Pengukuran Tingkat Kerentanan (Severity)

Kerentanan yang telah diidentifikasi perlu dinilai dan dikelompokkan tingkat kerentanannya (severity). Kerentanan ditangani secara priotitas berdasarkan tingkat kerentanannya.

Referensi:

https://www.first.org/

- Common Vulnerability Scoring System (CVSS)
- Metrik Eksploitasi (Exploitation Metrics)
- Metrik Dampak (Impact Metrics)
- Metrik Ancaman (Threat Metrics)
- Metrik Lingkungan (Environmental Metric)

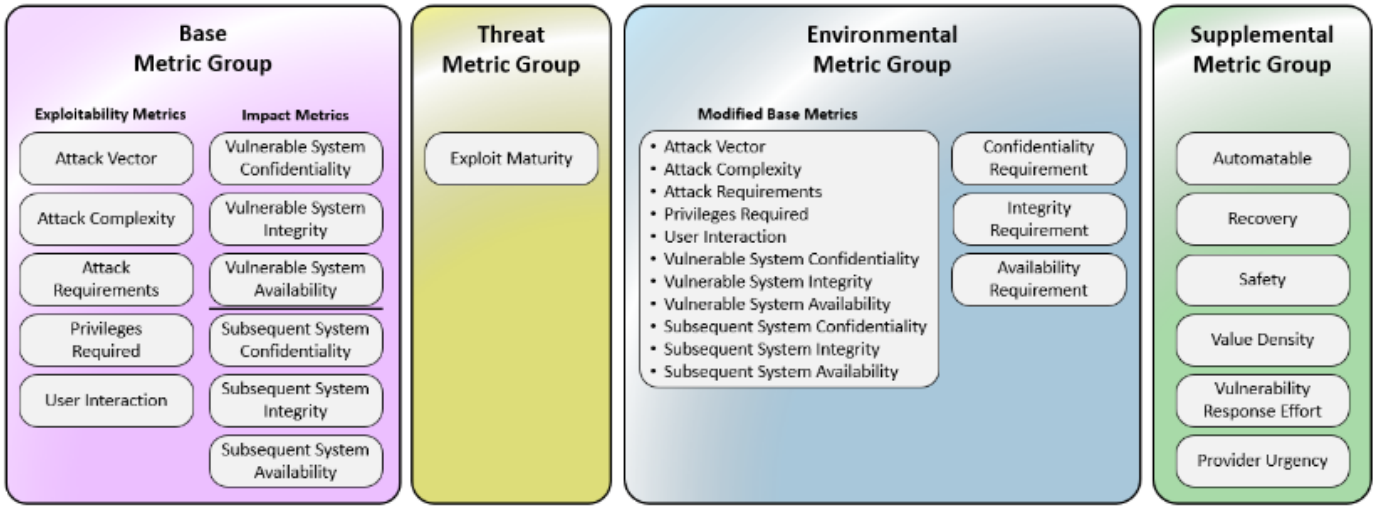
Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) adalah standar industri yang bebas dan terbuka untuk menilai tingkat keparahan (*severity*) kerentanan keamanan sistem. CVSS menetapkan skor severity dari sebuah kerentanan, memungkinkan responden untuk memprioritaskan object mana yang harus diperbaiki terlebih dahulu sesuai dengan tingkat resikonya. CVSS dikembangkan dan dikelola oleh FIRST.Org, organisasi yang bertujuan membantu Tim Tanggap Insiden Siber (*Computer Security Incident Response Team* /CSIRT).

CVSS terdiri dari 4 (empat) metric grup berikut:

- Base score (CVSS-B)
  - Base Score (CVSS-B)dirancang untuk mengukur tingkat keparahan (*severity*) kerentanan, dan tidak digunakan untuk mengukur risiko karena hanya mewakili karakteristik intristik dari kerentanan dan tidak bergantung pada faktor apapun yang terkait dengan ancaman / lingkungan sistem.
- Threat Metric (CVSS-BT)
  - Threat metric mengukur tingkat keparahan (*severity*) berdasarkan beberapa faktor, diantaranya ketersediaan pembuktian (*proof of concept*), atau eksploitasi aktif.
- Environmental Metric (CVSS-BE)
  - Environmental metric mengukur tingkat keparahan (*severity*) yang dihasilkan pada lingkungan komputasi tertentu, diantara bergantung pada faktor mitigasi dan kritikalitas sistem.
- Suplemental Metric (CVSS-BTE)
  - Supplemental metric menggambarkan dan mengukur atribut ekstrinsik tambahan dari kerentanan, dan untuk menambahkan konteks.

Keempat metric tersebut dapat digambarkan sebagai berikut.



Gambar 1. CVSS Metrics

CVSS adalah representasi numerik dari tingkat keparahan kerentanan yang juga dikenal sebagai " **Skor dasar (base score)** " dengan nilai skor dasar bervariasi dari 0 sampai 10. CVSS base score harus dilengkapi dengan analisis lingkungan (environmental metric) dan atribut yang dapat berubah dari waktu ke waktu (threat metric).

Versi terakhir yang dirilis adalah CVSS v.4.0.

Tingkat keparahan (severity) kerentanan dikelompokkan menjadi 4 (empat) sebagaimana ditunjukkan pada tabel berikut.

Tabel 1. *CVSS V 3.x dan 4.0 Severity Rating*

Kategori Kerentanan	Nilai CVSS
Kritikal (Critical)	9.0 s.d 10.0
Tinggi (High)	7.0 s.d. 8.9
Sedang (Medium)	4.0 s.d 6.9
Rendah (Low)	0.1 s.d. 3.9
None*	0.0

Metrik Eksploitasi (Exploitation Metrics)

Vektor Serangan (Attack Vector / AV)

Vektor serangan menggambarkan konteks kemungkinan eksploitasi serangan. Asumsinya, serangan melalui jaringan kemungkinannya lebih besar dari pada serangan yang memerlukan akses fisik terhadap perangkat sehingga juga akan berdampak lebih besar. Distribusi metrik vektor serangan ditunjukkan pada Tabel 2 berikut.

Tabel 1. Matrik Vektor Serangan

Nilai	Deskripsi
Network (N)	Sistem yang rentan terhubung dengan jaringan, sehingga dapat dieksploitasi dari jarak jauh
Adjacent (A)	Sistem yang rentan dibatasi pada protokol tertentu, sehingga serangan harus dilakukan pada jaringan yang sama (misal bluetooth, NFC, wifi), jaringan logic lainnya (satu subnet) atau dari dalam domain yang terbatas.
Local (L)	Sistem yang rentan terhubung pada jaringan lokal, sehingga serangan harus dilakukan pada sistem target secara lokal (keyboard, konsol) atau atau melalui emulasi terminal (SSH), atau menggunakan teknis social engineering untuk mengelabui pengguna agar membuka dokumen yang telah disisipi malware.
Physical (P)	Serangan mengharuskan adanya akses secara fisik terhadap sistem yang rentan, misalnya serangan harus dilakukan menggunakan USB.

Kompleksitas Serangan (Attack Complexity / AC)

Matrik menggambarkan tindakan yang harus dilakukan penyerang agar eksploitasi berhasil dilakukan.

Tabel 2. Kompleksitas Serangan

Nilai	Deskripsi

Low (L)	Penyerang tidak perlu melakukan tindakan tertentu untuk melakukan eksploitasi terhadap sistem yang rentan. Serangan dapat dilakukan secara berulang.
High (H)	Serangan bergantung pada keamanan pada pertahanan sistem yang rentan. Penyerang harus melakukan metode tambahan untuk melewati keamanan yang ada. Penyerang harus memiliki informasi kredensial sistem.

Persyaratan Serangan (Attack Requirement / AT)

Matrik menggambarkan persyaratan pengembangan dan eksekusi atau variabel yang diperlukan untuk menjalankan serangan.

Tabel 3. Persyaratan Serangan

Nilai	Deskripsi
None (N)	Keberhasilan serangan tidak bergantung pada kondisi pengembangan dan eksekusi pada sistem yang rentan. Eksploitasi terhadap kerentanan dapat dilakukan pada kondisi apapun.
Present (PR)	Keberhasilan serangan bergantung pada kondisi implementasi dan eksekusi tertentu dari sistem yang rentan untuk menjalankan serangan.

Hak Akses yang Diperlukan (Privileges Required/ PR)

Privileges Required menggambarkan tingkat kewenangan yang harus dimiliki oleh penyerang sebelum mengeksploitasi kerentanan, misalnya harus memperoleh kredensial sistem sebelum melakukan serangan. Nilai tertinggi adalah ketika penyerang tidak memerlukan hak akses tertentu untuk mengeksploitasi sistem.

Tabel 4. Matrik Kebutuhan Hak Akses

Nilai	Deskripsi
None (N)	Penyerang tidak diotentikasi sebelum melakukan serangan, sehingga tidak memerlukan akses tertentu terhadap konfigurasi / file pada sistem yang rentan.
Low (L)	Penyerang memerlukan hak akses dengan kemampuan minimal yang dimiliki oleh user biasa yang dapat mengakses file tidak sensitif.
High (H)	Penyerang memerlukan hak akses yang memiliki kontrol signifikan (misal admin) yang memungkinkan akses ke seluruh konfigurasi dan file pada sistem.

Interaksi Pengguna (User Interaction / UI)

Matrik menggambarkan persyaratan interakasi pengguna selain penyerang untuk berhasil melakukan serangan ke sistem yang rentan.

Tabel 5. Interaksi Pengguna

Nilai	Deskripsi
None (N)	Sistem yang rentan dapat dieksploitasi tanpa interaksi pengguna, selain penyerang. Misalnya penyerang dari jarak jauh dapat mengirimkan eksploit pada sistem dan mengekseskui kode untuk meningkatkan hak akses.
Passive (P)	Serangan memerlukan interaksi terbatas dari pengguna untuk melakukan eksploitasi.
Active (A)	Serangan memerlukan interaksi pengguna tertentu untuk melakukan eksploitasi, misal pengguna harus menyetujui peringatan terhadap tindakan tertentu.

Metrik Dampak (Impact Metrics)

Metrik menggambarkan dampak kerentanan yang berhasil dieksploitasi. Namun demikian, analis harus dapat menentukan batasan terhadap dampak akhir yang dapat dicapai oleh penyerang. Ketika mengidentifikasi nilai metrik dampak, perlu diperhitungkan dampak terhadap sistem yang rentan *(vulnerable system impact)* dan dampak diluar sistem yang rentan (*subsequent system impact*) yang ditentukan oleh dua hal yaitu dampak sistem rentan dan dampak selanjutnya yang muncul. Jika kerentanan tidak mempunyai dampak yang terjadi diluar sistem yang rentan, maka *subsequent metric* akan memiliki nilai NONE (N).

Metrik dampak terdiri atas beberapa kategori berikut.

Kerahasiaan / Confidentiality (VC/SC)

Metrik mengukur dampak kerahasiaan terhadap informasi karena keberhasilan eksploitasi kerentanan. Nilai dampak terhadap kerahasiaan ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Kerahasiaan

Nilai Metrik	Dampak pada *Vulnerable System* (VC)	Dampak pada *Subsequent System* (SC)
High (H)	Semua informasi didalam sistem dapat diakses penyerang, atau akses terhadap informasi yang terbatas namun berdampak serius, misalnya kredensial sistem.	Semua informasi didalam *subsequent system* dapat diakses penyerang, atau akses terhadap informasi yang terbatas namun berdampak serius, misalnya kredensial sistem.
Low (L)	Penyerang dapat mengakses terhadap informasi terbatas, namun tidak memiliki kendali atas informasi tersebut sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap sistem.	Penyerang dapat mengakses terhadap informasi terbatas, namun tidak memiliki kendali atas informasi tersebut sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap *subsequent system.*
None (N)	Tidak terdapat informasi yang terungkap / hilang	Tidak terdapat informasi yang terungkap / hilang pada *subsequent system.*

Integritas / Integrity (VI/SI)

Metrik mengukur dampak integritas terhadap informasi karena keberhasilan eksploitasi kerentanan. Integritas sistem terdampak ketika penyerang dapat melakukan modifikasi terhadap data / informasi di dalam sistem. Nilai dampak terhadap integritas sistem ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Integritas

Nilai Metrik	**Dampak pada *Vulnerable System* (VC)**	**Dampak pada *Subsequent System* (SC)**
High (H)	Hilangnya perlindungan integritas sistem. Penyerang dapat memodifikasi seluruh file yang dilindungi didalam sistem, atau hanya dapat melakukan modifikasi pada file tertentu, namun modifikasi yang berbahaya dapat berdampak serius pada sistem.	Hilangnya perlindungan integritas sistem. Penyerang dapat memodifikasi seluruh file yang dilindungi didalam sistem, atau hanya dapat melakukan modifikasi pada file tertentu, namun modifikasi yang berbahaya dapat berdampak serius pada *subsequent system.*
Low (L)	Penyerang dapat melakukan modifikasi, namun tidak memiliki kendali atas akibat dari modifikasi tersebut atau jumlah modifikasi dibatasi sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap sistem.	Penyerang dapat melakukan modifikasi, namun tidak memiliki kendali atas akibat dari modifikasi tersebut atau jumlah modifikasi dibatasi sehingga tidak berdampak serius atau tidak menimbulkan kerugian secara langsung terhadap *subsequent system.*
None (N)	Tidak terdapat integritas sistem yang hilang.	Tidak terdapat integritas *subsequent system* yang hilang.

Ketersediaan / Availability (VA/SA)

Metrik mengukur dampak ketersediaan terhadap informasi karena keberhasilan eksploitasi kerentanan. Ketersediaan sistem terdampak ketika penyerang dapat mengganggu ketersediaan akses / membuat sistem tidak dapat diakses oleh pengguna. Nilai dampak terhadap ketersediaan sistem ditunjukkan pada Tabel berikut.

Tabel. Metrik Dampak Ketersediaan

Nilai Metrik	**Dampak pada *Vulnerable System* (VC)**	**Dampak pada *Subsequent System* (SC)**
High (H)	Hilangnya perlindungan ketersediaan sistem. Penyerang dapat menolak seluruh akses kedalam sistem, baik bersifat sementara maupun terus menerus (persistent). Atau penyerang dapat menolak beberapa akses, namun berdampak serius terhadap ketersediaan sistem.	Hilangnya perlindungan ketersediaan layanan *subsequent system*. Penyerang dapat menolak seluruh akses kedalam *subsequent system*, baik bersifat sementara maupun terus menerus (persistent). Atau penyerang dapat menolak beberapa akses, namun berdampak serius terhadap ketersediaan *subsequent system*.

Low (L)	Terdapat gangguan terhadap ketersediaan sistem, namun tidak dapat sepenuhnya menolak layanan kepada pengguna yang sah.	Terdapat gangguan terhadap ketersediaan layanan *subsequent system*, namun tidak dapat sepenuhnya menolak layanan kepada pengguna yang sah.
None (N)	Tidak terdapat gangguan terhadap ketersediaan sistem .	Tidak terdapat gangguan terhadap ketersediaan *subsequent system*

Metrik Ancaman (Threat Metrics)

Metrik ancaman (*threat metrics*) mengukur kondisi teknik eksploitasi / ketersediaan kode untuk mengeksploitasi kerentanan.

Metrik ancaman diukur berdasarkan kematangan eksploit / *exploit maturity* (E)

Kematangan Eksploit / Exploit Maturity (E)

Metrik mengukur kemungkinan serangan terhadap kerentanan berdasaekan kondisi eksploit saat ini, ketersediaan kode eksploit, atau aktif "in the wild". Ketersediaan eksploit untuk publik atau kemudahan instruksi penggunaan meningkatkan kemungkinan serangan, termasuk bagi penyerang yang tidak terampil. Ketersediaan eksploit atau instruksi juga dapat berkembang bergantung pada tingkat keberhasilan pembuktian eksploitasi kerentanan (*proof of concept*). Pada beberapa kasus, eksploitasi dapat dijalankan otomatis menggunakan tools serangan tertentu. Informasi terkait teknik eksploitasi / instruksi teknis lainnya selanjutnya akan disebut dengan intelijen ancaman (*threat intelligence*). Pada operasional organisasi disarankan menggunakan banyak sumber threat intelligence.

Daftar kemungkinan nilai kematangan eksploit ditunjukkan pada Tabel berikut.

Tabel. Kematangan Eksploit (Exploit Maturity)

Nilai Metrik	Deskripsi
Not Defined (X)	*Threat intelligence* yang handal tidak tersedia untuk menentukan karakteristik kematangan eksploitasi. Not Defined (X) merupakan nilai default.
Attacked (A)	Tersedia *threat intelligence:* melaporkan serangan terhadap percobaan / keberhasilan eksploitasi, atau terdapat tools untuk memudahkan eksploitasi kerentanan.
Proof of Concept (P)	Terdapat *threat intelligence*: pembuktian eksploitasi (*proof of concept*) dapat diakses publik, tidak terdapat laporan percobaan eksploitasi kerentanan, tidak terdapat pengetahuan /tools untuk memudahkan eksploitasi yang dapat diakses publik.

Unreported (U)	Terdapat *threat intelligence:* Tidak terdapat pembuktian eksploitasi (*proof of concept*) dapat diakses publik, tidak terdapat laporan percobaan eksploitasi kerentanan, tidak terdapat pengetahuan /tools untuk memudahkan eksploitasi yang dapat diakses publik.

Metrik Lingkungan (Environmental Metric)

Metrik memungkinkan pengguna mengalisis nilai berdasarkan tingkat kritikalitas dari aset TI yang terdampak terhadap aspek kerahasiaan, integritas, dan ketersediaan, Metrik merupakan modifikasi dari *base metric*.

Persyaratan Keamanan Kerahasian (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*)

Setiap aspek memiliki 3 (tiga) kemungkinan nilai: Low, Medium, High, atau nilai defaultnya Not Defined (X). Dampak penuh terhadap nilai metrik lingkungan ditentukan oleh metrik dasar yang telah disesuaikan dengan kebutuhan. Nilai default X, setara dengan nilai metrik High (H). Nilai metrik digambarkan pada Tabel berikut.

Tabel. Metrik Persyaratan Keamanan (*Security Requirements*)

Nilai Metrik	Deskripsi
Not Defined (X)	Nilai default. Nilai ini menggambarkan tidak tercukupinya informasi untuk memililih salah satu nilai yang lain.
High (H)	Hilangnya [kerahasiaan|integritas|ketersediaan] memiliki dampak buruk paling besar terhadap organisasi atau individu dalam organisasi.
Medium (M)	Hilangnya [kerahasiaan|integritas|ketersediaan] memiliki dampak serius terhadap organisasi atau individu dalam organisasi.
Low (L)	Hilangnya [kerahasiaan|integritas|ketersediaan] memiliki dampak yang terbatas terhadap organisasi atau individu dalam organisasi.