W10D2-D3

GOOGLE HACKING

La traccia

Istruzioni:

1. Aprire un browser web e accedere a Google.

2. Utilizzare i seguenti comandi di Google Hacking per raccogliere informazioni sul sito web:
   - "site:nome-del-sito.com" per visualizzare tutte le pagine indicizzate di quel sito.
   - "inurl:nome-del-sito.com" per visualizzare tutte le pagine con l'URL contenente il nome del sito.
   - "intext:'parola chiave' site:nome-del-sito.com" per visualizzare tutte le pagine che contengono la parola chiave specificata nel testo del sito.
   - "filetype:estensione site:nome-del-sito.com" per visualizzare tutti i file con l'estensione specificata presenti sul sito.

3. Utilizzare i risultati per identificare eventuali informazioni sensibili o vulnerabilità presenti sul sito.

4. Utilizzare queste informazioni per valutare la sicurezza del sito e prendere le misure necessarie per proteggere le informazioni sensibili.

La traccia

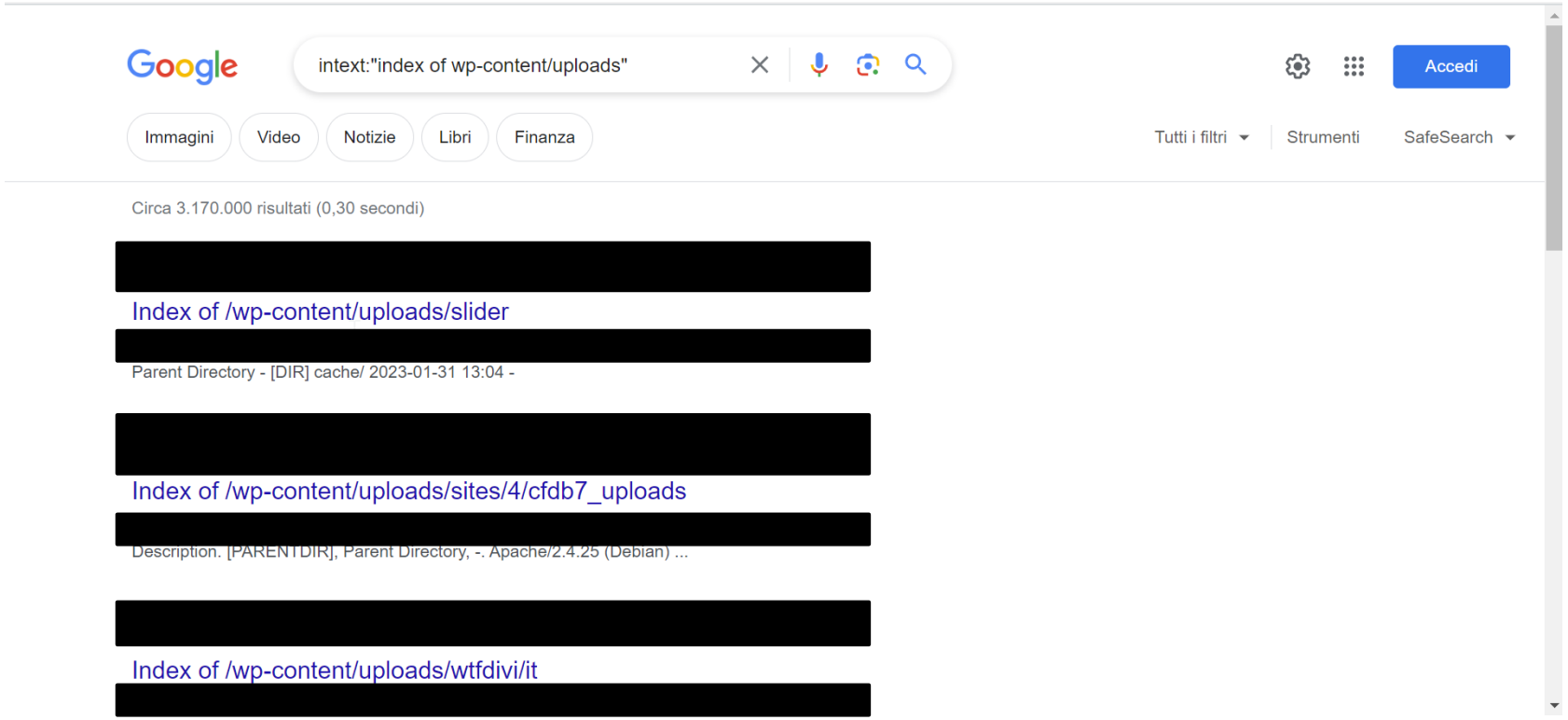
Nell'esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un **target a scelta**.

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

Ricerca del sito tramite google hacking

Inserendo la seguente ricerca ho avuto la possibilità di accedere alle directory pubbliche dei siti che compaiono nei risultati.



1) Dmirty

Prendendone uno in esame ho deciso di usare gli strumenti studiati per recuperare più info possibili.
Il primo è dmirty

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

HostIP:94.136.29.72
HostName:agfeo-service.at

Gathered Inet-whois information for 94.136.29.72
---------------------------------


inetnum:        94.136.29.0 - 94.136.29.255
netname:        KN-FTTH
descr:          kapper.net FTTH Block
country:        AT
admin-c:        KNET2-RIPE
tech-c:         KNET2-RIPE
status:         ASSIGNED PA
mnt-by:         KAPCOM-RIPE-MNT
created:        2010-05-25T23:24:48Z
last-modified:  2010-05-25T23:24:48Z
source:         RIPE

role:           kapper.net admin
ress:        Alserbachstrasse 11/6
address:        A-1090 Vienna, Austria
mnt-by:         KAPCOM-RIPE-MNT
abuse-mailbox:  abuse@kapper.net
remarks:        in case you do not know whom you
remarks:        would like to send an e-mail
remarks:        send it to the sysadmin mailbox.
admin-c:        HK617-RIPE
tech-c:         HK617-RIPE
tech-c:         MM10165-RIPE
tech-c:         SG9459-RIPE
nic-hdl:        KNET2-RIPE
created:        2005-03-11T18:05:36Z
last-modified:  2022-11-10T09:49:05Z
:         RIPE # Filtered

% Information related to '94.136.0.0/19AS48943'
```

```
route:          94.136.0.0/19
descr:          AT-KAPPERNET-20080717 PA
descr:          KAPPER NETWORK-COMMUNICATIONS GmbH
origin:         AS48943
mnt-by:         KAPCOM-RIPE-MNT
created:        2010-01-21T11:40:35Z
last-modified:  2011-09-30T13:47:13Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.109.1 (ABERDEEN)


Gathered Inic-whois information for agfeo-service.at
---------------------------------


domain:         agfeo-service.at
registrar:      INWX GmbH ( https://nic.at/registrar/453 )
registrant:     FJUS12562225-NICAT
tech-c:         FJUS12562225-NICAT
nserver:        ns1.justnet.at
nserver:        ns2.justnet.at
nserver:        ns3.justnet.at
nserver:        ns4.justnet.at
changed:        20200218 16:19:04
AT-DOM

personname:     Just Stefan
organization:   Franz Just und Soehne GmbH u. Co KG
street address: Koloniestrasse 33
postal code:    1210
city:           Wien
country:        Austria
phone:          <data not disclosed>
fax-no:         <data not disclosed>
e-mail:         <data not disclosed>
nic-hdl:        FJUS12562225-NICAT
changed:        20200214 13:14:01
source:         AT-DOM

Gathered Netcraft information for agfeo-service.at
---------------------------------


Retrieving Netcraft.com information for agfeo-service.at
Netcraft.com Information gathered

Gathered Subdomain information for agfeo-service.at
---------------------------------
```

Grazie a questo tool riesco ad ottenere info in merito al server dove viene hostato il sito, non vengono rilevati sottodomini.

2) Recon-ng

Ho usato recon-ng per trovare dei file sul sito che sono stati salvati su kali.

```
[recon-ng][default][profiler] > back
[recon-ng][default] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules ...
[recon-ng][default] > modules load discovery/info_disclosure/interesting_files
[recon-ng][default][interesting_files] > options set SOURCE agfeo-service.at
SOURCE ⇒ agfeo-service.at
[recon-ng][default][interesting_files] > run
[*] http://agfeo-service.at:80/robots.txt ⇒ 200. 'robots.txt' found!
[*] http://agfeo-service.at:80/sitemap.xml ⇒ 200. 'sitemap.xml' found!
[*] http://agfeo-service.at:80/sitemap.xml.gz ⇒ 404
[*] http://agfeo-service.at:80/crossdomain.xml ⇒ 404
[*] http://agfeo-service.at:80/phpinfo.php ⇒ 404
[*] http://agfeo-service.at:80/test.php ⇒ 404
[*] http://agfeo-service.at:80/elmah.axd ⇒ 404
[*] http://agfeo-service.at:80/server-status ⇒ 404
[*] http://agfeo-service.at:80/jmx-console/ ⇒ 404
[*] http://agfeo-service.at:80/admin-console/ ⇒ 404
[*] http://agfeo-service.at:80/web-console/ ⇒ 404
[*] 2 interesting files found.
[*] Files downloaded to '/home/kali/.recon-ng/workspaces/default/'
[recon-ng][default][interesting_files] >
```

3) Maltego

Con maltego ho la possibilità di recuperare info a 360 in base al dominio: persone, hosts, ip , sottodomini ecc.