

OSSTMM - MODULE 1

Approach

Created on 05 November 2020 | Our Reference: OWASP top10 Booklet.docx | Version: 1.8

Sensitivity: PUBLIC

proximus

This page intentionally left blank

2020 - 2021

Summary

1	Presentation	4
2	Passive information gathering with third party tools.....	6
3	Social media and documents	12
4	How to protect yourself.....	20

5	Conclusion.....	21
----------	------------------------	-----------



2020 - 2021

1 Presentation

One of the first stage of a penetration test is the information gathering phase. This phase helps pentesters producing a strategic plan to attack a target. It involves finding, selecting and acquiring data from publicly available sources and analyzing it to produce actionable intelligence. This phase is also often referred as OSINT which stands for Open Source INTElligence. Open source means here overt (opposed to clandestine and covert sources) and has no link with open-source software.

The information gathering phase allows pentesters to determine various entry points into an organization (either physical, electronic or human). Many companies fail to control what information is publicly available about them and how hackers can use this information. More importantly, many employees leak sensitive information about them or about their company, giving attackers a fast track to the company's system.

Passive information gathering s distinguished from active one.

The first meaning of passive OSINT is to have no interaction with the target. That means sending no traffic to the organization and using archives or third party instead. This method is limited and used only when explicitly asked by the organization. That is why semi passive OSINT is more used in OSSTMM tests.

With the semi-passive OSINT, the goal is to profile the target using methods that would appear like normal traffic and behavior for the organization. It does not include in depth domain analysis or brute force. Other information sources like metadata found in documents are useful during this step.

Active OSINT on the other hand should appear like malicious or at least suspicious for the target as it involves mapping the network infrastructure, full port scan, vulnerability scan, etc.

The first two modules focus on methods used to perform both passive and active information gathering. It is however not exhaustive as there is a very large number of information sources and as many tools to collect data from them. This document will only give the most common tools and technics to gather information about a target.



Be aware that information gathering is not an exact science and that collected information might be outdated or false (old website or disinformation to cloud the issue for instance). Another challenge is to extract the right amount of data and not to be overloaded.

See also HUMINT, SIGINT, GEOINT and MASINT, which are other information gathering technics.



2 Passive information gathering with third party tools

Google Dorks

Google dorks are search strings that make use of advanced search operators to find information that are not always readily available on a website.

This dorks can be used to find vulnerabilities on websites or hidden information such as usernames and passwords, sensitive documents, email lists, etc.

Useful links:

- www.exploit-db.com/google-hacking-database/

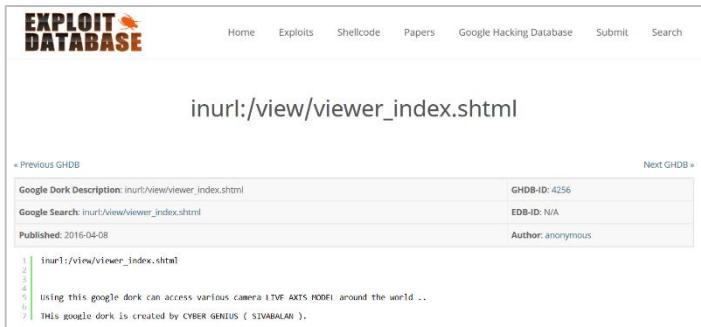
Hands on!

Use Google Dorks to find an online camera system.

Hands on!

ANSWERS

First, go on the google hacking database and search for 'camera'.

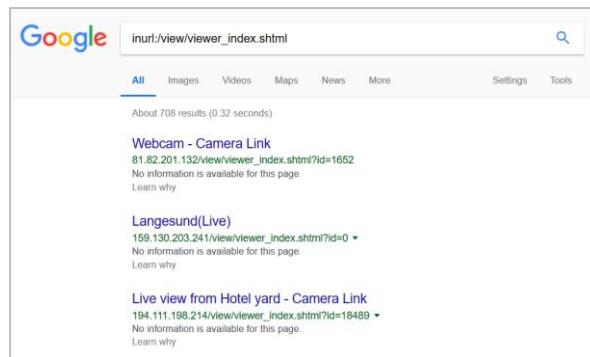


The screenshot shows a search results page from the Exploit Database's Google Hacking Database. The search query entered is "inurl:/view/viewer_index.shtml". The results table includes columns for Google Dark Description, GHDB-ID, EDB-ID, and Author. One result is shown with the following details:

Google Dark Description: inurl:/view/viewer_index.shtml	GHDB-ID: 4256
Google Search: inurl:/view/viewer_index.shtml	EDB-ID: N/A
Published: 2016-04-08	Author: anonymous

Below the table, there is a note: "Using this google dork can access various camera LIVE AXTS MODEL around the world .." and "This google dork is created by CYBER GENIUS (SIVABALAN)."

Google gives the following results when using the previous dork:



Google search results for "inurl:/view/viewer_index.shtml". The results show three links:

- Webcam - Camera Link**
81.82.201.132/view/viewer_index.shtml?id=1652
No information is available for this page.
[Learn why](#)
- Langesund(Live)**
159.130.203.241/view/viewer_index.shtml?id=0
No information is available for this page.
[Learn why](#)
- Live view from Hotel yard - Camera Link**
194.111.198.214/view/viewer_index.shtml?id=18489
No information is available for this page.
[Learn why](#)

Click on the first link to get access to a town camera:



Note: Google Dorks can also be used for Domain Name discovery, using the “site” dorks:

- First search for “**site:telindus.lu -site:www.telindus.lu**”
- Then add the domain you want to remove from results with the “-site” dorks.

Shodan

Shodan is a search engine for internet-connected devices. It works by scanning the entire Internet and by parsing the banners that it collects. It can give us

Fusion For Energy, OSSTMM - MODULE 1,

Proximus Luxembourg S.A. | 18, rue du Puits Romain - Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 - 1 | F +352 45 09 11

www.telindus.lu VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO

information about the type of web server that is running on a machine along with the version. It is important to notice that Shodan does not use nmap (see later) as scanner but its own scanner, which could give different results.

Useful links:

- www.shodan.io

Hands on!

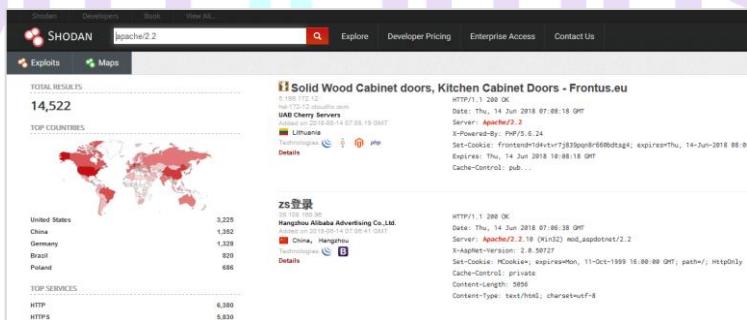
Use Shodan to find Apache 2.2 servers located in France.

Hands on!

ANSWERS

Filters require a Shodan account, but some useful information are available without using those filters, searching for example with:

Apache/2.2



With a free account, it is possible to perform filtered search:



Apache country:"FR"

TOTAL RESULTS: 1,067,110

TOP COUNTRIES:

- France: 1,067,110

TOP CITIES:

City	Count
Paris	73,054
Bordeaux	25,293
Strasbourg	16,533
Toulouse	15,092
Lyon	5,576

TOP SERVICES:

Service	Count
HTTP	539,021
HTTPS	353,801
HTTP (8000)	51,791
8081	36,722
HTTP (81)	10,681

TOP ORGANIZATIONS:

Organization	Count
OVH SAS	535,365
Orange	70,679
ONLINE SAS	57,530

Access forbidden!
Coriolis Telecoms SAS
Date: Thu, 14 Jun 2018 06:58:28 GMT
Server: Apache/2.2.21 (Linux/SUSE)
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
Content-Language: en

Index of /
92.222.237.2
Last modified: 2018-06-14 06:58:46 GMT
OVH SAS
Added on 2019-05-14 06:25:47 GMT
France, Paris
[Details](#)

5.135.228.150
OVH SAS
Date: 2018-06-14 06:20:00 GMT
France
[Details](#)

HTTP/1.1 200 OK
Date: Thu, 14 Jun 2018 06:19:32 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Content-Length: 4013
Content-type: text/html; charset=ISO-8859-1

Looking for nginx server in Dudelange:

nginx city:"Dudelange"

Total Results: 59

Top Services

Service	Count
Synology	18
Synology	14
HTTP	12
HTTPS	10
HTTP (81)	2

Top Organizations

Organization	Count
Entreprise des Postes e... 25	
Tango S.A.	13
PWU Luxembourg	11
Fondation RESTENA	6
EDPNET	4

94.252.93.15
asul 94-252-93-15.dyn.cust.tango.lu
City: Dudelange
Country: Luxembourg
Organization: Tango S.A.

Ports

Port	Count
81	1
3388	1
8089	1

Fusion For Energy, OSSTMM - MODULE 1,

Proximus Luxembourg S.A. | 18, rue du Puits Romain - Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 – 1 | F +352 45 09 11

www.telindus.lu VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO

9001 -

Page 9 of 22



Clicking on 'details' even gives the open ports and the services running on the server.

94.252.93.15 ads.94-252-93-15.dyn.cust.tango.lu

City: Dudelange
Country: Luxembourg
Organization: Tango S.A.
ISP: Tango S.A.
Last Update: 2019-06-12T15:17:51+0600
Hostnames: ads.94-252-93-15.dyn.cust.tango.lu
ASN: 4048526

Ports: 80, 443, 8080

Services:

- nginx
- HTTP/1.1 200 OK
- Date: Tue, 32 Jan 2018 05:17:39 GMT
- Content-Type: text/html
- Content-Length: 1024
- Connection: keep-alive
- Keep-Alive: timeout=20
- Accept-Ranges: bytes
- Vary: Accept-Encoding

- https
- Secure Socket Protection
- SSL Certificate

The Wayback Machine

The Wayback archive aims to be an archive of the Web. It allows people to crawl snapshots of websites. This could be useful to visit a website without actually requesting the company servers and so without any contact with the target. Moreover, this can give interesting information about the technology evolution and might allow attackers to find valuable information.

For instance, the Wayback machine has 364 snapshots of telindus.lu, from May 14, 1997 to June 13, 2018.

Internet Archive Wayback Machine

Explore more than 332 billion web pages saved over time

http://telindus.lu

Saved 364 times between May 14, 1997 and June 13, 2018

Summary of telindus.lu · Site Map of telindus.lu

Timeline visualization showing the frequency of snapshots taken each month from 1996 to 2018.

Month-by-month snapshot count:

Month	Year	Count
Jan	1997	1
Feb	1997	1
Mar	1997	1
Apr	1997	1
May	1997	1
Jun	1997	1
Jul	1997	1
Aug	1997	1
Sep	1997	1
Oct	1997	1
Nov	1997	1
Dec	1997	1
Jan	1998	1
Feb	1998	1
Mar	1998	1
Apr	1998	1
May	1998	1
Jun	1998	1
Jul	1998	1
Aug	1998	1
Sep	1998	1
Oct	1998	1
Nov	1998	1
Dec	1998	1
Jan	1999	1
Feb	1999	1
Mar	1999	1
Apr	1999	1
May	1999	1
Jun	1999	1
Jul	1999	1
Aug	1999	1
Sep	1999	1
Oct	1999	1
Nov	1999	1
Dec	1999	1
Jan	2000	1
Feb	2000	1
Mar	2000	1
Apr	2000	1
May	2000	1
Jun	2000	1
Jul	2000	1
Aug	2000	1
Sep	2000	1
Oct	2000	1
Nov	2000	1
Dec	2000	1
Jan	2001	1
Feb	2001	1
Mar	2001	1
Apr	2001	1
May	2001	1
Jun	2001	1
Jul	2001	1
Aug	2001	1
Sep	2001	1
Oct	2001	1
Nov	2001	1
Dec	2001	1
Jan	2002	1
Feb	2002	1
Mar	2002	1
Apr	2002	1
May	2002	1
Jun	2002	1
Jul	2002	1
Aug	2002	1
Sep	2002	1
Oct	2002	1
Nov	2002	1
Dec	2002	1
Jan	2003	1
Feb	2003	1
Mar	2003	1
Apr	2003	1
May	2003	1
Jun	2003	1
Jul	2003	1
Aug	2003	1
Sep	2003	1
Oct	2003	1
Nov	2003	1
Dec	2003	1
Jan	2004	1
Feb	2004	1
Mar	2004	1
Apr	2004	1
May	2004	1
Jun	2004	1
Jul	2004	1
Aug	2004	1
Sep	2004	1
Oct	2004	1
Nov	2004	1
Dec	2004	1
Jan	2005	1
Feb	2005	1
Mar	2005	1
Apr	2005	1
May	2005	1
Jun	2005	1
Jul	2005	1
Aug	2005	1
Sep	2005	1
Oct	2005	1
Nov	2005	1
Dec	2005	1
Jan	2006	1
Feb	2006	1
Mar	2006	1
Apr	2006	1
May	2006	1
Jun	2006	1
Jul	2006	1
Aug	2006	1
Sep	2006	1
Oct	2006	1
Nov	2006	1
Dec	2006	1
Jan	2007	1
Feb	2007	1
Mar	2007	1
Apr	2007	1
May	2007	1
Jun	2007	1
Jul	2007	1
Aug	2007	1
Sep	2007	1
Oct	2007	1
Nov	2007	1
Dec	2007	1
Jan	2008	1
Feb	2008	1
Mar	2008	1
Apr	2008	1
May	2008	1
Jun	2008	1
Jul	2008	1
Aug	2008	1
Sep	2008	1
Oct	2008	1
Nov	2008	1
Dec	2008	1
Jan	2009	1
Feb	2009	1
Mar	2009	1
Apr	2009	1
May	2009	1
Jun	2009	1
Jul	2009	1
Aug	2009	1
Sep	2009	1
Oct	2009	1
Nov	2009	1
Dec	2009	1
Jan	2010	1
Feb	2010	1
Mar	2010	1
Apr	2010	1
May	2010	1
Jun	2010	1
Jul	2010	1
Aug	2010	1
Sep	2010	1
Oct	2010	1
Nov	2010	1
Dec	2010	1
Jan	2011	1
Feb	2011	1
Mar	2011	1
Apr	2011	1
May	2011	1
Jun	2011	1
Jul	2011	1
Aug	2011	1
Sep	2011	1
Oct	2011	1
Nov	2011	1
Dec	2011	1
Jan	2012	1
Feb	2012	1
Mar	2012	1
Apr	2012	1
May	2012	1
Jun	2012	1
Jul	2012	1
Aug	2012	1
Sep	2012	1
Oct	2012	1
Nov	2012	1
Dec	2012	1
Jan	2013	1
Feb	2013	1
Mar	2013	1
Apr	2013	1
May	2013	1
Jun	2013	1
Jul	2013	1
Aug	2013	1
Sep	2013	1
Oct	2013	1
Nov	2013	1
Dec	2013	1
Jan	2014	1
Feb	2014	1
Mar	2014	1
Apr	2014	1
May	2014	1
Jun	2014	1
Jul	2014	1
Aug	2014	1
Sep	2014	1
Oct	2014	1
Nov	2014	1
Dec	2014	1
Jan	2015	1
Feb	2015	1
Mar	2015	1
Apr	2015	1
May	2015	1
Jun	2015	1
Jul	2015	1
Aug	2015	1
Sep	2015	1
Oct	2015	1
Nov	2015	1
Dec	2015	1
Jan	2016	1
Feb	2016	1
Mar	2016	1
Apr	2016	1
May	2016	1
Jun	2016	1
Jul	2016	1
Aug	2016	1
Sep	2016	1
Oct	2016	1
Nov	2016	1
Dec	2016	1
Jan	2017	1
Feb	2017	1
Mar	2017	1
Apr	2017	1
May	2017	1
Jun	2017	1
Jul	2017	1
Aug	2017	1
Sep	2017	1
Oct	2017	1
Nov	2017	1
Dec	2017	1
Jan	2018	1

Passive banner grabbing with Netcraft

Netcraft is an internet security company that provides services for a wide range of industries. It has powerful analyzing tools, which try to guess what technologies are powering websites.

Using Netcraft allows the pentester to not interact with the target system and still get information. In a full passive information gathering, this tool is a real asset.

For more information on banners, see "[Banner grabbing with netcat](#)".

Hands on!

What are the OS and the webservers running on:

- <http://sagsbox.telinduslab.lu>
- <http://sagsblog.telinduslab.lu>

What can be inferred from these results?

Hands on!

ANSWERS

Netcraft's results for sagsbox:

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
Telindus SAGS IP addresses used for ethical hacking purpose duly authorized by our customers For any urgent matters please contact telecoms@telindus.lu	185.3.45.3	Linux	Apache	12-Jun-2018

Netcraft's results for sagsblog:

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
Telindus SAGS IP addresses used for ethical hacking purpose duly authorized by our customers For any urgent matters please contact telecoms@telindus.lu	185.3.45.6	Linux	Microsoft-IIS/7.0	5-Jun-2016

Based on this information, sagsbox seems to be running on Linux, powered by an Apache server.

However, sagsblog appears to run Microsoft IIS/7.0 on Linux too, which is impossible. Banners can be altered to avoid giving sensitive information on the Internet.

3 Social media and documents

TheHarvester

As explained on the project's Github page, *theHarvester* is a tool that collects subdomain names, e-mail addresses, virtual hosts, open ports/banners, and employees' names from different public sources (search engines, PGP key servers, etc.).

Useful links:

- github.com/laramies/theHarvester
 - osintframework.com/
 - github.com/thewhiteh4t/pwnedOrNot

Hands on!

Find subdomains names and emails addresses for the domain *telindus.lu*.

Hands on!

ANSWERS

First using *theHarvester* ability to search on *google*:

```
root@kali:~/theHarvester# python theHarvester.py -d telindus.lu -b google
```



```
Searching 0 results...
Searching 100 results...
Searching 200 results...
Searching 300 results...
Searching 400 results...
Searching 500 results...
```

Harvesting results

[+] Emails found:

```
-----
contact@telindus.lu
Leclerc@telindus.lu
Cedric.Mauny@telindus.lu
Jeremy.Thimont@telindus.lu
marcom@telindus.lu
calldesk@telindus.lu
marketing@telindus.lu
csirt@telindus.lu
serviceprovidernetworks@telindus.lu
gerard.hoffmann@telindus.lu
info@telindus.lu
chantal.demmerle@telindus.lu
noemie.turpain@telindus.lu
Joany.boutet@telindus.lu
cybersecurity@telindus.lu
penelope.lembessi@telindus.lu
telecoms@telindus.lu
serge.munhoven@telindus.lu
sebastien.laurenti@telindus.lu
Jean.glod@telindus.lu
jean.glod@telindus.lu
Charles.hottelet@telindus.lu
joseph.paris@telindus.lu
armand.meyers@telindus.lu
Frank.roessig@telindus.lu
dns@telindus.lu
olivier.montee@telindus.lu
jean.calcada@telindus.lu
Lorenz.MEIS@telindus.lu
recrutement@telindus.lu
joelle.wingerter@telindus.lu
```

[+] Hosts found in search engines:

```
-----
Total hosts: 18
```

[+] Resolving hostnames IPs...

```
appsentry.telindus.lu : 31.204.90.59
corporate.telindus.lu : 85.93.219.14
dns.telindus.lu : empty
external.telindus.lu : empty
frankfurt.telindus.lu : empty
```

Fusion For Energy, OSSTMM - MODULE 1,

Proximus Luxembourg S.A. | 18, rue du Puits Romain - Z.A Bourmicht | L-8070 Bertrange - Luxembourg | T +352 45 09 15 - 1 | F +352 45 09 11

www.telindus.lu VAT LU 15605033 | RCS Luxembourg B 19.669 | Certifications ISO 27001 (Services Cybersécurité, Cloud, Managés et d'Externalisation) & ISO



```
gw-br02.frankfurt.telindus.lu : empty
ip...telindus.lu : empty
lyncrediscover.telindus.lu : 31.204.90.55
mail.telindus.lu : 31.204.90.85
mcis-external.telindus.lu : 31.204.90.35
purple-external.telindus.lu : empty
queue.bet.azurestack.telindus.lu : empty
roc-sai.telindus.lu : 31.204.88.193
tlullynco2.telindus.lu : empty
training.telindus.lu : 31.204.90.85
u-share.telindus.lu : 31.204.90.51
www.telindus.lu : 31.204.90.51
www.training.telindus.lu : 31.204.90.85
```

Then trying to look on *linkedin*:

```
root@kali:~/theHarvester# python theHarvester.py -d telindus.lu -b
linkedin

[-] Starting harvesting process for domain: telindus.lu

[-] Searching in Linkedin..
      Searching 100 results..
      Searching 200 results..
      Searching 300 results..
      Searching 400 results..
      Searching 500 results..

Users from Linkedin:
-----
Jean-Jacques Beasch
Gerard Hoffmann - CEO for Luxembourg - Proximus
Daniel Soriano
Yann Michel
Frank Roessig
Maria Kyriakoudi
Jean-Pierre Ceccacci
Jean-Marie Paris
Gerard Hoffmann - CEO for Luxembourg - Proximus
Nicolas Demonty - Network Engineer - Clearstream
Antonello Di Pinto - Lead Developer - Nvision Luxembourg
Gerard Hoffmann - CEO for Luxembourg - Proximus
Joany Boutet - Member - OWASP Foundation
Benoit Poncelet - Application Engineer - Web eMotion
Frank Roessig
Serge Munhoven
Yahia CHABNI - AVP - IT Manager - Silver Holdings
Vincent Artiguebieille - ITSM Senior Consultant - Amaris
Maurice Groben - Sales Director
olivier montee - Information risk and security officer - KPMG
Bruno Saravia - Account Manager - OpenField S.A.
Alexis Jouanne - System engineer - Elgon S.A.
Eric Hausman - Senior Account Executive - Microsoft
Laurianne Bouvet
```



Philippe Roux - VC Engineer - POST Telecom PSF S.A.
Vincent Williquet - Technical Manager - Netcore PSF SA
Ralf Hustadt
Julien Doussot - CEO - BLACKHORN
edgard belolo
Martial COLLOT
Sandra Parracho Soares
Franck Ludwig - Operations Manager IT - Online Banking
Alex STREITZ
Djuma Cauwenbergh
Jacques Ruckert
Fabrice Crompin
Danielle Vassard
Glauber Santos - Service Manager - LuxTrust S.A.
Marouan Darhnaj
Remi Meunier
Claude Schiltz
Laure Jalte

Looking in *PGP database* could also give interesting emails:

```
root@kali:~/theHarvester# python theHarvester.py -d telindus.lu -b pgp
```

```
[+] Emails found:
```

```
-----  
frederic.dhuez@telindus.lu  
anton.shkurenko@telindus.lu  
tristan.roussel@telindus.lu  
valentin.lacave@telindus.lu  
bruno.rubin@telindus.lu  
joany.boutet@telindus.lu  
damien.gitter@telindus.lu  
pierre-alain.francois@telindus.lu  
jeanfrancois.job@telindus.lu  
sebastien.grelot@telindus.lu  
csirt@telindus.lu  
frederic.hauss@telindus.lu  
cedric.mauny@telindus.lu  
jeremy.thimont@telindus.lu  
tom.leclerc@telindus.lu
```

NB: other tools can be useful to gather information about people such as hunter.io or to check if they have already been powned somewhere (haveibeenpwned.com).

Demo using *pwnedOrNot* tool:

```
root@kali:~/pwnedOrNot# python3 pwnedornot.py -f gathered-emails.txt
```



A complex musical score for two voices, featuring dense vertical stems and horizontal beams.

Developed by : thewhiteh4t
Version : 1.0.7

```
[+] Checking for updates...
[+] Script is up-to-date...
[+] Bypassing Cloudflare Restriction...
[+] Reading Emails Accounts from gathered-emails.txt
[+] Checking Breach status for contact@telindus.lu
[!] Account pwned...Listing Breaches...

[+] Breach      : Onliner Spambot
[+] Domain     :
[+] Date       : 2017-08-28
[+] Fabricated  : False
[+] Verified   : True
[+] Retired    : False
[+] Spam        : True

[+] Dumps Found...!

[+] Looking for Passwords...this may take a while...
...
```

Metagoofil

Metagoofil is a tool that uses Google to look for documents belonging to a specific domain, download them and extract metadata in order to gather information about a target. Information that can be found in those metadata include usernames, path, software in use, operating systems, etc.

Useful links:

- <https://github.com/laramies/metagoofil>

Hands on!

Find information about Telindus using documents' metadata with Metagoofil.



```
root@kali:~/metagoofil# python metagoofil.py -d telindus.lu -t doc,pdf,ppt,docx,pptx -f output file -l 200 -n 5 -o test
```

[–] Starting online search...

```
[-] Searching for doc files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 10 files found
Starting to download 5 of them:
```

```
[+] Searching for pdf files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...
```

Results: 96 files found
Starting to download 5 of them:

```
[+] Searching for ppt files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...
```

Results: 5 files found
Starting to download 5 of them:

```
[+] Searching for docx files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...
```

Results: 5 files found
Starting to download 5 of them:

```
[+] Searching for pptx files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...
```



Results: 5 files found
Starting to download 5 of them:

...

[+] List of users found:

??mcamy

[+] List of software found:

Adobe PDF library 7.77
Adobe Illustrator CS2
◆◆DocuCom PDF Driver 5.56 for NT(Light)
◆◆Microsoft Word
Adobe PDF Library 8.0
Adobe InDesign CS3 (5.0)
Adobe PDF Library 7.0
Adobe InDesign CS2 (4.0.4)

[+] List of paths and servers found:

[+] List of e-mails found:

marc.rob@telindus.lu
privacy@telindus.lu
Privacy@Telindus

FOCA 2020 - 2021

Foca (which stands for Fingerprinting Organizations with Collected Archives) is similar to Metagoofil: it collects documents from the internet (Google, Bing and DuckDuckGo) to find metadata and hidden information. It is capable of analyzing a variety of documents like MS Office, PDF, Adobe, etc.

With all these metadata, it can find usernames, software in use, operating systems, just as Metagoofil does.

Hands on!

DEMO



Using FOCA on telindus.lu and telindustelecom.lu, some interesting results can be observed:

In addition, some interesting usernames:



Attribute	Value
All users found (10) - Times found	
THIMONT Jeremy	12
Telindus-CSIRT	6
MAUNUY Cedric	7
jthimont	4
id047078	9
LODE Armelle	4
VALENDUC Laurence	6
Meyer	1
Jeremy Thimont	4
Ericsson	1

4 How to protect yourself

Banner Modification

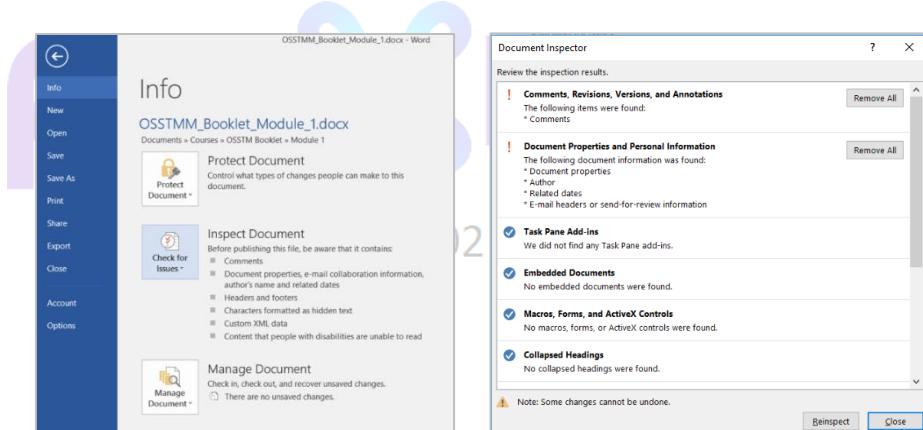
See Module 2.

Remove sensitive metadata

Metadata are a golden mine for information gathering. Prevent attacker to get results from this metadata is yet a fast and easy task.

In word, document can be inspected for hidden properties and information. Just go in File > Inspect document:

“Inspect document” suggest the user to delete hidden properties.

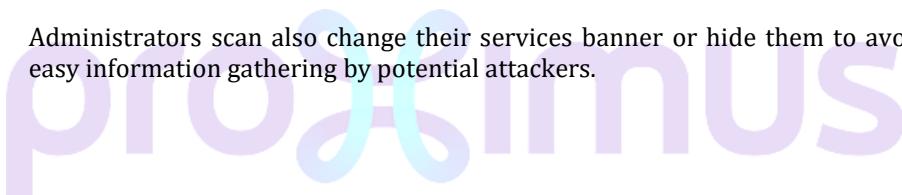


5 Conclusion

This section covered the very first steps of information gathering with passive data collection and analyze. This step is not to neglect as it often leads to technologies in use, emails and usernames. Some vulnerabilities can even be expected from a version found by passively grabbing banners and then by looking for vulnerabilities on this specific version.

Even if it is very difficult for a company to control all their employees on the internet, one can still try to mitigate the information leakage by doing a security awareness campaign. The goal of such a campaign is to prevent employee from having weak passwords, from reusing password and simply to pay more attention to what they are publishing on the internet.

Administrators can also change their services banner or hide them to avoid easy information gathering by potential attackers.



Contact information

Cybersecurity Department Proximus Luxembourg

cybersecurity@telindus.lu
pentest@telindus.lu

Twitter: [@S_Team_Approved](#)

.....
Proximus House
Z.A. Bourmicht - 18, rue du Puits Romain
L-8070 Bertrange
T +352 27 777 00
.....

Damien GITTER
Senior Ethical Hacker,
Technology leader Pentest at Cybersecurity Department
GIAC Certified (GSEC, GCIA, GCIH, GPEN, GWAPT, GMOB,
GXPN,GMON,GAWN)
Certified OSSTMM (OPST & OPSA)
T +352 23 28 20 7784
M +352 691 777 784
damien.gitter@telindus.lu