

Challenge 1

1- Collecting info from my local network (there are several devices)

```
leofigy@Angels-MacBook-Pro curso % nmap -sn 192.168.100.0/24 -oG -
# Nmap 7.93 scan initiated Sat May  6 12:34:03 2023 as: nmap -sn -oG - 192.168.100.0/24
Host: 192.168.100.1 () Status: Up
Host: 192.168.100.14 () Status: Up
Host: 192.168.100.73 () Status: Up
Host: 192.168.100.92 () Status: Up
Host: 192.168.100.95 () Status: Up
# Nmap done at Sat May  6 12:34:18 2023 -- 256 IP addresses (5 hosts up) scanned in 14.72 seconds
leofigy@Angels-MacBook-Pro curso %
```

Getting details for each active vm , saved previously the IPs in a file vm

```
leofigy@Angels-MacBook-Pro curso % nmap -iL vms
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-06 12:13 CST
Nmap scan report for 192.168.100.1
Host is up (0.0032s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
53/tcp    open       domain
80/tcp    open       http

Nmap scan report for 192.168.100.14
Host is up (0.0037s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
8008/tcp  open       http
8009/tcp  open       ajp13
8443/tcp  open       https-alt
9000/tcp  open       cslistener

Nmap scan report for 192.168.100.20
Host is up (0.0079s latency).
All 1000 scanned ports on 192.168.100.20 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.100.92
Host is up (0.0032s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
7000/tcp  open       afs3-fileserver
9080/tcp  open       glrpc

Nmap scan report for 192.168.100.95
Host is up (0.000098s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE      SERVICE
53/tcp    open       domain
5000/tcp  open       upnp
7000/tcp  open       afs3-fileserver

Nmap done: 5 IP addresses (5 hosts up) scanned in 23.82 seconds
```

2- Getting information from web sites using what web

There is a tool called whatweb, that allows you to get general information about a web site. It's a good start point , for the site www.udg.mx , it tell us it's running an nginx is written in php and for the front it has JQuery

```
ubuntu@primary:~$ whatweb -v www.udg.mx
WhatWeb report for http://www.udg.mx
Status      : 301 Moved Permanently
Title       : 301 Moved Permanently
IP          : 148.202.34.157
Country     : MEXICO, MX

Summary    : HTTPServer[nginx/1.12.2], nginx[1.12.2], RedirectLocation[https://www.udg.mx/]

Detected Plugins:
[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  String      : nginx/1.12.2 (from server string)

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and
  302

  String      : https://www.udg.mx/ (from location)

[ nginx ]
  Nginx (Engine-X) is a free, open-source, high-performance
  HTTP server and reverse proxy, as well as an IMAP/POP3
  proxy server.

  Version     : 1.12.2
  Website     : http://nginx.net/

HTTP Headers:
HTTP/1.1 301 Moved Permanently
Server: nginx/1.12.2
Date: Sat, 06 May 2023 23:04:24 GMT
Content-Type: text/html
Content-Length: 185
Connection: close
Location: https://www.udg.mx/

WhatWeb report for https://www.udg.mx
Status      : 200 OK
Title       : Inicio | Universidad de Guadalajara
IP          : 148.202.34.157
Country     : MEXICO, MX

Summary    : Content-Language[es], Cookies[SSESS6d6444d6a25dfd0ecf5e44a1b3d0af98],
Drupal, HTML5, HTTPServer[nginx/1.12.2],
HttpOnly[SSESS6d6444d6a25dfd0ecf5e44a1b3d0af98], JQuery[1.7], MetaGenerator[Drupal 7
(http://drupal.org)], nginx[1.12.2], PHP[5.4.16], Script[text/javascript],
```

UncommonHeaders[x-drupal-cache,x-content-type-options,permissions-policy,x-generator,link], **X-Frame-Options**[SAMEORIGIN], **X-Powered-By**[PHP/5.4.16]

Detected Plugins:

[**Content-Language**]

 Detect the content-language setting from the HTTP header.

 String : es

[**Cookies**]

 Display the names of cookies in the HTTP headers. The values are not returned to save on space.

 String : SSESS6d6444d6a25dfd0ecf5e44a1b3d0af98

[**Drupal**]

 Drupal is an opensource CMS written in PHP.

 Aggressive function available (check plugin file or details).

 Google Dorks: (1)

 Website : http://www.drupal.org

[**HTML5**]

 HTML version 5, detected by the doctype declaration

[**HTTPServer**]

 HTTP server header string. This plugin also attempts to identify the operating system from the server header.

 String : nginx/1.12.2 (from server string)

[**HttpOnly**]

 If the HttpOnly flag is included in the HTTP set-cookie response header and the browser supports it then the cookie cannot be accessed through client side script - More Info: http://en.wikipedia.org/wiki/HTTP_cookie

 String : SSESS6d6444d6a25dfd0ecf5e44a1b3d0af98

[**JQuery**]

 A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add AJAX.

 Version : 1.7

 Website : http://jquery.com/

[**MetaGenerator**]

 This plugin identifies meta generator tags and extracts its value.

 String : Drupal 7 (<http://drupal.org>)

[**PHP**]

 PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors,

modules and versions and extracts the local file path and username if present.

Version : **5.4.16**
Google Dorks: (2)
Website : <http://www.php.net/>

[Script]

This plugin detects instances of script HTML elements and returns the script language/type.

String : **text/javascript**

[UncommonHeaders]

Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspmx-version.
Info about headers can be found at www.http-stats.com

String : **x-drupal-cache,x-content-type-options,permissions-policy,x-generator,link** (from headers)

[X-Frame-Options]

This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info:
<http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx>

String : **SAMEORIGIN**

[X-Powered-By]

X-Powered-By HTTP header

String : **PHP/5.4.16** (from x-powered-by string)

[nginx]

Nginx (Engine-X) is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server.

Version : **1.12.2**
Website : <http://nginx.net/>

HTTP Headers:

HTTP/1.1 200 OK
Server: nginx/1.12.2
Date: Sat, 06 May 2023 23:04:29 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
X-Powered-By: PHP/5.4.16
X-Drupal-Cache: MISS
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
Content-Language: es
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff

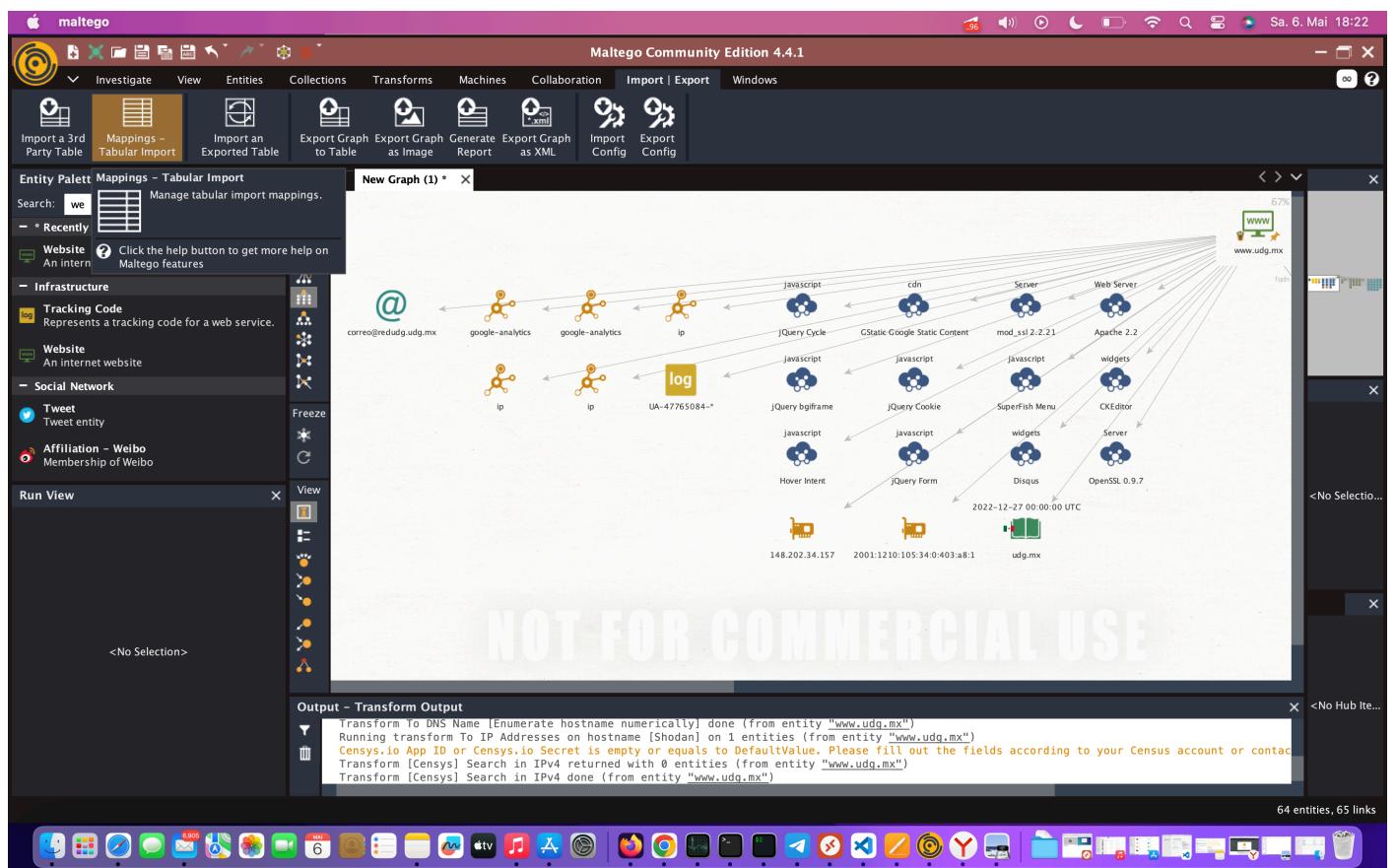
```

Permissions-Policy: interest-cohort=()
X-Generator: Drupal 7 (http://drupal.org)
Link: </es/inicio-0>; rel="canonical",</es/node/43622>; rel="shortlink"
Set-Cookie:
SSESS6d6444d6a25dfd0ecf5e44a1b3d0af98=MFP63xalTOFA0vxPlNAifVhB9yR9AjQWafxu5A_iwIY;
expires=Tue, 30-May-2023 02:37:49 GMT; path=/; SameSite=None; domain=.www.udg.mx;
secure; HttpOnly

```

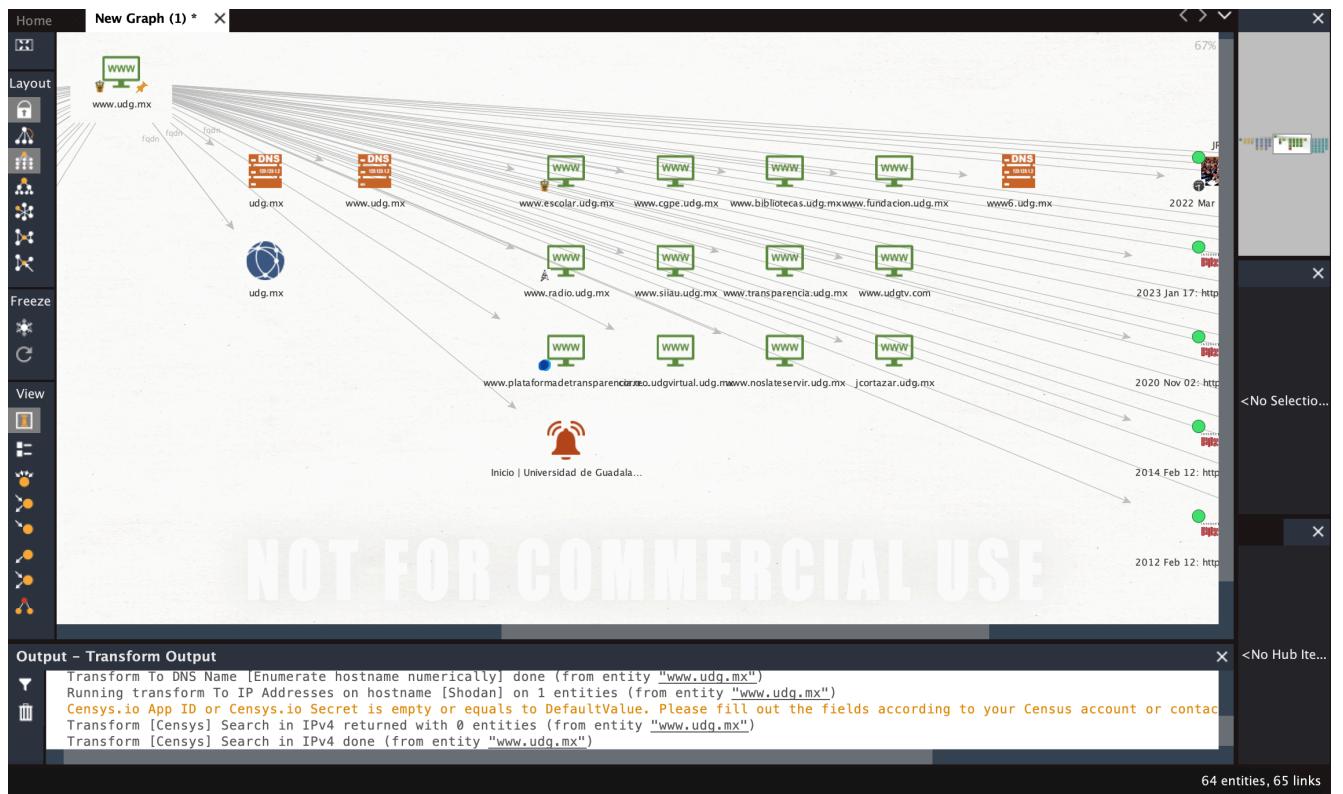
What we know about the site?

We know it uses nginx as server , and uses php with html5 . If we want to get more



details , we can use more tools like maltego that provides transformations to get more details about a domain.

Maltego can discover subdomains based on dns entries, and perform different transforms like looking for documents and discovering resources , if you add more transformations.



3- Identify kind of web site.

There is another fancy tool called OWASP ZAP, that has an spider to identify any sub-resource in the website , let's use again www.udg.mx domain

Verarbeitet	Methode	URI	Markierungen
GET	GET	https://www.udg.mx/rss/noticias/cucea	
GET	GET	https://www.udg.mx/noticias/cucea	
GET	GET	https://www.udg.mx/sites/default/files/li_cucea.jpg	
GET	GET	https://www.udg.mx/sites/default/files/styles/medium/public/...	
GET	GET	https://www.udg.mx/sites/default/files/cucea.png	
GET	GET	http://jquery.com/	Out of Scope
GET	GET	http://jquery.org/license	Out of Scope
GET	GET	http://sizzlejs.com/	Out of Scope
GET	GET	https://www.udg.mx/sites/default/files/adjuntos/pdi-udg-201...	

Warnungen: 1 5 9 4 Main Proxy: localhost:8080 Laufende Scans: 0 0 0 4 0 0 0 0 0 0 1

OZAP can return reports for all the sub-resources, but in addition it includes warnings for possible vulnerabilities, for Java script library jQuery v1.4.4 it has several known CVE , that a potential attacker might use, other warnings are related about personal information in the sites, or missing validations for CSRF.

The screenshot shows the OZAP application interface with the 'Warnungen' tab selected. On the left, a tree view lists various warning categories. A specific warning for a vulnerable JS library is highlighted in blue. The right panel provides detailed information about this vulnerability:

Vulnerable JS Library

- URL: <https://www.udg.mx/misc/jquery.js?v=1.4.4>
- Risiko: ⚠️ Medium
- Zuversicht: Medium
- Parameter:
- Attacke:
- Nachweis: * jQuery JavaScript Library v1.4.4
- CWE ID: 829
- WASC ID:
- Quelle: Passiv (10003 – Vulnerable JS Library (Powered by Retire.js))
- Input Vector:
- Beschreibung: The identified library jquery, version 1.4.4 is vulnerable.

Zusätzliche Infos:

- CVE-2011-4969
- CVE-2020-11023
- CVE-2020-11022

Lösung:

Please upgrade to the latest version of jquery.

Referenz:

- <https://nvd.nist.gov/vuln/detail/CVE-2012-6708>
- <https://github.com/jquery/jquery/issues/2432>
- <https://research.insecurelabs.org/jquery/test/>

Alert Tags:

Key	Wert
OWASP_2021_A06	https://owasp.org/Top10/A06_20...
CVE-2015-9251	https://nvd.nist.gov/vuln/detail/...
CVE-2019-11358	https://nvd.nist.gov/vuln/detail/...
CVE-2020-7656	https://nvd.nist.gov/vuln/detail/...

Laufende Scans: 🚧 0 🖱 0 🔍 4 🔥 0 🎯 0 🖊 0 🌐 0 🌐 1