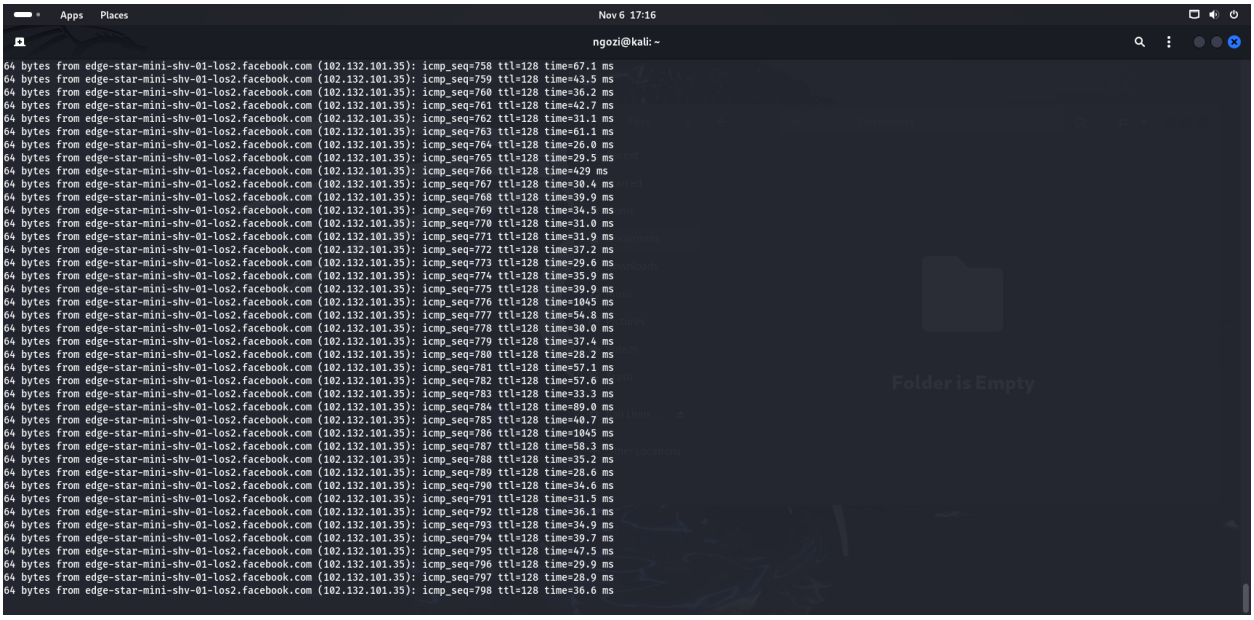
Week 1: Reconnaissance, Information Gathering, and Scanning

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: _____



2. twitter.com: _____

3. amazon.com: _____

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? _____

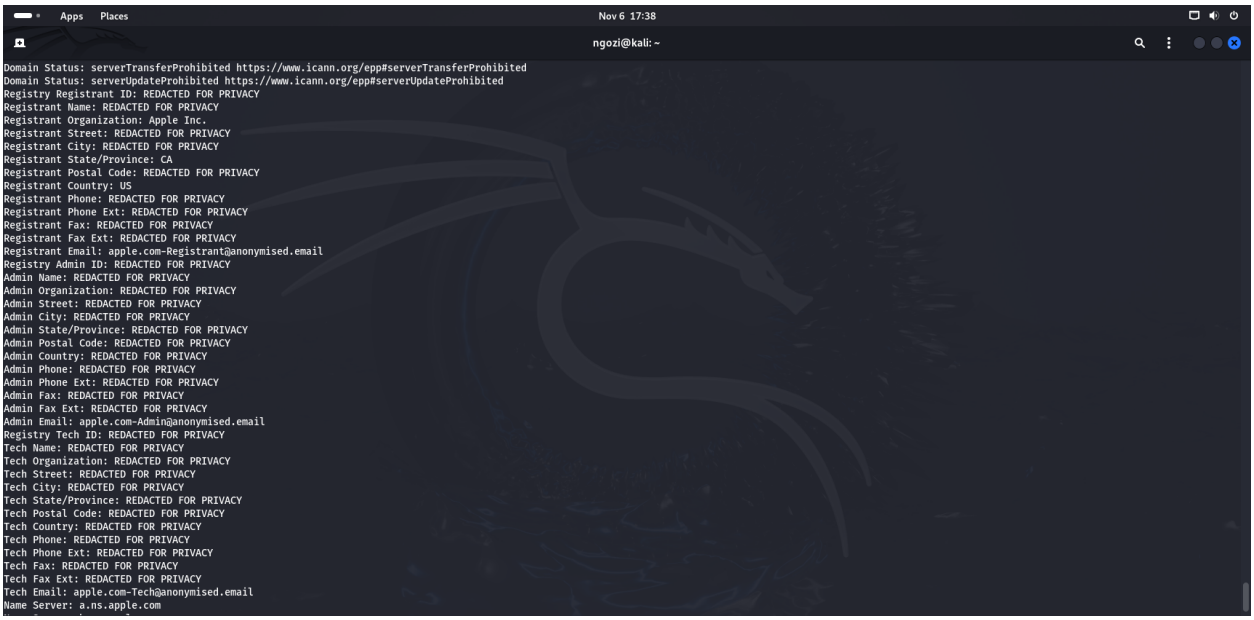
Answer: 2026-10-09

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

Answer: MarkMonitor, Inc.

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


Apps
Places
Nov 6 17:36
ngozi@kali: ~
(2) 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: 2023-08-28T18:33:11Z
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: 2024-11-06T22:35:35Z <<<


Apps
Places
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 Registrant 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

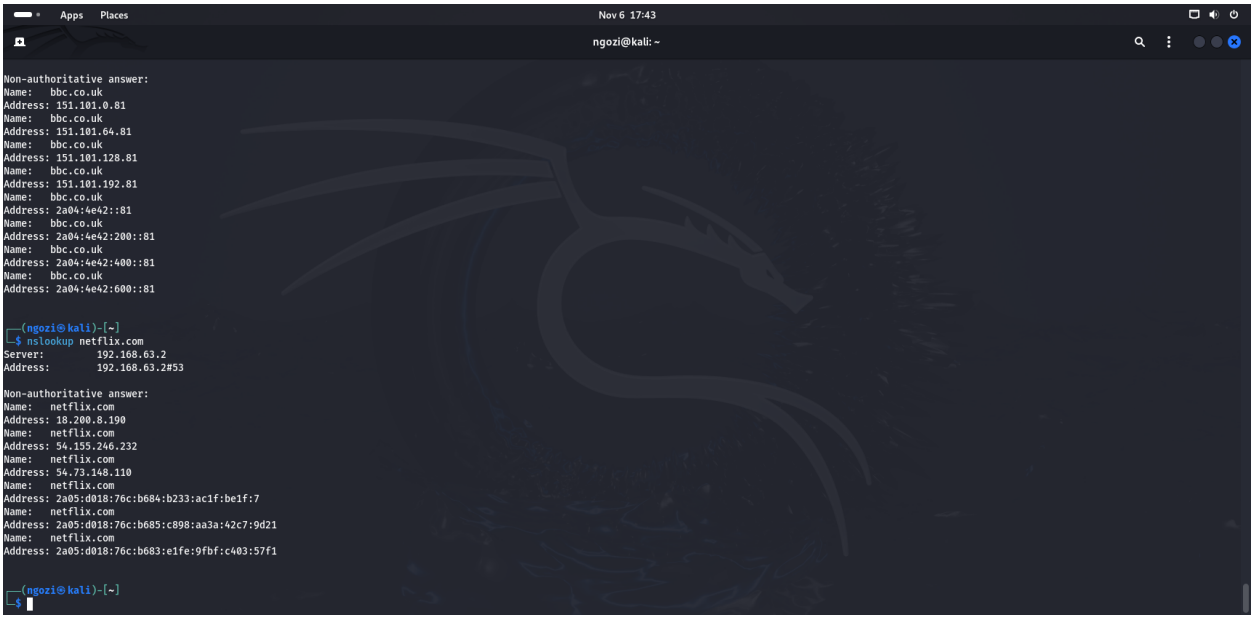
• netflix.com

Answer These Questions:

1. What is the IP address for bbc.co.uk? _____

Answer: 192.168.63.2#53

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



Answer: Netflix.com

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

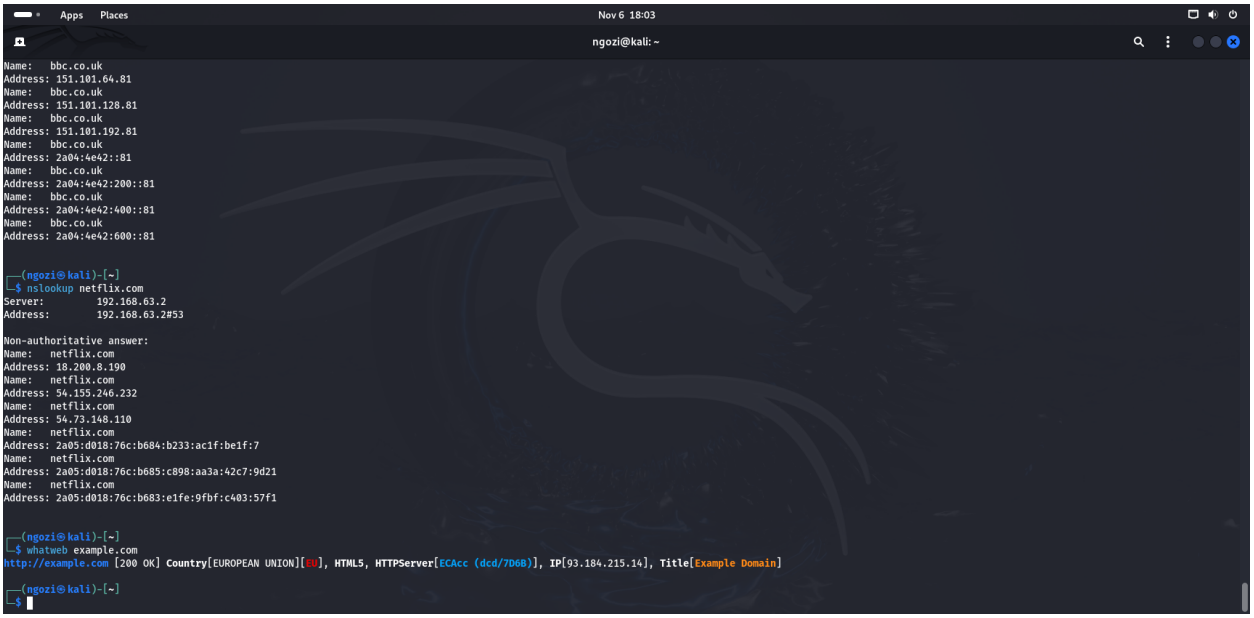
Lab Steps Step 1: Detect Web Technologies Using whatweb

Exercise 1: Run the whatweb command to detect technologies for the following targets:

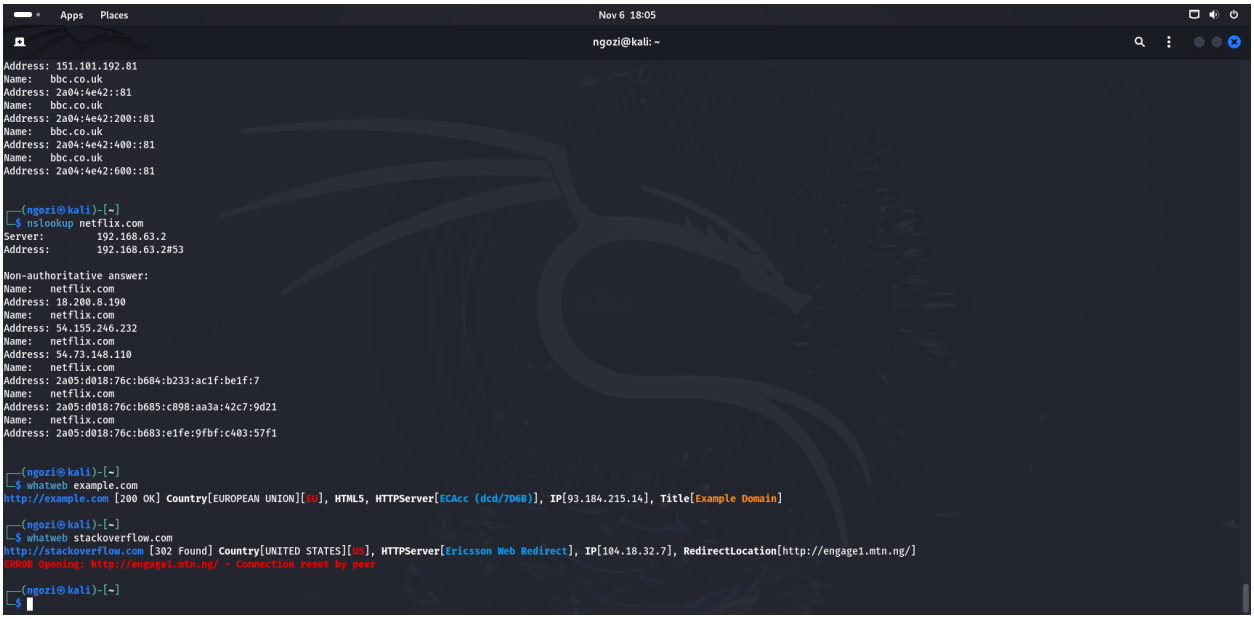
- example.com
- stackoverflow.com
- github.com

Record Your Findings:

1. example.com: _____



2. stackoverflow.com: _____



3. github.com: _____

Step 2: Perform Aggressive Scanning Using whatweb

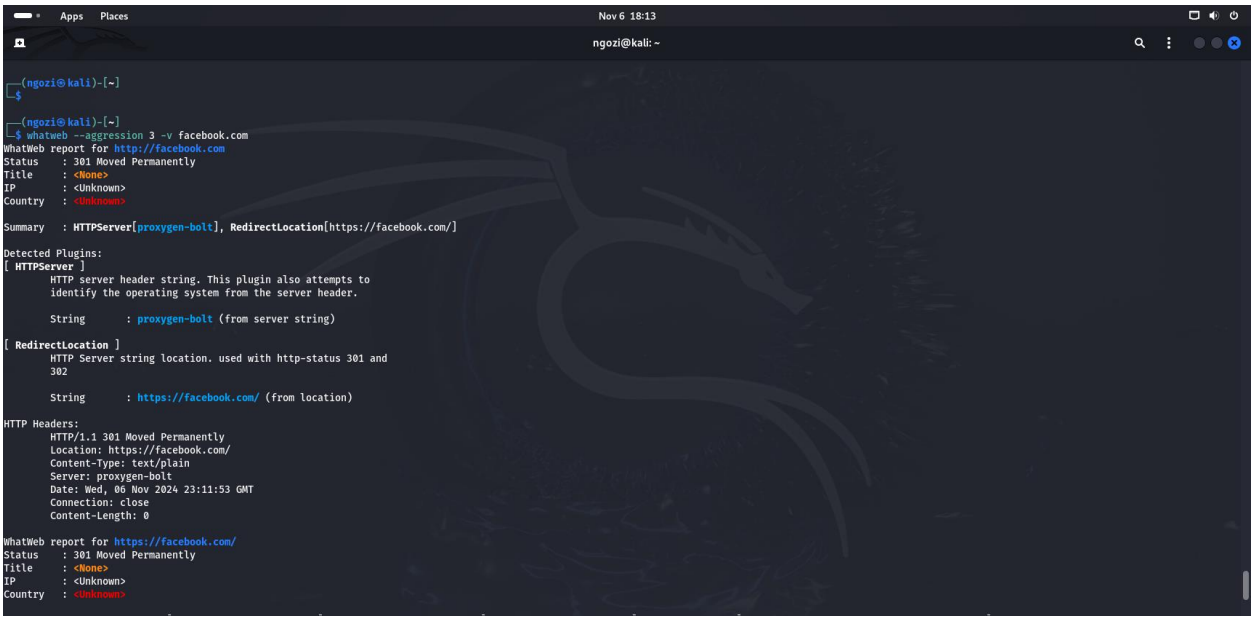
Exercise 2: Perform an aggressive scan on the following targets:

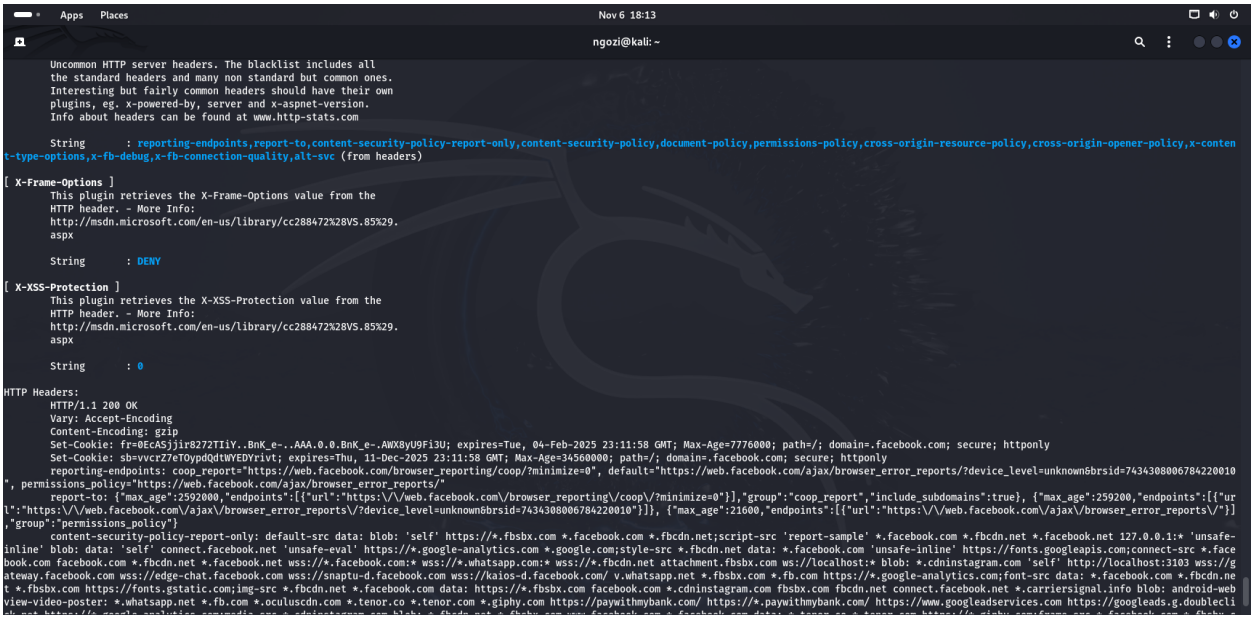
- google.com
- facebook.com

Record Your Findings:

1. google.com: _____

2. facebook.com: _____





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

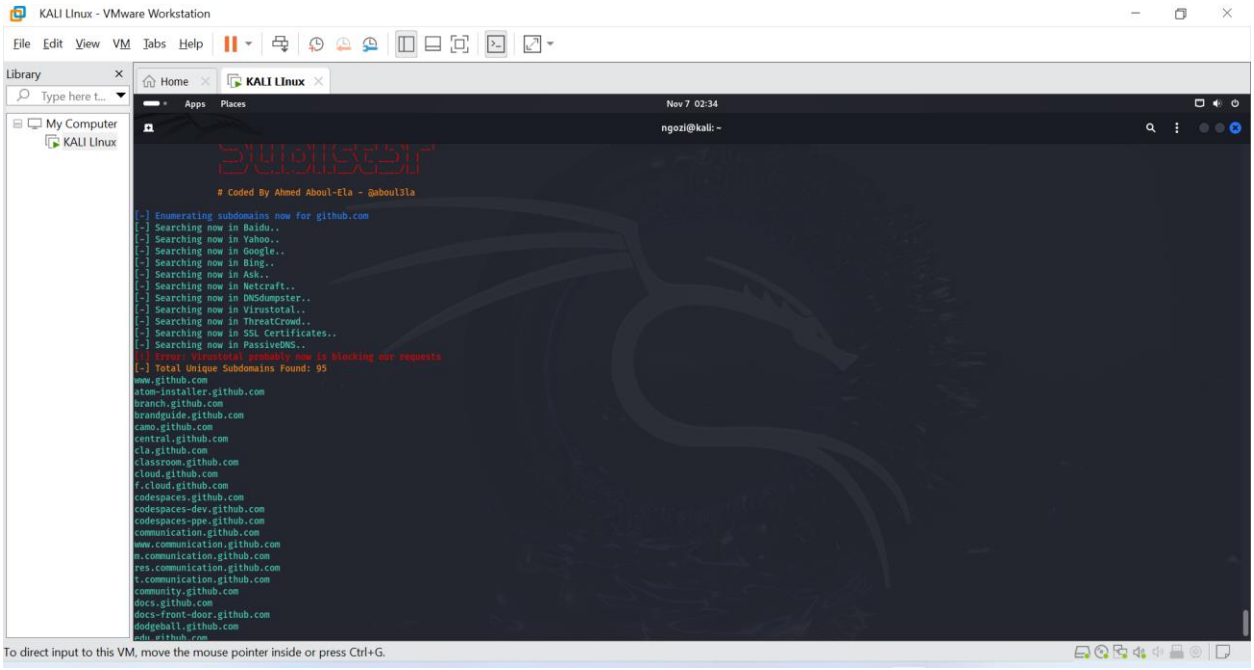
Step 1: Subdomain Enumeration Using sublist3r

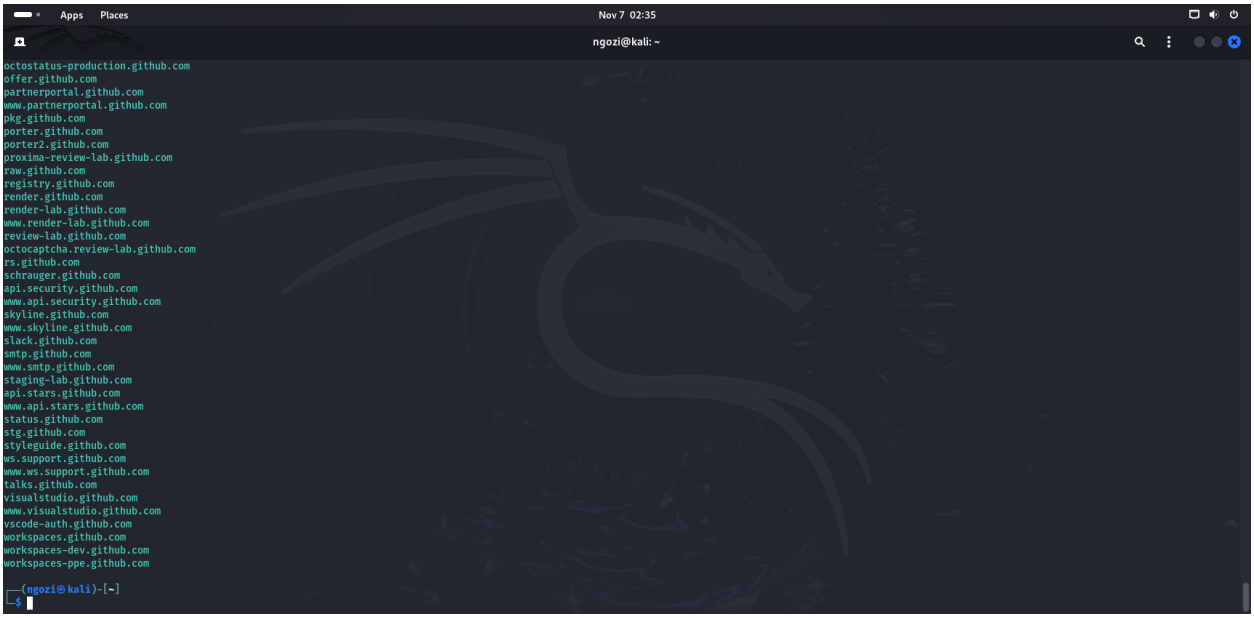
Exercise 1: Run the sublist3r command for the following domains:

- github.com
- google.com

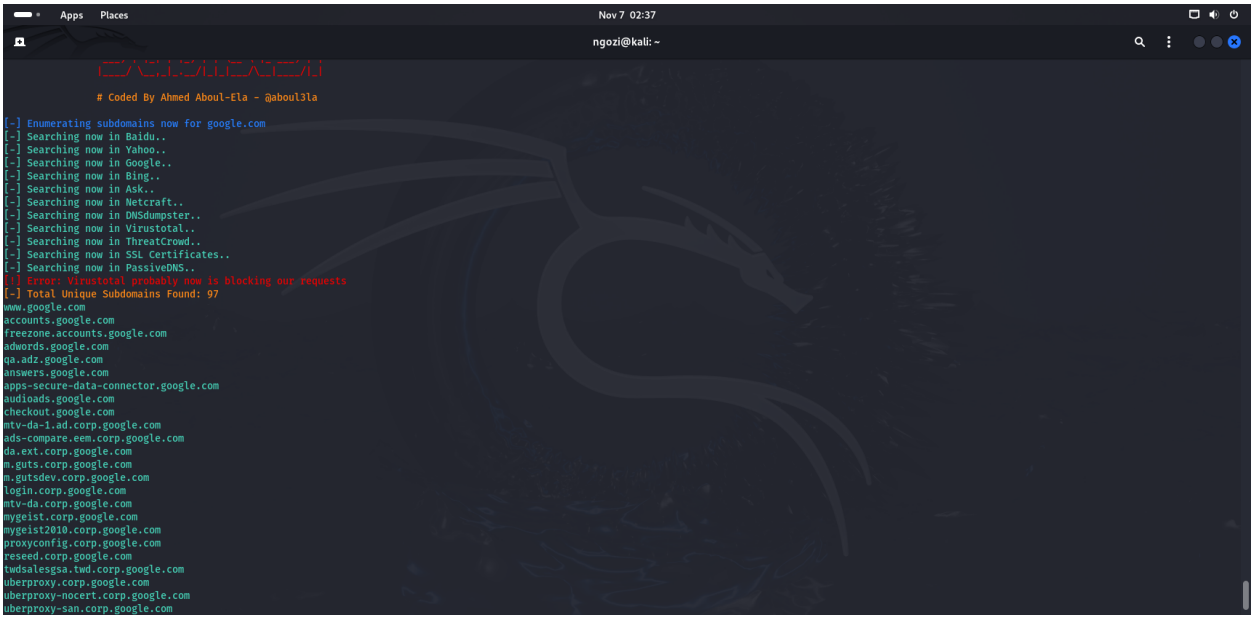
Record Your Findings:

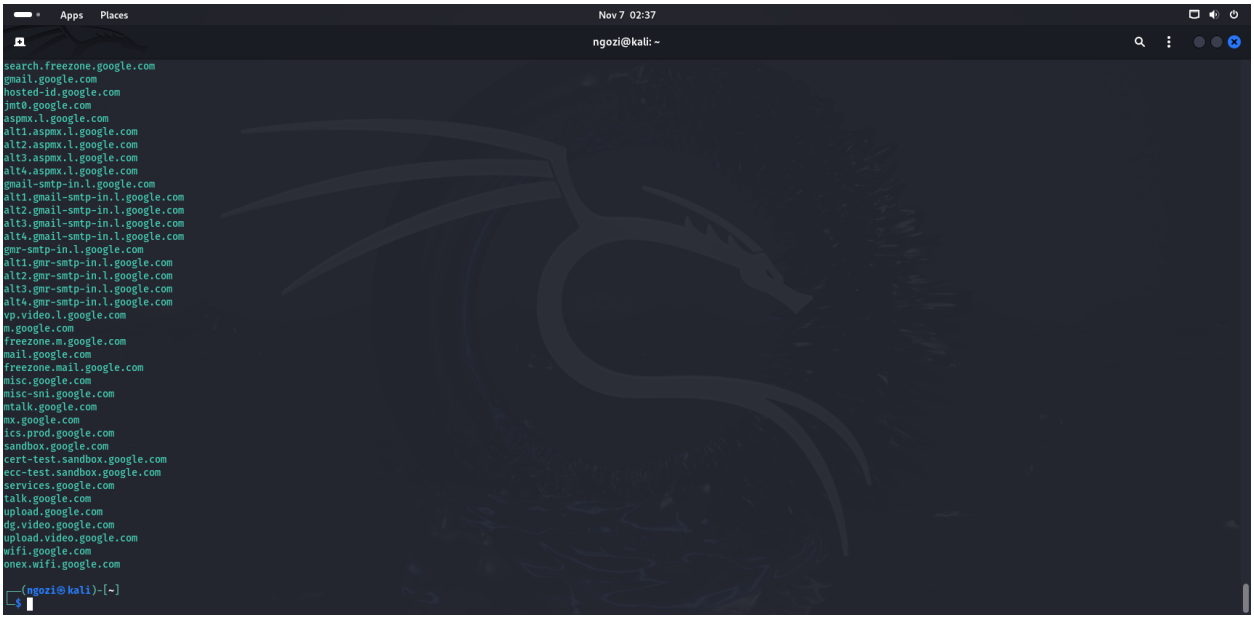
1. Subdomains for github.com:





2. Subdomains for google.com:





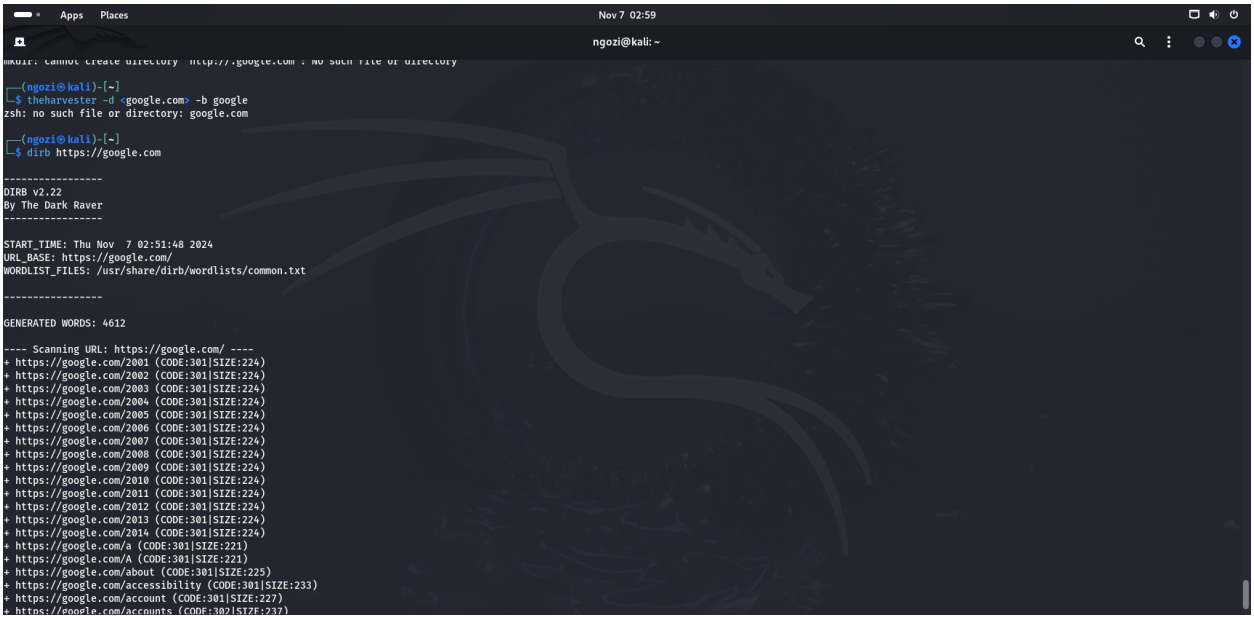
Step 2: Directory Discovery Using dir

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:



2. Directories for facebook.org:

Step 3: Information Gathering Using theHarvester

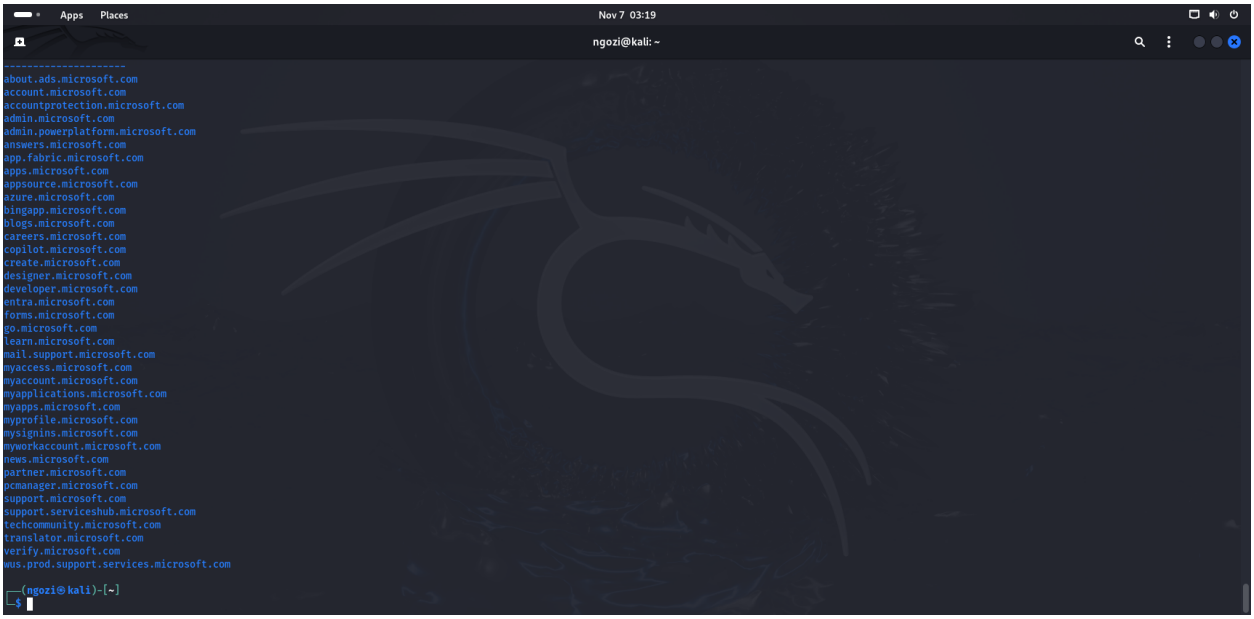
Exercise 3: Use theHarvester to gather information on the following domain:

- microsoft.com

Record Your Findings:

- Emails and Information Gathered


Apps Places
Nov 7 03:17
ngozi@kali: ~
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[!] Invalid source.
┌──(ngozi㉿kali)-[~]
└─$ theHarvester -d microsoft.com -b yahoo
Read proxies.yaml from /home/ngozi/.theHarvester/proxies.yaml
* theHarvester 4.6.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
[*] Target: microsoft.com
[*] Searching Yahoo.
[*] No IPs found.
[*] No emails found.
[*] Hosts found: 38
about.ads.microsoft.com
account.microsoft.com


Apps Places
Nov 7 03:19
ngozi@kali: ~
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
blogs.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
myprofile.microsoft.com
mysignins.microsoft.com
myworkaccount.microsoft.com
news.microsoft.com
partner.microsoft.com
pcmanager.microsoft.com
support.microsoft.com
support.serviceshub.microsoft.com
techcommunity.microsoft.com
translator.microsoft.com
verify.microsoft.com
wus.prod.support.services.microsoft.com
┌──(ngozi㉿kali)-[~]
└─$