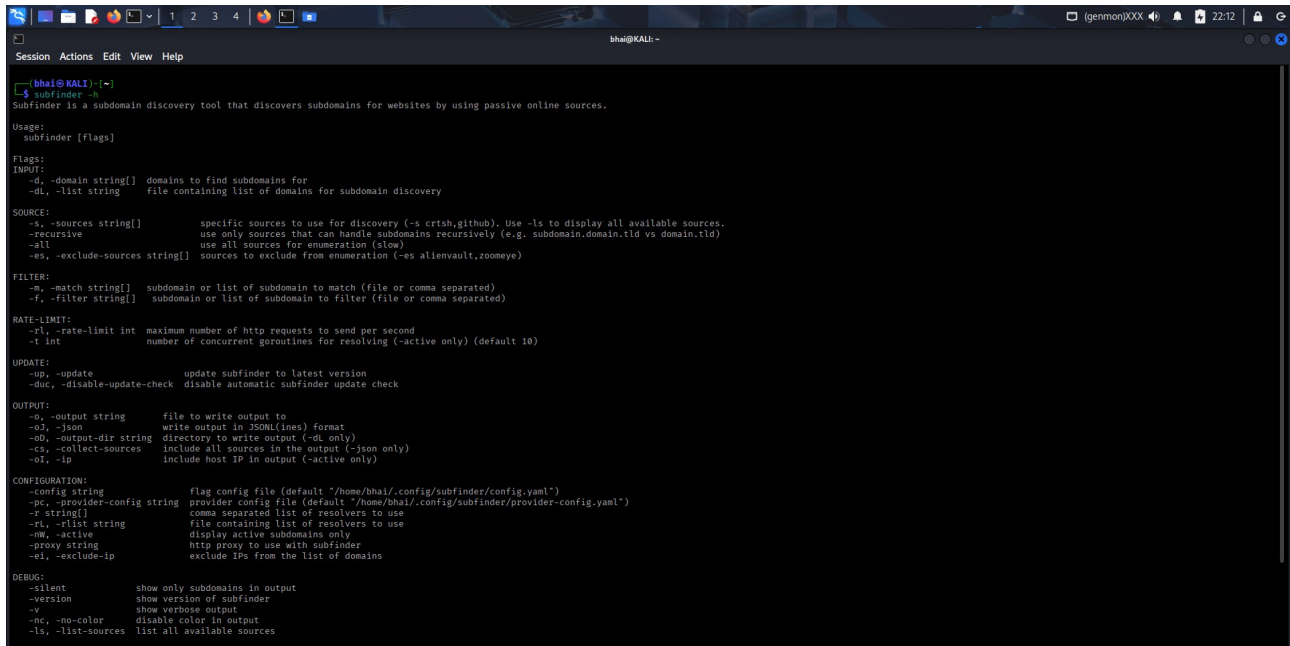


Skill Horizon Task2 (Day 15-Nov-2025) by:- Vikram Budania

Tasks

Install these scripts in the Kali Linux (go based)

• Subfinder



```
Session Actions Edit View Help

bhai@KALI: ~
$ subfinder -h
Subfinder is a subdomain discovery tool that discovers subdomains for websites by using passive online sources.

Usage:
  subfinder [flags]

Flags:
INPUT:
  -d, -domain string[]  domains to find subdomains for
  -dl, -list string      file containing list of domains for subdomain discovery

SOURCE:
  -s, -sources string[]  specific sources to use for discovery (--s crtsh,github). Use --ls to display all available sources.
  -recursive             use only sources that can handle subdomains recursively (e.g. subdomain.domain.tld vs domain.tld)
  -all                  use all sources for enumeration (slow)
  -es, -exclude-sources string[] sources to exclude from enumeration (--es alienvault,zoomeye)

FILTER:
  -m, -match string[]    subdomain or list of subdomain to match (file or comma separated)
  -f, -filter string[]   subdomain or list of subdomain to filter (file or comma separated)

RATE-LIMIT:
  -rl, -rate-limit int   maximum number of http requests to send per second
  -t int                 number of concurrent goroutines for resolving (-active only) (default 10)

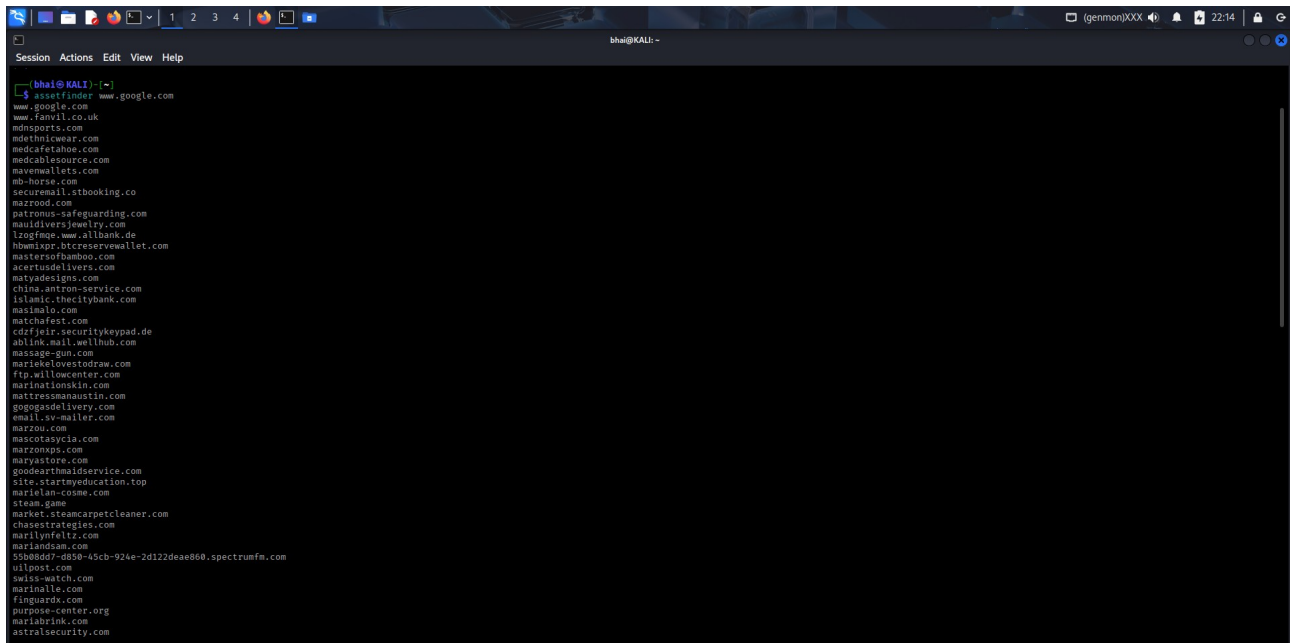
UPDATE:
  -up, -update           update subfinder to latest version
  -duc, -disable-update-check disable automatic subfinder update check

OUTPUT:
  -o, -output string      file to write output to
  -oJ, -json              write output in JSON(Lines) format
  -od, -output-dir string directory to write output (-od only)
  -cs, -collect-sources   include all sources in the output (-json only)
  -oi, -ip                include host IP in output (-active only)

CONFIGURATION:
  -config string          flag config file (default "/home/bhai/.config/subfinder/config.yaml")
  -pc, -provider-config string provider config file (default "/home/bhai/.config/subfinder/provider-config.yaml")
  -r string[]             comma separated list of resolvers to use
  -rl, -rlist string      file containing list of resolvers to use
  -ma, -active            display active subdomains only
  -proxy string           http proxy to use with subfinder
  -ei, -exclude-ip        exclude IPs from the list of domains

DEBUG:
  -silent               show only subdomains in output
  -version              show version of subfinder
  -v                   show verbose output
  -nc, -no-color         disable color in output
  -ls, -list-sources     list all available sources
```

• Assetfinder



```
Session Actions Edit View Help

bhai@KALI: ~
$ assetfinder www.google.com
www.google.com
www.fanvil.co.uk
mdnsparts.com
mdethnicwear.com
medcafetahoe.com
medcablesources.com
mavenwallets.com
mb-horse.com
securemail.stbooking.co
mazrood.com
patronus-safeguarding.com
mauidiversjewelry.com
l2ogfme.www.allbank.de
hbmixpr.btcrsreservewallet.com
mastersofbamboo.com
acertusdelivers.com
matyadesigns.com
china.antroni-service.com
islamic.thecitybank.com
masimalo.com
matchafest.com
cdfjfeir.securitykeypad.de
ablink.mail.wellhub.com
massage-gun.com
mariekelovestodraw.com
ftp.willowcenter.com
marinationskin.com
mattressnanaustin.com
gogogasdelivery.com
email-ay-maller.com
marzou.com
mascotasycia.com
marzomps.com
maryastore.com
goodearthmaidservice.com
site.startmyeducation.top
marielan-cosme.com
steam.game
market.steamcarpetcleaner.com
chasesstrategies.com
marilynfeltz.com
marlinsam.com
55b08dd7-d850-45cb-924e-2d122deae860.spectrumfm.com
uilpost.com
mlss-watch.com
marinalle.com
finguardx.com
purpose-center.org
marlabrink.com
astralsecurity.com
```

• Alterx

• Gau

```
(vikram@VIKRAM:~)$ gau --help
Usage of gau:
  --blacklist strings  list of extensions to skip
  --config string      location of config file (default $HOME/.gau.toml or %USERPROFILE%\ .gau.toml)
  --fc strings         list of status codes to filter
  --fp                remove different parameters of the same endpoint
  --from string        fetch urls from date (format: YYYYMM)
  --ft strings         list of mime-types to filter
  --json              output as json
  --mc strings         list of status codes to match
  --mt strings         list of mime-types to match
  --o string           filename to write results to
  --providers strings  list of providers to use (wayback,commoncrawl,otx,urlscan)
  --proxy string       http proxy to use
  --retries uint       retries for HTTP client
  --subs              include subdomains of target domain
  --threads uint       number of workers to spawn (default 1)
  --timeout uint       timeout (in seconds) for HTTP client (default 45)
  --to string          fetch urls to date (format: YYYYMM)
  --verbose            show verbose output
  --version            show gau version
(vikram@VIKRAM:~)$
```

• Fuzzuli

```
Mon Nov 17 10:25:40 PM
Terminal

(vikram@VIKRAM:~)$ fuzzuli -h
fuzzuli is a url fuzzing tool that aims to find critical backup files by creating a dynamic wordlist based on the domain.

Usage:
  fuzzuli [Flags]

Flags:
GENERAL OPTIONS:
  -w int    worker count (default 16)
  -f string  input file containing list of host/domain
  -pt string paths. separate with commas to use multiple paths. e.g. ./,db/,old/ (default "/")
  -p        print urls that is sent request
  -sl       silent mode
  -v        print version

WORDLIST OPTIONS:
  -mt string methods. available methods: regular, withoutdots, withoutvowels, reverse, mixed, withoutdv, shuffle
  -sf string suffix
  -pf string prefix
  -ex string file extension. default (rar, zip, tar.gz, tar, gz, jar, 7z, bz2, sql, backup, war)
  -rp string replace specified char
  -rm string remove specified char
  -jw        just generate wordlist do not http request

DOMAIN OPTIONS:
  -es string exclude domain that contains specified string or char. e.g. for OR operand google|bing|yahoo (default "#")
  -dl int    match domain length that specified. (default 40)

MATCHER OPTIONS:
  -ct string match response with specified content type
  -sc int    match response with specified status code (default 200)
  -cl int    match response with specified minimum content length. e.g. >100 (default 100)

HTTP OPTIONS:
  -to int    timeout in seconds. (default 10)
  -ua string user agent (default "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0")
  -hm string HTTP Method. (default "HEAD")
  -px string http proxy to use

(vikram@VIKRAM:~)$
```

• Waybackurls

```
(vikram@VIKRAM:~)$ waybackurls -h
Usage of waybackurls:
  -dates
      show date of fetch in the first column
  -get-versions
      list URLs for crawled versions of input URL(s)
  -no-sub
      don't include subdomains of the target domain
(vikram@VIKRAM:~)$
```