- **1. Installation of Tools**

Most subdomain enumeration tools are written in Go, so first install Go language:

Install Go

```bash
sudo apt update && sudo apt install golang -y
```

Install Subfinder

Subfinder is from ProjectDiscovery (fast passive subdomain finder).

```bash
go install github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest
```

Install Assetfinder

From TomNomNom (uses public sources like crt.sh).

```bash
go install github.com/tomnomnom/assetfinder@latest
```

Install Alterx

Generates permutations/variations of subdomains.

```bash
go install github.com/projectdiscovery/alterx/cmd/alterx@latest
```

Add Go bin to PATH

If tools don’t run after installation:

```bash
echo 'export PATH=$PATH:~/go/bin' >> ~/.bashrc
source ~/.bashrc
```

✅ *`subfinder`, `assetfinder`, and `alterx` will be available globally.*

- **2. Assignment Task**

The task says:

> Collect subdomains of any 2 targets with the help of 3 different tools: Subfinder, Assetfinder, Alterx.

Let’s say our targets are:

`example.com`
`test.com`

- 3. Step-by-Step Execution

Step 1: Prepare Domain List

```bash
echo -e "example.com\ntest.com" > domains.txt
```

Now you have `domains.txt` with 2 domains.

Step 2: Enumerate with Subfinder

```bash
subfinder -dL domains.txt -silent -o subfinder.txt
```

`-dL domains.txt` → input list of domains.

`-silent` → clean output.

`-o subfinder.txt` → save output.

Step 3: Enumerate with Assetfinder

```bash
for d in $(cat domains.txt); do
   assetfinder --subs-only $d
done > assetfinder.txt
```

Runs `assetfinder` for each domain.

`--subs-only` → filters only subdomains.

Saves all results into `assetfinder.txt`.

Step 4: Generate Alterations with Alterx

```bash
cat subfinder.txt assetfinder.txt | sort -u | alterx -o alterx.txt
```

Combines both tools’ results.

Removes duplicates (`sort -u`).

Pipes into `alterx` to generate permutations like:

`dev.example.com`

`test.example.com`

`stage.test.com`

Saves results to `alterx.txt`.

Step 5: Merge All Results

```bash
cat subfinder.txt assetfinder.txt alterx.txt | sort -u > all-subs.txt
```

Now `all-subs.txt` contains unique subdomains collected from all 3 tools.

Step 6 (Optional): Check Live Subdomains

Using `httpx`:

```bash
httpx -l all-subs.txt -o alive-subs.txt
```

Scans the list and finds which subdomains respond with HTTP/HTTPS.

`alive-subs.txt` → only reachable domains.

- 4. Output Files Explanation

subfinder.txt → Subdomains from Subfinder.

assetfinder.txt → Subdomains from Assetfinder.

alterx.txt → Permutations generated by Alterx.

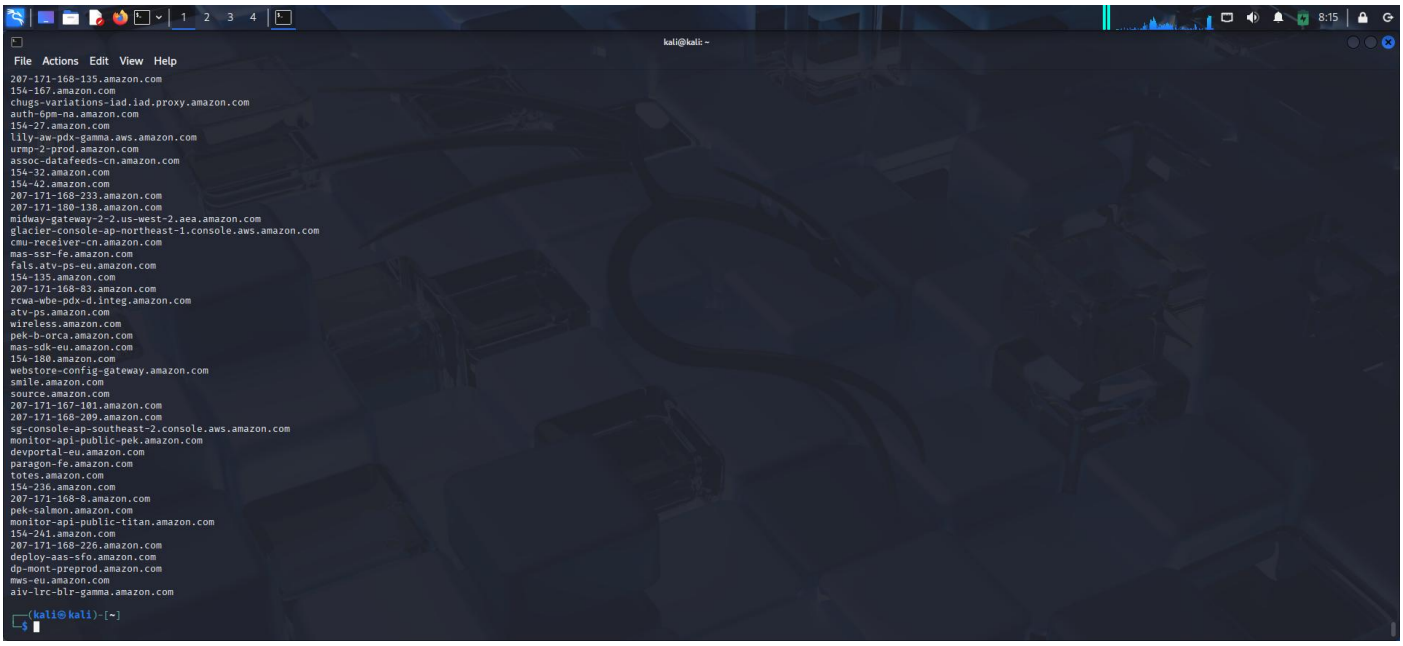
all-subs.txt → Combined unique results.

alive-subs.txt → Only live/active subdomains.

- 5. Automation (Optional Bash Script)

Here’s a script (`subenum.sh`) to automate everything:

```bash
!/bin/bash

 Input file with domains
DOMAINS="domains.txt"

 Run Subfinder
subfinder -dL $DOMAINS -silent -o subfinder.txt

 Run Assetfinder
> assetfinder.txt
for d in $(cat $DOMAINS); do
    assetfinder --subs-only $d >> assetfinder.txt
done

 Run Alterx on combined results
cat subfinder.txt assetfinder.txt | sort -u | alterx -o alterx.txt

 Merge all
cat subfinder.txt assetfinder.txt alterx.txt | sort -u > all-subs.txt
Results:
```


1 2 3 4
8:15
kali@kali: ~
File Actions Edit View Help
207-171-168-135.amazon.com
154-167.amazon.com
chugs-variations-iad.iad.proxy.amazon.com
auth-6pm-na.amazon.com
154-27.amazon.com
lily-aw-pdx-gamma.aws.amazon.com
urmp-2-prod.amazon.com
assoc-datafeeds-cn.amazon.com
154-32.amazon.com
154-42.amazon.com
207-171-168-233.amazon.com
207-171-180-138.amazon.com
midway-gateway-2-2.us-west-2.aea.amazon.com
glacier-console-ap-northeast-1.console.aws.amazon.com
cmu-receiver-cn.amazon.com
mas-ssr-fe.amazon.com
fals.atv-ps-eu.amazon.com
154-135.amazon.com
207-171-168-83.amazon.com
rcwa-wbe-pdx-d.integ.amazon.com
atv-ps.amazon.com
wireless.amazon.com
pek-b-orca.amazon.com
mas-sdk-eu.amazon.com
154-180.amazon.com
webstore-config-gateway.amazon.com
smile.amazon.com
source.amazon.com
207-171-167-101.amazon.com
207-171-168-209.amazon.com
sg-console-ap-southeast-2.console.aws.amazon.com
monitor-api-public-pek.amazon.com
devportal-eu.amazon.com
paragon-fe.amazon.com
totes.amazon.com
154-236.amazon.com
207-171-168-8.amazon.com
pek-salmon.amazon.com
monitor-api-public-titan.amazon.com
154-241.amazon.com
207-171-168-226.amazon.com
deploy-aas-sfo.amazon.com
dp-mont-preprod.amazon.com
mws-eu.amazon.com
a1v-lrc-blr-gamma.amazon.com
┌──(kali㉿kali)-[~]
└─$