[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@417ad3cebe76499aaa283073b7edf91f?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view" \l "main)

**Banner Grabbing Using Netcat**

Netcat is one of those few tools like [nmap](https://www.yeahhub.com/about-nmap-network-mapper/), [Metasploit](https://www.yeahhub.com/metasploit-framework-post-exploitation-tool-hackers-favorite-tool/), Wireshark and few others that every hacker should be familiar with. It is simple, elegant and has a multitude of uses.

For instance, netcat can be used to;

* Ability to scan if a port is open on a remote system
* Pull the banner information from a remote system
* Connect to a network service manually with listening
* Remote administration for transferring of files

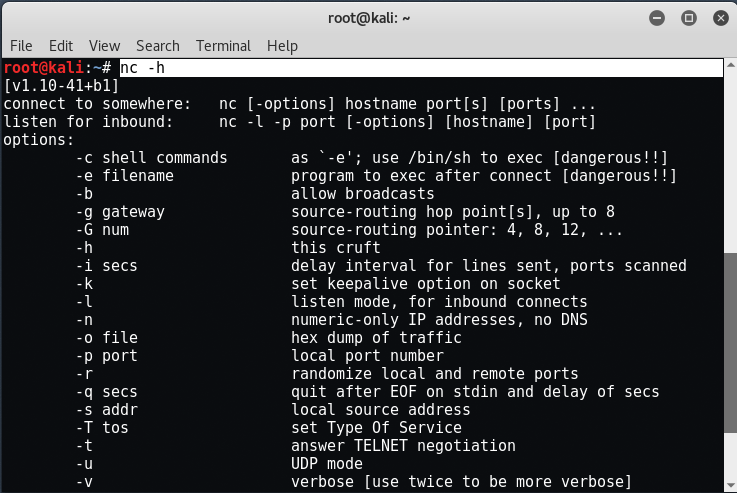
Like so many applications in the Linux world, netcat runs in a client and server mode. This means that we must designate one side the server and one side the client, when using netcat.

Here in this case, we are using two machines, one is Kali Linux 2017.1 VM in which netcat is pre-installed and other is Windows 10, which is our base machine where we installed netcat in C:\ directory with directory named “nc“.

**Netcat Basics**

Let’s start off by looking at the help screen for netcat. When using netcat, the command is simply “nc“. To get the help screen then, type;

Command: nc -h



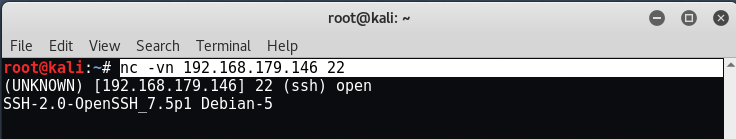
Note a few key switches;

* -e program to execute after connect
* -l listen mode for inbound connects
* -p designates the locat port
* -u UDP mode
* -v verbose output

**Create a Simple TCP Connection**

Netcat be used to create simple TCP or UDP connection to system to see whether the port and service available. So, for instance, if we wanted to connect to the SSH on remote system, we can type;

Command: nc -vn 192.168.179.146 22



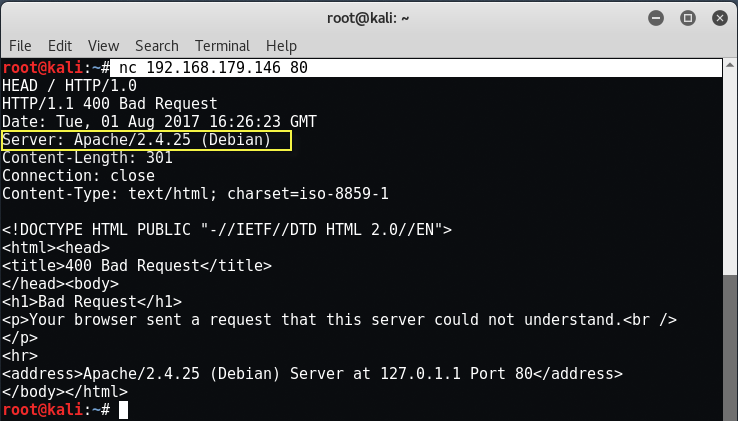
As you can see, netcat was able to connect to OpenSSH on a remote server and it advertised the service with its banner along with the openssh server version which might be useful for an attacker.

**Banner Grabbing**

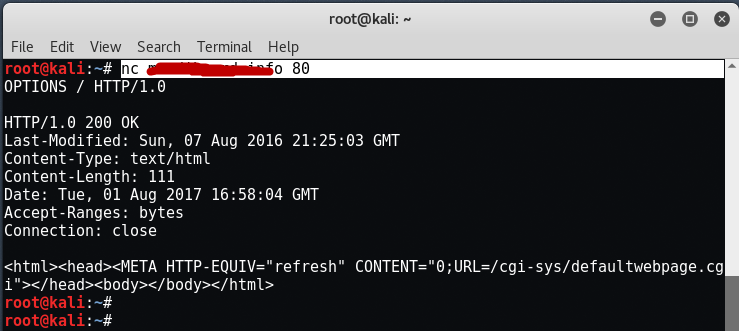
We can also use netcat to “grab” the banner on web servers by connecting to port 80 and then sending a HEAD / HTTP/1.0 or HEAD / HTTP/1.1 request depending upon the protocol which they’re using.

Command: nc 192.168.179.146 80

HEAD / HTTP/1.0



Make certain to hit “Enter” a couple times after typing the HEAD request to pull the banner. As you can see, we grabbed the banner of Apache 2.4.25 web server running on Debian. Through this method, you can even find the open HTTP methods against the target like CONNECT, DELETE, DEBUG, OPTIONS, PUT etc.



**Opening TCP connection between two machines for “chat”**

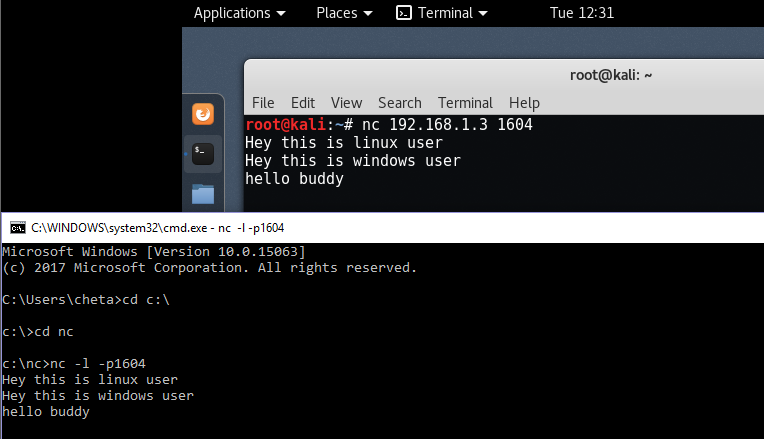
Netcat is capable of creating a simple TCP or UDP connection between two computers and then open a communication channel between them. Let’s open a listener on the remote system first i.e. on Windows 10 machine.

Command: nc -l -p1604

Then connect to that listener in Kali Linux from a remote machine by typing the below command.

Command: nc 192.168.1.3 1604

When it connects, we can then begin typing my message.



That message will then appear on the remote system with the listener. The listener machine can then respond and then the remote machine can respond. In this way, we can create a private “chat room” between any two machines!

**Transferring Files with Netcat**

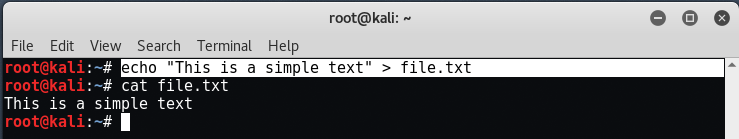
One of the simple wonders of netcat is its ability to transfer files between computers. By creating this simple connection, we can then use that connection to transfer files between two machines. This can be extremely useful as a network administrator and even more useful as a hacker. Netcat can be used to upload and download files from and to the target system.

Let’s create a file called “file.txt” by typing the below command.

Command: echo “This is a simple text” > file.txt

Then, let’s view the contents of that file using the Linux command “cat“.

Command: cat file.txt

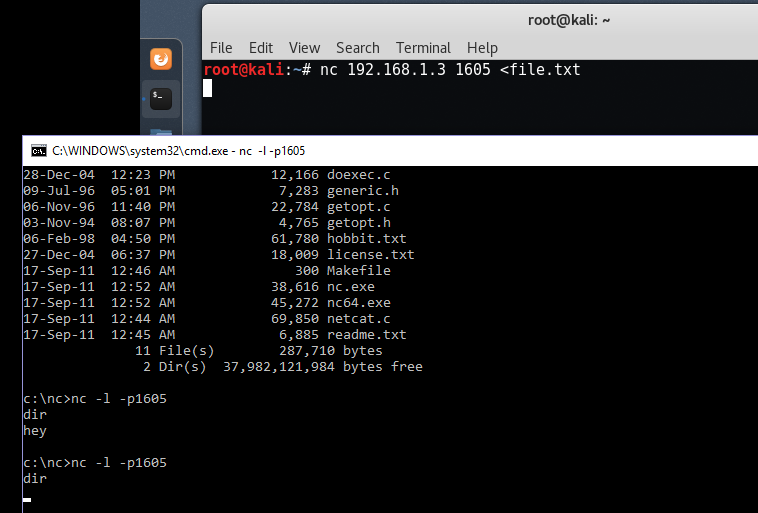


Now, let’s open a listener on the remote system i.e. on a windows machine by typing the below command.

Command: nc -l -p1605

Next, let’s send the file to the remote system from Kali Linux to Windows 10.

Command: nc 192.168.1.3 1605 < file.txt



Note, that we use the < to direct the file to netcat. ? Finally, go back to our listening system and we should find that the file has been transferred and appears on screen!