otw
Jan 22, 2021 5 min

Netcat- the All-Powerful Linux Utility

Welcome back, my aspiring cyberwarriors!

Netcat is one of those few tools--like nmap, Metasploit, 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;

- scan to see if a port is open on a remote system
- pull the banner from a remote system
- connect to a network service manually
- remote administration

This lesson will be dedicated to learning to use netcat and its encrypted cousin, cryptcat. Later in your studies, we will find many more uses for this simple tool.

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.

Step #1: 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;

kali > nc -h

```
kali@kali:~$ netcat -h
[v1.10-41.1+b1]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -c shell commands       as `-e'; use /bin/sh to exec [dangerous!!]
        -e filename             program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -k                      set keepalive option on socket
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -T tos                  set Type Of Service
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -C                      Send CRLF as line-ending
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-data').
```

Note a few key switches;

- -e execute
- -l listen mode
- -n numeric IP address mode (no DNS. Its faster)
- -p designates the port
- -u UDP mode
- -v verbose output

Step #2: 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 I wanted to connect to the SSH on another Linux system, I can type;

kali > nc -vn 192.168.1.103 22

```
kali@kali:~$ nc -vn 192.168.42.26 22
(UNKNOWN) [192.168.42.26] 22 (ssh) open
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu4
```

As you can see, netcat was able to connect to OpenSSH on a remote server and the server advertised the service with its banner
(SSH-2.0-OpenSSH_5.3p1 Debian-3Ubuntu4).

Step #3: Banner Grabbing

We can also use netcat to "grab" the banner on web servers by connecting to port 80 and then sending a HTTP / HEAD/1.0 request.

kali > nc -vn 192.168.42.26 80

```
kali@kali:~$ nc -vn 192.168.42.26 80
(UNKNOWN) [192.168.42.26] 80 (http) open
```

HEAD / HTTP/1.0

Make certain to hit "Enter" a couple times after typing the HEAD request to pull the banner.

```
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 20 Jan 2021 13:47:58 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod
_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.10
.1
Last-Modified: Fri, 31 Jul 2015 02:55:52 GMT
ETag: "45f13-6da3-51c22f5365e00"
Accept-Ranges: bytes
Content-Length: 28067
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

As you can see, we grabbed the banner of Apache 2.2.14 web server running on Ubuntu. In addition, the banner reveals the versions PHP, Python, OpenSSL, and Perl running on this system

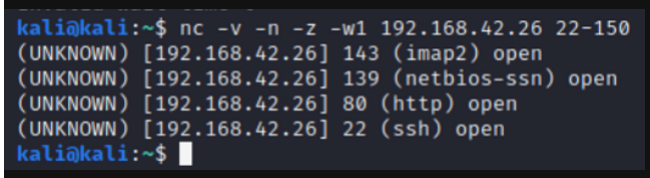
Step #4 Port Scanning with netcat

Netcat is capable of so many tasks. Among those is the port scan. You are already familiar with nmap the most widely used port scanner. Netcat can do something very similar without all the bells and whistles of nmap.

To run a port scan with netcat, enter;

kali > nc -v -n -z -w1 192.168.42.26 22-150

Where:
- nc is the netcat command
- -v means provide verbose (wordy) output
- -n means numeric only IP addresses (no DNS)
- -z means zero. This is non input/output mode
- -w1 means wait one second for connects



As you can se above, netcat was able to find each of the open ports on the remote system and tell us the default service running on that port.

Step #5: 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. A listener is opened by simply entering the netcat command (nc) followed -l (listen) and the port number you want to listen for connections on (in this case, let's try listening on port 4294, but you can use any port).

kali > nc -l -p4294

Then connect to that listener from a remote machine

kali > nc 192.168.100.111 4294

When it connects, I can then begin typing my message, such as "What is the Best Place to learn cybersecurity?"

```
root@kali-2019:~# nc 192.168.100.111 4294
What is the Best Place to cybersecurity?
```

That message will then appear on the remote system with the listener. The person the listener machine can then respond, "Undoubtedly, it is Hackers-Arise.com!"

```
kali@kali:~$ nc -l -p4294
What is the Best Place to cybersecurity?
Undoubtedly, it is Hackers-Arise.com!
```

...and then the remote machine receives the response!

```
root@kali-2019:~# nc 192.168.100.111 4294
What is the Best Place to cybersecurity?
Undoubtedly, it is Hackers-Arise.com!
```

In this way, we can create a private "chat room" between any two machines!

Step #5: 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 computers. 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 "hackers-arise".

kali > echo "Hackers-Arise is the best and most affordable place to study cybersecurity" > hackers-arise

Then, let's view the contents of that file using the Linux command "cat".

kali > cat hackers-arise

```
root@kali-2019:~# echo "Hackers-Arise.com is the best and most affordable place
to study cybersecurity">hackers-arise
root@kali-2019:~# cat hackers-arise
Hackers-Arise.com is the best and most affordable place to study cybersecurity
```

Now, let's open a listener on the remote system.

kali > nc -l -p4294

Next, let's send the file to the remote system.

kali > nc 192.168.100.111 4294 <hackers-arise

```
root@kali-2019:~# nc 192.168.100.111 4294 < hackers-arise
```

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 the screen!

```
kali@kali:~$ nc -l -p4294
Hackers-Arise.com is the best and most affordable place to study cybersecurity
```

Step #6: Remote Administration with netcat

Probably the most malicious use of netcat-- and the most effective for the hacker --is the ability to use netcat for remote administration. We can use netcat's ability to execute commands by a remote connection to a shell (/bin/sh) on the listening system. We can do this in a Linux/Unix machine by making /bin/sh available to the remote connection with the -e (execute), like below. If we were connecting to a Windows machine, we could use cmd.exe (-e cmd.exe) instead of /bin/sh.

kali > nc -l -p4294 -e /bin/sh

Now when I connect to the remote machine, I should be able to get a shell on the remote system. Notice that when I connect to the remote system, I get just a blank line, no command prompt, nothing (if we connect to a Windows system, though, we will get the traditional Windows C: > prompt). This can be confusing to the novice.

If we then type "ls -l" , we get a directory listing from the directory that where we started the netcat listener on the remote system.

```
root@kali-2019:~# nc 192.168.100.111 4294
ls -l
total 713656
drwxr-xr-x 2 kali kali      4096 Sep 29 13:23 armitage-tmp
drwxr-xr-x 2 kali kali      4096 May  8  2020 Desktop
drwxr-xr-x 2 kali kali      4096 May  8  2020 Documents
drwxr-xr-x 2 kali kali      4096 Nov 30 13:09 Downloads
drwxr-xr-x 2 kali kali      4096 Sep 28 19:30 hackers-Arise
drwxr-xr-x 2 kali kali      4096 Sep 28 19:30 Hackers-Arise
-rw-r--r-- 1 kali kali     76434 Aug 28 14:46 HackersAriseMalwareApp.apk
-rw-r--r-- 1 kali kali        92 Sep 28 19:40 hackers-arise_pentest.csv
-rw-r--r-- 1 kali kali      1645 Sep 28 19:41 hackers-arise_services.csv
-rwxr-xr-x 1 kali kali      3482 Oct 20 16:23 HackersAriseWiFiScanner
drwxr-xr-x 8 kali kali      4096 Aug  4 14:06 hcxdumptool
drwxr-xr-x 6 kali kali      4096 Aug  4 14:06 hcxtools
```

Then, we can enter pwd to get the present working directory and whoami to find the user whose permissions we are using (kali, in this case).

```
pwd
/home/kali
whoami
kali
```

Step #7: Cryptcat

Cryptcat is netcat's encrypted cousin. This means that we can make a connection to a remote machine where all our traffic is encrypted with some of the strongest encryption algorithms available anywhere, Two-fish (Two-fish encryption is nearly as strong as AES). You can download it at www.cryptcat.sourceforge.net, but if you are using Kali, it is already installed. Although the switches are largely the same as netcat, the command is "cryptcat" rather than "nc".

Summary

Netcat, like Metasploit, nmap, and Wireshark, is a key tool for the hacker and network administrator alike. It's versatility makes it an essential tool for multiple purposes.