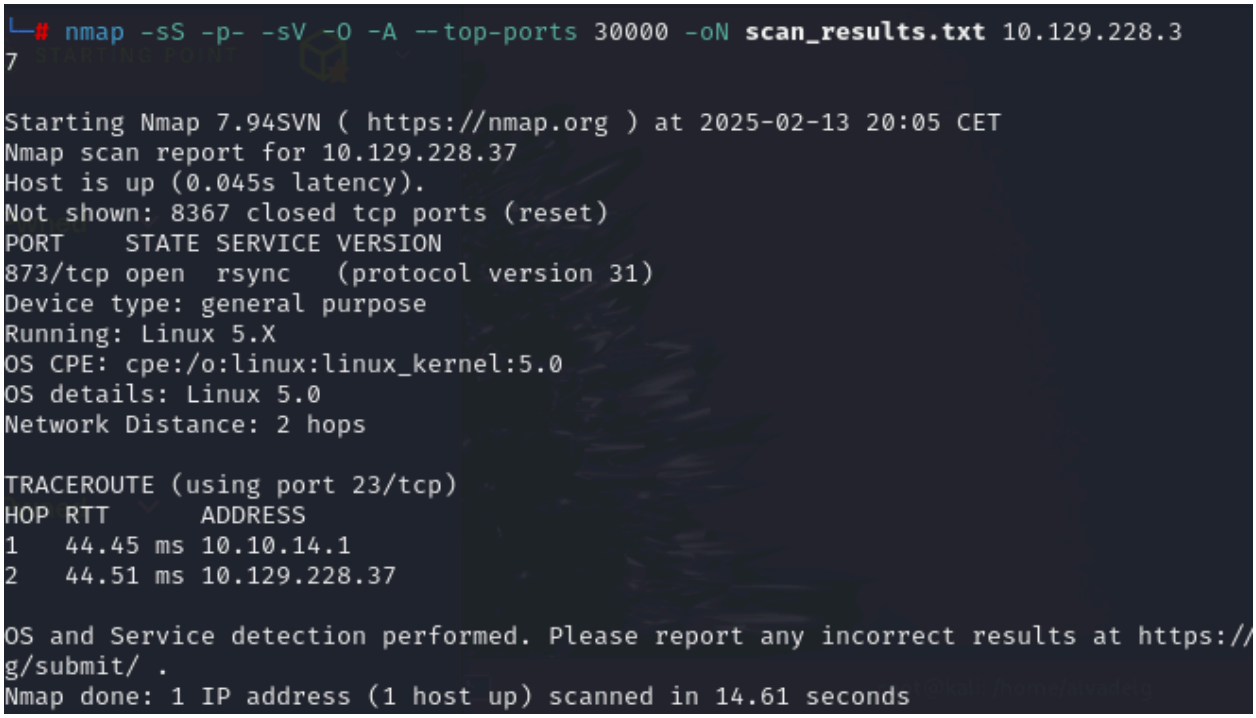
Synced

Álvaro Delgado Hernández



```
└─# 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
```

Explanation of Each Argument

-sS: SYN Scan

This performs a TCP SYN scan, which is a stealthy scan method. It sends SYN packets and waits for SYN-ACK responses, allowing you to discover open ports without completing the TCP handshake.

-p-: Scan All Ports

This option tells Nmap to scan all 65,535 TCP ports instead of just the default 1,000 ports.

-sV: Version Detection

This option tells Nmap to detect the versions of the services running on open ports.

-O: OS Detection

This flag enables OS detection, allowing Nmap to determine the operating system of the target host.

-A: Aggressive Scan

This enables several advanced and intrusive options, including OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute.

--top-ports 30000: Scan the Top 30,000 Ports

This tells Nmap to scan the top 30,000 commonly used ports, which is a subset of all 65,535 ports.

-oN scan_results.txt: Output to a File

This option specifies that the scan results should be saved in normal format to a file named scan_results.txt.

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 

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
```

Explanation of Each Argument

rsync:

This is the command itself, used for synchronizing files and directories between different locations.

-a: Archive Mode

This option ensures that the synchronization is recursive, preserves symbolic links, permissions, timestamps, and other file attributes. It essentially performs a comprehensive backup.

-v: Verbose Mode

This option increases the verbosity of the command, meaning it provides detailed output about what rsync is doing during the synchronization process.

rsync://anonymous@10.129.228.37/pubblic:

This is the source location from which files are being synchronized. It specifies an rsync daemon running on the server at IP 10.129.228.37 with a module named public. The anonymous user is used to connect, implying that no authentication is required or that anonymous access is allowed.

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

72eaf5344ebb84908ae543a719830519