

Subject: Security Testing

SENG 8061

ASSIGNMENT - 1

Name	Student ID
Shivani Varu	8941914
Mohammed Rafique	8954785

Tools Used	Recon-ng
Target Website	Microsoft.com
Command Used	Workspaces create Assignment1

```

[recon-ng][default] > workspaces create Assignment1
[!] 'twitter_api' key not set, twitter module will likely fail at runtime. See 'keys add'.
[!] 'twitter_secret' key not set, twitter module will likely fail at runtime. See 'keys add'.
[!] 'flickr_api' key not set, flickr module will likely fail at runtime. See 'keys add'.
[!] 'google_api' key not set, youtube module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set, shodan module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set, bing_linkedin module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/companies-contacts/censys_email_address' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'bing_api' key not set, bing_paste module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set, bing_breach module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/companies-hosts/censys_org' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'Module 'recon/companies-hosts/censys_tls_subjects' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'github_api' key not set, github_commits module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/domains-credentials/ownedlist/account_creds' disabled. Dependency required: ''pyaes''.
[!] 'Module 'recon/domains-credentials/ownedlist/domain_creds' disabled. Dependency required: ''pyaes''.
[!] 'ownedlist_apl' key not set, leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'ownedlist_secret' key not set, leaks_dump module will likely fail at runtime. See 'keys add'.
[!] 'ownedlist_apl' key not set, domain_isowned module will likely fail at runtime. See 'keys add'.
[!] 'ownedlist_secret' key not set, domain_isowned module will likely fail at runtime. See 'keys add'.
[!] 'ownedlist_apl' key not set, whois_usage module will likely fail at runtime. See 'keys add'.
[!] 'ownedlist_secret' key not set, apic_usage module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set, virustotal module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set, shodan_net module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/netblocks-hosts/censys_netblock' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'whoxy_api' key not set, whoxy_whois module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/domains-companies/censys_companies' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'censysio_id' key not set, censysio module will likely fail at runtime. See 'keys add'.
[!] 'censysio_secret' key not set, censysio module will likely fail at runtime. See 'keys add'.
[!] 'fullcontact_apl' key not set, fullcontact module will likely fail at runtime. See 'keys add'.
[!] 'hashes_apl' key not set, hashes_org module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set, bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set, github_users module will likely fail at runtime. See 'keys add'.
[!] 'virustotal_api' key not set, virustotal module will likely fail at runtime. See 'keys add'.
[!] 'ipstack_apl' key not set, ipstack module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/hosts-hosts/censys_query' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'Module 'recon/hosts-hosts/censys_ip' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'Module 'recon/hosts-hosts/censys_hostname' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.
[!] 'bing_apl' key not set, bing_lo module will likely fail at runtime. See 'keys add'.
[!] 'ipinfoapi_apl' key not set, ipinfofd module will likely fail at runtime. See 'keys add'.
[!] 'github_apl' key not set, github_miner module will likely fail at runtime. See 'keys add'.
[!] 'shodan_api' key not set, shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'github_apl' key not set, github_repos module will likely fail at runtime. See 'keys add'.
[!] 'hunter_lo' key not set, hunter_lo module will likely fail at runtime. See 'keys add'.
[!] 'Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: 'pyPDF2'.
[!] 'Module 'recon/netblocks-companies/censys_netblock_company' disabled. Dependency required: 'me 'CensysIPV4' from 'censys.search' (/usr/lib/python3/dist-packages/censys/search/_init__.py)'.

```

Modules Used	modules load recon/domains-contacts/whois_pocs
Command Used	Show Contacts

- The "modules load/recon/domains-contacts/whois_pocs" command in Recon-ng is used to load the "whois_pocs" module from the "domains-contacts" category.
- This module is designed to gather and display the Point of Contacts (POCs) obtained from Whois records for a given domain.
- Recon-ng, being a modular framework, allows users to load specific modules for different purposes, such as information gathering, and the "whois_pocs" module is one of the many modules available in Recon-ng for this purpose.
- The tool provides a variety of modules, including geoip lookup, banner grabbing, DNS lookup, and port scanning, making it a powerful asset for reconnaissance and open source intelligence gathering

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shivanivar@shivanivar: ~
File Actions Edit View Help
+----+-----+-----+-----+-----+-----+
| recon/profiles-repositories/github_repos | 0.1 | installed | 2020-05-15 | | * |
| recon/repositories-profiles/github_commits | 1.0 | installed | 2019-06-24 | | * |
| recon/repositories-vulnerabilities/gists_search | 1.0 | installed | 2019-06-24 | | * |
| recon/repositories-vulnerabilities/github_dorks | 1.0 | installed | 2019-06-24 | | * |
| reporting/csv | 1.0 | installed | 2019-06-24 | | |
| reporting/html | 1.0 | installed | 2019-06-24 | | |
| reporting/json | 1.0 | installed | 2019-06-24 | | |
| reporting/list | 1.0 | installed | 2019-06-24 | | |
| reporting/proxifier | 1.0 | installed | 2019-06-24 | | |
| reporting/pushpin | 1.0 | installed | 2019-06-24 | | * |
| reporting/xlsx | 1.0 | installed | 2019-06-24 | | |
| reporting/xml | 1.1 | installed | 2019-06-24 | | |
+----+-----+-----+-----+-----+-----+
D - Has dependencies. See info for details. They have all moved to the marketplace. So you have to manually install them.
K - Requires keys. See info for details.

[recon-ng][Assignment1] > module load recon/domains-contacts/whois_pocs
[recon-ng][Assignment1] > modules load recon/domains-contacts/whois_pocs
[recon-ng][Assignment1][whois_pocs] > info
  Name: Whois POC Harvester
  Author: Tim Tomes (@lanmaster53)
  Version: 1.0
  Description: This module would guess what modules you are trying to use, depending on the ultimate response you may want to check your firewall logs. I just ran
    Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the
    'contacts' table with the results.
  Options:
  +----+-----+-----+-----+
  | Name | Current Value | Required | Description |
  +----+-----+-----+-----+
  | SOURCE | default | yes | source of input (see 'info' for details) |
  +----+-----+-----+-----+
  Source Options:
  default <string> SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string> string representing a single input
  <path> path to a file containing a list of inputs
  query <sql> database query returning one column of inputs
[recon-ng][Assignment1][whois_pocs] > options unset SOURCE
SOURCE => None
[recon-ng][Assignment1][whois_pocs] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][Assignment1][whois_pocs] >
```

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 | 20:51 | 
File Kali Linux Modules are completely up-to-date
shivanivar@shivanivar: ~
[recon-ng][Assignment1][whois_pocs] > options unset SOURCE
SOURCE => None
[recon-ng][Assignment1][whois_pocs] > options set SOURCE microsoft.com
SOURCE => microsoft.com
[recon-ng][Assignment1][whois_pocs] > info
Name: Whois POC Harvester
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain. Updates the 'contacts' table with the results.

Options: So there are no modules installed because they have all moved to the marketplace. So you have to manually install them. Just
Name Current Value Required Description
SOURCE microsoft.com yes source of input (see 'info' for details)
marketplace shell_all

Source Options:
default SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string> string representing a single input
<path> absolute path to a file containing a list of inputs
query <sql> database query returning one column of inputs
[recon-ng][Assignment1][whois_pocs] > run
MICROSOFT.COM
[*] I would like installed. Not sure what error you are running into above with the HTTPS
[*] was coming to the github repo so you may want to check your firewall logs. I just ran
[*] marketplace install-all on my Kali instance and had no issues installing everything.

[*] URL: http://whois.arin.net/rest/pocs;domain=microsoft.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE231-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/MAC74-ARIN
[*] Country: United States
[*] Email: abuse@microsoft.com
Right Ctrl
```

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 | 21:55 | 
File Actions Edit View Help
shivanivar@shivanivar: ~
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/DELEO108-ARIN
[*] Country: United States
[*] Email: v-micde@microsoft.com
[*] First_Name: Michael
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/DELEO109-ARIN
[*] Country: United States
[*] Email: v-micde@microsoft.com
[*] First_Name: Michael
[*] Last_Name: De Leon
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/CHINN6-ARIN "the quieter you become, the more you are able to hear"
[*] Country: United States
[*] Email: v-timchi@microsoft.com
[*] First_Name: Tim
[*] Last_Name: Chinn
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Redmond, WA
[*] Title: Whois contact
[*]
SUMMARY
[*] 135 total (13 new) contacts found.
```

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar: ~

60	whois_pocs	Microsoft Corporation	noc@microsoft.com	Whois contact	Redmond, WA	United States	
61	PATRICK	HICKS	pahick@microsoft.com	Whois contact	Seattle, WA	United States	
62	PETER	LEE	peterlee@microsoft.com	Whois contact	Tukwila, WA	United States	
63	whois_pocs	Powerset Network Operations	psdnsadm@microsoft.com	Whois contact	San Francisco, CA	United States	
64	whois_pocs	Powerset Network Operations	psnetops@microsoft.com	Whois contact	San Francisco, CA	United States	
65	Ram	Balakrishnan	rambala@microsoft.com	Whois contact	Redmond, WA	United States	
66	whois_pocs	ROCKY	ELLIS	Whois contact	West Des Moines, IA	United States	
67	Robert	Lemons	rlemon@microsoft.com	Whois contact	Redmond, WA	United States	
68	Robert	Ferguson	robertfe@microsoft.com	Whois contact	Seattle, WA	United States	
69	Staci	Hestilow	rsegala@microsoft.com	Whois contact	Issaquah, WA	United States	
70	CA	MOBILE	Russell.Penar@microsoft.com	Whois contact	Overland Park, KS	United States	
71	SANDRA	WALLER	sandra.waller@microsoft.com	Whois contact	Redmond, WA	United States	
72	whois_pocs	waller	sandra.waller@microsoft.com	Whois contact	Redmond, WA	United States	
73	Sandra	waller	sawaller@microsoft.com	Whois contact	Redmond, WA	United States	
74	whois_pocs	appnexus-ipadmin	xdr-ipadmin@microsoft.com	Whois contact	New York, NY	United States	
75	Scott	Rickelton	scottri@microsoft.com	Whois contact	Bothell, WA	United States	
76	Brian	Lehr	blehr@microsoft.com	Whois contact	Seattle, WA	United States	
77	Steve	Bowman	stevebow@microsoft.com	Whois contact	Portland, OR	United States	
78	Somesh	Chaturmohta	someshch@microsoft.com	Whois contact	Redmond, WA	United States	
79	Adam	Randell	v-adran@microsoft.com	Whois contact	Redmond, WA	United States	
80	Christina	Aadland	v-chrisa@microsoft.com	Whois contact	Redmond, WA	United States	

[80 rows returned]

Here, we got information about company's URL, where the servers are located email address of employees of company, employee's first name, last name, server's region etc

Modules Used	modules load recon/domains-hosts/bing_domain_web
Command Used	Show Domains

```

kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
shivanivar@shivanivar: ~
MICROSOFT.COM
[*] URL: https://www.bing.com/search?first=0&q=domain%3Amicrosoft.com
[recon-ng][Assignment1][bing_domain_web] > show domains
+-----+
| rowid | domain | notes | module |
+-----+
| 1     | microsoft.com | Microsoft | user_defined |
+-----+
[*] 1 rows returned
[recon-ng][Assignment1][bing_domain_web] > db insert domains www.microsoft.com-Microsoft
[*] 1 rows affected.
[recon-ng][Assignment1][bing_domain_web] > show domains
+-----+
| rowid | domain | notes | module |
+-----+
| 1     | microsoft.com | Microsoft | user_defined |
| 2     | www.microsoft.com | Microsoft | user_defined |
+-----+
[*] 2 rows returned
[recon-ng][Assignment1][bing_domain_web] >
[recon-ng][Assignment1] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][Assignment1][bing_domain_web] > show domains
+-----+
| rowid | domain | notes | module |
+-----+
| 1     | microsoft.com | Microsoft | user_defined |
| 2     | www.microsoft.com | Microsoft | user_defined |
+-----+
[*] 2 rows returned
[recon-ng][Assignment1][bing_domain_web] > modules load recon/domains-contacts/whois_pocs
[recon-ng][Assignment1][whois_pocs] > modules load recon/domains-hosts/bing_domain_web
[recon-ng][Assignment1][bing_domain_web] > run

MICROSOFT.COM
[*] URL: https://www.bing.com/search?first=0&q=domain%3Amicrosoft.com
[recon-ng][Assignment1][bing_domain_web] > █

```

Modules Used	modules load recon/domains-hosts/hackertarget
Command Used	Info Options set SOURCE Microsoft.com Run

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shivanivar@shivanivar: ~

[recon-ng][Assignment1][shodan_ip] > modules load recon/domains-hosts/hackertarget
[recon-ng][Assignment1][hackertarget] > info

  Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
  Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  SOURCE    default       yes        source of input (see 'info' for details)

Source Options:
  default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>  string representing a single input
  <path>    path to a file containing a list of inputs
  query <sql> database query returning one column of inputs

[recon-ng][Assignment1][hackertarget] > options set SOURCE Microsoft.com
SOURCE => Microsoft.com
[recon-ng][Assignment1][hackertarget] > info

  Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
  Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  SOURCE    Microsoft.com yes        source of input (see 'info' for details)

Source Options:
  default   SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>  string representing a single input
  <path>    path to a file containing a list of inputs
  query <sql> database query returning one column of inputs

[recon-ng][Assignment1][hackertarget] > run
```

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
shivanivar@shivanivar: ~

[recon-ng][Assignment1][hackertarget] > run

MICROSOFT.COM

[*] Country: None
[*] Host: microsoft.com
[*] Ip_Address: 20.236.44.162
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: 064-smtp-in-2a.microsoft.com
[*] Ip_Address: 157.54.41.37
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: 2015hsc-microsoft.com
[*] Ip_Address: 40.112.151.224
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: 4afrikaskillslab.microsoft.com
[*] Ip_Address: 13.81.118.193
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: 4afrikaskillslabprograms.microsoft.com
[*] Ip_Address: 13.81.118.193
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```



```
File Machine View Input Devices Help
[ 1 2 3 4 ] [ 5 6 ]
File Actions Edit View Help
[*] Country: None
[*] Host: coprofile06.microsoft.com
[*] Ip_Address: 157.56.60.52
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coprofile07.microsoft.com
[*] Ip_Address: 65.55.57.123
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coprofile08.microsoft.com
[*] Ip_Address: 157.56.60.54
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coprofile09.microsoft.com
[*] Ip_Address: 157.56.60.54
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coprofile10.microsoft.com
[*] Ip_Address: 65.55.57.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: coprofile11.microsoft.com
[*] Ip_Address: 157.56.60.55
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

SUMMARY
[*] 501 total (501 new) hosts found.
[recon-ng][Assignment1][hackertarget] > 
```

Here, we obtained 501 total hosts after running the "hackertarget" module with the source set to "Microsoft.com," it indicates that the module has successfully gathered information on 501 hosts related to Microsoft.com. Along with hostname, we retrieved different IP Address as well.

Modules Used	modules load recon/hosts-locations/migrate_hosts
Command Used	Info Run Options set SOURCE Microsoft.com

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[recon-ng][Assignment1][fullcontact] > modules load recon/hosts-locations/migrate_hosts
[recon-ng][Assignment1][migrate_hosts] > info
    Name: Hosts to Locations Data Migrator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Adds a new location for all the locations stored in the 'hosts' table.
Options:
    Name Current Value Required Description
    SOURCE default yes source of input (see 'info' for details)
Source Options:
    default      SELECT DISTINCT latitude, longitude FROM hosts WHERE latitude IS NOT NULL AND longitude IS NOT NULL
    <string>    string representing a single input
    <path>     path to a file containing a list of inputs
    query <sql> database query returning one column of inputs
[recon-ng][Assignment1][migrate_hosts] > options set SOURCE Microsoft.com
[recon-ng][Assignment1][migrate_hosts] > info
    Name: Hosts to Locations Data Migrator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Adds a new location for all the locations stored in the 'hosts' table.
Options:
    Name Current Value Required Description
    SOURCE Microsoft.com yes source of input (see 'info' for details)
Source Options:
    default      SELECT DISTINCT latitude, longitude FROM hosts WHERE latitude IS NOT NULL AND longitude IS NOT NULL
    <string>    string representing a single input
    <path>     path to a file containing a list of inputs
    query <sql> database query returning one column of inputs
[recon-ng][Assignment1][migrate_hosts] > run
[*] Latitude: M
[*] Longitude: i
[*] Notes: None
[*] Street_Address: None
[*]
[recon-ng][Assignment1][migrate_hosts] > SUMMARY
[*] 1 total (1 new) locations found.
[recon-ng][Assignment1][migrate_hosts] >
```

```
File Actions Edit View Help
shivanivar@shivanivar:~
File Actions Edit View Help
File Machine View Input Devices Help
File Actions Edit View Help
[recon-ng][Assignment1][fullcontact] > modules load recon/hosts-locations/migrate_hosts
[recon-ng][Assignment1][migrate_hosts] > info
    Name: Hosts to Locations Data Migrator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Adds a new location for all the locations stored in the 'hosts' table.
Options:
    Name Current Value Required Description
    SOURCE default yes source of input (see 'info' for details)
Source Options:
    default      SELECT DISTINCT latitude, longitude FROM hosts WHERE latitude IS NOT NULL AND longitude IS NOT NULL
    <string>    string representing a single input
    <path>     path to a file containing a list of inputs
    query <sql> database query returning one column of inputs
[recon-ng][Assignment1][migrate_hosts] > options set SOURCE Microsoft.com
[recon-ng][Assignment1][migrate_hosts] > info
    Name: Hosts to Locations Data Migrator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Adds a new location for all the locations stored in the 'hosts' table.
Options:
    Name Current Value Required Description
    SOURCE Microsoft.com yes source of input (see 'info' for details)
Source Options:
    default      SELECT DISTINCT latitude, longitude FROM hosts WHERE latitude IS NOT NULL AND longitude IS NOT NULL
    <string>    string representing a single input
    <path>     path to a file containing a list of inputs
    query <sql> database query returning one column of inputs
[recon-ng][Assignment1][migrate_hosts] > run
[*] Latitude: M
[*] Longitude: i
[*] Notes: None
[*] Street_Address: None
[*]
[recon-ng][Assignment1][migrate_hosts] > SUMMARY
[*] 1 total (1 new) locations found.
[recon-ng][Assignment1][migrate_hosts] >
```

Modules Used	modules load recon/domains-domains/brute_suffix
Command Used	<ul style="list-style-type: none">➤ Info➤ Options set SOURCE Microsoft.com➤ Run

kali linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar: ~

File Actions Edit View Help

K - Requires keys. See info for details.

```
[recon-ng][Assignment1] > modules load recon/domains-domains/brute_suffix
[recon-ng][Assignment1][brute_suffix] > info
```

Name: DNS Public Suffix Brute Forcer
Author: Marcus Watson (@BranMacMuffin)
Version: 1.1

Description:
Brute forces TLDs and SLDs using DNS. Updates the 'domains' table with the results.

Options:

Name	Current Value	Required	Description
SOURCE	default	yes	source of input (see 'info' for details)
SUFFIXES	/home/shivanivar/.recon-ng/data/suffixes.txt	yes	path to public suffix wordlist

Source Options:

```
default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
<string>    string representing a single input
<xpath>     path to a file containing a list of inputs
query <sql> database query returning one column of inputs
```

Comments:

- * TLDs: <https://data.iana.org/TLD/tlds-alpha-by-domain.txt>
- * SLDs: <https://raw.githubusercontent.com/gavingmiller/second-level-domains/master/SLDs.csv>

```
[recon-ng][Assignment1][brute_suffix] > options set SOURCE Microsoft.com
SOURCE => Microsoft.com
[recon-ng][Assignment1][brute_suffix] > run
```

"the quieter you become, the more you

MICROSOFT.COM

```
[*] Microsoft.0 => No record found.
[*] Microsoft.01 => No record found.
[*] Microsoft.02 => No record found.
[*] Microsoft.03 => No record found.
[*] Microsoft.1 => No record found.
[*] Microsoft.10 => No record found.
[*] Microsoft.11 => No record found.
[*] Microsoft.12 => No record found.
[*] Microsoft.13 => No record found.
[*] Microsoft.14 => No record found.
[*] Microsoft.15 => No record found.
```

data = Thunar

File Edit View Go Bookmarks Help

Places

- Comp...
- shivan...
- Desktop
- Recent
- Trash
- Docu...
- Music
- Pictures
- Videos
- Downl...

adobe_blocks.json av_domains.lst ghdb.json

gist_keywords.txt github_dorks.txt hostnames.txt

interesting_files_ve rify.csv suffixes.txt template_html.html

template_map.html template_media.ht ml

"suffixes.txt" | 11.7 KIB (11957 bytes) | plain text document

File Sy...

Devices

Network

Brows...

Right Ctrl

kali linux (Running) – Oracle VM VirtualBox

File Machine View Input Devices Help

shivenivar@shivenivar: ~

```
[*] Microsoft.adserver => No record found.  
[*] Microsoft.adsl => No record found.  
[*] Microsoft.ae => (SOA) Microsoft.ae  
[*] Domain: Microsoft.ae  
[*] Notes: None  
[*]  
[*] Microsoft.af => (SOA) Microsoft.af  
[*] Domain: Microsoft.af  
[*] Notes: None  
[*]  
[*] Microsoft.affiliate => No record found.  
[*] Microsoft.affiliates => No record found.  
[*] Microsoft.afiliados => No record found.  
[*] Microsoft.ag => (SOA) Microsoft.ag  
[*] Domain: Microsoft.ag  
[*] Notes: None  
[*]  
[*] Microsoft.agenda => No record found.  
[*] Microsoft.agent => No record found.  
[*] Microsoft.ai => (SOA) Microsoft.ai  
[*] Domain: Microsoft.ai  
[*] Notes: None  
[*]  
[*] Microsoft.ajax => No record found.  
[*] Microsoft.ajax => No record found.  
[*] Microsoft.ak => No record found.  
[*] Microsoft.akamai => No record found.  
[*] Microsoft.al => (SOA) Microsoft.al  
[*] Domain: Microsoft.al  
[*] Notes: None  
[*]  
[*] Microsoft.alabama => No record found.  
[*] Microsoft.alaska => No record found.  
[*] Microsoft.albuquerque => No record found.  
[*] Microsoft.alerts => No record found.  
[*] Microsoft.alpha => No record found.  
[*] Microsoft.alterwind => No record found.  
[*] Microsoft.am => (SOA) Microsoft.am  
[*] Domain: Microsoft.am  
[*] Notes: None  
[*]  
[*] Microsoft.amarillo => No record found.  
[*] Microsoft.americas => No record found.  
[*] Microsoft.an => No record found.  
[*] Microsoft.anahiem => No record found.  
[*] Microsoft.analyzer => No record found.
```



```
File Machine View Input Devices Help
shivanivar@shivanivar: ~
File Actions Edit View Help
[*] Microsoft.www-2 ⇒ No record found.
[*] Microsoft.www-int ⇒ No record found.
[*] Microsoft.www0 ⇒ No record found.
[*] Microsoft.www01 ⇒ No record found.
[*] Microsoft.www02 ⇒ No record found.
[*] Microsoft.www1 ⇒ No record found.
[*] Microsoft.www2 ⇒ No record found.
[*] Microsoft.www3 ⇒ No record found.
[*] Microsoft.wwwchat ⇒ No record found.
[*] Microsoft.wwwdev ⇒ No record found.
[*] Microsoft.wwwmail ⇒ No record found.
[*] Microsoft.wy ⇒ No record found.
[*] Microsoft.wyoming ⇒ No record found.
[*] Microsoft.x ⇒ No record found.
[*] Microsoft.x-ray ⇒ No record found.
[*] Microsoft.xi ⇒ No record found.
[*] Microsoft.xlogan ⇒ No record found.
[*] Microsoft.xmail ⇒ No record found.
[*] Microsoft.xml ⇒ No record found.
[*] Microsoft.xp ⇒ No record found.
[*] Microsoft.y ⇒ No record found.
[*] Microsoft.yankee ⇒ No record found.
[*] Microsoft.ye ⇒ No record found.
[*] Microsoft.yellow ⇒ No record found.
[*] Microsoft.young ⇒ No record found.
[*] Microsoft.yt ⇒ (SOA) Microsoft.yt
[*] Domain: Microsoft.yt
[*] Notes: None
[*]
Microsoft.yu ⇒ No record found.
Microsoft.z ⇒ No record found.
Microsoft.z-log ⇒ No record found.
[*] Microsoft.za ⇒ No record found.
[*] Microsoft.zebra ⇒ No record found.
[*] Microsoft.zera ⇒ No record found.
[*] Microsoft.zeus ⇒ No record found.
[*] Microsoft.zlog ⇒ No record found.
[*] Microsoft.zm ⇒ No record found.
[*] Microsoft.zulu ⇒ No record found.
[*] Microsoft.zw ⇒ No record found.

SUMMARY
[*] 240 total (239 new) domains found.
[recon-ng][Assignment1][brute_suffix] > 
```

Suffixes.txt file generate.

```
File Edit Search View Document Help
~/recon-ng/data/suffixes.txt - Mousepad
File Edit Search View Document Help
97 ar
98 archie
99 arcsight
100 argentina
101 arizona
102 arkansas
103 arlington
104 as
105 as400
106 asia
107 asterix
108 at
109 athena
110 atlanta
111 atlas
112 att
113 au
114 auction
115 austin
116 auth
117 auto
118 autodiscover
```

Tools Used	Whois
Target Website	Microsoft.com

Utilized WHOIS databases to extract information about Microsoft's domain registration, including the registrant contact, administrative contact, technical contact, registration date, and contact details.

microsoft.com Updated 1 second ago Please try again in 29 minutes

Domain Information

Domain:	microsoft.com
Registrar:	MarkMonitor Inc.
Registered On:	1991-05-02
Expires On:	2025-05-03
Updated On:	2023-08-18
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1-39.azure-dns.com ns2-39.azure-dns.net ns3-39.azure-dns.org ns4-39.azure-dns.info

Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft



Technical Contact

Name: MSN Hostmaster
Organization: Microsoft Corporation
Street: One Microsoft Way,
City: Redmond
State: WA
Postal Code: 98052
Country: US
Phone: +1.4258828080
Fax: +1.4259367329
Email: msnhst@microsoft.com



Administrative Contact

Name: Domain Administrator
Organization: Microsoft Corporation
Street: One Microsoft Way,
City: Redmond
State: WA
Postal Code: 98052
Country: US
Phone: +1.4258828080
Fax: +1.4259367329
Email: admin@domains.microsoft

Raw Whois Data

Domain Name: microsoft.com
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-18T16:15:54+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2025-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
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>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)
Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA

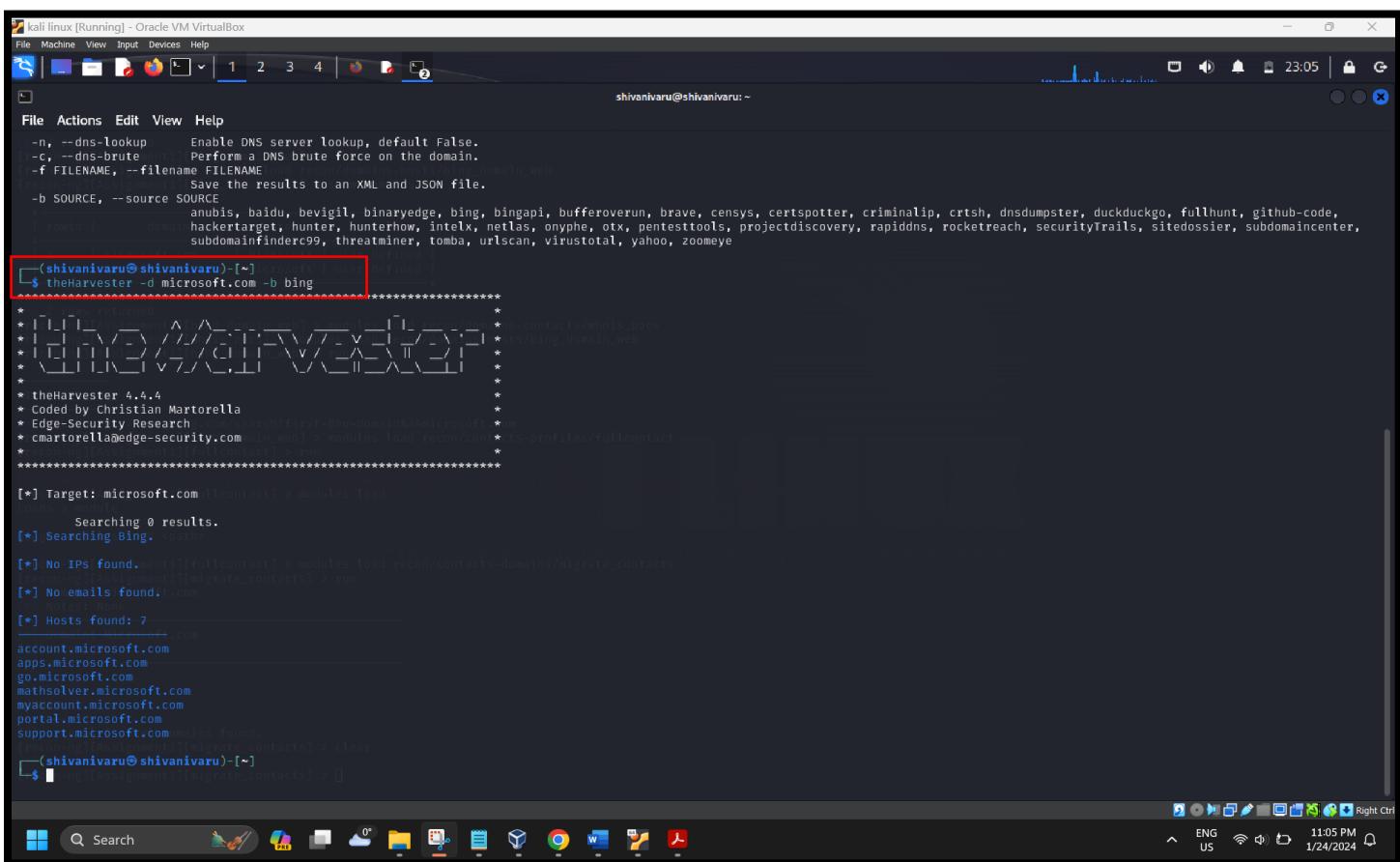
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: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

Company Contact Details

- We are looking for the organization's domain information, administration, registrant, and technical contact information.
- We have identified the contact information by using "Whois." The Internet Assigned Number Authority (IANA) is responsible for managing the root zone in the Domain Name System (DNS), media types, autonomous system numbers, and other symbols and Internet numbers linked to Internet Protocol.
- All the passive information we've acquired will assist us in obtaining the organization's employee information. We can access all systems connected to the same domain by using the organization's registrar domain and IANA number.
- We have registrar servers that connect URLs with webserver IP addresses.

Tools Used	Harvester
Target Website	Microsoft.com
Command Used	theHarvester -d microsoft.com -b bing

- The command "theHarvester -d microsoft.com -b bing" is used to extract information about the domain "microsoft.com" from the Bing search engine using theHarvester tool.
- theHarvester is an open-source tool for gathering email accounts, subdomain names, virtual hosts, open ports, banners, and employee names from various public sources. (**MaxiSoler, 2012**)
- It supports multiple public sources, including Bing, Google, Censys, and others.
- The tool is commonly used for open-source intelligence (OSINT) gathering to help determine an organization's external threat posture. (**Nmmapper.com**)
- It can be an asset for penetration testers and system administrators in the early stages of a security assessment.



```

shivanivar@shivanivar: ~
File Machine View Input Devices Help
File Actions Edit View Help
-n, --dns-lookup      Enable DNS server lookup, default False.
-c, --dns-brute       Perform a DNS brute force on the domain.
-f FILENAME, --filename FILENAME
--recon-domains      Save the results to an XML and JSON file.
--source SOURCE
-anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave, censys, certspotter, criminalip, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code,
-hackertarget, hunter, hunterhow, intelix, netlas, onyphe, otx, pentesttools, projectdiscovery, rapiddns, rocketreach, securitytrails, sitesdossier, subdomaincenter,
-subdomainfinderc99, threatminer, tomba, urlscan, virustotal, yahoo, zoomeye
(shivanivar@shivanivar)-[~] $ theHarvester -d microsoft.com -b bing
*****
[*] Target: microsoft.com [contact] > modules load
[*] No modules found.
[*] Searching 0 results.
[*] Searching Bing. results
[*] No IPs found.
[*] No emails found.
[*] Notes: None
[*] Hosts Found: 7
account.microsoft.com
apps.microsoft.com
go.microsoft.com
mathsolver.microsoft.com
myaccount.microsoft.com
portal.microsoft.com
support.microsoft.com
*****[migrat_contacts] > clear
(shivanivar@shivanivar)-[~] $ 

```

As a result, we have found above open ports/ IP addresses, email accounts, and 7 host of different websites they use. we found 16 emails.

Command Used

TheHarvester -d microsoft.com -b bing -c

The `-c` flag is used to activate the DNS brute force plugin, which runs a dictionary brute force enumeration. This can be helpful in identifying additional subdomains associated with the target domain.

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
support.microsoft.com
(shivanivar@shivanivar) [~]
$ theHarvester -d microsoft.com -b bing -c
*****
* [!] The Harvester v4.4.4
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****
```

[*] Target: microsoft.com

Searching @ results.

[*] Searching Bing.

[*] No IPs found.

[*] Emails found: 1

weshelp@microsoft.com

[*] Hosts found: 34

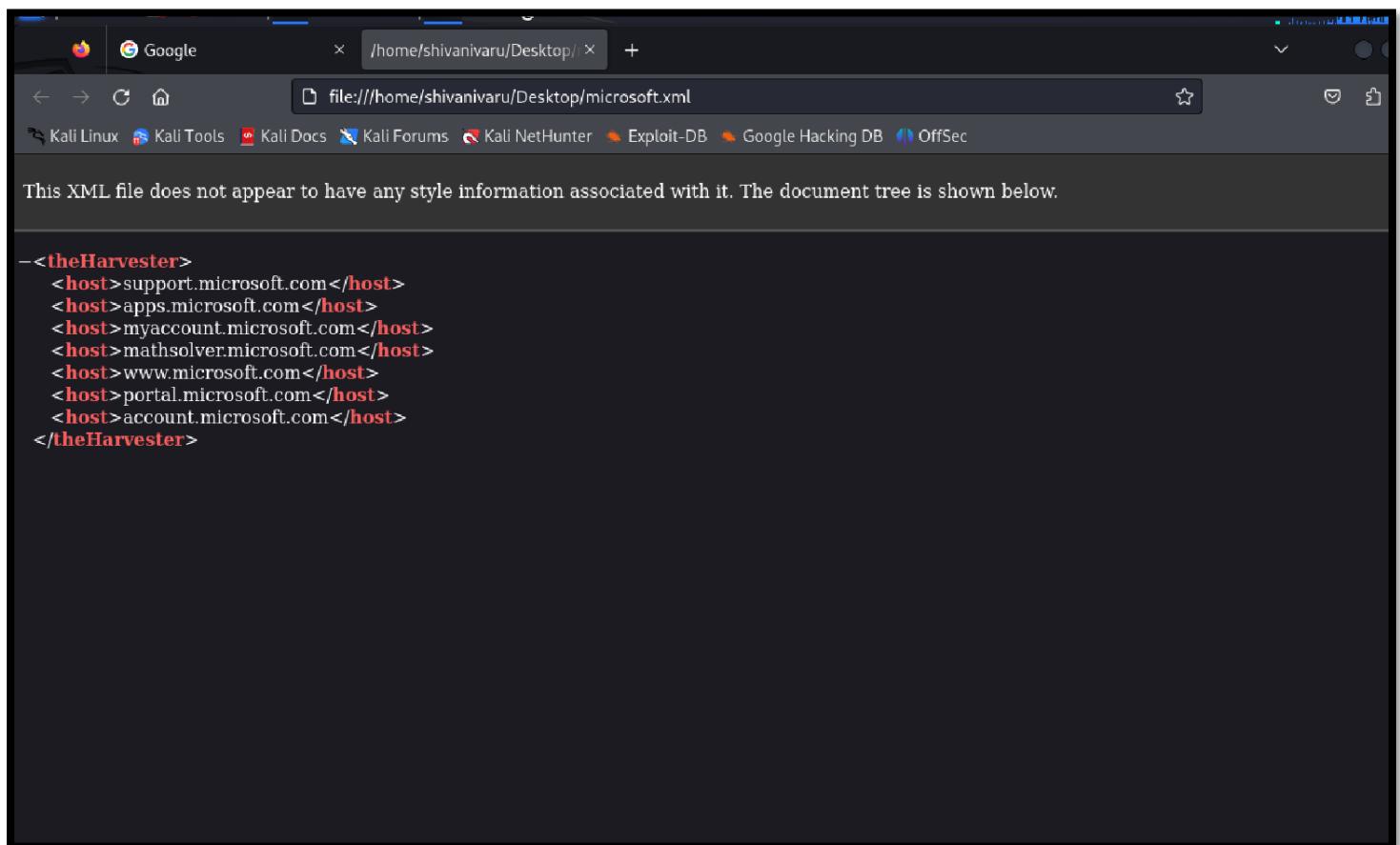
about.ads.microsoft.com
account.microsoft.com
admin.microsoft.com
answers.microsoft.com
apps.microsoft.com
azure.microsoft.com
bing.microsoft.com
bingapp.microsoft.com
blogs.microsoft.com
careers.microsoft.com
con-symmetry.microsoft.com
cool.microsoft.com
create.microsoft.com
developer.microsoft.com
docs.microsoft.com

```
kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
shivanivar@shivanivar: ~
File Actions Edit View Help
lamer.microsoft.com;
virtual.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
buscador.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
dialup.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
thankyou.microsoft.com;
house.microsoft.com;
xenapp.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
ash.microsoft.com;
int.microsoft.com:13.107.213.35,13.107.246.35 > modules load recon/domains-hosts/bing_domain_web
img13.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
nyx.microsoft.com;
upload.microsoft.com;
livehelp.microsoft.com;
youth.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
castor.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
clicks.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
hybrid.microsoft.com;
oc.microsoft.com;
orders.microsoft.com:131.107.97.20
atl.microsoft.com;
uf001jc.microsoft.com; > modules load recon/domains-hosts/bing_domain_web
horo.microsoft.com; > modules load recon/contactdb-profile/fullcontact
gollum.microsoft.com; > modules load recon/contactdb-profile/fullcontact
ect.microsoft.com;
msn-smtp-out.microsoft.com;
wini.microsoft.com;
vci.microsoft.com;
rs1.microsoft.com;
luxury.microsoft.com;
autoconfig.test.microsoft.com;
resource.microsoft.com; > modules load recon/contactdb-domains/migrate_contacts
mailer.microsoft.com; > modules load recon/contactdb-domains/migrate_contacts
print.microsoft.com:20.70.246.20
print.microsoft.com:20.70.246.20
fix.microsoft.com;
lifestyle.microsoft.com;
remedy.microsoft.com;
m5.microsoft.com;
```

Command Used	<code>TheHarvester -d microsoft.com -b bing -f~/Desktop/Microsoft</code>
--------------	--

The **-d** flag specifies the domain to scan, the **-b** flag specifies the search engine to use, and the **-f** flag specifies an output file for the found results, which will be saved on the Desktop with the name "microsoft".

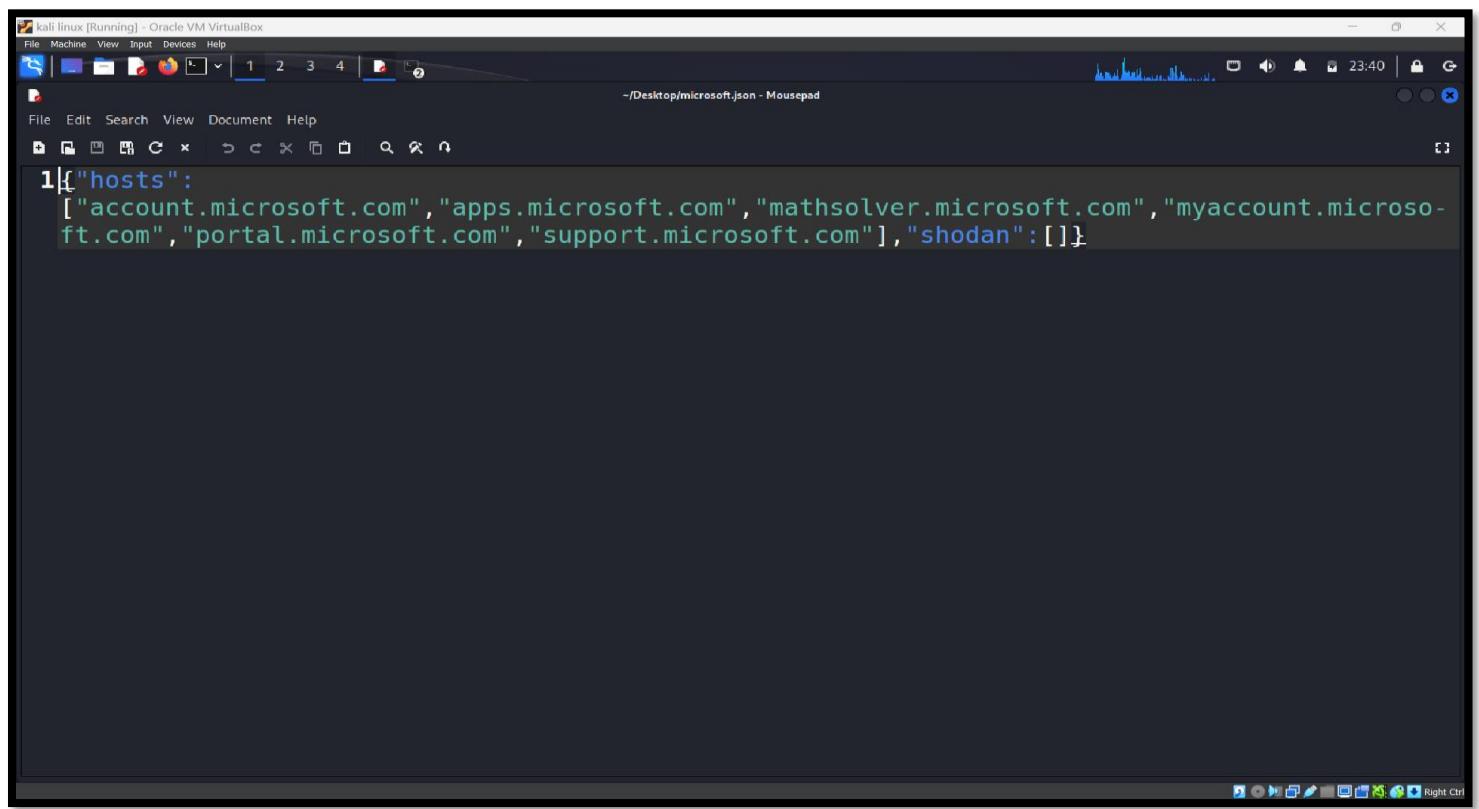
❖ XML Format



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
--<theHarvester>
<host>support.microsoft.com</host>
<host>apps.microsoft.com</host>
<host>myaccount.microsoft.com</host>
<host>mathsolver.microsoft.com</host>
<host>www.microsoft.com</host>
<host>portal.microsoft.com</host>
<host>account.microsoft.com</host>
</theHarvester>
```

❖ Json format



```
1|{"hosts": ["account.microsoft.com", "apps.microsoft.com", "mathsolver.microsoft.com", "myaccount.microsoft.com", "portal.microsoft.com", "support.microsoft.com"], "shodan": []}
```

References

- 1) Admin, T. (2024, January 5). Recon-*ng* tutorial. HackerTarget.com. [https://hackertarget.com/recon-*ng*-tutorial/](https://hackertarget.com/recon-ng-tutorial/)
- 2) Moulik. (2023, December 30). Recon-*ng*: A full tutorial from NOOB to pro [updated 2024]. TECHYRICK. <https://techyrick.com/recon-ng/>
- 3) GeeksforGeeks. (2021, April 16). Recon-*ng* information gathering tool in Kali Linux. GeeksforGeeks. <https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/>
- 4) Recon-*NG*: Kali linux tools. Kali Linux. (2022, November 16). <https://www.kali.org/tools/recon-ng/>
- 5) Recon-*ng* information gathering tool in Kali Linux - javatpoint. www.javatpoint.com. (n.d.). <https://www.javatpoint.com/recon-ng-information-gathering-tool-in-kali-linux>
- 6) Securitytrails. (n.d.). <https://securitytrails.com/blog/recon-ng>
- 7) MaxiSoler. (2012, April 17). Home. ToolsWatch Cyber Security Tools Events. <https://toolswatch.org/2012/04/theharvester-v2-2-released/>
- 8) Nmmapper.com. (n.d.). *Online platform for network pentesting and mapping tool for penetration testers and system administrators*. nmmapper.com. <https://www.nmmapper.com/sys/theharvester/email-harvester-tool/online/>

Video Recording Link:

<https://conestogac.zoom.us/rec/share/-WaUywpUeU5kQlxDhKMgB6ABiR7DmlQRgqMVH1tVC4-xGRZgrUTQ2i0zYi6dqnAg.qCPAoPKJTclM5GeI?startTime=1706314693000>