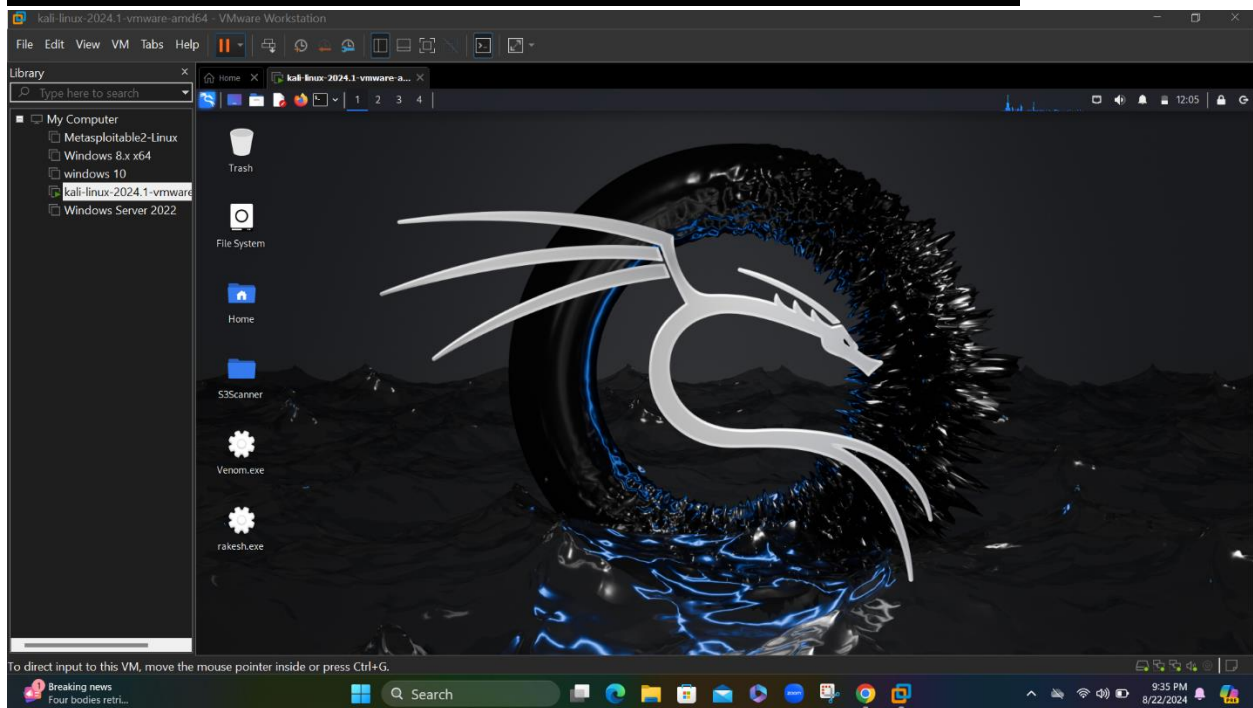


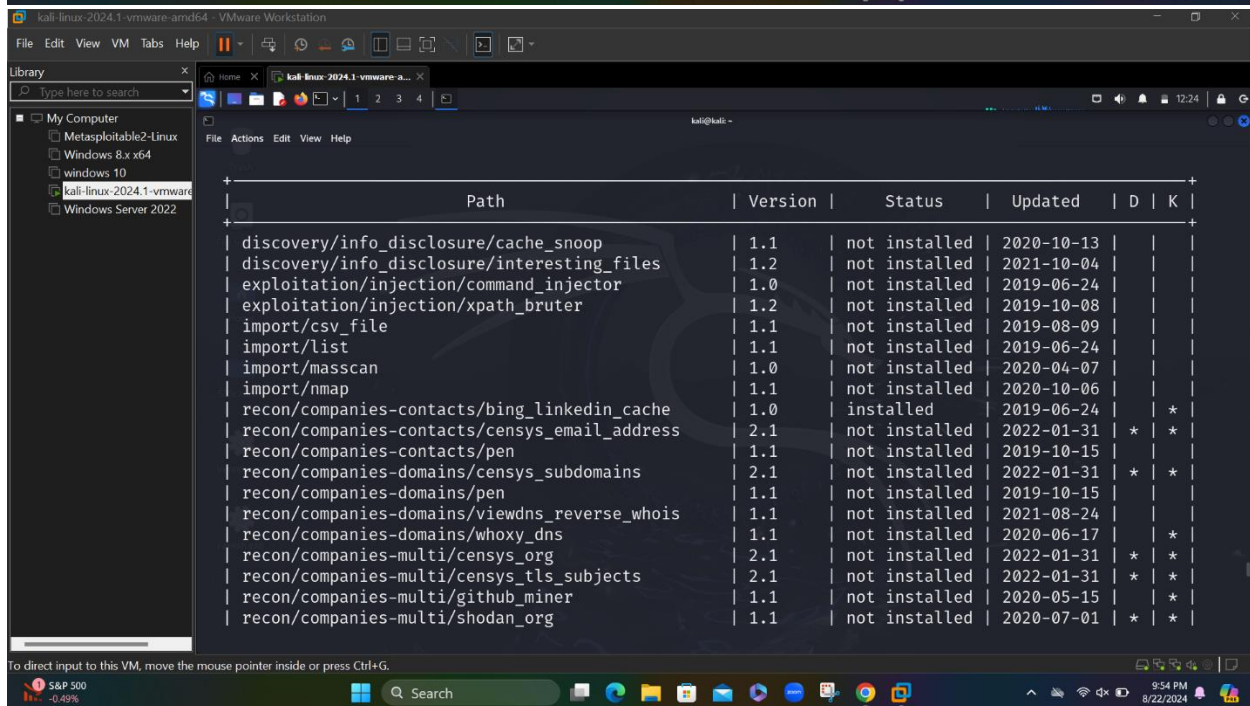
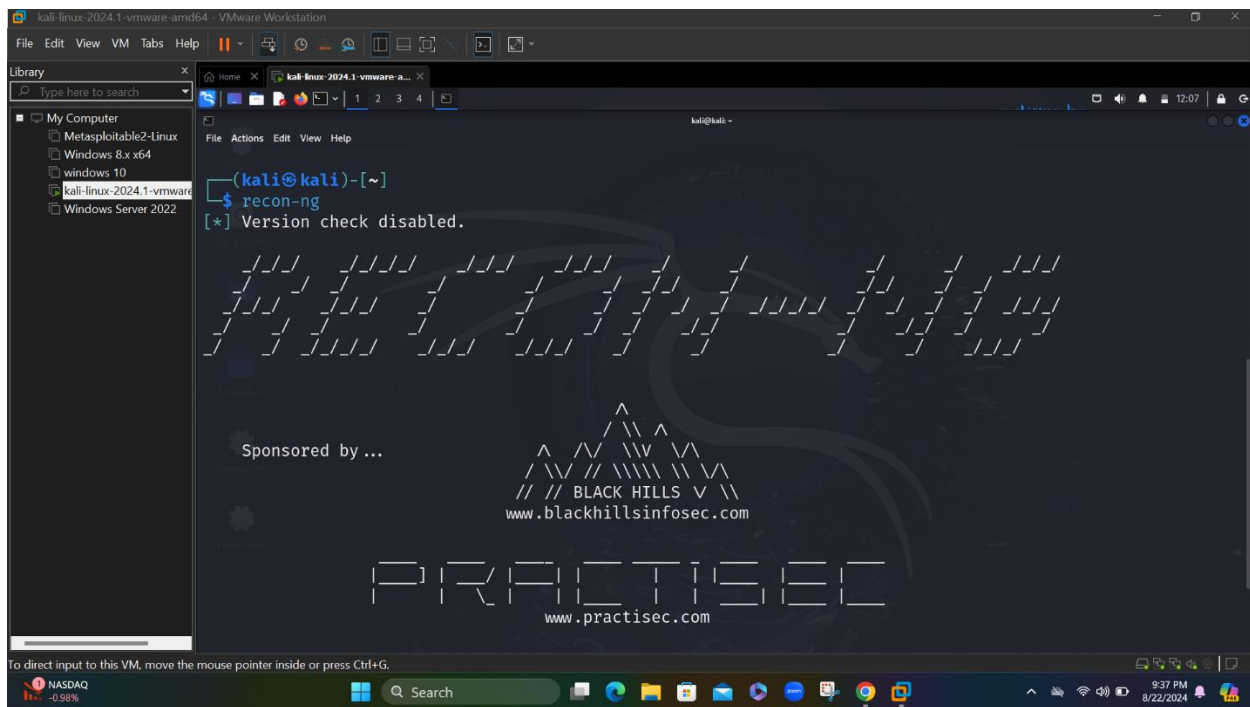
Executive Post Graduate Certification in Cyber Security and Ethical Hacking

ASSIGNMENT-01

Objectives: 01

- Footprint a target using Recon-ng.





```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
[recon-ng][default] > marketplace search whois
[*] Searching module index for 'whois' ...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+-----+
| recon/companies-domains/viewdns_reverse_whois | 1.1 | not installed | 2021-08-24 | | |
| recon/companies-multi/whois_miner | 1.1 | installed | 2019-10-15 | | |
| recon/domains-companies/whoxy_whois | 1.1 | not installed | 2020-06-24 | | * |
| recon/domains-contacts/whois_pocs | 1.0 | installed | 2019-06-24 | | |
| recon/netblocks-companies/whois_orgs | 1.0 | not installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Reloading modules ...
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
USD/JPY +0.64%
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[recon-ng][default] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [ ... ]

[recon-ng][default] > modules load
Loads a module

Usage: modules load <path>

[recon-ng][default] > modules load recon/domains-contacts/whois_pocs
[recon-ng][default][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.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
78°F Mostly cloudy
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali ~
File Actions Edit View Help

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:
  Name      Current Value  Required  Description
  SOURCE                                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][default][whois_pocs] >
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali ~
File Actions Edit View Help

[recon-ng][default][whois_pocs] > options set SOURCE ebay.com
SOURCE ⇒ ebay.com
[recon-ng][default][whois_pocs] > run

EBAY.COM

[*] URL: http://whois.arin.net/rest/pocs;domain=ebay.com
[*] URL: http://whois.arin.net/rest/poc/TRIEG1-ARIN
[*] Country: United States
[*] Email: atrieger@ebay.com
[*] First_Name: Drew
[*] Last_Name: Trieger
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Tempe, AZ
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/FOSTE84-ARIN
[*] Country: United States
```



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali ~
[+] Title: Whois contact
[+]
[+] URL: http://whois.arin.net/rest/poc/FOSTE84-ARIN
[+] Country: United States
[+] Email: bifoster@ebay.com
[+] First_Name: Bill
[+] Last_Name: Foster
[+] Middle_Name: None
[+] Notes: None
[+] Phone: None
[+] Region: San Jose, CA
[+] Title: Whois contact
[+]
[+] URL: http://whois.arin.net/rest/poc/BMC126-ARIN
[+] Country: United States
[+] Email: bmckay@ebay.com
[+] First_Name: Brent
[+] Last_Name: McKay
[+] Middle_Name: None
[+] Notes: None
[+] Phone: None
[+] Region: San Jose, CA

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
USD/CNY +0.13%
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali ~
[+] Title: Whois contact
[+]
[+] URL: http://whois.arin.net/rest/poc/EAC15-ARIN
[+] Country: United States
[+] Email: dl-ebay-rir-abuse-c@ebay.com
[+] First_Name: None
[+] Last_Name: eBay Abuse Contact
[+] Middle_Name: None
[+] Notes: None
[+] Phone: None
[+] Region: San Jose, CA
[+] Title: Whois contact
[+]
[+] URL: http://whois.arin.net/rest/poc/GSL19-ARIN
[+] Country: United States
[+] Email: gslater@ebay.com
[+] First_Name: Gary
[+] Last_Name: Slater
[+] Middle_Name: None
[+] Notes: None
[+] Phone: None
[+] Region: San Jose, CA

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
USD/CNY +0.13%
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/FH198-ARIN
[*] Country: United States
[*] Email: ksandford@ebay.com
[*] First_Name: Faye
[*] Last_Name: Hall
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/EBAYN-ARIN
[*] Country: United States
[*] Email: network@ebay.com
[*] First_Name: None
[*] Last_Name: eBay Network
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
78°F Mostly cloudy 10:13 PM 8/22/2024
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
[*]
[*] URL: http://whois.arin.net/rest/poc/SSL984-ARIN
[*] Country: United States
[*] Email: ssleiman@ebay.com
[*] First_Name: Sharif
[*] Last_Name: Sleiman
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/VKR6-ARIN
[*] Country: United States
[*] Email: vkrishnan@ebay.com
[*] First_Name: Verraghavan
[*] Last_Name: Krishnan
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
78°F Mostly cloudy 10:14 PM 8/22/2024
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/VKR6-ARIN
[*] Country: United States
[*] Email: vkrishnan@ebay.com
[*] First_Name: Verraghavan
[*] Last_Name: Krishnan
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Jose, CA
[*] Title: Whois contact
[*]
SUMMARY
[*] 10 total (10 new) contacts found.
[recon-ng][default][whois_pocs] > options set SOURCE ebay.com
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali ~
PRACTISEC
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[4] Recon modules

[recon-ng][default] > marketplace install recon/domains-hosts/brute_hosts
[*] Module installed: recon/domains-hosts/brute_hosts
[*] Reloading modules ...
[!] 'bing_api' key not set, bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set, bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[recon-ng][default] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > info

    Name: DNS Hostname Brute Forcer
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0

Description:
    Brute forces host names using DNS. Updates the 'hosts' table with the results.

Options:
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali -
File Actions Edit View Help
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Brute forces host names using DNS. Updates the 'hosts' table with the results.

Options:


| Name     | Current Value                           | Required | Description                              |
|----------|-----------------------------------------|----------|------------------------------------------|
| SOURCE   | default                                 | yes      | source of input (see 'info' for details) |
| WORDLIST | /home/kali/.recon-ng/data/hostnames.txt | yes      | path to hostname wordlist                |



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][default][brute_hosts] > options set SOURCE ebay.com
SOURCE => ebay.com
[recon-ng][default][brute_hosts] > info

Name: DNS Hostname Brute Forcer
Author: Tim Tomes (@lanmaster53)
Version: 1.0

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

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

kali@kali -
File Actions Edit View Help

Name: DNS Hostname Brute Forcer
Author: Tim Tomes (@lanmaster53)
Version: 1.0

Description:
Brute forces host names using DNS. Updates the 'hosts' table with the results.

Options:


| Name     | Current Value                           | Required | Description                              |
|----------|-----------------------------------------|----------|------------------------------------------|
| SOURCE   | ebay.com                                | yes      | source of input (see 'info' for details) |
| WORDLIST | /home/kali/.recon-ng/data/hostnames.txt | yes      | path to hostname wordlist                |



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][default][brute_hosts] > run

EBAY.COM

[*] No Wildcard DNS entry found.

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



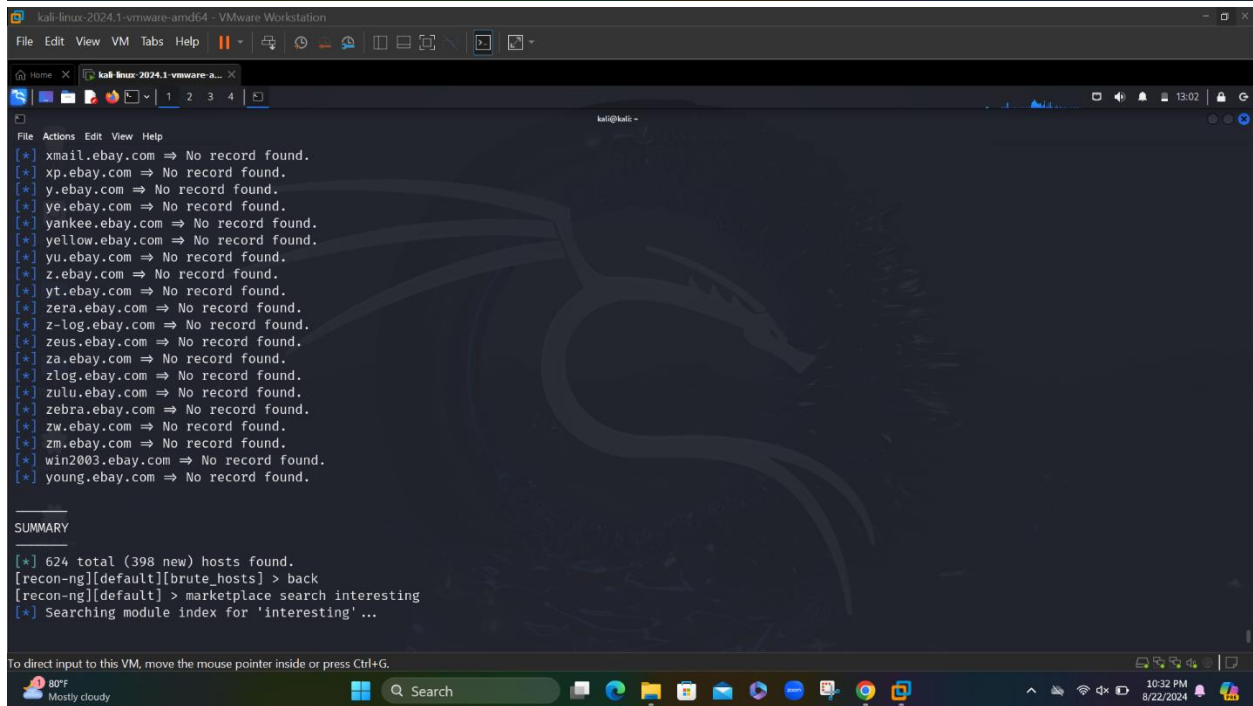
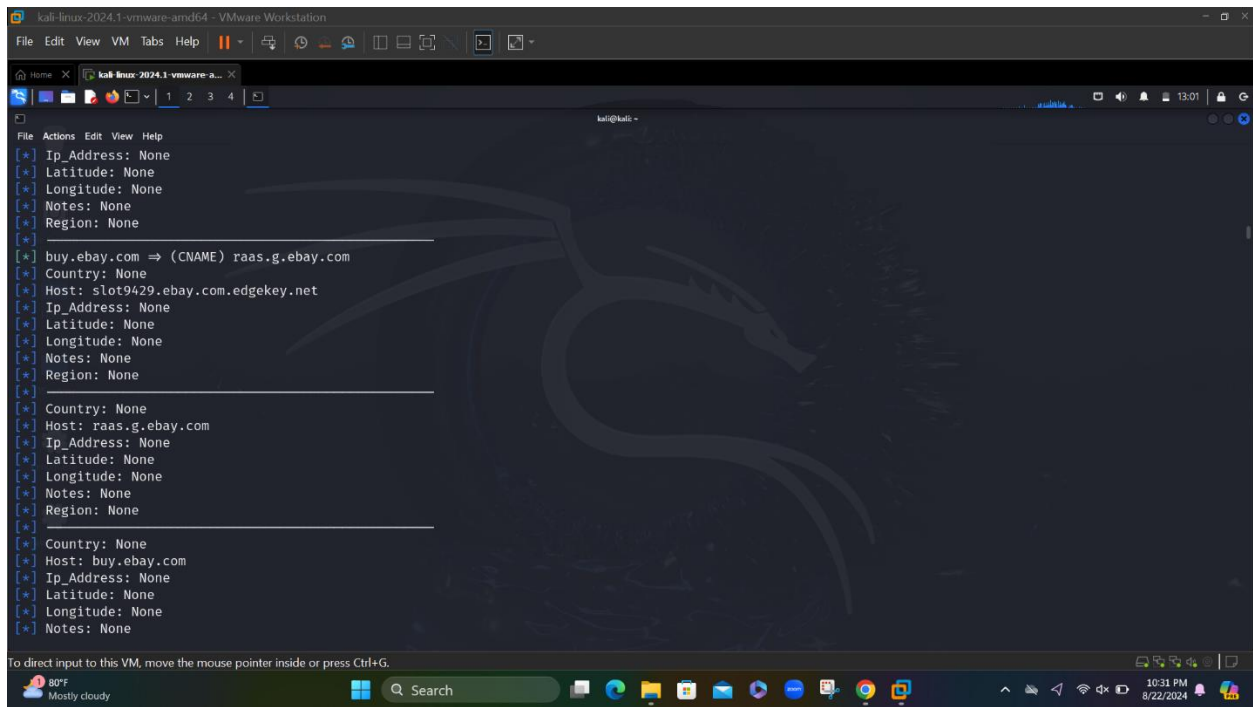
```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
query <sql> database query returning one column of inputs

[recon-ng][default][brute_hosts] > run

EBAY.COM

[*] No Wildcard DNS entry found.
[*] 01.ebay.com => No record found.
[*] 0.ebay.com => No record found.
[*] 02.ebay.com => No record found.
[*] 12.ebay.com => No record found.
[*] 03.ebay.com => No record found.
[*] 1.ebay.com => No record found.
[*] 13.ebay.com => No record found.
[*] 14.ebay.com => No record found.
[*] 11.ebay.com => No record found.
[*] 10.ebay.com => No record found.
[*] 17.ebay.com => No record found.
[*] 15.ebay.com => No record found.
[*] 18.ebay.com => No record found.
[*] 16.ebay.com => No record found.
[*] 4.ebay.com => No record found.
[*] 5.ebay.com => No record found.
[*] 3.ebay.com => No record found.
[*] 3com.ebay.com => No record found.
[*] 6.ebay.com => No record found.
[*] 20.ebay.com => No record found.
[*] 2.ebay.com => No record found.
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
[*] admins.ebay.com => No record found.
[*] Country: None
[*] Host: slot12771.ebay.com.edgekey.net
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: accounts.ebay.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] accounts.ebay.com => (CNAME) e12771.a.akamaiedge.net
[*] Country: None
[*] Host: e12771.a.akamaiedge.net
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: accounts.ebay.com
[*] Ip_Address: None
```



```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali -
[*] Searching module index for 'interesting'...

+-----+
|  | Path | Version | Status |
+-----+
Updated | D | K |
+-----+
| discovery/info_disclosure/interesting_files | 1.2 | not installed | 2021-10-04 |
+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules...
[!] 'bing_api' key not set. bing_linkedin_contacts module will likely fail at runtime. See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime. See 'keys add'.
[recon-ng][default] > marketplace load discovery/info_disclosure/interesting_files
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

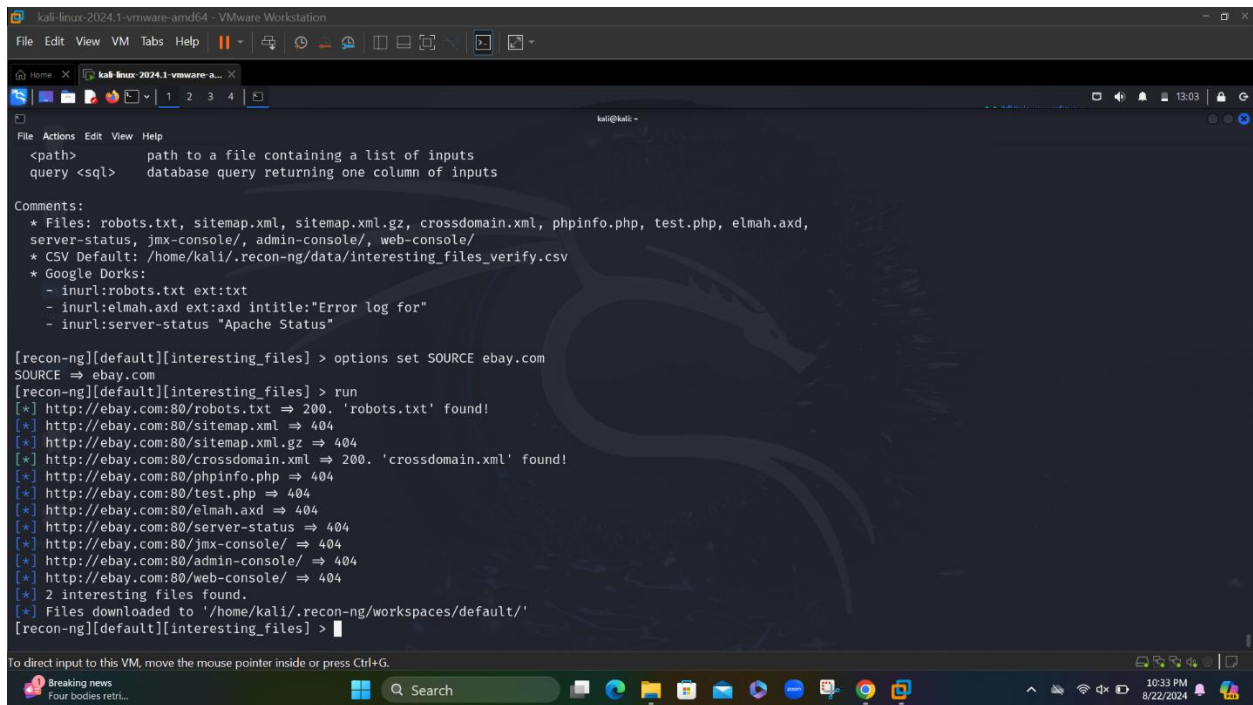
[recon-ng][default] > info
[!] Invalid command: info.
[recon-ng][default] > modules load discovery/info_disclosure/interesting_files
```

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
kali@kali -
Options:
Name      Current Value      Required  Description
-----
CSV_FILE  /home/kali/.recon-ng/data/interesting_files_verify.csv  yes       custom filename map
DOWNLOAD  True               yes       download discovered files
PORT      80                yes       request port
PROTOCOL  http              yes       request protocol
SOURCE     default           yes       source of input (see 'info' for details)

Source Options:
default    SELECT DISTINCT host FROM hosts WHERE host 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

Comments:
* Files: robots.txt, sitemap.xml, sitemap.xml.gz, crossdomain.xml, phpinfo.php, test.php, elmah.axd,
server-status, jmx-console/, admin-console/, web-console/
* CSV Default: /home/kali/.recon-ng/data/interesting_files_verify.csv
* Google Dorks:
- inurl:robots.txt ext:txt
- inurl:elmah.axd ext:axd intitle:"Error log for"
- inurl:server-status "Apache Status"

[recon-ng][default][interesting_files] > options set SOURCE ebay.com
SOURCE => ebay.com
[recon-ng][default][interesting_files] > run
[*] http://ebay.com:80/robots.txt => 200. 'robots.txt' found!
[*] http://ebay.com:80/sitemap.xml => 404
```



```
kali@kali:~$ recon-ng
[recon-ng][default][interesting_files] > options set SOURCE ebay.com
SOURCE => ebay.com
[recon-ng][default][interesting_files] > run
[*] http://ebay.com:80/robots.txt => 200. 'robots.txt' found!
[*] http://ebay.com:80/sitemap.xml => 404
[*] http://ebay.com:80/sitemap.xml.gz => 404
[*] http://ebay.com:80/crossdomain.xml => 200. 'crossdomain.xml' found!
[*] http://ebay.com:80/phpinfo.php => 404
[*] http://ebay.com:80/test.php => 404
[*] http://ebay.com:80/elmah.axd => 404
[*] http://ebay.com:80/server-status => 404
[*] http://ebay.com:80/jmx-console/ => 404
[*] http://ebay.com:80/admin-console/ => 404
[*] http://ebay.com:80/web-console/ => 404
[*] 2 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/workspaces/default/'
[recon-ng][default][interesting_files] >
```

Objectives: 02

● Footprint a target using Maltego

- I have selected my target as “ebay.com”

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

MaRego Community Edition 4.7.0

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Entity Palette

- Cryptocurrency
 - Bitcoin Cash Address
 - An address in a Bitcoin Cash blockchain
 - Bitcoin Cash Block
 - A generic block in a Bitcoin Cash blockchain
 - BitcoinCash Block Height
 - The incremental block number in the block
 - Bitcoin Cash Transaction
 - A transaction in a Bitcoin Cash blockchain
 - Bitcoin Address
 - An address in a Bitcoin blockchain
 - Bitcoin Block
 - A generic block in a Bitcoin blockchain

Run View

- Transforms
- Machines
 - Company Stalker CE
 - This machine will try to get all...
 - URL To Network And Domains...

New Graph (13)

Output - Transform Output

1 of 3 entities

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

80°F Mostly cloudy

Search

10:43 PM 8/22/2024

kali-linux-2024.1-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

MaRego Community Edition 4.7.0

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Entity Palette

- Cryptocurrency
 - Bitcoin Cash Address
 - An address in a Bitcoin Cash blockchain
 - Bitcoin Cash Block
 - A generic block in a Bitcoin Cash blockchain
 - BitcoinCash Block Height
 - The incremental block number in the block
 - Bitcoin Cash Transaction
 - A transaction in a Bitcoin Cash blockchain
 - Bitcoin Address
 - An address in a Bitcoin blockchain
 - Bitcoin Block
 - A generic block in a Bitcoin blockchain

Run View

- Transforms
- Machines
 - Company Stalker CE
 - This machine will try to get all...
 - URL To Network And Domains...

New Graph (13)

Output - Transform Output

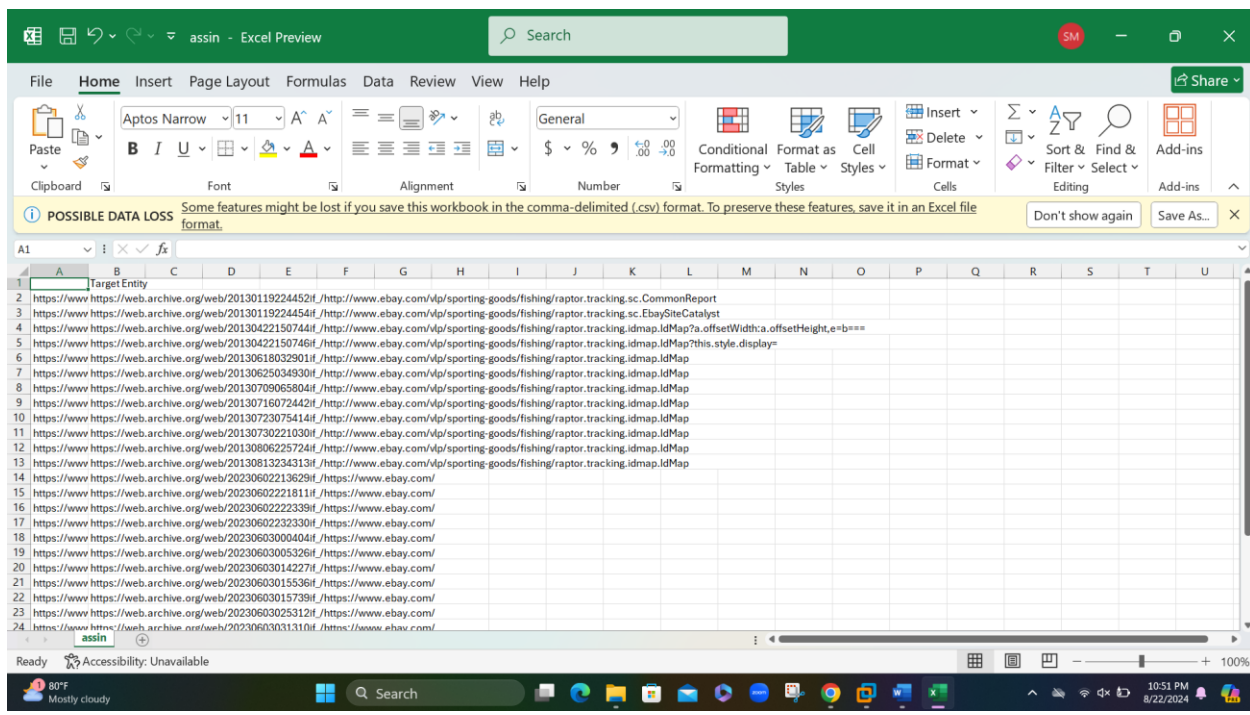
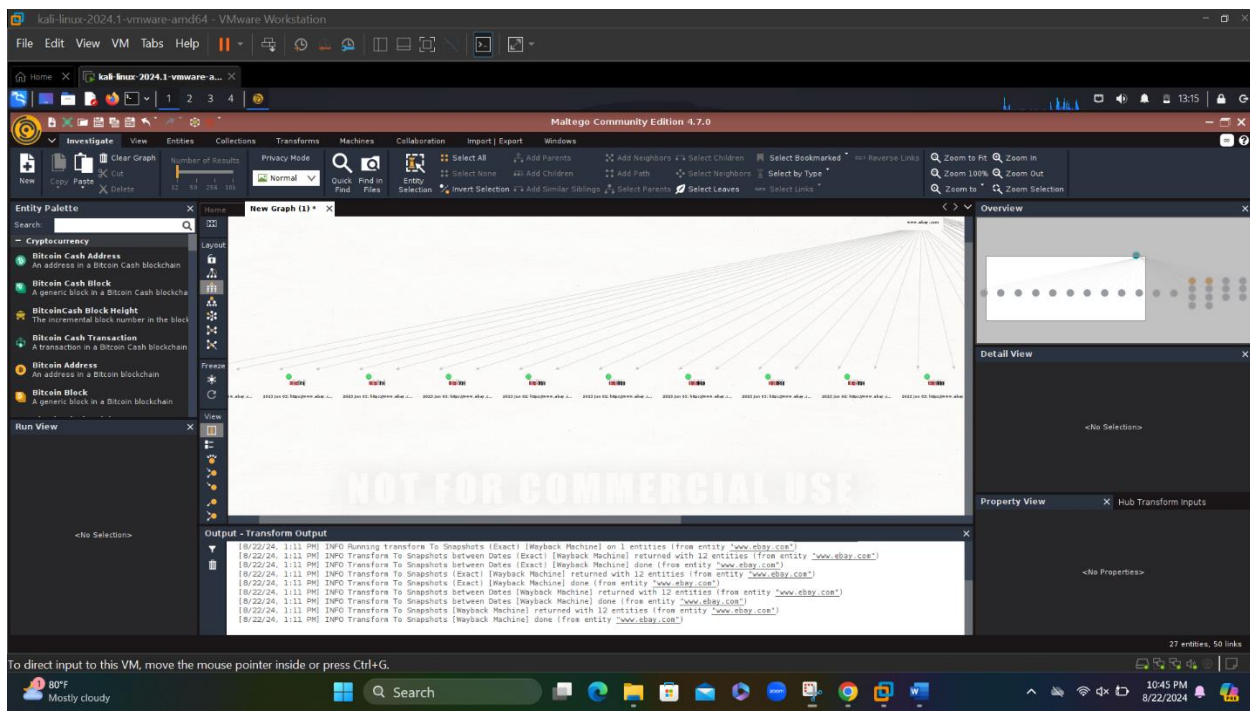
27 entities, 50 links

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

80°F Mostly cloudy

Search

10:44 PM 8/22/2024



Submitted By
Sairaj Mothukuri
[sairajmothukuri28@gmail.com]

