ESERCIZIO

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:

1. Google, per la raccolta passiva delle info
2. dmirty
3. Recon-ng
4. Maltego

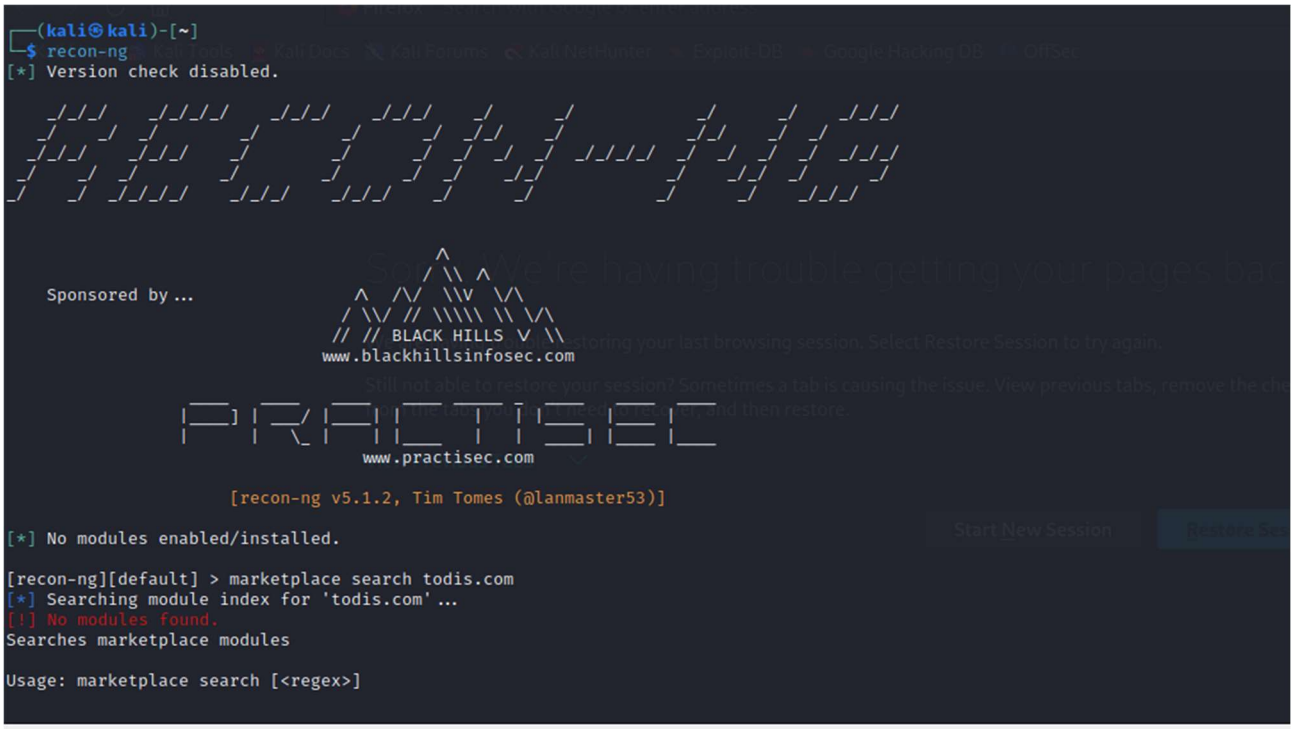
Alla fine dell'analisi, lo studente dovrà produrre un piccolo report dove indicherà per ogni tool utilizzato: Il target Le query utilizzate (dove applicabile) I moduli utilizzati (dove applicabile) I risultati ottenuti.

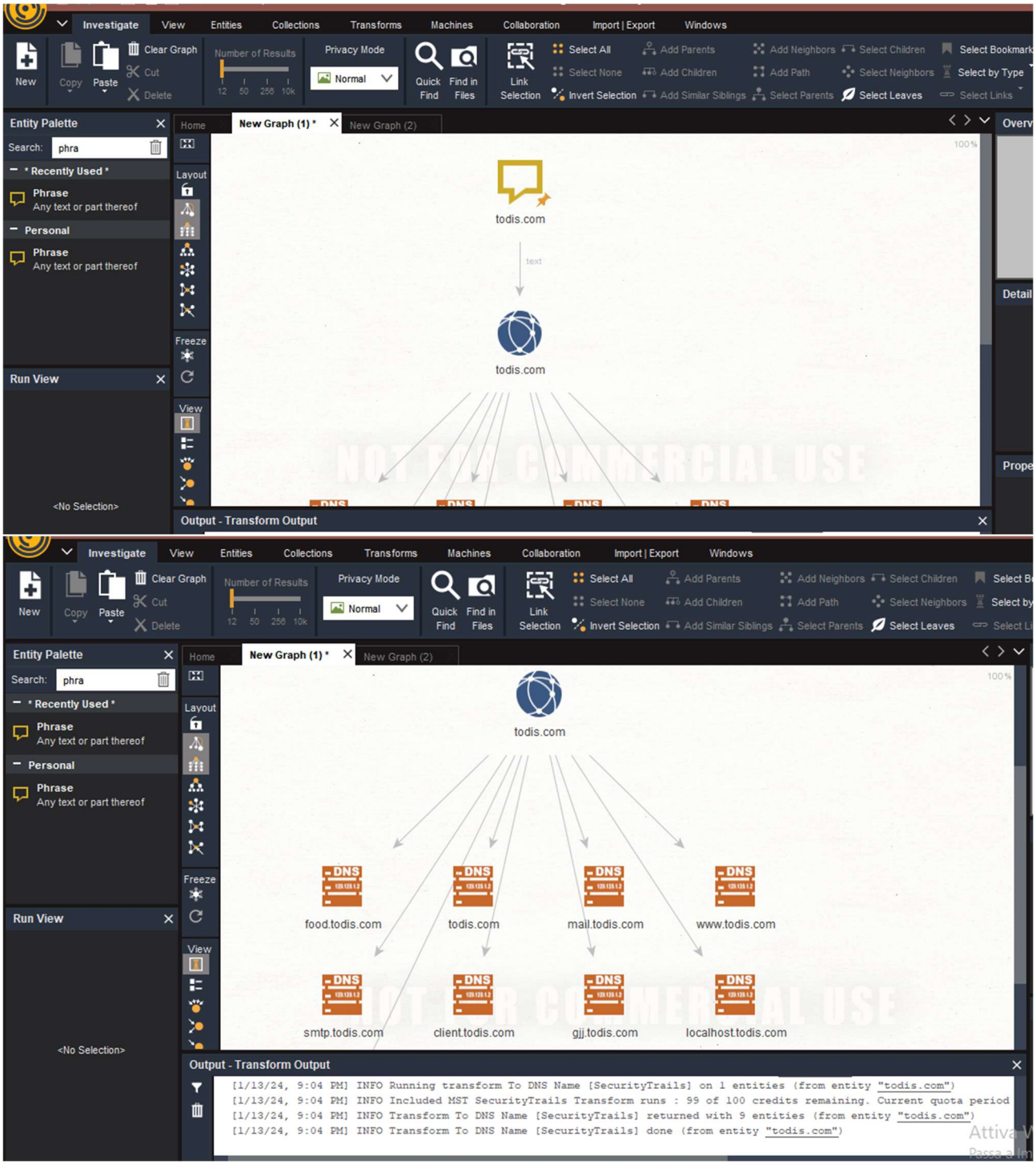
NOME	VERSIONE	SCOPO	NOTE
DMIRTY	1.109.1	GATHERING	
RECON-NG	5.1.2	GATHERING	
MALTEGO	COMMUNITY 4.4.1	GATHERING	

```
└─$ dmitry -i todis.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:199.59.243.225
HostName:todis.com

Gathered Inet-whois information for 199.59.243.225
---------------------------------

inetnum:        199.54.0.0 - 199.66.127.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
```

```
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ----------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ----------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2022-04-14T12:57:42Z
last-modified:  2022-04-14T12:57:42Z
source:         RIPE

role:           Internet Assigned Numbers Authority
```

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

HostIP:199.59.243.225
HostName:todis.com

Gathered Inic-whois information for todis.com
---------------------------------------------
   Domain Name: TODIS.COM
   Registry Domain ID: 2540400762_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namebright.com
   Registrar URL: http://www.NameBright.com
   Updated Date: 2023-06-22T20:15:38Z
   Creation Date: 2020-06-20T18:35:13Z
   Registry Expiry Date: 2024-06-20T18:35:13Z
   Registrar: TurnCommerce, Inc. DBA NameBright.com
   Registrar IANA ID: 1441
   Registrar Abuse Contact Email: support@namebright.com
   Registrar Abuse Contact Phone: 17204960020
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.BODIS.COM
   Name Server: NS2.BODIS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-01-13T18:15:25Z <<<
```


┌──(kali㉿kali)-[~]
└─$ recon-ng
[*] Version check disabled.
Sponsored by ...
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.
[recon-ng][default] > marketplace search todis.com
[*] Searching module index for 'todis.com' ...
[!] No modules found.
Searches marketplace modules
Usage: marketplace search [<regex>]


Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
New
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12 50 256 10k
Privacy Mode
Normal
Quick Find
Find in Files
Link Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Select Bookmarks
Select by Type
Select Links
Entity Palette
Search:
phra
* Recently Used *
Phrase
Any text or part thereof
Personal
Phrase
Any text or part thereof
Run View
<No Selection>
Home
New Graph (1) *
New Graph (2)
Layout
Freeze
View
todis.com
text
todis.com
Output - Transform Output
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
New
Copy
Paste
Clear Graph
Cut
Delete
Number of Results
12 50 256 10k
Privacy Mode
Normal
Quick Find
Find in Files
Link Selection
Select All
Select None
Invert Selection
Add Parents
Add Children
Add Similar Siblings
Add Neighbors
Add Path
Select Parents
Select Children
Select Neighbors
Select Leaves
Entity Palette
Search:
phra
* Recently Used *
Phrase
Any text or part thereof
Personal
Phrase
Any text or part thereof
Run View
<No Selection>
Home
New Graph (1) *
New Graph (2)
Layout
Freeze
View
todis.com
food.todis.com
todis.com
mail.todis.com
www.todis.com
smtp.todis.com
client.todis.com
gjj.todis.com
localhost.todis.com
Output - Transform Output
[1/13/24, 9:04 PM] INFO Running transform To DNS Name [SecurityTrails] on 1 entities (from entity "todis.com")
[1/13/24, 9:04 PM] INFO Included MST SecurityTrails Transform runs : 99 of 100 credits remaining. Current quota period
[1/13/24, 9:04 PM] INFO Transform To DNS Name [SecurityTrails] returned with 9 entities (from entity "todis.com")
[1/13/24, 9:04 PM] INFO Transform To DNS Name [SecurityTrails] done (from entity "todis.com")