A-I Vocational Training Institute of Cyber Security (AIVTIC)

PROGRAMME: BAZE UNIVERSITY INTERNSHIP

ASSIGNMENT

PRESENTED BY

PHILIP AKISANNI AKWUCHI
IDEAS/24/29921

COURSE CODE: INT302
COURSE TITLE: Kali Linux Tools and System Security

COURSE FACILITATOR: AHMED BUKAR

NOVEMBER, 2024.

Lab 1: Reconnaissance (Information Gathering)

Exercise 1: Use the ping command to find the IP addresses of the following domains:

1. facebook.com: 102.132.101.35

2. twitter.com: 104.244.42.193

3. amazon.com: 54.239.28.85

Exercise 2: Run the whois command for the following domains:

Answer These Questions:

1. What is the registration expiration date for github.com? 2026-10-09T18:20:50Z

2. Who is the registrar for linkedin.com? MarkMonitor Inc.

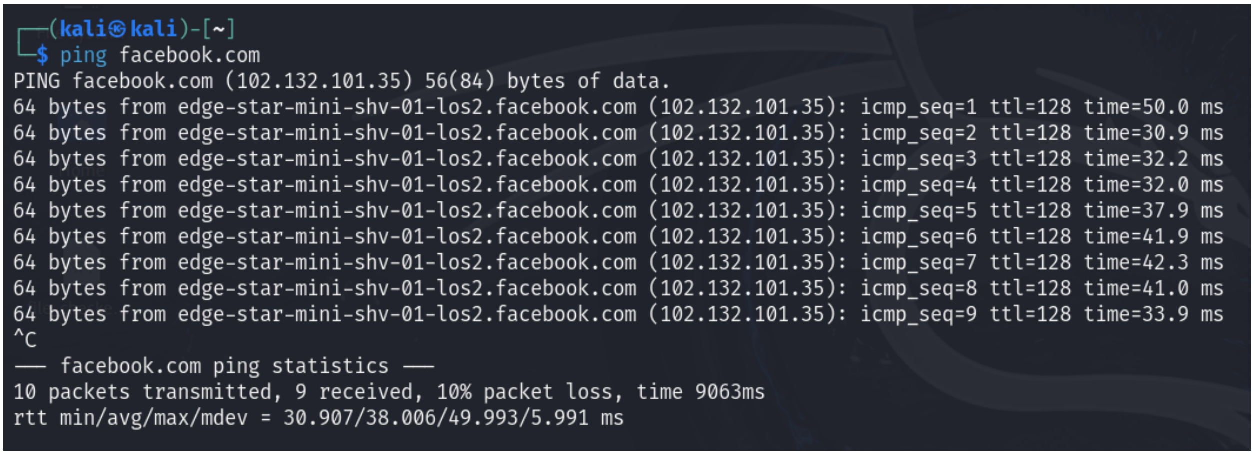
3. What country is the registrant of apple.com from? US

Exercise 3: Use nslookup to look up DNS information for the following domains:

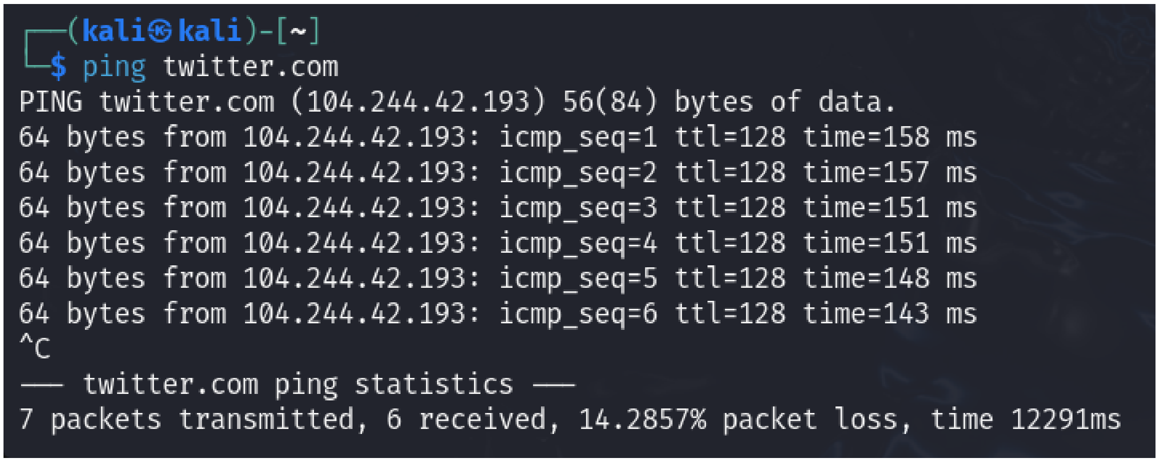
Answer These Questions:

1. What is the IP address for bbc.co.uk? 192.168.253.2#53

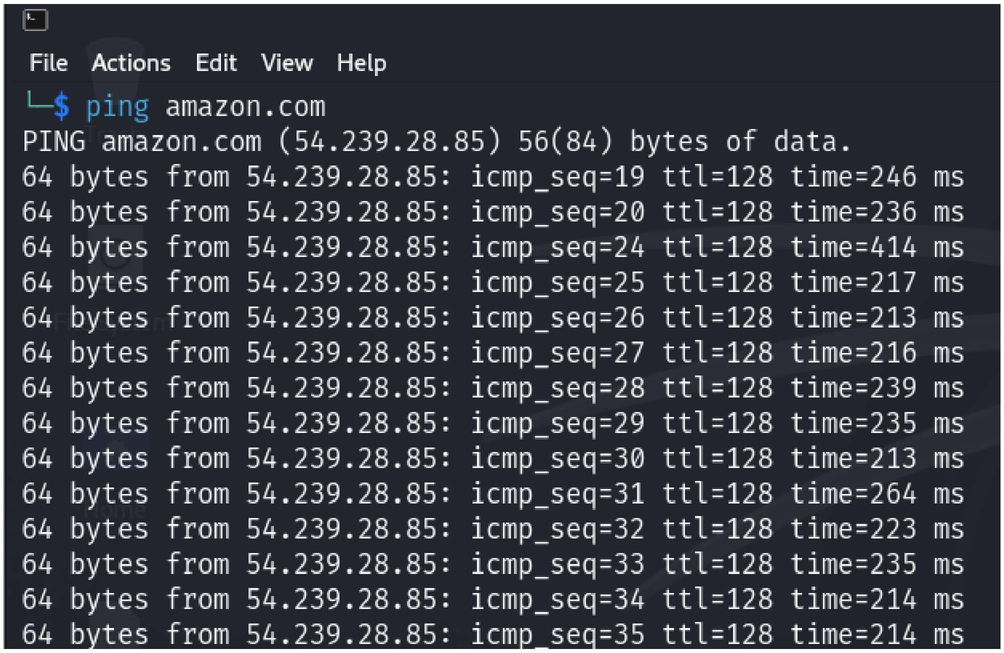
2. What are the name servers (NS) for netflix.com? 192.168.253.2/netlix.com



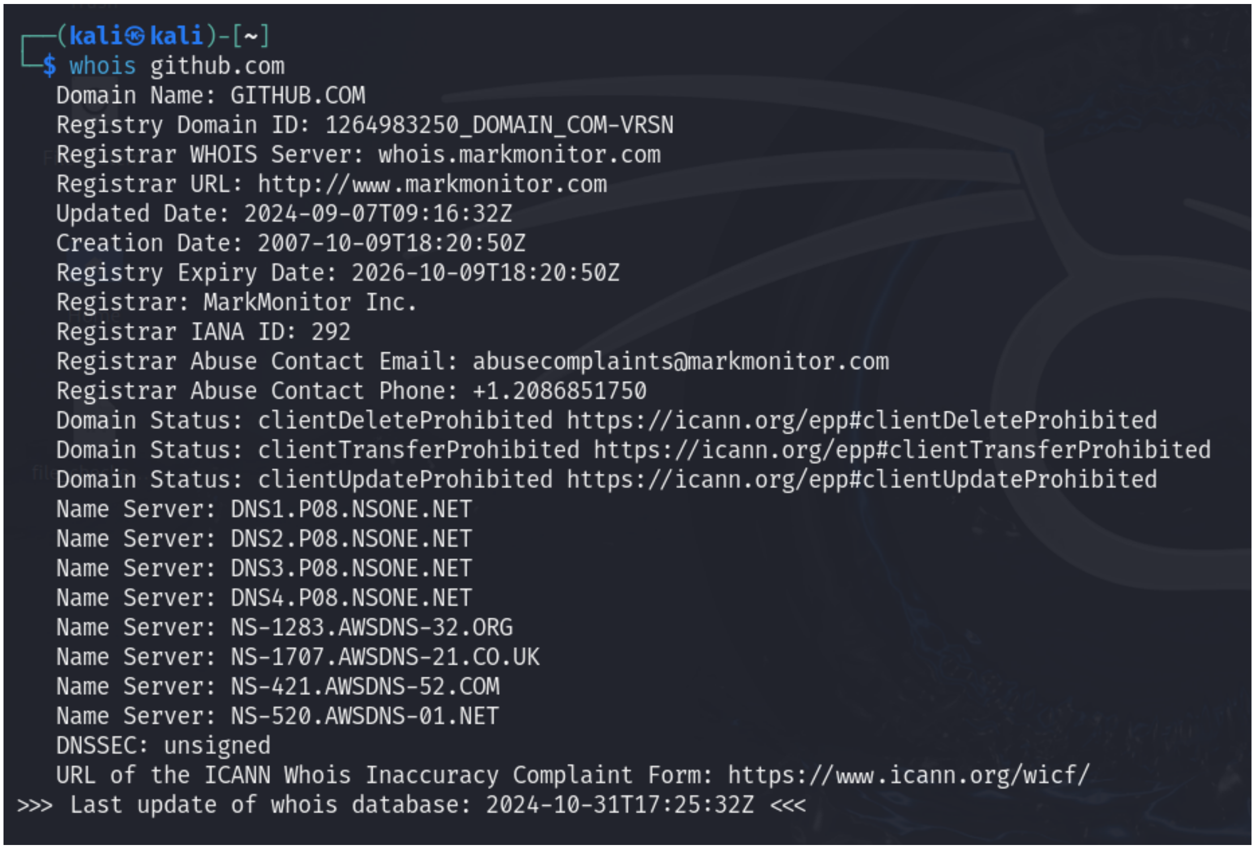
```
┌──(kali㉿kali)-[~]
└─$ ping facebook.com
PING facebook.com (102.132.101.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=1 ttl=128 time=50.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=2 ttl=128 time=30.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=3 ttl=128 time=32.2 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=4 ttl=128 time=32.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=5 ttl=128 time=37.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=6 ttl=128 time=41.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=7 ttl=128 time=42.3 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=8 ttl=128 time=41.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.35): icmp_seq=9 ttl=128 time=33.9 ms
^C
--- facebook.com ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 9063ms
rtt min/avg/max/mdev = 30.907/38.006/49.993/5.991 ms
```



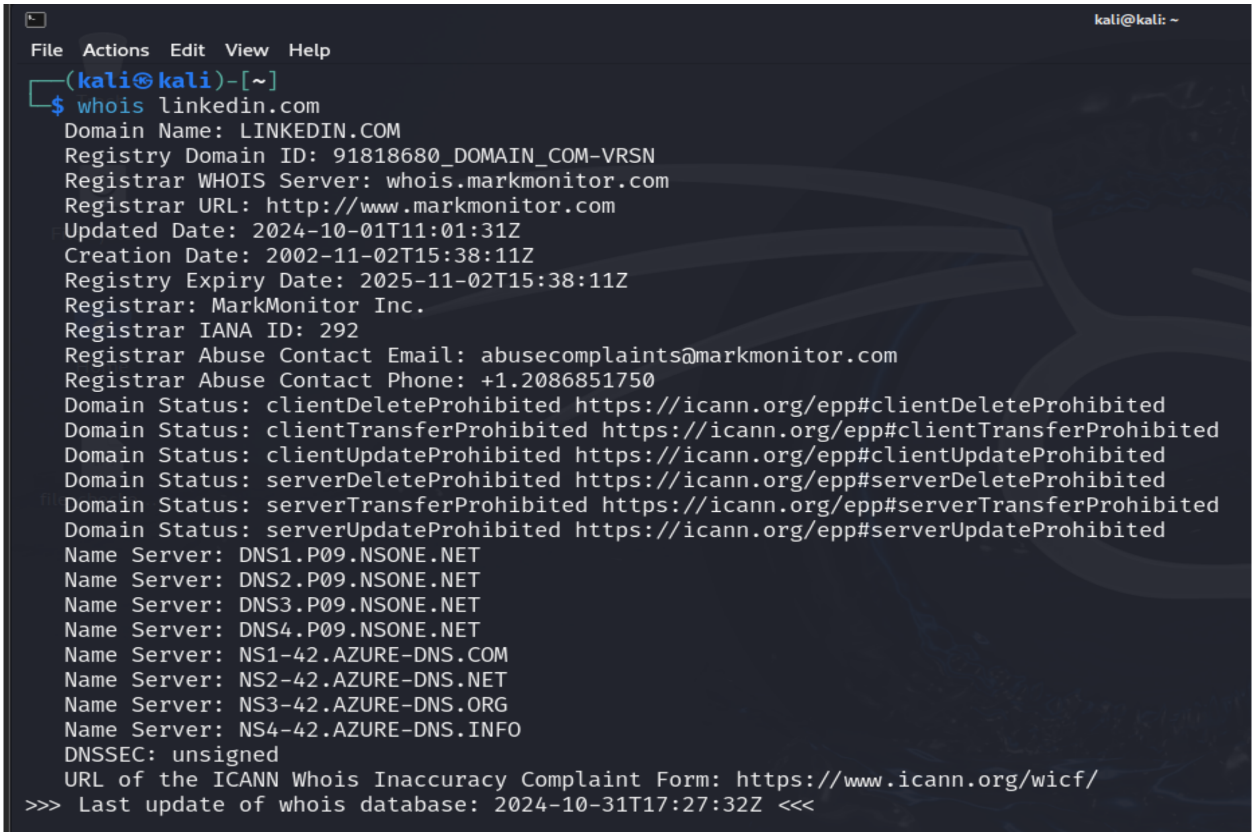
```
┌──(kali㉿kali)-[~]
└─$ ping twitter.com
PING twitter.com (104.244.42.193) 56(84) bytes of data.
64 bytes from 104.244.42.193: icmp_seq=1 ttl=128 time=158 ms
64 bytes from 104.244.42.193: icmp_seq=2 ttl=128 time=157 ms
64 bytes from 104.244.42.193: icmp_seq=3 ttl=128 time=151 ms
64 bytes from 104.244.42.193: icmp_seq=4 ttl=128 time=151 ms
64 bytes from 104.244.42.193: icmp_seq=5 ttl=128 time=148 ms
64 bytes from 104.244.42.193: icmp_seq=6 ttl=128 time=143 ms
^C
─── twitter.com ping statistics ───
7 packets transmitted, 6 received, 14.2857% packet loss, time 12291ms
```



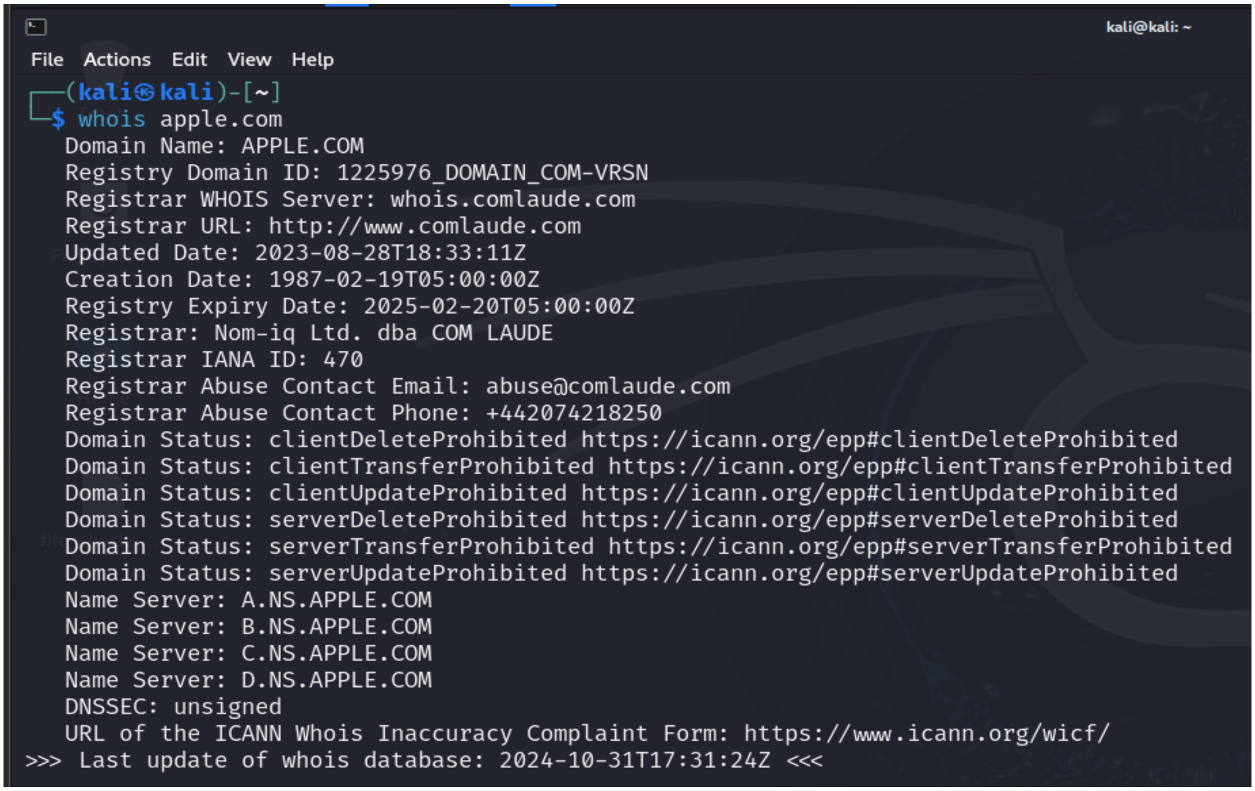
```
└─$ ping amazon.com
PING amazon.com (54.239.28.85) 56(84) bytes of data.
64 bytes from 54.239.28.85: icmp_seq=19 ttl=128 time=246 ms
64 bytes from 54.239.28.85: icmp_seq=20 ttl=128 time=236 ms
64 bytes from 54.239.28.85: icmp_seq=24 ttl=128 time=414 ms
64 bytes from 54.239.28.85: icmp_seq=25 ttl=128 time=217 ms
64 bytes from 54.239.28.85: icmp_seq=26 ttl=128 time=213 ms
64 bytes from 54.239.28.85: icmp_seq=27 ttl=128 time=216 ms
64 bytes from 54.239.28.85: icmp_seq=28 ttl=128 time=239 ms
64 bytes from 54.239.28.85: icmp_seq=29 ttl=128 time=235 ms
64 bytes from 54.239.28.85: icmp_seq=30 ttl=128 time=213 ms
64 bytes from 54.239.28.85: icmp_seq=31 ttl=128 time=264 ms
64 bytes from 54.239.28.85: icmp_seq=32 ttl=128 time=223 ms
64 bytes from 54.239.28.85: icmp_seq=33 ttl=128 time=235 ms
64 bytes from 54.239.28.85: icmp_seq=34 ttl=128 time=214 ms
64 bytes from 54.239.28.85: icmp_seq=35 ttl=128 time=214 ms
```



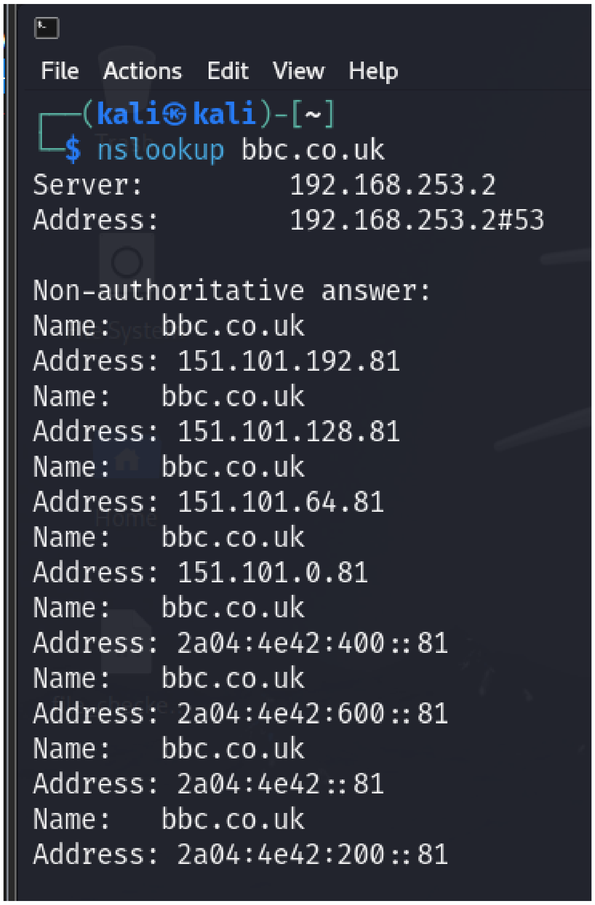
```
┌──(kali㉿kali)-[~]
└─$ whois github.com
   Domain Name: GITHUB.COM
   Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-09-07T09:16:32Z
   Creation Date: 2007-10-09T18:20:50Z
   Registry Expiry Date: 2026-10-09T18:20:50Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: DNS1.P08.NSONE.NET
   Name Server: DNS2.P08.NSONE.NET
   Name Server: DNS3.P08.NSONE.NET
   Name Server: DNS4.P08.NSONE.NET
   Name Server: NS-1283.AWSDNS-32.ORG
   Name Server: NS-1707.AWSDNS-21.CO.UK
   Name Server: NS-421.AWSDNS-52.COM
   Name Server: NS-520.AWSDNS-01.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-31T17:25:32Z <<<
```



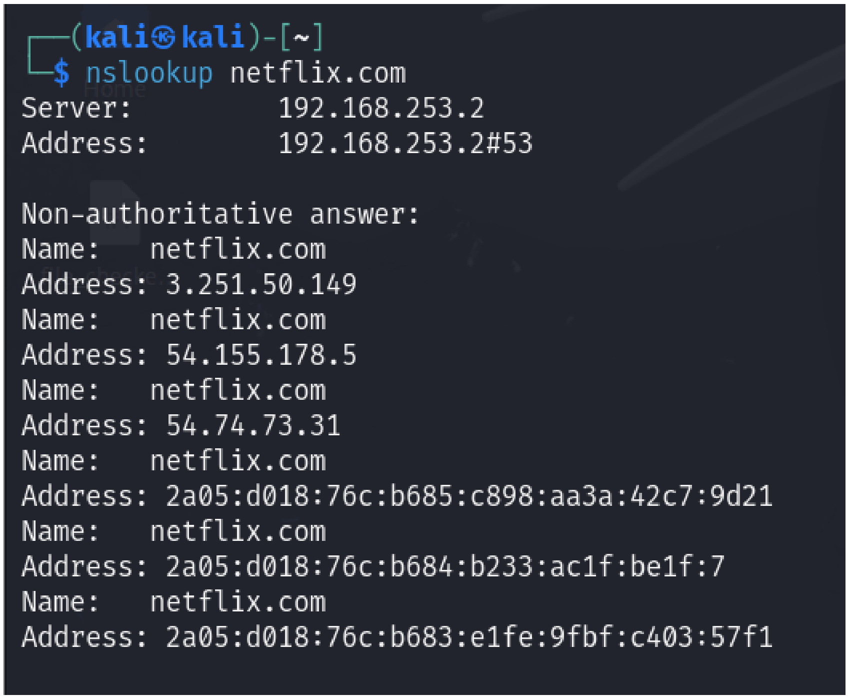
```
┌──(kali㉿kali)-[~]
└─$ whois linkedin.com
   Domain Name: LINKEDIN.COM
   Registry Domain ID: 91818680_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-10-01T11:01:31Z
   Creation Date: 2002-11-02T15:38:11Z
   Registry Expiry Date: 2025-11-02T15:38:11Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: DNS1.P09.NSONE.NET
   Name Server: DNS2.P09.NSONE.NET
   Name Server: DNS3.P09.NSONE.NET
   Name Server: DNS4.P09.NSONE.NET
   Name Server: NS1-42.AZURE-DNS.COM
   Name Server: NS2-42.AZURE-DNS.NET
   Name Server: NS3-42.AZURE-DNS.ORG
   Name Server: NS4-42.AZURE-DNS.INFO
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-31T17:27:32Z <<<
```



```
┌──(kali㉿kali)-[~]
└─$ whois apple.com
   Domain Name: APPLE.COM
   Registry Domain ID: 1225976_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.comlaude.com
   Registrar URL: http://www.comlaude.com
   Updated Date: 2023-08-28T18:33:11Z
   Creation Date: 1987-02-19T05:00:00Z
   Registry Expiry Date: 2025-02-20T05:00:00Z
   Registrar: Nom-iq Ltd. dba COM LAUDE
   Registrar IANA ID: 470
   Registrar Abuse Contact Email: abuse@comlaude.com
   Registrar Abuse Contact Phone: +442074218250
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: A.NS.APPLE.COM
   Name Server: B.NS.APPLE.COM
   Name Server: C.NS.APPLE.COM
   Name Server: D.NS.APPLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-10-31T17:31:24Z <<<
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup bbc.co.uk
Server:         192.168.253.2
Address:        192.168.253.2#53

Non-authoritative answer:
Name:   bbc.co.uk
Address: 151.101.192.81
Name:   bbc.co.uk
Address: 151.101.128.81
Name:   bbc.co.uk
Address: 151.101.64.81
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
Address: 2a04:4e42:400::81
Name:   bbc.co.uk
Address: 2a04:4e42:600::81
Name:   bbc.co.uk
Address: 2a04:4e42::81
Name:   bbc.co.uk
Address: 2a04:4e42:200::81
```



```
┌──(kali㉿kali)-[~]
└─$ nslookup netflix.com
Server:         192.168.253.2
Address:        192.168.253.2#53

Non-authoritative answer:
Name:   netflix.com
Address: 3.251.50.149
Name:   netflix.com
Address: 54.155.178.5
Name:   netflix.com
Address: 54.74.73.31
Name:   netflix.com
Address: 2a05:d018:76c:b685:c898:aa3a:42c7:9d21
Name:   netflix.com
Address: 2a05:d018:76c:b684:b233:ac1f:be1f:7
Name:   netflix.com
Address: 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1
```

Lab 2: Website Enumeration and Information Gathering

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

Record Your Findings:

1. **example.com**: http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECAcc (dcd/7D43)], IP[93.184.215.14], Title[Example Domain]

2. **stackoverflow.com**: http://stackoverflow.com [301 Moved Permanently] Cookies[__cf_bm,_cfuvid], Country[RESERVED][ZZ], HTTPServer[cloudflare], HttpOnly[__cf_bm,_cfuvid], IP[172.64.155.249], RedirectLocation[https://stackoverflow.com/], Title[301 Moved Permanently], UncommonHeaders[x-dns-prefetch-control,cf-ray]

https://stackoverflow.com/ [200 OK] Cookies[__cf_bm,__cflb,_cfuvid,prov], Country[UNITED STATES][US], Email[apple-touch-icon@2.png], HTML5, HTTPServer[cloudflare], 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=15552000], Title[Stack Overflow - Where Developers Learn, Share, &amp; Build Careers], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,feature-policy,x-request-guid,x-dns-prefetch-control], X-Frame-Options[SAMEORIGIN]

3. **github.com**: http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[140.82.121.3], 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], HttpOnly[_gh_sess,logged_in], IP[140.82.121.3], Open-Graph-Protocol[object][1401488693436528], OpenSearch[/opensearch.xml], Script[application/javascript,application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomains; preload], Title[GitHub · Build and ship software on a single, collaborative platform · GitHub], UncommonHeaders[x-content-type-options,referrer-policy,content-security-policy,x-github-request-id], X-Frame-Options[deny], X-XSS-Protection[0]

Exercise 2: Perform an aggressive scan on the following targets:

Record Your Findings:

1. **google.com**: WhatWeb report for http://google.com

```
Status    : 301 Moved Permanently

Title     : 301 Moved

IP        : 142.250.178.174

Country   : UNITED STATES, US

Summary   : HTTPServer[gws], RedirectLocation[http://www.google.com/], UncommonHeaders[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

          String       : SAMEORIGIN

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

          String       : 0
```

```
HTTP Headers:
    HTTP/1.1 301 Moved Permanently
    Location: http://www.google.com/
    Content-Type: text/html; charset=UTF-8
    Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-RsPRFXjiGq2eiK1aWFyFgQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
    Date: Thu, 31 Oct 2024 17:52:19 GMT
    Expires: Sat, 30 Nov 2024 17:52:19 GMT
    Cache-Control: public, max-age=2592000
    Server: gws
    Content-Length: 219
    X-XSS-Protection: 0
    X-Frame-Options: SAMEORIGIN
    Connection: close
```

2. **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, 31 Oct 2024 17:54:13 GMT
        Connection: close
        Content-Length: 0\
WhatWeb report for https://facebook.com/
Status    : 301 Moved Permanently
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>
Summary   : RedirectLocation[https://www.facebook.com/], Strict-Transport-
Security[max-age=15552000; preload], UncommonHeaders[x-fb-debug,x-fb-
connection-quality,alt-svc]\
Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302
```

```
	String       : https://www.facebook.com/ (from location)
[ Strict-Transport-Security ]
	Strict-Transport-Security is an HTTP header that restricts
	a web browser from accessing a website without the security
	of the HTTPS protocol.


	String       : max-age=15552000; preload
[ 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       : x-fb-debug,x-fb-connection-quality,alt-svc (from headers)
HTTP Headers:
	HTTP/1.1 301 Moved Permanently
	Location: https://www.facebook.com/
	Strict-Transport-Security: max-age=15552000; preload
	Content-Type: text/html; charset="utf-8"
	X-FB-Debug:
cwAzQXQjgU43J3nCtEW9mSDar3zehF1EEOng7hrasOcf4guD68vnVANCsUaqn
wVlSt6fqphW7EpSmFFia8okXA==
	Date: Thu, 31 Oct 2024 17:54:16 GMT
	X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=48, rtx=0, c=10,
mss=1392, tbw=2519, tp=-1, tpl=-1, uplat=190, ullat=0
	Alt-Svc: h3=":443"; ma=86400
```

```
    Connection: close
    Content-Length: 0
WhatWeb report for https://www.facebook.com/
Status    : 302 Found
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>\
Summary   : RedirectLocation[https://web.facebook.com/?_rdc=1&_rdr], Strict-
Transport-Security[max-age=15552000; preload], UncommonHeaders[reporting-
endpoints,report-to,cross-origin-embedder-policy-report-only,cross-origin-opener-
policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-quality,alt-svc]
Detected Plugins:
[ RedirectLocation ]
    HTTP Server string location. used with http-status 301 and
    302
    String       : https://web.facebook.com/?_rdc=1&_rdr (from location)
[ Strict-Transport-Security ]
    Strict-Transport-Security is an HTTP header that restricts
    a web browser from accessing a website without the security
    of the HTTPS protocol.
    String       : max-age=15552000; preload
[ 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 : reporting-endpoints,report-to,cross-origin-embedder-policy-report-only,cross-origin-opener-policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

HTTP Headers:

```
HTTP/1.1 302 Found

Location: https://web.facebook.com/?_rdc=1&_rdr

reporting-endpoints: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0", coep_report="https://www.facebook.com/browser_reporting/coep/?minimize=0"

report-to: {"max_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":86400,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser_reporting\/coep\/?minimize=0"}],"group":"coep_report"}

cross-origin-embedder-policy-report-only: require-corp;report-to="coep_report"

cross-origin-opener-policy: unsafe-none

x-fb-zr-redirect: 02|1730483658|

Strict-Transport-Security: max-age=15552000; preload

Content-Type: text/html; charset="utf-8"

X-FB-Debug: HxrZS/BvZuYlRJHd2EFNzYDi1fy4JWfiDXlEImCITDXyYU5tVW8Unu1QbZMcVbCgLNQKvAog90ruf5V7Q0oBbg==

Date: Thu, 31 Oct 2024 17:54:18 GMT

X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=38, rtx=0, c=10, mss=1392, tbw=2522, tp=-1, tpl=-1, uplat=176, ullat=0

Alt-Svc: h3=":443"; ma=86400

Connection: close
```

```
        Content-Length: 0
WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr
Status    : 200 OK
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>
Summary   : Cookies[fr,sb], HTML5, HttpOnly[fr,sb], Meta-Refresh-
Redirect[/?_rdc=1&_rdr&_fb_noscript=1], PasswordField[pass],
Script[application/ld+json,text/javascript], Strict-Transport-Security[max-
age=15552000; preload], UncommonHeaders[reporting-endpoints,report-
to,content-security-policy,document-policy,permissions-policy,cross-origin-
resource-policy,nel,cross-origin-opener-policy,x-content-type-options,x-fb-
debug,x-fb-connection-quality,alt-svc], X-Frame-Options[DENY], X-XSS-
Protection[0]\
Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.
        String       : fr
        String       : sb\
[ HTML5 ]
        HTML version 5, detected by the doctype declaration
[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie
        String       : fr,sb
```

```
[ Meta-Refresh-Redirect ]
        Meta refresh tag is a deprecated URL element that can be
        used to optionally wait x seconds before reloading the
        current page or loading a new page. More info:
        https://secure.wikimedia.org/wikipedia/en/wiki/Meta_refresh
        String       : /?_rdc=1&_rdr&_fb_noscript=1
[ PasswordField ]
        find password fields
        String       : pass (from field name)
[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.
        String       : application/ld+json,text/javascript
[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.
        String       : max-age=15552000; preload
[ 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       : reporting-endpoints,report-to,content-security-policy,document-
policy,permissions-policy,cross-origin-resource-policy,nel,cross-origin-opener-
```

```
policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc (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
        String      : DENY
[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx
        String      : 0
HTTP Headers:
        HTTP/1.1 200 OK
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Set-Cookie: fr=0rIESd6by32uL97EB..BnI8RT..AAA.0.0.BnI8RT.AWU-
Mu9h6G4; expires=Wed, 29-Jan-2025 17:54:27 GMT; Max-Age=7776000; path=/;
domain=.facebook.com; secure; httponly
        Set-Cookie: sb=U8QjZ_egILZ8seD5EuMtZADK; expires=Fri, 05-Dec-2025
17:54:27 GMT; Max-Age=34560000; path=/; domain=.facebook.com; secure;
httponly
        reporting-endpoints:
coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0",
default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unk
```

nown&brsid=7431999672342730080", permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"

report-to: {"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&brsid=7431999672342730080"}]}, {"max_age":3600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&brsid=7431999672342730080"}],"group": "network-errors"}, {"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}],"group":"permissions_policy"}

content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;

document-policy: force-load-at-top

permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self), camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=(self);report-to="permissions_policy"

cross-origin-resource-policy: same-origin

nel: {"report_to":"network-errors","max_age":3600,"failure_fraction":0.01}

cross-origin-opener-policy: unsafe-none

Pragma: no-cache

Cache-Control: private, no-cache, no-store, must-revalidate

Expires: Sat, 01 Jan 2000 00:00:00 GMT

X-Content-Type-Options: nosniff

X-XSS-Protection: 0

X-Frame-Options: DENY

Strict-Transport-Security: max-age=15552000; preload

Content-Type: text/html; charset="utf-8"

```
	X-FB-Debug: NptHvPr1QdjfSSdGE1RruapdnRBQfuRmrt6z4jsSYqQnVjZb0L59h//7XwdMPQPnue/tQdd/7UKBGueSuvlz6Q==
	Date: Thu, 31 Oct 2024 17:54:27 GMT
	X-FB-Connection-Quality: GOOD; q=0.7, rtt=63, rtx=0, c=10, mss=1392, tbw=2521, tp=-1, tpl=-1, uplat=236, ullat=0
	Alt-Svc: h3=":443"; ma=86400
	Transfer-Encoding: chunked
	Connection: close
WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr&_fb_noscript=1
Status    : 200 OK
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>
Summary   : Cookies[fr,noscript,sb], HTML5, HttpOnly[fr,sb], PasswordField[pass], Script[application/ld+json,text/javascript], Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[reporting-endpoints,report-to,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,nel,cross-origin-embedder-policy-report-only,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc], X-Frame-Options[DENY], X-XSS-Protection[0]
Detected Plugins:
[ Cookies ]
	Display the names of cookies in the HTTP headers. The
	values are not returned to save on space.
	String       : fr
	String       : noscript
	String       : sb
```

```
[ HTML5 ]
        HTML version 5, detected by the doctype declaration
[ HttpOnly ]
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie
        String       : fr,sb
[ PasswordField ]
        find password fields
        String       : pass (from field name)
[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.
        String       : application/ld+json,text/javascript
[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.
        String       : max-age=15552000; preload
[ 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       : reporting-endpoints,report-to,content-security-policy,document-
policy,permissions-policy,cross-origin-resource-policy,nel,cross-origin-embedder-
policy-report-only,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-
fb-connection-quality,alt-svc (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
        String       : DENY
[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx
        String       : 0
HTTP Headers:
        HTTP/1.1 200 OK
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Set-Cookie:
fr=0Ufktur8T4Zy246l5..BnI8RW..AAA.0.0.BnI8RW.AWWvCZarJiw;
expires=Wed, 29-Jan-2025 17:54:30 GMT; Max-Age=7776000; path=/;
domain=.facebook.com; secure; httponly
        Set-Cookie: noscript=1; path=/; domain=.facebook.com; secure
```

Set-Cookie: sb=VsQjZ204F8H5Gkwtrme2eXS5; expires=Fri, 05-Dec-2025 17:54:30 GMT; Max-Age=34560000; path=/; domain=.facebook.com; secure; httponly

reporting-endpoints: coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0", coep_report="https://web.facebook.com/browser_reporting/coep/?minimize=0", default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unknown&brsid=7431999684443613582", permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"

report-to: {"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":86400,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coep\/?minimize=0"}],"group":"coep_report"}, {"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&brsid=7431999684443613582"}]}, {"max_age":3600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&brsid=7431999684443613582"}],"group": "network-errors"}, {"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}],"group":"permissions_policy"}

content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com

*.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;

document-policy: force-load-at-top

permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self), camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=(self);report-to="permissions_policy"

cross-origin-resource-policy: same-origin

nel: {"report_to":"network-errors","max_age":3600,"failure_fraction":0.01}

cross-origin-embedder-policy-report-only: require-corp;report-to="coep_report"

cross-origin-opener-policy: unsafe-none

Pragma: no-cache

```
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; preload
Content-Type: text/html; charset="utf-8"
X-FB-Debug: flZUacs9TKRxHKM7jian44dT6f7xGBqf/jP7pFj3B3C33AWFXY0WjxB9N3fNZIvYXAMZvsr66ZT2WOK9K1M5Bg==
Date: Thu, 31 Oct 2024 17:54:31 GMT
X-FB-Connection-Quality: GOOD; q=0.7, rtt=59, rtx=0, c=10, mss=1392, tbw=2522, tp=-1, tpl=-1, uplat=250, ullat=0
Alt-Svc: h3=":443"; ma=86400
Transfer-Encoding: chunked
Connection: close
```

Lab 3: Subdomain Hunting

Exercise 1: Run the sublist3r command for the following domains:

Record Your Findings:

1. Subdomains for github.com: 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

t.communication.github.com

community.github.com

docs.github.com

docs-front-door.github.com

dodgeball.github.com

edu.github.com

education.github.com

emails.github.com

enterprise.github.com

support.enterprise.github.com

www.support.enterprise.github.com

examregistration.github.com

examregistration-api.github.com

examregistration-uat.github.com

examregistration-uat-api.github.com

fast.github.com

garage.github.com

gist.github.com

graphql.github.com

www.graphql.github.com

graphql-stage.github.com

www.graphql-stage.github.com

help.github.com

helpnext.github.com

hq.github.com

vpn-ca.iad.github.com

id.github.com

import.github.com

import2.github.com

importer2.github.com

jira.github.com

www.jira.github.com

jobs.github.com

lab.github.com

lab-sandbox.github.com

learn.github.com

mac-installer.github.com

maintainers.github.com

www.maintainers.github.com

octostatus-production.github.com

offer.github.com

partnerportal.github.com

www.partnerportal.github.com

pkg.github.com

porter.github.com

porter2.github.com

proxima-review-lab.github.com

raw.github.com

registry.github.com

render.github.com

render-lab.github.com

www.render-lab.github.com

review-lab.github.com

octocaptcha.review-lab.github.com

rs.github.com

schrauger.github.com

api.security.github.com

www.api.security.github.com

skyline.github.com

www.skyline.github.com

slack.github.com

smtp.github.com

www.smtp.github.com

staging-lab.github.com

api.stars.github.com

www.api.stars.github.com

status.github.com

stg.github.com

styleguide.github.com

ws.support.github.com

www.ws.support.github.com

talks.github.com

visualstudio.github.com

www.visualstudio.github.com

vscode-auth.github.com

workspaces.github.com

workspaces-dev.github.com

workspaces-ppe.github.com

2. Subdomains for google.com: 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

ads-compare.eem.corp.google.com

da.ext.corp.google.com

m.guts.corp.google.com

m.gutsdev.corp.google.com

login.corp.google.com

mtv-da.corp.google.com

mygeist.corp.google.com

mygeist2010.corp.google.com

proxyconfig.corp.google.com

reseed.corp.google.com

twdsalesgsa.twd.corp.google.com

uberproxy.corp.google.com

uberproxy-nocert.corp.google.com

uberproxy-san.corp.google.com

ext.google.com

cag.ext.google.com

cod.ext.google.com

da.ext.google.com

eggroll.ext.google.com

fra-da.ext.google.com

glass.ext.google.com

glass-eur.ext.google.com

glass-mtv.ext.google.com

glass-twd.ext.google.com

hot-da.ext.google.com

hyd-da.ext.google.com

ice.ext.google.com

meeting.ext.google.com

mtv-da.ext.google.com

soaproxyprod01.ext.google.com

soaproxytest01.ext.google.com

spdy-proxy.ext.google.com

spdy-proxy-debug.ext.google.com

twd-da.ext.google.com

flexpack.google.com

www.flexpack.google.com

accounts.flexpack.google.com

gaiastaging.flexpack.google.com

mail.flexpack.google.com

plus.flexpack.google.com

search.flexpack.google.com

freezone.google.com

www.freezone.google.com

accounts.freezone.google.com

gaiastaging.freezone.google.com

mail.freezone.google.com

news.freezone.google.com

plus.freezone.google.com

search.freezone.google.com

gmail.google.com

hosted-id.google.com

jmt0.google.com

aspmx.l.google.com

alt1.aspmx.l.google.com

alt2.aspmx.l.google.com

alt3.aspmx.l.google.com

alt4.aspmx.l.google.com

gmail-smtp-in.l.google.com

alt1.gmail-smtp-in.l.google.com

alt2.gmail-smtp-in.l.google.com

alt3.gmail-smtp-in.l.google.com

alt4.gmail-smtp-in.l.google.com

gmr-smtp-in.l.google.com

alt1.gmr-smtp-in.l.google.com

alt2.gmr-smtp-in.l.google.com

alt3.gmr-smtp-in.l.google.com

alt4.gmr-smtp-in.l.google.com

vp.video.l.google.com

m.google.com

freezone.m.google.com

mail.google.com

freezone.mail.google.com

misc.google.com

misc-sni.google.com

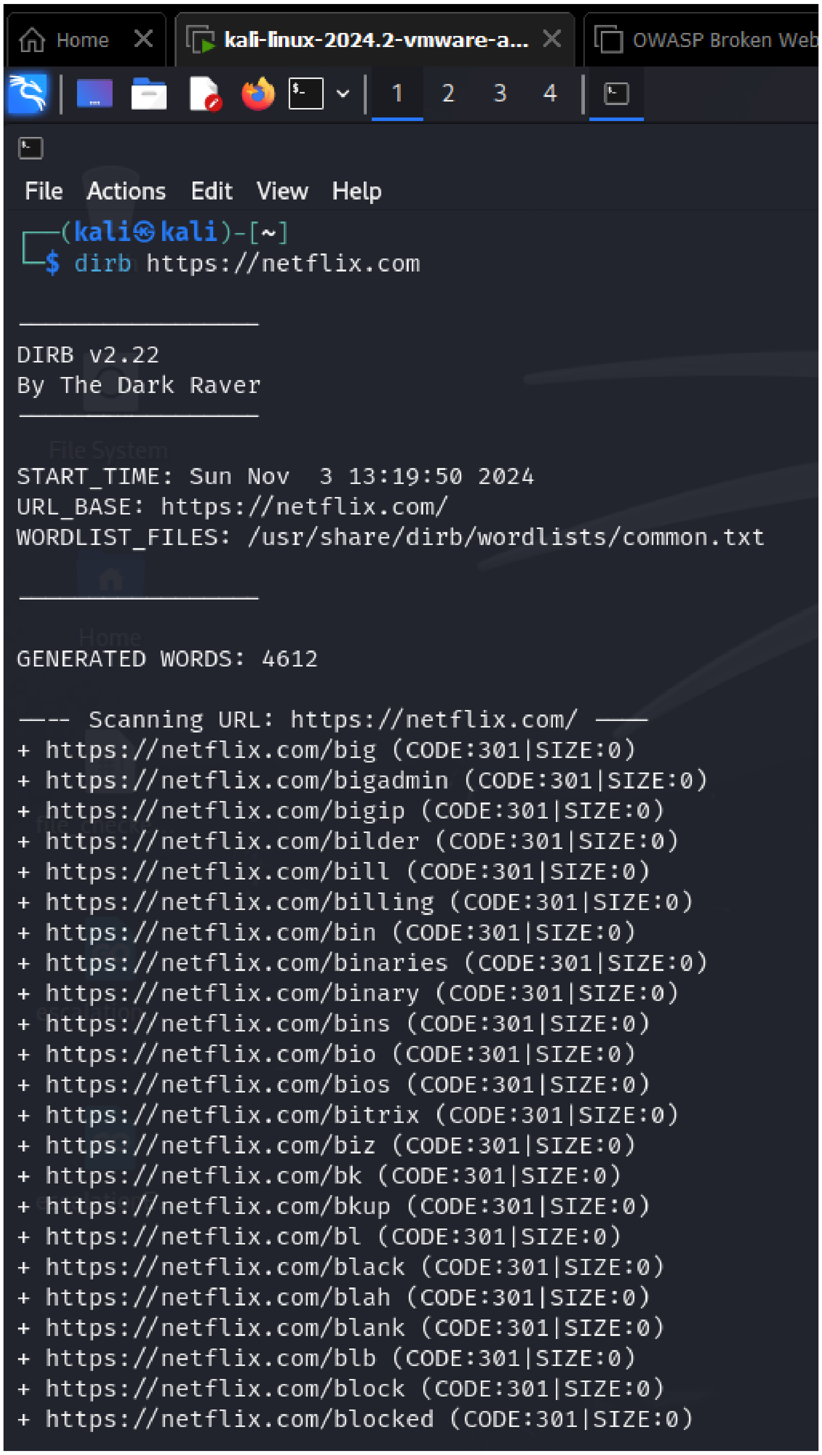
mtalk.google.com

```
mx.google.com
ics.prod.google.com
sandbox.google.com
cert-test.sandbox.google.com
ecc-test.sandbox.google.com
services.google.com
talk.google.com
upload.google.com
dg.video.google.com
upload.video.google.com
wifi.google.com
onex.wifi.google.com
```

Exercise 2: Perform a directory discovery scan on the following targets:

1. Directories for netflix.com:

```
GENERATED WORDS: 4612

---- Scanning URL: https://netflix.com/ ----
+ https://netflix.com/big (CODE:301|SIZE:0)
+ https://netflix.com/bigadmin (CODE:301|SIZE:0)
+ https://netflix.com/bigip (CODE:301|SIZE:0)
+ https://netflix.com/bilder (CODE:301|SIZE:0)
+ https://netflix.com/bill (CODE:301|SIZE:0)
+ https://netflix.com/billing (CODE:301|SIZE:0)
+ https://netflix.com/bin (CODE:301|SIZE:0)
+ https://netflix.com/binaries (CODE:301|SIZE:0)
+ https://netflix.com/binary (CODE:301|SIZE:0)

+ https://netflix.com/bins (CODE:301|SIZE:0)

+ https://netflix.com/bio (CODE:301|SIZE:0)

+ https://netflix.com/bios (CODE:301|SIZE:0)

+ https://netflix.com/bitrix (CODE:301|SIZE:0)

+ https://netflix.com/biz (CODE:301|SIZE:0)

+ https://netflix.com/bk (CODE:301|SIZE:0)

+ https://netflix.com/bkup (CODE:301|SIZE:0)

+ https://netflix.com/bl (CODE:301|SIZE:0)

+ https://netflix.com/black (CODE:301|SIZE:0)

+ https://netflix.com/blah (CODE:301|SIZE:0)

+ https://netflix.com/blank (CODE:301|SIZE:0)

+ https://netflix.com/blb (CODE:301|SIZE:0)

+ https://netflix.com/block (CODE:301|SIZE:0)

+ https://netflix.com/blocked (CODE:301|SIZE:0)

+ https://netflix.com/blocks (CODE:301|SIZE:0)

+ https://netflix.com/blog (CODE:301|SIZE:0)

+ https://netflix.com/Blog (CODE:301|SIZE:0)

+ https://netflix.com/blog_ajax (CODE:301|SIZE:0)

+ https://netflix.com/blog_inlinemod (CODE:301|SIZE:0)

+ https://netflix.com/blog_report (CODE:301|SIZE:0)

+ https://netflix.com/blog_search (CODE:301|SIZE:0)

+ https://netflix.com/blog_usercp (CODE:301|SIZE:0)

+ https://netflix.com/blogger (CODE:301|SIZE:0)

+ https://netflix.com/bloggers (CODE:301|SIZE:0)
+ https://netflix.com/blogindex (CODE:301|SIZE:0)
+ https://netflix.com/blogs (CODE:301|SIZE:0)
+ https://netflix.com/blogspot (CODE:301|SIZE:0)
+ https://netflix.com/blow (CODE:301|SIZE:0)
+ https://netflix.com/blue (CODE:301|SIZE:0)
+ https://netflix.com/bm (CODE:301|SIZE:0)
+ https://netflix.com/bmz_cache (CODE:301|SIZE:0)
+ https://netflix.com/bnnr (CODE:301|SIZE:0)
+ https://netflix.com/bo (CODE:301|SIZE:0)
+ https://netflix.com/board (CODE:301|SIZE:0)
+ https://netflix.com/boards (CODE:301|SIZE:0)
+ https://netflix.com/bob (CODE:301|SIZE:0)
+ https://netflix.com/body (CODE:301|SIZE:0)
+ https://netflix.com/bofh (CODE:301|SIZE:0)
+ https://netflix.com/boiler (CODE:301|SIZE:0)
+ https://netflix.com/boilerplate (CODE:301|SIZE:0)
+ https://netflix.com/bonus (CODE:301|SIZE:0)
+ https://netflix.com/bonuses (CODE:301|SIZE:0)
+ https://netflix.com/book (CODE:301|SIZE:0)
+ https://netflix.com/booker (CODE:301|SIZE:0)
+ https://netflix.com/booking (CODE:301|SIZE:0)
+ https://netflix.com/bookmark (CODE:301|SIZE:0)
+ https://netflix.com/bookmarks (CODE:301|SIZE:0)
+ https://netflix.com/books (CODE:301|SIZE:0)
+ https://netflix.com/Books (CODE:301|SIZE:0)
+ https://netflix.com/bookstore (CODE:301|SIZE:0)
+ https://netflix.com/boost_stats (CODE:301|SIZE:0)
+ https://netflix.com/boot (CODE:301|SIZE:0)
+ https://netflix.com/bot (CODE:301|SIZE:0)
+ https://netflix.com/bots (CODE:301|SIZE:0)
+ https://netflix.com/bottom (CODE:301|SIZE:0)
+ https://netflix.com/bot-trap (CODE:301|SIZE:0)
+ https://netflix.com/boutique (CODE:301|SIZE:0)
+ https://netflix.com/box (CODE:301|SIZE:0)
+ https://netflix.com/boxes (CODE:301|SIZE:0)
+ https://netflix.com/br (CODE:301|SIZE:0)
+ https://netflix.com/brand (CODE:301|SIZE:0)
+ https://netflix.com/brands (CODE:301|SIZE:0)
+ https://netflix.com/broadband (CODE:301|SIZE:0)
+ https://netflix.com/brochure (CODE:301|SIZE:0)
+ https://netflix.com/brochures (CODE:301|SIZE:0)
+ https://netflix.com/broken (CODE:301|SIZE:0)
+ https://netflix.com/broken_link (CODE:301|SIZE:0)
+ https://netflix.com/broker (CODE:301|SIZE:0)
+ https://netflix.com/browse (CODE:301|SIZE:0)
+ https://netflix.com/browser (CODE:301|SIZE:0)
+ https://netflix.com/Browser (CODE:301|SIZE:0)
+ https://netflix.com/bs (CODE:301|SIZE:0)
+ https://netflix.com/bsd (CODE:301|SIZE:0)
+ https://netflix.com/bt (CODE:301|SIZE:0)
+ https://netflix.com/bug (CODE:301|SIZE:0)
+ https://netflix.com/bugs (CODE:301|SIZE:0)
+ https://netflix.com/build (CODE:301|SIZE:0)
+ https://netflix.com/BUILD (CODE:301|SIZE:0)
+ https://netflix.com/builder (CODE:301|SIZE:0)
+ https://netflix.com/buildr (CODE:301|SIZE:0)
+ https://netflix.com/bulk (CODE:301|SIZE:0)
+ https://netflix.com/bulksms (CODE:301|SIZE:0)
+ https://netflix.com/bullet (CODE:301|SIZE:0)
+ https://netflix.com/busca (CODE:301|SIZE:0)
+ https://netflix.com/buscador (CODE:301|SIZE:0)
+ https://netflix.com/buscar (CODE:301|SIZE:0)
+ https://netflix.com/business (CODE:301|SIZE:0)
+ https://netflix.com/Business (CODE:301|SIZE:0)
+ https://netflix.com/button (CODE:301|SIZE:0)
+ https://netflix.com/buttons (CODE:301|SIZE:0)
+ https://netflix.com/buy (CODE:301|SIZE:0)
+ https://netflix.com/buynow (CODE:301|SIZE:0)
(!) WARNING: Too many responses for this directory seem to be FOUND.
    (Something is going wrong - Try Other Scan Mode)
    (Use mode '-w' if you want to scan it anyway)
-----------------
END_TIME: Sun Nov  3 13:26:02 2024
DOWNLOADED: 721 - FOUND: 101
```



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

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

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

START_TIME: Sun Nov  3 13:19:50 2024
URL_BASE: https://netflix.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: https://netflix.com/ ----
+ https://netflix.com/big (CODE:301|SIZE:0)
+ https://netflix.com/bigadmin (CODE:301|SIZE:0)
+ https://netflix.com/bigip (CODE:301|SIZE:0)
+ https://netflix.com/bilder (CODE:301|SIZE:0)
+ https://netflix.com/bill (CODE:301|SIZE:0)
+ https://netflix.com/billing (CODE:301|SIZE:0)
+ https://netflix.com/bin (CODE:301|SIZE:0)
+ https://netflix.com/binaries (CODE:301|SIZE:0)
+ https://netflix.com/binary (CODE:301|SIZE:0)
+ https://netflix.com/bins (CODE:301|SIZE:0)
+ https://netflix.com/bio (CODE:301|SIZE:0)
+ https://netflix.com/bios (CODE:301|SIZE:0)
+ https://netflix.com/bitrix (CODE:301|SIZE:0)
+ https://netflix.com/biz (CODE:301|SIZE:0)
+ https://netflix.com/bk (CODE:301|SIZE:0)
+ https://netflix.com/bkup (CODE:301|SIZE:0)
+ https://netflix.com/bl (CODE:301|SIZE:0)
+ https://netflix.com/black (CODE:301|SIZE:0)
+ https://netflix.com/blah (CODE:301|SIZE:0)
+ https://netflix.com/blank (CODE:301|SIZE:0)
+ https://netflix.com/blb (CODE:301|SIZE:0)
+ https://netflix.com/block (CODE:301|SIZE:0)
+ https://netflix.com/blocked (CODE:301|SIZE:0)
```

2. Directories for google.com:

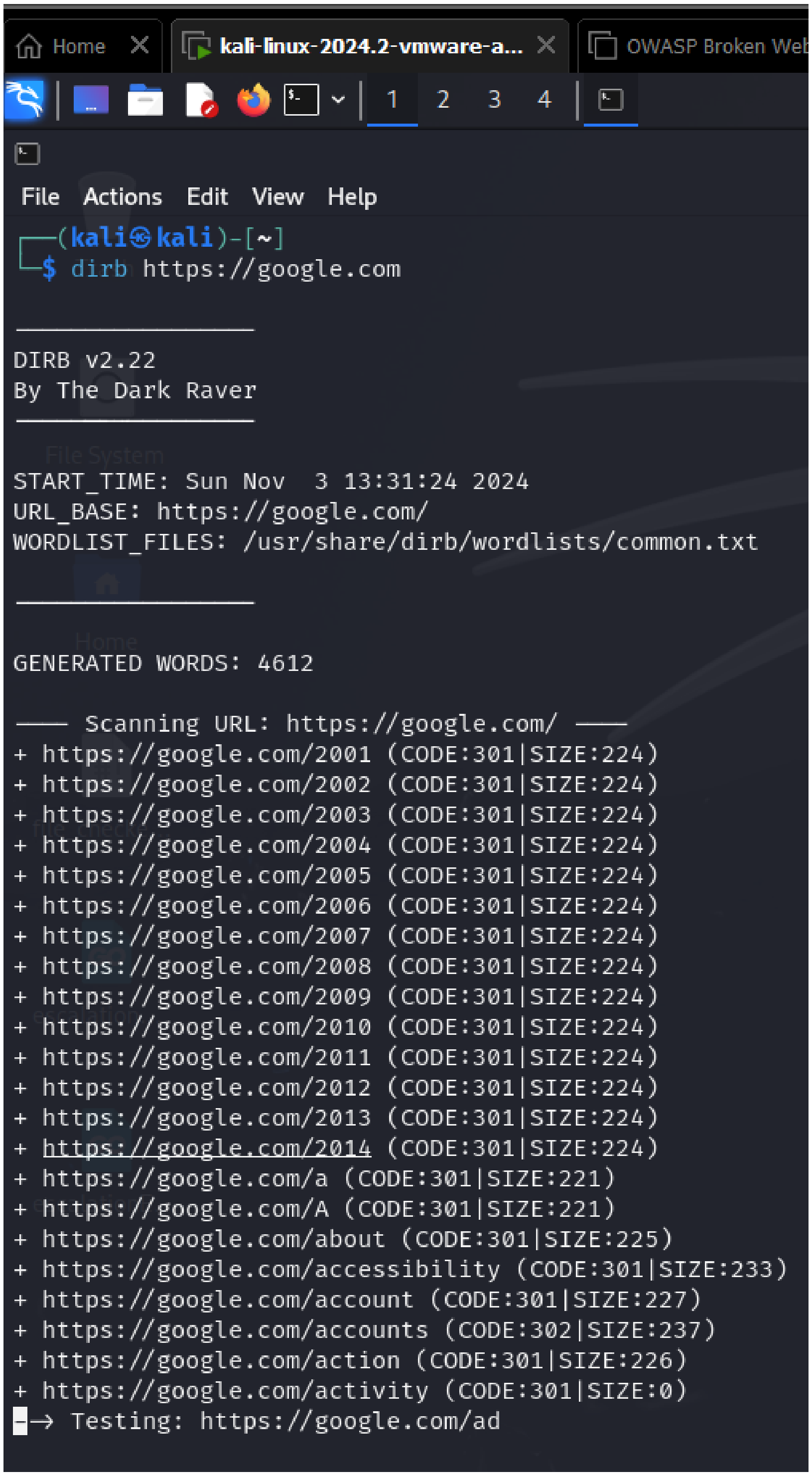
GENERATED WORDS: 4612

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

+ https://google.com/2001 (CODE:301|SIZE:224)

```
+ https://google.com/2002 (CODE:301|SIZE:224)
+ https://google.com/2003 (CODE:301|SIZE:224)
+ https://google.com/2004 (CODE:301|SIZE:224)
+ https://google.com/2005 (CODE:301|SIZE:224)
+ https://google.com/2006 (CODE:301|SIZE:224)
+ https://google.com/2007 (CODE:301|SIZE:224)
+ https://google.com/2008 (CODE:301|SIZE:224)
+ https://google.com/2009 (CODE:301|SIZE:224)
+ https://google.com/2010 (CODE:301|SIZE:224)
+ https://google.com/2011 (CODE:301|SIZE:224)
+ https://google.com/2012 (CODE:301|SIZE:224)
+ https://google.com/2013 (CODE:301|SIZE:224)
+ https://google.com/2014 (CODE:301|SIZE:224)
+ https://google.com/a (CODE:301|SIZE:221)
+ https://google.com/A (CODE:301|SIZE:221)
+ https://google.com/about (CODE:301|SIZE:225)
+ https://google.com/accessibility (CODE:301|SIZE:233)
+ https://google.com/account (CODE:301|SIZE:227)
+ https://google.com/accounts (CODE:302|SIZE:237)
+ https://google.com/action (CODE:301|SIZE:226)
+ https://google.com/activity (CODE:301|SIZE:0)
(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT CONNECT)
-----------------
END_TIME: Sun Nov  3 13:44:01 2024
```

DOWNLOADED: 267 - FOUND: 22



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

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

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

START_TIME: Sun Nov  3 13:31:24 2024
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: https://google.com/ ----
+ https://google.com/2001 (CODE:301|SIZE:224)
+ https://google.com/2002 (CODE:301|SIZE:224)
+ https://google.com/2003 (CODE:301|SIZE:224)
+ https://google.com/2004 (CODE:301|SIZE:224)
+ https://google.com/2005 (CODE:301|SIZE:224)
+ https://google.com/2006 (CODE:301|SIZE:224)
+ https://google.com/2007 (CODE:301|SIZE:224)
+ https://google.com/2008 (CODE:301|SIZE:224)
+ https://google.com/2009 (CODE:301|SIZE:224)
+ https://google.com/2010 (CODE:301|SIZE:224)
+ https://google.com/2011 (CODE:301|SIZE:224)
+ https://google.com/2012 (CODE:301|SIZE:224)
+ https://google.com/2013 (CODE:301|SIZE:224)
+ https://google.com/2014 (CODE:301|SIZE:224)
+ https://google.com/a (CODE:301|SIZE:221)
+ https://google.com/A (CODE:301|SIZE:221)
+ https://google.com/about (CODE:301|SIZE:225)
+ https://google.com/accessibility (CODE:301|SIZE:233)
+ https://google.com/account (CODE:301|SIZE:227)
+ https://google.com/accounts (CODE:302|SIZE:237)
+ https://google.com/action (CODE:301|SIZE:226)
+ https://google.com/activity (CODE:301|SIZE:0)
-→ Testing: https://google.com/ad
```

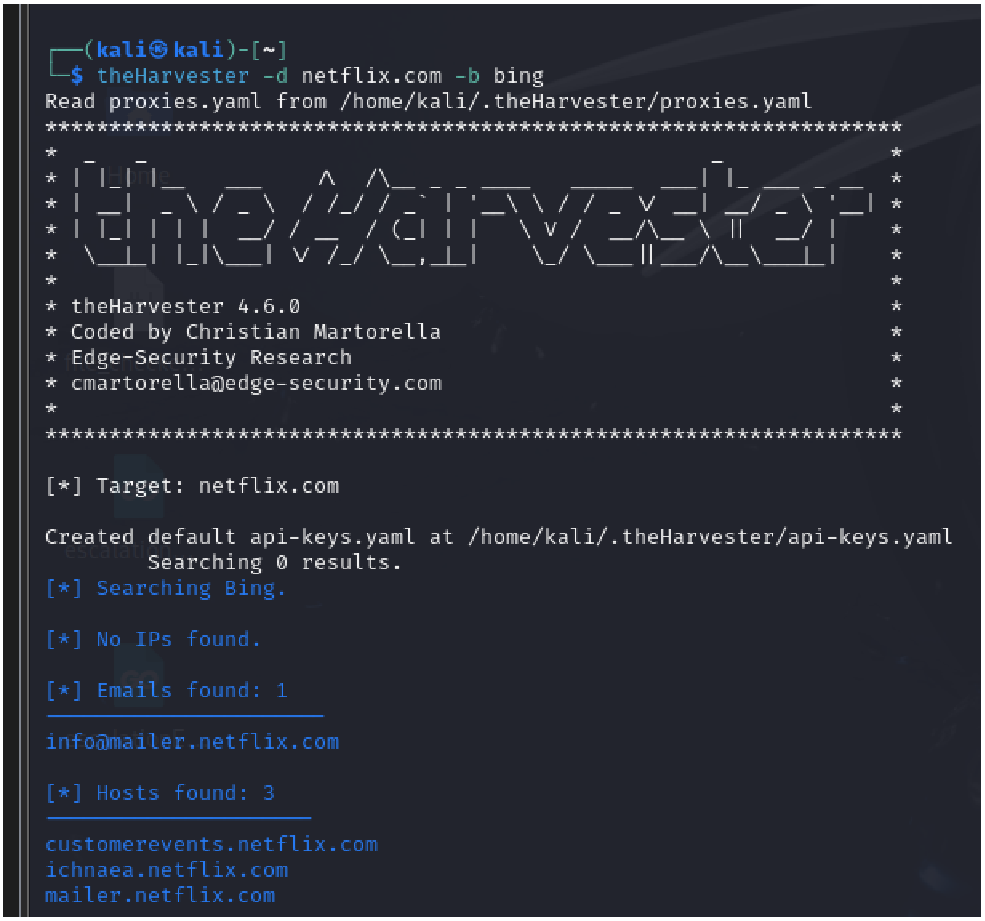
Step 3: Information Gathering Using theHarvester

Exercise 3:

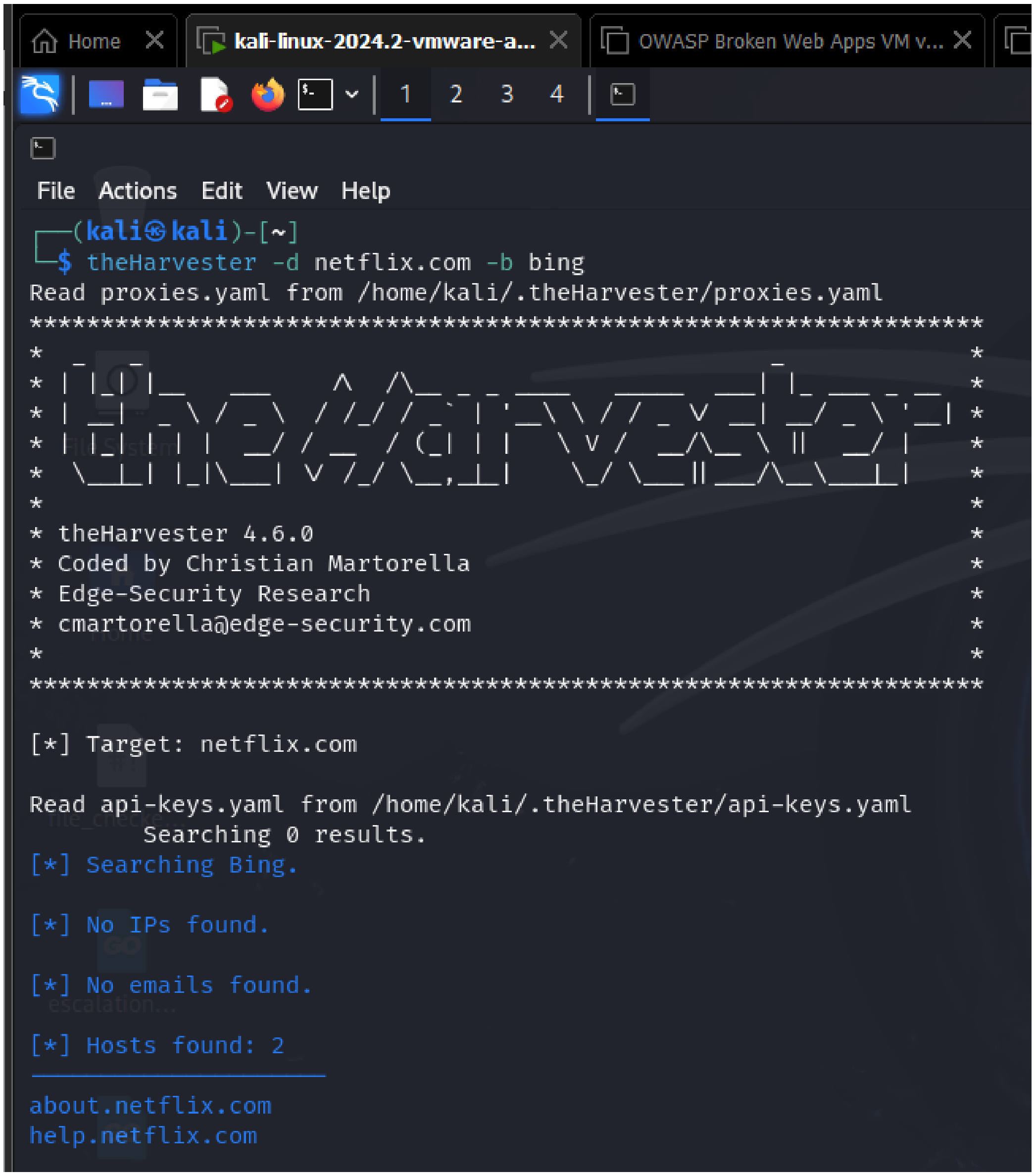
Use theHarvester to gather information on the following domain:

- **netflix.com**

Record Your Findings:



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d netflix.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: netflix.com

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

[*] No IPs found.

[*] Emails found: 1
----------------------
info@mailer.netflix.com

[*] Hosts found: 3
---------------------
customerevents.netflix.com
ichnaea.netflix.com
mailer.netflix.com
```



```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d netflix.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: netflix.com

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

[*] No IPs found.

[*] No emails found.

[*] Hosts found: 2
  ---------------------
about.netflix.com
help.netflix.com
```