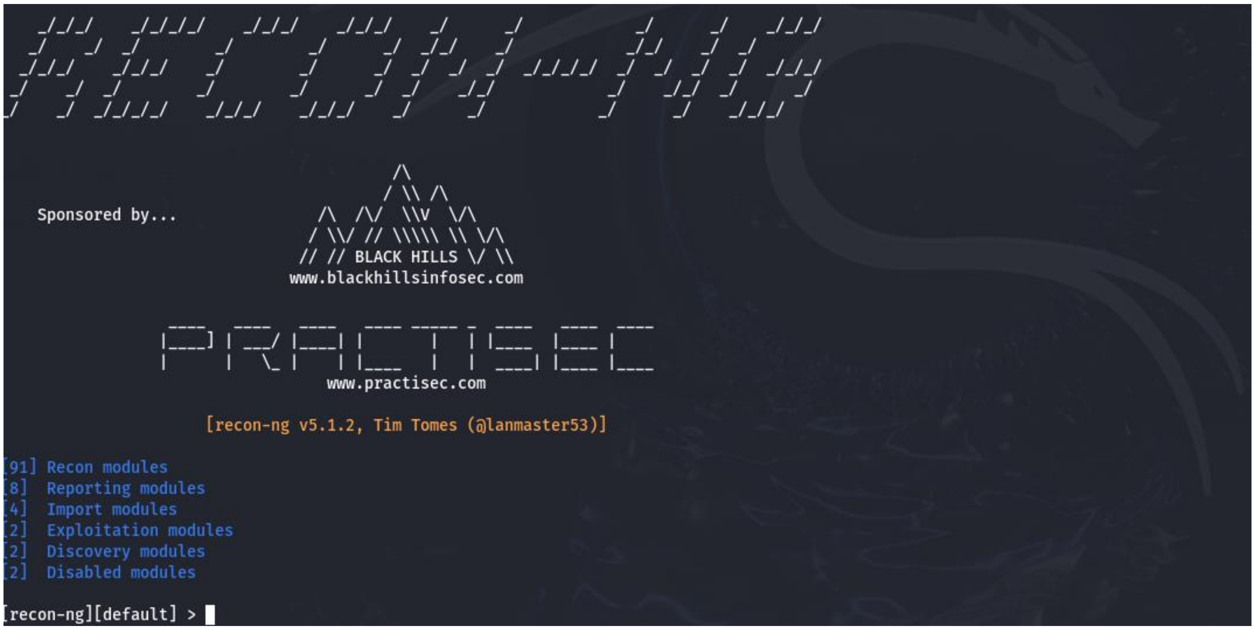
# Executive Post Graduate Certification in Cyber Security and Ethical Hacking

# Assignment 01

- **<u>Footprint a target using Recon-ng:</u>**

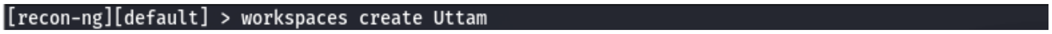
Here I am using kali linux.

Login kali linux in VMware then open terminal Type sudo su  then enter the password then recon-ng



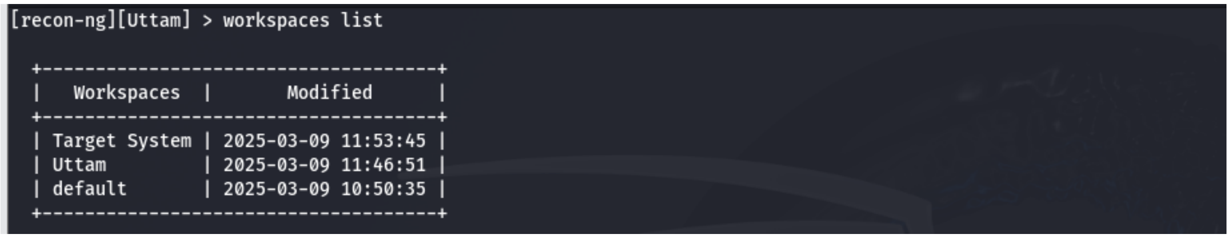
```
    Sponsored by...
                         // // BLACK HILLS \/ \\
                        www.blackhillsinfosec.com

                           www.practisec.com

                [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[91] Recon modules
[8]  Reporting modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules
[2]  Disabled modules

[recon-ng][default] >
```

We need to create workspaces, work place created as Uttam.



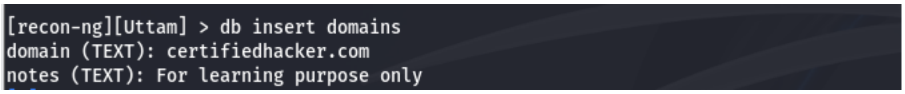
```
[recon-ng][default] > workspaces create Uttam
```

Workspace list check, we have 3 work workspaces.

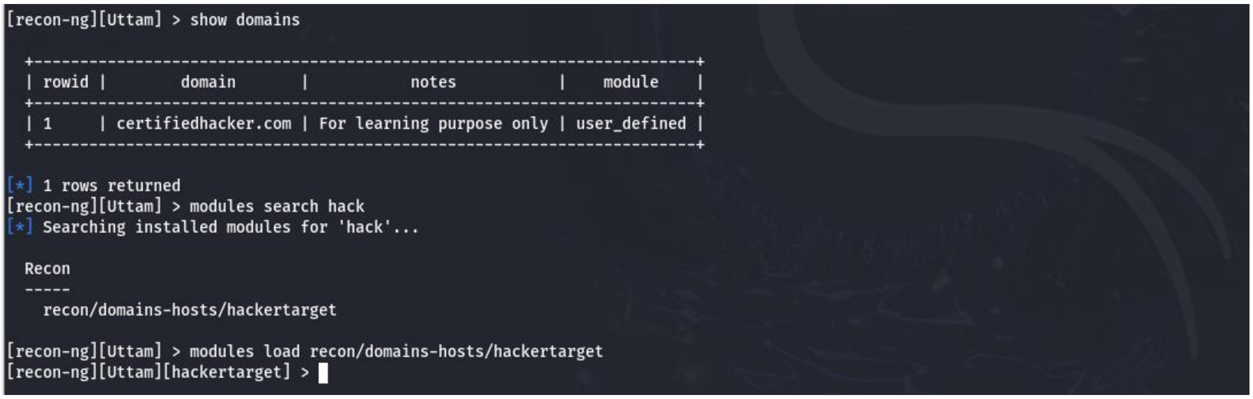


```
[recon-ng][Uttam] > workspaces list

  +-------------------------------------+
  |   Workspaces  |       Modified      |
  +-------------------------------------+
  | Target System | 2025-03-09 11:53:45 |
  | Uttam         | 2025-03-09 11:46:51 |
  | default       | 2025-03-09 10:50:35 |
  +-------------------------------------+
```

We need to add the Target Domains, domain name added as certifiedhacker.com

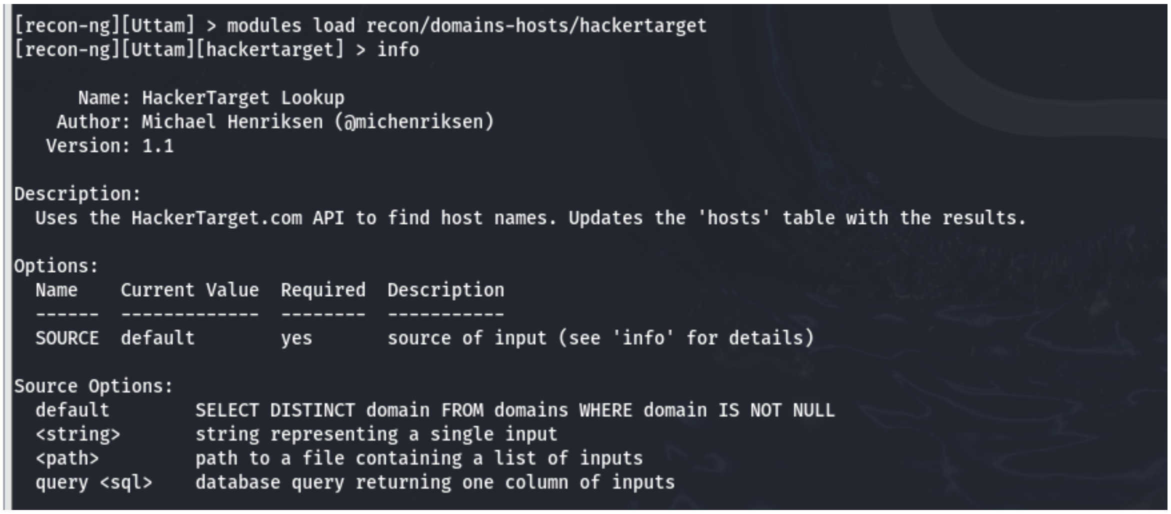


```
[recon-ng][Uttam] > db insert domains
domain (TEXT): certifiedhacker.com
notes (TEXT): For learning purpose only
```

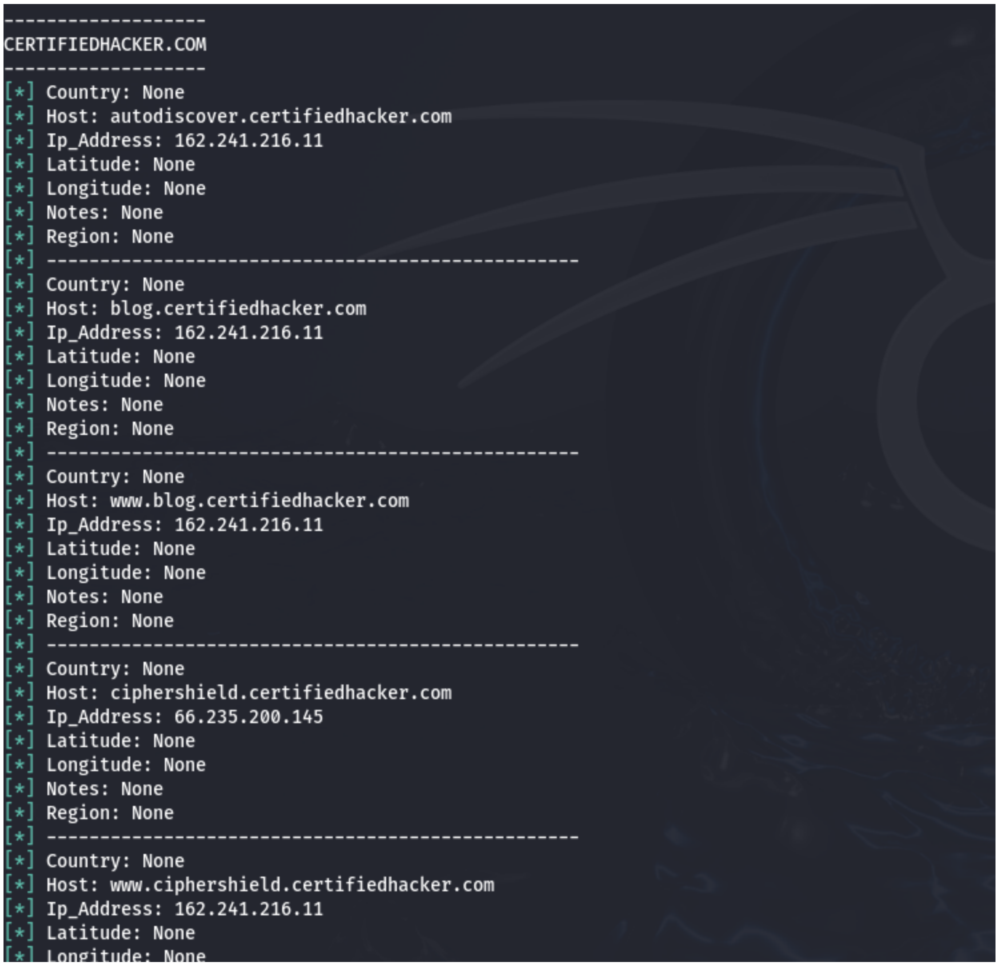


```
[recon-ng][Uttam] > show domains

  +-----------------------------------------------------------------------+
  | rowid |        domain       |           notes          |    module    |
  +-----------------------------------------------------------------------+
  | 1     | certifiedhacker.com | For learning purpose only | user_defined |
  +-----------------------------------------------------------------------+

[*] 1 rows returned
[recon-ng][Uttam] > modules search hack
[*] Searching installed modules for 'hack'...

  Recon
  -----
    recon/domains-hosts/hackertarget

[recon-ng][Uttam] > modules load recon/domains-hosts/hackertarget
[recon-ng][Uttam][hackertarget] >
```

For more details use info command

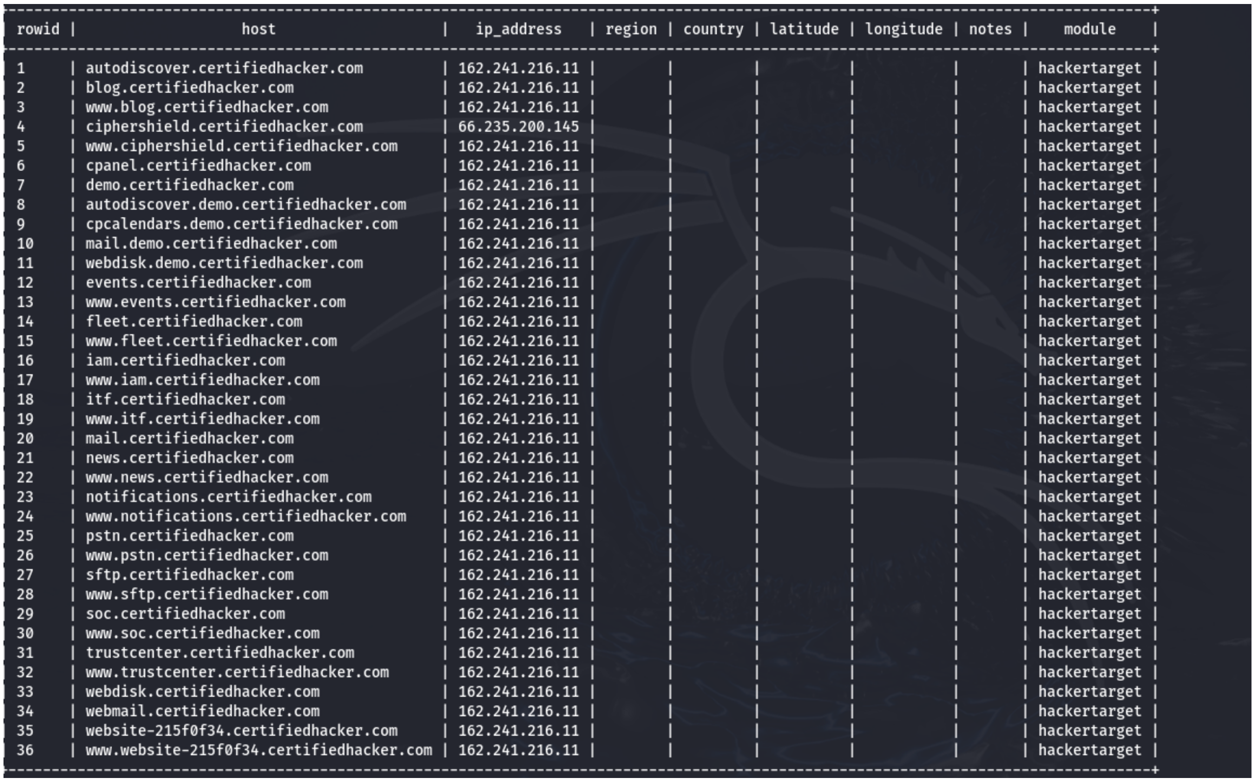


```
[recon-ng][Uttam] > modules load recon/domains-hosts/hackertarget
[recon-ng][Uttam][hackertarget] > info

      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
```



```
-------------------
CERTIFIEDHACKER.COM
-------------------
[*] Country: None
[*] Host: autodiscover.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: www.blog.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: ciphershield.certifiedhacker.com
[*] Ip_Address: 66.235.200.145
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: www.ciphershield.certifiedhacker.com
[*] Ip_Address: 162.241.216.11
[*] Latitude: None
[*] Longitude: None
```

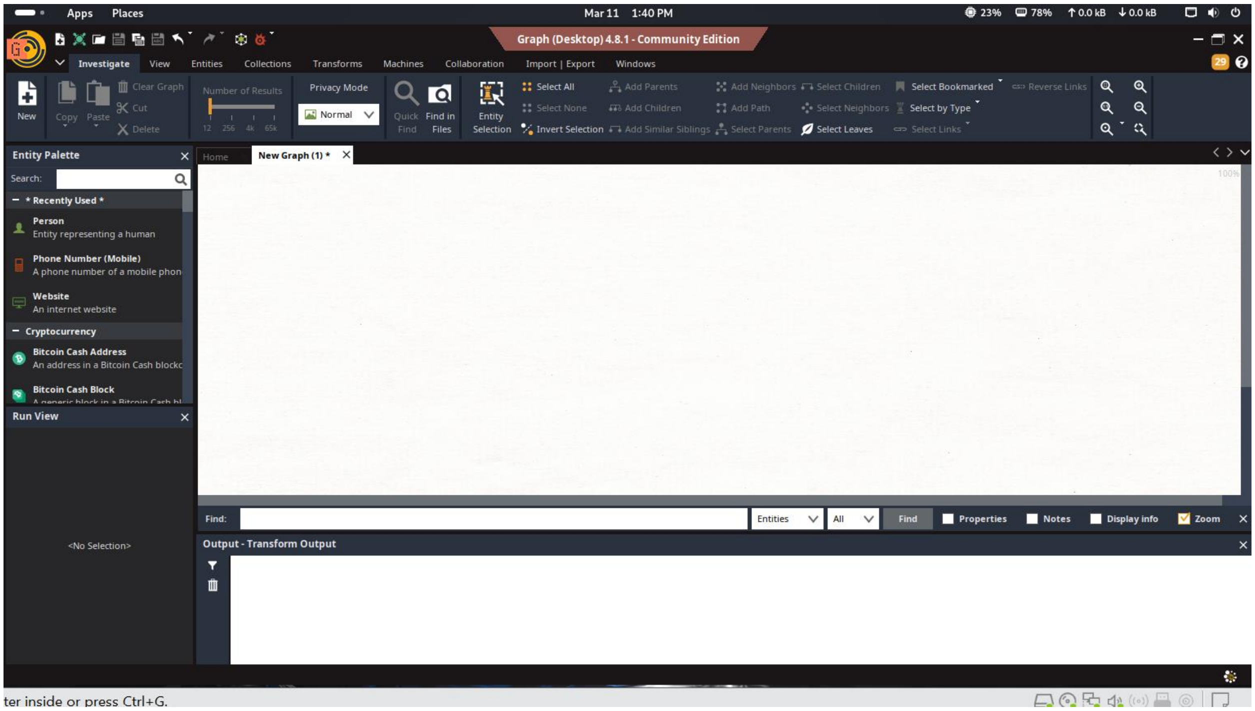
36 total (36 new) hosts found.



```
-----------------------------------------------------------------------------------------------------------------------------------+
rowid |                   host                   |  ip_address    | region | country | latitude | longitude | notes |    module    |
-----------------------------------------------------------------------------------------------------------------------------------+
1     | autodiscover.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | hackertarget |
2     | blog.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
3     | www.blog.certifiedhacker.com             | 162.241.216.11 |        |         |          |           |       | hackertarget |
4     | ciphershield.certifiedhacker.com         | 66.235.200.145 |        |         |          |           |       | hackertarget |
5     | www.ciphershield.certifiedhacker.com     | 162.241.216.11 |        |         |          |           |       | hackertarget |
6     | cpanel.certifiedhacker.com               | 162.241.216.11 |        |         |          |           |       | hackertarget |
7     | demo.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
8     | autodiscover.demo.certifiedhacker.com    | 162.241.216.11 |        |         |          |           |       | hackertarget |
9     | cpcalendars.demo.certifiedhacker.com     | 162.241.216.11 |        |         |          |           |       | hackertarget |
10    | mail.demo.certifiedhacker.com            | 162.241.216.11 |        |         |          |           |       | hackertarget |
11    | webdisk.demo.certifiedhacker.com         | 162.241.216.11 |        |         |          |           |       | hackertarget |
12    | events.certifiedhacker.com               | 162.241.216.11 |        |         |          |           |       | hackertarget |
13    | www.events.certifiedhacker.com           | 162.241.216.11 |        |         |          |           |       | hackertarget |
14    | fleet.certifiedhacker.com                | 162.241.216.11 |        |         |          |           |       | hackertarget |
15    | www.fleet.certifiedhacker.com            | 162.241.216.11 |        |         |          |           |       | hackertarget |
16    | iam.certifiedhacker.com                  | 162.241.216.11 |        |         |          |           |       | hackertarget |
17    | www.iam.certifiedhacker.com              | 162.241.216.11 |        |         |          |           |       | hackertarget |
18    | itf.certifiedhacker.com                  | 162.241.216.11 |        |         |          |           |       | hackertarget |
19    | www.itf.certifiedhacker.com              | 162.241.216.11 |        |         |          |           |       | hackertarget |
20    | mail.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
21    | news.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
22    | www.news.certifiedhacker.com             | 162.241.216.11 |        |         |          |           |       | hackertarget |
23    | notifications.certifiedhacker.com        | 162.241.216.11 |        |         |          |           |       | hackertarget |
24    | www.notifications.certifiedhacker.com    | 162.241.216.11 |        |         |          |           |       | hackertarget |
25    | pstn.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
26    | www.pstn.certifiedhacker.com             | 162.241.216.11 |        |         |          |           |       | hackertarget |
27    | sftp.certifiedhacker.com                 | 162.241.216.11 |        |         |          |           |       | hackertarget |
28    | www.sftp.certifiedhacker.com             | 162.241.216.11 |        |         |          |           |       | hackertarget |
29    | soc.certifiedhacker.com                  | 162.241.216.11 |        |         |          |           |       | hackertarget |
30    | www.soc.certifiedhacker.com              | 162.241.216.11 |        |         |          |           |       | hackertarget |
31    | trustcenter.certifiedhacker.com          | 162.241.216.11 |        |         |          |           |       | hackertarget |
32    | www.trustcenter.certifiedhacker.com      | 162.241.216.11 |        |         |          |           |       | hackertarget |
33    | webdisk.certifiedhacker.com              | 162.241.216.11 |        |         |          |           |       | hackertarget |
34    | webmail.certifiedhacker.com              | 162.241.216.11 |        |         |          |           |       | hackertarget |
35    | website-215f0f34.certifiedhacker.com     | 162.241.216.11 |        |         |          |           |       | hackertarget |
36    | www.website-215f0f34.certifiedhacker.com | 162.241.216.11 |        |         |          |           |       | hackertarget |
-----------------------------------------------------------------------------------------------------------------------------------+
```

- **Footprint a target using Maltego:**
  Here I am using Maltego in Kali Linus

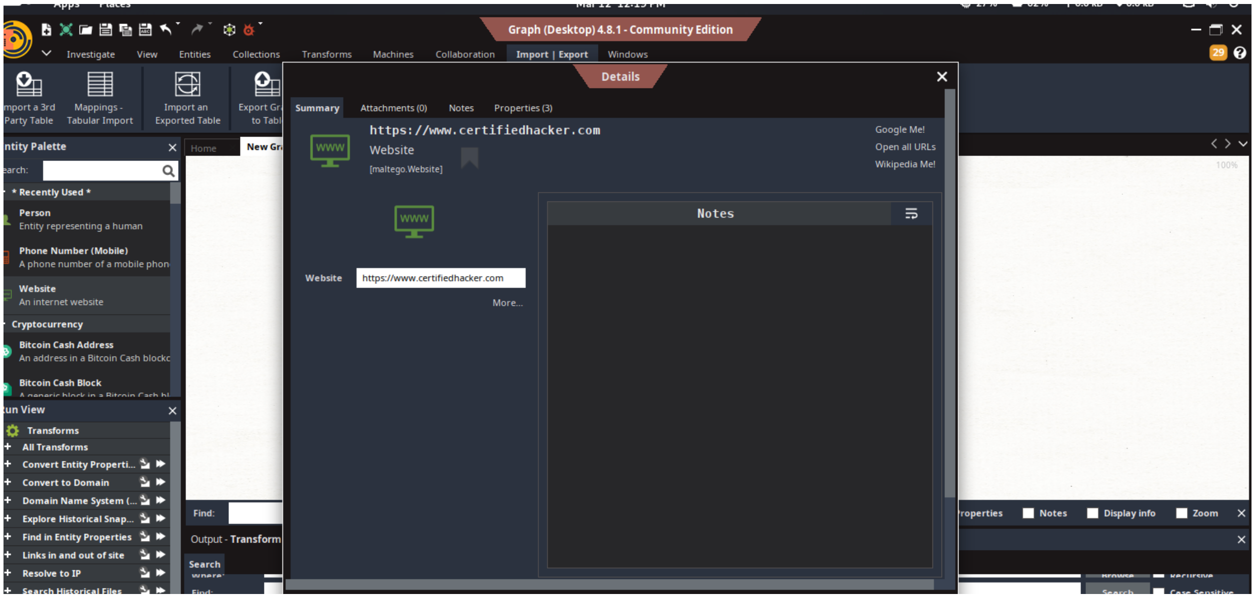
  Login kali linux in VMware then go to apps then information gathering then Maltego



Privacy Mode: Normal

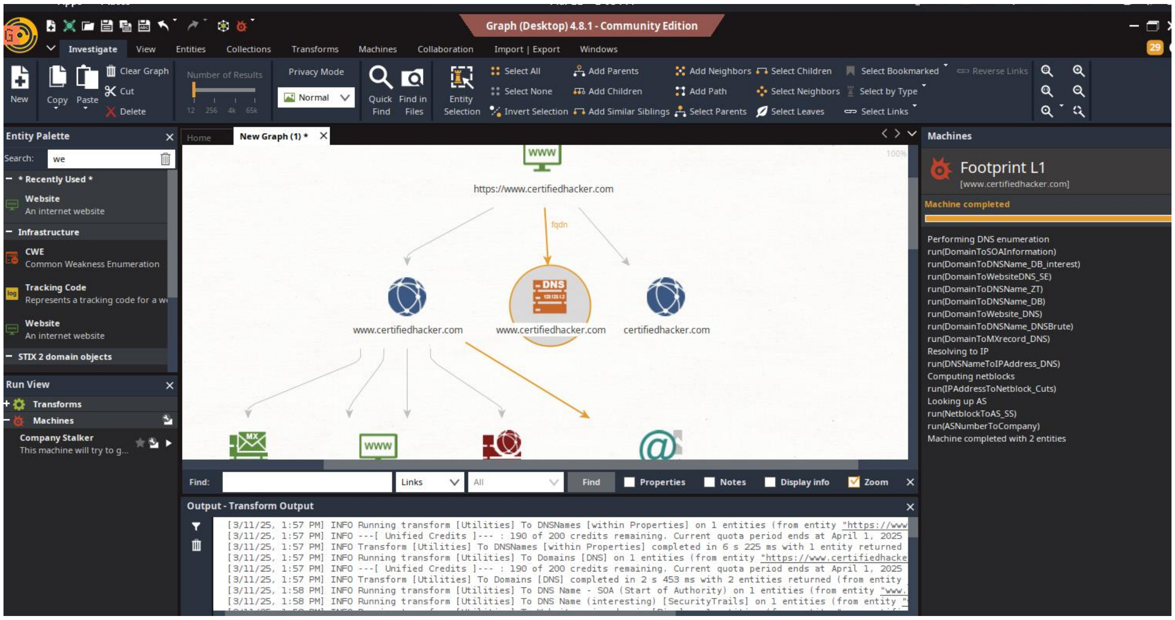
Target can be: Website, Personal, Domain, DNS, Location…etc

1$^{s}$ target is Websit https://www.certifiedhacker.com, searching Domains DNS



https://www.certifiedhacker.com
Website
[maltego.Website]

Website: https://www.certifiedhacker.com



```
Performing DNS enumeration
run(DomainToSOAInformation)
run(DomainToDNSName_DB_interest)
run(DomainToWebsiteDNS_SE)
run(DomainToDNSName_ZT)
run(DomainToDNSName_DB)
run(DomainToWebsite_DNS)
run(DomainToDNSName_DNSBrute)
run(DomainToMXrecord_DNS)
Resolving to IP
run(DNSNameToIPAddress_DNS)
Computing netblocks
run(IPAddressToNetblock_Cuts)
Looking up AS
run(NetblockToAS_SS)
run(ASNumberToCompany)
Machine completed with 2 entities
```

Output - Transform Output

```
[3/11/25, 1:57 PM] INFO Running transform [Utilities] To DNSNames [within Properties] on 1 entities (from entity "https://www
[3/11/25, 1:57 PM] INFO ---[ Unified Credits ]--- : 190 of 200 credits remaining. Current quota period ends at April 1, 2025
[3/11/25, 1:57 PM] INFO Transform [Utilities] To DNSNames [within Properties] completed in 6 s 225 ms with 1 entity returned
[3/11/25, 1:57 PM] INFO Running transform [Utilities] To Domains [DNS] on 1 entities (from entity "https://www.certifiedhacke
[3/11/25, 1:57 PM] INFO ---[ Unified Credits ]--- : 190 of 200 credits remaining. Current quota period ends at April 1, 2025
[3/11/25, 1:57 PM] INFO Transform [Utilities] To Domains [DNS] completed in 2 s 453 ms with 2 entities returned (from entity
[3/11/25, 1:58 PM] INFO Running transform [Utilities] To DNS Name - SOA (Start of Authority) on 1 entities (from entity "www.
[3/11/25, 1:58 PM] INFO Running transform [Utilities] To DNS Name (interesting) [SecurityTrails] on 1 entities (from entity "
```

Here Domain DNS are visible and can be checked mail also.

- **Vulnerabilities and loopholes identified:**
  **Recon-ng** : Host Name and IP are found, attackers can target the system for network scanning, exploitation, and attacks.

  **Recommendations for improving the security:**
  Disable unnecessary services running on the server, Hide IP addresses behind **load balancers or VPNs** and Implement Intrusion Detection/Prevention Systems **(IDS/IPS)**

- **Maltego** : DNS Detail found and Mail, attackers can use this information for **phishing, spoofing, reconnaissance, and direct attacks** on the organization's email infrastructure.

  **Recommendations for improving the security:**
  Restrict DNS zone transfers to trusted name servers only, Hide sensitive subdomains from public exposure, Enable logging for DNS queries and email server activity, Perform regular security audits on DNS configurations and email policies.