

Footprinting Câmara Vila Nova de Famalicão



Whois results:

```
$whois cm-vnfamalicao.pt
Domain: cm-vnfamalicao.pt
Domain Status: Registered
Creation Date: 27/11/1998 00:00:00
Expiration Date: 28/06/2024 23:59:50
Owner Name: Camara Municipal de Vila Nova de Famalicao
Owner Address: Praaa lvaro Marques
Owner Locality: Vila Nova de Famalico
Owner ZipCode: 4764-502
Owner Locality ZipCode: Vila Nova de Famalico
Owner Country Code: PT
Owner Email: geral@cm-vnfamalicao.pt
Admin Name: Brainhouse, Tecnologias de Informacao e Multimedia Lda
Admin Address: Rua 25 de Abril, N. 408
Admin Locality: Braga
Admin ZipCode: 4710-914
Admin Locality ZipCode: Braga
Admin Country Code: PT
Admin Email: info@brainhouse.pt
Name Server: ns11.brainhouse.pt | IPv4:  and IPv6:
Name Server: ns9.brainhouse.pt | IPv4:  and IPv6:
```

Nslookup results:

```
$nslookup cm-vnfamalicao.pt
Server:      192.168.71.2
Address:     192.168.71.2#53

Non-authoritative answer:
Name:   cm-vnfamalicao.pt
Address: 195.22.20.186
```

Whatweb results:

```
#whatweb -v -a 3 195.22.20.186
WhatWeb report for http://195.22.20.186
Status      : 200 OK
Title       : <None>
IP          : 195.22.20.186
Country     : PORTUGAL, PT

Summary     : HTTPServer[nginx/1.10.3], nginx[1.10.3]
UA-Compatible[IE=edge], HTML5, Apache[2.2,2.2.22], HTTPServer[Ubuntu Linux][Apache/2.2.22]
Detected Plugins:
[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
    identify the operating system from the server header.
    String      : nginx/1.10.3 (from server 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     : 1.10.3
    Website     : http://nginx.net/
    the doctype declaration
HTTP Headers:
    HTTP/1.1 200 OK
    Server: nginx/1.10.3
    Date: Fri, 13 Mar 2020 15:39:05 GMT
    Content-Type: text/html; charset=UTF-8
    Transfer-Encoding: chunked
    Connection: close
    Content-Encoding: gzip
```

Nginx 1.10.3 (CVE's):

[Nginx](#) » [Nginx](#) » [1.10.3](#) : Security Vulnerabilities

Cpe Name: `cpe:/a:nginx:nginx:1.10.3`

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-16845	835			2018-11-07	2019-10-02	5.8	None	Remote	Medium	Not required	Partial	None	Partial
nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.														
2	CVE-2018-16844	400			2018-11-07	2019-09-10	7.8	None	Remote	Low	Not required	None	None	Complete
nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.														
3	CVE-2018-16843	400			2018-11-07	2019-09-10	7.8	None	Remote	Low	Not required	None	None	Complete
nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.														
Total number of vulnerabilities : 3 Page : 1 (This Page)														

Sublist3r results:

```
[root@parrot]--[home/kaiub/Documents/Sublist3r]
#python3 sublist3r.py -d cm-vnfamalicao.pt results in realtime

--threads      Number of threads to use for subbrute bruteforce
--engines       Specify a comma separated list of search engines
--output        Save the results to text file
--help          show the help message and exit

# Coded By Ahmed Aboul-Ela - @aboul3la

[+] Enumerating subdomains now for cm-vnfamalicao.pt
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSDumpster..
[+] Searching now in Virustotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
[+] Total Unique Subdomains Found: 5
www.cm-vnfamalicao.pt
equalidade.cm-vnfamalicao.pt
horde.cm-vnfamalicao.pt
cm-vnfamalicao.pt<BR>www.cm-vnfamalicao.pt
webmail.cm-vnfamalicao.pt
```

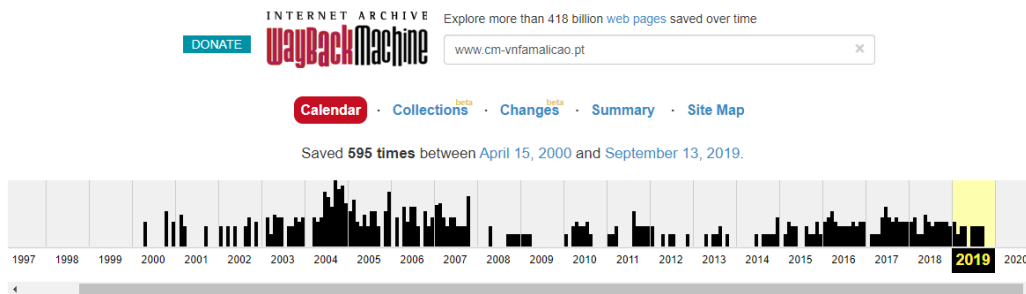
Amass results:

```
[x]-[root@parrot]-[/home/kaiub/Documents/ReconTools]
#amass enum -d cm-vnfamalicao.pt

www.cm-vnfamalicao.pt
equalidade.cm-vnfamalicao.pt
webmail.cm-vnfamalicao.pt
horde.cm-vnfamalicao.pt
mail.cm-vnfamalicao.pt
Starting DNS queries for altered names
Average DNS queries performed: 103/sec
Average DNS queries performed: 0/sec

OWASP Amass v3.4.4
-----
5 names discovered - cert: 1, scrape: 3, api: 1
-----
ASN: 8426 - CLARANET-AS ClaraNET LTD
      195.22.0.0/19      1 Subdomain Name(s)
ASN: 5533 - CLARANET-PT, PT
      195.22.0.0/19      4 Subdomain Name(s)
```

WayBackMachine results:



Shodan results:

Host:

195.22.20.186 s15.plako.net

Country	Portugal
Organization	Claranet Portugal S.A
ISP	Claranet Portugal S.A
Last Update	2020-03-13T09:59:34.277081
Hostnames	s15.plako.net
ASN	AS8426

Open TCP/UDP ports:

Open TCP/UDP ports

Status well known TCP and UDP ports. Note: we do not perform any port scan but use data of the ZMap project.

Description	Protocol/Port	Status
HTTP	tcp80	Open
HTTPS	tcp443	Open
DNS	udp53	Closed
Network Time Protocol (NTP)	udp123	Closed
NetBIOS Name Service	udp137	Closed
Session Initiation Protocol (SIP)	udp5060	Closed

Domains:

Domains on 195.22.20.186

Domain	Tools
4por4.pt	Whois+
visitportoandnorth.travel	Whois+
cm-vnfamaliao.pt	Whois+
revistadevinhos.pt	Whois+
cm-lamego.pt	Whois+
vilanovadefamaliao.org	Whois+
aeba.pt	Whois+
cultour.com.pt	Whois+
virose.pt	Whois+
vitaeprofessionals.com	Whois+
Reverse IP for 195.22.20.186	

Domains around 195.22.20.186

IP address	#domains
195.22.20.4	37
195.22.20.48	1
195.22.20.53	3
195.22.20.84	8
195.22.20.89	21
195.22.20.90	6
195.22.20.146	1
195.22.20.149	3
195.22.20.155	2
195.22.20.162	20
See more items	

Blocklist lookup:

Blocklist lookup

Adult hosting	not listed ✓
Hackers, Spyware, Botnets etc.	not listed ✓
Open proxy	not listed ✓

SPAM database lookup:


SPAM database lookup


DROP/EDROP list Spamhaus	not listed ✓
dnsbl-1.uceprotect.net	not listed ✓
Number of SPAM hosts on 195.22.0.0/19	1
SPAM tools	DNSBL 195.22.20.186


Web Technologies:

⚡ Web Technologies

 animate.css


 Bootstrap

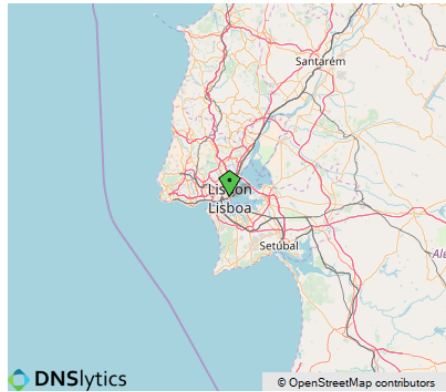
 Google Font API

 jQuery

Geo information:

Geo information

Location	Portugal (PT) 
Latitude and Longitude	38.71, -9.14



Country information (Portugal)

Capital	Lisbon
Continent	EU
Population	10,676,000
Area	92,391 km ²
Currency	EUR
Top Level Domain	.pt



Vulnerabilities:

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2011-5000	The <code>ssh_gssapi_parse_ename</code> function in <code>gss-serv.c</code> in OpenSSH 5.8 and earlier, when <code>gssapi-with-mic</code> authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
CVE-2010-4478	OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.
CVE-2014-1692	The <code>hash_buffer</code> function in <code>schnorr.c</code> in OpenSSH through 6.4, when <code>Makefile.inc</code> is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.
CVE-2010-5107	The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.
CVE-2017-15906	The <code>process_open</code> function in <code>sftp-server.c</code> in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2016-10708	<code>sshd</code> in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence <code>NEWKEYS</code> message, as demonstrated by Honggfuzz, related to <code>kex.c</code> and <code>packet.c</code> .
CVE-2016-0777	The <code>resend_bytes</code> function in <code>roaming_common.c</code> in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2011-4327	<code>ssh-keysign.c</code> in <code>ssh-keysign</code> in OpenSSH before 5.8p2 on certain platforms executes <code>ssh-rand-helper</code> with unintended open file descriptors, which allows local users to obtain sensitive key information via the <code>ptrace</code> system call.
CVE-2010-4755	The (1) <code>remote_glob</code> function in <code>sftp-glob.c</code> and the (2) <code>process_put</code> function in <code>sftp.c</code> in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted <code>glob</code> expressions that do not match any pathnames, as demonstrated by <code>glob</code> expressions in <code>SSH_FXP_STAT</code> requests to an <code>sftp</code> daemon, a different vulnerability than CVE-2010-2632.
CVE-2012-0814	The <code>auth_parse_options</code> function in <code>auth-options.c</code> in <code>sshd</code> in OpenSSH before 5.7 provides debug messages containing <code>authorized_keys</code> command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an <code>authorized_keys</code> file in its own home directory.

Maltego results:

