

**TUGAS MATA KULIAH KEAMANAN JARINGAN INFORMASI  
DOSEN : Dr. BUDI RAHARDJO**

**LUBANG KEAMANAN WINDOWS 9X DAN CARA  
MEMINIMALKANNYA**

DISUSUN OLEH :  
WASIS SUPENO  
NIM : 23202152



**PROGRAM MAGISTER TEKNIK ELEKTRO  
BIDANG KHUSUS TEKNOLOGI INFORMASI  
PROGRAM PASCA SARJANA  
INSTITUT TEKNOLOGI BANDUNG  
2003**

## **Abstrak.**

*Sistem operasi Microsoft Window's 9X dibuat oleh perusahaan perangkat lunak Microsoft Corporation. Dikenal Microsoft Window's 9X setelah diluncurkannya Microsoft Window's Milenium. Bagi pengguna Window's 95, 98 dan ME sering disebut pengguna Window's 9X*

*Window's ME merupakan pengembangan dari Window's 98, Window's 98 merupakan pengembangan dari Window's 95. Sehingga secara dasar banyak persamaan antara ketiga sistem operasi tersebut*

*Sistem operasi Windows 9X menggunakan metode user friendly dalam pembangunannya, sehingga diharapkan user dari sistem operasi ini dapat dengan mudah mengoperasikan sistem operasi ini walaupun belum pernah mengenal komputer sama-sekali. Dilihat dari sisi user, hal ini sangatlah menguntungkan, dikarenakan user dimanja dengan berbagai kemudahan yang didukung tampilan grafis yang mengagumkan. Namun konsep user friendly ini harus dibayar dengan mengorbankan sisi keamanan dari sebuah sistem operasi.*

*Artikel ini tidak bertujuan mendidik menjadi seorang craker atau hacker tetapi bertujuan meminimalkan kemungkinan serangan yang diakibatkan adanya lubang keamanan pada sistem operasi Microsoft Window's 9X (Windows 95, 98, ME).*

## Daftar Isi

Judul	
Abstraks .....	i
Usulan Judul .....	ii
Daftar Isi .....	iii
1. Pendahuluan .....	1
2. Lubang Keamanan Sistem Operasi Windows 9X .....	4
2.1. Bypassing Security Reboot .....	4
2.2. Autorun and Ripping the Screen-Saver Password .....	5
2.3. Hacking Password Dial-UP in Memory .....	6
2.4. PWL Craking .....	6
2.5. Remote Hacking Windows 9X .....	7
2.6. Recovering Password from Compressed Folder .....	7
2.7. Hacking Windows 9X File and Print Sharing .....	8
2.8. Replaying The Win 9X Autentication Hash .....	10
2.9. Hacking Windows 9X Dial-Up Server .....	10
2.10. Windows 9X and Network Management Tools .....	11
2.11. Windows 9X Back Door Server and Trojans .....	12
2.11.1. Back Orifice .....	12
2.11.2. NetBus .....	13
2.11.3. SubSeven .....	13
3. Kesimpulan .....	15

# Lubang Keamanan Windows 9X dan Cara Meminimalkan

## 1. Pendahuluan.

Antisthenes, filosof dari Athena Yunani mengatakan “ Musuh Utama Adalah Ketidaktahuan“. Berangkat dari tulisan Antisthenes ini maka dapat diimplementasikan di sistem operasi komputer. Sistem operasi komputer diibaratkan suatu sistem kerja yang meliputi berbagai aspek yang dapat diibaratkan suatu bangunan atau rumah. Suatu rumah atau bangunan akan aman dari serangan pencuri apabila pemilik rumah mengetahui segala seluk-beluk dari rumah tersebut. Apabila pemilik rumah mengetahui seluk-beluk dari rumah tersebut, maka pemilik rumah akan mengetahui disisi mana terdapat lubang keamanan dari rumah yang dimilikinya. Setelah mengetahui sisi lubang keamanan rumah miliknya tentunya pemilik rumah akan berusaha menutup atau paling tidak meminimalkan sisi lubang keamanan rumah miliknya.

Demikian halnya sistem operasi komputer, sistem operasi komputer akan aman apabila pemilik atau pengguna sistem operasi tersebut mengetahui lubang keamanannya dan menutup lubang keamanan atau meminimalkan kemungkinan adanya penyerangan dengan menggunakan lubang keamanan dari sistem operasi miliknya.

Menurut Budi Raharjo dalam tulisannya “ Keamanan Sistem Informasi Berbasis Internet” pada halaman 12 mengatakan :

*Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (source code) yang digunakan sehingga semakin besar probabilitas terjadinya lubang keamanan (yang disebabkan kesalahan pemrograman, bugs). Lihat tabel di bawah untuk melihat peningkatan kompleksitas operating system Microsoft Windows. Seperti diungkapkan oleh Bruce Schneier dalam bukunya [38], “complexity is the worst enemy of security”.*

Tabel 1. Trend Meningkatnya Kompleksitas Software ( dari Bruce Schneier hal 357).

<b>Operating System</b>	<b>Tahun</b>	<b>Jumlah baris code (Lines of codes)</b>
Windows 3.1	1992	3 juta
Windows NT	1992	4 juta
Windows 95	1995	15 juta
Windows NT 4.0	1996	16,5 juta
Windows 98	1998	18 juta
Windows 2000	2000	35 s/d 60 juta (perkiraan, tergantung dari sumber informasi)

Dilihat dari tabel diatas sistem operasi Windows '95 mempunyai jumlah baris code 15 juta, sedangkan Windows '98 18 juta, jumlah baris kode yang cukup besar ini memungkinkan adanya kesalahan program atau bug yang menyebabkan terjadinya lubang keamanan.

Sistem operasi Windows 9X adalah sistem operasi komputer yang dibuat oleh perusahaan Microsoft, yang berkedudukan di Amerika. Sebutan sistem operasi Windows 9X muncul setelah diluncurkannya sistem operasi Windows Millenium (ME) pada tahun 1999. Sistem operasi Windows '95, '98 dan ME disebut Windows 9X, hal ini dikarenakan ketiga sistem operasi tersebut adalah hasil dari pengembangan sistem operasi Windows '95. Sehingga sejak saat itu sistem operasi Windows '95, '98 dan ME disebut Windows 9X.

Sistem operasi Windows 9X menggunakan metode user friendly dalam pembangunannya, sehingga diharapkan user dari sistem operasi ini dapat dengan mudah mengoperasikan sistem operasi ini walaupun belum pernah mengenal komputer sama-sekali. Dilihat dari sisi user, hal ini sangatlah menguntungkan, dikarenakan user dimanja dengan berbagai kemudahan yang didukung tampilan grafis yang mengagumkan. Namun konsep user friendly ini harus dibayar dengan mengorbankan sisi keamanan dari sebuah sistem operasi. Konsep keamanan suatu sistem operasi sengaja dikurangi atau mungkin dihilangkan demi mendukung user friendly. Sehingga pada kenyataannya lubang keamanan sistem operasi Windows 9X

sangat banyak, bahkan akses file oleh user tidak dibatasi sama-sekali, sehingga user yang bukan pemilik komputer tersebut (PENYUSUP) dapat dengan mudah masuk ke sistem, mengakses file dan bahkan diperkenankan untuk memformat harddisk, hal ini tentunya sangat berbahaya apabila sistem ini digunakan untuk aplikasi dengan data penting dan dihubungkan dengan jaringan. Sehingga sistem operasi ini hanya cocok digunakan untuk komputer tunggal di rumah dan tanpa akses jaringan dan user hanya satu orang.

Sistem operasi Windows '9X merupakan sistem operasi yang khusus digunakan untuk komputer pribadi dan tidak dianjurkan dipakai diluar pemilik komputer tersebut. Hal ini dikarenakan sistem operasi Windows 9X dari segi arsitektur dan keamanan sangat tidak mendukung bila dipakai oleh komputer dipakai oleh orang lain. Setiap orang yang memakai komputer tersebut dianggap sebagai pengguna tanpa adanya batasan dalam mengakses file yang ada. Misalnya sebuah komputer pribadi dengan sistem operasi Windows 98, maka password login dapat bypass hanya dengan menekan tombol esc, kemudian setelah komputer booting pengguna tersebut dapat mengakses semua file yang ada termasuk memformat harddisk.

Tulisan ini bertujuan mengupas beberapa lubang keamanan dari sistem operasi window's 9X dan cara meminimalkan lubang keamanan tersebut dari penyerang. Beberapa lubang keamanan Window's 9X yang akan dibahas pada tulisan ini antara lain :

- *bypassing security reboot,*
- *autorun and ripping screen saver password,*
- *hacking passwords in memory,*
- *pwl cracking,*
- *remote hacking Windows 9X,*
- *recovering passwords from compressed folder,*
- *hacking Windows 9X file and print sharing,*
- *replaying the Windows 9X Authentication Hash,*
- *hacking Windwos 9X Dial-Up Server,*
- *Windows 9X and Network Management Tools,*

- *Windows 9X Backdoor Server and Trojans.*

## **2. Lubang keamanan Sistem Operasi Windows 9X.**

Sistem operasi Windows 9X mengasumsikan semua user mempunyai wewenang penuh atas semua data yang ada didalam komputer tersebut. Hal ini disebabkan sistem filenya menggunakan *file allocation table* (FAT), Windows '95 menggunakan FAT 16, sedangkan Windows 98 dan ME menggunakan FAT 32. Sistem file FAT tidak membatasi user, semua user dapat mengaksesnya.

Dimisalkan suatu file transaksi toko disimpan di harddisk dengan format FAT 32. Harddisk ini dibuka dengan komputer lain, maka file transaksi tersebut dapat dibaca dengan mudah. Ini merupakan lubang keamanan sistem FAT yang digunakan di Windows.

Bila dibandingkan dengan sistem operasi Windows NT atau Windows 2000 sangat berbeda, Windows NT membatasi adanya pengguna. Pengguna sebagai guest tidak dapat menghapus file sistem atau membaca file yang bukan miliknya. Hal ini dikarenakan Windows NT menggunakan sistem file NTFS (NT File Sistem) yang membatasi wewenang dalam mengakses file.

Lubang keamanan dari sistem file FAT yang digunakan di Windows 9X tidak dapat diminimalkan, karena Windows 9X hanya dapat bekerja pada file sistem ini. Windows 9X tidak dapat bekerja di format NTFS yang mempunyai keamanan yang lebih baik.

### **2.1. *Bypassing Security Reboot.***

*Bypassing Security Reboot* adalah salah satu lubang keamanan Windows 9X, yaitu password login dapat dibypass dengan menekan tombol esc. Tidak seperti Windows NT, Windows 9X tidak mempunyai konsep keamanan multiuser yang logon. Setiap orang dapat masuk ke sistem dengan cara membooting ulang kemudian setelah muncul menu logon tekan tombol esc atau klik cancel, dan sistem tetap berjalan normal.

Selain cara diatas ada satu cara lagi untuk dapat mengakses sistem yaitu dengan cara pada saat muncul menu user logon, buat user baru dengan nama sembarang lengkap dengan passwordnya, kemudian apabila diminta menyetikkan

password lagi ketik password sekali lagi, kemudian tekan OK atau enter maka sistem akan membuat user baru dan semua sistem dapat diakses.

Solusi pemecahan dari lubang keamanan ini dengan metode tradisional yaitu dengan cara menyeting BIOS password sehingga saat komputer booting user diharuskan mengisi password. Konsep password BIOS diterapkan pertama kali di komputer IBM PC compatible. Selain dari pada itu pemasangan screen sever password sangat dianjurkan.

## ***2.2. Autorun and Ripping The Screen-Saver Password.***

Autorun and ripping the screen-saver password adalah salah satu lubang keamanan Windows 9X yaitu komputer file autorun.inf dari CD ROM pada saat screen-saver dikunci menggunakan password. Jadi sementara user diminta memasukkan password screen-saver untuk dapat mengakses sistem, sebenarnya sistem sudah diakses apabila user memasukan CD yang mempunyai autorun ke CD ROM drive. Hal ini dapat dimanfaatkan untuk menjalankan program apa saja, terutama trojan seperti NetBus atau BackOrifice. Selain dari pada itu data mengenai screen-saver password disimpan dalam registry tepatnya dibawah segmen HKEY\_USERS\DEFAULT\ Control Panel\Desktop serta didalam file USER.DAT pada direktori Windows. Dengan menggunakan program SSBypass (dapat dibeli di situsnya, [www.amecisco.com/ssbypass.htm](http://www.amecisco.com/ssbypass.htm)) . Cara menggunakannya cukup mudah, pada saat muncul password screen-saver, masukkan CD program tersebut kedalam CD ROM drive, program akan mem-bypass password. Software ini pada dasarnya menarik data dari registry atau file USER.DAT kemudian men-dekripsi file ini untuk mendapatkan password, kemudian memasukkannya kedalam sistem.

Solusi mengatasi lubang keamanan ini dengan cara me-nonaktifkan fasilitas autorun pada sistem, yaitu :

- Klik tombol start, klik setting, klik control panel, double klik system,
- Klik tab Device Manager,
- Double klik CD ROM, double klik entri CD ROM driver,
- Pada tab setting, pastikan check box Auto Insert Notification kosong,
- Klik OK, tutup control panel dan restart sistem.

### ***2.3. Hacking Password Dial-Up in Memory.***

Sistem Windows 9X mempunyai fasilitas koneksi jaringan menggunakan dial-up modem. Pada saat menu dial-up networking terdapat fasilitas save password, apabila fasilitas ini diaktifkan maka komputer akan menyimpan password dial-up kedalam memory. Sistem Windows 9X hanya menyembunyikan tampilan di layar saja, dengan menggunakan program SnadBoy ([www.snandboy.com](http://www.snandboy.com)) password dial-up networking dengan mudah dapat dipecahkan. Selain SnandBoy ada lagi program pemecah password dial-up networking, program ini dikenal dengan ShoWin dari Robin Keir ([www.foundstone.com/rdlabs/tools.php?kategory=Forensic](http://www.foundstone.com/rdlabs/tools.php?kategory=Forensic)).

Solusi pemecahan lubang keamanan ini cukup mudah yaitu, pada saat menggunakan fasilitas dial-up networking tidak mengaktifkan save password.

### ***2.4. PWL Craking.***

Sistem Windows 9X menyimpan password logon kedalam file \*.pwl, file ini disimpan didalam direktori Windows. Untuk mendapatkan file ini klik find \*.pwl maka semua password logon akan ditemukan. File pwl merupakan file utama yang digunakan untuk masuk didalam sistem. Sebelum diluncurkannya OEM system release 2 (OSR2) Windows 95 menggunakan teknik yang lemah didalam mengenkripsi file pwl. Terdapat banyak sekali program untuk mengcraking file pwl pada Windows 95. Pada Windows 98 teknik enkripsi file pwl diperbaiki namun beberapa software mampu memecahkan enkripsi ini, contoh adalah program yang dibuat oleh Vitas Ramanchaukas dan Eugene Korolev dengan nama Pwltool ([www.webdon.com](http://www.webdon.com)). Kemampuan program ini memecahkan file pwl tergantung dari panjang password dan komputer yang digunakan, semakin sedikit panjang password maka semakin cepat dipecahkan dan semakin tinggi komputer yang digunakan semakin cepat juga dipecahkan. Selain program Pwltool, masih ada program pwl crak yang lebih baik yaitu CAIN. CAIN dibuat oleh Break-Dance ([www.confine.com](http://www.confine.com)) selain mempunyai kemampuan dalam memecahkan file pwl juga mempunyai kemampuan memecahkan screen-saver password dari registry Windows, cached password dan masih banyak lagi.

Solusi untuk mengatasi lubang keamanan ini adalah, apabila sistem operasi yang digunakan Windows 95 sebelum dirilisnya OSR2 maka dianjurkan untuk mengupdate pwl algoritmanya di situs <http://support.microsoft.com/support/kb/article/Q132/8/07.asp>. Sedangkan untuk sistem operasi Windows 98 dengan cara mendisable password caching pada Win 98 System Policy Editornya dan menyetting DWORD registry dengan menset menjadi HKEY\_LOCAL\_MACHINE \SOFTWARE\Microsoft\CurrentVersion\Policies\Network\DisablePwdCaching = 1.

### ***2.5. Remote Hacking Windows 9X.***

Sistem operasi Windows 9X secara default tidak menyediakan remote access untuk sistem registrynya. Namun remote access registry memungkinkan jika di install program Microsoft Remote Registry Service. Program ini dapat ditemukan di CD Installer Windows 9X yaitu di folder \admin\nettools\remoteregistry.

Service remote registry pengamanannya menggunakan user-level security, yang dapat diakses apabila user dapat meng-enable password user pada saat melakukan booting. Kemudian penyerang dapat memanfaatkan remote service ini untuk mendapatkan data registry sistem dan mungkin mengubahnya jika didapat akses tanpa batas di sistem.

Untuk meminimalkan kemungkinan serangan dengan memanfaatkan remote registry yang hanya dilindungi oleh password user-level, maka yang perlu dilakukan adalah tidak menginstall Microsoft Remote Registry Service jika memang tidak mutlak dibutuhkan. Namun jika mengharuskan menginstall service ini maka buatlah password yang sulit ditebak dengan menggunakan karakter khusus, misalnya : ‘ ^ } ~ ` | ? > dan jumlah password yang panjang, misalnya 10 karakter atau lebih bila dimungkinkan.

### ***2.6. Recovering Password from Compressed Folder.***

Windows 98 Plus dan Windows ME menyediakan fasilitas yang disebut Compressed Folders, yaitu mengkompres file sehingga menjadi file yang lebih kecil sehingga menghemat tempat pada harddisk. Microsoft menyediakan fasilitas perlindungan file terkompres dengan password. Sehingga diharapkan para pelaku

bisnis yang menggunakan sistem Windows 98 plus dan ME dapat menghemat tempat dan file tersebut terlindungi.

Namun apa yang diharapkan oleh Microsoft mempunyai banyak lubang keamanan, yaitu password compress folder disimpan pada direktori Windows, tepatnya di c:\Windows\dynazip.log. Semua orang dapat mengakses file ini dan celakanya file ini file cleartext yang tidak terenkripsi sama sekali, sehingga dapat dengan mudah dibaca setiap orang.

Solusi dari lubang keamanan ini tidaklah menggembirakan karena memang belum ada pemecahannya. Pemecahan yang mudah dengan tidak memanfaatkan fasilitas ini. Sedangkan menurut Microsoft adalah dengan mengupdate Windows 9X ke Windows 2000 atau NT yang menggunakan sistem file NTFS sehingga lebih aman. Namun solusi ini tidaklah bijaksana, karena user harus mengeluarkan biaya untuk mengupdate menjadi Windows 2000 atau NT. Solusi yang lebih bijaksanan dengan memanfaatkan software PGPdisk dari Network Associates, Inc dapat dilihat di situsnya ([www.nai.com](http://www.nai.com)).

### ***2.7. Hacking Windows 9X File and Print Sharing.***

Windows 9X mempunyai fasilitas file sharing dan print sharing yang dapat digunakan pada jaringan agar user lain dapat menakses file dan printer yang ada. Fasilitas file sharing didalam Windows 9X mempunyai 3 (tiga) tingkatan, yaitu : tidak disharing, disharing dengan mode read only, disharing dengan otoritas password dan disharing full atau mode baca tulis. Untuk file-file yang dianggap tidak penting user menggunakan mode read only, sedangkan untuk file yang perlu otoritas disharing dengan mode otoritas password. Namun ada beberapa tool yang dapat digunakan untuk mendapatkan akses password file sharing, yaitu software Brute Force(BF). BF tools dapat menscan IP dari komputer Windows 9X yang menyediakan file sharing serta memecahkan password sharing yang ada. Kecepatan memecahkan password file sharing tergantung dari kecepatan prosesor yang digunakan, kamus password dan panjang password yang digunakan.

Selain dari software BF tool ada satu virus yang dapat membuka file sharing Windows 9X, yaitu worm w32/nimda. Virus ini memanfaatkan fasilitas email built-

in di Windows dan sekaligus memanfaatkan lubang keamanannya, yaitu outlook express. Outlook Express (OE) merupakan mail klient yang terinstall secara otomatis apabila user menginstall sistem operasi Windows 9X. Sedangkan kelemahan dari OE adalah adanya fasilitas menampilkan attachment file secara otomatis kedalam ikon yang bagus, sehingga user tergoda untuk membukanya. Worm w32/nimda memanfaatkan kelemahan ini dengan mengirim ke user yang menggunakan mail klient OE dengan membuat file attachment dengan nama yang sangat menggiurkan misalnya : loveyou, beatifullgirls, mp3, dll. Apabila attachment ini di klik oleh user maka worm w32/nimda akan masuk kesistem, di sistem worm ini akan mendata semua informasi dan alamat yang tersimpan pada mailbox OE. Setelah mendapatkan alamat-alamat yang tersimpan didalam mailbox, worm w32/nimda berusaha mengirimkan e-mail yang serupa dengan menggunakan nama pengirim dari komputer terinfeksi dan nama e-mail yang terdapat pada mailbox dan semua komputer pada group jaringan tersebut. Apabila jaringan terkoneksi dengan internet maka worm w32/nimda akan mengirimkan e-mail bervirus ke alamat yang ada di mailbox.

Sebenarnya tujuan utama dari worm w32/nimda adalah sebagai berikut, setelah worm w32/nimda masuk ke sistem, maka semua disk akan disharing dengan mode full. Sehingga apabila ada penyusup yang masuk kesistem maka dapat mengakses semua sistem bahkan dapat menghapus semua file di sistem, hal ini sangat berbahaya jika sistem terhubung dengan internet. Selain dari pada itu worm win32/nimda akan menduplikasikan diri pada semua folder di sistem dengan nama file berekstensi .eml. Ukuran file worm win32/nimda kurang lebih 18 Kbit. Apabila didalam sistem terdapat 500 folder maka worm win32/nimda akan menghabiskan space harddisk sebesar  $18 \text{ Kbit} \times 500 = 9 \text{ Mbit}$  hal ini menyebabkan kerja sistem menjadi lambat sekali. Disamping itu worm win32/nimda akan memaksa sistem untuk terus-menerus bekerja dengan mengirimkan e-mail secara terus-menerus.

Solusi pemecahan dari lubang keamanan ini adalah sebagai berikut. Tidak memasang file sharing dan print sharing jika memang tidak dibutuhkan. Apabila diharuskan menggunakan file sharing maka diusahakan menggunakan mode otoritas

password dalam mengaksesnya. Password dibuat panjang dan menggunakan karakter yang tidak lazim, misalnya : ‘ ^ } ~ ` | ? >.

Sedangkan untuk mencegah worm win32/nimda masuk ke sistem dengan cara meng-*uninstall* OE dan menggunakan mail klient yang lain, misalnya eudora mail. Apabila mendapatkan kiriman e-mail dengan attachment yang menggiurkan tidak membuka dan langsung menghapus attachment tersebut. Langkah antisipasi worm w32/nimda dengan memasang anti virus terbaru. Sehingga kemungkinan penularan worm win32/nimda melalui disket atau flashdisk dapat dicegah.

### ***2.8. Replaying the Win 9X Autentication Hash.***

Pada tanggal 5 Januari 1999 sebuah group research L0pht Advisory merealise laporan tentang autentication file sharing pada jaringan Windows 9X. Windows 9X menggunakan kombinasi user name menggunakan teknik encripsi *Hash* (cryptographically scramble). Dibutuhkan waktu 15 menit untuk memecahkan password file sharing dan remote conection yang telah di enkripsi menggunakan *Hash*. Walaupun kesalahan klasik criptografi yang dilakukan Microsoft harus dihindari tetapi sulit untuk di eksploitasi. Rekomendasi yang diajukan oleh L0pht Advisory tidaklah ditanggapi serius oleh pihak Microsoft.

Hal ini berbeda pada saat L0pht Advisory memberikan masukan kepada developer SAMBA (software networking Windows to Unix) dengan ditemukannya beberapa lubang keamanan, maka developer SAMBA segera melakukan perbaikan.

Solusi dari lubang keamanan ini tidaklah begitu menggembirakan, sebab pihak Microsoft menganjurkan untuk melakukan up-date dengan sistem Windows 2000 atau NT.

### ***2.9. Hacking Windwos 9X Dial-Up Server.***

Applet Windows 9X merupakan paket yang terintegrasi dalam sistem yang memiliki untung dan rugi. Setiap user dapat masuk melalui Back Door (pintu belakang) kedalam jaringan dengan cara memasang modem dan menginstall Dial-Up server komponen pada Windows '95. Sedangkan pada Windows '98 dan ME sudah terintegrasi. Sistem yang bagus apabila mempunyai file sharing apabila digunakan

didalam suatu jaringan. Ini memungkinkan menjajaki satu persatu sistem dan mencoba-coba password jika ada untuk membagi end modem yang lain, tentunya penyusup tidak lama lagi akan mendapatkan akses ke sistem. Penyusup yang dapat memecahkan Dial-Up Server dan password share file maka dapat melakukan apa saja didalam sistem, hal ini dikarenakan sistem Windows 9X tidak dilengkapi dengan Route Network Traffic sebagaimana Windows NT atau 2000.

Untuk menutupi lubang keamanan ini hanya ada satu cara, yaitu tidak menggunakan Dial-Up Server apabila tidak dibutuhkan dan memperbaiki sistem yang ada menggunakan fasilitas System Policy Editor. Apabila fasilitas ini memang dibutuhkan, password untuk mengakses dial-up server harus di set agar aman, misalnya passwrd yang panjang dengan karakter yang jarang digunakan, kemudian menggunakan teknik enkripsi pada saat memakai kotak dialog dial-up server dan dalam outentikasinya memakai user-level security.

#### ***2.10. Windows 9X and Network Management Tools.***

The last but no least, kalimat ini kiranya cocok untuk Network Management Tools sistem Windows 9X. Kalau dilihat dari sejarah perlengkapan untuk manajemen jaringan Windows 9X tergolong paling akhir bila dibandingkan sistem Unix, Novell atau NT. Namun walaupun fasilitas ini tergolong yang paling sedikit dibandingkan sistem operasi lainnya, dan lucunya banyak mengandung lubang keamanan.

Network Management Tools di sistem Windows 9X disebut Simple Network Management Protocol (SNMP). Informasi mengenai SNMP yang ada di Windows 9X dapat dilihat satu persatu pada folder \tools\reskit\netadmin\snmp. Sayangnya Windows 9X tidak mempunyai fasilitas untuk memantau siapa saja yang masuk di sistem dan menggunakan sharing file didalam SNMP versi 1MIB, sehingga fasilitas ini dapat digunakan untuk mengekloitasi sistem oleh penyusup.

Solusi menutup lubang keamanan ini dengan cara tidak menginstall fasilitas SNMP pada sistem apabila memang tidak diperlukan, namun apabila memang diperlukan dianjurkan untuk mengupgrade ke Windows NT atau 2000.

### **2.11. Windows 9X Backdoor Server and Trojans.**

Jika diasumsikan sistem file sharing, Dial-Up Server dan Remote Registry Access tidak diaktifkan, apakah dijamin sistem ini aman, jawabnya adalah TIDAK. Jika penyusup dihalangi oleh remote administration yang jelek, maka dengan mudah akan masuk dan mengakses sistem.

Apabila fasilitas diatas tidak diaktifkan penyusup akan menggunakan Back Door (pintu belakang) dan mengirim Trojan horse untuk masuk ke sistem. Beberapa software yang sering digunakan untuk masuk ke sistem melalui pintu belakang adalah : Back Orifice, NetBus dan SubSeven.

#### **2.11.1. Back Orifice.**

Back Orifice (BO) adalah software yang digunakan untuk menghacking remote administration tools di sistem Windows 9X. BO di released pada musim panas 1998 oleh perusahaan Black Hat security Convention ([www.blackhat.com](http://www.blackhat.com)), dan dapat di download secara bebas dari situs [www.cultdeadcow.com/tools](http://www.cultdeadcow.com/tools) . BO hampir mendekati fasilitas Remote Control dari Windows 9X, yang didalamnya mempunyai fasilitas menambah dan menghapus registry, mereboot sistem, mengirim dan menerima file, menampilkan cached password, spawn proses dan membuat file sharing.

BO dapat di konfigurasi dan di install dengan sembarang nama file dengan catatan nomor IP server Windows sudah diketahui. Apabila BO sudah dijalankan akan masuk ke registry HKEY\_LOCAL MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Service dan akan merestart sistem. Teknik yang digunakan dengan cara menyadapkan UDP pada port 31337 yang tidak dikonfigurasi.

Pada versi berikutnya BO ( BO 2000 dapat dilihat di <http://sourceforge.net/projects/bo2k>) merupakan program favorit yang digunakan oleh hacker untuk masuk ke sistem Windows, termasuk Windows NT dan Windows 2000. BO2k original dapat digunakan untuk dua server/client Windows dan sulit dideteksi. Konfigurasi standard BO2k akan menyadap pada TCP port 54320 dan UDP 54321 dan akan mengkopi file secara otomatis dengan nama UMGR32.exe di folder %systemroot%. Jika dibiarkan akan menyebar ke Stealth mode dan segera meng-*install* secara

otomatis service yang disebut “Remote Administration Service” dibawah registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunService, kemudian menghapus file aslinya. Kemudian sistem akan mengganti remote service asli dengan remote service dari BO2k.

### **2.11.2. NetBus.**

NetBus adalah varian dari BO, ditulis oleh Carl-Frederik Neikter yang dapat digunakan untuk meremote sistem Windows termasuk NT dan 2000. NetBus menawarkan kemudahan dalam penggunaannya dibandingkan BO. Pada jaringan dengan lebar band yang besar, dapat menggunakan mode GUI (Graphical User Interface). NetBus secara default menggunakan nama file patch.exe dalam menginfeksi sistem, namun nama file dapat diganti dengan sembarang nama. Teknik yang digunakan apabila file NetBus di klik oleh user, NetBus akan menulis dalam registry HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run, dan sistem akan diupdate apabila booting ulang. NetBus menyadap di TCP port 12345 atau 20034 secara default, dan ini dapat diubah.

### **2.11.3. SubSeven.**

SubSeven menggabungkan keunggulan BO dan NetBus. SubSevenServer (S7S) menyadap pada TCP port 27374 secara default, port ini merupakan port dasar untuk menghubungkan dengan klient. S7S memberikan kemudahan kepada penyusup dengan fasilitas control yang sangat komplit, diantaranya :

- *louncing port scan* (dari sistem yang terinfeksi),
- *starting* dari FTP server pada direktori root dengan mode baca-tulis,
- meremote registry dan dapat mengubahnya,
- dapat mencari password cached, RAS, ICQ dan password dari aplikasi lainnya,
- *aplication and port redirection*,
- *printing*,
- merestart sistem terinfeksi melalui remote,
- *keystroke logger (listen on port 2737 by default)*,

- meremote terminal (pada matrix secara default menyadap port 7215),
- pengendalian mouse jarak jauh,
- membuka aplikasi dan memata-matai di ICQ, AOL Instant Messenger, MSN Messenger dan Yahoo Messenger melalui port 5428,
- membuka web broser kemudian menggunakannya dengan nama user dari sistem yang terinfeksi.

Selain dari fasilitas diatas S7S juga dapat mengirimkan semua informasi sistem yang terinfeksi diantaranya, nomor IP, port penyadap dan semua password yang ada, melalui fasilitas IRC.

Departemen Telekomunikasi di USA melaporkan adanya infeksi S7S di banyak komputer yang menggunakan sistem operasi Windows, sehingga antara bulan January sampai dengan Maret 2000 banyak komputer telah mengirimkan nomor IP, port penyadap dan semua password kedalam alamat IRC generic (irc.ircnetwork.net) setiap lima menit.

Solusi untuk menutup lubang keamanan ini dengan cara menutup pintu belakang dengan cara memasang program khusus yang disebut FireWalls. Fire Walls akan melaporkan adanya penyusup yang masuk melalui port tertentu ke sistem. Selain dari pada itu dengan tidak membuka port yang tidak digunakan untuk melayani jaringan.

Solusi yang lain adalah dengan memasang anti virus dari vendor terkenal, misalnya AntiViral Toolkit untuk mengantisipasi penyusupan melalui pintu belakang dan trojan ( dapat dilihat disitus [www.centralcommand.com](http://www.centralcommand.com)), Defanse Suite(TDS) dapat dilihat disitus [www.multimania.com/ilikeit/tds2.htm](http://www.multimania.com/ilikeit/tds2.htm), BO-removal tool yang disebut BoSniffer yang dapat digunakan untuk memonitor adanya serangan BO.

### 3. Intidari Lubang Keamanan Windows 9X.

Tabel dibawah ini adalah tabel rangkuman dari lubang keamanan Windows 9x dan cara meminimalkannya.

Tebel 2. Lubang keamanan Windows 9X dan Solusi pemecahan.

NO.	Lubang Keamanan	Microsoft Windows			Solusi Pemecahan
		Win '95	Win '98	Win ME	
1	Sistem File, mengijinkan semua user untuk mengaksesnya.	FAT 16	FAT 32	FAT 32	Upgrade ke Windows NT atau 2000.
2	<i>Bypassing Security Reboot</i>	V	V	V	Setting Password BIOS .
3	<i>Autorun and Ripping the Screen-Saver Password</i>	V	V	V	Nonaktifkan fasilitas aotu run.
4	<i>Hacking Password Dial-UP in Memory</i>	V	V	V	Tidak mengaktifkan save password.
5	<i>PWL Craking</i>	-	V	V	Update PWL algoritma untuk Win '95, disable password caching.
6	<i>Remote Hacking Windows 9X</i>	V	V	V	Nonaktifkan fasilitas ini, gunakan password dengan karakter khusus.
7	<i>Recovering Password from Compressed Folder</i>	-	V	V	Upgrade ke Windows NT atau 2000.
8	<i>Hacking Windows 9X File and Print Sharing</i>	V	V	V	Non aktifkan file/print sharing, gunakan metode otoritas password dengan karakter khusus, pasang antivirus terbaru.
9	<i>Replaying The Win 9X Autenti - cation Hash</i>	V	V	V	Upgrade ke Windows NT atau 2000.
10	<i>Hacking Windows 9X Dial-Up Server</i>	V	V	V	Non aktifkan Dial-UpServer gunakan metode otoritas password dengan karakter khusus
11	<i>Windows 9X and Network Mana- gement Tools</i>	V	V	V	Non aktifkan SNMP, up- grade ke windows NT/2000
12	<i>Windows 9X Back Door Server and Trojans</i>	V	V	V	Pasang Fire Walls, nonaktifkan port yg tidak digunakan, pasang anti virus terbaru.

#### **4. Kesimpulan.**

Sistem Operasi Windows 9X yang meliputi Windows '95, Windows '98 dan Windows Millennium (ME) tidak dianjurkan untuk aplikasi jaringan dan aplikasi dengan data penting. Mengingat sistem operasi ini banyak sekali mengandung lubang keamanan yang dapat digunakan oleh penyusup untuk mengakses sistem.

Apabila sistem operasi ini sudah dilengkapi dengan Fire Walls dan beberapa lubang keamanan sudah ditutup dapat digunakan di dalam jaringan dan internet, namun penulis tidak menjamin data-data didalam sistem dapat dijaga apabila komputer digunakan oleh lebih dari satu user, mengingat sistem file Windows 9X menggunakan FAT 16 dan FAT 32 yang mengijinkan semua user mengakses semua sistem.

## Daftar Pustaka

1. Budi Rahardjo. 2002. Keamanan Sistem Informasi Berbasis Internet, versi 5.1#id :PT Insan Infonesia-Bandung & PT INDOCISC – Jakarta.
2. McClure Stuart, Scambray Joel dan Kurtz George. 2001. Hacking Exposed:Network Security Secrets and Solution, Third Edition: Osborne/McGraw-Hill.
3. Anonim. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network Macmillan Computer Publishing.
4. [www.atstake.com/research/advisories/1999/95replay.txt](http://www.atstake.com/research/advisories/1999/95replay.txt)
5. [www.tlsecurity.net/main.html](http://www.tlsecurity.net/main.html)
6. [www.tlsecurity.net/trojanh.html](http://www.tlsecurity.net/trojanh.html)
7. [www.tlsecurity.net/tlfaq.htm](http://www.tlsecurity.net/tlfaq.htm)
8. [www.eqla.demon.co.uk/trojanhorses.html](http://www.eqla.demon.co.uk/trojanhorses.html)
9. <http://subseven.slak.org>