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.

Revision #5
Created 5 September 2024 02:38:52 by Tim Persandian
Updated 11 September 2024 04:18:27 by Tim Persandian