ESERCITAZIONE W10D1(2)

EPICODE

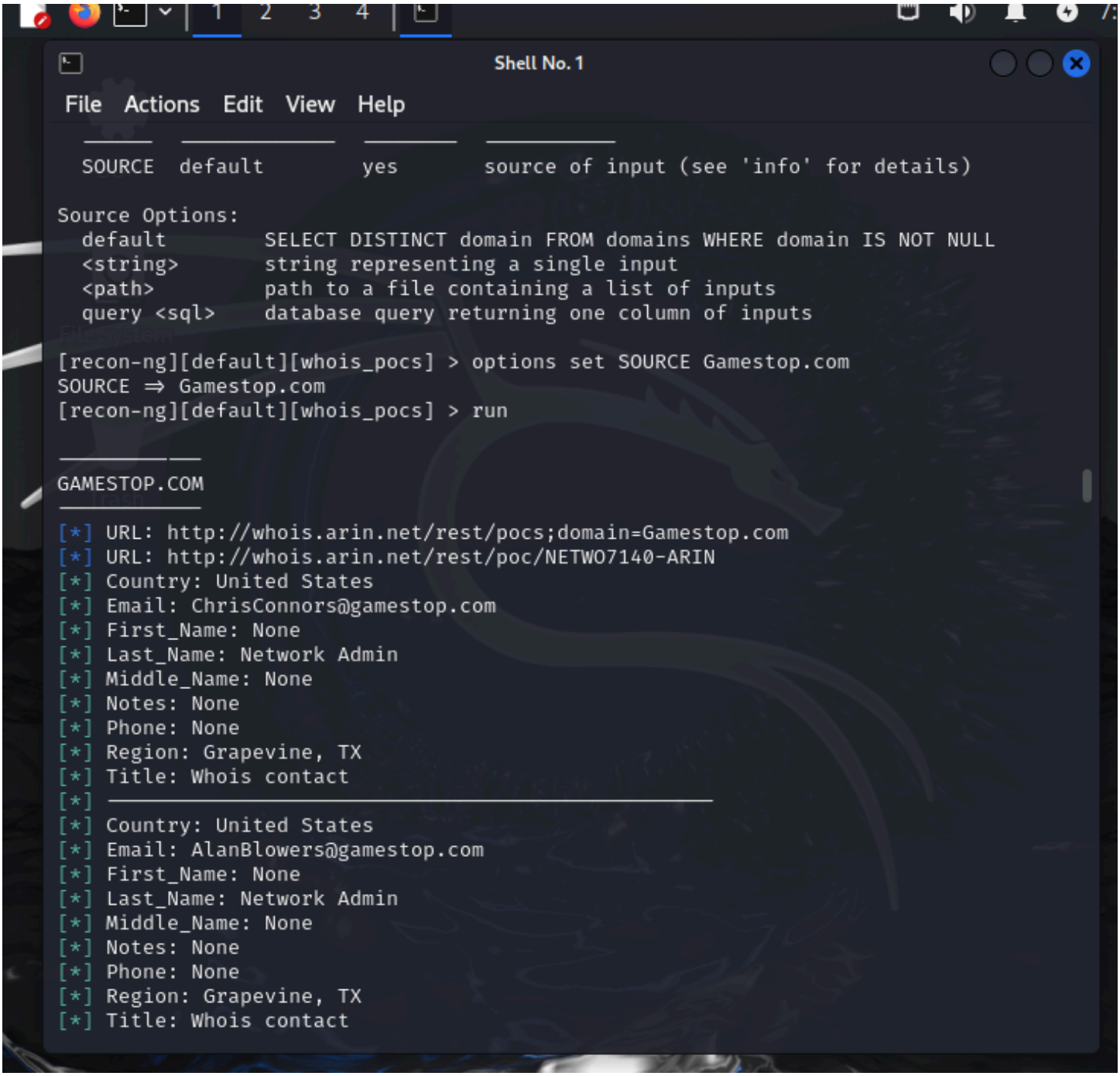
Esercizio
Info Gathering

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

Recon-ng


Shell No. 1
File Actions Edit View Help
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][default][whois_pocs] > options set SOURCE Gamestop.com
SOURCE ⇒ Gamestop.com
[recon-ng][default][whois_pocs] > run
GAMESTOP.COM
[*] URL: http://whois.arin.net/rest/pocs;domain=Gamestop.com
[*] URL: http://whois.arin.net/rest/poc/NETWO7140-ARIN
[*] Country: United States
[*] Email: ChrisConnors@gamestop.com
[*] First_Name: None
[*] Last_Name: Network Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact
[*]
[*] Country: United States
[*] Email: AlanBlowers@gamestop.com
[*] First_Name: None
[*] Last_Name: Network Admin
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Grapevine, TX
[*] Title: Whois contact