

Utility untuk Administrator Keamanan

Menggunakan Netcat

Netcat (nc) adalah utility jaringan yang mengizinkan anda untuk membuat koneksi raw socket ke port, data dapat dikirim atau diterima. Nc merupakan alat debug yang mengesankan dan alat eksplorasi yang dapat menjadi 'backend' yang melayani suatu client atau server dengan menggunakan protokol, TCP atau UDP.

Instalasi NETCAT

Petunjuk untuk meng'install Netcat pada sistem anda :

1. Cari source RPM netcat dari <http://www.rpmfind.net>.
2. Download *netcat-version-src.rpm*.
3. Sebagai root, jalankan `rpm -ivh netcat-version-src.rpm`. Ini akan menginstall file tar ball di direktori `/usr/src/redhat/SOURCES`. Jalankan perintah

```
mkdir -p /usr/src/redhat/SOURCES/netcat  
mv /usr/src/redhat/SOURCES/nc*.tgz /usr/src/redhat/SOURCES/netcat
```

Untuk membuat subdirektori netcat di `/usr/src/redhat/SOURCES` dan pindahkan file *ncversion.tgz*.

4. Ubah direktori ke `/usr/src/redhat/SOURCES/netcat`, dari direktori ini, jalankan perintah `tar zxvf ncversion.tgz` untuk meng'ekstrak source'nya.
5. Setelah di ekstrak, jalankan perintah `make linux` untuk meng'compile source code. Jika terjadi kesalahan, coba `make nc`. Jika berhasil anda akan mendapatkan binari baru yaitu nc di direktori ini. Install binari tersebut di direktori binari seperti `/usr/bin` menggunakan perintah

```
cp nc /usr/bin  
chmod 755 /usr/bin/nc
```

Kini anda memiliki binari netcat pada sistem anda. Netcat memiliki kemampuan utama sebagai berikut :

- Koneksi TCP atau UDP ke dan dari port manapun
- Kapabilitas full DNS (*forward/reverse*) lookup
- Kemampuan untuk menggunakan port lokal manapun dan alamat jaringan
- Kemampuan untuk melakukan scanning port
- Kemampuan source-routing
- mode slow-send, satu baris setiap N detik

- Hex dump data yang dikirim dan diterima
- opsional abilliti untuk membolehkan program lainnya membuat koneksi
- Opsional telnet-options responder

Cara termudah menggunakan Netcat adalah dengan menjalankan *nc hostname portnumber*. Ini akan membuat koneksi TCP untuk host dan pada port tersebut. Masih banyak opsi lain yang dapat digunakan. Ketik *nc -h* untuk mengetahui seluruh opsi nya.

Membuat Client/Server Sederhana Menggunakan NC

1. Jalankan perintah pada window shell atau xterm :

```
/usr/bin/nc -l -p 9999 -v
```

Perintah ini menginstruksikan netcat untuk menggunakan port 9999 dan memperlihatkan proses yang terjadi , dan ini merupakan server nya.

Jika anda tidak meng'spesifikasikan nomor port, nc secara otomatis akan mencari port yang tidak dipakai dan menggunakannya untuk koneksi. Lalu opsi -v untuk melihat port mana yang dipakai.

2. Jalankan perintah berikut di window shell yang lain :

```
/usr/bin/nc -v localhost 9999
```

Perintah diatas dijalankan sebagai client nc dengan menggunakan port 9999.

```
listening on [any] 9999 ...
connect to [127.0.0.1] from rhat.nitec.com [127.0.0.1] 1407
```

Hasil data Koneksi berupa Hex dump

Seringkali merupakan ide yang bagus melihat hasil hex dump pada saat terjadi komunikasi di jaringan sehingga dapat terlihat dengan lengkap data yang dikirim dan diterima. Dengan *nc* anda dapat melakukannya dengan opsi -o. Sebagai contohnya :

```
/usr/bin/nc -v localhost 25 -o /tmp/smtp.hex
```

Dengan perintah ini akan menghubungkan ke lokal SMTP server di port 25 dan mencatat data yang masuk dan keluar di */tmp/smtp.hex* dalam hex format. Sebagai contoh, contoh sesi singkat nya yaitu :

```
220 rhat.nitec.com ESMTP Sendmail 8.11.0/8.11.0; Tue, 27 Mar 2001 10:50:57 -0800
helo domain.com
250 rhat.nitec.com Hello IDENT:kabir@rhat.nitec.com [127.0.0.1], pleased to meet
you
quit
```

221 2.0.0 rhat.nitec.com closing connection

Setelah terhubung ke lokal STMP server melalui nc, ketikkan perintah helo, maka server akan merespon dengan sambutan, lalu ketikkan perintah quit untuk log out. Data yang dikumpulkan di simpan di `/tmp/sntp.hex` terlihat seperti di bawah ini :

```
< 00000000 32 32 30 20 72 68 61 74 2e 6e 69 74 65 63 2e 63 # 220 rhat.nitec.c
< 00000010 6f 6d 20 45 53 4d 54 50 20 53 65 6e 64 6d 61 69 # om ESMTP Sendmai
< 00000020 6c 20 38 2e 31 31 2e 30 2f 38 2e 31 31 2e 30 3b # | 8.11.0/8.11.0;
< 00000030 20 54 75 65 2c 20 32 37 20 4d 61 72 20 32 30 30 # Tue, 27 Mar 200
< 00000040 31 20 31 30 3a 35 30 3a 35 37 20 2d 30 38 30 30 # 1 10:50:57 -0800
< 00000050 0d 0a # ..
> 00000000 68 65 6c 6f 20 64 6f 6d 61 69 6e 2e 63 6f 6d 0a # helo domain.com.
< 00000052 32 35 30 20 72 68 61 74 2e 6e 69 74 65 63 2e 63 # 250 rhat.nitec.c
< 00000062 6f 6d 20 48 65 6c 6c 6f 20 49 44 45 4e 54 3a 6b # om Hello IDENT:k
< 00000072 61 62 69 72 40 72 68 61 74 2e 6e 69 74 65 63 2e # abir@rhat.nitec.
< 00000082 63 6f 6d 20 5b 31 32 37 2e 30 2e 30 2e 31 5d 2c # com [127.0.0.1],
< 00000092 20 70 6c 65 61 73 65 64 20 74 6f 20 6d 65 65 74 # pleased to meet
< 000000a2 20 79 6f 75 0d 0a # you..
> 00000010 71 75 69 74 0a # quit.
< 000000a8 32 32 31 20 32 2e 30 2e 30 20 72 68 61 74 2e 6e # 221 2.0.0 rhat.n
< 000000b8 69 74 65 63 2e 63 6f 6d 20 63 6c 6f 73 69 6e 67 # itec.com closing
< 000000c8 20 63 6f 6e 6e 65 63 74 69 6f 6e 0d 0a # connection..
```

Perintah nc tercetak tebal.

- Baris yang dimulai dengan karakter < menyatakan data yang diterima nc dari remote server.
- Baris yang dimulai dengan karakter > menyatakan data dihasilkan oleh pemakai lokal nc.

Port Scanner Menggunakan nc

Anda dapat menggunakan nc sebagai port scanner dengan menjalankan nc seperti berikut :

```
/usr/bin/nc -v -w 2 -z hostname port_range
```

- `-w` : timeout dalam detik setelah terjadi koneksi
- `-z` : zero I/O mode untuk scanning, dimana mencegah pengiriman data ke koneksi TCP dan membatasi probing data ke koneksi UDP.
- `port_range` : range port, misal 1-1024. Contohnya :

```
/usr/bin/nc -v -w 2 -z rhat.nitec.com 1-1024
```

Perintah ini akan meng'scan port dari 1-1024 pada sistem `rhat.nitec.com`. Contohnya :

```
rhat.nitec.com [127.0.0.1] 1024 (?) open
rhat.nitec.com [127.0.0.1] 587 (?) open
rhat.nitec.com [127.0.0.1] 515 (printer) open
rhat.nitec.com [127.0.0.1] 514 (shell) open
rhat.nitec.com [127.0.0.1] 513 (login) open
```

```
rhat.nitec.com [127.0.0.1] 139 (netbios-ssn) open
rhat.nitec.com [127.0.0.1] 113 (auth) open
rhat.nitec.com [127.0.0.1] 111 (sunrpc) open
rhat.nitec.com [127.0.0.1] 80 (www) open
rhat.nitec.com [127.0.0.1] 79 (finger) open
rhat.nitec.com [127.0.0.1] 53 (domain) open
rhat.nitec.com [127.0.0.1] 25 (smtp) open
rhat.nitec.com [127.0.0.1] 23 (telnet) open
rhat.nitec.com [127.0.0.1] 22 (ssh) open
rhat.nitec.com [127.0.0.1] 21 (ftp) open
```

Serperti yang terlihat nc memperlihatkan sejumlah port yang terbuka. Jika anda ingin memperlambat scanning, gunakan opsi -i detik untuk meng'delay tiap scan dengan menentukan detiknya. Untuk scan dengan range port multiple yaitu :

```
/usr/bin/nc -v -w 2 -z rhat.nitec.com 20-50 100-300
```

perintah diatas akan meng'scan port antara 20-50 dan 100-300 saja.

File Transfer Sederhana dengan nc

1. Jalankan nc di mesin dimana anda akan menerima satu atau lebih files, sebagai berikut :

```
/usr/bin/nc -l -p port_number | /bin/tar xvzfp -
```

2. Ubahlah nomor port, misalnya 1024. Contohnya :

```
/usr/bin/nc -l -p 9999 | /bin/tar xvzfp -
```

Host yang menerima menggunakan port 9999, data yang diterima nc dilewatkan ke program tar, dimana meng'ekstrak data dari STDIN dan menulis file ke disk.

3. Pada mesin pengirim, jalankan perintah berikut.

```
/bin/tar cvzfp - path | /usr/bin/nc -w 3 receiver_host 9999
```

Ubah 'path' ke path name direktori yang ingin di transfer, dan receiver_host menjadi host yang akan menerima data. Contohnya :

```
/bin/tar cvzfp - /etc | /usr/bin/nc -w 3 rhat.nitec.com 9999
```

Perintah ini akan meng'transfer semua file yang berada di direktori /etc ke rhat.nitec.com melalui port 9999.

Referensi : RedHat Linux Security and Optimization - Oreilly

Mohammed J. Kabir

Semoga Bermanfaat - Faiz :-)