Tugas
Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Yonatan Riyadhi

NIM : 09011181419009

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

Melanjutkan dari tugas sebelumnya, disini akan membahas tentang beberapa CVE dari operating system yang saya gunakan yaitu windows NT4. Adapun hasil CVE tersebut diambil dari rating yang tertinggi yakni;

1. CVE-2000-0222

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

Instalasi untuk Windows 2000 tidak mengaktifkan kata sandi Administrator sampai sistem melakukan reboot, yang memungkinkan penyerang jarak jauh terhubung ke ADMIN $ share tanpa kata sandi sampai reboot terjadi.

2. CVE-2000-1218

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

Pada CVE tipe ini, Konfigurasi default untuk resolver nama domain untuk Microsoft Windows 98, NT 4.0, 2000, dan XP menetapkan parameter QueryIpMatching ke 0, yang menyebabkan Windows menerima update DNS dari host yang tidak di-query, yang memungkinkan penyerang jarak jauh meracuni DNS cache.

3. CVE-2000-1227

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

Host Windows NT 4.0 dan Windows 2000 memungkinkan penyerang jarak jauh menyebabkan penolakan layanan (koneksi yang tidak tersedia) dengan mengirimkan beberapa permintaan SMBnegprot, SMB namun tidak membaca respons yang dikirim kembali.

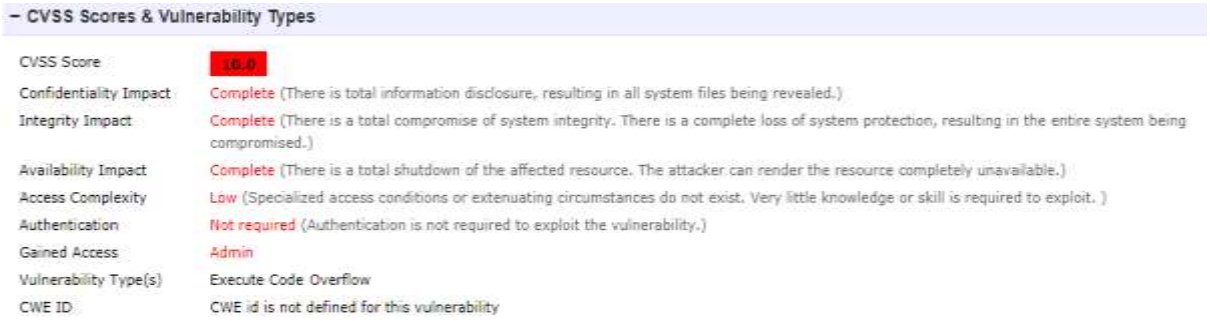
4. CVE-2002-1141

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

Kesalahan validasi masukan di perpustakaan RPC Sun Microsystems Layanan untuk Unix 3.0 Interix SD, seperti yang diterapkan pada Microsoft Windows NT4, 2000, dan XP, memungkinkan penyerang jarak jauh menyebabkan penolakan layanan melalui paket klien RPC yang terfragmentasi, alias "Denial of service dengan mengirimkan permintaan RPC yang tidak valid. "

5. CVE-2004-0574



– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	Admin
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability

Komponen Network News Transfer Protocol (NNTP) dari Microsoft Windows NT Server 4.0, Windows 2000 Server, Windows Server 2003, Exchange 2000 Server, dan Exchange Server 2003 memungkinkan penyerang remote untuk mengeksekusi kode sewenang-wenang melalui pola XPAT, mungkin terkait dengan validasi panjang yang tidak tepat dan sebuah "buffer yang tidak dicentang," yang menyebabkan buffer over-by-one dan heap berbasis overflow.

ANALISA

Dari kelima jenis CVE diatas, dari vulneranility yang dijelaskan bahwa kebanyakan dari hole tersebut mengarah pada serangan buffer overflow. Dari serangan ini pun digunakan pada remote access dari sistem operasi tersebut. Pada dasarnya juga serangan serangan yang terjadi pada sistem operasi ini adalah kesalahan dari validasi ataupun dari program yang berlebihan. Di Buffer overflow ini juga program yang berlebihan juga dapat menyebabkan proses terjadinya serangan buffer overflow itu sendiri dan hal itulah yang dapat menjadi vulnerability dari sistem operasi ini.