

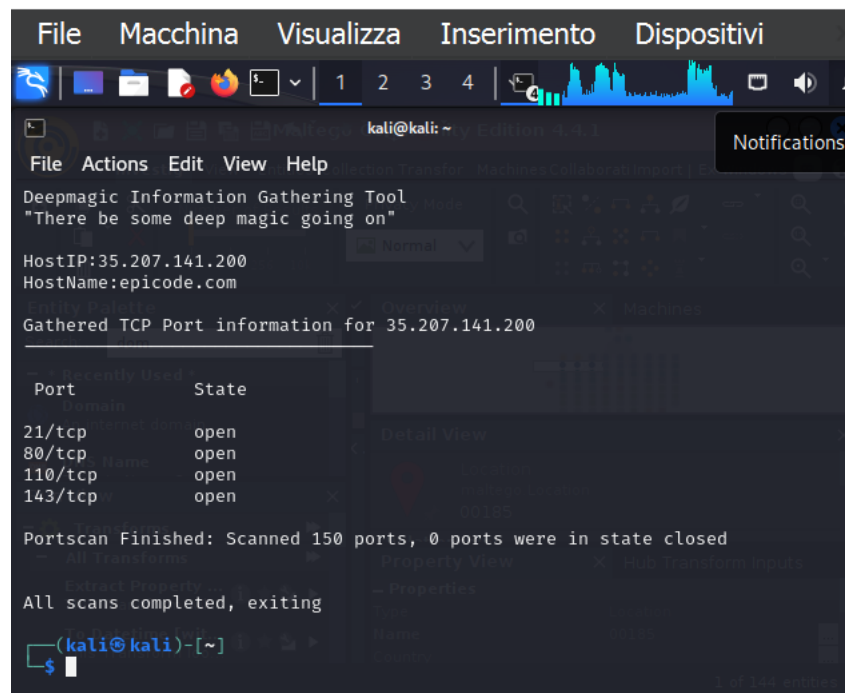
Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali:

Google, per la raccolta passiva delle info

Dmitry

Recon-ng

Maltego



```
File Macchina Visualizza Inserimento Dispositivi
kali@kali: ~
File Actions Edit View Help
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:35.207.141.200
HostName:epicode.com
Gathered TCP Port information for 35.207.141.200
Port State
21/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)-[~]
$
```



```
File Actions Edit View Help
kali@kali: ~
(kali@kali)-[~]
$ dmitry -p www.uniroma1.it
Deepmagic Information Gathering Tool
"There be some deep magic going on"
HostIP:151.100.101.140
HostName:www.uniroma1.it
Gathered TCP Port information for 151.100.101.140
Port State
80/tcp open
Portscan Finished: Scanned 150 ports, 0 ports were in state closed
All scans completed, exiting
(kali@kali)-[~]
$
```



```
File Actions Edit View Help

- inurl:robots.txt ext:txt
- inurl:elmah.axd ext:axd intitle:"Error log for"
- inurl:server-status "Apache Status"

[recon-ng][default][interesting_files] > SOURCE
[!] Invalid command: SOURCE.
[recon-ng][default][interesting_files] > options set SOURCE uniroma1.it
SOURCE => uniroma1.it
[recon-ng][default][interesting_files] > run
[*] http://uniroma1.it:80/robots.txt => 200. 'robots.txt' found!
[*] http://uniroma1.it:80/sitemap.xml => 200. 'sitemap.xml' found!
[*] http://uniroma1.it:80/sitemap.xml.gz => 404
[*] http://uniroma1.it:80/crossdomain.xml => 404
[*] http://uniroma1.it:80/phpinfo.php => 404
[*] http://uniroma1.it:80/test.php => 200. 'test.php' found but unverified.
[*] http://uniroma1.it:80/elmah.axd => 404
[*] http://uniroma1.it:80/server-status => 403 here in state closed
[*] http://uniroma1.it:80/jmx-console/ => 404
[*] http://uniroma1.it:80/admin-console/ => 404
[*] http://uniroma1.it:80/web-console/ => 404
[*] 2 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/workspaces/default/'
[recon-ng][default][interesting_files] > |
```

