ETHICAL HACKING

LAB ASSIGNMENT -3

Name: Dasari Sanath Kumar

ID: 700760349

CRN: 22285

Reconnaissance phase is nothing but information gathering phase where we gather all the required information of a particular organization, system information or a network information without effecting the target machine.

In this Lab report we will be exploring how can we achieve the reconnaissance phase.

Here we have two types of reconnaissance :

a. Active Reconnaissance -- effects directly the target machine
b. Passive Reconnaissance -- it doesn't effects the target machine

Commands and their description:

1. ***recon-ng*** : This command is used to speed up the information gathering process from open sources .And it is a python framework.
2. ***[recon-ng][default] > help*** : This command would provide information about the available modules in Recon-ng.
3. ***[recon-ng] [default]*** *> options list* : In the context of Recon-ng, the command "options list" is used to display the current configuration settings for a specific module
4. ***[recon-ng] [default] > marketplace install all*** : This command is used to install all the modules in marketplace.
5. ***[recon-ng] [default] > workspaces create SampleWS*** : This command is used to create a sample workspaces nothing but the folder for reconnaissance
6. ***[recon-ng] > options set nameserver [Ip]*** **:** This command is used to set nameserver to the workspaces of our target machine
7. ***[recon-ng] > marketplace refresh , [recon-ng] > marketplace search , [recon-ng] > marketplace search resolve*** these three commands used on marketplaces to refresh ,search and resolve discrepancies if there any.
8. ***[recon-ng] > marketplace install all :*** *This will* allow you to install all the modules in the marketplace
9. ***[recon-ng] > modules load [Name of the module]*** *eg.* recon/domains-hosts/bing_domain_web will allow you to load the module to your workspaces
10. ***[recon-ng] > show :*** *gives you all the db tables in the workspace*

After creating a workspaces we will be having a database in each workspaces with some database tables.

Companies,contacts,credentials,domains,hosts,leaks,locations,netblocks,ports,profiles,pushpin,repositories,vulnerabilities

Here in this Lab we are going to create a insert some data into netblocks table

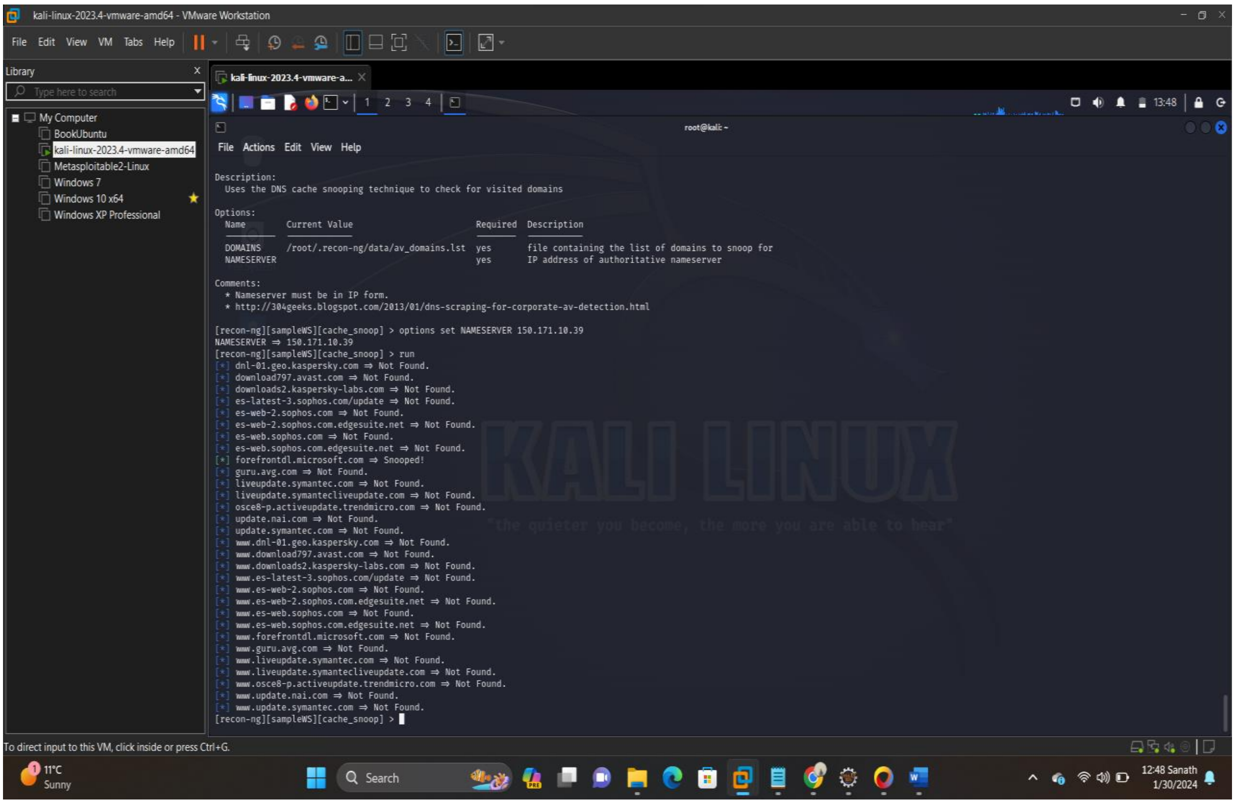
- And target will be Microsoft.com - 150.171.10.39

Tasks to be completed :

1. Run the cache_snoop module against Microsoft's DNS server. What antivirus software does Microsoft use?

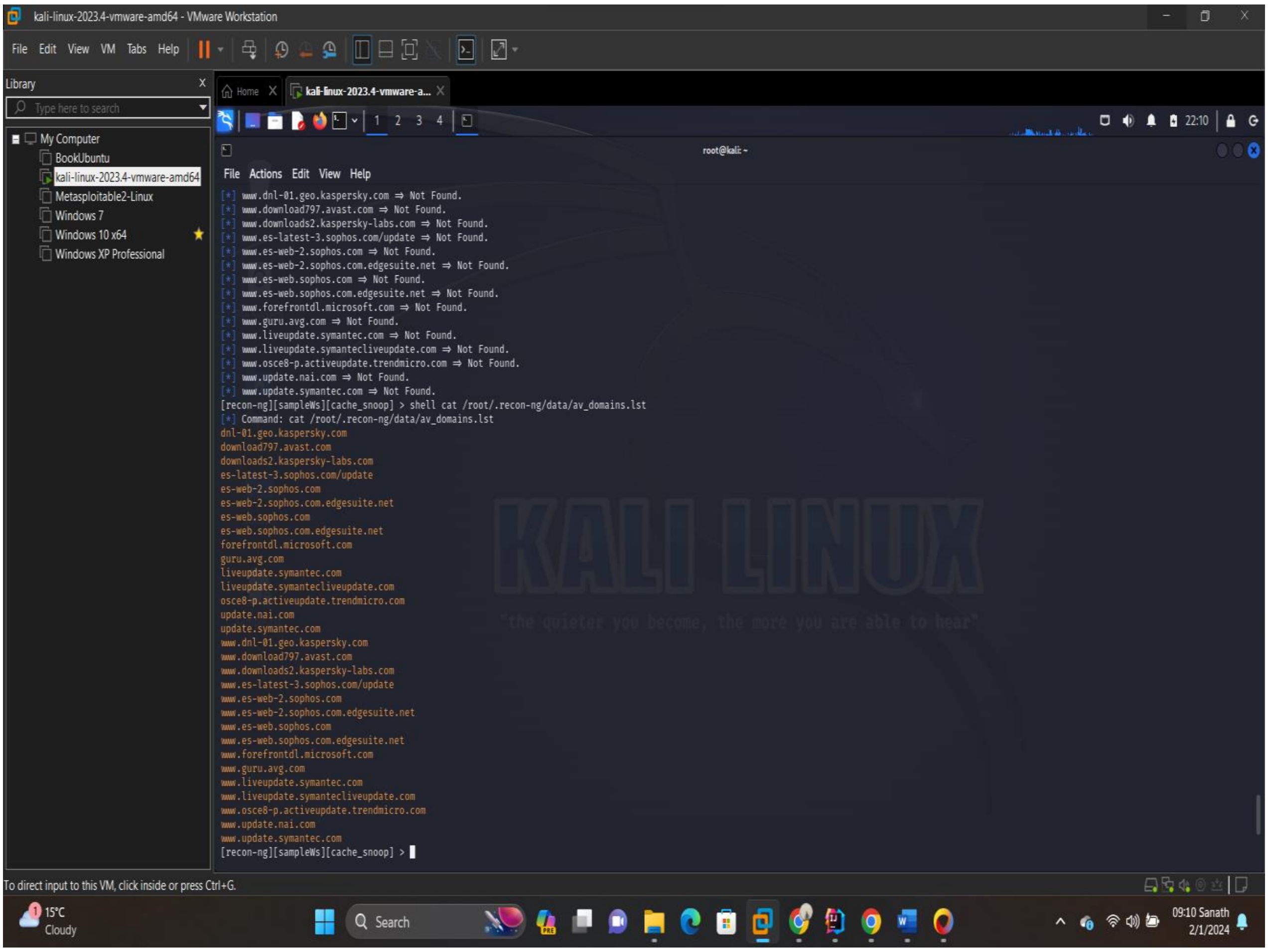
   We need to load the cache_snoop module for that we need to follow the below command

   a) ***[recon-ng] > modules load discovery/info_disclosure/cache_snoop***
   b) ***[recon-ng]*** **> options set NAMESERVER 150.171.10.39**
   c) ***[recon-ng] > run***



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

```
Description:
  Uses the DNS cache snooping technique to check for visited domains

Options:
  Name        Current Value                      Required  Description
  ----------  ---------------------------------  --------  -----------
  DOMAINS     /root/.recon-ng/data/av_domains.lst yes      file containing the list of domains to snoop for
  NAMESERVER                                     yes       IP address of authoritative nameserver

Comments:
  * Nameserver must be in IP form.
  * http://304geeks.blogspot.com/2013/01/dns-scraping-for-corporate-av-detection.html

[recon-ng][sampleWS][cache_snoop] > options set NAMESERVER 150.171.10.39
NAMESERVER ⇒ 150.171.10.39
[recon-ng][sampleWS][cache_snoop] > run
[*] dnl-01.geo.kaspersky.com ⇒ Not Found.
[*] download797.avast.com ⇒ Not Found.
[*] downloads2.kaspersky-labs.com ⇒ Not Found.
[*] es-latest-3.sophos.com/update ⇒ Not Found.
[*] es-web-2.sophos.com ⇒ Not Found.
[*] es-web-2.sophos.com.edgesuite.net ⇒ Not Found.
[*] es-web.sophos.com ⇒ Not Found.
[*] es-web.sophos.com.edgesuite.net ⇒ Not Found.
[*] forefrontdl.microsoft.com ⇒ Snooped!
[*] guru.avg.com ⇒ Not Found.
[*] liveupdate.symantec.com ⇒ Not Found.
[*] liveupdate.symantecliveupdate.com ⇒ Not Found.
[*] osce8-p.activeupdate.trendmicro.com ⇒ Not Found.
[*] update.nai.com ⇒ Not Found.
[*] update.symantec.com ⇒ Not Found.
[*] www.dnl-01.geo.kaspersky.com ⇒ Not Found.
[*] www.download797.avast.com ⇒ Not Found.
[*] www.downloads2.kaspersky-labs.com ⇒ Not Found.
[*] www.es-latest-3.sophos.com/update ⇒ Not Found.
[*] www.es-web-2.sophos.com ⇒ Not Found.
[*] www.es-web-2.sophos.com.edgesuite.net ⇒ Not Found.
[*] www.es-web.sophos.com ⇒ Not Found.
[*] www.es-web.sophos.com.edgesuite.net ⇒ Not Found.
[*] www.forefrontdl.microsoft.com ⇒ Not Found.
[*] www.guru.avg.com ⇒ Not Found.
[*] www.liveupdate.symantec.com ⇒ Not Found.
[*] www.liveupdate.symantecliveupdate.com ⇒ Not Found.
[*] www.osce8-p.activeupdate.trendmicro.com ⇒ Not Found.
[*] www.update.nai.com ⇒ Not Found.
[*] www.update.symantec.com ⇒ Not Found.
[recon-ng][sampleWS][cache_snoop] >
```

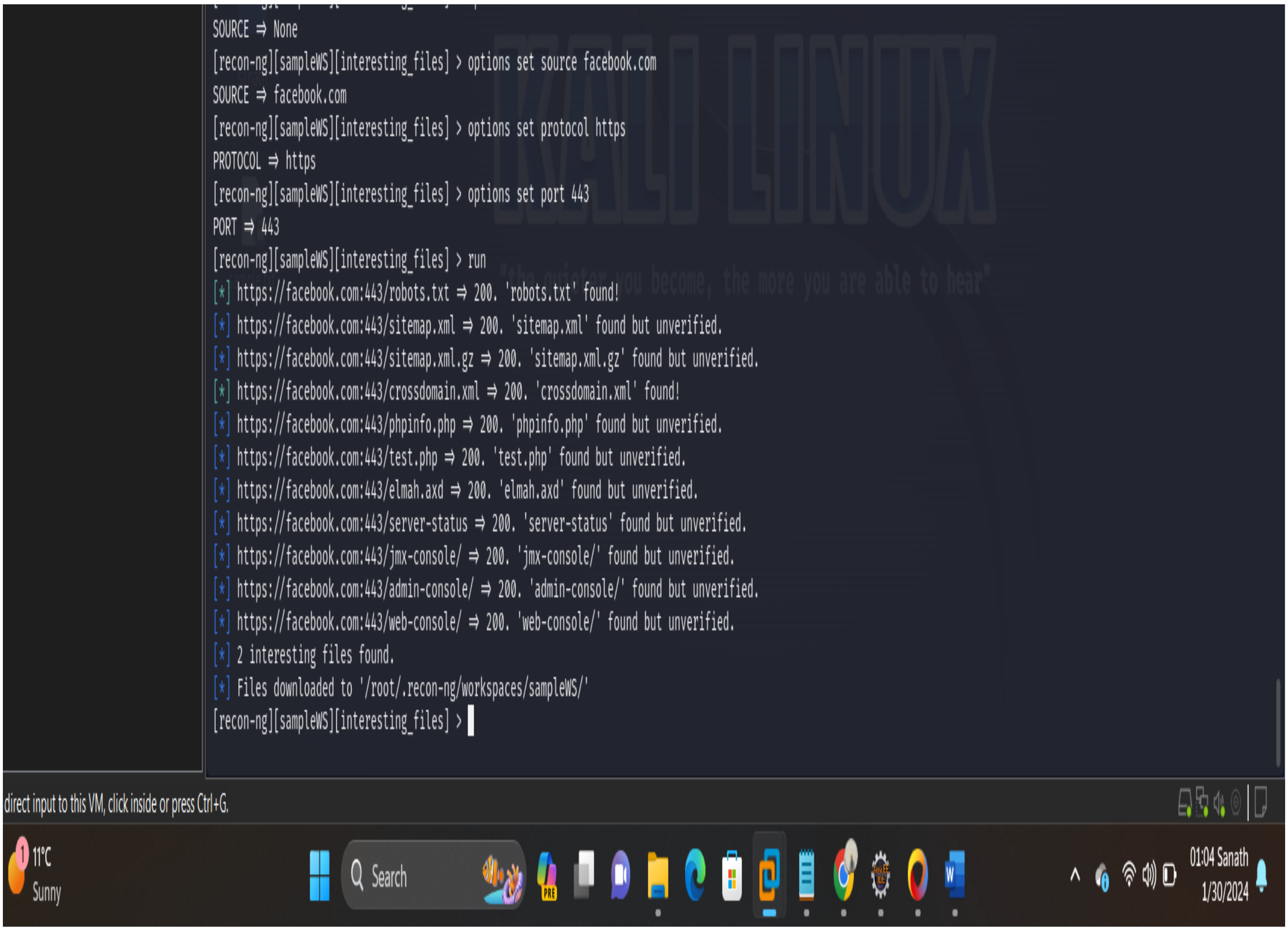


```
[*] www.dnl-01.geo.kaspersky.com ⇒ Not Found.
[*] www.download797.avast.com ⇒ Not Found.
[*] www.downloads2.kaspersky-labs.com ⇒ Not Found.
[*] www.es-latest-3.sophos.com/update ⇒ Not Found.
[*] www.es-web-2.sophos.com ⇒ Not Found.
[*] www.es-web-2.sophos.com.edgesuite.net ⇒ Not Found.
[*] www.es-web.sophos.com ⇒ Not Found.
[*] www.es-web.sophos.com.edgesuite.net ⇒ Not Found.
[*] www.forefrontdl.microsoft.com ⇒ Not Found.
[*] www.guru.avg.com ⇒ Not Found.
[*] www.liveupdate.symantec.com ⇒ Not Found.
[*] www.liveupdate.symantecliveupdate.com ⇒ Not Found.
[*] www.osce8-p.activeupdate.trendmicro.com ⇒ Not Found.
[*] www.update.nai.com ⇒ Not Found.
[*] www.update.symantec.com ⇒ Not Found.
[recon-ng][sampleWs][cache_snoop] > shell cat /root/.recon-ng/data/av_domains.lst
[*] Command: cat /root/.recon-ng/data/av_domains.lst
dnl-01.geo.kaspersky.com
download797.avast.com
downloads2.kaspersky-labs.com
es-latest-3.sophos.com/update
es-web-2.sophos.com
es-web-2.sophos.com.edgesuite.net
es-web.sophos.com
es-web.sophos.com.edgesuite.net
forefrontdl.microsoft.com
guru.avg.com
liveupdate.symantec.com
liveupdate.symantecliveupdate.com
osce8-p.activeupdate.trendmicro.com
update.nai.com
update.symantec.com
www.dnl-01.geo.kaspersky.com
www.download797.avast.com
www.downloads2.kaspersky-labs.com
www.es-latest-3.sophos.com/update
www.es-web-2.sophos.com
www.es-web-2.sophos.com.edgesuite.net
www.es-web.sophos.com
www.es-web.sophos.com.edgesuite.net
www.forefrontdl.microsoft.com
www.guru.avg.com
www.liveupdate.symantec.com
www.liveupdate.symantecliveupdate.com
www.osce8-p.activeupdate.trendmicro.com
www.update.nai.com
www.update.symantec.com
[recon-ng][sampleWs][cache_snoop] > 
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
15°C
Cloudy
Search
09:10 Sanath
2/1/2024

2. Run the interesting_files module against a domain of your choice. Provide a screenshot of the module output.

The below is the screenshot for finding interesting_files on facebook.com



```
SOURCE => None
[recon-ng][sampleWS][interesting_files] > options set source facebook.com
SOURCE => facebook.com
[recon-ng][sampleWS][interesting_files] > options set protocol https
PROTOCOL => https
[recon-ng][sampleWS][interesting_files] > options set port 443
PORT => 443
[recon-ng][sampleWS][interesting_files] > run
[*] https://facebook.com:443/robots.txt => 200. 'robots.txt' found!
[*] https://facebook.com:443/sitemap.xml => 200. 'sitemap.xml' found but unverified.
[*] https://facebook.com:443/sitemap.xml.gz => 200. 'sitemap.xml.gz' found but unverified.
[*] https://facebook.com:443/crossdomain.xml => 200. 'crossdomain.xml' found!
[*] https://facebook.com:443/phpinfo.php => 200. 'phpinfo.php' found but unverified.
[*] https://facebook.com:443/test.php => 200. 'test.php' found but unverified.
[*] https://facebook.com:443/elmah.axd => 200. 'elmah.axd' found but unverified.
[*] https://facebook.com:443/server-status => 200. 'server-status' found but unverified.
[*] https://facebook.com:443/jmx-console/ => 200. 'jmx-console/' found but unverified.
[*] https://facebook.com:443/admin-console/ => 200. 'admin-console/' found but unverified.
[*] https://facebook.com:443/web-console/ => 200. 'web-console/' found but unverified.
[*] 2 interesting files found.
[*] Files downloaded to '/root/.recon-ng/workspaces/sampleWS/'
[recon-ng][sampleWS][interesting_files] >
```

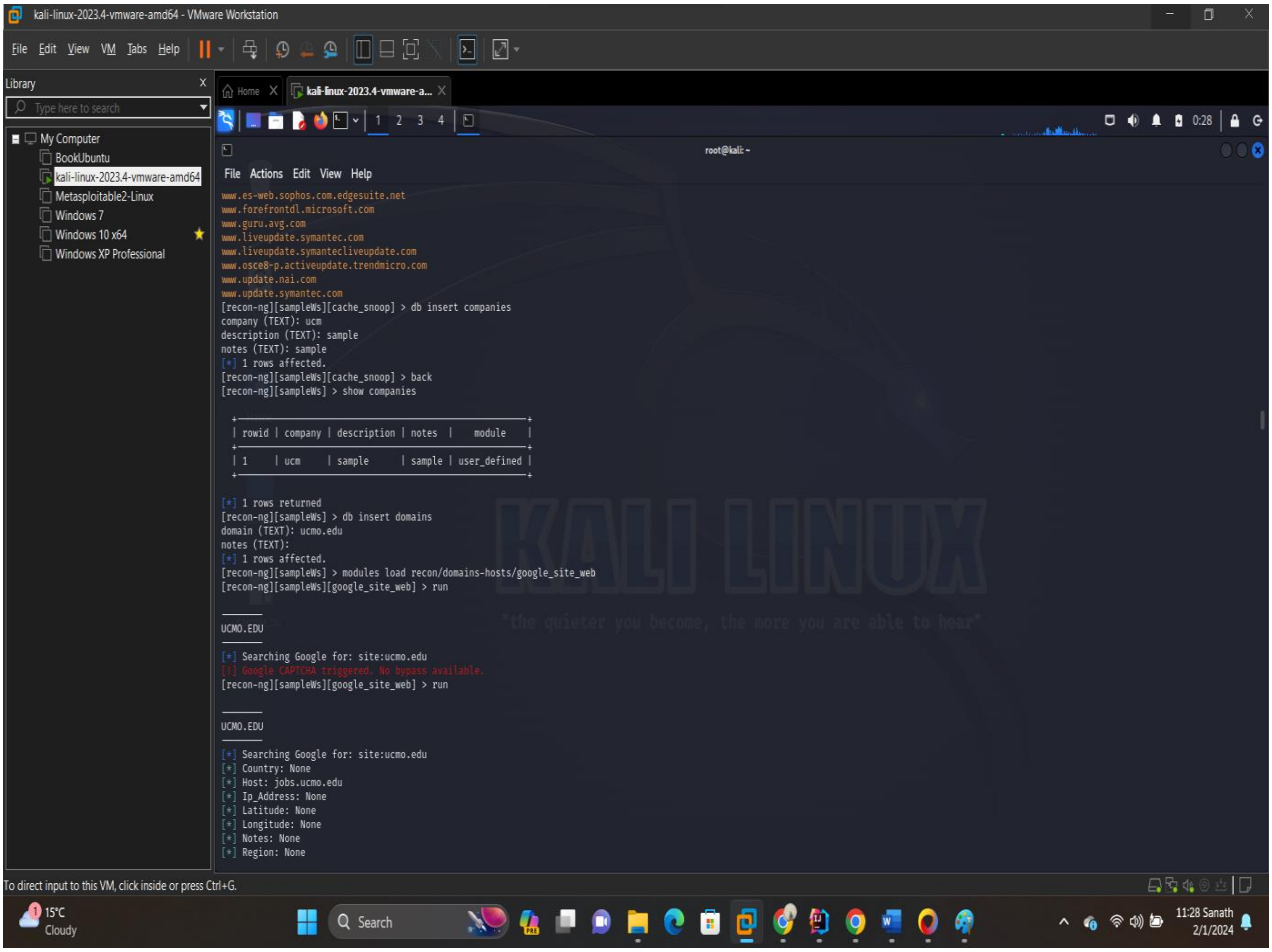
direct input to this VM, click inside or press Ctrl+G.

We have found two interesting files for facebook.com they are robots.txt and crossdomain.xml

We can we the content of these files by searching www.facebook.com/robots.txt and www.facebook.com/crossdomain.xml

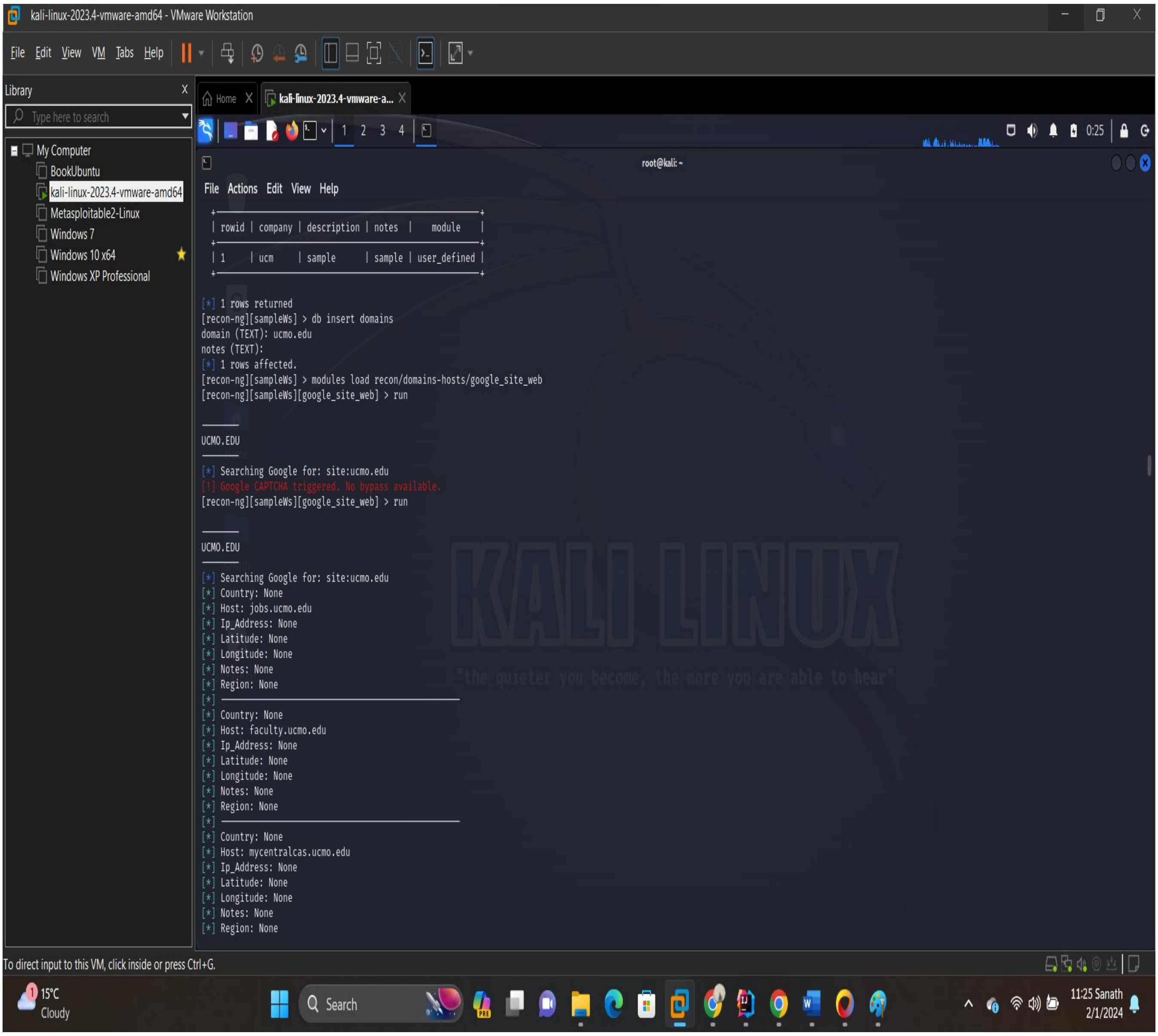
3. Continue from step 14. After obtaining the hostnames from the ucmo.edu domain, we'd like to find the corresponding IP addresses for those identified hosts. We will use the recon/hosts- hosts/resolve module. Provide a screenshot of the module output.

   In this task we have to find IP Address of ucmo.edu hosts and below are the screenshots for achieving IP Address with recon/hosts-hosts/resolve module , please find the below screenshots.

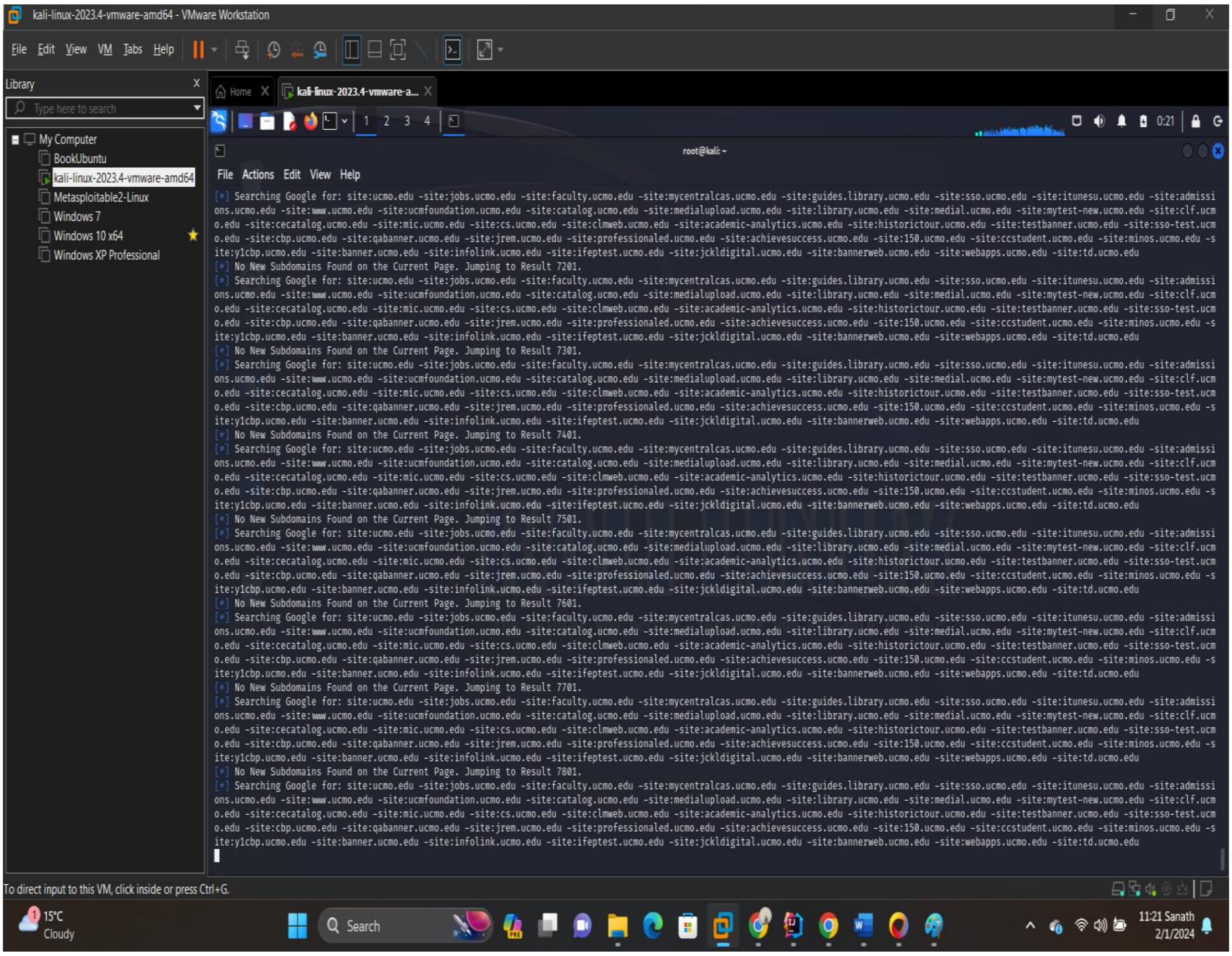


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
15°C
Cloudy
Search
11:28 Sanath
2/1/2024

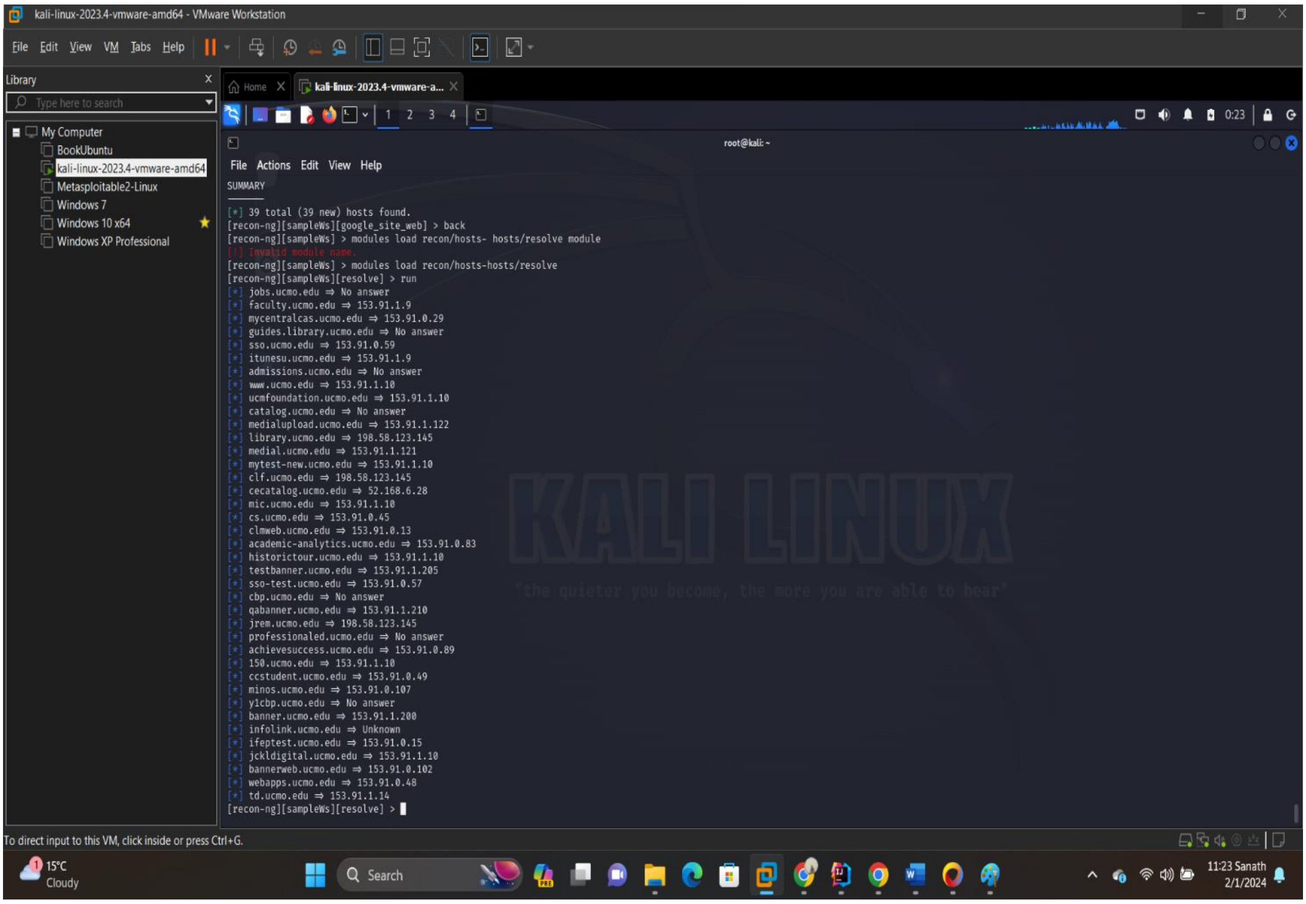
```
www.es-web.sophos.com.edgesuite.net
www.forefrontdl.microsoft.com
www.guru.avg.com
www.liveupdate.symantec.com
www.liveupdate.symantecliveupdate.com
www.osce8-p.activeupdate.trendmicro.com
www.update.nai.com
www.update.symantec.com
[recon-ng][sampleWs][cache_snoop] > db insert companies
company (TEXT): ucm
description (TEXT): sample
notes (TEXT): sample
[*] 1 rows affected.
[recon-ng][sampleWs][cache_snoop] > back
[recon-ng][sampleWs] > show companies

  +--------------------------------------------------------+
  | rowid | company | description | notes  |    module     |
  +--------------------------------------------------------+
  | 1     | ucm     | sample      | sample | user_defined  |
  +--------------------------------------------------------+

[*] 1 rows returned
[recon-ng][sampleWs] > db insert domains
domain (TEXT): ucmo.edu
notes (TEXT):
[*] 1 rows affected.
[recon-ng][sampleWs] > modules load recon/domains-hosts/google_site_web
[recon-ng][sampleWs][google_site_web] > run

--------
UCMO.EDU
--------
[*] Searching Google for: site:ucmo.edu
[!] Google CAPTCHA triggered. No bypass available.
[recon-ng][sampleWs][google_site_web] > run

--------
UCMO.EDU
--------
[*] Searching Google for: site:ucmo.edu
[*] Country: None
[*] Host: jobs.ucmo.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
0:25
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
15°C
Cloudy
Search
11:25 Sanath
2/1/2024

```
  +-----------------------------------------------------+
  | rowid | company | description | notes |    module    |
  +-----------------------------------------------------+
  | 1     | ucm     | sample      | sample | user_defined |
  +-----------------------------------------------------+

[*] 1 rows returned
[recon-ng][sampleWs] > db insert domains
domain (TEXT): ucmo.edu
notes (TEXT):
[*] 1 rows affected.
[recon-ng][sampleWs] > modules load recon/domains-hosts/google_site_web
[recon-ng][sampleWs][google_site_web] > run

--------
UCMO.EDU
--------
[*] Searching Google for: site:ucmo.edu
[!] Google CAPTCHA triggered. No bypass available.
[recon-ng][sampleWs][google_site_web] > run

--------
UCMO.EDU
--------
[*] Searching Google for: site:ucmo.edu
[*] Country: None
[*] Host: jobs.ucmo.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: faculty.ucmo.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: mycentralcas.ucmo.edu
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```


kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
1 2 3 4
0:21
root@kali: ~
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.
15°C
Cloudy
Search
11:21 Sanath
2/1/2024

```
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7201.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7301.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7401.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7501.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7601.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7701.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
[*] No New Subdomains Found on the Current Page. Jumping to Result 7801.
[*] Searching Google for: site:ucmo.edu -site:jobs.ucmo.edu -site:faculty.ucmo.edu -site:mycentralcas.ucmo.edu -site:guides.library.ucmo.edu -site:sso.ucmo.edu -site:itunesu.ucmo.edu -site:admissi
ons.ucmo.edu -site:www.ucmo.edu -site:ucmfoundation.ucmo.edu -site:catalog.ucmo.edu -site:medialupload.ucmo.edu -site:library.ucmo.edu -site:medial.ucmo.edu -site:mytest-new.ucmo.edu -site:clf.ucm
o.edu -site:cecatalog.ucmo.edu -site:mic.ucmo.edu -site:cs.ucmo.edu -site:clmweb.ucmo.edu -site:academic-analytics.ucmo.edu -site:historictour.ucmo.edu -site:testbanner.ucmo.edu -site:sso-test.ucm
o.edu -site:cbp.ucmo.edu -site:qabanner.ucmo.edu -site:jrem.ucmo.edu -site:professionaled.ucmo.edu -site:achievesuccess.ucmo.edu -site:150.ucmo.edu -site:ccstudent.ucmo.edu -site:minos.ucmo.edu -s
ite:y1cbp.ucmo.edu -site:banner.ucmo.edu -site:infolink.ucmo.edu -site:ifeptest.ucmo.edu -site:jckldigital.ucmo.edu -site:bannerweb.ucmo.edu -site:webapps.ucmo.edu -site:td.ucmo.edu
```



```
SUMMARY
[*] 39 total (39 new) hosts found.
[recon-ng][sampleWs][google_site_web] > back
[recon-ng][sampleWs] > modules load recon/hosts- hosts/resolve module
[!] Invalid module name.
[recon-ng][sampleWs] > modules load recon/hosts-hosts/resolve
[recon-ng][sampleWs][resolve] > run
[*] jobs.ucmo.edu ⇒ No answer
[*] faculty.ucmo.edu ⇒ 153.91.1.9
[*] mycentralcas.ucmo.edu ⇒ 153.91.0.29
[*] guides.library.ucmo.edu ⇒ No answer
[*] sso.ucmo.edu ⇒ 153.91.0.59
[*] itunesu.ucmo.edu ⇒ 153.91.1.9
[*] admissions.ucmo.edu ⇒ No answer
[*] www.ucmo.edu ⇒ 153.91.1.10
[*] ucmfoundation.ucmo.edu ⇒ 153.91.1.10
[*] catalog.ucmo.edu ⇒ No answer
[*] medialupload.ucmo.edu ⇒ 153.91.1.122
[*] library.ucmo.edu ⇒ 198.58.123.145
[*] medial.ucmo.edu ⇒ 153.91.1.121
[*] mytest-new.ucmo.edu ⇒ 153.91.1.10
[*] clf.ucmo.edu ⇒ 198.58.123.145
[*] cecatalog.ucmo.edu ⇒ 52.168.6.28
[*] mic.ucmo.edu ⇒ 153.91.1.10
[*] cs.ucmo.edu ⇒ 153.91.0.45
[*] clmweb.ucmo.edu ⇒ 153.91.0.13
[*] academic-analytics.ucmo.edu ⇒ 153.91.0.83
[*] historictour.ucmo.edu ⇒ 153.91.1.10
[*] testbanner.ucmo.edu ⇒ 153.91.1.205
[*] sso-test.ucmo.edu ⇒ 153.91.0.57
[*] cbp.ucmo.edu ⇒ No answer
[*] qabanner.ucmo.edu ⇒ 153.91.1.210
[*] jrem.ucmo.edu ⇒ 198.58.123.145
[*] professionaled.ucmo.edu ⇒ No answer
[*] achievesuccess.ucmo.edu ⇒ 153.91.0.89
[*] 150.ucmo.edu ⇒ 153.91.1.10
[*] ccstudent.ucmo.edu ⇒ 153.91.0.49
[*] minos.ucmo.edu ⇒ 153.91.0.107
[*] y1cbp.ucmo.edu ⇒ No answer
[*] banner.ucmo.edu ⇒ 153.91.1.200
[*] infolink.ucmo.edu ⇒ Unknown
[*] ifeptest.ucmo.edu ⇒ 153.91.0.15
[*] jckldigital.ucmo.edu ⇒ 153.91.1.10
[*] bannerweb.ucmo.edu ⇒ 153.91.0.102
[*] webapps.ucmo.edu ⇒ 153.91.0.48
[*] td.ucmo.edu ⇒ 153.91.1.14
[recon-ng][sampleWs][resolve] >
```

kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
15°C
Cloudy
Search
11:23 Sanath
2/1/2024

4. Run the recon/domains-hosts/bing_domain_web to against a domain of your choice. Provide a screenshot of the module output.

   In this we will be using the recon/domains-hosts/bing_domain_web module to see all the hosts of a particular domain, here I am using tesla.com and following screenshot is having all the subdomains.

   a) recon-ng][sampleWS] > modules load recon/domains-hosts/bing_domain_web

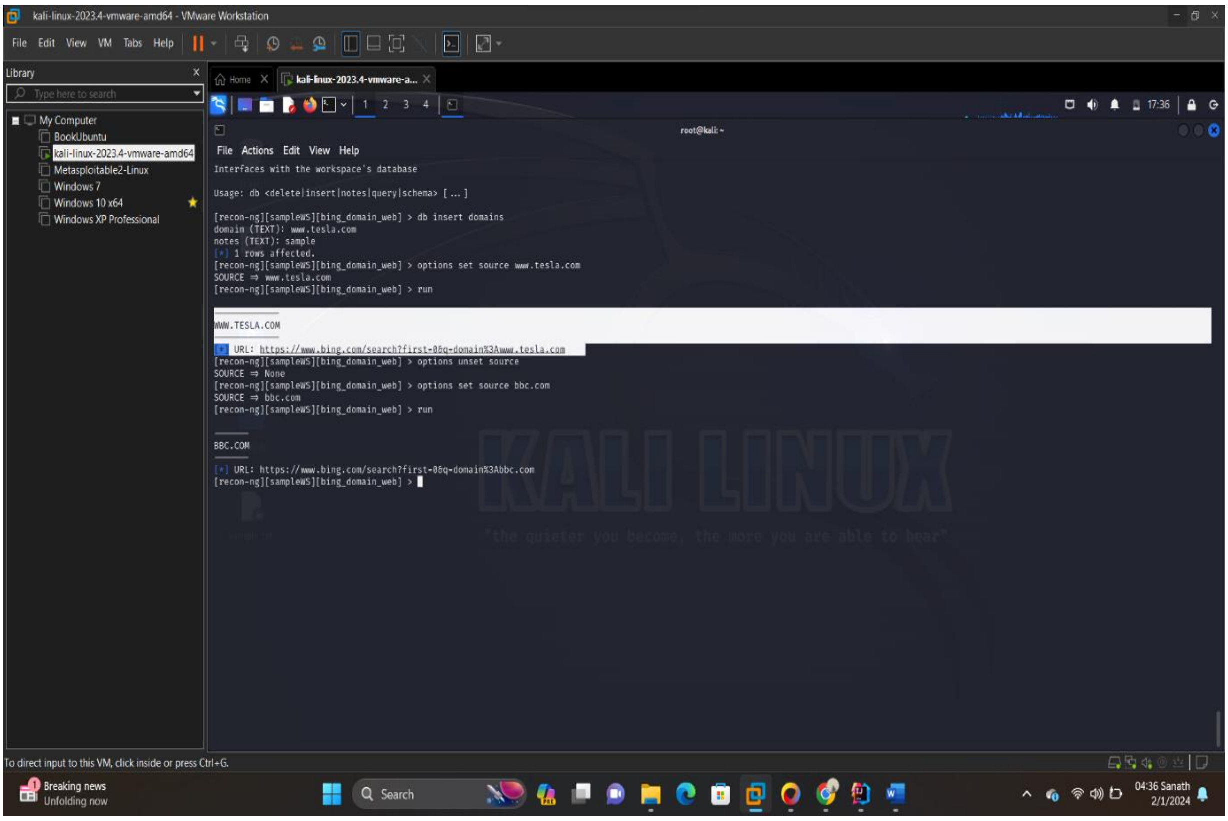
   b) [recon-ng][sampleWS][bing_domain_web] > db insert domains

   domain (TEXT): www.tesla.com

notes (TEXT): sample

[recon-ng][sampleWS][bing_domain_web] > options set source www.tesla.com

[recon-ng][sampleWS][bing_domain_web] > run



kali-linux-2023.4-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
BookUbuntu
kali-linux-2023.4-vmware-amd64
Metasploitable2-Linux
Windows 7
Windows 10 x64
Windows XP Professional
Home
kali-linux-2023.4-vmware-a...
root@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, click inside or press Ctrl+G.
Breaking news
Unfolding now
Search
17:36
04:36 Sanath
2/1/2024

```
Interfaces with the workspace's database

Usage: db <delete|insert|notes|query|schema> [ ... ]

[recon-ng][sampleWS][bing_domain_web] > db insert domains
domain (TEXT): www.tesla.com
notes (TEXT): sample
[*] 1 rows affected.
[recon-ng][sampleWS][bing_domain_web] > options set source www.tesla.com
SOURCE ⇒ www.tesla.com
[recon-ng][sampleWS][bing_domain_web] > run

-------------
WWW.TESLA.COM
-------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awww.tesla.com
[recon-ng][sampleWS][bing_domain_web] > options unset source
SOURCE ⇒ None
[recon-ng][sampleWS][bing_domain_web] > options set source bbc.com
SOURCE ⇒ bbc.com
[recon-ng][sampleWS][bing_domain_web] > run

-------
BBC.COM
-------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Abbc.com
[recon-ng][sampleWS][bing_domain_web] >
```