

BAB VI

Eksploitasi Keamanan





Pendahuluan

- Dalam bab ini akan dibahas beberapa contoh eksploitasi lubang keamanan. Contoh-contoh yang dibahas ada yang bersifat umum dan ada yang bersifat khusus untuk satu jenis operating system tertentu, atau untuk program tertentu dengan versi tertentu. Biasanya lubang keamanan ini sudah ditutup pada versi baru dari paket program tersebut sehingga mungkin tidak dapat anda coba. Pembahasan dalam bab ini tentunya tidak komplis dikarenakan batasan jumlah halaman. Jika diinginkan pembahasan yang lebih komplis ada buku “Hacking Exposed”
- Menurut “Hacking Exposed”, metodologi dari penyusup biasanya mengikuti langkah sebagai berikut:
 - *Target acquisition and information gathering*
 - *Initial access*
 - *Privilege escalation*
 - *Covering tracks*



Mencari informasi

- Sebelum melakukan penyerangan, seorang cracker biasanya mencari informasi tentang targetnya. Banyak informasi tentang sebuah sistem yang dapat diperoleh dari Internet. Sebagai contoh, informasi dari DNS (Domain Name System) kadang-kadang terlalu berlebihan sehingga memberikan terlalu banyak informasi kepada orang yang bermaksud jahat.
- DNS dapat memberikan informasi tentang nama-nama server beserta nomor IP yang dimiliki oleh sebuah perusahaan. Seseorang yang tidak tahu apa-apa, dengan mengetahui domain dari sebuah perusahaan dapat mengetahui informasi yang lebih banyak tentang server-server dari perusahaan tersebut. Paling tidak, informasi tentang name server merupakan informasi awal yang dapat berguna.



Mencari informasi

- Informasi tentang DNS tersedia secara terbuka di Internet dan dapat dicari dengan menggunakan berbagai tools seperti:
 - whois, host, nslookup, dig (tools di sistem UNIX)
 - Sam Spade (tools di sistem Windows)
 - web dari Network Solutions inc. yang menyediakan informasi tentang data-data gTLD (.com, .net, .org, dan seterusnya) melalui webnya di <http://www.networksolutions.com>

Host, Whois, dig

- Berikut ini adalah contoh beberapa session untuk mencari informasi tentang domain dan server-server yang digunakan oleh domain tersebut. Untuk mencari name server, dapat digunakan program “host” dengan option “-t ns”. Sementara itu untuk mencari nomor IP dari sebuah host, langsung gunakan program host tanpa option.

```
unix$ host -t ns yahoo.com
yahoo.com          NS          NS3.EUROPE.yahoo.com
yahoo.com          NS          NS1.yahoo.com
yahoo.com          NS          NS5.DCX.yahoo.com

unix$ host ns1.yahoo.com
ns1.yahoo.com      A           204.71.200.33
```

Host, Whois

- Cara yang sama dapat dilakukan dengan menggunakan program whois. Contoh di bawah ini adalah untuk mencari informasi tentang domain yahoo.com dengan menggunakan server whois yang berada di Network Solutions Inc.

```
unix$ whois -h whois.networksolutions.com yahoo.com

Registrant:
Yahoo (YAHOO-DOM)
3420 Central Expressway
Santa Clara, CA 95051
US

Domain Name: YAHOO.COM

Administrative Contact, Technical Contact:
Balling, Derek (DJB470) tech-contact@YAHOO-INC.COM
Yahoo!
701 First Ave
Sunnyvale, CA 94089
US
+1-408-349-5062
Billing Contact:
Billing, Domain (DB28833) domainbilling@YAHOO-INC.COM
Yahoo! Inc.
225 Broadway, 13th Floor
San Diego, CA 92101
1-408-731-3300

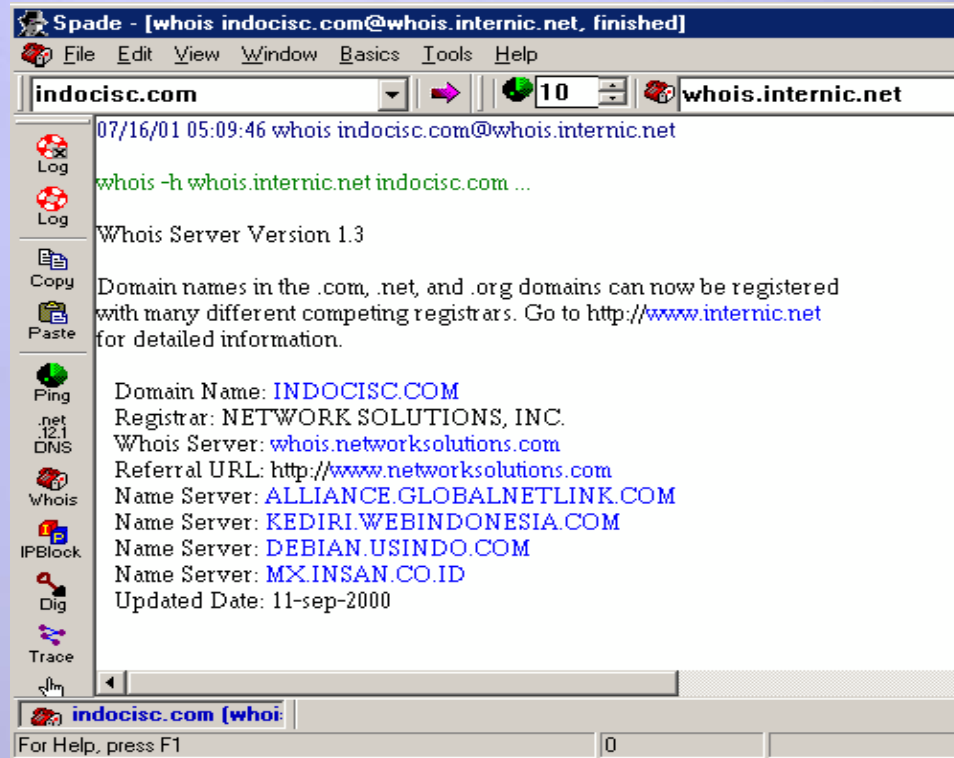
Record last updated on 28-Jun-2001.
Record expires on 20-Jan-2010.
Record created on 18-Jan-1995.
Database last updated on 20-Jul-2001 00:12:00 EDT.

Domain servers in listed order:

NS1.YAHOO.COM                204.71.200.33
NS5.DCX.YAHOO.COM            216.32.74.10
NS3.EUROPE.YAHOO.COM         217.12.4.71
```


Sam Spade, utility untuk MS Windows

- Untuk anda yang menggunakan sistem yang berbasis Microsoft Windows, anda dapat menggunakan program Sam Spade. Program ini dapat diperoleh secara gratis dari web <http://www.samspade.org>. Gambar berikut menunjukkan sebuah sesi Sam Spade untuk mencari informasi tentang domain INDOCISC.com.



```
Spade - [whois indocisc.com@whois.internic.net, finished]
File Edit View Window Basics Tools Help
indocisc.com | 10 | whois.internic.net
07/16/01 05:09:46 whois indocisc.com@whois.internic.net
whois -h whois.internic.net indocisc.com ...
Whois Server Version 1.3
Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.
Domain Name: INDOCISC.COM
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: http://www.networksolutions.com
Name Server: ALLIANCE.GLOBALNETLINK.COM
Name Server: KEDIRI.WEBINDONESIA.COM
Name Server: DEBIAN.USINDO.COM
Name Server: MX.INSAN.CO.ID
Updated Date: 11-sep-2000
indocisc.com [whois]
For Help, press F1
```



Eksplorasi Web Server

- Web server menyediakan jasa untuk publik. Dengan demikian dia harus berada di depan publik. Sayangnya banyak lubang keamanan dalam implementasi beberapa web server. Di bagian ini akan dicontohkan beberapa eksploitasi tersebut.
- **Defacing Microsoft IIS**

Salah satu lubang keamanan dari web yang berbasis IIS adalah adanya program atau script yang kurang baik implementasinya. Sebagai contoh, bugtraq id 1806 menunjukkan cara untuk melihat isi direktori dari sebuah web server yang berbasis IIS.

Eksplorasi Web Server

```
http://target/scripts/..%c1%1c../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c0%9v../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c0%qf../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c1%8s../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c1%9c../winnt/system32/cmd.exe?/  
c+dir  
http://target/scripts/..%c1%pc../winnt/system32/cmd.exe?/  
c+dir
```

perintah “dir” untuk melihat direktori di server IIS tersebut. Selain melihat direktori dengan perintah “dir”, anda dapat juga menjalankan perintah lain di server tersebut, seperti misalnya meng-copy file. Salah satu exploit adalah dengan mengambil file dari sebuah tempat dengan “TFTP” ke server IIS tersebut. Prinsipnya adalah menggunakan perintah yang command line sebagai perintah “dir” tersebut, seperti dnegan printah “tftp” dan menggantikan spasi dengan tanda tambah (+). Setelah itu, file dapat ditempatkan dimana saja termasuk di direktori yang digunakan untuk memberikan layanan web. Atau dengan kata lain web tersebut dapat diubah (*deface*).

Eksplorasi Web Server



SUND4NYMOUZ
Mang_Aj0 | Blackshadow



Greets To :

Hubbi Defacer - Hacker-Newbie - Medan Cyber Team - Yogyacardlink - Indonesian Blackhat - Submit Defacer Crew - Surabaya Hackerlink - Borneo Attacker - Code Breaking Force - Ma

transferring data from divine-music.info...



Denial of Service Attack

- “*Denial of Service (DoS) attack*” merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya (*denial of service*) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi “bengong” (*hang, crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).

Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial. Sebagai contoh apabila sistem yang diserang merupakan server yang menangani transaksi “*commerce*”, maka apabila server tersebut tidak berfungsi, transaksi tidak dapat dilangsungkan. Bayangkan apabila sebuah bank diserang oleh bank saingan dengan melumpuhkan outlet ATM (Anjungan Tunai Mandiri, *Automatic Teller Machine*) yang dimiliki oleh bank tersebut. Atau sebuah credit card merchant server yang diserang sehingga tidak dapat menerima pembayaran melalui credit card.



Denial of Service Attack

- “*Denial of Service (DoS) attack*” merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya (*denial of service*) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi “bengong” (*hang, crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).
- Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial. Sebagai contoh apabila sistem yang diserang merupakan server yang menangani transaksi “*commerce*”, maka apabila server tersebut tidak berfungsi, transaksi tidak dapat dilangsungkan. Bayangkan apabila sebuah bank diserang oleh bank saingan dengan melumpuhkan outlet ATM (Anjungan Tunai Mandiri, *Automatic Teller Machine*) yang dimiliki oleh bank tersebut. Atau sebuah credit card merchant server yang diserang sehingga tidak dapat menerima pembayaran melalui credit card.



Denial of Service Attack

- “*Denial of Service (DoS) attack*” merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya (*denial of service*) atau tingkat servis menurun dengan drastis. Cara untuk melumpuhkan dapat bermacam-macam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi “bengong” (*hang, crash*), tidak berfungsi, atau turun kinerjanya (beban CPU tinggi).
- Serangan denial of service berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan DoS tidak ada yang dicuri. Akan tetapi, serangan DoS dapat mengakibatkan kerugian finansial. Sebagai contoh apabila sistem yang diserang merupakan server yang menangani transaksi “*commerce*”, maka apabila server tersebut tidak berfungsi, transaksi tidak dapat dilangsungkan. Bayangkan apabila sebuah bank diserang oleh bank saingan dengan melumpuhkan outlet ATM (Anjungan Tunai Mandiri, *Automatic Teller Machine*) yang dimiliki oleh bank tersebut. Atau sebuah credit card merchant server yang diserang sehingga tidak dapat menerima pembayaran melalui credit card.
- Selain itu, serangan DoS sering digunakan sebagai bagian dari serangan lainnya. Misalnya, dalam serangan *IPspoofing* (seolah serangan datang dari tempat lain dengan nomor IP milik orang lain), seringkali DoS digunakan untuk membungkam server yang akan *dispoof*.



Land attack

- Land attack merupakan serangan kepada sistem dengan menggunakan program yang bernama “*land*”. Apabila serangan diarahkan kepada sistem Windows 95, maka sistem yang tidak diproteksi akan menjadi *hang* (dan bisa keluar layar biru). Demikian pula apabila serangan diarahkan ke beberapa jenis UNIX versi lama, maka sistem akan *hang*. Jika serangan diarahkan ke sistem Windows NT, maka sistem akan sibuk dengan penggunaan CPU mencapai 100% untuk beberapa saat sehingga sistem terlihat seperti macet.
- Serangan land ini membutuhkan nomor IP dan nomor port dari server yang dituju. Untuk sistem Windows, biasanya port 139 yang digunakan untuk menyerang.
- Program land menyerang server yang dituju dengan mengirimkan packet palsu yang seolah-olah berasal dari server yang dituju. Dengan kata lain, source dan destination dari packet dibuat seakan-akan berasal dari server yang dituju. Akibatnya server yang diserang menjadi bingung.
- **Latierra**
- Program *latierra* merupakan “perbaikan” dari program land, dimana port yang digunakan berubah-ubah sehingga menyulitkan bagi pengamanan.



Ping-o-death

- *Ping-o-death* sebenarnya adalah eksploitasi program *ping* dengan memberikan packet yang ukurannya besar ke sistem yang dituju. Beberapa sistem UNIX ternyata menjadi hang ketika diserang dengan cara ini. Program ping umum terdapat di berbagai operating system, meskipun umumnya program ping tersebut mengirimkan packet dengan ukuran kecil (tertentu) dan tidak memiliki fasilitas untuk mengubah besarnya packet. Salah satu implementasi program ping yang dapat digunakan untuk mengubah ukuran packet adalah program ping yang ada di sistem Windows 95.

Ping broadcast (smurf)

- Ping broadcast (smurf)
- Salah satu mekanisme serangan yang baru-baru ini mulai marak digunakan adalah menggunakan ping ke alamat *broadcast*, ini yang sering disebut dengan *smurf*. Seluruh komputer (*device*) yang berada di alamat broadcast tersebut akan menjawab.

Smurf attack biasanya dilakukan dengan menggunakan *IP spoofing*, yaitu mengubah nomor IP dari datangnya *request*, tidak seperti contoh di atas. Dengan menggunakan *IP spoofing*, respon dari *ping* tadi dialamatkan ke komputer yang IPnya *dispoof*. Akibatnya komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosan penggunaan (bandwidth) jaringan yang menghubungkan komputer tersebut. Dapat dibayangkan apabila komputer yang *dispoof* tersebut memiliki hubungan yang berkecepatan rendah dan ping diarahkan ke sistem yang memiliki banyak host. Hal ini dapat mengakibatkan DoS attack.

```
$ ping 192.168.1.255
PING 192.168.1.255 (192.168.1.255): 56 data bytes
64 bytes from 192.168.1.4: icmp_seq=0 ttl=64 time=2.6 ms
64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.0 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=4.7 ms
(DUP!)
--- 192.168.1.255 ping statistics ---
4 packets transmitted, 4 packets received, +4 duplicates, 0%
packet loss
round-trip min/avg/max = 2.5/6.0/24.0 ms
```

Ping broadcast (smurf)

- Ping broadcast (smurf)
- Salah satu mekanisme serangan yang baru-baru ini mulai marak digunakan adalah menggunakan ping ke alamat *broadcast*, ini yang sering disebut dengan *smurf*. Seluruh komputer (*device*) yang berada di alamat broadcast tersebut akan menjawab.

Smurf attack biasanya dilakukan dengan menggunakan *IP spoofing*, yaitu mengubah nomor IP dari datangnya *request*, tidak seperti contoh di atas. Dengan menggunakan *IP spoofing*, respon dari *ping* tadi dialamatkan ke komputer yang IPnya *dispoof*. Akibatnya komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosan penggunaan (bandwidth) jaringan yang menghubungkan komputer tersebut. Dapat dibayangkan apabila komputer yang *dispoof* tersebut memiliki hubungan yang berkecepatan rendah dan ping diarahkan ke sistem yang memiliki banyak host. Hal ini dapat mengakibatkan DoS attack.

```
$ ping 192.168.1.255
PING 192.168.1.255 (192.168.1.255): 56 data bytes
64 bytes from 192.168.1.4: icmp_seq=0 ttl=64 time=2.6 ms
64 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=24.0 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=1 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=2 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=4.7 ms
(DUP!)
64 bytes from 192.168.1.4: icmp_seq=3 ttl=64 time=2.5 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=4.7 ms
(DUP!)
--- 192.168.1.255 ping statistics ---
4 packets transmitted, 4 packets received, +4 duplicates, 0%
packet loss
round-trip min/avg/max = 2.5/6.0/24.0 ms
```




Sniffer

- Program sniffer adalah program yang dapat digunakan untuk menyadap data dan informasi melalui jaringan komputer. Di tangan seorang admin, program sniffer sangat bermanfaat untuk mencari (*debug*) kesalahan di jaringan atau untuk memantau adanya serangan. Di tangan cracker, program sniffer dapat digunakan untuk menyadap password (jika dikirimkan dalam bentuk *clear text*).
- **Sniffit**
- Program sniffit dijalankan dengan userid root (atau program dapat di-setuid root sehingga dapat dijalankan oleh siapa saja) dan dapat menyadap data. Untuk contoh penggunaan sniffit, silahkan baca dokumentasi yang menyertainya. (Versi berikut dari buku ini akan menyediakan informasi tentang penggunaannya.)
- **tcpdump**
- Program tcpdump merupakan program gratis yang umum digunakan untuk menangkap paket di sistem UNIX. Implementasi untuk sistem Window juga tersedia dengan nama *windump*. Setelah ditangkap, data-data (paket) ini dapat diolah dengan program lainnya, seperti dengan menggunakan program *tcpshow*, *tcptrace*, dan sejenisnya.



Sniffer

- **Sniffer Pro**
- Sniffer Pro merupakan program sniffer komersial yang berjalan di sistem Windows. Program ini dibuat oleh Network Associates dan cukup lengkap fasilitasnya. Sniffer Pro dapat menangkap packet dengan aturan-aturan (rules) tertentu. Bahkan dia dilengkapi dengan visualisasi yang sangat menarik dan membantu administrator.
- **Anti Sniffer**
- Untuk menutup lubang keamanan dari kegiatan sniffing, administrator dapat membuat jaringannya bersegmen dan menggunakan perangkat switch sebagai pengganti hub biasa. Selain itu dapat juga digunakan program untuk mendeteksi adanya penggunaan sniffer di jaringan yang dikelolanya. Program pendeteksi sniffer ini disebut anti-sniffer.
- Program anti-sniffer bekerja dengan mengirimkan packet palsu ke dalam jaringan dan mendeteksi responnya. Ethernetcard yang diset ke dalam *promiscuous mode* (yang umumnya digunakan ketika melakukan sniffing) dan program yang digunakan untuk menyadap sering memberikan jawaban atas packet palsu ini. Dengan adanya jawaban tersebut dapat diketahui bahwa ada yang melakukan kegiatan sniffing.

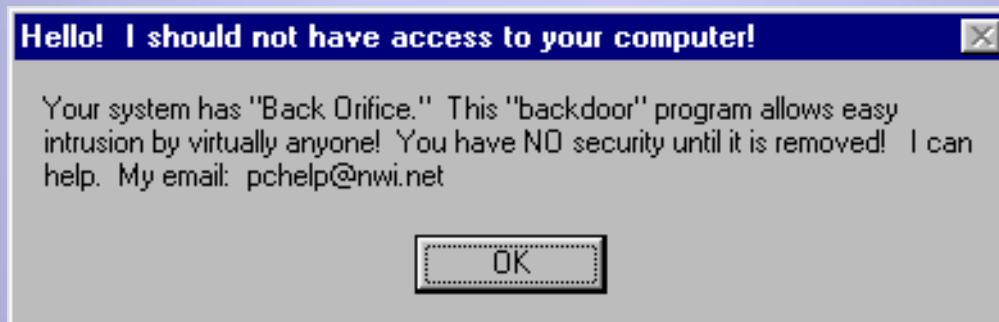


Trojan Horse

- Trojan horse di sistem komputer adalah program yang disisipkan tanpa pengetahuan si pemilik komputer. Trojan horse ini kemudian dapat diaktifkan dan dikendalikan dari jarak jauh, atau dengan menggunakan timer (pewaktu). Akibatnya, komputer yang disisipi trojan horse tersebut dapat dikendalikan dari jarak jauh.
- Ada yang mengatakan bahwa sebetulnya program ini mirip remote administration. Memang sifat dan fungsinya sama. Remote administration / access program seperti pcAnywhere digunakan untuk keperluan yang benar (legitimate). Sementara trojan horse biasanya digunakan untuk keperluan yang negatif.
-

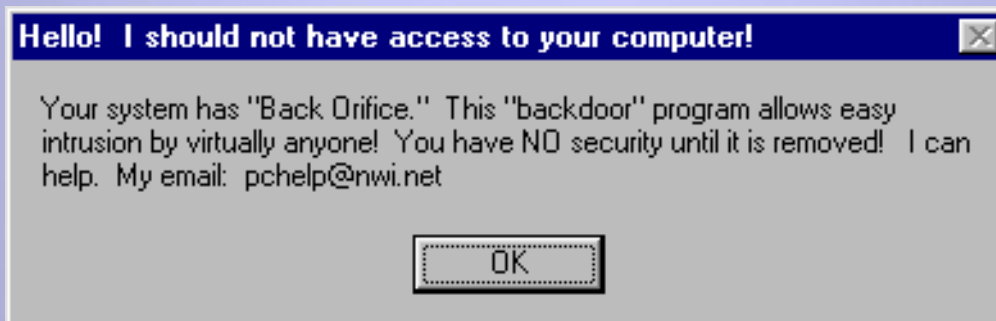
Back Orifice (BO)

- Back Orifice (BO) merupakan trojan horse untuk sistem yang menggunakan operating system Windows (95, 98, NT, 2000). BO Merupakan produk dari Cult of the Dead Cow, pertama kali dikeluarkan 3 Agustus 1998 dan sangat populer di kalangan bawah tanah. Pada saat dokumen ini ditulis, telah keluar BO 2000 untuk sistem operasi Windows 2000.
- BO terdiri dari server (yang dipasang atau disisipkan di komputer target) dan client (yang digunakan untuk mengendalikan server). Akses ke server BO dapat diproteksi dengan menggunakan password sehingga mengecohkan atau membatasi akses oleh orang lain



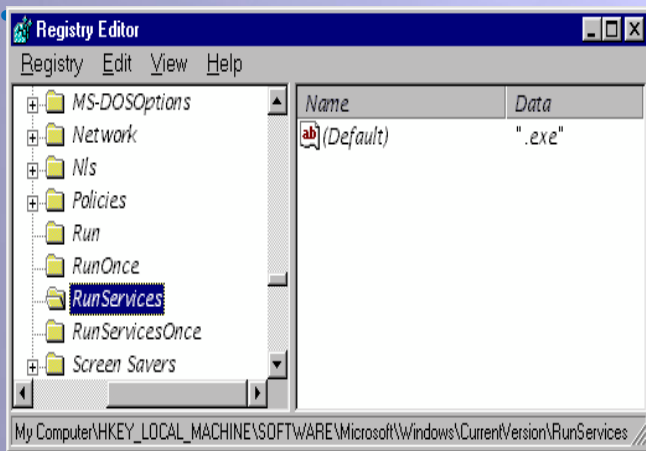
Back Orifice (BO)

- Mengirim pesan mungkin tidak terlalu bermasalah, meskipun mengganggu. Bayangkan jika intruder tersebut memformat harddisk anda atau menangkan keystroke anda (apalagi kalau anda menuliskan userid dan password).
- Server BO menggunakan TCP/IP dan menunggu di port 31337. Jika di komputer anda port tersebut terbuka, ada kemungkinan BO sudah terpasang di sana. Namun, nomor port dari BO dapat dipindahkan ke nomor port lain sehingga mengelabui administrator.



Mendeteksi BO

- Gunakan program "REGEDIT" dan cari *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices*
- Jika variabel tersebut berisi, maka anda sudah terkena BO. Catatan: nama file adalah space-dot-exe. Cek di direktory "Windows\SYSTEM\" jika ada nama file yang kosong atau titik, dan ukurannya (sama dengan atau lebih besar dari) 122KB, kemungkinan itu BO. File tersebut tidak dapat dihapus begitu saja.



Sumber informasi tentang BO dapat diperoleh dari

- <http://www.nwi.net/~pchelp/bo/bo.html>
- <http://www.bo2k.com>
- <http://www.iss.net/xforce/alerts/advise5.html>



NetBus

- NetBus merupakan trojan horse yang mirip Back Orifice. NetBus dapat digunakan untuk mengelola komputer Windows 95/98/NT dari jarak jauh untuk mengakses data dan fungsi dari komputer tersebut. NetBus terdiri dari client dan server. Versi 1.60 dari NetBus server adalah Windows PE file yang bernama PATCH.EXE. Jika dia terpasang (*installed*) maka dia akan langsung dijalankan ketika komputer di"StartUp".
- Porsi dari server NetBus cukup canggih dimana dia menghilangkan jejaknya dari daftar proses yang jalan, dan tidak memperbolehkan dirinya dihapus atau di"rename". Jika server tersebut dijalankan dengan menggunakan "/remove", maka dia akan menghilangkan diri (remove) dari sistem itu. Porsi client digunakan untuk mengendalikan komputer yang sudah terpasang NetBus. Komunikasi dilakukan dengan menggunakan TCP/IP. Client dapat melakukan port scanning untuk mencari dimana server berada. NetBus dapat mengirimkan "keystroke" seolah-olah user yang mengetikkannya di depan layar, dan juga dapat menangkap "keystroke" serta menyimpannya dalam sebuah berkas.
- Pengamanan terhadap serangan NetBus dapat dilakukan dengan menggunakan program Busjacker dan F-Secure. Informasi mengenai NetBus dapat diperoleh di <http://www.netbus.org>.



Merci bien
ありがとう
Matur Nuwun
Hatur Nuhun
Obrigado
Dank
Thanks
Matur se Kelangkong
Syukron
Kheili Mammun
ευχαριστιες
Danke
Grazias
谢谢
Terima Kasih



irawan_afrianto@yahoo.com



[irawan.afrianto](https://www.facebook.com/irawan.afrianto)



[@irawan_afrianto](https://twitter.com/irawan_afrianto)



+628170223513