

Week 1: Reconnaissance, Information Gathering, and Scanning

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

Lab Steps

Step 1: Get the IP Address of a Domain Using ping

1. facebook.com: _____

```
Nov 6 17:16
ngozi@kali:~ 

64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=758 ttl=128 time=67.1 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=759 ttl=128 time=43.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=760 ttl=128 time=43.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=761 ttl=128 time=42.7 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=762 ttl=128 time=31.1 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=763 ttl=128 time=61.1 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=764 ttl=128 time=26.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=765 ttl=128 time=29.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=766 ttl=128 time=429 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=767 ttl=128 time=30.4 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=768 ttl=128 time=39.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=769 ttl=128 time=34.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=770 ttl=128 time=31.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=771 ttl=128 time=31.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=772 ttl=128 time=37.2 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=773 ttl=128 time=29.6 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=774 ttl=128 time=34.7 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=775 ttl=128 time=39.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=776 ttl=128 time=1045 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=777 ttl=128 time=54.8 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=778 ttl=128 time=30.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=779 ttl=128 time=37.4 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=780 ttl=128 time=28.2 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=781 ttl=128 time=57.1 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=782 ttl=128 time=57.6 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=783 ttl=128 time=33.3 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=784 ttl=128 time=89.0 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=785 ttl=128 time=40.7 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=786 ttl=128 time=1045 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=787 ttl=128 time=58.3 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=788 ttl=128 time=35.2 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=789 ttl=128 time=32.7 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=790 ttl=128 time=34.6 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=791 ttl=128 time=31.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=792 ttl=128 time=36.1 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=793 ttl=128 time=34.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=794 ttl=128 time=39.7 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=795 ttl=128 time=47.5 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=796 ttl=128 time=29.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=797 ttl=128 time=28.9 ms
64 bytes from edge-star-mini-shv-01-los2.facebook.com (102.132.101.39): icmp_seq=798 ttl=128 time=36.6 ms
```

2. twitter.com: _____

```
Nov 6 17:24
ngozi@kali:~ 

64 bytes from 104.244.42.65: icmp_seq=12 ttl=128 time=203 ms
64 bytes from 104.244.42.65: icmp_seq=12 ttl=128 time=210 ms
64 bytes from 104.244.42.65: icmp_seq=122 ttl=128 time=201 ms
64 bytes from 104.244.42.65: icmp_seq=123 ttl=128 time=230 ms
64 bytes from 104.244.42.65: icmp_seq=124 ttl=128 time=253 ms
64 bytes from 104.244.42.65: icmp_seq=125 ttl=128 time=193 ms
64 bytes from 104.244.42.65: icmp_seq=126 ttl=128 time=186 ms
64 bytes from 104.244.42.65: icmp_seq=127 ttl=128 time=207 ms
64 bytes from 104.244.42.65: icmp_seq=128 ttl=128 time=214 ms
64 bytes from 104.244.42.65: icmp_seq=129 ttl=128 time=227 ms
64 bytes from 104.244.42.65: icmp_seq=130 ttl=128 time=236 ms
64 bytes from 104.244.42.65: icmp_seq=131 ttl=128 time=243 ms
64 bytes from 104.244.42.65: icmp_seq=132 ttl=128 time=188 ms
64 bytes from 104.244.42.65: icmp_seq=133 ttl=128 time=262 ms
64 bytes from 104.244.42.65: icmp_seq=134 ttl=128 time=270 ms
64 bytes from 104.244.42.65: icmp_seq=135 ttl=128 time=1030 ms
64 bytes from 104.244.42.65: icmp_seq=136 ttl=128 time=278 ms
64 bytes from 104.244.42.65: icmp_seq=137 ttl=128 time=195 ms
64 bytes from 104.244.42.65: icmp_seq=138 ttl=128 time=204 ms
64 bytes from 104.244.42.65: icmp_seq=139 ttl=128 time=215 ms
64 bytes from 104.244.42.65: icmp_seq=140 ttl=128 time=222 ms
64 bytes from 104.244.42.65: icmp_seq=141 ttl=128 time=229 ms
64 bytes from 104.244.42.65: icmp_seq=142 ttl=128 time=206 ms
64 bytes from 104.244.42.65: icmp_seq=143 ttl=128 time=255 ms
64 bytes from 104.244.42.65: icmp_seq=144 ttl=128 time=263 ms
64 bytes from 104.244.42.65: icmp_seq=145 ttl=128 time=623 ms
64 bytes from 104.244.42.65: icmp_seq=146 ttl=128 time=200 ms
64 bytes from 104.244.42.65: icmp_seq=147 ttl=128 time=298 ms
64 bytes from 104.244.42.65: icmp_seq=148 ttl=128 time=306 ms
64 bytes from 104.244.42.65: icmp_seq=149 ttl=128 time=204 ms
64 bytes from 104.244.42.65: icmp_seq=150 ttl=128 time=221 ms
64 bytes from 104.244.42.65: icmp_seq=151 ttl=128 time=332 ms
64 bytes from 104.244.42.65: icmp_seq=152 ttl=128 time=238 ms
64 bytes from 104.244.42.65: icmp_seq=153 ttl=128 time=246 ms
64 bytes from 104.244.42.65: icmp_seq=154 ttl=128 time=253 ms
`C
-- twitter.com ping statistics --
154 packets transmitted, 125 received, 18.8312% packet loss, time 164438ms
rtt min/avg/max/mdev = 158.157/262.394/1031.036/135.592 ms, pipe 2
(ngozi㉿kali)-[~]
```

3. amazon.com: _____



```
Nov 6 17:25
ngozi@kali: ~
PING amazon.com (54.239.28.85) 56(94) bytes of data.
64 bytes from 54.239.28.85: icmp_seq=1 ttl=128 time=255 ms
64 bytes from 54.239.28.85: icmp_seq=2 ttl=128 time=271 ms
64 bytes from 54.239.28.85: icmp_seq=3 ttl=128 time=268 ms
64 bytes from 54.239.28.85: icmp_seq=4 ttl=128 time=301 ms
64 bytes from 54.239.28.85: icmp_seq=5 ttl=128 time=316 ms
64 bytes from 54.239.28.85: icmp_seq=6 ttl=128 time=237 ms
64 bytes from 54.239.28.85: icmp_seq=7 ttl=128 time=361 ms
64 bytes from 54.239.28.85: icmp_seq=8 ttl=128 time=267 ms
64 bytes from 54.239.28.85: icmp_seq=9 ttl=128 time=1042 ms
64 bytes from 54.239.28.85: icmp_seq=10 ttl=128 time=268 ms
64 bytes from 54.239.28.85: icmp_seq=11 ttl=128 time=280 ms
64 bytes from 54.239.28.85: icmp_seq=12 ttl=128 time=307 ms
64 bytes from 54.239.28.85: icmp_seq=13 ttl=128 time=313 ms
64 bytes from 54.239.28.85: icmp_seq=14 ttl=128 time=321 ms
64 bytes from 54.239.28.85: icmp_seq=15 ttl=128 time=333 ms
64 bytes from 54.239.28.85: icmp_seq=16 ttl=128 time=360 ms
64 bytes from 54.239.28.85: icmp_seq=17 ttl=128 time=219 ms
64 bytes from 54.239.28.85: icmp_seq=18 ttl=128 time=286 ms
64 bytes from 54.239.28.85: icmp_seq=19 ttl=128 time=274 ms
64 bytes from 54.239.28.85: icmp_seq=20 ttl=128 time=303 ms
64 bytes from 54.239.28.85: icmp_seq=21 ttl=128 time=226 ms
64 bytes from 54.239.28.85: icmp_seq=22 ttl=128 time=232 ms
64 bytes from 54.239.28.85: icmp_seq=23 ttl=128 time=242 ms
64 bytes from 54.239.28.85: icmp_seq=24 ttl=128 time=246 ms
64 bytes from 54.239.28.85: icmp_seq=25 ttl=128 time=258 ms
64 bytes from 54.239.28.85: icmp_seq=26 ttl=128 time=367 ms
64 bytes from 54.239.28.85: icmp_seq=27 ttl=128 time=275 ms
64 bytes from 54.239.28.85: icmp_seq=28 ttl=128 time=284 ms
64 bytes from 54.239.28.85: icmp_seq=29 ttl=128 time=951 ms
64 bytes from 54.239.28.85: icmp_seq=30 ttl=128 time=233 ms
64 bytes from 54.239.28.85: icmp_seq=31 ttl=128 time=244 ms
64 bytes from 54.239.28.85: icmp_seq=32 ttl=128 time=249 ms
64 bytes from 54.239.28.85: icmp_seq=33 ttl=128 time=361 ms
64 bytes from 54.239.28.85: icmp_seq=34 ttl=128 time=381 ms
^C
--- amazon.com ping statistics ---
34 packets transmitted, 34 received, 0% packet loss, time 3335ms
rtt min/avg/max/mdev = 219.004/332.651/1042.050/173.354 ms, pipe 2
--(ngoziz@kali)-[~]
```

Step 2: Retrieve Domain Registration Details Using whois

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? _____

```

Nov 6 17:28 ngozi@kali:~ 
--- amazon.com ping statistics ---
34 packets transmitted, 34 received, 0% packet loss, time 33359ms
rtt min/avg/max/mdev = 219.004/332.651/1042.056/173.354 ms, pipe 2

(ngozi㉿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: +1.2086851798
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.NS0NE.NET
Name Server: DNS2.P08.NS0NE.NET
Name Server: DNS3.P08.NS0NE.NET
Name Server: DNS4.P08.NS0NE.NET
Name Server: NS-1283.AWSNS-32.ORG
Name Server: NS-1707.AWSNS-21.CO.UK
Name Server: NS-421.AWSNS-52.COM
Name Server: NS-520.AWSNS-01.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-06T22:27:15Z <<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois

```

Answer: 2026-10-09

2. Who is the registrar for linkedin.com? _____

```

Nov 6 17:32 ngozi@kali:~ 
----- -----
By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via email, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
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: linkedin.com
Registry Domain ID: 1173182852_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-08-02T02:17:33+0000
Creation Date: 2007-08-22T18:47:15+0000
Registrar Registration/Expiry Date: 2025-08-22T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851798
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: ClientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: LinkedIn Corporation
Registrant Street: 1000 W. Maude Ave
Registrant City: Sunnyvale
Registrant State/Province: CA
Registrant Postal Code: 94085
Registrant Country: US
Registrant Phone: +1.6506873600

```

Answer: MarkMonitor, Inc.

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

```
Nov 6 17:36
ngozi@kali:~
```

(*) enable high volume, automated, or electronic processes that send queries, data, or email to MarkMonitor (or its systems) or the domain name contacts (or its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>
Contact us at +1.8007459229
In Europe, at +44.02032062220

```
__(ngozi@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: 2023-02-28T05:13:11Z
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
URI of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-07T22:35:35Z <<
```

```
Nov 6 17:38
ngozi@kali:~
```

Domain Status: serverTransferProhibited https://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org/epp#serverUpdateProhibited
Registry Registry ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Apple Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: CA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: apple.com-Registrant@anonymised.email
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: apple.com-Admin@anonymised.email
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: apple.com-Tech@anonymised.email
Name Server: a.ns.apple.com

Answer: US

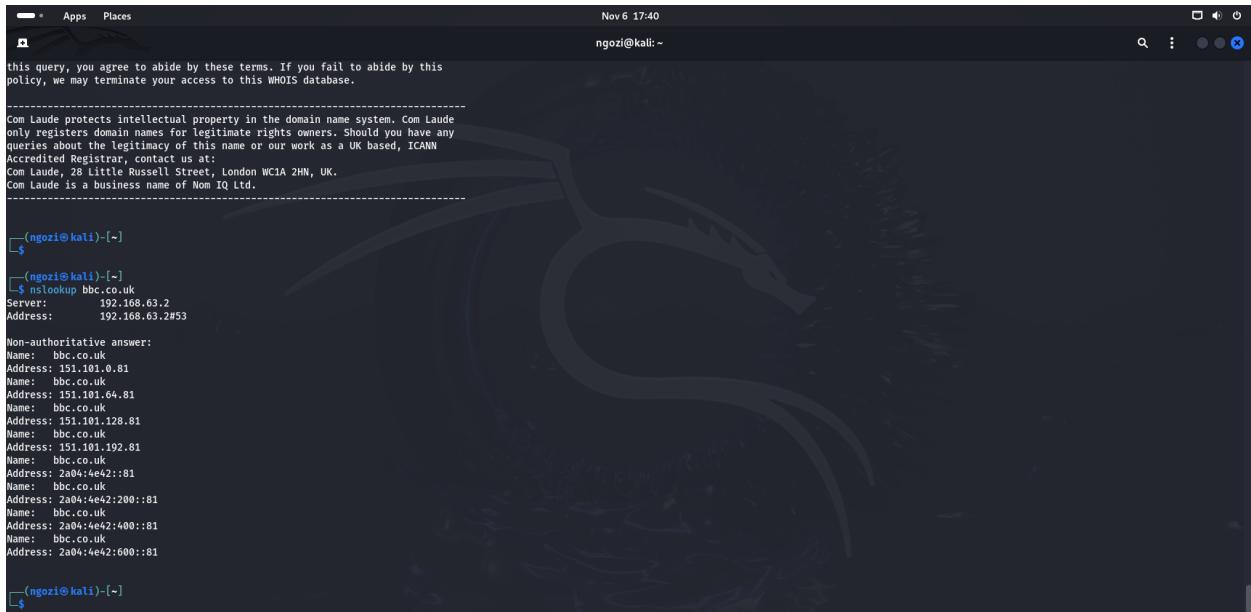
Step 3: Perform a DNS Lookup Using nslookup

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? _____



```
Nov 6 17:40
ngozzi@kali: ~

this query, you agree to abide by these terms. If you fail to abide by this
policy, we may terminate your access to this WHOIS database.

-----
Com Laude protects intellectual property in the domain name system. Com Laude
only registers domain names for legitimate rights owners. Should you have any
queries about the legitimacy of this name or our work as a UK based, ICANN
Accredited Registrar, contact us at:
Com Laude, 28 Little Russell Street, London WC1A 2HN, UK.
Com Laude is a business name of Nom 1Q Ltd.

-----
(ngozzi@kali)-[~]
$ nslookup bbc.co.uk
Server:      192.168.63.2
Address:     192.168.63.2#53

Non-authoritative answer:
Name:  bbc.co.uk
Address: 151.101.60.81
Name:  bbc.co.uk
Address: 151.101.64.81
Name:  bbc.co.uk
Address: 151.101.128.81
Name:  bbc.co.uk
Address: 151.101.192.81
Name:  bbc.co.uk
Address: 2a04:4e42::81
Name:  bbc.co.uk
Address: 2a04:4e42:200::81
Name:  bbc.co.uk
Address: 2a04:4e42:400::81
Name:  bbc.co.uk
Address: 2a04:4e42:600::81

(ngozzi@kali)-[~]
$
```

Answer: 192.168.63.2#53

2. What are the name servers (NS) for netflix.com? _____



```
Nov 6 17:43
ngozi@kali: ~

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

_____(ngoziz@kali)-[~]
└$ nslookup netflix.com
Server:      192.168.63.2
Address:    192.168.63.2#53

Non-authoritative answer:
Name: netflix.com
Address: 18.208.100.190
Name: netflix.com
Address: 54.155.246.232
Name: netflix.com
Address: 54.73.148.110
Name: netflix.com
Address: 2a05:dd18:76c:b684:b233:ac1f:be1f:7
Name: netflix.com
Address: 2a05:dd18:76c:b685:c898:aa3a:42c7:9d21
Name: netflix.com
Address: 2a05:dd18:76c:b683:e1fe:9fbf:c403:57f1

_____(ngoziz@kali)-[~]
```

Answer: Netflix.com

INT302: Kali Linux Tools and System Security – Lab 2: Website Enumeration and Information Gathering

Lab Steps Step 1: Detect Web Technologies Using whatweb

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: _____

```
Nov 6 18:03
ngozi@kali: ~

Name: bbc.co.uk
Address: 151.101.64.81
Name: bbc.co.uk
Address: 151.101.128.81
Name: bbc.co.uk
Address: 151.101.192.81
Name: bbc.co.uk
Address: 2a04:4e42::81
Name: bbc.co.uk
Address: 2a04:4e42:200::81
Name: bbc.co.uk
Address: 2a04:4e42:400::81
Name: bbc.co.uk
Address: 2a04:4e42:600::81

__(ngozzi㉿kali)-[~]
└─$ nslookup netflix.com
Server: 192.168.63.2
Address: 192.168.63.2#53

Non-authoritative answer:
Name: netflix.com
Address: 18.200.8.190
Name: netflix.com
Address: 54.155.246.232
Name: netflix.com
Address: 54.73.148.110
Name: netflix.com
Address: 2a05:d018:76c:b684:b233:ac1f:be1f:
Name: netflix.com
Address: 2a05:d018:76c:b685:c898:aa3a:42c7:9d21
Name: netflix.com
Address: 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1

__(ngozzi㉿kali)-[~]
└─$ whatweb example.com
http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECAcc (dcd/7D6B)], IP[93.184.215.14], Title[Example Domain]

__(ngozzi㉿kali)-[~]
└─$
```

2. stackoverflow.com: _____

```
Nov 6 18:05
ngozi@kali: ~

Name: bbc.co.uk
Address: 151.101.192.81
Name: bbc.co.uk
Address: 2a04:4e42::81
Name: bbc.co.uk
Address: 2a04:4e42:200::81
Name: bbc.co.uk
Address: 2a04:4e42:400::81
Name: bbc.co.uk
Address: 2a04:4e42:600::81

__(ngozzi㉿kali)-[~]
└─$ nslookup netflix.com
Server: 192.168.63.2
Address: 192.168.63.2#53

Non-authoritative answer:
Name: netflix.com
Address: 18.200.8.190
Name: netflix.com
Address: 54.155.246.232
Name: netflix.com
Address: 54.73.148.110
Name: netflix.com
Address: 2a05:d018:76c:b684:b233:ac1f:be1f:
Name: netflix.com
Address: 2a05:d018:76c:b685:c898:aa3a:42c7:9d21
Name: netflix.com
Address: 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1

__(ngozzi㉿kali)-[~]
└─$ whatweb example.com
http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECAcc (dcd/7D6B)], IP[93.184.215.14], Title[Example Domain]

__(ngozzi㉿kali)-[~]
└─$ whatweb stackoverflow.com
http://stackoverflow.com [302 Found] Country[UNITED STATES][US], HTTPServer[Ericsson Web Redirect], IP[104.18.32.7], RedirectLocation[http://engage1.mtn.ng/]
ERROR: Opening: http://engage1.mtn.ng/ - Connection reset by peer

__(ngozzi㉿kali)-[~]
└─$
```

3. github.com: _____

```

Nov 6 18:05
ngozi@kali: ~

Address: 2a04:4e42::81
Name: bbc.co.uk
Address: 2a04:4e42:200::81
Name: bbc.co.uk
Address: 2a04:4e42:400::81
Name: bbc.co.uk
Address: 2a04:4e42:600::81

__(ngozzi㉿kali)-[~]
└─$ nslookup netflix.com
Server:      192.168.63.2
Address:    192.168.63.2#53

Non-authoritative answer:
Name:  netflix.com
Address: 18.200.8.190
Name:  netflix.com
Address: 54.155.246.232
Name:  netflix.com
Address: 54.73.148.110
Name:  netflix.com
Address: 2a05:d018:76c:b684:b233:ac1f:be1f:7
Name:  netflix.com
Address: 2a05:d018:76c:b685:c998:aa3a:42c7:9d21
Name:  netflix.com
Address: 2a05:d018:76c:b683:e1fe:9fbf:c403:57f1

__(ngozzi㉿kali)-[~]
└─$ whatweb example.com
http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECacc (ddc/7D6B)], IP[93.184.215.14], Title[Example Domain]

__(ngozzi㉿kali)-[~]
└─$ whatweb stackoverflow.com
http://stackoverflow.com [302 Found] Country[UNITED STATES][US], HTTPServer[Ericsson Web Redirect], IP[104.18.32.7], RedirectLocation[http://engage1.mtn.ng/]
ERROR: Opening: http://engage1.mtn.ng/ - Connection reset by peer

__(ngozzi㉿kali)-[~]
└─$ whatweb github.com
http://github.com [302 Found] Country[UNITED STATES][US], HTTPServer[Ericsson Web Redirect], IP[140.82.121.3], RedirectLocation[http://engage1.mtn.ng/]

```

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: _____

```

Nov 6 18:10
ngozi@kali: ~

__(ngozzi㉿kali)-[~]
└─$ whatweb --aggression 3 -v google.com
WhatWeb report for http://google.com
Status   : 301 Moved Permanently
Title    : 301 Moved
IP       : 216.58.223.238
Country  : UNITED STATES, US
Summary  : HTTPServer[gus], 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     : gus (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-aspart-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 ]
```

```
Nov 6 18:10
ngozi@kali:~

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/1.1 200 OK
Date: Wed, 06 Nov 2024 23:10:03 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
Content-Security-Policy-Report-Only: object-src 'none';script-src 'nonce-a7EX6GoGf3RKuViKYE8DQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http;report-uri http://csp.whatweb.google.com/csp/gws/other-hp
PSP: CP="This is not a PSP policy! See g.co/p3phelp for more info."
Content-Encoding: gzip
Server: gws
Content-Length: 9060
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Set-Cookie: AEC=AyVB7cpCPm707xuR65nAd6R7eKifCslX8aVy4LQHsfl_1RXNV4e-HxOqA; expires=Mon, 05-May-2025 23:10:03 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
Set-Cookie: NID=519-R7bj57Tu6CcGV0a0zXth_y1wV0U0T7Zz--d4UlgZE2n2c4ou9gJce7W/xI26LPcMZ2wUK_83CkDLYb1cQ4EDrPxAcEVKiccu_JMrMpJ_Fkmfm-avtyIG9yfshZmnIZQn5jByRtqLN4wRqlKpIKpITsD8zwPYLUAo5iYgdSckz_PohZ4wBSGizDFo13cE; expires=Thu, 08-May-2025 23:10:03 GMT; path=/; domain=.google.com; HttpOnly
Connection: close

(ngoziz@kali)-[~]
```

2. facebook.com: _____

```
Nov 6 18:13
ngozi@kali:~

(ngoziz@kali)-[~]
$ 
(ngoziz@kali)-[~]
$ whatweb -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: Wed, 06 Nov 2024 23:11:53 GMT
Connection: close
Content-Length: 0

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

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

Step 1: Subdomain Enumeration Using sublist3r

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

- github.com
 - google.com

Record Your Findings:

1. Subdomains for github.com:

KALI Linux - VMware Workstation

File Edit View VM Tabs Help

Library Type here... KALI Linux

My Computer KALI Linux

Home Apps Places

Nov 7 02:34

ngozi@kali: ~

BURP SUITE

Coded By Ahmed Aboul-Ela - @abouel3la

```
[!] 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 SSL Certificates...
[!] Searching now in PassiveDNS...
[!] Error: VirusTotal probably now is blocking our requests
[!] Total Unique Subdomains Found: 95
www.github.com
atom-hacker.github.com
atomicgithub.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
communicating.github.com
community.caterpillar.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
dogehall.github.com
audio.github.com
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Nov 7 02:35

ngozi@kali: ~

```
octostatus-production.github.com
offer.github.com
partnerportal.github.com
www.partnerportal.github.com
pkg.github.com
porter.github.com
porter2.github.com
proxina-review-lab.github.com
raw.github.com
registry.github.com
render.github.com
rendersite.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.staging-lab.com
www.wi_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
```

(ngoziz@kali)-[~]

2. Subdomains for google.com:

```

Nov 7 02:37
ngozi@kali:~ 

[!] 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
[!] Total Subdomains Found: 97

www.google.com
accounts.google.com
freezezone.accounts.google.com
adwords.google.com
qa.adz.google.com
answers.google.com
apps-secure-data-connector.google.com
audios.google.com
checkout.google.com
mtv-dc-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
logos.corp.google.com
mtv-dc.corp.google.com
mygizt.corp.google.com
mygizt010.corp.google.com
proxycfg.corp.google.com
resseed.corp.google.com
twdsalesgsa.twd.corp.google.com
uberproxy.corp.google.com
uberproxy-nocert.corp.google.com
uberproxy-san.corp.google.com

Nov 7 02:37
ngozi@kali:~ 

search.freezezone.google.com
gmail.google.com
hosted-d-id.google.com
jnto.google.com
aspxl.google.com
alt1.aspxl.google.com
alt2.aspxl.google.com
alt3.aspxl.google.com
alt4.aspxl.google.com
gmai-smtp-inl.google.com
alt1.gmai-smtp-inl.google.com
alt2.gmai-smtp-inl.google.com
alt3.gmai-smtp-inl.google.com
alt4.gmai-smtp-inl.google.com
gma-smtp-inl.google.com
alt1.gmr-smtp-inl.google.com
alt2.gmr-smtp-inl.google.com
alt3.gmr-smtp-inl.google.com
alt4.gmr-smtp-inl.google.com
vp.video.l.google.com
m.google.com
freezezone.m.google.com
mail.google.com
freezezone.mail.google.com
misc.google.com
misc-sni.google.com
mtalk.google.com
mx.google.com
ics-pst.google.com
annobox.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
[~(ngozi@kali)-~]
-$ 

```

Step 2: Directory Discovery Using dir

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

- <http://example.com>
- <http://example.org>

Record Your Findings:

1. Directories for google.com:

```

Nov 7 02:59
ngozi@kali:~>

MKULL: cannot create directory http://google.com ; no such file or directory
(ngoziz@kali)-[~]
-$ theharvester -d google.com -b google
zsh: no such file or directory: google.com

(ngoziz@kali)-[~]
-$ dirb https://google.com

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

START TIME: Thu Nov 7 02:51:48 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:24)
+ https://google.com/2002 (CODE:301|SIZE:24)
+ https://google.com/2003 (CODE:301|SIZE:24)
+ https://google.com/2004 (CODE:301|SIZE:24)
+ https://google.com/2005 (CODE:301|SIZE:24)
+ https://google.com/2006 (CODE:301|SIZE:24)
+ https://google.com/2007 (CODE:301|SIZE:24)
+ https://google.com/2008 (CODE:301|SIZE:24)
+ https://google.com/2009 (CODE:301|SIZE:24)
+ https://google.com/2010 (CODE:301|SIZE:24)
+ https://google.com/2011 (CODE:301|SIZE:24)
+ https://google.com/2012 (CODE:301|SIZE:24)
+ https://google.com/2013 (CODE:301|SIZE:24)
+ https://google.com/2014 (CODE:301|SIZE:24)
+ 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)

Nov 7 03:01
ngozi@kali:~>

+ https://google.com/doubleclick (CODE:301|SIZE:231)
+ https://google.com/downloads (CODE:301|SIZE:229)
+ https://google.com/ebooks (CODE:301|SIZE:226)
+ https://google.com/edu (CODE:301|SIZE:223)
+ https://google.com/education (CODE:301|SIZE:229)
+ https://google.com/enterprise (CODE:301|SIZE:230)
+ https://google.com/errors (CODE:301|SIZE:226)
+ https://google.com/favicon.ico (CODE:301|SIZE:231)
+ https://google.com/fi (CODE:302|SIZE:0)
+ https://google.com/files (CODE:301|SIZE:225)
+ https://google.com/finance (CODE:301|SIZE:227)
+ https://google.com/firefox (CODE:301|SIZE:227)
+ https://google.com/fitness (CODE:301|SIZE:220)
+ https://google.com/forms (CODE:301|SIZE:223)
+ https://google.com/fotos (CODE:301|SIZE:225)
+ https://google.com/friends (CODE:301|SIZE:227)
+ https://google.com/fusion (CODE:301|SIZE:226)
+ https://google.com/games (CODE:301|SIZE:225)
+ https://google.com/get (CODE:301|SIZE:223)
+ https://google.com/get (CODE:301|SIZE:223)
+ https://google.com/grants (CODE:301|SIZE:226)
+ https://google.com/green (CODE:301|SIZE:225)
+ https://google.com/groups (CODE:301|SIZE:226)
+ https://google.com/health (CODE:301|SIZE:226)
+ https://google.com/hire (CODE:301|SIZE:24)
+ https://google.com/history (CODE:301|SIZE:0)
+ https://google.com/home (CODE:301|SIZE:24)
(!) 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)

---- Entering directory: https://google.com/business/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')

END_TIME: Thu Nov 7 02:57:38 2024
DOWNLOADED: 1907 - FOUND: 101

(ngoziz@kali)-[~]
-$

```

2. Directories for facebook.org:

```
  Apps  Places          Nov 7 03:03:03  
  ↗  
START_TIME: Thu Nov  7 03:02:11 2024  
URL_BASE: https://facebook.com/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----  
GENERATED WORDS: 4612  
---- Scanning URL: https://facebook.com/ ----  
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs [30X].  
  (Try using FineTuning: '-f')  
-----  
END_TIME: Thu Nov  7 03:02:13 2024  
DOWNLOADED: 0 - FOUND: 0  
---(ngazi㉿kali)-[~]  
└─$ dirb https://facebook.org  
-----  
DIRB v2.22  
By The Dark Raver  
-----  
START_TIME: Thu Nov  7 03:03:16 2024  
URL_BASE: https://facebook.org/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt  
-----  
GENERATED WORDS: 4612  
---- Scanning URL: https://facebook.org/ ----  
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs [30X].  
  (Try using FineTuning: '-f')  
-----  
END_TIME: Thu Nov  7 03:03:19 2024  
DOWNLOADED: 0 - FOUND: 0  
---(ngazi㉿kali)-[~]  
└─$
```

Step 3: Information Gathering Using theHarvester

Exercise 3: Use theHarvester to gather information on the following domain:

- microsoft.com

Record Your Findings:

- Emails and Information Gathered

```
  Apps  Places
Nov 7 03:17
ngozi@kali: ~
* [!] Invalid source.

[ngzi@kali:~] -$ theHarvester -d microsoft.com -b yahoo
Read proxies.yaml from /home/ngozi/.theHarvester/proxies.yaml
* [*] Target: microsoft.com
[*] Searching Yahoo.
[*] No IPs found.
[*] No emails found.
[*] Hosts Found: 38
about.ads.microsoft.com
account.microsoft.com
```

```
about.ads.microsoft.com
account.microsoft.com
accountprotection.microsoft.com
admin.microsoft.com
admin.powerplatform.microsoft.com
answers.microsoft.com
app.fabric.microsoft.com
apps.microsoft.com
appsource.microsoft.com
azure.microsoft.com
bingapp.microsoft.com
bluemix.microsoft.com
careers.microsoft.com
copilot.microsoft.com
create.microsoft.com
designer.microsoft.com
developer.microsoft.com
entra.microsoft.com
forms.microsoft.com
go.microsoft.com
learn.microsoft.com
mail.support.microsoft.com
myaccess.microsoft.com
myaccount.microsoft.com
myapplications.microsoft.com
myapps.microsoft.com
myprofilefile.microsoft.com
mysignins.microsoft.com
myticketaccount.microsoft.com
news.microsoft.com
partner.microsoft.com
pcomanager.microsoft.com
support.microsoft.com
support.serviceshub.microsoft.com
techcommunity.microsoft.com
translator.microsoft.com
verify.microsoft.com
wus.prod.support.services.microsoft.com

(ngizi@kali)-[~]
-$
```