netcat

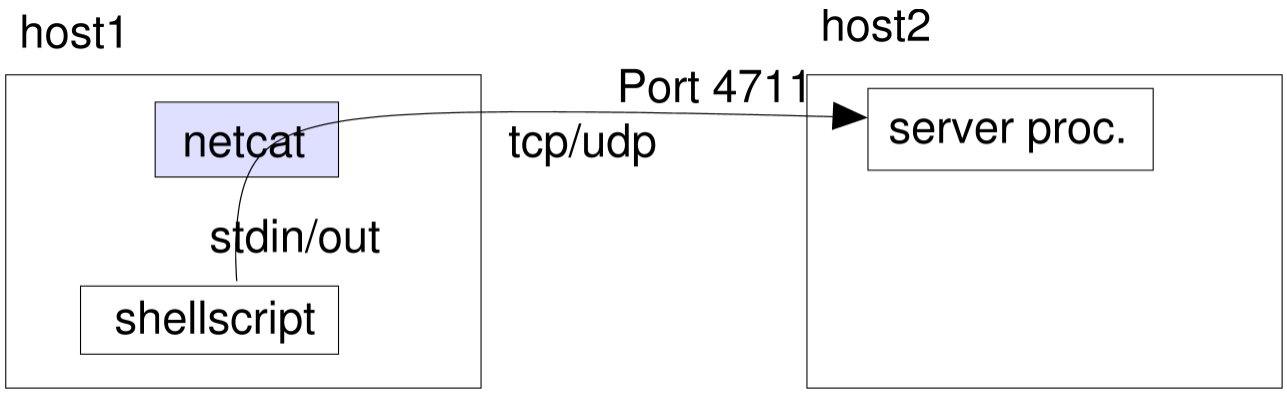
Tuguldur BiBO <tugldr@yahoo.com>

Гарчиг

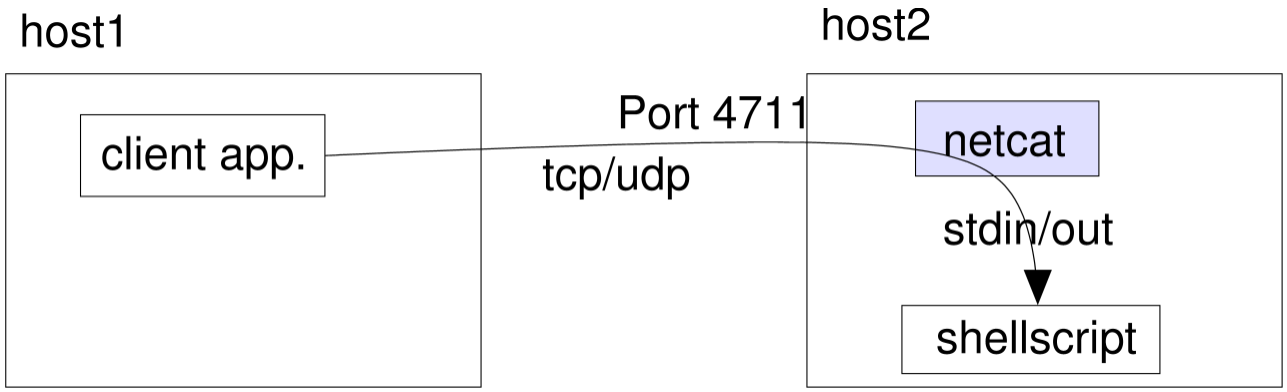
Хэрэглээ

Netcat нь tcp эсвэл udp Холболтыг stdin/out-р дажуулан хийнэ. Удирдах талбар нь Schellscript мөн MS-DOS байх болно.

Netcat нь холболтыг (удирдах) өөрөө хийж чадна (Client-Modus):



эсвэл холбуулагч (удирдуулагч) (Server-Modus):



Мөн netcat нь Clientmodus-с Port хайгчаар ажилна.

Client (Удирдагч)-аас холбогдох нь

Webserver-тэй холбогдох

Жишээ: Schell эсвэл MS-Dos-с Telnet-дэд холбогдох үед холбогдоод ямар нэг үйлдэл хийхэд тухайн Server-тэй холбоо тасардаг:

```
$ printf 'GET / HTTP/1.0\n\n'  | telnet www.jfranken.de 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Connection closed by foreign host.
$
```

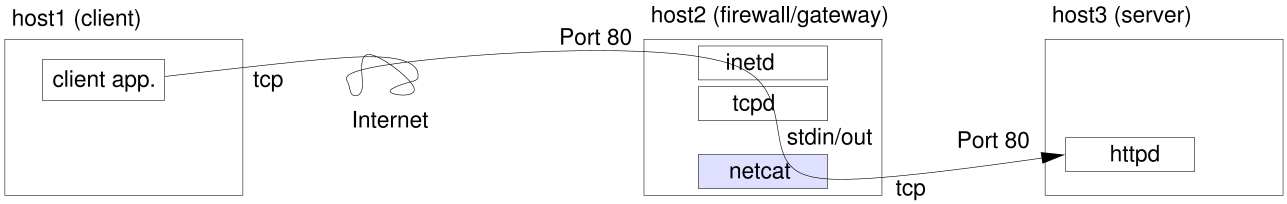
Тэгвэл netcat–тай бол:

```
$ printf 'GET / HTTP/1.0\n\n'  | netcat -w 10 www.jfranken.de 80
HTTP/1.0 200 OK
Server: thttpd/2.21b 23apr2001
Content-Type: text/html; charset=iso-8859-1
[...]
<HTML>
```

```
[...]
</HTML>
```
Холбоо тасарсаны дараа netcat дуусаж байна. Parameter –w 10 энд үйлчилэж байна. 10 сек гэсэн үг юм.

Port дамжуулах

Netcat-р inetd–г ашиглан local Port–г өөр Host–р дамжуулаж болно.



Жишээ нь Shell дээр `/etc/inetd.conf` host2-р холбогдон Port 80-ийг host3-руу lokal болгож байна:
```
80 stream tcp nowait nobody /usr/bin/nc /usr/bin/nc -w 3 host3 80
```
Хэрэв Protokoll хийхээр бол эхний `/usr/bin/nc` гэдэгийг `/usr/sbin/tcpd` болго.

Ямар Software DNS-Server ажиллаж байгааг мэдэх

Гаднаас нь ямар Software DNS-server ажиллаж байгааг мэдэж болно.
```
$ dig @pns.dtag.de version.bind. txt CHAOS|grep "^V"
VERSION.BIND.           0S CHAOS TXT    "BIND 8.3.4"
```
Мөн bash хэрэглэж болно.
```
$ whatdns() {
   printf 'begin-base64 644 -\np8IBAAABAAAAAAAAB3ZlcnNpb24EYmluZAAAAEAADCg==\n====='|
   uudecode| nc -uw 1 $1 domain | strings| tail -1; }
$ whatdns pns.dtag.de
BIND 8.3.4
$ whatdns 141.2.1.1
4.9.7
```

Server-ийн өмнөөс дуудах

Хэрэв би
```
PROGRAM | nc -l -p PORT -w TIMEOUT
```
эсвэл
```
nc -l -p PORT -w TIMEOUT | PROGRAM
```
дуудхад,

1. Netcat яг энэ Port-р холболт үүсгэнэ `PORT`
2. Энэ Program-р холбогдоно `PROGRAM`
3. `TIMEOUT` Сек хүлээнэ холболт тасартал

1024 Port-р бол root байх ёстой.

Харамсалтай нь netcat-р Program-н Parameter шууд өгөж болдогүй харин 2 мөр Schellscript оруулан орлуулаж болно.

Хамгийн сүүлд холболт тасархад зөвхөн ганц холболт ашиглах л үлдэнэ. Хэрэр олон холболт үүсгэх бол дараалал эсвэл зэрэг холболт хий Энэ 3 мөр Schellscript ашиглан:

```
$ cat <<EOF>mydemon
#!/bin/bash
export port=${port:-$1} # inherit $1 as $port
nc -l -p $port -e $0 &  # await further connections on this port
```

```
[ $1 ]|| PROGRAM        # do the work (not for the first invocation)
EOF
$ chmod +x mydemon
$ ./mydemon 3000
$
```

Parameter `-e` зөвхөн netcat `-DGAPING_SECURITY_HOLE` compile хийсэн тохиолдолд.

Shell-р удирдах

Энэ Shellscript daemon shell-р холбогдон удирдаж болно:

```
#!/bin/bash
#BiBO

# on first invocation, export $PW and $port to subshells
export PW port
if [ $1 ] ; then
        port=$1
        echo -n pass:
        read PW
fi

# do we know the port to listen on?
if [ ! $port ]; then
        echo USAGE: $0 port ;
        exit;
fi

# wait for further connections (veiling params)
echo "-l -p $port -e $0" | nc 2>/dev/null &
[ $1 ] && exit; # first invocation exit here

# ask for password
unset p
until [ "$p" = "$PW" ]; do
        echo -n pass:
        read p
done

# received good password. present a shell
bash --noediting -i
```

Хэрэв түлхүүр үг асуувал,

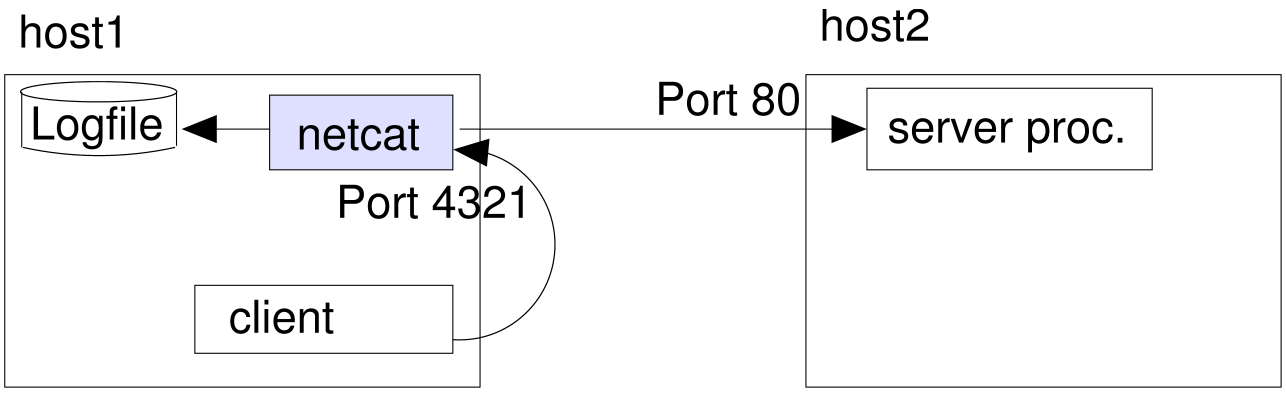
```
bibo@tp:~$ ./pershd 1234
pass:secret
bibo@tp:~$
```

Энэ түлхүүр үгээр өөр Com-с өррийнхөө Com-н Shell холбогдоно:

```
$ nc tp.bibo.org 1234
pass:secret
bibo@tp:~$
bibo@tp:~$ exit
exit
$
```

Network сүлжээг чагнах

Sniffer-тай адил жишээ нь `tcpdump`, `snoop`, `iptraf` мөн `ethereal`. Netcat-р Sniffer хийж болно.




```
$ cat <<EOF>mydemon
#!/bin/bash
export port=${port:-$1} # inherit $1 as $port
nc -l -p $port -e $0 &  # await further connections on this port
[ $1 ]|| PROGRAM        # do the work (not for the first invocation)
EOF
$ chmod +x mydemon
$ ./mydemon 3000
$
```

`PROGRAM` ашиглан

```
netcat -o /tmp/sniffer.`date +%s.$$` tp.bibo.org 80
```

netcat одоо Logfile `/tmp` дотор үүсгэнэ

Жишээ: Би өөрийнхөө `http://localhost:4321` дуудахад энхүү Logfile үүсэв:

```
$ cat /tmp/sniffer.1045474262.5864
> 00000000 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a # GET /
HTTP/1.1..
> 00000010 55 73 65 72 2d 41 67 65 6e 74 3a 20 4f 70 65 72 # User-Agent:
Oper
> 00000020 61 2f 36 2e 31 31 20 28 4c 69 6e 75 78 20 32 2e # a/6.11 (Linux
2.
[...]
< 00000000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d # HTTP/1.1 200
OK.
< 00000010 0a 53 65 72 76 65 72 3a 20 74 68 74 74 70 64 2f # .Server:
thttpd/
< 00000020 32 2e 32 31 62 20 32 33 61 70 72 32 30 30 31 0d # 2.21b
23apr2001.
< 00000030 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 # .Content-Type:
t
[...]
< 00002180 0a 3c 2f 46 52 41 4d 45 53 45 54 3e 0a 3c 2f 48 #
.</FRAMESET>.</H
< 00002190 54 4d 4c 3e 0a                                 # TML>.
```

Folder-н бүтэц(мод) Internet-р хуулах

Netcat, (gnu)tar мөн bash ашиглан Folder-н бүтэцийг хуулаж авч болно.Хуулахдаа Attribute (Эрх/Хугцаа)-тай нь илгээнэ.

Жишээ Port 51330 ашиглаж:

```
$ alias receive='nc -vlp 51330 | tar xzvp'
$ receive
listening on [any] 51330 ...
```

Одоо илгээх:

```
$ send() {j=$*; tar cpz ${j/%${!#}/}|nc -w 1 ${!#} 51330;}
$ send dir* tp.bibo.org
```

Bash-o-magic:

- `${!#}` Parameter бол Host нэр,
- `${j/%${!#}/}` үлдсэн нь (File мөн Folder).

Portscanner

Port хайх:

```
nc -vz PARAMETER host PORTRANGES
```

`PARAMETER`:

Parameter	Bedeutung
`-v`	Хаалттай Port харуулах
`-w` <Sek>	Үргэлжлэх хугцаа
`-u`	udp оронд tcp. `-w` Хэргэлсэн нь дээр
`-r`	Port-г замбраагүй харуулах
`-i` <Sekunden>	Завсарлах тасарсан тохиолдолд дахин холбогдох

Жишээ:

```
$ nc -vz www.bibo.org 1-1024
www.jfranken.de [195.88.176.20] 443 (https) open
www.jfranken.de [195.88.176.20] 110 (pop3) open
www.jfranken.de [195.88.176.20] 80 (www) open
www.jfranken.de [195.88.176.20] 53 (domain) open
www.jfranken.de [195.88.176.20] 25 (smtp) open
www.jfranken.de [195.88.176.20] 22 (ssh) open
$
$ nc -vz -vur -i 1 -w 2 localhost 1024 108-112
localhost [127.0.0.1] 1024 (?) open
localhost [127.0.0.1] 109 (pop2) : Connection refused
localhost [127.0.0.1] 112 (?) : Connection refused
localhost [127.0.0.1] 111 (sunrpc) open
localhost [127.0.0.1] 110 (pop3) : Connection refused
localhost [127.0.0.1] 108 (?) : Connection refused
 sent 0, rcvd 0
```

Бусад Parameter

-v : Алдаа болон мэдээлэл хэвлэдэг.
-p portarg : Өөрийн port-оо үзэх, 512-1023 port үзээрэй
-w : Мэдээ дамжуулах хязгаар тогтооно -w 2 : гэсэн тохиолдолд 2 удаа давталт хийнэ
-z : TCP/UDP Мэдээлэл дажуулахаас сэргийлнэ.
-r : Эмх цэгцгүй замбраагүй хайлт хийх
-g : router дамжин олон төрлийн холболт хийнэ.
-i : scan хийхэд завсарлага авна
-u : UDP холболт хийнэ
-s : source хаяг
-e : exe-г ажилуулна

http://www.tuguldur.tk
BiBO 2005