```
└─# nmap -sS -p- -sV -O -A --top-ports 30000 -oN scan_results.txt 10.129.228.3
7

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-13 20:05 CET
Nmap scan report for 10.129.228.37
Host is up (0.045s latency).
Not shown: 8367 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
873/tcp open  rsync   (protocol version 31)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   44.45 ms 10.10.14.1
2   44.51 ms 10.129.228.37

OS and Service detection performed. Please report any incorrect results at https://
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
```

What is the default port for rsync?

873

How many TCP ports are open on the remote host?

1

What is the protocol version used by rsync on the remote machine?

31 `873/tcp open  rsync   (protocol version 31)`

What is the most common command name on Linux to interact with rsync?

Rsync

What credentials do you have to pass to rsync in order to use anonymous authentication? anonymous:anonymous, anonymous, None, rsync:rsync

none

What is the option to only list shares and files on rsync? (No need to include the leading -- characters)

list-only

```
┌──(root㉿kali)-[~alvadelg]
└─# rsync -av rsync://anonymous@10.129.228.37/public /home/alvadelg

receiving incremental file list
./
flag.txt

sent 50 bytes  received 161 bytes  32,46 bytes/sec
total size is 33  speedup is 0,16
```

```
┌──(root㉿kali)-[~alvadelg]
└─# cat flag.txt
72eaf5344ebb84908ae543a719830519
```

72eaf5344ebb84908ae543a719830519