Lab 02: Infrastructure Recon

Table of Contents

Lab 02: Infrastructure Recon 1

Goals 1

Requirements 1

1. Identify the target's domain names 1

2. Enumerate subdomains of the discovered domains 10

3. Resolve the IP addresses of the discovered domains and subdomains 13

4. Use the resolved IP addresses to identify netblocks 16

Additional resources 19

Goals

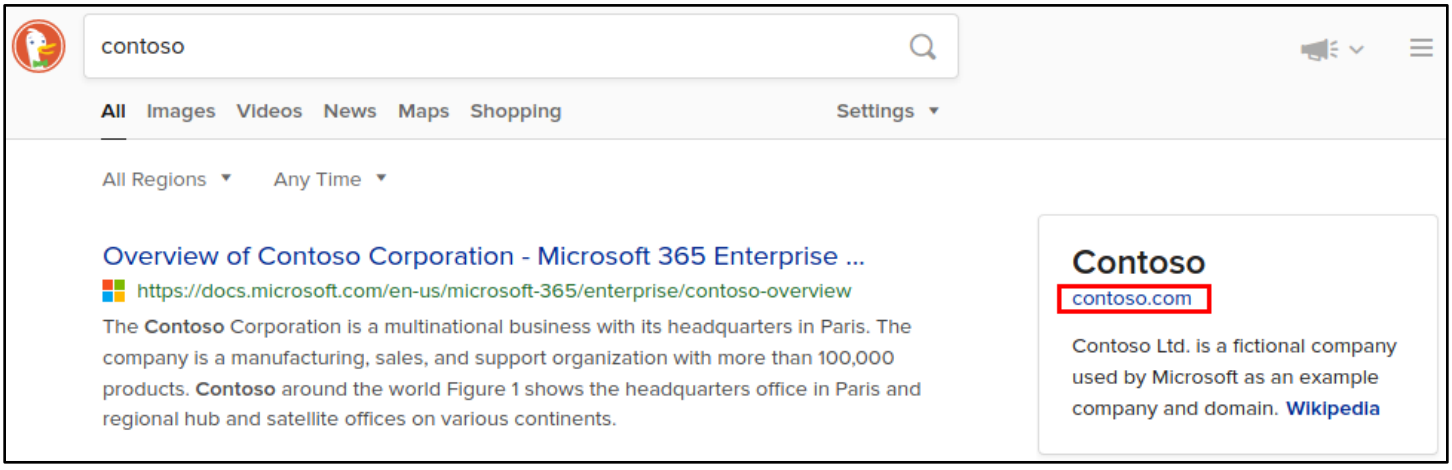
- Identify domains, subdomains, IP addresses, and netblocks owned by an organization.

Requirements

- Kali Linux VM with Internet access.
- An organization to target for reconnaissance.

1. Identify the target's domain names

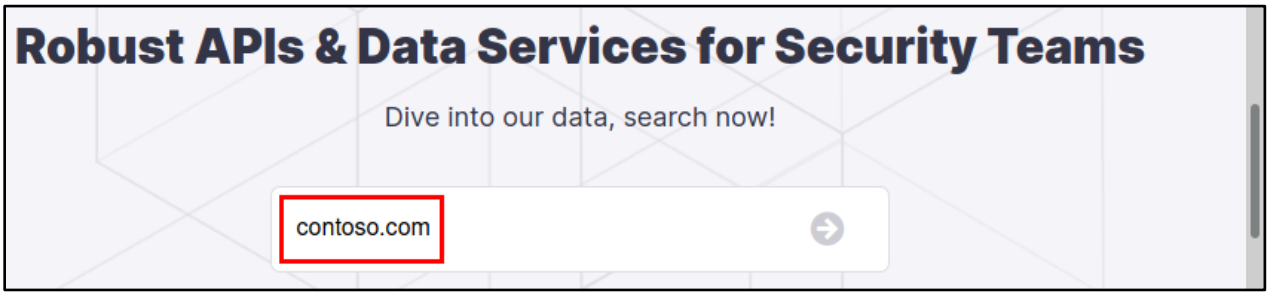
1. If you don't already know the primary domain name of your target organization, use a search engine like DuckDuckGo or Google to search for the company name and find their domain.



DuckDuckGo Search for Contoso

2. After you have the organization's domain name, visit the SecurityTrails website at the URL below. Scroll down to the search box on the homepage and use it to search for the domain name owned by your target organization.

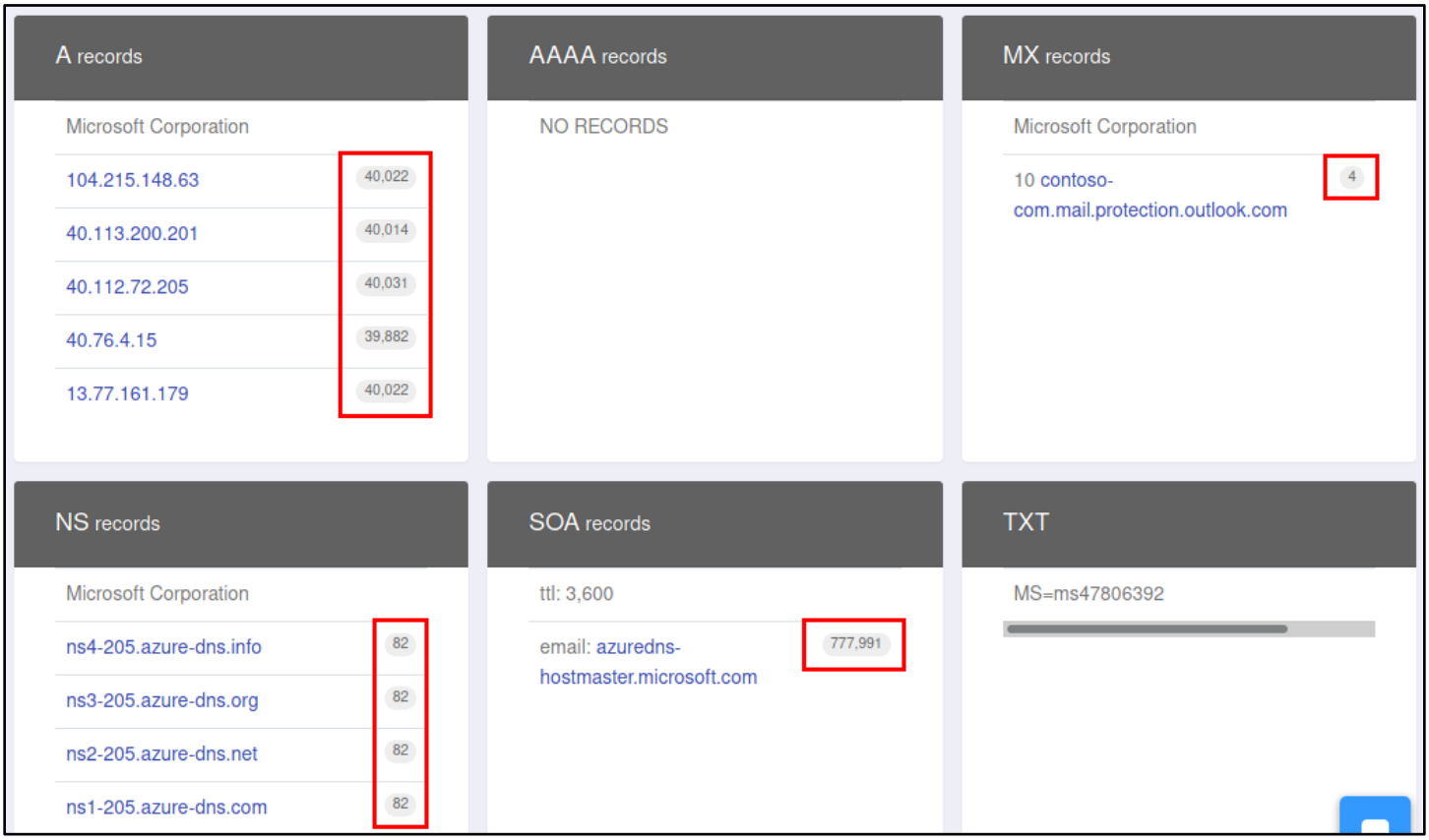
```
https://www.SecurityTrails.com
```



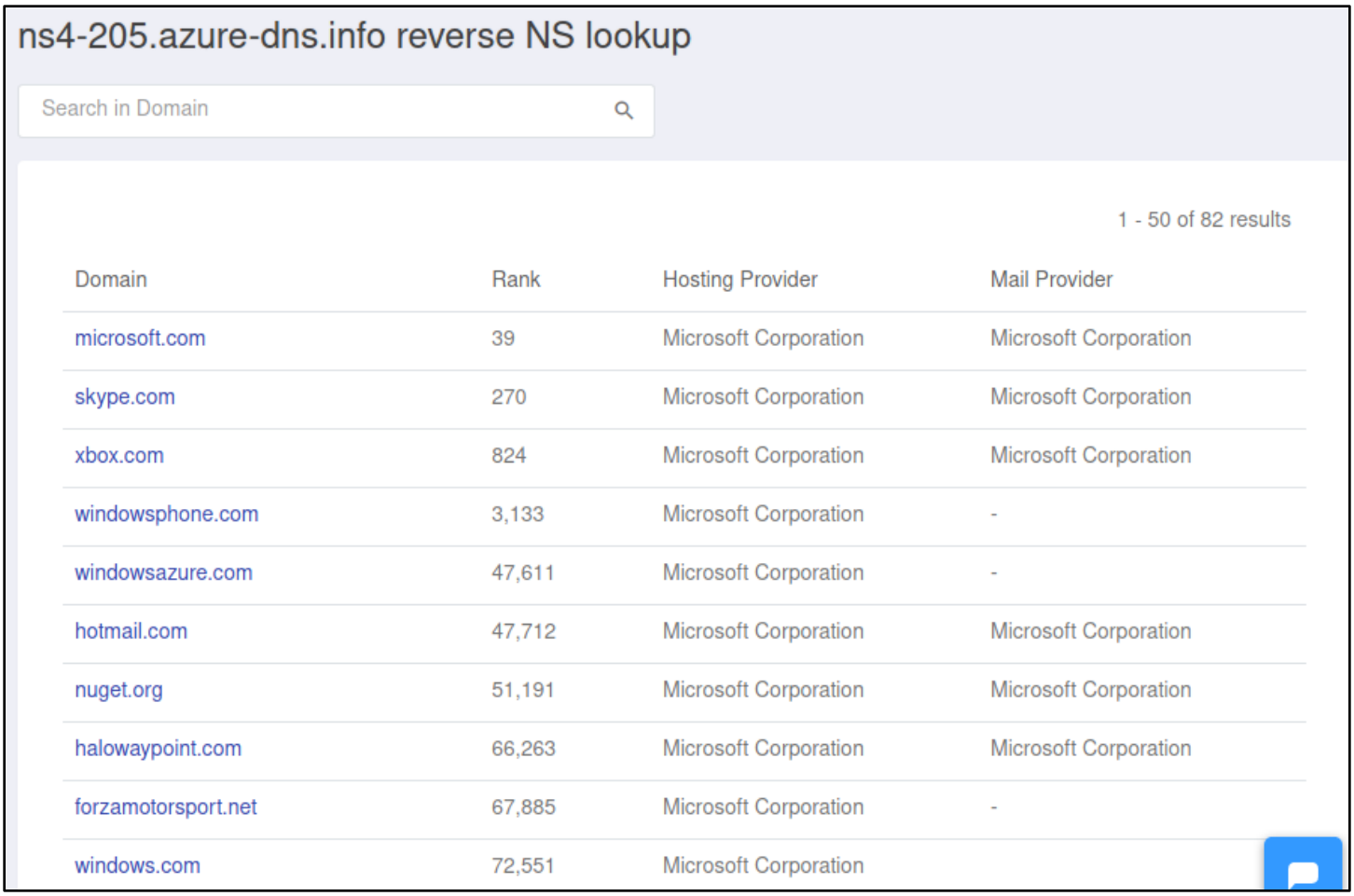
SecurityTrails Search for Contoso.com

3. The number on the right side of each SecurityTrails search result indicates how many other DNS records SecurityTrails identified that contain identical information. This may be an indicator that other domains with matching details are owned by the same organization - especially for record types where relatively few results are found (like the MX records and NS records in the screenshot below), or for records that point to resources that are unlikely to be shared with other organizations. For example, the value in the MX records shown below appears to be specifically created for the contoso.com domain since it contains "contoso-com".

   Click on each SecurityTrails result for your target domain and observe which results appear to contain additional domains belonging to your target organization.

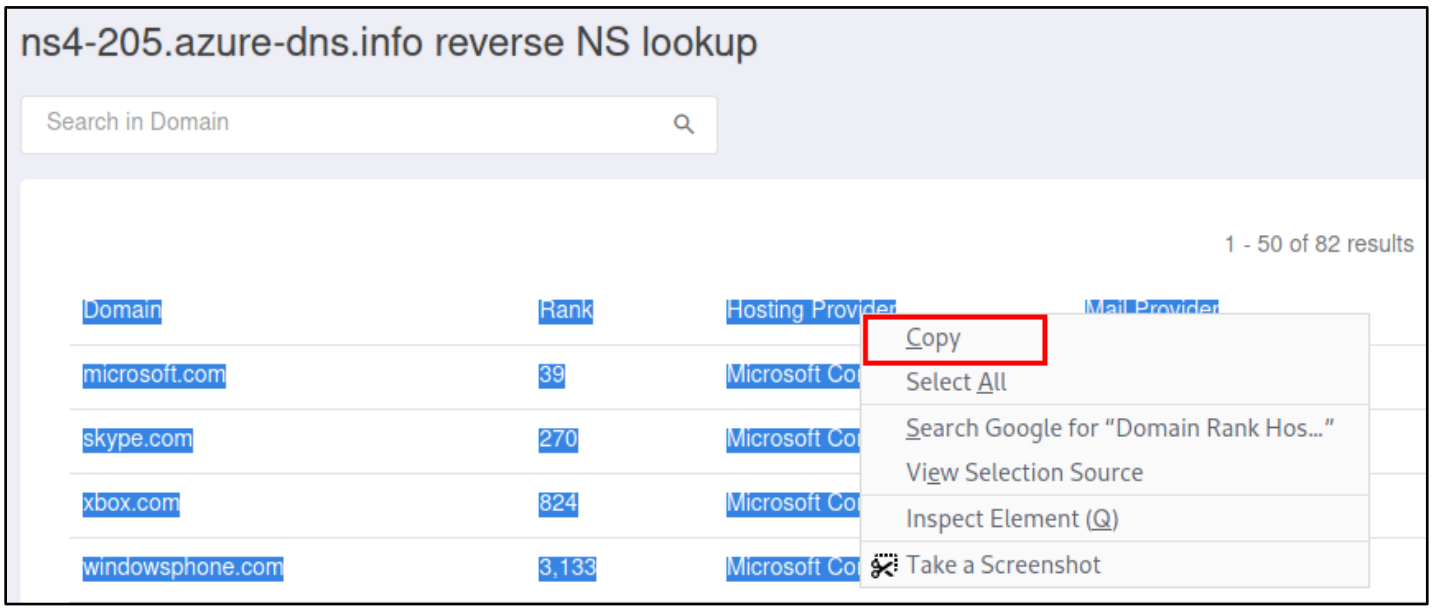


Partial SecurityTrails for Contoso.com

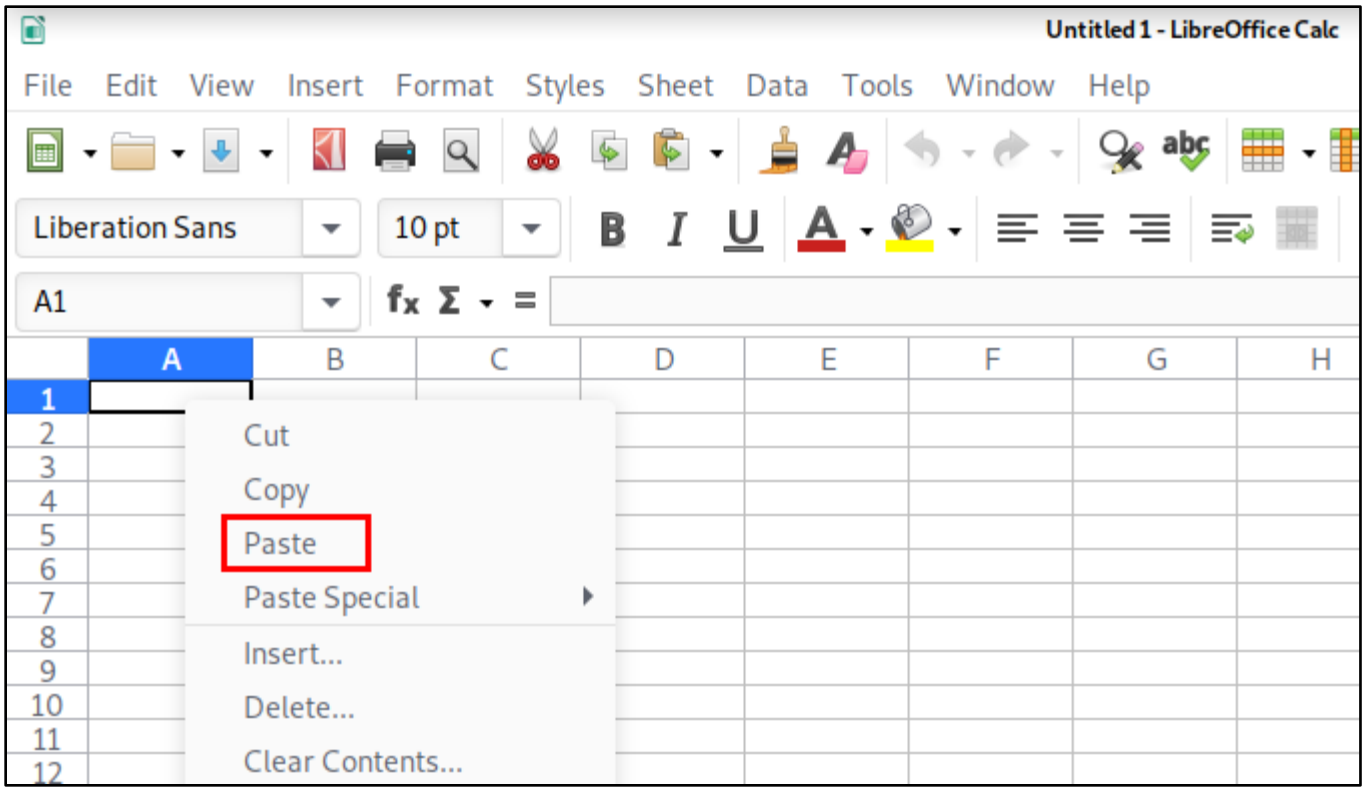


NS Records Reveal Several Other Domains Owned by the Same Organization

4. Open LibreOffice Calc in your Kali applications menu, and copy and paste the domains that appear to be owned by your target organization into a new spreadsheet.



Copying SecurityTrails Search Results



Pasting Data into LibreOffice Calc

J8

	A	B	C	D
1	**Domain**	**Rank**	**Hosting Provider**	**Mail Provider**
2	microsoft.com	39	Microsoft Corporation	Microsoft Corporation
3	skype.com	270	Microsoft Corporation	Microsoft Corporation
4	xbox.com	824	Microsoft Corporation	Microsoft Corporation
5	windowsphone.com	3133	Microsoft Corporation	-
6	windowsazure.com	47611	Microsoft Corporation	-
7	hotmail.com	47712	Microsoft Corporation	Microsoft Corporation
8	nuget.org	51191	Microsoft Corporation	Microsoft Corporation
9	halowaypoint.com	66263	Microsoft Corporation	Microsoft Corporation
10	forzamotorsport.net	67885	Microsoft Corporation	-
11	windows.com	72551	Microsoft Corporation	
12	zune.net	75605	Microsoft Corporation	Microsoft Corporation

Pasted Results Appear in the Spreadsheet

5. In addition to cross-referencing DNS records with other domains, you can also use reverse WHOIS services to cross-reference domain registration information. To retrieve the domain registration records for your target domain, open a Terminal window on your Kali VM, and use the "whois" command with your target domain as shown below. Remember to replace "contoso.com" with the domain you are targeting.

```
whois contoso.com
```

```
┌──(kali㉿kali)-[~]
└─$ whois contoso.com
   Domain Name: CONTOSO.COM
   Registry Domain ID: 1891582_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2020-07-30T09:31:06Z
   Creation Date: 1998-09-01T04:00:00Z
   Registry Expiry Date: 2021-08-31T04:00:00Z
```

WHOIS Query of Contoso.com

6. Scroll through the WHOIS output and find the Registrant Email for the target domain.

```
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: domains@microsoft.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
```

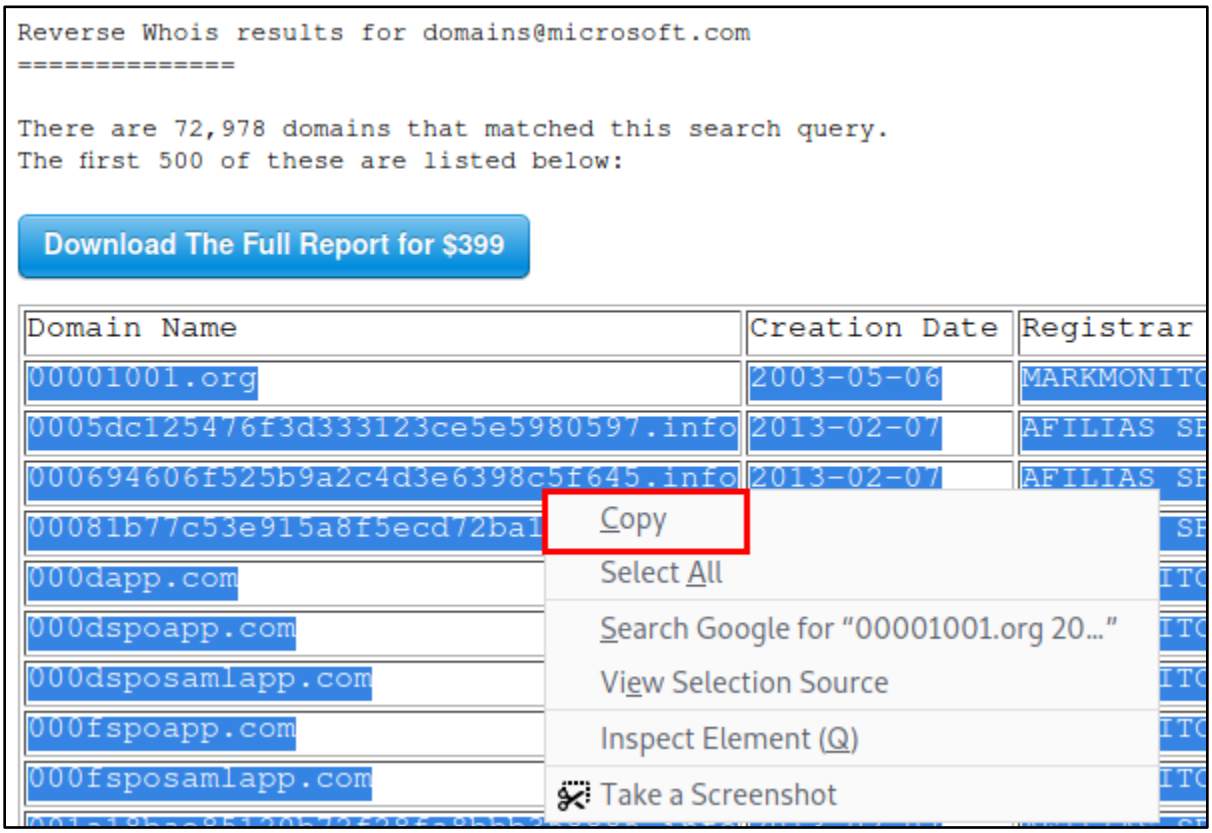
Registrant Email Address of Contoso.com

7. In your web browser, visit the free Reverse WHOIS Lookup tool at the URL below, and use it to search for other domains registered to the same Registrant Email.

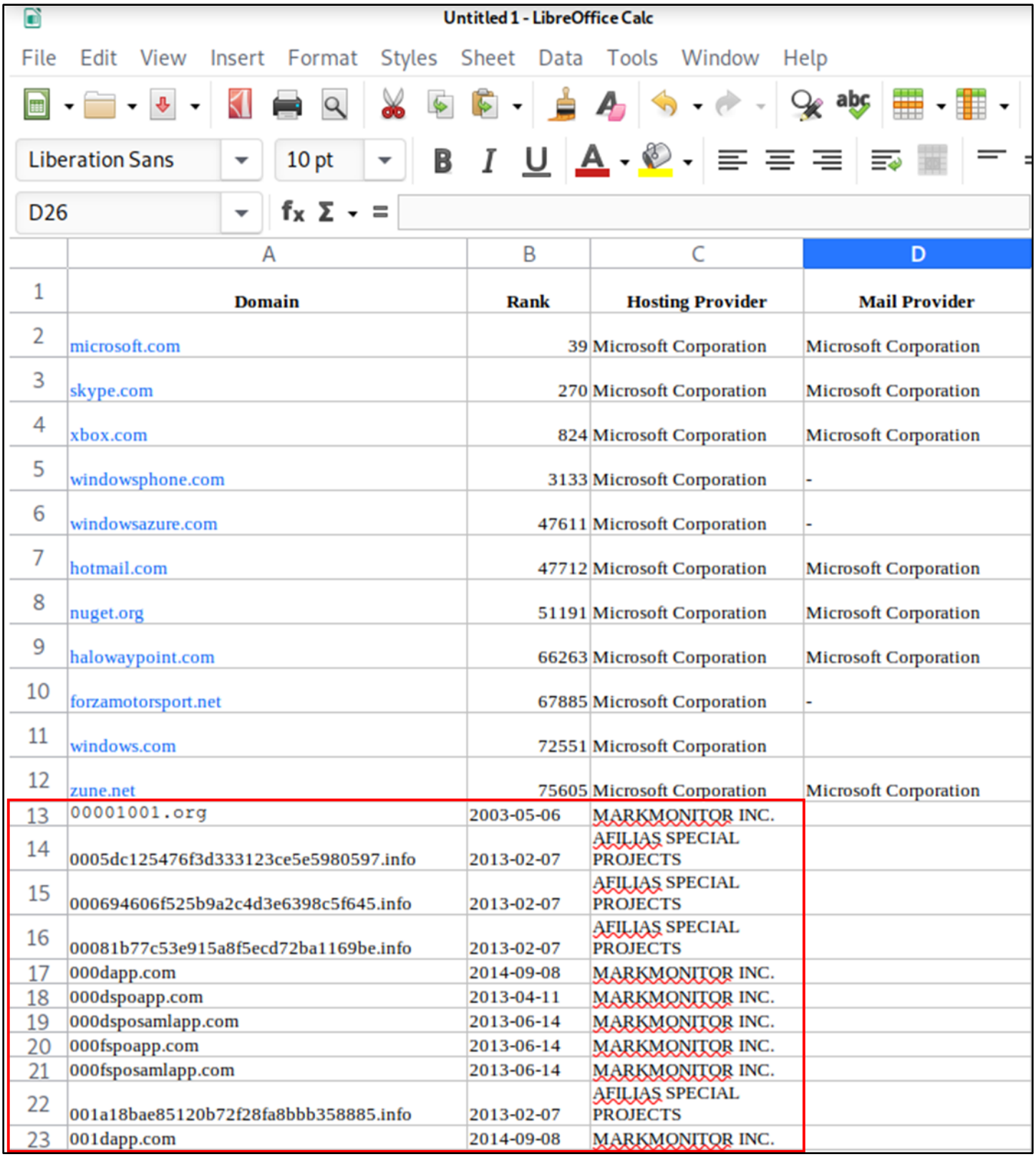
```
https://viewdns.info/reversewhois/
```

Searching Reverse WHOIS Data for the Contoso.com Registrant Email Address

8. Examine the reverse WHOIS results and copy and paste the relevant domains into the same spreadsheet where you pasted your data from SecurityTrails.



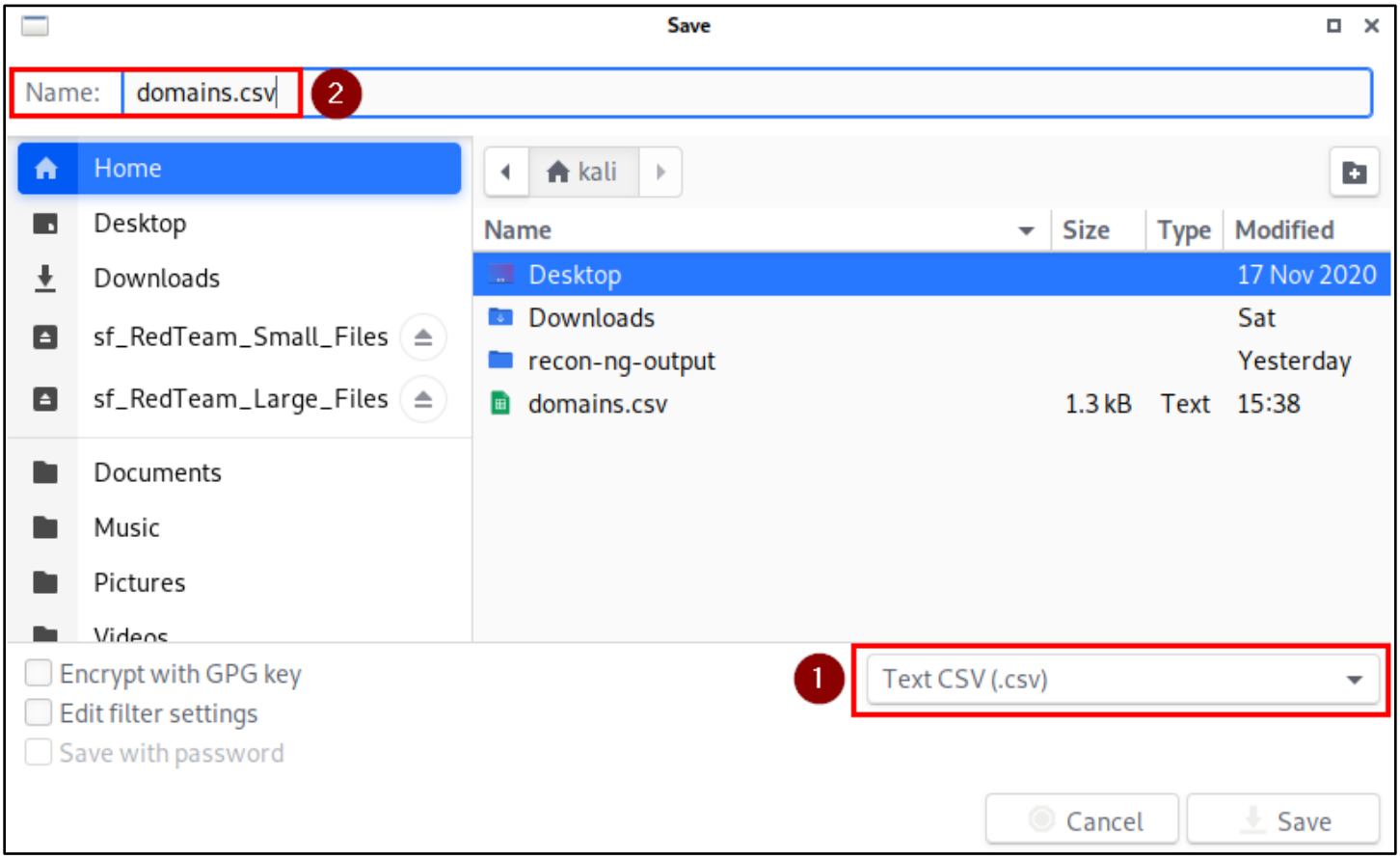
Copying Relevant Reverse WHOIS Search Results



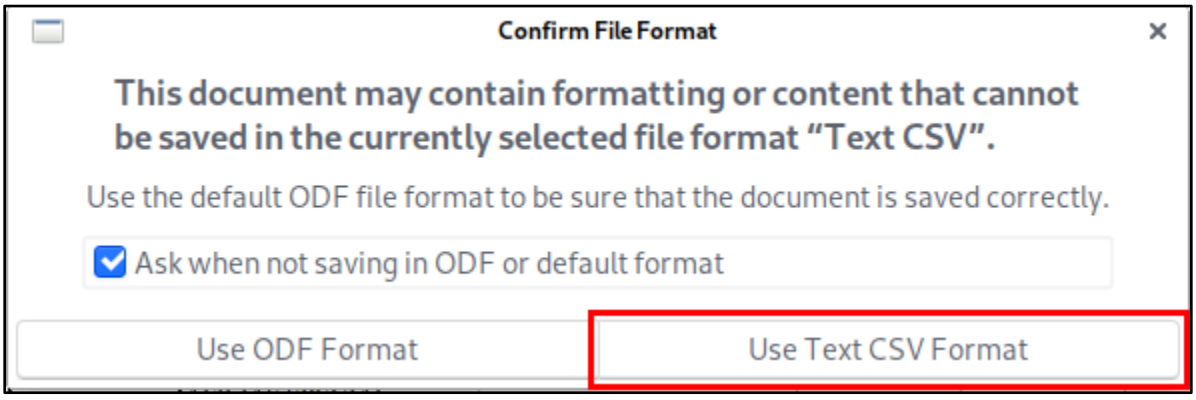
	A	B	C	D
1	**Domain**	**Rank**	**Hosting Provider**	**Mail Provider**
2	microsoft.com	39	Microsoft Corporation	Microsoft Corporation
3	skype.com	270	Microsoft Corporation	Microsoft Corporation
4	xbox.com	824	Microsoft Corporation	Microsoft Corporation
5	windowsphone.com	3133	Microsoft Corporation	-
6	windowsazure.com	47611	Microsoft Corporation	-
7	hotmail.com	47712	Microsoft Corporation	Microsoft Corporation
8	nuget.org	51191	Microsoft Corporation	Microsoft Corporation
9	halowaypoint.com	66263	Microsoft Corporation	Microsoft Corporation
10	forzamotorsport.net	67885	Microsoft Corporation	-
11	windows.com	72551	Microsoft Corporation	
12	zune.net	75605	Microsoft Corporation	Microsoft Corporation
13	00001001.org	2003-05-06	MARKMONITOR INC.	
14	0005dc125476f3d333123ce5e5980597.info	2013-02-07	AFILIAS SPECIAL PROJECTS	
15	000694606f525b9a2c4d3e6398c5f645.info	2013-02-07	AFILIAS SPECIAL PROJECTS	
16	00081b77c53e915a8f5ecd72ba1169be.info	2013-02-07	AFILIAS SPECIAL PROJECTS	
17	000dapp.com	2014-09-08	MARKMONITOR INC.	
18	000dspoapp.com	2013-04-11	MARKMONITOR INC.	
19	000dsposamlapp.com	2013-06-14	MARKMONITOR INC.	
20	000fspoapp.com	2013-06-14	MARKMONITOR INC.	
21	000fsposamlapp.com	2013-06-14	MARKMONITOR INC.	
22	001a18bae85120b72f28fa8bbb358885.info	2013-02-07	AFILIAS SPECIAL PROJECTS	
23	001dapp.com	2014-09-08	MARKMONITOR INC.	

Reverse WHOIS Results Pasted Beneath Results Collected from SecurityTrails

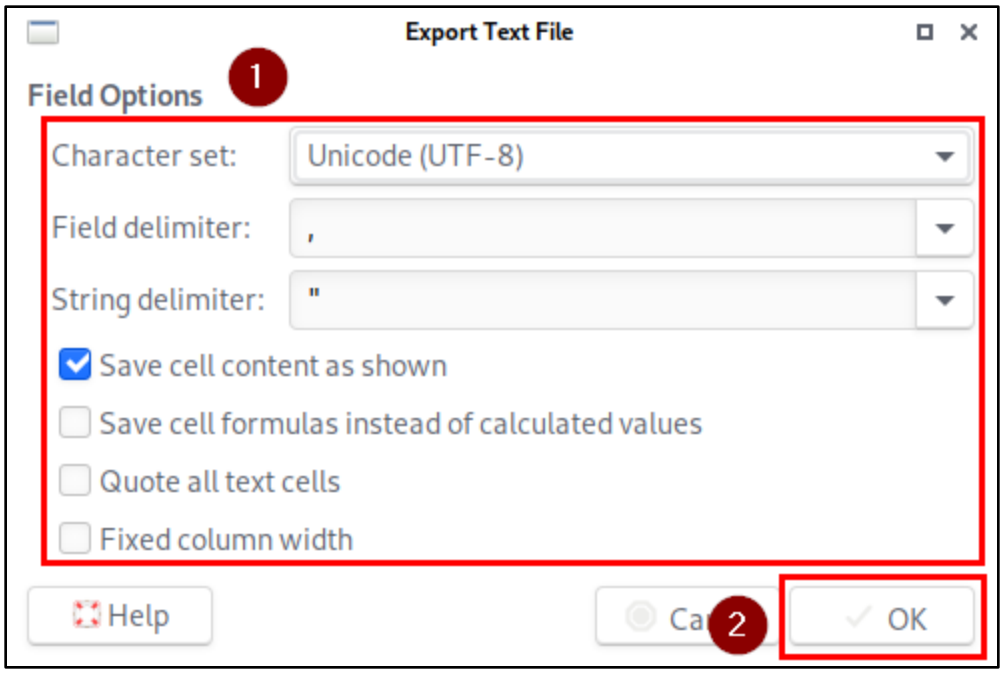
9. Make sure that all of the domain names you've collected appear in the first column (column A) of your spreadsheet. Then save the spreadsheet as "domains.csv" in your Kali user's home directory. Be sure to set the output format to "Text CSV (.csv)" as shown in the screenshot below. Then click the additional prompts to save in Text CSV format with default settings.



Selecting "Text CSV" Format and Saving as "domains.csv"



Confirming Use of the Text CSV Format



Default CSV Settings Accepted

10. To make generating a list of domains from your spreadsheet easier, a script named "clean-domains" has been included with your Kali VM.

    In a Terminal window, run the command below to extract the domain names from the CSV file you created and save them to a text file called "domains.clean.txt". This file will be used in the next section.

```
cat ~/domains.csv | clean-domains | tee ~/domains.clean.txt
```

```
┌──(kali㉿kali)-[~]
└─$ cat domains.csv | clean-domains | tee domains.clean.txt
00001001.org
0005dc125476f3d333123ce5e5980597.info
000694606f525b9a2c4d3e6398c5f645.info
00081b77c53e915a8f5ecd72ba1169be.info
000dapp.com
000dspoapp.com
000dsposamlapp.com
000fspoapp.com
000fsposamlapp.com
001a18bae85120b72f28fa8bbb358885.info
001dapp.com
001dspoapp.com
forzamotorsport.net
halowaypoint.com
hotmail.com
microsoft.com
```

Exporting Domains from the CSV File to "domains.clean.txt"

2. Enumerate subdomains of the discovered domains

1. In your terminal window, run "recon-ng" to start the Recon-NG tool.

```
recon-ng
```

Execution of recon-ng

2. At the [recon-ng] prompt, run the following commands to import your list of domain names into the "domains" table in Recon-NG.

```
modules load import/list

options set filename /home/kali/domains.clean.txt

options set table domains

options set column domain

run
```

```
[recon-ng][default][list] > modules load import/list
[recon-ng][default][list] > options set filename /home/kali/domains.clean.txt
FILENAME => /home/kali/domains.clean.txt
[recon-ng][default][list] > options set table domains
TABLE => domains
[recon-ng][default][list] > options set column domain
COLUMN => domain
[recon-ng][default][list] > run
[*] 00001001.org
[*] Domain: 00001001.org
```

Importing "domains.clean.txt" into Recon-NG

3. Running the command "show domains" will list all of the domains that were imported into Recon-NG.

```
show domains
```

```
[recon-ng][default][list] > show domains

  +-----------------------------------------------------------------+
  | rowid |                 domain                | notes | module |
  +-----------------------------------------------------------------+
  | 1     | 00001001.org                          |       | list   |
  | 2     | 0005dc125476f3d333123ce5e5980597.info |       | list   |
  | 3     | 000694606f525b9a2c4d3e6398c5f645.info |       | list   |
  | 4     | 00081b77c53e915a8f5ecd72ba1169be.info |       | list   |
  | 5     | 000dapp.com                           |       | list   |
  | 6     | 000dspoapp.com                        |       | list   |
  | 7     | 000dsposamlapp.com                    |       | list   |
  | 8     | 000fspoapp.com                        |       | list   |
  | 9     | 000fsposamlapp.com                    |       | list   |
  | 10    | 001a18bae85120b72f28fa8bbb358885.info |       | list   |
  | 11    | 001dapp.com                           |       | list   |
  | 12    | 001dspoapp.com                        |       | list   |
  | 13    | forzamotorsport.net                   |       | list   |
  | 14    | halowaypoint.com                      |       | list   |
  | 15    | hotmail.com                           |       | list   |
  | 16    | microsoft.com                         |       | list   |
  | 17    | nuget.org                             |       | list   |
  | 18    | skype.com                             |       | list   |
  | 19    | windowsazure.com                      |       | list   |
  | 20    | windows.com                           |       | list   |
  | 21    | windowsphone.com                      |       | list   |
  | 22    | xbox.com                              |       | list   |
  | 23    | zune.net                              |       | list   |
  +-----------------------------------------------------------------+
```

Imported Domain Names Displayed

4. Since domains can also point to individual hosts, you might also want to import your list of domains into the hosts table with the commands below.

```
modules load import/list

options set filename /home/kali/domains.clean.txt

options set table hosts

options set column host

run
```



```
[recon-ng][default][resolve] > modules load import/list
[recon-ng][default][list] > options set filename /home/kali/domains.clean.txt
FILENAME => /home/kali/domains.clean.txt
[recon-ng][default][list] > options set table hosts
TABLE => hosts
[recon-ng][default][list] > options set column host
COLUMN => host
[recon-ng][default][list] > run
[*] 00001001.org
[*] Country: None
[*] Host: 00001001.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] 0005dc125476f3d333123ce5e5980597.info
[*] Country: None
[*] Host: 0005dc125476f3d333123ce5e5980597.info
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

Domain Names Imported into Recon-NG's Hosts Table

5. Run the next set of commands to search the certificate transparency logs at CRT.sh for SSL/TLS certificates that have been issued to hosts within each domain. Discovered host/subdomain names will automatically be imported into the hosts table in Recon-NG as they are discovered.

```
modules load recon/domains-hosts/certificate_transparency

run
```

```
[recon-ng][default][certificate_transparency] > modules load recon/domains-hosts/certificate_transparency
[recon-ng][default][certificate_transparency] > run

-----------
00001001.ORG
-----------

-----------------------------------
0005DC125476F3D333123CE5E5980597.INFO
-----------------------------------

-----------------------------------
000694606F525B9A2C4D3E6398C5F645.INFO
-----------------------------------
```

Searching Certificate Transparency Logs for Discovered Domain Names

6. To view the list of hosts discovered by the previous commands, run "show hosts" in recon-ng.

```
show hosts
```

```
[recon-ng][default][certificate_transparency] > show hosts

  +-------------------------------------------------------------
  | rowid |                          host
  +-------------------------------------------------------------
  | 1     | *.001dspoapp.com
  | 2     | *.fm7.forzamotorsport.net
  | 3     | *.fh4.forzamotorsport.net
  | 4     | *.fh3.forzamotorsport.net
  | 5     | *.forzamotorsport.net
  | 6     | forzamotorsport.net
  | 7     | gameservices.forza5.forzamotorsport.net
  | 8     | *.preview.forzamotorsport.net
  | 9     | preview.forzamotorsport.net
  | 10    | support.forzamotorsport.net
  | 11    | *.staging.forzamotorsport.net
  | 12    | service.horizon.forzamotorsport.net
  | 13    | *.fm6.forzamotorsport.net
  | 14    | *.apex.forzamotorsport.net
  | 15    | service.fh2360.forzamotorsport.net
```

Hostnames Discovered in Certificate Transparency Logs Displayed

3. Resolve the IP addresses of the discovered domains and subdomains

1. In the previous step, you might have noticed that some of the host/subdomain names discovered contained asterisks (*). This is because a wildcard SSL/TLS certificate issued for that domain and was found in the results from CRT.sh. Hostnames containing asterisks aren't always resolved correctly, so a Recon-NG script has been included with your Kali VM to help resolve this issue.

   Run the following command to execute the "fix_hosts" script and add additional entries to your hosts table with the asterisks removed.

```
script execute /opt/recon_scripts/fix_hosts
```



```
[recon-ng][default][list] > script execute /opt/recon_scripts/fix_hosts
[recon-ng][default][list] > shell mkdir /tmp/recon-ng
[*] Command: mkdir /tmp/recon-ng
mkdir: cannot create directory '/tmp/recon-ng': File exists
[recon-ng][default][list] >
[recon-ng][default][list] > modules load reporting/list
[recon-ng][default] > modules load reporting/list
[recon-ng][default][list] > options set filename /tmp/recon-ng/hosts
FILENAME => /tmp/recon-ng/hosts
[recon-ng][default][list] > options set table hosts
TABLE => hosts
[recon-ng][default][list] > options set column host
COLUMN => host
[recon-ng][default][list] > run
*.001dspoapp.com
*.admin.halowaypoint.com
*.admin.test.halowaypoint.com
*.apex.forzamotorsport.net
*.cert.halowaypoint.com
*.dev.forzamotorsport.net
*.dev.services.forzamotorsport.net
```

Execution of the "fix_hosts" Script in Recon-NG

2. Now use Recon-NG's "resolve" module to resolve the IP address of each host present in your hosts table.

```
modules load recon/hosts-hosts/resolve

run
```

```
[recon-ng][default][list] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > run
[*] *.001dspoapp.com => DNS Error
[*] *.fm7.forzamotorsport.net => Unknown
[*] *.fh4.forzamotorsport.net => Unknown
[*] *.fh3.forzamotorsport.net => Unknown
[*] *.forzamotorsport.net => Unknown
[*] forzamotorsport.net => 40.84.59.174
[*] gameservices.forza5.forzamotorsport.net => 104.208.160.155
[*] *.preview.forzamotorsport.net => Unknown
[*] preview.forzamotorsport.net => 40.70.147.9
[*] support.forzamotorsport.net => 104.16.53.111
[*] support.forzamotorsport.net => 104.16.51.111
[*] *.staging.forzamotorsport.net => Unknown
[*] service.horizon.forzamotorsport.net => 13.68.16.25
[*] *.fm6.forzamotorsport.net => Unknown
[*] *.apex.forzamotorsport.net => Unknown
```

Resolving Hostnames to IP Addresses

3. You can now view the IP address of all resolved domain and subdomain names with the "show hosts" command.

```
show hosts
```

```
[recon-ng][default][resolve] > show hosts

  +---------------------------------------------------------------------------------
  | rowid |                          host                          |    ip_address
  +---------------------------------------------------------------------------------
  | 1     | *.001dspoapp.com                                       |
  | 2     | *.fm7.forzamotorsport.net                              |
  | 3     | *.fh4.forzamotorsport.net                              |
  | 4     | *.fh3.forzamotorsport.net                              |
  | 5     | *.forzamotorsport.net                                  |
  | 6     | forzamotorsport.net                                    | 40.84.59.174
  | 7     | gameservices.forza5.forzamotorsport.net                | 104.208.160.155
  | 8     | *.preview.forzamotorsport.net                          |
  | 9     | preview.forzamotorsport.net                            | 40.70.147.9
  | 10    | support.forzamotorsport.net                            | 104.16.53.111
  | 11    | *.staging.forzamotorsport.net                          |
  | 12    | service.horizon.forzamotorsport.net                    | 13.68.16.25
  | 13    | *.fm6.forzamotorsport.net                              |
  | 14    | *.apex.forzamotorsport.net                             |
  | 15    | service.fh2360.forzamotorsport.net                     | 40.84.62.110
  | 16    | service.forza4.forzamotorsport.net                     | 13.68.75.123
  | 17    | service.forza5.forzamotorsport.net                     | 40.123.49.141
  | 18    | *.ff7.forzamotorsport.net                              |
  | 19    | *.fh2.forzamotorsport.net                              |
  | 20    | serverservices.forza5.forzamotorsport.net              | 40.79.81.15
  | 21    | service.ff7360.forzamotorsport.net                     | 13.68.27.161
  | 22    | *.staging.preview.forzamotorsport.net                  |
  | 23    | *.dev.forzamotorsport.net                              |
  | 24    | dev.forzamotorsport.net                                | 13.66.138.102
  | 25    | *.staging.dev.forzamotorsport.net                      |
  | 26    | *.services.forzamotorsport.net                         |
```

IP Addresses of Resolved Hostnames Displayed

4. Use the resolved IP addresses to identify netblocks

1. Run the following command to list all the IP addresses identified by Recon-NG and sort them alphabetically:

```
db query select distinct ip_address from hosts order by ip_address asc
```

```
[recon-ng][default][list] > db query select distinct ip_address from hosts order by ip_addr
ess asc

  +-----------------+
  |    ip_address   |
  +-----------------+
  |                 |
  | 104.16.51.111   |
  | 104.16.53.111   |
  | 104.208.160.155 |
  | 104.215.148.63  |
  | 104.40.50.126   |
  | 104.40.92.107   |
  | 13.107.246.13   |
  | 13.66.138.102   |
  | 13.66.244.249   |
  | 13.68.16.25     |
  | 13.68.27.161    |
  | 13.68.75.123    |
  | 13.77.161.179   |
  | 13.83.131.111   |
  | 13.91.40.166    |
  | 137.135.107.235 |
  | 152.195.19.97   |
  | 157.56.152.169  |
  | 157.56.152.170  |
  | 157.56.152.171  |
  | 157.56.152.210  |
  | 157.56.152.222  |
  | 199.2.137.139   |
  | 204.79.197.212  |
  | 23.101.125.65   |
  | 23.102.255.237  |
  | 23.96.1.109     |
  | 40.112.72.205   |
  | 40.113.200.201  |
  | 40.115.34.155   |
  | 40.121.80.200   |
  | 40.123.49.141   |
  | 40.67.136.136   |
  | 40.67.147.111   |
```

Unique IP Addresses Identified by Recon-NG Displayed

2. Copy one of the IP addresses from the list, and in a new terminal window, use the "whois" command to view registration information for the Netblock where the IP address is assigned. Remember to replace the red IP address in the command below with an IP address from your own list.

```
whois 104.208.160.155
```

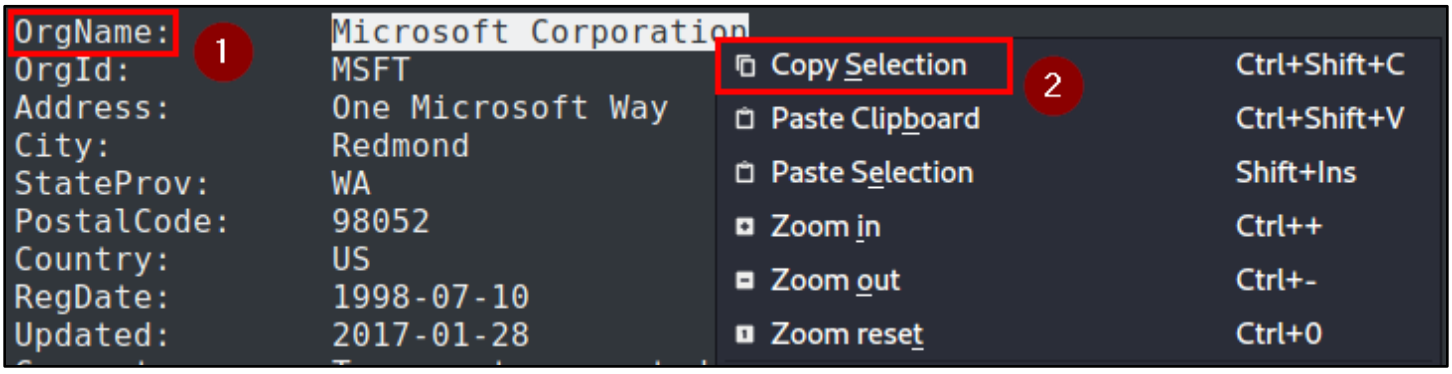
```
┌──(kali㉿kali)-[~]
└─$ whois 104.208.160.155

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       104.208.0.0 - 104.215.255.255
CIDR:           104.208.0.0/13
NetName:        MSFT
NetHandle:      NET-104-208-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS8075
Organization:   Microsoft Corporation (MSFT)
```

Registration Information for the Queried IP Address

3. If the Netblock is owned by your target organization, the organization name will appear in the output of the whois command. Try running the whois command on several IP addresses in your list until you find one whose Netblock is owned by your target. When you find one, copy the entire organization name displayed in the "OrgName" field to your clipboard, exactly as it appears in the whois output.



Copying the OrgName from "whois" Command Output

4. Back in the window where you are running Recon-NG, use the "db insert" command shown below to add the organization's name to your Recon-NG database. Also make sure to include two tilde (~) characters immediately following the company name.

```
db insert companies Microsoft Corporation~~
```

```
[recon-ng][default][whois_miner] > db insert companies Microsoft Corporation~~
[*] 1 rows affected.
[recon-ng][default][whois_miner] >
```

Organization Name Added to Recon-NG

5. Now use Recon-NG's "whois_miner" module to find additional netblocks that are registered to the same organization.

```
modules load recon/companies-multi/whois_miner

run
```

```
[recon-ng][default] > modules load recon/companies-multi/whois_miner
[recon-ng][default][whois_miner] > run
[*] URL: http://whois.arin.net/rest/orgs;name=Microsoft%20Corporation

---------------------
MICROSOFT CORPORATION
---------------------
[*] Company: MICROSOFT CORPORATION
[*] Description: org
[*] Notes: None
[*] ------------------------------------------------
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Street_Address: 7400 San Pedro Ave, San Antonio, TX 78216, United States
[*] ------------------------------------------------
[*] URL: http://whois.arin.net/rest/org/MC-1000/nets
[*] Netblock: 65.155.75.200/29
[*] Notes: None
```

Execution of the "whois_miner" Module

6. After execution completes, you can view the collected Netblocks with the following command:

```
show netblocks
```

```
[recon-ng][default][whois_miner] > show netblocks

  +-----------------------------------------------------------+
  | rowid |         netblock          | notes |    module    |
  +-----------------------------------------------------------+
  | 1     | 65.155.75.200/29          |       | whois_miner |
  | 2     | 65.125.19.224/29          |       | whois_miner |
  | 3     | 65.125.19.144/29          |       | whois_miner |
  | 4     | 209.211.188.88/29         |       | whois_miner |
  | 5     | 67.132.237.136/29         |       | whois_miner |
  | 6     | 67.132.237.144/29         |       | whois_miner |
  | 7     | 198.233.204.112/29        |       | whois_miner |
  | 8     | 198.233.245.32/29         |       | whois_miner |
  | 9     | 66.198.12.0/25            |       | whois_miner |
  | 10    | 2001:5a0:3c06::/48        |       | whois_miner |
  | 11    | 2001:1890:1c1e:c100::/56  |       | whois_miner |
  | 12    | 2001:1890:1c33:fa00::/56  |       | whois_miner |
  | 13    | 2001:1890:1c33:f900::/56  |       | whois_miner |
  | 14    | 2001:1890:1c1e:c200::/56  |       | whois_miner |
  | 15    | 2001:1890:1c1e:c300::/56  |       | whois_miner |
```

Netblocks Identified by "whois_miner"

Additional resources

- SecurityTrails
- ViewDNS.info Reverse WHOIS tool
- Recon-NG project on GitHub
- CRT.sh certificate transparency logs search tool

