EPICODE

W10D1 - Pratica (2) PDF

Esercizio
Info Gathering

Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un **target a scelta**.

Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:

- Google, per la raccolta passiva delle info
- dmirty
- Recon-ng
- Maltego

EPICODE

W10D1 - Pratica (2) PDF

Esercizio
Info Gathering

Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato:

- Il target
- Le query utilizzate (dove applicabile)
- I moduli utilizzati (dove applicabile)
- I risultati ottenuti

Nome	Versione	Scopo	Note
Maltego	Community Edition 4.3.0		

Dmitry:

```
┌──(kali㉿kali)-[~]
└─$ dmitry -s -e epicode.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:35.207.141.200
HostName:epicode.com

Gathered Subdomain information for epicode.com
---------------------------------------
Searching Google.com:80 ...
HostName:www.epicode.com
HostIP:35.207.141.200
HostName:instituteoftechnology.epicode.com
HostIP:35.207.141.200
HostName:learn.epicode.com
HostIP:108.157.194.86
Searching Altavista.com:80 ...
Found 3 possible subdomain(s) for host epicode.com, Searched 0 pages containing 0 results

Gathered E-Mail information for epicode.com
---------------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host epicode.com, Searched 0 pages containing 0 results

All scans completed, exiting
```

```
┌──(kali㉿kali)-[~]
└─$ dmitry -s -p epicode.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:35.207.141.200
HostName:epicode.com

Gathered Subdomain information for epicode.com
---------------------------------------
Searching Google.com:80 ...
HostName:www.epicode.com
HostIP:35.207.141.200
HostName:instituteoftechnology.epicode.com
HostIP:35.207.141.200
HostName:learn.epicode.com
HostIP:108.157.194.48
Searching Altavista.com:80 ...
Found 3 possible subdomain(s) for host epicode.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 35.207.141.200
---------------------------------------

 Port          State

21/tcp         open
25/tcp         open
80/tcp         open
110/tcp        open
143/tcp        open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting

┌──(kali㉿kali)-[~]
└─$
```

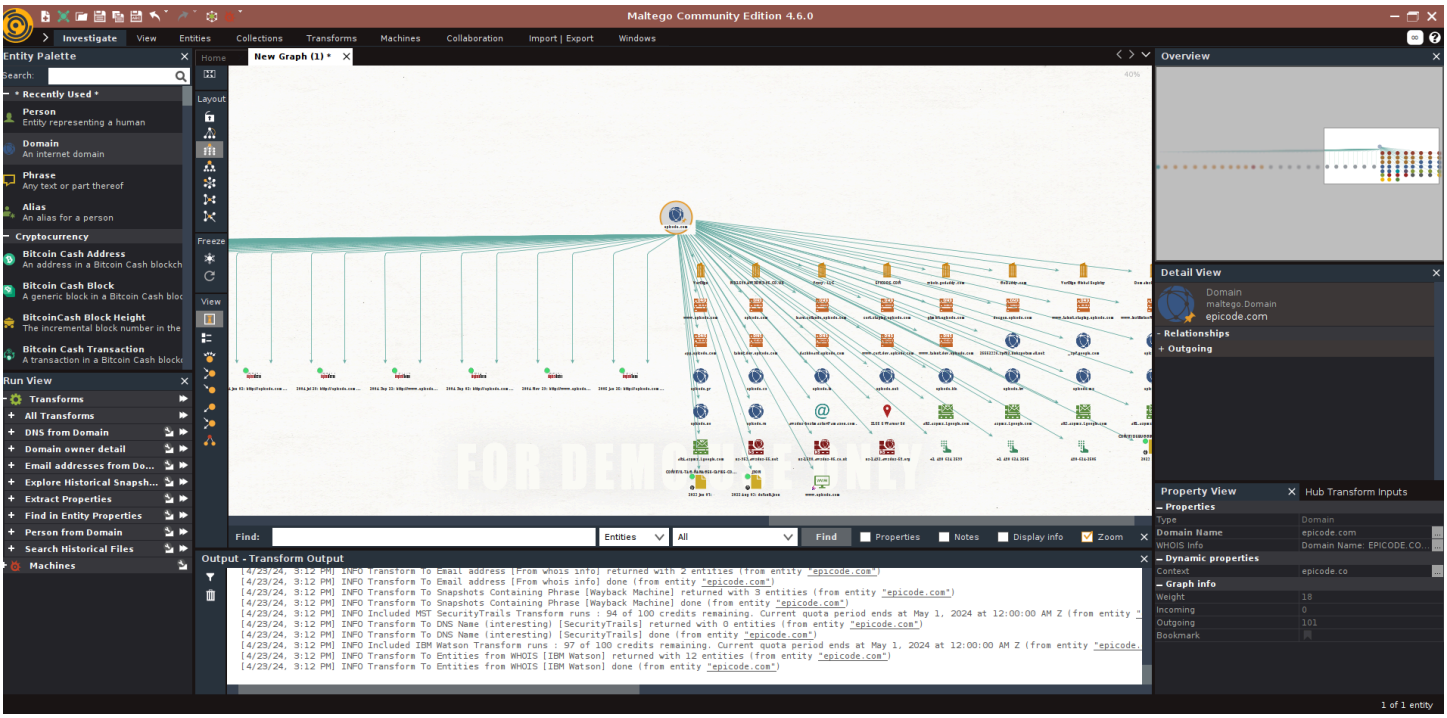
Recon-ng

```
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    epicode.com                                            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][Test][interesting_files] > run
[*] http://epicode.com:80/robots.txt => 200. 'robots.txt' found!
[*] http://epicode.com:80/sitemap.xml => 200. 'sitemap.xml' found!
[*] http://epicode.com:80/sitemap.xml.gz => 404
[*] http://epicode.com:80/crossdomain.xml => 404
[*] http://epicode.com:80/phpinfo.php => 403
[*] http://epicode.com:80/test.php => 404
[*] http://epicode.com:80/elmah.axd => 404
[*] http://epicode.com:80/server-status => 403
[*] http://epicode.com:80/jmx-console/ => 403
[*] http://epicode.com:80/admin-console/ => 404
[*] http://epicode.com:80/web-console/ => 404
[*] 2 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/workspaces/Test/'
[recon-ng][Test][interesting_files] > options set SOURCE epicode.com
```

```
--------
EPICODE.COM
--------
[*] Country: None
[*] Host: epicode.com
[*] Ip_Address: 35.207.141.200
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: www.cert.epicode.com
[*] Ip_Address: 99.84.238.109
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: learn.dev.epicode.com
[*] Ip_Address: 108.138.246.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: www.learn.dev.epicode.com
[*] Ip_Address: 108.138.246.2
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------------
[*] Country: None
[*] Host: talent.dev.epicode.com
[*] Ip_Address: 99.84.66.13
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
+--------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| rowid  |         host          |   ip_address  | region | country | latitude | longitude | notes |    module   |
+--------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+
| 1      | epicode.com           | 35.207.141.200|        |         |          |           |       | hackertarget |
| 2      | www.cert.epicode.com  | 99.84.238.109 |        |         |          |           |       | hackertarget |
| 3      | learn.dev.epicode.com | 108.138.246.18|        |         |          |           |       | hackertarget |
| 4      | www.learn.dev.epicode.com | 108.138.246.2 |        |         |          |           |       | hackertarget |
| 5      | talent.dev.epicode.com| 99.84.66.13   |        |         |          |           |       | hackertarget |
| 6      | docgen.epicode.com    | 52.59.97.94   |        |         |          |           |       | hackertarget |
+--------+-----------------------+---------------+--------+---------+----------+-----------+-------+-------------+

[*] 6 rows returned
[recon-ng][default][hackertarget] >
```

Maltigo



Trovati, sottodomini, IP, varie pagine collegate a epicode.com e fatto scan delle porte sul server epicode.com