Tugas

Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Yonatan Riyadhi

NIM : 09011181419009

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Windows NT4

Microsoft Windows NT 4.0 merupakan sebuah versi lanjutan dari sistem operasi sebelumnya berbasis kernel NT diluncurkan oleh Microsoft Corporation pada 29 Juli 1996. Sistem operasi ini dapat mendukung beberapa platform perangkat keras, mulai dari Intel IA-32 (x86), PowerPC dari IBM, MIPS, dan DEC Alpha dari Digital Equipment Corporation. Sama seperti halnya pendahulunya (Windows NT 3.51), Windows NT 4.0 ini merupakan sistem operasi yang murni 32-bit, yang mendukung beberapa aplikasi DOS, OS/2 modus karakter, Windows 16-bit, Windows 32-bit, serta aplikasi POSIX. Karena merupakan sistem operasi 32-bit, Windows NT 4.0 mendukung hingga 4 gibibyte memori fisik.

Windows NT 4.0 menawarkan stabilitas terhadap Windows 95, Windows NT 4.0 kurang fleksibel jika dilihat dari perspektif pengguna desktop. Banyak dari kestabilan sistem operasi ini diperoleh dari proses virtualisasi terhadap perangkat keras dan membuat aplikasi perangkat lunak mengakses Application Programming Interface (API) milik Windows NT dibandingkan dengan mengakses perangkat keras secara langsung seperti dalam Windows 95 dan juga MS-DOS. Kekurangan dari metode ini adalah banyaknya pekerjaan yang harus dilakukan oleh komputer, sehingga aplikasi yang menggunakan perangkat keras secara intensif (seperti halnya game komputer) akan berjalan jauh lebih lambat dibandingkan dengan Windows 95 atau MS-DOS. Meskipun banyak program yang ditulis dengan Win32 API dapat berjalan di atas Windows 95 dan Windows NT, banyak aplikasi game tiga dimensi tidak dapat berjalan di atasnya, mengingat dukungan Windows NT 4.0 terhadap DirectXmasih terbatas.

Meskipun memiliki antarmuka grafis yang sama dengan Windows 95, Windows NT 4.0 tidaklah semudah dengan Windows 95, khususnya ketika melakukan beberapa pekerjaan seperti maintenance (perawatan) dan manajemen. dari suatu sistemnya. Dikotomi antara jajaran Windows NT dan Windows 9x berakhir dengan datangnya Windows XP, pada saat beberapa API gamepopuler seperti halnya DirectX dan OpenGL telah lebih "dewasa" dan efisien untuk dibuat program aplikasinya dan tentunya perangkat keras telah cukup kuat untuk menjalankan pemrosesan API yang dulu sempat menjadi masalah.

Windows NT 4.0 adalah versi Windows NT terakhir yang mendukung arsitektur DEC Alpha, MIPS, dan IBM PowerPC. Penerus Windows NT 4.0, Windows 2000 telah menghilangkan dukungan terhadap arsitektur-arsitektur prosesor tersebut, dan hanya mendukung prosesor Intel x86 saja.

Berdasarkan pembahasan diatas, saya mengambil contoh website dari salah satu perusahaan alat berat yang terkemuka di Indonesia yaitu PT KOMATSU INDONESIA (***http://www.komi.co.id.)*** dan didapati bahwa perusahaan tersebut menggunakan Sistem Operasi Windows NT4 dan Web Server Microsoft-IIS/4.0 yang informasinya saya dapatkan menggunakan Netcraft.com yang bisa dilihat pada gambar dibawah ini:

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT INDONESIA COMNETS PLUS Jl. EHV Gandul Limo - Depok	202.162.219.226	Linux	Microsoft-IIS/6.0	1-Jan-2008
Indosat Internet Service Provider	202.155.3.106	NT4/Windows 98	Microsoft-IIS/4.0	10-Jan-2005
INDOSATM2 Dedicated Emerald Customer	202.155.3.106	NT4/Windows 98	Microsoft-IIS/4.0	8-Jun-2001
INDOSATM2 Dedicated Emerald Customer	202.155.3.106	NT4/Windows 98	Microsoft-IIS/3.0	19-Nov-2000

Berdasarkan informasi yang didapat dari gambar diatas yang digunakan oleh *komi.co.id* ialah 202.162.219.226 untuk yang terakhir diupdate pada 1 Januari 2008 dan untuk mencari celah keamanannya menggunakan CVE, yaitu Common Vulnerabilities and Exposures.

– CVSS Scores & Vulnerability Types

CVSS Score	4.6
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	User
Vulnerability Type(s)	Gain privileges
CWE ID	CWE id is not defined for this vulnerability

Data diatas merupakan hasil dari celah keamanan dari CVE dengan identitas **CVE 2000-0197** dimana penjadwalan pada Windows NT4 menggunakan pemetaan drive pengguna interaktif yang saat masuk ke sistem, yang memungkinkan pengguna lokal memperoleh hak istimewa dengan menyediakan file batch Trojan di tempat file batch asli.

Namun tidak hanya sampai disitu , ada juga metode lain yaitu dengan menggunakan metasploit console seperti pada gambar dibawah ini:

```
msf > use exploit/windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > show targets
      ...targets...
msf exploit(ms06_040_netapi) > set TARGET <target-id>
msf exploit(ms06_040_netapi) > show options
      ...show and set options...
msf exploit(ms06_040_netapi) > exploit
```

Pada modul ini akan mengeksploitasi stack buffer overflow pada fungsi NetApi32 CanonicalizePathName menggunakan panggilan NetpwPathCanonicalize RPC di Server Service. Kemungkinan panggilan RPC lainnya dapat digunakan untuk memanfaatkan layanan ini. Eksploitasi ini akan menghasilkan penolakan layanan pada Windows XP SP2 atau Windows 2003 SP1. Upaya yang gagal dalam mengeksploitasi kemungkinan akan menghasilkan reboot lengkap pada Windows 2000 dan penghentian semua layanan terkait SMB di Windows XP. Target default untuk eksploitasi ini harus berhasil pada Windows NT 4.0, Windows 2000 SP0-SP4 +, Windows XP SP0-SP1 dan Windows 2003 SP0.

Analisa:

Dari data yang diperoleh, tentunya dari setiap sistem operasi yang digunakan akan memiliki celah ataupun kekurangan yang pastinya dapat ditembus, pada windows NT4 ini hal yang paling mendasar adalah bahwa pada versi ini merupakan versi lama dari produk Microsoft dan tentunya masih banyaknya kekurangan dalam sisi keamanannya, maka dari itu seperti yang terdapat pada CVE dengan identitas 2000-0197 mendapati bahwa Author mendapatkan celah pada windows NT4 tersebut.dimana didalam menggunakan pemetaan drive pengguna interaktif yang saat masuk ke sistem, yang memungkinkan pengguna lokal memperoleh hak istimewa dengan menyediakan file batch Trojan di tempat file batch asli. Maka dari itu dari sinilah terdapat celah yang tentunya menjadi suatu perbaikan dari sistem ataupun vendor itu sendiri.