kententuan penilaian kerentanan sebagai berikut

Tabel 2. 2 Score CVSS

Rating	CVSS Score
None	0,0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

2.2.12 Attack Vector

Metrik ini mencerminkan konteks di mana eksploitasi kerentanan dimungkinkan. Nilai metrik ini (dan akibatnya skor Base) akan lebih besar semakin jauh (secara logis, dan fisik) penyerang dapat mengeksploitasi komponen rentan. Asumsinya adalah bahwa jumlah penyerang potensial untuk kerentanan yang dapat dieksploitasi dari seluruh Internet lebih besar

daripada jumlah penyerang potensial yang dapat mengeksploitasi kerentanan yang memerlukan akses fisik ke suatu perangkat, dan karenanya menjamin skor yang lebih besar. Daftar nilai yang mungkin disajikan pada tabel berikut.

Tabel 2. 3 Attack Vector

Nilai Metrik	Deskripsi	Nilai Numerik
Network (N)	Kerentanan yang dapat dieksploitasi dengan akses jaringan berarti komponen yang rentan terikat pada tumpukan jaringan dan jalur penyerang adalah melalui OSI layer 3 (lapisan jaringan). Kerentanan seperti itu sering disebut "dapat dieksploitasi dari jarak jauh" dan dapat dianggap sebagai serangan yang dapat dieksploitasi satu atau lebih jaringan melompat jauh (mis. Melintasi batas 3 layer dari router). Contoh serangan jaringan adalah penyerang yang menyebabkan penolakan layanan (DoS) dengan mengirimkan paket TCP yang dibuat khusus dari seluruh Internet publik.	0.85
Adjancent (A)	Kerentanan yang dapat dieksploitasi dengan akses jaringan yang berdekatan berarti komponen yang rentan terikat pada tumpukan jaringan, namun serangannya terbatas pada fisik bersama yang sama (misalnya Bluetooth, IEEE 802.11), atau jaringan logis (mis. Subnet IP lokal), dan tidak dapat dilakukan melintasi batas OSI layer 3 (mis. router). Contoh serangan yang berdekatan akan menjadi banjir ARP (IPv4) atau penemuan tetangga (IPv6) yang mengarah ke penolakan layanan di segmen LAN lokal.	0.62
Local (L)	Kerentanan yang dapat dieksploitasi dengan akses Lokal berarti bahwa komponen yang rentan tidak terikat pada tumpukan jaringan, dan jalur penyerang adalah melalui kemampuan baca / tulis / eksekusi. Dalam beberapa kasus, penyerang dapat login secara lokal untuk mengeksploitasi kerentanan, jika tidak, ia dapat mengandalkan	0.55

	Interaksi Pengguna untuk mengeksekusi file berbahaya.	
Physical (P)	Suatu kerentanan yang dapat dieksploitasi dengan akses Fisik mengharuskan penyerang menyentuh secara fisik atau memanipulasi komponen yang rentan. Interaksi fisik mungkin singkat (mis. Serangan pelayan jahat) atau gigih. Contoh serangan semacam itu adalah serangan boot dingin yang memungkinkan penyerang mengakses kunci enkripsi disk setelah mendapatkan akses fisik ke sistem, atau serangan periferal seperti serangan Akses Memori Langsung USB / Firewire.	0.2

2.2.13 Attack Complexity

Metrik ini menjelaskan kondisi di luar kendali penyerang yang harus ada untuk mengeksploitasi kerentanan. Seperti dijelaskan di bawah ini, kondisi tersebut mungkin memerlukan pengumpulan informasi lebih lanjut tentang target, keberadaan pengaturan konfigurasi sistem tertentu, atau pengecualian komputasi. Yang penting, penilaian metrik ini mengecualikan segala persyaratan untuk interaksi pengguna untuk mengeksploitasi kerentanan (kondisi tersebut ditangkap dalam metrik Interaksi Pengguna). Nilai metrik ini adalah terbesar untuk serangan paling kompleks. Daftar nilai yang mungkin disajikan pada tabel berikut.

Tabel 2. 4 Attack Complexity

Nilai Metrik	Deskripsi	Nilai Numerik
Low (L)	Kondisi akses khusus atau keadaan khusus tidak ada. Seorang penyerang dapat mengharapkan keberhasilan berulang terhadap komponen yang rentan.	0.77
High (H)	Serangan yang berhasil tergantung pada kondisi di luar kendali penyerang. Yaitu, serangan yang berhasil tidak dapat dicapai sesuka hati, tetapi mengharuskan penyerang untuk berinvestasi dalam sejumlah upaya yang terukur dalam persiapan atau eksekusi terhadap komponen yang rentan sebelum serangan yang berhasil dapat diharapkan. 2 Misalnya, serangan yang berhasil mungkin bergantung pada penyerang yang mengatasi salah satu dari kondisi berikut: - Penyerang harus melakukan pengintaian target-spesifik. Misalnya, pada pengaturan konfigurasi target, nomor urut, rahasia bersama, dll. - Penyerang harus menyiapkan lingkungan target untuk meningkatkan keandalan eksploitasi. Misalnya, eksploitasi berulang untuk memenangkan kondisi balapan, atau mengatasi teknik mitigasi eksploitasi tingkat lanjut. - Penyerang harus menyuntikkan dirinya ke jalur jaringan logis antara target dan sumber daya yang diminta oleh korban untuk membaca dan / atau memodifikasi komunikasi jaringan (mis. Pria dalam serangan tengah).	0.44

2.2.14 Privileges Required

Metrik ini menjelaskan tingkat hak istimewa yang harus dimiliki oleh penyerang sebelum berhasil mengeksploitasi kerentanan. Metrik ini paling bagus jika tidak ada hak istimewa yang diperlukan. Daftar nilai yang mungkin disajikan pada tabel berikut.

Tabel 2. 5 Privileges Required

Nilai Metrik	Deskripsi	Nilai Numerik
None (N)	Penyerang tidak sah sebelum serangan, dan oleh karena itu tidak memerlukan akses ke pengaturan atau file untuk melakukan serangan.	0.85
Low (L)	Penyerang diotorisasi dengan (yaitu membutuhkan) hak istimewa yang menyediakan kemampuan dasar pengguna yang biasanya hanya dapat memengaruhi pengaturan dan file yang dimiliki oleh pengguna. Atau, penyerang dengan hak istimewa Rendah mungkin memiliki kemampuan untuk menyebabkan dampak hanya pada sumber daya yang tidak sensitif.	0.62(0.68 jika Scope berubah)
High (H)	Penyerang diberi wewenang dengan (yaitu membutuhkan) hak istimewa yang memberikan kontrol (mis. Administratif) yang signifikan atas komponen rentan yang dapat memengaruhi pengaturan dan file di seluruh komponen.	0.27(0.50 jika Scope berubah)

2.2.15 User Interaction

Metrik ini menangkap persyaratan bagi pengguna, selain penyerang, untuk berpartisipasi dalam kompromi yang berhasil dari komponen yang rentan. Metrik ini menentukan apakah kerentanan dapat dieksploitasi semata-mata atas kehendak penyerang, atau apakah pengguna yang terpisah (atau proses yang diprakarsai pengguna) harus berpartisipasi dengan cara tertentu. Nilai metrik ini paling baik bila tidak ada interaksi pengguna yang diperlukan. Daftar nilai yang mungkin disajikan pada tabel berikut.

Tabel 2. 6 User Interaction

Nilai Metrik	Deskripsi	Nilai Numerik
None (N)	Sistem rentan dapat dieksploitasi tanpa interaksi dari pengguna mana pun.	0.85
Required (R)	Eksploitasi yang berhasil dari kerentanan ini mengharuskan pengguna untuk mengambil tindakan sebelum kerentanan tersebut dapat dieksploitasi. Misalnya, eksploit yang berhasil hanya dimungkinkan selama instalasi aplikasi oleh administrator sistem.	0.62

2.2.16 Scope

Properti penting yang ditangkap oleh CVSS v3.0 adalah kemampuan untuk kerentanan dalam satu komponen perangkat lunak untuk memengaruhi sumber daya di luar kemampuan atau keistimewaannya. Konsekuensi ini diwakili oleh Lingkup Otorisasi metrik, atau hanya Lingkup. Secara formal, Lingkup mengacu pada kumpulan hak istimewa yang ditentukan oleh otoritas komputasi (mis. Aplikasi, sistem operasi, atau lingkungan kotak pasir) ketika memberikan akses ke sumber daya komputasi (mis. File, CPU, memori, dll). Hak istimewa ini diberikan berdasarkan beberapa metode identifikasi dan otorisasi. Dalam beberapa kasus, otorisasi mungkin sederhana atau dikontrol secara longgar berdasarkan aturan atau standar yang telah ditentukan. Misalnya, dalam kasus lalu lintas Ethernet yang dikirim ke switch jaringan, switch menerima lalu lintas yang tiba di port-nya dan merupakan otoritas yang mengontrol aliran lalu lintas ke port switch lainnya. Ketika kerentanan komponen perangkat lunak yang diatur oleh satu ruang lingkup otorisasi dapat

memengaruhi sumber daya yang diatur oleh ruang lingkup otorisasi lain, perubahan Lingkup telah terjadi. Secara intuitif, orang mungkin berpikir tentang perubahan ruang lingkup sebagai keluar dari kotak pasir, dan sebuah contoh akan menjadi kerentanan dalam mesin virtual yang memungkinkan penyerang untuk menghapus file pada OS host (mungkin bahkan VM sendiri). Dalam contoh ini, ada dua otoritas otorisasi yang terpisah: satu yang mendefinisikan dan menegakkan hak istimewa untuk mesin virtual dan penggunanya, dan satu yang mendefinisikan dan menegakkan hak istimewa untuk sistem host di mana mesin virtual berjalan. Perubahan cakupan tidak akan terjadi, misalnya, dengan kerentanan di Microsoft Word yang memungkinkan penyerang kompromi semua file sistem OS host, karena otoritas yang sama menegakkan hak istimewa dari instance pengguna Word, dan file sistem host. Skor Base lebih besar ketika perubahan lingkup telah terjadi. Daftar nilai yang mungkin disajikan pada tabel berikut.

Tabel 2. 7 Scope

Nilai Metrik	Deskripsi	Nilai Numerik
Unchanged (U)	Kerentanan yang dieksploitasi hanya dapat memengaruhi sumber daya yang dikelola oleh otoritas yang sama. Dalam hal ini komponen yang rentan dan komponen yang terkena dampak adalah sama.	Null
Changed (C)	Kerentanan yang dieksploitasi dapat mempengaruhi sumber daya di luar hak otorisasi yang dimaksudkan oleh komponen rentan. Dalam hal ini komponen yang rentan dan komponen yang terkena dampak berbeda.	1.08

2.2.17 Confidentiality

Metrik ini mengukur dampak terhadap kerahasiaan sumber daya informasi yang dikelola oleh komponen perangkat lunak karena kerentanan yang berhasil dieksploitasi. Kerahasiaan mengacu pada membatasi akses informasi dan pengungkapan hanya kepada pengguna yang berwenang, serta mencegah akses oleh, atau pengungkapan kepada, pengguna yang tidak sah. Daftar nilai yang mungkin disajikan pada tabel dibawah. Nilai metrik ini meningkat dengan tingkat kehilangan komponen yang terkena dampak.

Tabel 2. 8 Confidentiality

Nilai Metrik	Deskripsi	Nilai Numerik
High (H)	Ada total kehilangan kerahasiaan, yang mengakibatkan semua sumber daya di dalam komponen yang terkena dampak diungkapkan kepada penyerang. Atau, akses ke hanya beberapa informasi terbatas diperoleh, tetapi informasi yang diungkapkan menyajikan dampak langsung dan serius. Misalnya, seorang penyerang mencuri kata sandi administrator, atau kunci enkripsi pribadi dari server web.	0.56
Low (L)	Ada beberapa kehilangan kerahasiaan. Akses ke beberapa informasi terbatas diperoleh, tetapi penyerang tidak memiliki kendali atas informasi apa yang diperoleh, atau jumlah atau jenis kerugian dibatasi. Pengungkapan informasi tidak menyebabkan kerugian langsung dan serius pada komponen yang terkena dampak.	0.22
None (N)	Tidak ada kehilangan kerahasiaan dalam komponen yang terkena dampak.	0

2.2.18 Integrity

Metrik ini mengukur dampak integritas integritas yang berhasil dieksploitasi. Integritas mengacu pada kepercayaan dan kebenaran informasi. Daftar nilai yang mungkin disajikan pada tabel dibawah. Nilai metrik ini meningkat dengan konsekuensi pada komponen yang terkena dampak.

Tabel 2. 9 Integrity

Nilai Metrik	Deskripsi	Nilai Numerik
High (H)	Ada total kehilangan integritas, atau benar-benar kehilangan perlindungan. Sebagai contoh, penyerang dapat memodifikasi semua / semua file yang dilindungi oleh komponen yang terkena dampak. Atau, hanya beberapa file yang dapat dimodifikasi, tetapi modifikasi berbahaya akan menghadirkan konsekuensi langsung dan serius terhadap komponen yang terpengaruh.	0.56
Low (L)	Modifikasi data dimungkinkan, tetapi penyerang tidak memiliki kendali atas konsekuensi modifikasi, atau jumlah modifikasi terkendala. Modifikasi data tidak memiliki dampak langsung dan serius pada komponen yang terkena dampak.	0.22
None (N)	Tidak ada kehilangan integritas dalam komponen yang terkena dampak.	0

2.2.19 Availability

Metrik ini mengukur dampak terhadap ketersediaan komponen yang terkena dampak yang dihasilkan dari kerentanan yang berhasil dieksploitasi. Meskipun metrik dampak Kerahasiaan dan Integritas berlaku untuk hilangnya kerahasiaan atau integritas data (misalnya, informasi, file) yang digunakan oleh komponen yang terkena dampak, metrik ini mengacu pada hilangnya

ketersediaan komponen yang terkena dampak itu sendiri, seperti layanan jaringan (mis. web, database, email). Karena ketersediaan mengacu pada aksesibilitas sumber daya informasi, serangan yang menggunakan bandwidth jaringan, siklus prosesor, atau ruang disk semuanya memengaruhi ketersediaan komponen yang terpengaruh. Daftar nilai yang mungkin disajikan pada tabel dibawah. Nilai metrik ini meningkat dengan konsekuensi pada komponen yang terkena dampak.

Tabel 2. 10 Availabilty

Nilai Metrik	Deskripsi	Nilai Numerik
High (H)	Ada total hilangnya ketersediaan, yang menyebabkan penyerang dapat sepenuhnya menolak akses ke sumber daya dalam komponen yang terkena dampak; kerugian ini bisa berkelanjutan (sementara penyerang terus mengirimkan serangan) atau gigih (kondisi tetap ada bahkan setelah serangan selesai). Atau, penyerang memiliki kemampuan untuk menolak beberapa ketersediaan, tetapi hilangnya ketersediaan menghadirkan konsekuensi langsung yang serius terhadap komponen yang terkena dampak (misalnya, penyerang tidak dapat mengganggu koneksi yang ada, tetapi dapat mencegah koneksi baru, penyerang berulang kali dapat mengeksploitasi kerentanan. bahwa, dalam setiap contoh serangan yang berhasil, kebocoran memori hanya sedikit, tetapi setelah eksploitasi berulang menyebabkan layanan menjadi benar-benar tidak tersedia).	0.56
Low (L)	Ada penurunan kinerja atau gangguan dalam ketersediaan sumber daya. Bahkan jika eksploitasi berulang terhadap kerentanan dimungkinkan, penyerang tidak memiliki kemampuan untuk sepenuhnya menolak layanan bagi pengguna yang sah. Sumber daya dalam komponen yang terkena dampak sebagian tersedia sepanjang waktu, atau hanya sepenuhnya tersedia sebagian saja, tetapi secara	0.22

	keseluruhan tidak ada konsekuensi langsung dan serius terhadap komponen yang terkena dampak.	
None (N)	Tidak ada dampak terhadap ketersediaan dalam komponen yang terpengaruh.	0