**TUGAS**

**KEAMANAN JARINGAN KOMPUTER**



DISUSUN OLEH:

NAMA : ARIFQI BAHARA

NIM : 09011281419049

DOSEN PEMBIMBING : Dr. Deris Stiawan, M.T.

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2018**

**ANALISA CVE**

Dokumentasi MITER Corporation mendefinisikan pengidentifikasi CVE (juga disebut "nama CVE", "nomor CVE", "CVE-IDs", dan "CVEs") sebagai pengenal umum yang unik untuk kerentanan keamanan informasi yang diketahui publik dalam paket perangkat lunak yang dirilis di depan umum. Secara historis, pengidentifikasi CVE memiliki status "kandidat" ("CVE-"), dan kini pengidentifikasi sekarang ditugaskan sebagai CVE. Penugasan entri CVE CVE (mis., CVE mungkin tidak benar ditugaskan untuk masalah yang bukan merupakan kerentanan keamanan, atau yang menduplikat entri yang ada).

CVE ditugaskan oleh Otoritas Nomor CVE (CVE Numbering Authority / CNA). Ada tiga jenis utama penugasan CVE nomor:

1. The Mitre Corporation berfungsi sebagai Editor dan Primary CNA.
2. Berbagai CNA menetapkan nomor CVE untuk produk mereka sendiri (misalnya Microsoft, Oracle, HP, Red Hat, dll).
3. Koordinator pihak ketiga seperti CERT Coordination Center dapat menetapkan nomor CVE untuk produk yang tidak tercakup oleh CNA lainnya.

Saat menyelidiki kerentanan atau potensi kerentanan, ini membantu memperoleh nomor CVE sejak dini. Nomor CVE mungkin muncul di database MITE atau NVD CVE untuk beberapa waktu (hari, minggu, bulan atau berpotensi bertahun-tahun) karena masalah yang diembargo (nomor CVE telah ditetapkan namun masalahnya belum dipublikasikan), atau dalam kasus dimana entri tersebut tidak diteliti dan ditulis oleh MITER karena masalah sumber daya. Manfaat pencantuman CVE awal adalah bahwa semua nomor CVE dapat merujuk ke nomor CVE. Informasi tentang pengidentifikasi CVE untuk masalah dengan proyek open source tersedia dari Red Hat.

CVE adalah untuk perangkat lunak yang telah dipublikasikan publik; Ini bisa mencakup beta dan versi pra-rilis lainnya jika sudah digunakan. Perangkat lunak komersial disertakan dalam kategori "publik yang dirilis", namun perangkat lunak yang dibuat khusus yang tidak didistribusikan umumnya tidak diberi CVE. Selain itu layanan (mis., Penyedia email berbasis web) tidak memberikan CVE untuk kerentanan yang ditemukan dalam layanan ini (misalnya kerentanan XSS) kecuali jika ada masalah pada produk perangkat lunak yang mendasari yang didistribusikan secara publik.

**Deskripsi :**
Calon ini telah dipesan oleh organisasi atau individu yang akan menggunakannya saat mengumumkan masalah keamanan baru. Saat kandidat telah dipublikasikan, rincian untuk calon ini akan diberikan. Ini berarti bahwa nomor entri telah dipesan oleh Mitre untuk sebuah masalah atau CNA telah mencadangkan nomornya. Jadi, dalam kasus di mana CNA meminta satu blok nomor CVE terlebih dahulu (misalnya, Red Hat saat ini meminta CVE di blok 500), nomor CVE akan ditandai sebagai dicadangkan walaupun CVE itu sendiri mungkin tidak ditugaskan oleh CNA untuk beberapa waktu. Sampai CVE ditugaskan DAN Mitre dibuat menyadarinya (misalnya, embargo berlalu dan masalahnya dipublikasikan), DAN Mitre telah meneliti masalah ini dan menuliskan deskripsi tentangnya, dan entri pun akan muncul sebagai hole atau lubang. Informasi inilah yang akan digunakan sebagai “penyerang” untuk “how to attack” untuk si target.

**Contoh tampilan CVE :**

