Laboratorio #2

Seguridad informática

```
disse_plaintiff.pdf
https://static.reuters.com/resources/media/editorial/20180102/fdicvpwc.pdf
http://static.reuters.com/resources/media/editorial/20130719/CNH20130719SC.pd
f
http://static.reuters.com/resources/media/editorial/20120420/20120420SC.pdf
https://static.reuters.com/resources/media/editorial/20201223/12232020nyjudge
s.pdf
https://static.reuters.com/resources/media/editorial/20200916/09162020postal_
doj.pdf
http://static.reuters.com/resources/media/editorial/20140725/140725_Simplifie
d.pdf
https://static.reuters.com/resources/media/editorial/20180131/interceptpharma
.pdf
http://static.reuters.com/resources/media/editorial/20120713/20120713SC.pdf
https://static.reuters.com/resources/media/editorial/20210211/02102021faceboo
k.pdf
[+] Done!

┌──(kali㊙kali)-[~]
└─$ exiftool -r /temp/archivos/* | egrep -i "Author|Creator|Email|Producer|Te
mplate" | sort -u
Error: File not found - /temp/archivos/*

┌──(kali㊙kali)-[~]
└─$
```

"the quieter you become, the more you are able to hear"

File   Actions   Edit   View   Help

```
    -f, --file <file>      Read subdomains from this file to perform brute force
. (Takes priority over default dns.txt)
    -u, --update <a|g|r|z>
                           Update the file specified with the -f switch with val
id subdomains.
         a (all)           Update using all results.
         g                 Update using only google scraping results.
         r                 Update using only reverse lookup results.
         z                 Update using only zonetransfer results.
    -r, --recursion        Recursion on subdomains, brute force all discovered s
ubdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
    -d, --delay <value>   The maximum value of seconds to wait between whois qu
eries, the value is defined randomly, default: 3s.
    -w, --whois            Perform the whois queries on c class network ranges.
                           **Warning**: this can generate very large netranges
and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
    -e, --exclude <regexp>
                           Exclude PTR records that match the regexp expression
from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
    -o --output <file>    Output in XML format. Can be imported in MagicTree (w
ww.gremwell.com)

  ┌──(kali㉿kali)-[~]
  └─$ ▊
```

"the quieter you become, the more you are able to hear"

```
ns-emea-2.thomsonreuters.net.          246      IN    A      155.46.154.1
2
ns-amers-3.thomsonreuters.net.         97       IN    A      155.46.152.1
2
ns-amers-1.thomsonreuters.net.         112      IN    A      155.46.165.1
33
ns-emea-1.thomsonreuters.net.          300      IN    A      155.46.156.1
2


Mail (MX) Servers:
───────────────────

mxa-00160c04.gslb.pphosted.com.        30       IN    A      205.220.167.
179
mxb-00160c04.gslb.pphosted.com.        30       IN    A      205.220.167.
179


Trying Zone Transfers and getting Bind Versions:
────────────────────────────────────────────────
```

"the quieter you become, the more you are able to hear"

kali@kali: ~

File Actions Edit View Help

Netcraft.com Information gathered

Gathered Subdomain information for reuters.com
————————————————————————————————

Searching Google.com:80 ...
HostName:www.reuters.com
HostIP:52.84.150.42
HostName:pictures.reuters.com
HostIP:13.43.68.19
HostName:jp.reuters.com
HostIP:186.15.236.139
Searching Altavista.com:80 ...
Found 3 possible subdomain(s) for host reuters.com, Searched 0 pages containing 0 results

Gathered E-Mail information for reuters.com
————————————————————————————————

Searching Google.com:80 ...
misha.wolf@reuters.com
News@reuters.com
Searching Altavista.com:80 ...
Found 2 E-Mail(s) for host reuters.com, Searched 0 pages containing 0 results

All scans completed, exiting

┌──(kali㉿kali)-[~]
└─$ ▮

"the quieter you become, the more you are able to hear"