Tools Installation:

```
┌──(root💀barot)-[/home/kali]
└─# amass



        . +++ : .                    :                              . +++ .
       +Wⓐⓐⓐⓐⓐⓐ8          &+Wⓐ#              o8W8:          +Wⓐⓐⓐⓐⓐ#.      oWⓐⓐⓐW#+
      &ⓐ#+    .oⓐ##.     .ⓐⓐⓐoⓐW.oⓐⓐo        :ⓐⓐ#&W8o     .ⓐ#:   .:oW+    .ⓐ# +++&#&
      +ⓐ&          &ⓐ&    #ⓐ8 +ⓐWⓐ&8ⓐ+        :ⓐW.    +ⓐ8    +ⓐ:       .ⓐ8
      8ⓐ          ⓐⓐ     8ⓐo  8ⓐ8  WW        .ⓐW     Wⓐ+    .ⓐW.        oⓐ#:
      WW          &ⓐo    8ⓐ:  oⓐ+   oⓐ+      #ⓐ.    8ⓐo    +Wⓐ#+.       +Wⓐ8:
      #ⓐ         :ⓐW     &ⓐ+  &ⓐ+   ⓐ8      :ⓐo     oⓐo    oWⓐⓐW+       oWⓐ8
      oⓐ+        ⓐⓐ&     &ⓐ+  &ⓐ+   #ⓐ  &ⓐ.      .WⓐW      .+#ⓐ&        oⓐW.
       WW        +ⓐWⓐ8.  &ⓐ+   :&    oⓐ+ #ⓐ       :ⓐW&ⓐ&       &ⓐ:    ..     :ⓐo
       :ⓐW:      oⓐ#  +Wo &ⓐ+        :W: +ⓐW&o++oⓐW.  &ⓐ&    8ⓐ#o+&ⓐW.  #ⓐ:      oⓐ+
       :WⓐⓐWWWWⓐⓐ8       +              :&Wⓐⓐⓐⓐ&    &W    .o#ⓐⓐW&.   :WⓐWWWⓐⓐ&
         +o&&&&+.                                                     +oooo.


                                                      v4.2.0
                                   OWASP Amass Project - @owaspamass
                            In-depth Attack Surface Mapping and Asset Discovery


Usage: amass intel|enum [options]
```

```
┌──(root💀barot)-[/home/kali]
└─# go install -v github.com/tomnomnom/anew@latest
go: downloading github.com/tomnomnom/anew v0.1.1
github.com/tomnomnom/anew

┌──(root💀barot)-[/home/kali]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root💀barot)-[/home/kali]
└─# anew


^C

┌──(root💀barot)-[/home/kali]
└─# ls $(go env GOPATH)/bin | grep anew

anew

┌──(root💀barot)-[/home/kali]
```

```
$: command not found


┌──(root💀barot)-[/home/kali]
└─# go install github.com/lc/gau/v2/cmd/gau@latest
go: downloading github.com/lc/gau v1.2.0
go: downloading github.com/lc/gau/v2 v2.2.4
go: downloading github.com/deckarep/golang-set/v2 v2.3.0
go: downloading github.com/sirupsen/logrus v1.8.1
go: downloading github.com/lynxsecurity/pflag v1.1.3
go: downloading github.com/lynxsecurity/viper v1.10.0
go: downloading github.com/valyala/fasthttp v1.31.0
go: downloading github.com/modern-go/concurrent v0.0.0-20180228061459-e0a39a4cb421
go: downloading github.com/bobesa/go-domain-util v0.0.0-20190911083921-4033b5f7dd89
go: downloading github.com/fsnotify/fsnotify v1.5.1
go: downloading github.com/magiconair/properties v1.8.5
go: downloading github.com/mitchellh/mapstructure v1.4.2
go: downloading github.com/spf13/afero v1.6.0
go: downloading github.com/spf13/cast v1.4.1
go: downloading github.com/spf13/jwalterweatherman v1.1.0
go: downloading github.com/subosito/gotenv v1.2.0
go: downloading gopkg.in/ini.v1 v1.64.0
go: downloading github.com/hashicorp/hcl v1.0.0
go: downloading github.com/pelletier/go-toml v1.9.4
```



```
┌──(root💀barot)-[/home/kali]
└─# go install github.com/tomnomnom/waybackurls@latest
go: downloading github.com/tomnomnom/waybackurls v0.1.0

┌──(root💀barot)-[/home/kali]
└─# waybackurls
^C

┌──(root💀barot)-[/home/kali]
└─# 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-subs
        don't include subdomains of the target domain

┌──(root💀barot)-[/home/kali]
└─#
```

```
(Reading database ... 504367 files and directories currently installed.)
Preparing to unpack .../httpx-toolkit_1.1.5-0kali2_amd64.deb ...
Unpacking httpx-toolkit (1.1.5-0kali2) ...
Setting up httpx-toolkit (1.1.5-0kali2) ...
Processing triggers for kali-menu (2025.3.2) ...
```

```
┌──(root㉿barot)-[/home/kali]
└─# httpx-toolkit


   _   _____  _____  __ __
  / / / / _/ /_  __/ __ \ \/ // /
 / /_/ // /   / / / /_/ /\  // /
/ __  // /   / / / ____//  //_/
/_/ /_/___/  /_/ /_/    /_/ /_/
        /_/                v1.1.5


            projectdiscovery.io


Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
```

```
┌──(root㉿barot)-[/home/kali]
└─#
```

```
┌──(root㉿barot)-[/home/kali]
└─# httprobe
Command 'httprobe' not found, but can be installed with:
apt install httprobe
Do you want to install it? (N/y)y
apt install httprobe
The following packages were automatically installed and are no longer required:
  libgdal36         libgeos3.13.1   libqt5ct-common1.8   libsoup-2.4-1        libvpx9
  libgdata-common   libhdf4-0-alt   libsframe1           libsoup2.4-common    node-sellside-emitter
  libgdata22        libogdi4.1      libsigsegv2          libtheora0
Use 'sudo apt autoremove' to remove them.

Installing:
  httprobe

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 4
  Download size: 1,597 kB
  Space needed: 4,653 kB / 4,372 MB available


Get:1 http://kali.download/kali kali-rolling/main amd64 httprobe amd64 0.2-0kali1 [1,597 kB]
Fetched 1,597 kB in 1s (1,787 kB/s)
```

```
┌──(root💀barot)-[/home/kali]
└─# go install github.com/hahwul/dalfox/v2@latest
go: downloading github.com/hahwul/dalfox/v2 v2.12.0
go: downloading github.com/hahwul/dalfox v1.2.1
go: downloading github.com/briandowns/spinner v1.23.2
go: downloading github.com/hahwul/volt v1.0.7
go: downloading github.com/spf13/cobra v1.9.1
go: downloading github.com/spf13/pflag v1.0.6
go: downloading golang.org/x/term v0.32.0
go: downloading github.com/PuerkitoBio/goquery v1.10.3
go: downloading github.com/chromedp/cdproto v0.0.0-20250403032234-65de8f5d025b
go: downloading github.com/labstack/echo/v4 v4.13.4
go: downloading github.com/chromedp/chromedp v0.13.7
go: downloading github.com/sirupsen/logrus v1.9.3
go: downloading github.com/tidwall/sjson v1.2.5
go: downloading github.com/mark3labs/mcp-go v0.32.0
go: downloading github.com/swaggo/echo-swagger v1.4.1
go: downloading github.com/tylerb/graceful v1.2.15
go: downloading golang.org/x/sys v0.33.0
go: downloading github.com/andybalholm/cascadia v1.3.3
go: downloading golang.org/x/net v0.40.0
go: downloading github.com/alecthomas/template v0.0.0-20190718012654-fb15b899a751
```

```
golang.org/x/term
golang.org/x/crypto/ssh/terminal
github.com/schollz/progressbar/v3
github.com/musana/fuzzuli

┌──(root💀barot)-[/home/kali]
└─# fuzzuli

[*] Scan starting time: 2025-09-08 00:53:58


  /_|                        | | (_)
 | |_   _ ___ ____ _   _| | _
 | __| | | |_  /_  / | | | | | |
 | |_| |_| |/ / / /| |_| | | | |
 |_|  \__,_| /__|/__| \__,_|_| |_|

musana.net | @musana
_____

[!] No data found in pipe. Urls must be given using pipe or f parameter!


┌──(root💀barot)-[/home/kali]
└─#
```

```
go: downloading github.com/pierrec/lz4/v4 v4.1.2
go: downloading github.com/ulikunitz/xz v0.5.11
go: downloading github.com/xi2/xz v0.0.0-20171230120015-48954b6210f8

┌──(root💀barot)-[/home/kali]
└─# alterex
alterex: command not found

┌──(root💀barot)-[/home/kali]
└─# alterx


    __    _  ____  ____   ___  __ __
   / /   | |/ / / /___   ___  |  |/_/
  / /_   |   / _/ -_) __/ / / /    <
 /_/ |_/_/\_\_/\__/_/ /_/ /_/|_|


              projectdiscovery.io

[INF] Current alterx version v0.0.6 (latest)
[FTL] alterx: no input found

┌──(root💀barot)-[/home/kali]
└─#
```

```
└─# go install github.com/channyein1337/jsleak@latest
go: downloading github.com/channyein1337/jsleak v0.0.0-20250125082306-7c594ea6c02a
go: finding module for package gopkg.in/yaml.v2
go: found gopkg.in/yaml.v2 in gopkg.in/yaml.v2 v2.4.0

┌──(root💀barot)-[/home/kali]
└─# jsleak
^C

┌──(root💀barot)-[/home/kali]
└─# jsleak -h
Usage of jsleak:
  -c int
        Number of concurrent workers (default 10)
  -e    Complete scope URL or not
  -k    Check status codes for found links
  -l    Enable linkFinder
  -s    Enable secretFinder
  -t string
        Path to YAML file containing regex patterns

┌──(root💀barot)-[/home/kali]
└─#
```

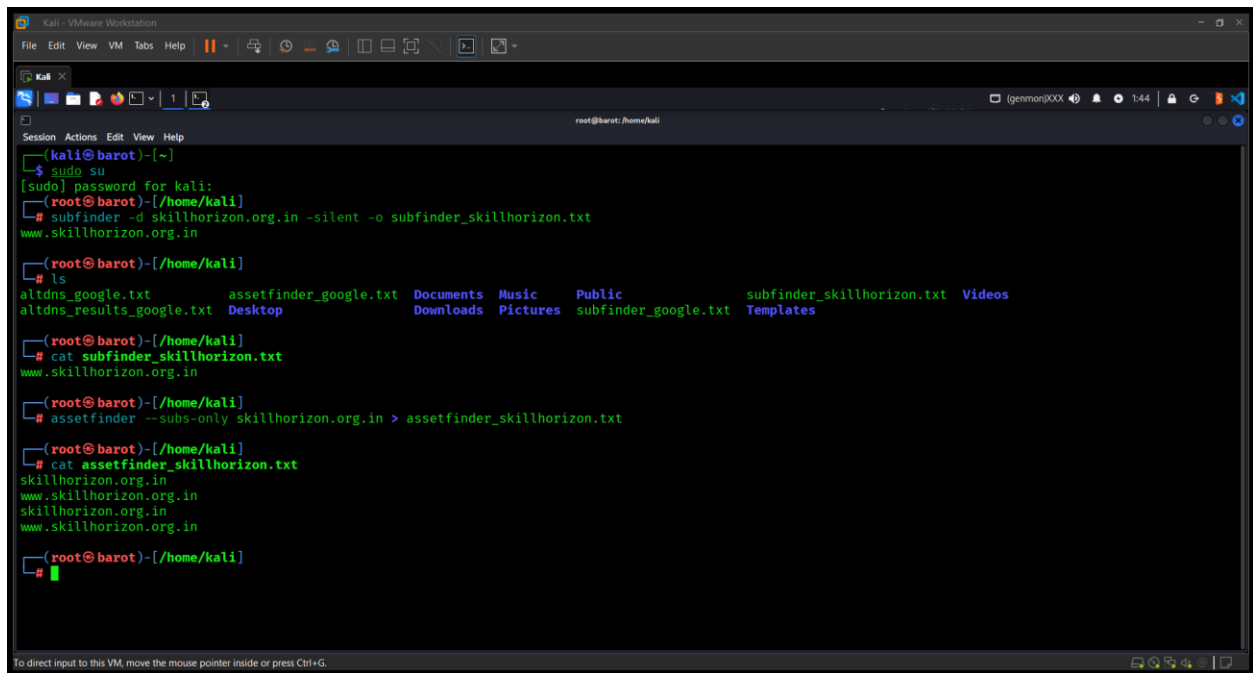Target 1: google.com

```
┌──(root💀barot)-[/home/kali]
└─# assetfinder --subs-only google.com > assetfinder_google.txt

┌──(root💀barot)-[/home/kali]
└─# ls
assetfinder_google.txt    Documents   Music       Public                  Templates
Desktop                   Downloads   Pictures    subfinder_google.txt    Videos

┌──(root💀barot)-[/home/kali]
└─# cat assetfinder_google.txt
meet.google.com
workspace.google.com
google.com
216-239-45-10.google.com
216-239-45-32.google.com
216-239-45-33.google.com
216-239-45-36.google.com
216-239-45-4.google.com
216-239-45-6.google.com
216-239-45-63.google.com
216-239-45-8.google.com
360suite.google.com
```

Target 1: skillhorizon.org.in