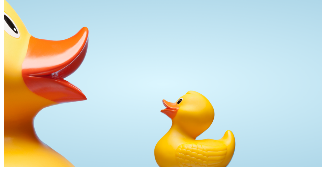
by Pradeep Kumar Published December 6, 2017 Updated February 6, 2020

ncat or **nc** is networking utility with functionality similar to cat command but for network. It is a general purpose CLI tool for reading, writing, redirecting data across a network. It is designed to be a reliable back-end tool that can be used with scripts or other programs. It's also a great tool for network debugging, as it can create any kind of connect one can need.

ncat/nc can be a port scanning tool, or a **security tool**, or **monitoring tool** and is also a simple **TCP proxy**. Since it has so many features, it is known as a network swiss army knife. It's one of those tools that every System Admin should know & master.



In most of Debian distributions 'nc' is available and its package is automatically installed during installation. But in minimal CentOS 7 / RHEL 7 installation you will not find nc as a default package. You need to install using the following command.

```
[root@linuxtechi ~]# yum install nmap-ncat -y
```

System admins can use it audit their system security, they can use it find the ports that are opened & than secure them. Admins can also use it as a client for auditing web servers, telnet servers, mail servers etc, with 'nc' we can control every character sent & can also view the responses to sent queries.

We can also cause it to capture data being sent by client to understand what they are upto.

In this tutorial, we are going to learn about how to use 'nc' command with 10 examples,

Example: 1) Listen to inbound connections

Ncat can work in listen mode & we can listen for inbound connections on port number with option 'l'. Complete command is,

$ ncat -l port_number

For example,

```
$ ncat -l 8080
```

Server will now start listening to port 8080 for inbound connections.

Most Popular Post

How to Extend EBS Boot Disk of EC2 Instance without Reboot

How to Add and Delete Static Route in Linux using IP Command

9 'diff' Command Examples in Linux

How to Use When Conditionals Statement in Ansible Playbook

20 ps Command Examples to Monitor Linux Processes

How to Sync Time in Linux Server using Chrony

How to Integrate Grafana with Prometheus for Monitoring

Example: 2) Connect to a remote system

To connect to a remote system with nc, we can use the following command,

$ ncat IP_address port_number

Let's take an example,

```
$ ncat 192.168.1.100 80
```

Now a connection to server with IP address 192.168.1.100 will be made at port 80 & we can now send instructions to server. Like we can get the complete page content with

GET / HTTP/1.1

or get the page name,

GET / HTTP/1.1

or we can get banner for OS fingerprinting with the following,

HEAD / HTTP/1.1

This will tell what software is being used to run the web Server.

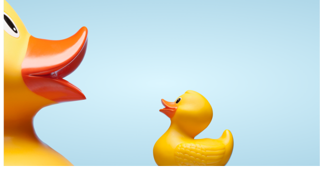
Example: 3) Connecting to UDP ports

By default , the nc utility makes connections only to TCP ports. But we can also make connections to UDP ports, for that we can use option 'u',

```
$ ncat -l -u 1234
```

Now our system will start listening a udp port '1234', we can verify this using below netstat command,

```
$ netstat -tunlp | grep 1234
udp           0          0 0.0.0.0:1234                 0.0.0.0:*               17341/nc
udp6          0          0 :::1234                      :::*                    17341/nc
```



Let's assume we want to send or test UDP port connectivity to a specific remote host, then use the following command,

$ ncat -v -u {host-ip} {udp-port}

example:

```
[root@localhost ~]# ncat -v -u 192.168.105.150 53
Ncat: Version 6.40 ( http://nmap.org/ncat )
Ncat: Connected to 192.168.105.150:53.
```

Example: 4) NC as chat tool

NC can also be used as chat tool, we can configure server to listen to a port & than can make connection to server from a remote machine on same port & start sending message. On server side, run

```
$ ncat -l 8080
```

On remote client machine, run

```
$ ncat 192.168.1.100 8080
```

Than start sending messages & they will be displayed on server terminal.

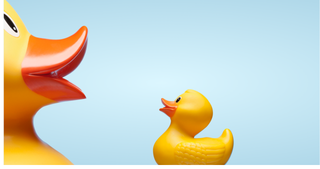
Example: 5) NC as a proxy

NC can also be used as a proxy with a simple command. Let's take an example,

```
$ ncat -l 8080 | ncat 192.168.1.200 80
```

Now all the connections coming to our server on port 8080 will be automatically redirected to 192.168.1.200 server on port 80. But since we are using a pipe, data can only be transferred & to be able to receive the data back, we need to create a two way pipe. Use the following commands to do so,

```
$ mkfifo 2way
$ ncat -l 8080 0<2way | ncat 192.168.1.200 80 1>2way
```



Now you will be able to send & receive data over nc proxy.

Example: 6) Copying Files using nc/ncat

NC can also be used to copy the files from one system to another, though it is not recommended & mostly all systems have ssh/scp installed by default. But none the less if you have come across a system with no ssh/scp, you can also use nc as last ditch effort.

Start with machine on which data is to be received & start nc is listener mode,

```
$ ncat -l  8080 > file.txt
```

Now on the machine from where data is to be copied, run the following command,

```
$ ncat 192.168.1.100 8080 --send-only < data.txt
```

Here, data.txt is the file that has to be sent. –send-only option will close the connection once the file has been copied. If not using this option, than we will have press ctrl+c to close the connection manually.

We can also copy entire disk partitions using this method, but it should be done with caution.

Example: 7) Create a backdoor via nc/nact

NC command can also be used to create backdoor to your systems & this technique is actually used by hackers a lot. We should know how it works in order to secure our system. To create a backdoor, the command is,

```
$ ncat -l 10000 -e /bin/bash
```

'**e**' flag attaches a bash to port 10000. Now a client can connect to port 10000 on server & will have complete access to our system via bash,

```
$ ncat 192.168.1.100 1000
```

Example: 8) Port forwarding via nc/ncat

We can also use NC for port forwarding with the help of option 'c' , syntax for accomplishing port forwarding is,

```
$ ncat -u -l  80 -c  'ncat -u -l 8080'
```

Now all the connections for port 80 will be forwarded to port 8080.

Example: 9) Set Connection timeouts

Listener mode in ncat will continue to run & would have to be terminated manually. But we can configure timeouts with option 'w',

```
$ ncat -w 10 192.168.1.100 8080
```

This will cause connection to be terminated in 10 seconds, but it can only be used on client side & not on server side.

Example: 10) Force server to stay up using -k option in ncat

When client disconnects from server, after sometime server also stops listening. But we can force server to stay connected & continuing port listening with option 'k'. Run the following command,

```
$ ncat -l -k 8080
```

Now server will stay up, even if a connection from client is broken.

With this we end our tutorial, please feel free to ask any question regarding this article using the comment box below.

Read Also: **How to Add and Delete Static Route in Linux using IP Command**

Facebook Twitter LinkedIn Reddit

Tags: ncat linux

Previous story
20 Red Hat Satellite Server Interview Questions and Answers

Next story
How to enable Nested Virtualization in KVM on CentOS 7 / RHEL 7

5 RESPONSES

Comments 5 Pingbacks 0

Daniel December 7, 2017 at 8:27 am

Worked like a charm

Reply

Tomas December 8, 2017 at 8:48 am

At example 3 you use say that it's for connecting to UDP ports yet you use the "-l" switch which is for listening to incoming connections, and not for connecting to UDP. You may want to fix that.

One of the best real-life usages of netcat is to send application logs to a remote syslog server via UDP.

Reply

> **Pradeep Kumar** December 9, 2017 at 1:47 am
>
> Hi Tomas,
>
> I have corrected the example 3 as your per suggestion. Thank you for identifying the gap.
>
> Reply

rino19ny March 25, 2018 at 12:18 pm

cool. but is there a way to secure ncat on servers short of disabling them?

Reply

Rudra April 14, 2019 at 12:48 am

what is the best way to test if my udp port working using ncat? I have service running on the server with port 10000 using UDP. And I want to test if I can access that service before I start using that.

Reply

LEAVE A REPLY

Comment

Name *

Email *

Website

– seven = zero

Post Comment

Linux Desktop Linux Commands Linux How To's

- How to Use TimeShift to Backup and Restore Ubuntu Linux
- How to dual boot Windows 10 and Debian 10
- Installation Guide of Manjaro 18.1 (KDE Edition) with Screenshots
- Top 8 Things to do after Installing Debian 10 (Buster)
- Debian 10 (Buster) Installation Steps with Screenshots
- 9 ‘diff’ Command Examples in Linux
- 20 ps Command Examples to Monitor Linux Processes
- How to Use htop to Monitor Linux System Processes
- 14 SCP Command Examples to Securely Transfer Files in Linux
- 18 Quick ‘lsof’ command examples for Linux Geeks
- How to Extend EBS Boot Disk of EC2 Instance without Reboot
- How to Add and Delete Static Route in Linux using IP Command
- How to Use When Conditionals Statement in Ansible Playbook
- How to Sync Time in Linux Server using Chrony
- How to Setup DNS Server (Bind) on CentOS 8 / RHEL8