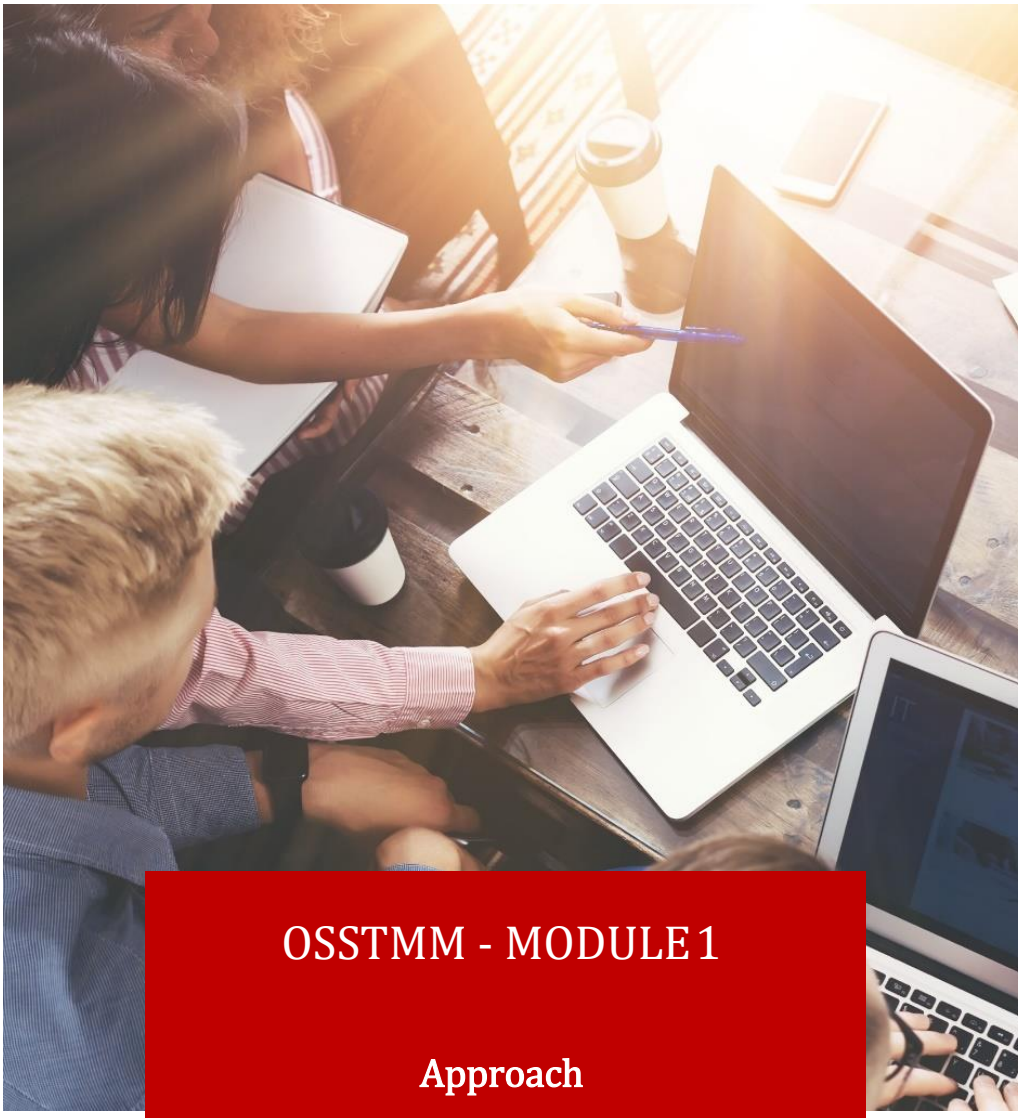


OSSTMM - MODULE 1

Approach

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

Sensitivity: PUBLIC

Summary

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 **O**pen **S**ource **INT**elligence. 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:

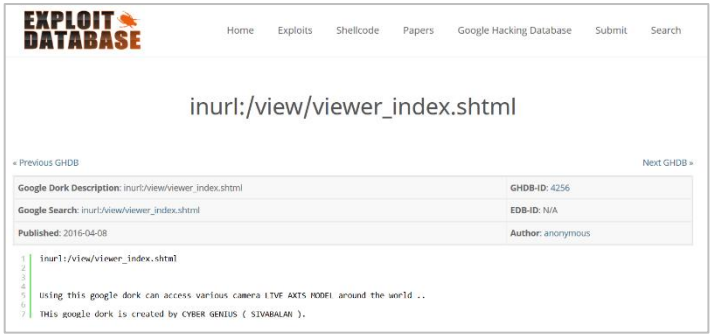
- www.exploit-db.com/google-hacking-database/

Hands on!

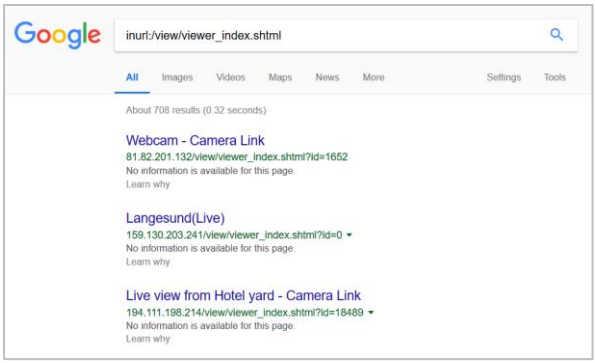
Use Google Dorks to find an online camera system.

Hands on! **ANSWERS**

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



Google gives the following results when using the previous dork:



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

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

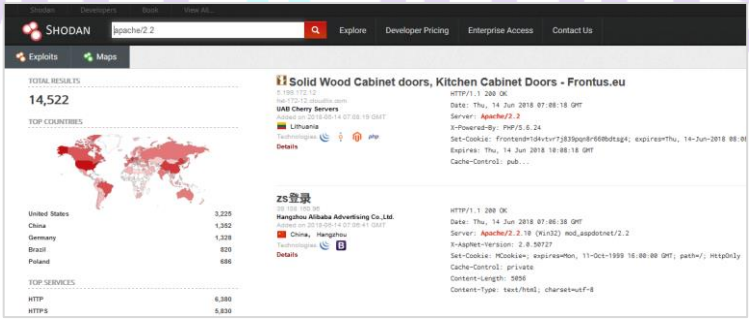
Hands on!

Use Shodan to find Apache 2.2 servers located in France.

Hands on! ANSWERS

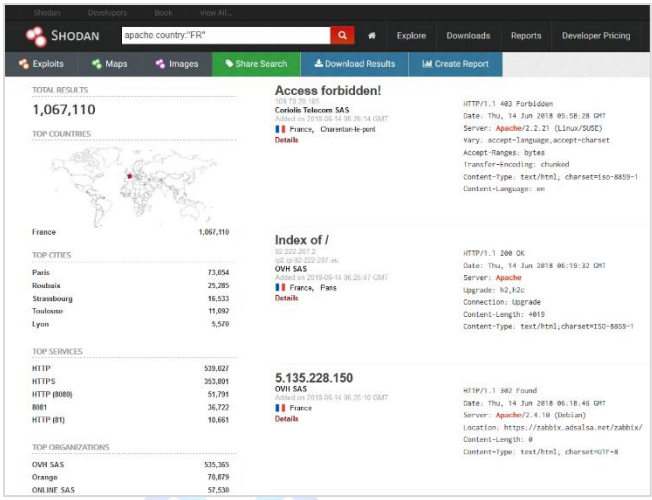
Filters require a Shodan account, but some useful information are available without using those filters, searching for example with:

```
Apache/2.2
```



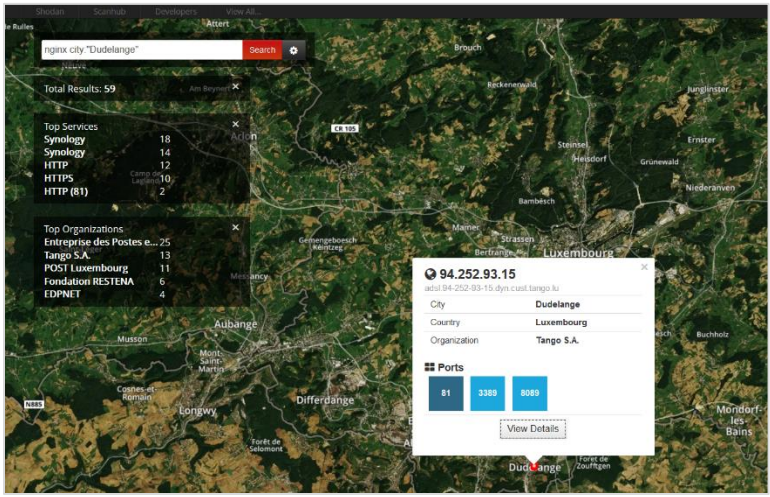
With a free account, it is possible to perform filtered search:

```
Apache country:"FR"
```

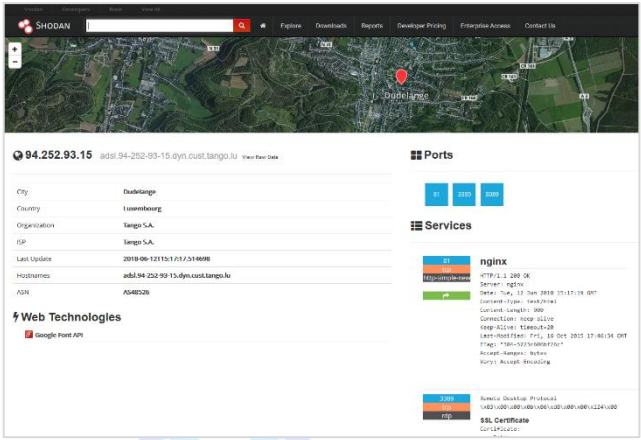


Looking for nginx server in Dudelange:

```
nginx city:"Dudelange"
```



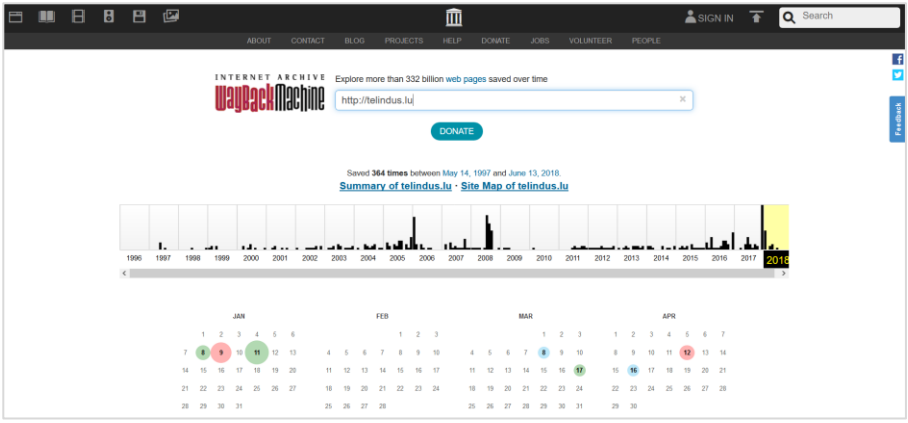
Clicking on ‘details’ even gives the open ports and the services running on the server.



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.



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 (Refresh)
Telindus SAGS ---------- IP addresses used for ethical hacking purpose duly authorized by our customers For any urgent matters please contact telecomsdtelindus.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 (Refresh)
Telindus SAGS ---------- IP addresses used for ethical hacking purpose duly authorized by our customers For any urgent matters please contact telecomsdtelindus.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

*************************************************************************
*                                                                       *
* | |_| |__   ___       /\  /\__ _ _ _____   _____ ___| |_ ___ _ __   *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                       *
* TheHarvester Ver. 3.0                                                 *
* Coded by Christian Martorella                                         *
* Edge-Security Research                                                *
* cmartorella@edge-security.com                                         *
*************************************************************************

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

[-] Searching in 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
telecomsd@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
```

```
gw-br02.frankfurt.telindus.lu : empty
ip...telindus.lu : empty
lyncdiscover.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
tlu1lync02.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 Jaltel
```

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
```

```
           _____ _       _______  ___  ____/ / __ \_____/ | / /___  / /_
          /     \ | /| / /     \/   \/      / / / /     /  |/ /    \/   /
         / /_/ / |/ |/ / / / /  __/ /_/ / /_/ / /  / /|  / /_/ / /_
        / .___/|__/|__/_/ /_/\___/\__,_/\____/_/  /_/ |_/\____/\__/
       /_/

       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

*****************************************************
*     /\/\   ___| |_ __ _   __ _   ___   ___   / _(_) | *
*    /    \ / _ \ __/ _` | / _` | / _ \ / _ \ | |_| | | *
*   / /\/\ \  __/ || (_| | (_| | (_) | (_) |  _| | | | *
*   \/    \/\___|\__\__,_|\__, |\___/ \___/|_| |_|_| | *
*                         |___/                       *
* Metagoofil Ver 2.2                                  *
* Christian Martorella                                *
* Edge-Security.com                                   *
* cmartorella_at_edge-security.com                    *
*****************************************************

[-] 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

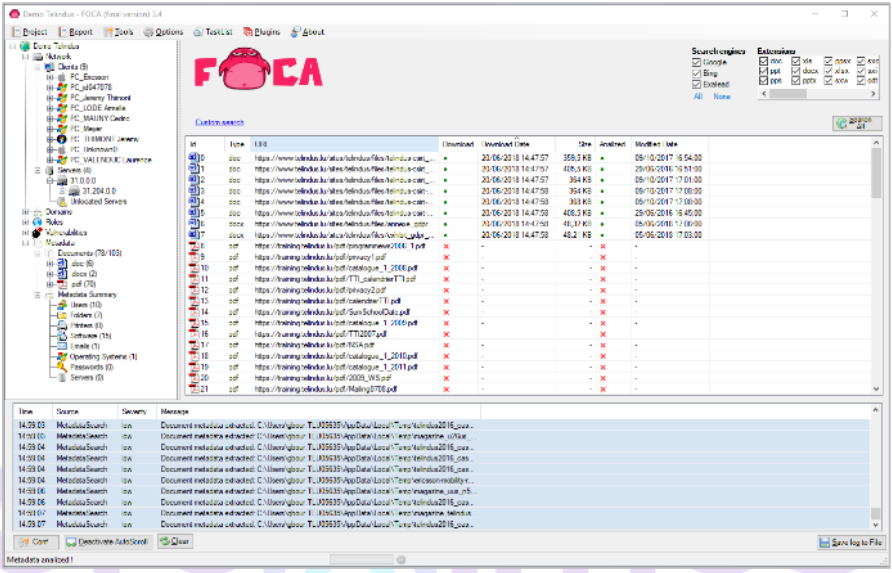
2020 - 2021

Foca (which stands for **F**ingerprinting **O**rganizations with **C**ollected **A**rchives) 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.

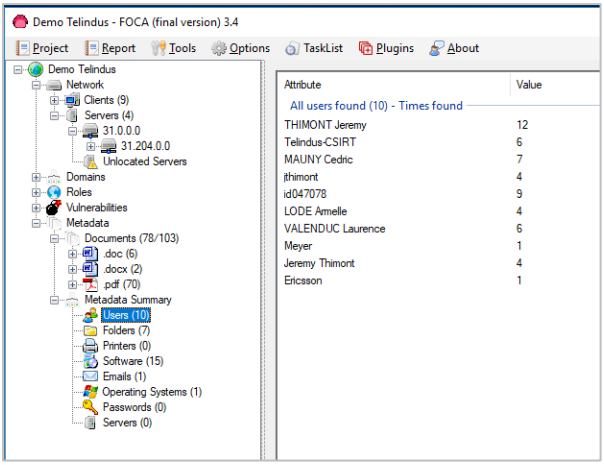
With all these metadata, it can find usernames, software in use, operating systems, just as Metagoofil does.

Hands on!	DEMO

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



In addition, some interesting usernames:



4 How to protect yourself

Banner Modification

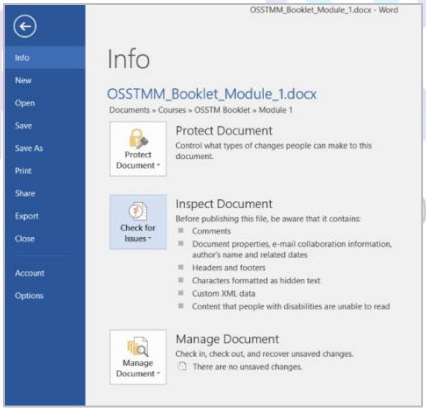
See Module 2.

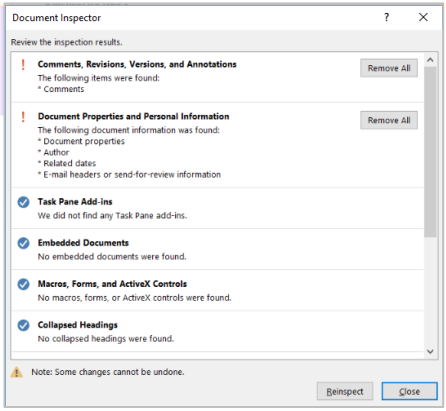
Remove sensitive metadata

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 scan 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