interweb

Generated on 21/10/2026 16:09

KNOWLEDGE BASE · PUBLIC DOCUMENT

Your VPS is scanning other networks: finding and stopping the process behind a netscan notice

Security

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-2250	v2026.10.21	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/2250

Your VPS is scanning other networks: finding and stopping the process behind a netscan notice

Security Created on **October 21, 2026** 4 min read

The short answer: a **netscan** notice means your server opened, within minutes, connections to many addresses in a range, always on the same ports (for example 22, 80 and 443, or 6379). It is nearly always **malware** that got into the server and is looking for new victims; sometimes it is a scanning tool someone ran against networks that are not theirs, which is abuse as well. This article is for **VPS and dedicated server** customers: you find the process through its connections, stop it, and look for the way in.

What the ports in the notice tell you

Destination ports in the log	What the program is doing
22 (SSH)	Trying to guess SSH passwords on other servers. That is often how yours was caught too.
80 and 443 (web)	Looking for sites and applications with known flaws.
6379 (Redis)	Looking for open Redis servers. If your Redis is open, that is probably how it got in: **Redis open to the internet**.
Many destinations in a row (a whole range)	A scan: the program goes through the addresses one by one.
Source IP	Your server's IP. If you have several, the notice says which.

Finding the process and stopping it

1. **Note the ports and the time (UTC) in the notice,** and log in over SSH as root. If the scan is still running, you will see it now; if it has stopped, go straight to step 5.

2. **List pending outgoing connections:** a scan leaves many connections in `SYN-SENT` (attempts nobody answered). The commands in the block below show them and count them per process.

3. **Identify the program:** with the process number (PID), see the file with `ls -l /proc/PID/exe` and the command line with `/proc/PID/cmdline`. If `iftop` or `nethogs` are installed, they show traffic per connection or per process; they may not be.

4. **Freeze it, copy it, and only then kill the process** (second block). `kill -STOP` halts it without removing it from memory, so you can copy the program for analysis.

5. **Find what starts it again:** there is nearly always a cron job, a systemd service or an SSH key bringing it back. Follow **checking processes, cron jobs, users and keys**.

6. **Close the way it got in** (open Redis, a weak SSH password, an outdated application), confirm with `ss -tnp state syn-sent` that the scan has stopped, and send the report: **writing the reply to an abuse notice**.

Finding the process through its connections

Replace PID with the number the first command shows at the end of each line. These commands only read: `ss -tnp state syn-sent`

```
ss -tnp state syn-sent | awk 'NR>1 {print $NF}' | sort | uniq -c | sort -rn | head
ss -tunap | grep ':6379'
ls -l /proc/PID/exe
tr '\0' ' ' < /proc/PID/cmdline; echo
systemctl status PID
```

Freeze, copy and stop

Copy the program before killing it: once it is dead, there may be no file left on disk. `kill -STOP PID`

```
mkdir -p /root/analysis
cp /proc/PID/exe /root/analysis/sample-PID
sha256sum /root/analysis/sample-PID
kill -9 PID
```

Cutting outgoing traffic while you clean up

With **ufw** you block outgoing traffic to one port; if you use nftables directly, the third command shows the rules you have. First make sure none of your applications needs to go out on that port: `ufw deny out 6379/tcp`

```
ufw status numbered
nft list ruleset
```

Killing the process is not enough.

If you do not remove what starts it (cron, service, key) and close the way in, the scan comes back, sometimes minutes later, and the server is switched off. And do not block outgoing ports 80 and 443 for good: the server itself needs them for updates and for your applications.

The server firewall helps while you investigate:

Blocking outgoing traffic to the port the program scans (the block uses 6379 as the example) cuts the abuse without touching anything else. Remove the rule once you have cleaned up, if you need that port. **On a compromised server, the safest route is to reinstall the system and restore a clean copy** (**reinstalling the VPS operating system** and **which backup to restore**). Cleaning in place is for people who know what they are doing: an attacker with root access can leave ways back in that are not obvious at first.

NEED A HAND?

Got a netscan notice and cannot find the process? Send us the output of ss -tunap in the support ticket for the notice.

Open a support ticket →

SEE ALSO

- Is my VPS compromised? Checking processes, cron jobs, users, SSH keys and temporary folders
- Writing the reply to an abuse notice: cause, what you removed and how it will not happen again
- Redis open to the internet: close it with bind, protected mode, a password and the firewall
- Setting up the ufw firewall on Ubuntu without locking yourself out
- Installing fail2ban on a VPS to stop SSH password guessing
- Ports and firewall on a VPS: why your app is not reachable

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-2250 · v2026.10.21 · Generated on 21/10/2026 16:09