Socat Cheatsheet (https://blog.xathrya.id/2016/12/26/socat-cheatsheet/)

December 26, 2016 | Article (https://blog.xathrya.id/category/article/) | 1 Comment

(https://blog.xathrya.id/2016/12/26/socat-cheatsheet/)

Socat (http://www.dest-unreach.org/socat/doc/socat.html), a powerful tools you should have in you arsenal. Some say socat is another swiss army knife beside netcat. It is a command line based utility that establishes two bidirectional byte streams and transfer data between them. Socat has been long used for creating a simple forwarder. But, did you know that we can do more than that?

Basic Knowledge

Basically socat is a tool to manipulate sockets (https://secure.wikimedia.org/wikipedia/en/wiki/Unix_domain_socket). To give you a hint, socat comes from socket and cat.

The idea of sockets is too restrictive. Speaking socat we should speaks in the level of "data channel". It can be combinations of:

- a file
- a pipe
- a device (ex: a serial line)
- a socket (IPv4, IPv6, raw, TCP, UDP, SSL)
- a FD (STDIN, STDOUT)
- a program or script

Now socat has a different syntax on what you are used to with netcat or other standard unix tools. Here is the simple syntax:

```
socat [options] <channel> <channel>
```

both channel should be provided. The channel should be like this:

```
<protocol>:<ip>:<port>
```

All you need to remember is: socat is bidirectional. It is like a pipe so there is no strict definition of which one should be source or destination. Both address can have src/dst role.

Tips and Trick

Now, come to our actual topic. For the sake of simplicity, we will pretend there are two distinct hosts namely HOST-L and HOST-R.These hosts can be anywhere with any IP. In most case HOST-L is our local machine while HOST-R is remote machine. On most case we will use port 13510 and 18210 as example.

Let's see our catalog:

- Basic network connection
  - Connect to remote machine
  - Listening to a socket
  - UDP traffic
  - Execute program when connection come
  - SSLify connection
  - Make a tunnel
  - Make a tunnel via proxy
- File transfer
  - Display content of file to standard output
  - Create and write to a file
  - Transfer file
- UDP tunneling through SSH connection
- Local serial line
- Get HTTP content without browser

– Connect to remote machine

```
socat - TCP4:HOST-R:13510
socat STDIN TCP4:HOST-R:13510
socat STDIO TCP:HOST-R:13510
```

or

```
socat TCP4:HOST-R:13510 -
socat TCP4:HOST-R:13510 STDIN
socat TCP:HOST-R:13510 STDIO
```

As we see here, one end is HOST-R so in essence, we are connecting to remote machine.

– Listening to a socket

```
socat TCP-LISTEN:13510 -
```

or

```
socat - TCP-LISTEN:13510
```

We explicitly say we are listening to a port. There exist TCP4, TCP6, TCP4-LISTEN, and TCP6-LISTEN variations, as well.

What if both end is a TCP-LISTEN? see tunnel.

– UDP traffic

It's similar to previous section but with UDP traffic.

```
socat - UDP-LISTEN:13510
socat - UDP:HOST-R:13510
```

– Execute program when a connection come

For example, shell (https://blog.xathrya.id/2016/12/26/reverse-shell-cheatsheet).

```
socat TCP-LISTEN:13510 EXEC:"/bin/bash"
```

for multiple connection

```
socat -L TCP-LISTEN:13510 EXEC:/bin/bash
```

we also have SYSTEM address, which uses the system() (https://manpages.ubuntu.com/manpages/hardy/en/man3/system.3posix.html) call rather than a call to exec() (https://manpages.ubuntu.com/manpages/hardy/en/man3/exec.3posix.html). We can do something like this (something netcat can't do).

```
socat TCP-LISTEN:2323,reuseaddr SYSTEM:'echo $HOME; ls -la'
```

– SSLify connection

In short, strip incoming SSL to plain traffic.

```
socat OPENSSL-LISTEN:443,reuseaddr,pf=ip4,fork,cert=cert.pem,cafile=client.crt TCP4-CONNECT:HOST-L:80
```

– Make a tunnel

```
socat TCP4-LISTEN:13510,reuseaddr,fork TCP:xathrya.id:22
```

– Make a tunnel via proxy

```
socat TCP4-LISTEN:13510,reuseaddr,fork PROXY:certain.proxy.id:xathrya.id22,proxyport=3128,proxyauth=user:pass
```

– Display content of file to standard output

address can be a file. Thus directive FILE: is used to read content of file.txt and then pipe it.

```
socat FILE:file.txt STDOUT
```

To give you a hint, socat comes from socket and cat.

– Create and write to a file

Don't forget to CTRL+D or CTRL+C to end session.

```
socat -u STDIN OPEN:file.txt,creat,trunc
```

– Transfer file

and as you might expect, pipe a file to remote host.

```
HOST-L# socat FILE:file.txt TCP:HOST-R:13510
HOST-R# socat TCP-LISTEN:13510 OPEN:file.txt,creat,trunc
```

– UDP tunneling through SSH connection

see this article (https://blog.xathrya.id/2016/12/26/udp-tunneling-ssh-connection/).

```
LOCAL# ssh -L 13510:LOCAL:13510 SERVER
SERVER# socat tcp4-listen:13510,reuseaddr,fork UDP:NAMESERVER:53
LOCAL# socat -T15 udp4-recvfrom:53,reuseaddr,fork tcp:LOCAL:13510
```

– Local serial line

Use as a local serial line. For example, to configure a network device, modem, or embedded device without a terminal emulator.

```
socat \
READLINE,history:/tmp/serial.cmds \
OPEN:/dev/ttyS0,ispeed=9600,ospeed=9600,crnl,raw,sane,echo=false
```

READLINE data channel use GNU readline (https://savannah.gnu.org/projects/readline) to allow editing and reusing input lines like a classic shell.

– Grab some HTTP content without a browser

```
# cat <<EOF | socat - TCP4:xathrya.id:80
GET / HTTP/1.1
Host: xathrya.id

EOF
```

GET to EOF is something we need to type in.

networking (https://blog.xathrya.id/tag/networking/)

By xathrya (https://blog.xathrya.id/author/xathrya/)

About Author

A WP Life

xathrya

A man who is obsessed to low level technology.

« Prev Post (https://blog.xathrya.id/2016/12/26/udp-tunneling-ssh-connection/)

Next Post » (https://blog.xathrya.id/2016/12/27/reverse-shell-cheatsheet/)

1 Comment

Reverse Shell Cheatsheet - Xathrya.ID

December 27, 2016 (https://blog.xathrya.id/2016/12/26/socat-cheatsheet/#comment-175)

[…] if we are using socat, we can use […]

Reply (https://blog.xathrya.id/2016/12/26/socat-cheatsheet/?replytocom=175#respond)

Leave a Reply

COMMENT

NAME

EMAIL

Notify me of follow-up comments by email.

Notify me of new posts by email.

Post Comment