Netcat

Information Security Inc.

Contents

- About Netcat
- Netcat feature lineup
- Syntax and usage
- Features detailed
- Conclusion
- References

About Netcat

- "**Netcat**" is a computer networking function for analyzing from and writing to network connections using TCP or UDP

```
NAME
       nc - TCP/IP swiss army knife

SYNOPSIS
       nc [-options] hostname port[s] [ports] ...
       nc -l -p port [-options] [hostname] [port]
```

Netcat features

- Banner grabbing
- Reverse shell
- Chatting
- Data Transfer
- Port scanning
- Port knocking
- Port forwarding

Syntax and Usage

- Client/Server Model

◎ Netcat client

nc IP Port

◎ Netcat listener

nc -vlp Port

Features detailed

- Banner grabbing

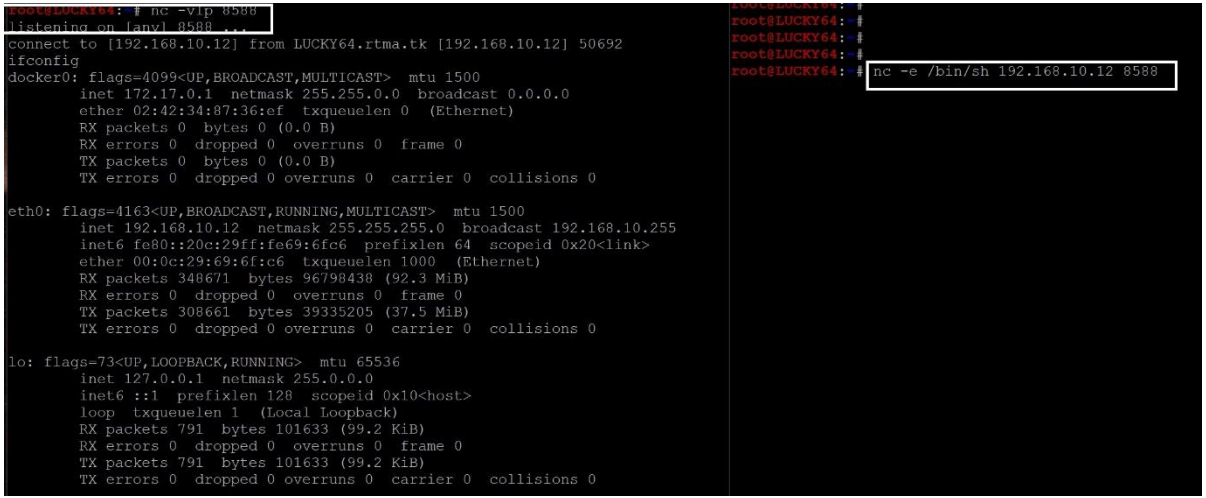
```
root@LUCKY64:~# nc 127.0.0.1 80
GET / HTTP/1.0

127.0.0.1 - - [03/Aug/2017 00:03:40] "GET / HTTP/1.0" 200 -
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.13
Date: Thu, 03 Aug 2017 04:03:40 GMT
Content-type: text/html; charset=UTF-8
Content-Length: 5194
```

```
root@LUCKY64:~# nc 192.168.10.12 25
220 LUCKY64.rtma.tk Python SMTP proxy version 0.2
```

Features detailed

- Reverse shell

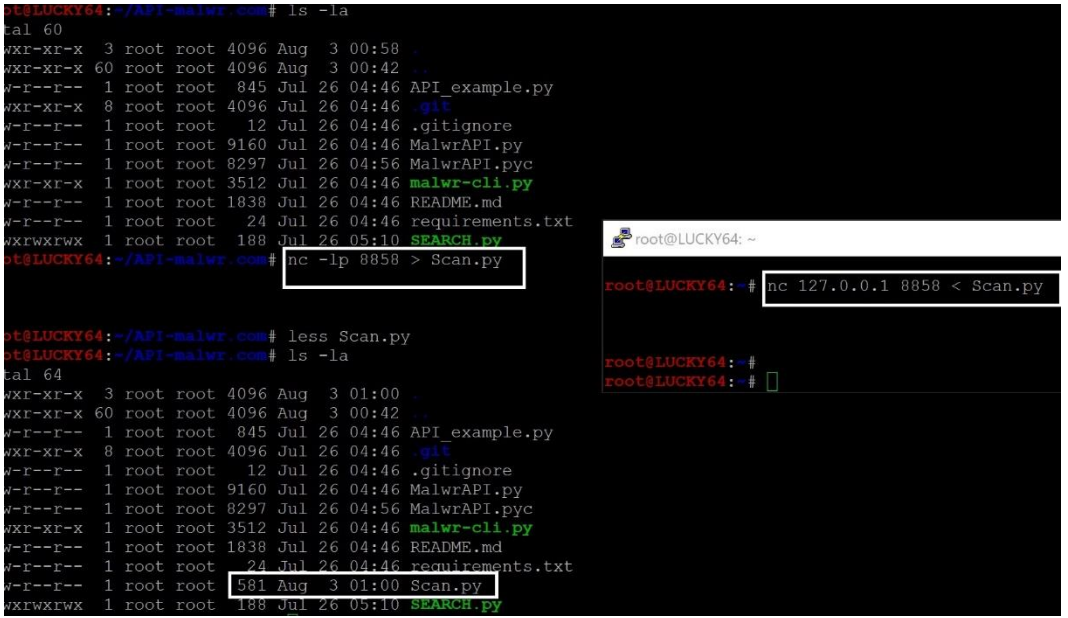


Features detailed

- Chatting

Features detailed

- Data Transfer



Features detailed

- Port scanning

```
root@LUCKY64:~/API-malwr.com# nc -vnz -w 1 127.0.0.1 1-65535


(UNKNOWN) [127.0.0.1] 8834 (?) open
(UNKNOWN) [127.0.0.1] 22 (ssh) open
```

- Port knocking (find out hidden services)

```
root@LUCKY64:~# nc 127.0.0.1 10025
220 LUCKY64.rtma.tk Python SMTP proxy version 0.2
root@LUCKY64:~# nc 127.0.0.1 11808
HEAD / HTTP/1.0

127.0.0.1 - - [03/Aug/2017 01:28:31] "HEAD / HTTP/1.0" 200 -
HTTP/1.0 200 OK
```

Features detailed

- Port forwarding

▲ Topology

Sending_Host >>> Forwarder_Host >>> Receiving_Host

forward port 8000 to remote-host:80

Conclusion

- There are many other sophisticated tools for every feature provided by Netcat, yet no other tool is powerful enough to provide so many functionalities in a single package

- Netcat is not only useful for a pentester but it can also be utilized by system administrators for their daily activities

References

- Wikipedia
https://en.wikipedia.org/wiki/Netcat

- SecTools
http://sectools.org/tool/netcat/