

Lab 26 – Using Scanless for easy anonymous port scanning

✓ What is this lab about?

You're going to use a tool called **Scanless**. Scanless is special because it **lets you scan other computers or servers anonymously** — meaning, it hides *your* real IP address by using online scanning services instead.

Basically, **Scanless acts like a middleman**. Instead of scanning the target directly with your own machine, it tells an online service to do it, then shows you the results. That way, your personal IP is not revealed to the target.

✓ What is the purpose of this lab?

- Learn how to install Scanless
 - Learn how to see what scanners it can use
 - Practice scanning a test server (scanme.nmap.org)
 - Try out multiple scanners to see what they find
-

✓ Lab Environment

You'll use **Kali Linux**, either on your main PC or inside a virtual machine (which is safer and more common).

Task 1 – Installing Scanless on Kali Linux using pipx — Step-by-Step

Step 1: Update apt source:

```
sudo apt update
```

```
(root@KALI)-[/home/femi]
# sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Err:1 http://kali.download/kali kali-rolling InRelease
  Sub-process /usr/bin/sq returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462EC8D5E4C5, which is needed to verify signature.
Fetched 41.5 kB in 12s (3,578 B/s)
418 packages can be upgraded. Run 'apt list --upgradable' to see them.
Warning: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: http://kali.download/kali kali-rolling InRelease: Sub-process /usr/bin/sq returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462EC8D5E4C5, which is needed to verify signature.
Warning: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease Sub-process /usr/bin/sq returned an error code (1), error message is: Missing key 827C8569F2518CC677FECA1AED65462EC8D5E4C5, which is needed to verify signature.
Warning: Some index files failed to download. They have been ignored, or old ones used instead.
```



Step 2: Check and install pipx

You proceeded to install **pipx**, a safe tool to install python-based command-line utilities:

sudo apt install pipx

```
(root@KALI)-[/home/femi]
# sudo apt install pipx
pipx is already the newest version (1.7.1-1).
The following package was automatically installed and is no longer required:
  ruby-zeitwerk
Use 'sudo apt autoremove' to remove it.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 418
```

Since **pipx** was already installed on your system, nothing changed.

Step 3: Clean up unused packages

You ran:

sudo apt autoremove

```
(root@KALI)-[/home/femi]
# sudo apt autoremove
REMOVING:
  ruby-zeitwerk
  ruby-zeitwerk
Summary:
  Upgrading: 0, Installing: 0, Removing: 1, Not Upgrading: 418
  Freed space: 115 kB

Continue? [Y/n] Y
(Reading database ... 431929 files and directories currently installed.)
Removing ruby-zeitwerk (2.6.8-1) ...
```

To remove an unused package (**ruby-zeitwerk**), freeing up 115kB of space. Always a good habit to keep the system clean.

Step 4: Ensure pipx path is added

You told pipx to configure your **PATH** so that it can run globally-installed tools:

pipx ensurepath

```
(root@KALI)-[/home/femi]
$ pipx ensurepath
Success! Added /root/.local/bin to the PATH environment variable.

Consider adding shell completions for pipx. Run 'pipx completions' for instructions.

You will need to open a new terminal or re-login for the PATH changes to take effect. Alternatively, you can source your shell's config file with e.g. 'source ~/.bashrc'.

Otherwise pipx is ready to go! 🌟
```

Step 5: Install scanless with pipx

Now you installed **scanless** using pipx:

pipx install scanless

```
(root@KALI)-[/home/femi]
$ pipx install scanless
installed package scanless 2.2.1, installed using Python 3.13.2
These apps are now globally available
- scanless
△ Note: '/root/.local/bin' is not on your PATH environment variable. These apps will not be globally accessible until your PATH is updated. Run 'pipx ensurepath' to automatically add it, or manually modify your PATH in your shell's config file (e.g. ~/.bashrc).
done! 🌟
```

Step 6: Final path fix

You ran **pipx ensurepath** again just to confirm the **PATH** change, and the message reminded you:

You will need to open a new terminal or re-login

which is correct — either restart your terminal or type:

✓ Final check

After restarting your terminal, verify the install:

scanless --help

```
(root@KALI)-[/home/femi]
$ scanless --help
usage: scanless [-h] [-v] [-t TARGET] [-s SCANNER] [-r] [-l] [-a] [-d]
scanless, an online port scan scraper.

options:
  -h, --help            show this help message and exit
  -v, --version          display the current version: 0.0.0
  -t, --target TARGET    ip or domain to scan
  -s, --scanner SCANNER scanner to use (default: yougetsignal)
  -r, --random           use a random scanner
  -l, --list             list scanners
  -a, --all             use all the scanners
  -d, --debug           debug mode (cli mode off & show network errors)

After restarting your terminal, verify the install:
scanless --help

You should see the scanless help menu.

Beginner Explanation:
Think of this like an online scanner for Dufour's program. Scanless is a Dufour-based
```

You should see the scanless help menu.

Then, list the **available scanners**:

`scanless -l`

```
(root@KALI)-[/home/femi]
# scanless -l
You should see the scanless help menu.

+-----+-----+
| Scanner Name | Website |
+-----+-----+
| ipfingerprints | https://www.ipfingerprints.com |
| pingeu | https://ping.eu |
| spiderip | https://spiderip.com |
| standingtech | https://portscanner.standingtech.com |
| viewdns | https://viewdns.info |
| yougetsignal | https://www.yougetsignal.com |
+-----+-----+
list the available scanners.

scanless -h

(root@KALI)-[/home/femi]
#
```

This shows you a list of public online scanners that Scanless can use, for example:

- hackertarget
- spiderip
- t1shopper
- ipfingerprints

You'll see their names and which websites they belong to.

✓ Task 3 — Scanning a Target

Beginner Explanation

Scanless uses these online scanners to scan a target you specify.

For this lab, you'll scan **scanme.nmap.org**, which is a public test server *set up on purpose for scanning*. That way you're not breaking any rules.

The command is:

`scanless -t scanme.nmap.org -s [scanner-name]`

```
(root@KALI) [/home/femi]
scanless -t axia.africa -s ipfingerprints
Running scanless v2.2.1 ...
ipfingerprints:
Host is up (0.086s latency).
Not shown: 490 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
Aggressive OS guesses: Linux 2.6.32 (93%), Linux 3.10 (93%), Linux 3.10 - 4.2 (93%), Linux 3.2
- 5.6 (93%), Linux 3.4 - 3.10 (93%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.13 (92%),
Synology DiskStation Manager 5.2-5644 (91%), Linux 2.6.22 - 2.6.36 (89%), Linux 2.6.39 (89%)
No exact OS matches for host (test conditions non-ideal).
```

Replace [scanner-name] with the name of the scanner you want.

✓ For example:

- Using hackertarget:

```
scanless -t scanme.nmap.org -s hackertarget
```

- Using spiderip:

```
scanless -t scanme.nmap.org -s spiderip
```

- Using t1shopper:

```
scanless -t scanme.nmap.org -s t1shopper
```

- Using ipfingerprints:

```
scanless -t scanme.nmap.org -s ipfingerprints
```

✓ **ipfingerprints** is cool because it also tries to guess the operating system (like Windows or Linux) of the target, and tells you a confidence percentage.

Between each scan, you can simply run:

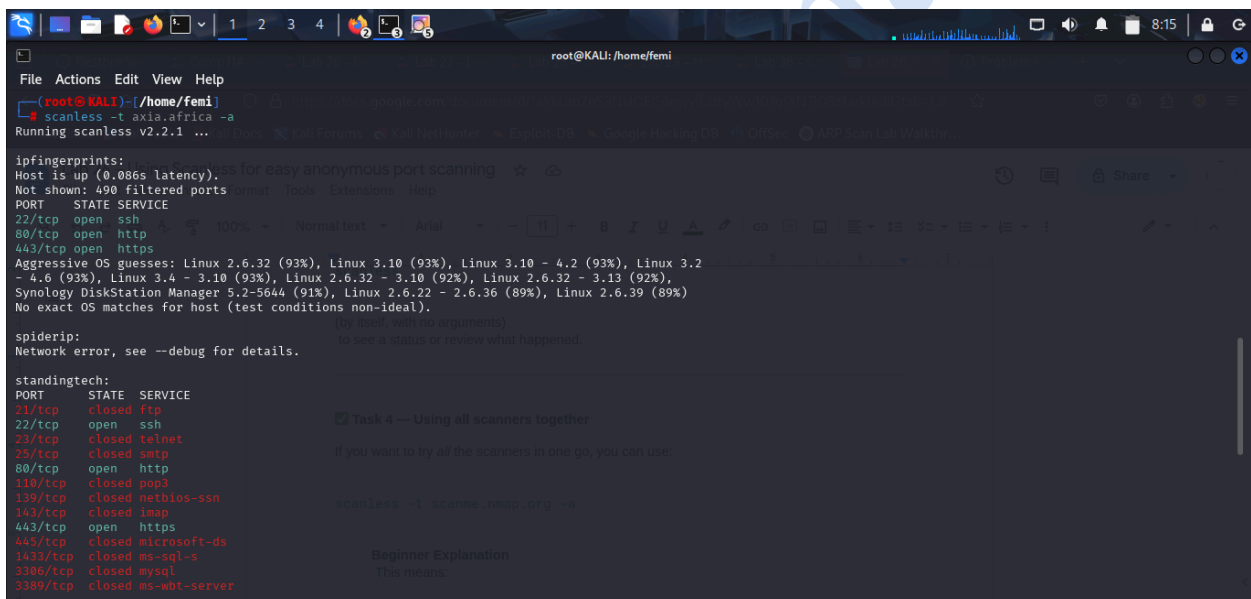
`scanless`

(by itself, with no arguments)
to see a status or review what happened.

✓ Task 4 — Using all scanners together

If you want to try *all* the scanners in one go, you can use:

`scanless -t scanme.nmap.org -a`



```
root@KALI: /home/femi
File Actions Edit View Help
root@KALI: /home/femi
scanless -t axia.africa -a
Running scanless v2.2.1 ...

ipfingerprints:
Host is up (0.086s latency).
Not shown: 490 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp    open  https

Aggressive OS guesses: Linux 2.6.32 (93%), Linux 3.10 (93%), Linux 3.10 - 4.2 (93%), Linux 3.2
- 4.6 (93%), Linux 3.4 - 3.10 (93%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.32 - 3.13 (92%),
Synology DiskStation Manager 5.2-5644 (91%), Linux 2.6.22 - 2.6.36 (89%), Linux 2.6.39 (89%)
No exact OS matches for host (test conditions non-ideal).

spiderip:
Network error, see --debug for details.

standingtech:
PORT      STATE SERVICE
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
25/tcp    closed smtp
80/tcp    open  http
110/tcp   closed pop3
139/tcp   closed netbios-ssn
143/tcp   closed imap
443/tcp   open  https
445/tcp   closed microsoft-ds
1433/tcp  closed ms-sql-s
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
```

Beginner Explanation

This means:

- `-t` → your target
- `-a` → use all available scanners

That way you get a broader picture of what ports are open and what services are running on the target.

✓ Important Reminders

⚠ Always **have permission** to scan a target. In this lab, **scanme.nmap.org** is safe because it is intentionally public for security testing.

⚠ Scanning random sites on the internet without permission is *illegal* and can get you in trouble.

✓ In short, here's what you're doing

1. Install Scanless
2. Check what scanners it can use
3. Practice scanning a legal test target
4. Compare how each online scanner shows results
5. Try scanning with all of them at once