OLUWAFIKAYO OYEWOLE

IDEAS/24/95560

Week 1: Reconnaissance, Information Gathering, and Scanning

INT302: Kali Linux Tools and System Security – Lab 1: Reconnaissance (Information Gathering)

Exercise 1:

Use the ping command to find the IP addresses of the following domains:

- facebook.com
- twitter.com
- amazon.com

Record Your Answers:

1. facebook.com: ____102.132.101.35______
2. twitter.com: ___104.244.42.129_______
3. amazon.com: ___54.239.28.85___

Exercise 2:

Run the whois command for the following domains:

- github.com
- linkedin.com
- apple.com

Answer These Questions:

1. What is the registration expiration date for github.com? ____2026-10-03______
2. Who is the registrar for linkedin.com? ___www.markmonitor.com_______
3. What country is the registrant of apple.com from? __ California, USA________

Exercise 3:

Use nslookup to look up DNS information for the following domains:

- bbc.co.uk
- netflix.com

Answer These Questions:

1. What is the IP address for bbc.co.uk? ___151.101.0.81_______

What are the name servers (NS) for netflix.com? ___ns1.p63.dynect.net, ns1.p63.dynect.net, ns2.p63.dynect.net, ns3.p63.dynect.net, ns4.p63.dynect.net_______

Submission Instructions

Submit your results for the exercises above, including:

- IP addresses retrieved using ping
- Domain registration details from whois
- DNS information from nslookup

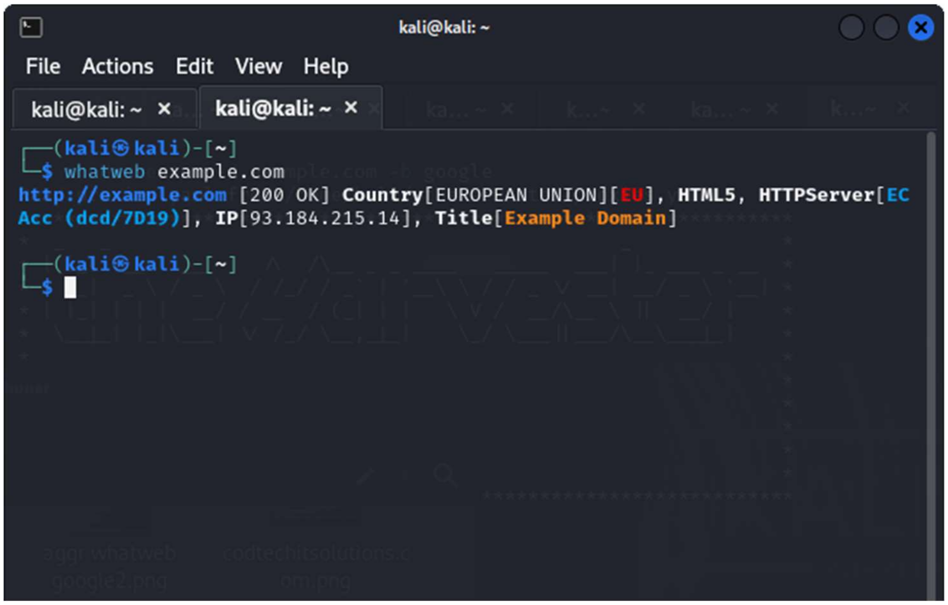
Exercise 1:

Run the whatweb command to detect technologies for the following targets:

- example.com
- stackoverflow.com
- github.com

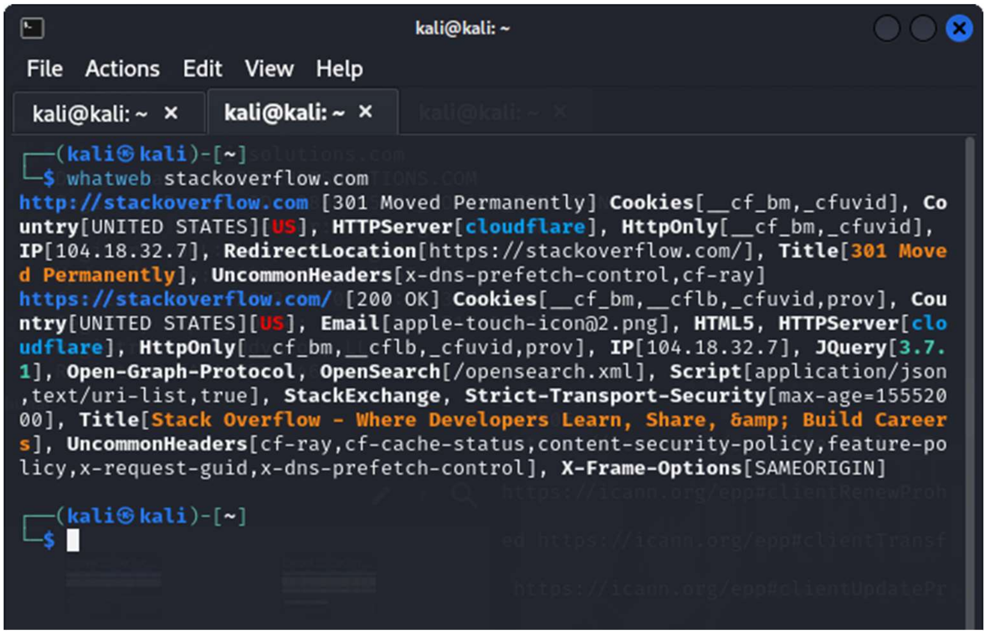
Record Your Findings:

1. **example.com**: ___________



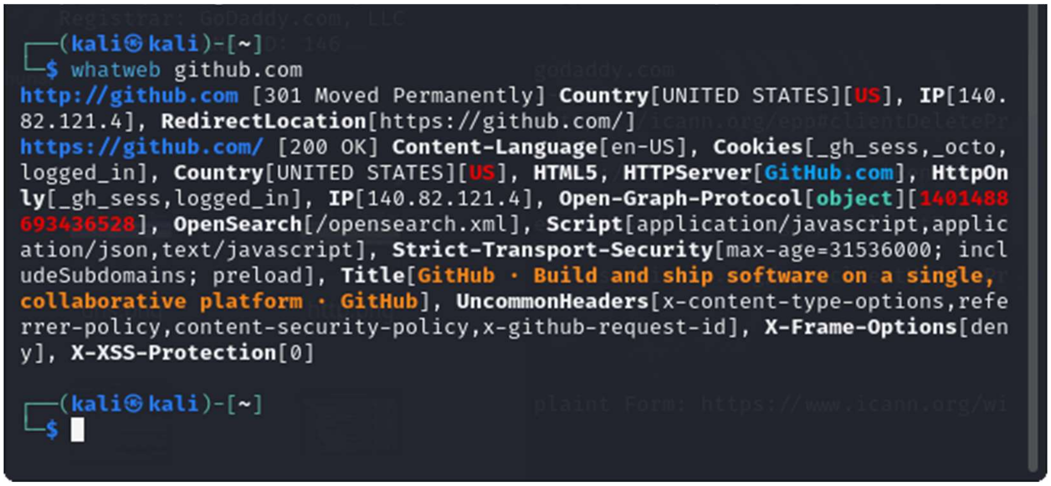
```
┌──(kali㉿kali)-[~]
└─$ whatweb example.com
http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[EC
Acc (dcd/7D19)], IP[93.184.215.14], Title[Example Domain]

┌──(kali㉿kali)-[~]
└─$ █
```

2. **stackoverflow.com**: ___________



```
┌──(kali㉿kali)-[~]
└─$ whatweb stackoverflow.com
http://stackoverflow.com [301 Moved Permanently] Cookies[__cf_bm,_cfuvid], Co
untry[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[__cf_bm,_cfuvid],
IP[104.18.32.7], RedirectLocation[https://stackoverflow.com/], Title[301 Move
d Permanently], UncommonHeaders[x-dns-prefetch-control,cf-ray]
https://stackoverflow.com/ [200 OK] Cookies[__cf_bm,__cflb,_cfuvid,prov], Cou
ntry[UNITED STATES][US], Email[apple-touch-icon@2.png], HTML5, HTTPServer[clo
udflare], HttpOnly[__cf_bm,__cflb,_cfuvid,prov], IP[104.18.32.7], JQuery[3.7.
1], Open-Graph-Protocol, OpenSearch[/opensearch.xml], Script[application/json
,text/uri-list,true], StackExchange, Strict-Transport-Security[max-age=155520
00], Title[Stack Overflow - Where Developers Learn, Share, &amp; Build Career
s], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,feature-po
licy,x-request-guid,x-dns-prefetch-control], X-Frame-Options[SAMEORIGIN]

┌──(kali㉿kali)-[~]
└─$ █
```

3. **github.com**: ___________



```
┌──(kali㉿kali)-[~]
└─$ whatweb github.com
http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[140.
82.121.4], RedirectLocation[https://github.com/]
https://github.com/ [200 OK] Content-Language[en-US], Cookies[_gh_sess,_octo,
logged_in], Country[UNITED STATES][US], HTML5, HTTPServer[GitHub.com], HttpOn
ly[_gh_sess,logged_in], IP[140.82.121.4], Open-Graph-Protocol[object][1401488
693436528], OpenSearch[/opensearch.xml], Script[application/javascript,applic
ation/json,text/javascript], Strict-Transport-Security[max-age=31536000; incl
udeSubdomains; preload], Title[GitHub · Build and ship software on a single,
collaborative platform · GitHub], UncommonHeaders[x-content-type-options,refe
rrer-policy,content-security-policy,x-github-request-id], X-Frame-Options[den
y], X-XSS-Protection[0]

┌──(kali㉿kali)-[~]
└─$ 
```

Step 2: Perform Aggressive Scanning Using whatweb

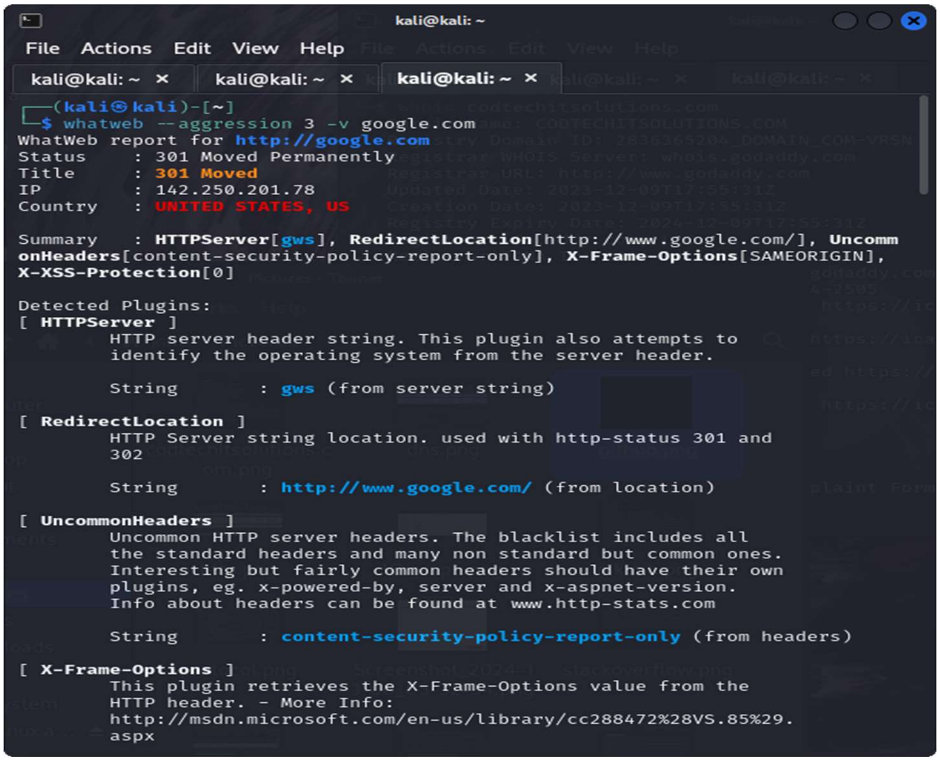
Exercise 2:

Perform an aggressive scan on the following targets:

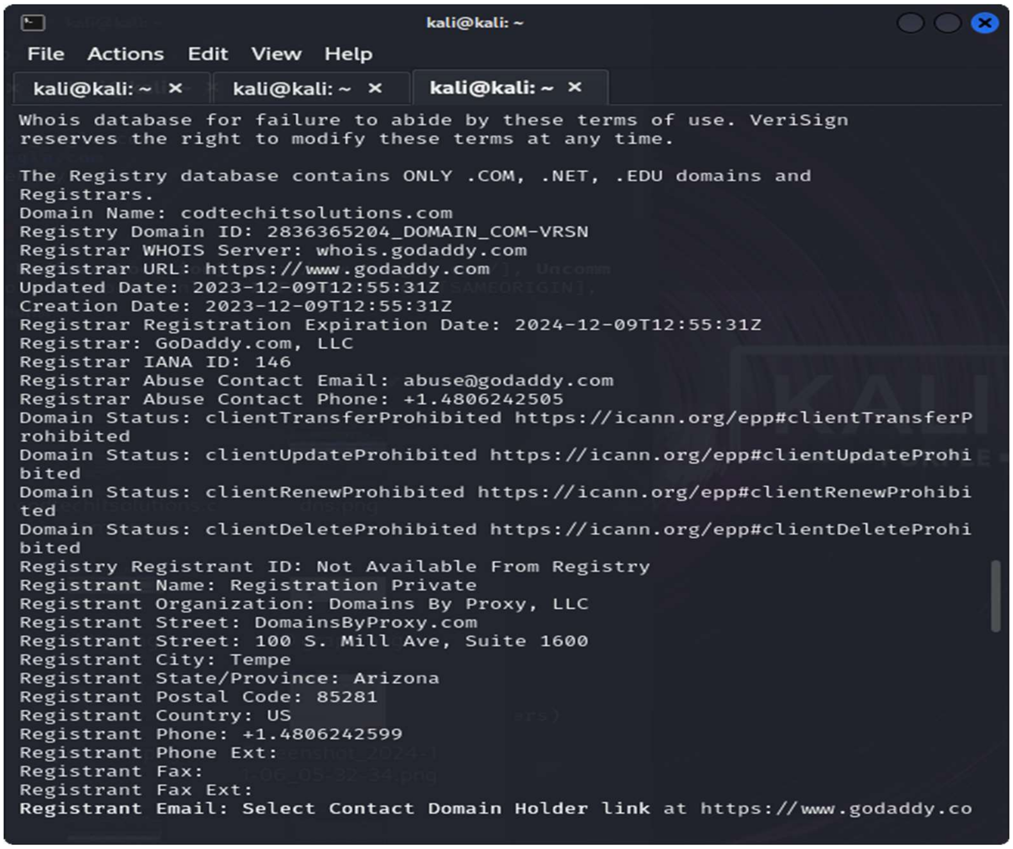
- google.com
- facebook.com

Record Your Findings:

1. **google.com**: ___________

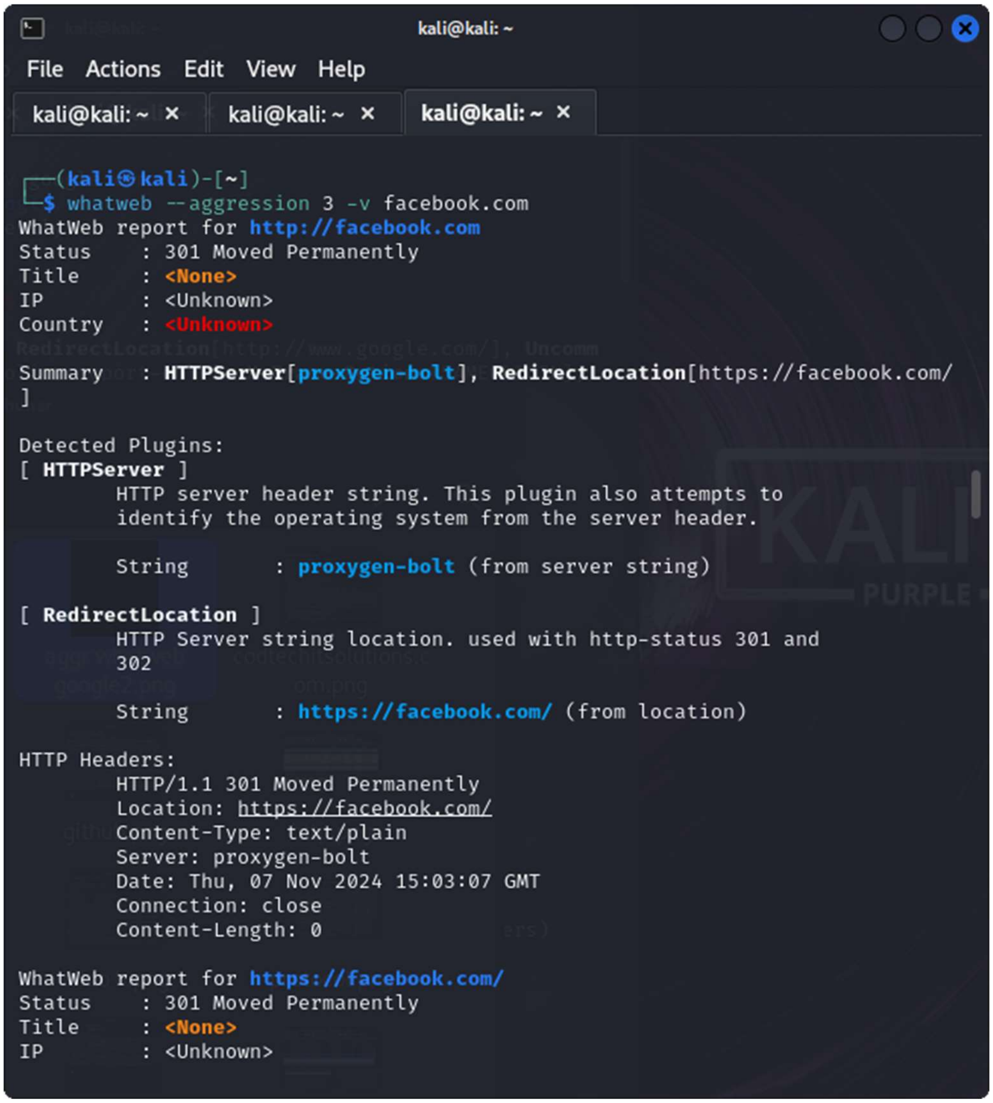


```
┌──(kali㉿kali)-[~]
└─$ whatweb --aggression 3 -v google.com
WhatWeb report for http://google.com
Status    : 301 Moved Permanently
Title     : 301 Moved
IP        : 142.250.201.78
Country   : UNITED STATES, US

Summary   : HTTPServer[gws], RedirectLocation[http://www.google.com/], Uncomm
onHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN],
X-XSS-Protection[0]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : gws (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : http://www.google.com/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : content-security-policy-report-only (from headers)

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx
```



```
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: codtechitsolutions.com
Registry Domain ID: 2836365204_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2023-12-09T12:55:31Z
Creation Date: 2023-12-09T12:55:31Z
Registrar Registration Expiration Date: 2024-12-09T12:55:31Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP
rohibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi
bited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibi
ted
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
bited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 100 S. Mill Ave, Suite 1600
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85281
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.co
```

2. **facebook.com**: ___________



```
┌──(kali㉿kali)-[~]
└─$ whatweb --aggression 3 -v facebook.com
WhatWeb report for http://facebook.com
Status    : 301 Moved Permanently
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>

Summary   : HTTPServer[proxygen-bolt], RedirectLocation[https://facebook.com/
]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : proxygen-bolt (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://facebook.com/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://facebook.com/
        Content-Type: text/plain
        Server: proxygen-bolt
        Date: Thu, 07 Nov 2024 15:03:07 GMT
        Connection: close
        Content-Length: 0

WhatWeb report for https://facebook.com/
Status    : 301 Moved Permanently
Title     : <None>
IP        : <Unknown>
```

Submission Instructions

Submit your results from both exercises, including:

- Detected web technologies from the whatweb command.
- Detailed findings from the aggressive scans.

INT302: Kali Linux Tools and System Security – Lab 3: Subdomain Hunting

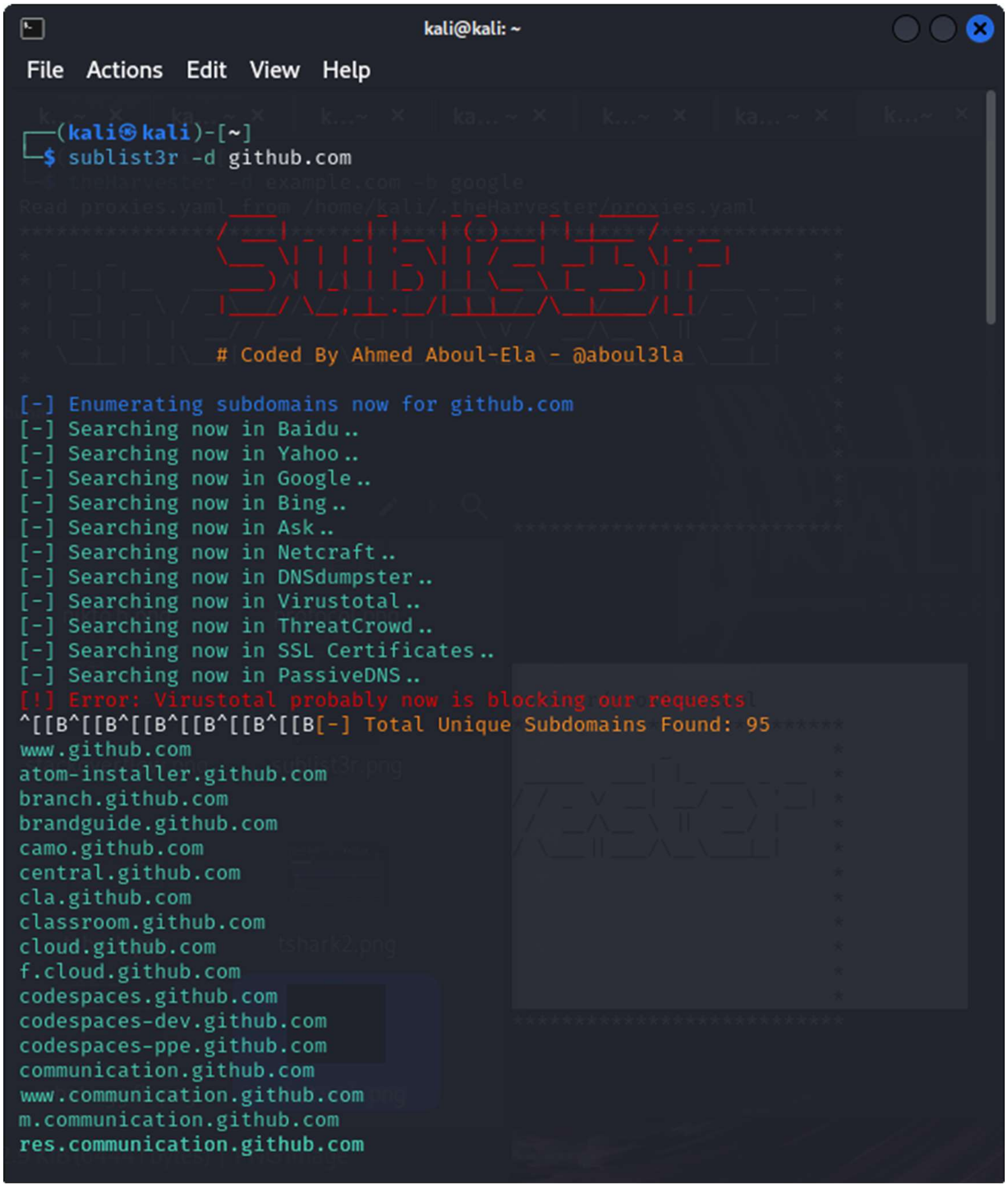
Exercise 1:

Run the sublist3r command for the following domains:

- github.com
- google.com

Record Your Findings:

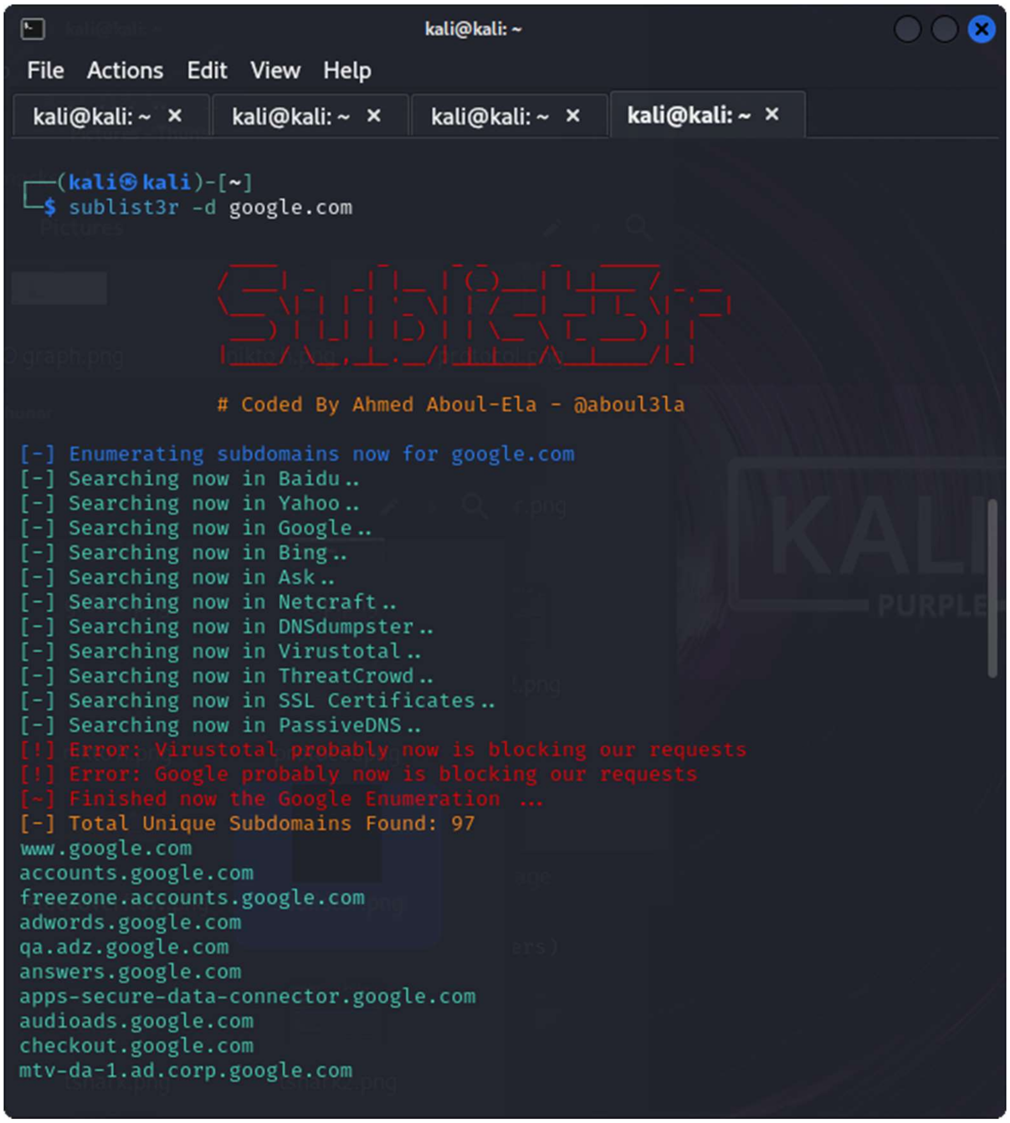
1. **Subdomains for github.com**:



```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d github.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for github.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
^[[B^[[B^[[B^[[B^[[B^[[B[-] Total Unique Subdomains Found: 95
www.github.com
atom-installer.github.com
branch.github.com
brandguide.github.com
camo.github.com
central.github.com
cla.github.com
classroom.github.com
cloud.github.com
f.cloud.github.com
codespaces.github.com
codespaces-dev.github.com
codespaces-ppe.github.com
communication.github.com
www.communication.github.com
m.communication.github.com
res.communication.github.com
```

○

2. **Subdomains for google.com**:



```
┌──(kali㉿kali)-[~]
└─$ sublist3r -d google.com

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 97
www.google.com
accounts.google.com
freezone.accounts.google.com
adwords.google.com
qa.adz.google.com
answers.google.com
apps-secure-data-connector.google.com
audioads.google.com
checkout.google.com
mtv-da-1.ad.corp.google.com
```

Step 2: Directory Discovery Using dirb dirb is a powerful tool for discovering hidden directories and files on web servers.

Instructions:

1. In the terminal, run the dirb command followed by the target URL.

Command Syntax:

dirb <target URL>

Example: dirb

https://example.com

Expected Output:
The command will return a list of directories and files found on the web server.

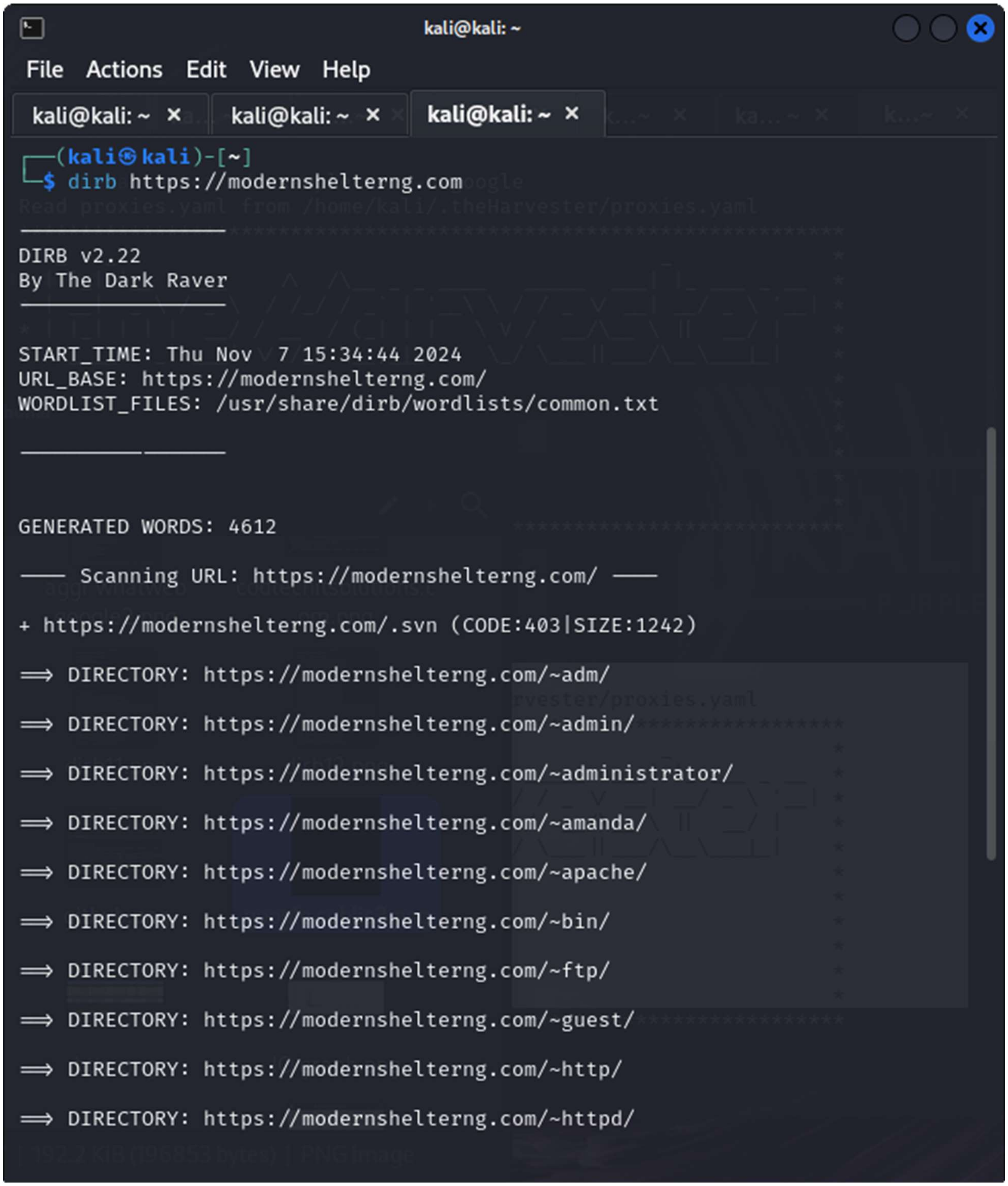
Exercise 2:

Perform a directory discovery scan on the following targets:

- http://example.com (modernshelterng.com)
- http://example.org (godownloads.org)

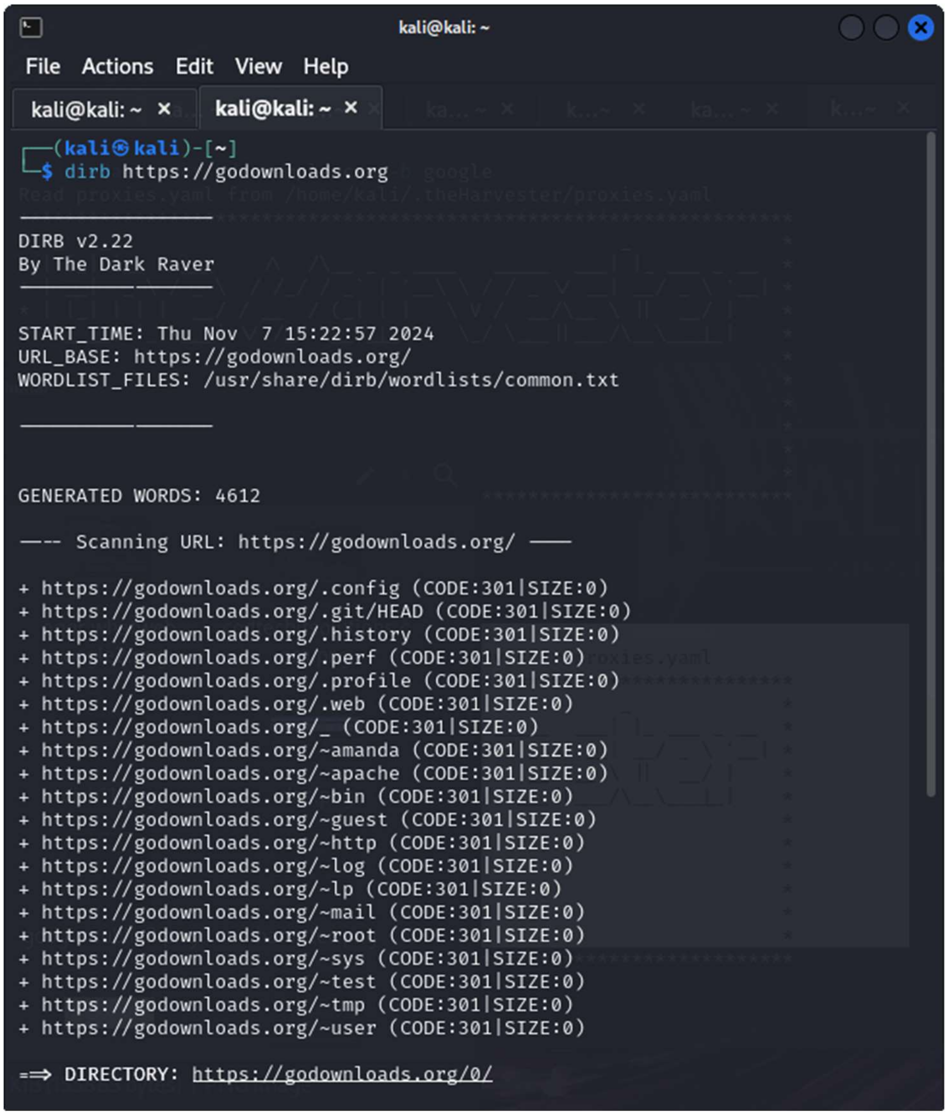
Record Your Findings:

1. **Directories for modernshelterng.com**:

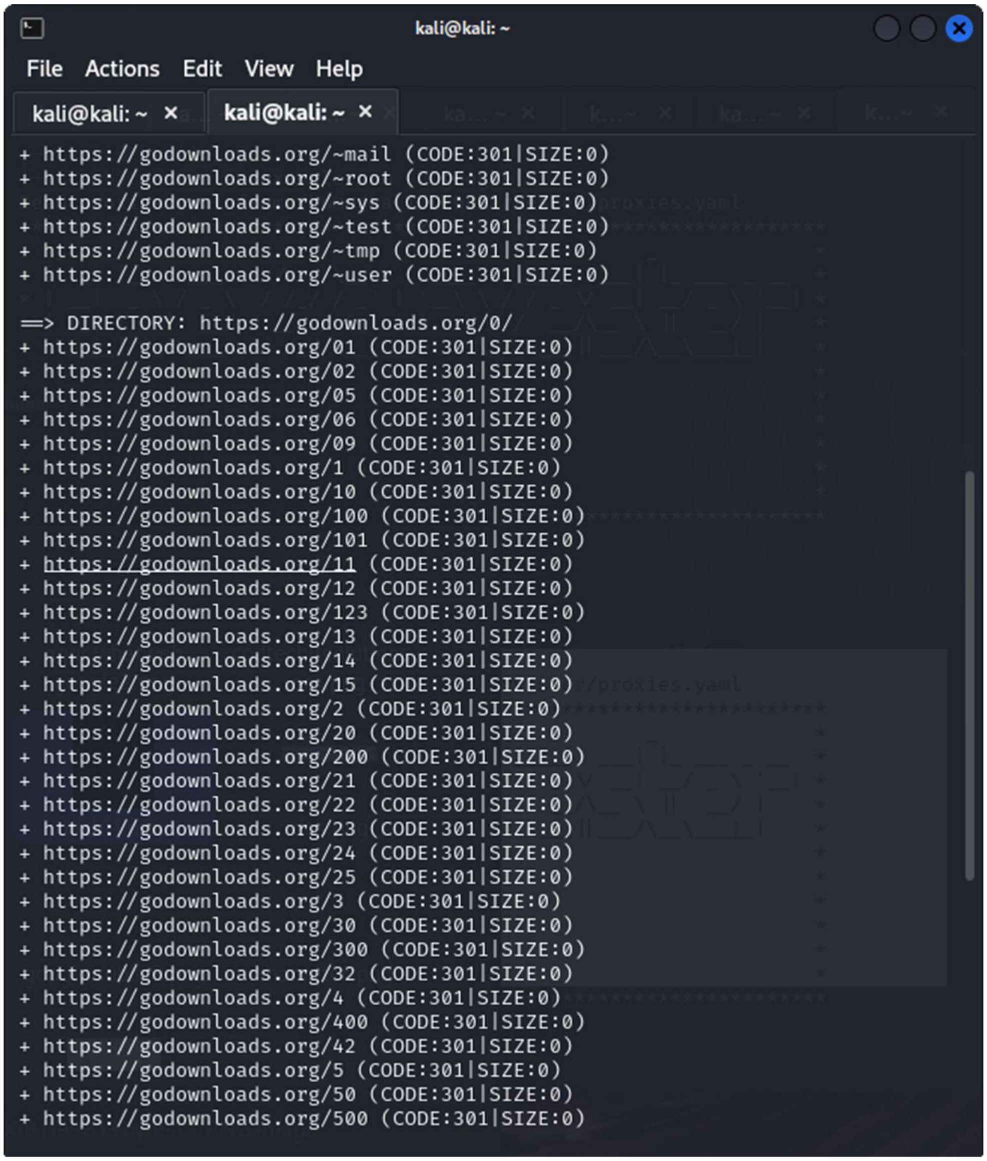


```
┌──(kali㉿kali)-[~]
└─$ dirb https://modernshelterng.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  7 15:34:44 2024
URL_BASE: https://modernshelterng.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://modernshelterng.com/ ----

+ https://modernshelterng.com/.svn (CODE:403|SIZE:1242)

==> DIRECTORY: https://modernshelterng.com/~adm/

==> DIRECTORY: https://modernshelterng.com/~admin/

==> DIRECTORY: https://modernshelterng.com/~administrator/

==> DIRECTORY: https://modernshelterng.com/~amanda/

==> DIRECTORY: https://modernshelterng.com/~apache/

==> DIRECTORY: https://modernshelterng.com/~bin/

==> DIRECTORY: https://modernshelterng.com/~ftp/

==> DIRECTORY: https://modernshelterng.com/~guest/

==> DIRECTORY: https://modernshelterng.com/~http/

==> DIRECTORY: https://modernshelterng.com/~httpd/
```

2. **Directories for godownloads.org**:



```
┌──(kali㉿kali)-[~]
└─$ dirb https://godownloads.org

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Nov  7 15:22:57 2024
URL_BASE: https://godownloads.org/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: https://godownloads.org/ ----

+ https://godownloads.org/.config (CODE:301|SIZE:0)
+ https://godownloads.org/.git/HEAD (CODE:301|SIZE:0)
+ https://godownloads.org/.history (CODE:301|SIZE:0)
+ https://godownloads.org/.perf (CODE:301|SIZE:0)
+ https://godownloads.org/.profile (CODE:301|SIZE:0)
+ https://godownloads.org/.web (CODE:301|SIZE:0)
+ https://godownloads.org/_ (CODE:301|SIZE:0)
+ https://godownloads.org/~amanda (CODE:301|SIZE:0)
+ https://godownloads.org/~apache (CODE:301|SIZE:0)
+ https://godownloads.org/~bin (CODE:301|SIZE:0)
+ https://godownloads.org/~guest (CODE:301|SIZE:0)
+ https://godownloads.org/~http (CODE:301|SIZE:0)
+ https://godownloads.org/~log (CODE:301|SIZE:0)
+ https://godownloads.org/~lp (CODE:301|SIZE:0)
+ https://godownloads.org/~mail (CODE:301|SIZE:0)
+ https://godownloads.org/~root (CODE:301|SIZE:0)
+ https://godownloads.org/~sys (CODE:301|SIZE:0)
+ https://godownloads.org/~test (CODE:301|SIZE:0)
+ https://godownloads.org/~tmp (CODE:301|SIZE:0)
+ https://godownloads.org/~user (CODE:301|SIZE:0)

==> DIRECTORY: https://godownloads.org/0/
```



```
+ https://godownloads.org/~mail (CODE:301|SIZE:0)
+ https://godownloads.org/~root (CODE:301|SIZE:0)
+ https://godownloads.org/~sys (CODE:301|SIZE:0)
+ https://godownloads.org/~test (CODE:301|SIZE:0)
+ https://godownloads.org/~tmp (CODE:301|SIZE:0)
+ https://godownloads.org/~user (CODE:301|SIZE:0)

==> DIRECTORY: https://godownloads.org/0/
+ https://godownloads.org/01 (CODE:301|SIZE:0)
+ https://godownloads.org/02 (CODE:301|SIZE:0)
+ https://godownloads.org/05 (CODE:301|SIZE:0)
+ https://godownloads.org/06 (CODE:301|SIZE:0)
+ https://godownloads.org/09 (CODE:301|SIZE:0)
+ https://godownloads.org/1 (CODE:301|SIZE:0)
+ https://godownloads.org/10 (CODE:301|SIZE:0)
+ https://godownloads.org/100 (CODE:301|SIZE:0)
+ https://godownloads.org/101 (CODE:301|SIZE:0)
+ https://godownloads.org/11 (CODE:301|SIZE:0)
+ https://godownloads.org/12 (CODE:301|SIZE:0)
+ https://godownloads.org/123 (CODE:301|SIZE:0)
+ https://godownloads.org/13 (CODE:301|SIZE:0)
+ https://godownloads.org/14 (CODE:301|SIZE:0)
+ https://godownloads.org/15 (CODE:301|SIZE:0)
+ https://godownloads.org/2 (CODE:301|SIZE:0)
+ https://godownloads.org/20 (CODE:301|SIZE:0)
+ https://godownloads.org/200 (CODE:301|SIZE:0)
+ https://godownloads.org/21 (CODE:301|SIZE:0)
+ https://godownloads.org/22 (CODE:301|SIZE:0)
+ https://godownloads.org/23 (CODE:301|SIZE:0)
+ https://godownloads.org/24 (CODE:301|SIZE:0)
+ https://godownloads.org/25 (CODE:301|SIZE:0)
+ https://godownloads.org/3 (CODE:301|SIZE:0)
+ https://godownloads.org/30 (CODE:301|SIZE:0)
+ https://godownloads.org/300 (CODE:301|SIZE:0)
+ https://godownloads.org/32 (CODE:301|SIZE:0)
+ https://godownloads.org/4 (CODE:301|SIZE:0)
+ https://godownloads.org/400 (CODE:301|SIZE:0)
+ https://godownloads.org/42 (CODE:301|SIZE:0)
+ https://godownloads.org/5 (CODE:301|SIZE:0)
+ https://godownloads.org/50 (CODE:301|SIZE:0)
+ https://godownloads.org/500 (CODE:301|SIZE:0)
```

Step 3: Information Gathering Using theHarvester

theHarvester is a tool for gathering emails, subdomains, and other relevant information from search engines.

Instructions:

1. In the terminal, run the theHarvester command followed by the target domain.

Command Syntax:

```
theharvester -d <target domain> -b google
```

Example:

```
theharvester -d example.com -b google
```

Expected Output:
The output will show collected emails and other information about the specified domain.

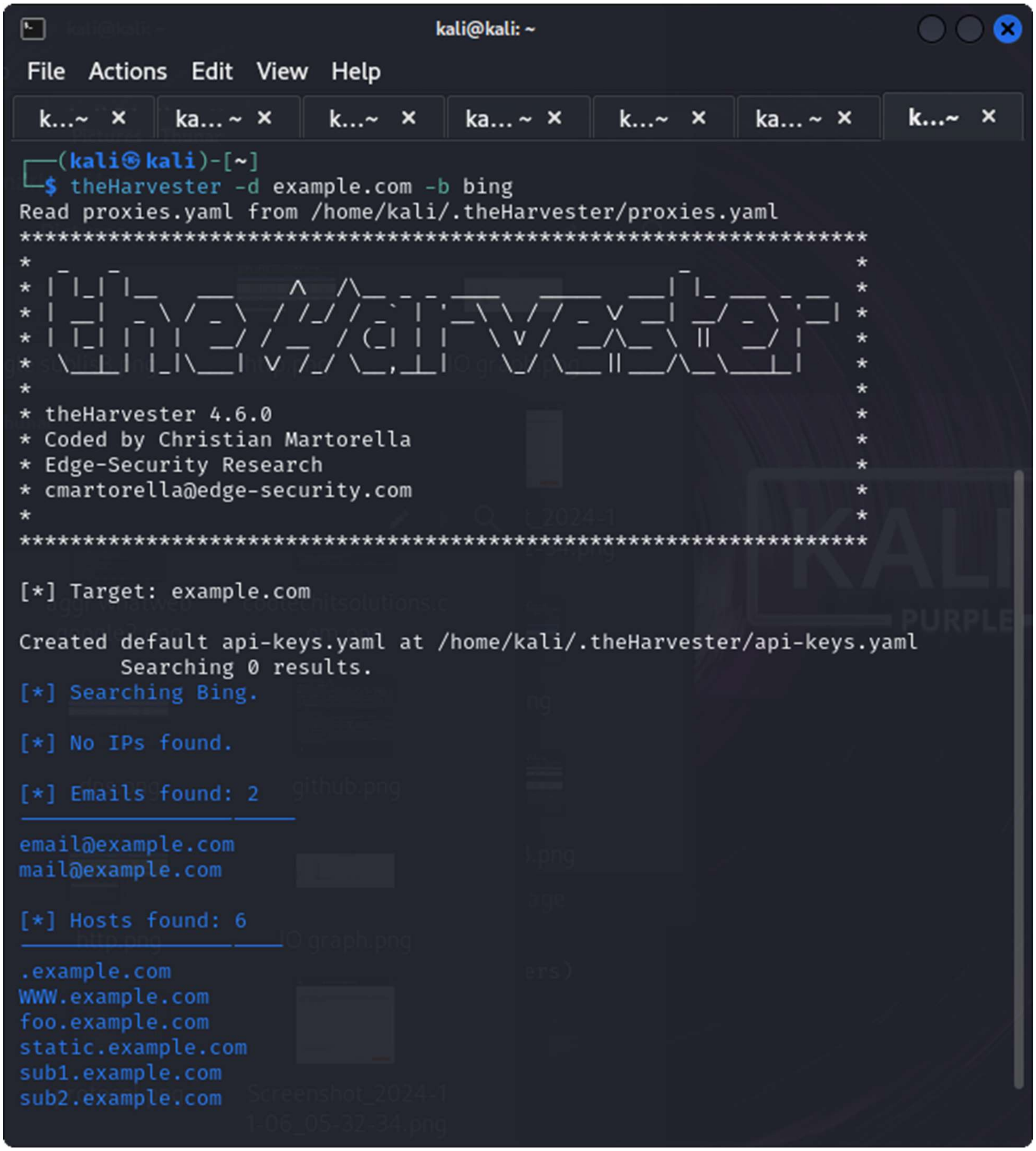
Exercise 3:

Use theHarvester to gather information on the following domain:

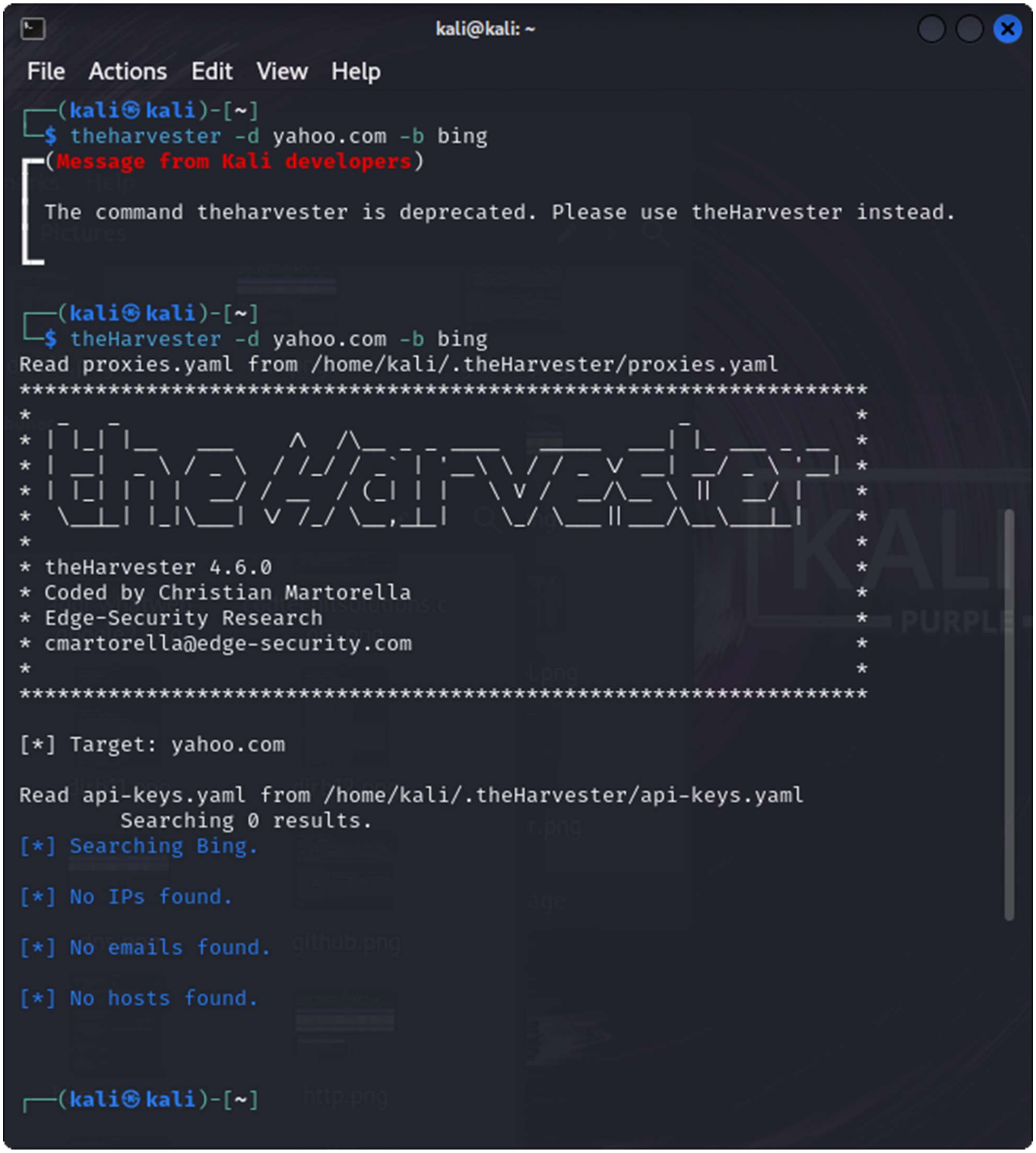
- example.com

Record Your Findings:

- **Emails and Information Gathered**:



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d example.com -b bing
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: example.com

Created default api-keys.yaml at /home/kali/.theHarvester/api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 2
______________________
email@example.com
mail@example.com

[*] Hosts found: 6
_____________________
.example.com
WWW.example.com
foo.example.com
static.example.com
sub1.example.com
sub2.example.com
```



```
┌──(kali㉿kali)-[~]
└─$ theharvester -d yahoo.com -b bing
┏━(Message from Kali developers)
┃
┃ The command theharvester is deprecated. Please use theHarvester instead.
┃
┗━

┌──(kali㉿kali)-[~]
└─$ theHarvester -d yahoo.com -b bing
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] Target: yahoo.com

Read api-keys.yaml from /home/kali/.theHarvester/api-keys.yaml
        Searching 0 results.
[*] Searching Bing.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.


┌──(kali㉿kali)-[~]
```

○

Submission Instructions

Submit your results from all exercises, including:

- Detected subdomains from sublist3r.

- Discovered directories from dirb.
- Information gathered using theHarvester.