Footprinting and Reconnaissance

DURATION : 0’30

Previously

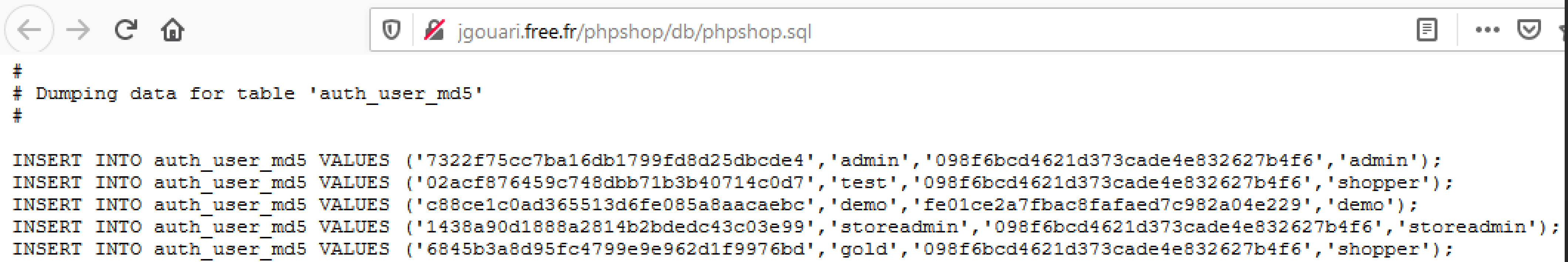
- Footprinting is the step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system.
  - **Passive footprinting** (without direct interaction) :
    - Finding information through search engines;
    - Finding the Top-Level Domains and subdomains of a target through web services;
    - Gathering infrastructure details on website (like Linkedin);
    - Monitoring the target using alert services;
    - Etc.
  - **Active foorprinting** (with direct interaction) :
    - Searching digital files;
    - Gathering website information using mirroring tools;
    - Harvesting email lists;
    - Performing social engineering;
    - Etc.

What to look for?

- Organization information :
  - Web technologies;
  - Documents related to the organization;
  - Employee details
  - Etc.
- Network information :
  - List all IP and DNS;
  - Detect FW, IPS/IDS, WAF, etc.
- System information :
  - Web server OS;
  - Location of web servers;
  - Usernames and password;
  - Etc.

Google Hacking Database (GHDB)

- GHDB or Google Dorks is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using: https://www.exploit-db.com/google-hacking-database
- You can search documents or other information.
- Use operators like intitle, inurl, intext, filetype, and more, exemple : ***filetype:sql "MySQL dump" (pass|password|passwd|pwd)***



```
#
# Dumping data for table 'auth_user_md5'
#

INSERT INTO auth_user_md5 VALUES ('7322f75cc7ba16db1799fd8d25dbcde4','admin','098f6bcd4621d373cade4e832627b4f6','admin');
INSERT INTO auth_user_md5 VALUES ('02acf876459c748dbb71b3b40714c0d7','test','098f6bcd4621d373cade4e832627b4f6','shopper');
INSERT INTO auth_user_md5 VALUES ('c88ce1c0ad365513d6fe085a8aacaebc','demo','fe01ce2a7fbac8fafaed7c982a04e229','demo');
INSERT INTO auth_user_md5 VALUES ('1438a90d1888a2814b2bdedc43c03e99','storeadmin','098f6bcd4621d373cade4e832627b4f6','storeadmin');
INSERT INTO auth_user_md5 VALUES ('6845b3a8d95fc4799e9e962d1f9976bd','gold','098f6bcd4621d373cade4e832627b4f6','shopper');
```

Google Hacking Database (GHDB)

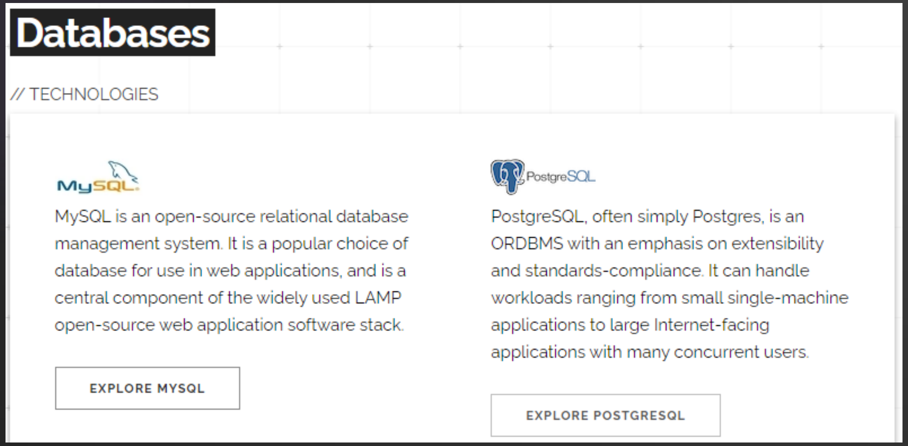
- Google hacking refers to the use of advanced Google search operators for creating complex search queries to extract sensitive or hidden information that helps attackers find vulnerable targets.
- List of popular Google advanced search operators
  - [site:] or [domain:] ➔ Restricts the results to those websites in the given domain.
  - [filetype:] ➔ Used to search for any kind of file extensions (filetype:pdf).
  - [cache:] ➔ Displays the web pages stored in the Google cache
  - [intitle:] ➔ Restricts the results to documents containing the search keyword in the title.
  - [inurl:] ➔ Restricts the results to documents containing the search keyword in the URL.

Google Hacking Database (GHDB)

- Examples of sensitive information on public servers with GHDB:
  - Error messages that contain sensitive information;
  - Files containing passwords;
  - Sensitive directories;
  - Pages containing logon portals;
  - Pages containing network or vulnerability data (IPS/IDS, FW, etc.);
  - Software version information;
  - Web application source code;
  - Etc.

Shodan

- Shodan is a search engines that crawls the internet for IoT devices that are publicly accessible.
- With the help of search engines such as Shodan attackers can obtain information such as the manufacturer details, geographical location, IP address, hostname and open ports of the target IoT device.



Databases

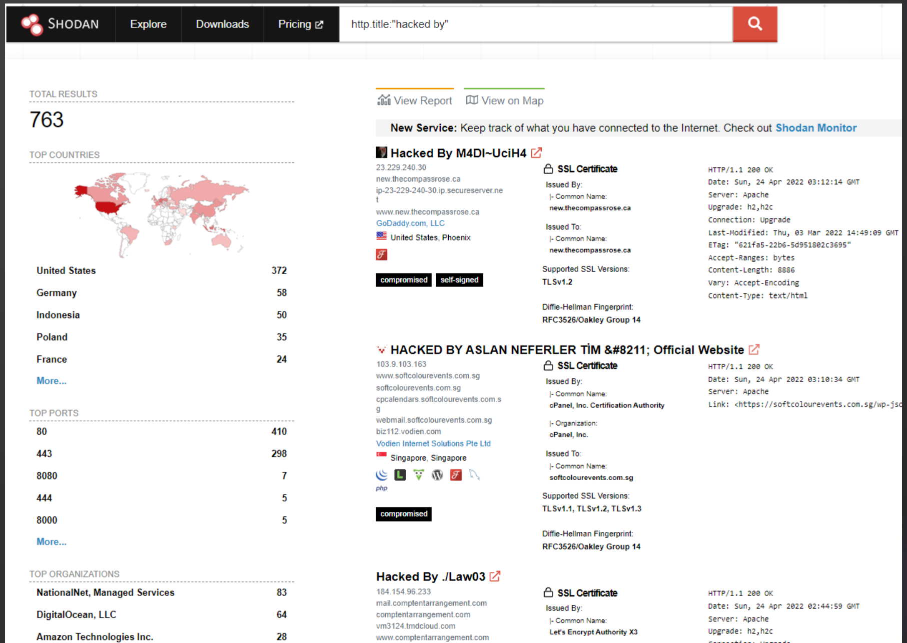
// TECHNOLOGIES

MySQL is an open-source relational database management system. It is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open-source web application software stack.

EXPLORE MYSQL

PostgreSQL, often simply Postgres, is an ORDBMS with an emphasis on extensibility and standards-compliance. It can handle workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users.

EXPLORE POSTGRESQL



http.title:"hacked by"

TOTAL RESULTS

763

TOP COUNTRIES

United States	372
Germany	58
Indonesia	50
Poland	35
France	24
More...	

TOP PORTS

80	410
443	298
8080	7
444	5
8000	5
More...	

TOP ORGANIZATIONS

NationalNet, Managed Services	83
DigitalOcean, LLC	64
Amazon Technologies Inc.	28

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

Hacked By M4DI~UciH4

23.229.240.30
new.thecompassrose.ca
ip-23-229-240-30.ip.secureserver.net
www.new.thecompassrose.ca
GoDaddy.com, LLC
United States, Phoenix

compromised self-signed

SSL Certificate

Issued By:
|- Common Name:
new.thecompassrose.ca

Issued To:
|- Common Name:
new.thecompassrose.ca

Supported SSL Versions:
TLSv1.2

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2022 03:12:14 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Thu, 03 Mar 2022 14:49:09 GMT
ETag: "621fa5-22b6-5d951802c3695"
Accept-Ranges: bytes
Content-Length: 8886
Vary: Accept-Encoding
Content-Type: text/html
```

HACKED BY ASLAN NEFERLER TİM &#8211; Official Website

103.9.103.163
www.softcolourevents.com.sg
softcolourevents.com.sg
cpcalendars.softcolourevents.com.sg
webmail.softcolourevents.com.sg
biz112.vodien.com
Vodien Internet Solutions Pte Ltd
Singapore, Singapore

compromised

SSL Certificate

Issued By:
|- Common Name:
cPanel, Inc. Certification Authority
|- Organization:
cPanel, Inc.

Issued To:
|- Common Name:
softcolourevents.com.sg

Supported SSL Versions:
TLSv1.1, TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2022 03:10:34 GMT
Server: Apache
Link: <https://softcolourevents.com.sg/wp-jsc
```

Hacked By ./Law03

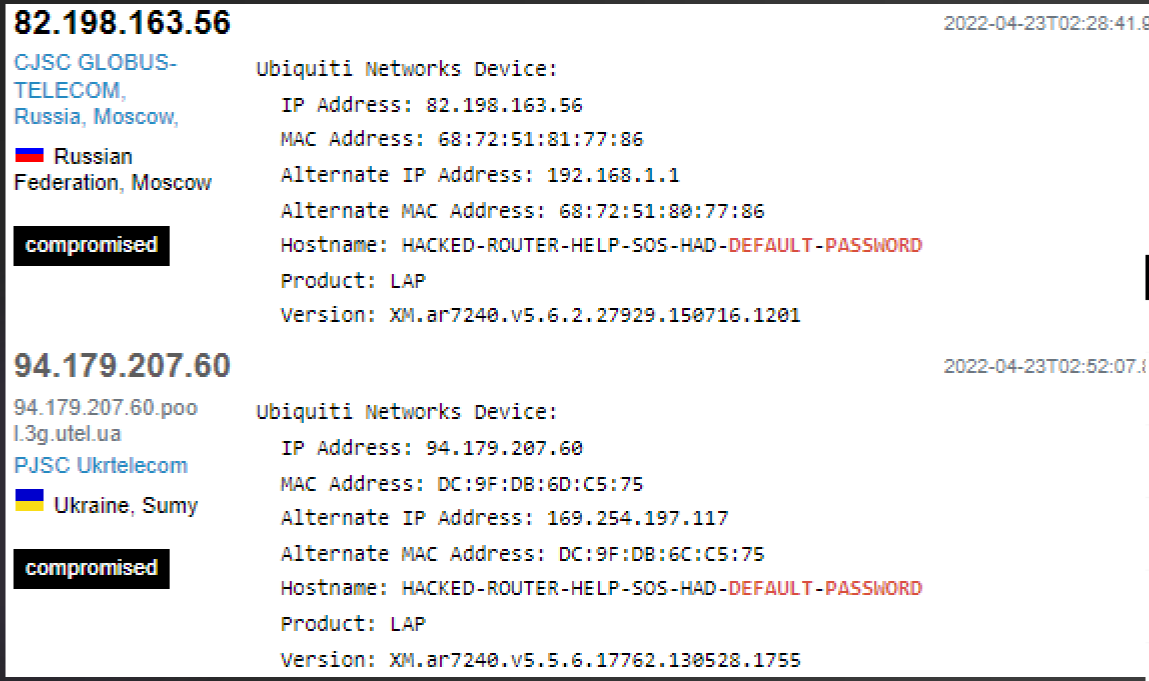
184.154.96.233
mail.comptentarrangement.com
comptentarrangement.com
vm3124.tmdcloud.com
www.comptentarrangement.com

SSL Certificate

Issued By:
|- Common Name:
Let's Encrypt Authority X3

```
HTTP/1.1 200 OK
Date: Sun, 24 Apr 2022 02:44:59 GMT
Server: Apache
Upgrade: h2,h2c
```

Shodan



82.198.163.56 2022-04-23T02:28:41.902645

CJSC GLOBUS-TELECOM, Russia, Moscow,

Russian Federation, Moscow

compromised

```
Ubiquiti Networks Device:
  IP Address: 82.198.163.56
  MAC Address: 68:72:51:81:77:86
  Alternate IP Address: 192.168.1.1
  Alternate MAC Address: 68:72:51:80:77:86
  Hostname: HACKED-ROUTER-HELP-SOS-HAD-DEFAULT-PASSWORD
  Product: LAP
  Version: XM.ar7240.v5.6.2.27929.150716.1201
```

94.179.207.60 2022-04-23T02:52:07.

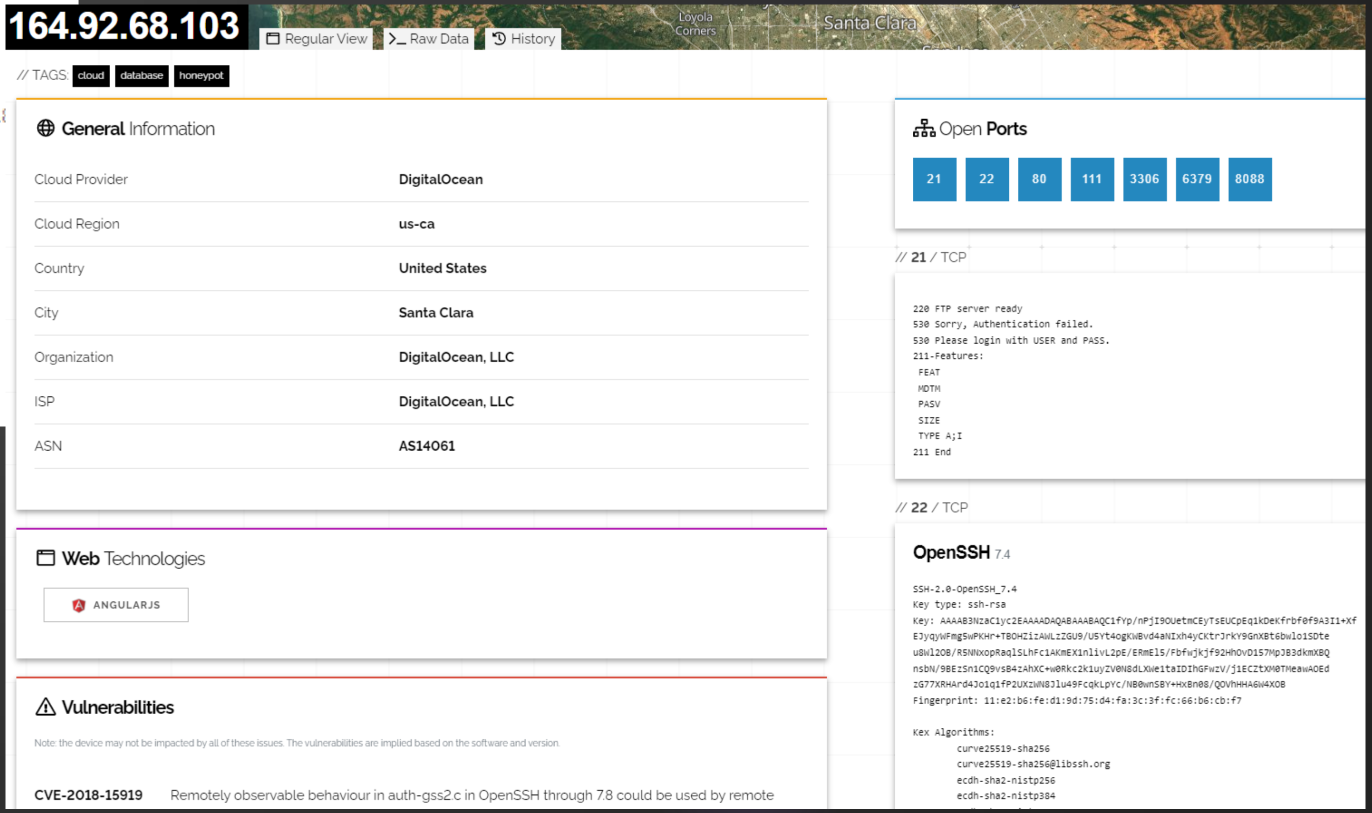
94.179.207.60.pool.3g.utel.ua

PJSC Ukrtelecom

Ukraine, Sumy

compromised

```
Ubiquiti Networks Device:
  IP Address: 94.179.207.60
  MAC Address: DC:9F:DB:6D:C5:75
  Alternate IP Address: 169.254.197.117
  Alternate MAC Address: DC:9F:DB:6C:C5:75
  Hostname: HACKED-ROUTER-HELP-SOS-HAD-DEFAULT-PASSWORD
  Product: LAP
  Version: XM.ar7240.v5.5.6.17762.130528.1755
```



164.92.68.103

// TAGS: cloud database honeypot

General Information

Cloud Provider	DigitalOcean
Cloud Region	us-ca
Country	United States
City	Santa Clara
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061

Web Technologies

ANGULARJS

Vulnerabilities

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

CVE-2018-15919 Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote

Open **Ports**

21 22 80 111 3306 6379 8088

// **21** / TCP

```
220 FTP server ready
530 Sorry, Authentication failed.
530 Please login with USER and PASS.
211-Features:
 FEAT
 MDTM
 PASV
 SIZE
 TYPE A;I
211 End
```

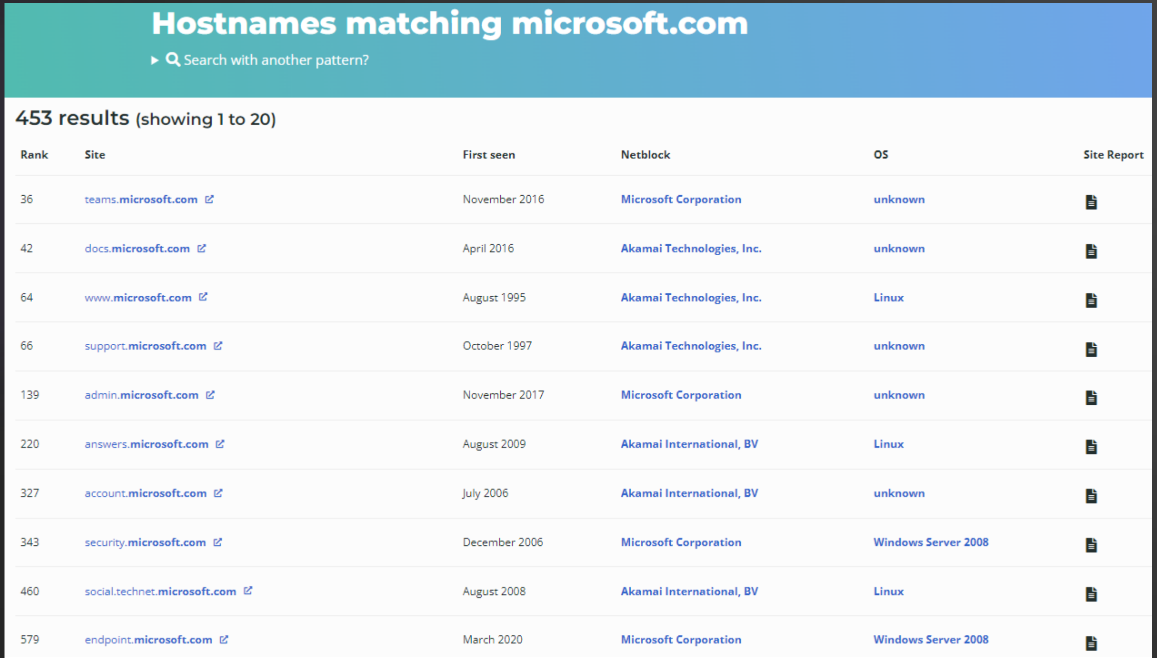
// **22** / TCP

OpenSSH 7.4

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC1fYp/nPjI9OUetmCEyTsEUCpEq1kDeKfrbf0f9A3I1+Xf
EJyqyWFmg5wPKHr+TBOHZizAWLzZGU9/U5Yt4ogKWBvd4aNIxh4yCKtrJrkY9GnXBt6bwlo1SDte
u8Wl2OB/R5NNxopRaqlSLhFc1AKmEX1nlivL2pE/ERmEl5/Fbfwjkjf92HhOvD157MpJB3dkmXBQ
nsbN/9BEzSn1CQ9vsB4zAhXC+w0Rkc2k1uyZV0N8dLXWe1taIDIhGFwzV/j1ECZtXM0TMeawAOEd
zG77XRHArd4Jo1q1fP2UXzWN8Jlu49FcqkLpYc/NB0wnSBY+HxBn08/QOVhHHA6W4XOB
Fingerprint: 11:e2:b6:fe:d1:9d:75:d4:fa:3c:3f:fc:66:b6:cb:f7

Kex Algorithms:
	curve25519-sha256
	curve25519-sha256@libssh.org
	ecdh-sha2-nistp256
	ecdh-sha2-nistp384
```

Netcraft

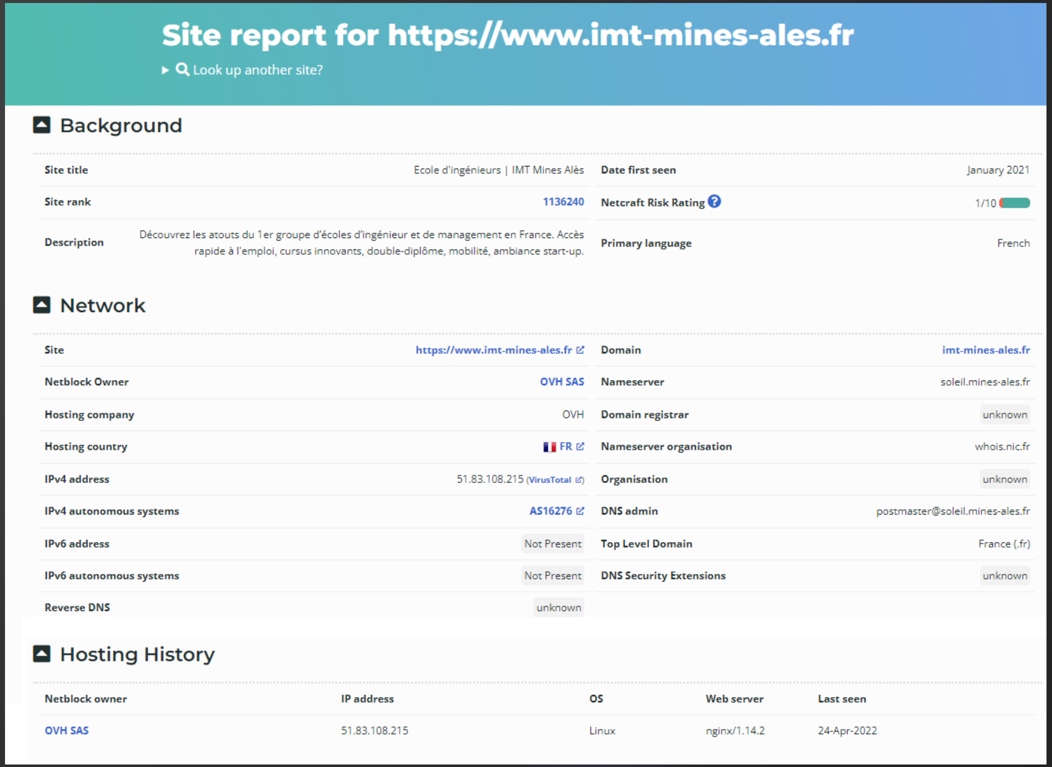
- Netcraft is a website to get information on a target company. We can find Top Level Domains and sub-domains and many others informations like nameserver, the hosting company, etc.



Hostnames matching microsoft.com

453 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS	Site Report
36	teams.microsoft.com	November 2016	Microsoft Corporation	unknown	
42	docs.microsoft.com	April 2016	Akamai Technologies, Inc.	unknown	
64	www.microsoft.com	August 1995	Akamai Technologies, Inc.	Linux	
66	support.microsoft.com	October 1997	Akamai Technologies, Inc.	unknown	
139	admin.microsoft.com	November 2017	Microsoft Corporation	unknown	
220	answers.microsoft.com	August 2009	Akamai International, BV	Linux	
327	account.microsoft.com	July 2006	Akamai International, BV	unknown	
343	security.microsoft.com	December 2006	Microsoft Corporation	Windows Server 2008	
460	social.technet.microsoft.com	August 2008	Akamai International, BV	Linux	
579	endpoint.microsoft.com	March 2020	Microsoft Corporation	Windows Server 2008	



Site report for https://www.imt-mines-ales.fr

Background

Site title	Ecole d'ingénieurs | IMT Mines Alès	Date first seen	January 2021
Site rank	1136240	Netcraft Risk Rating	1/10
Description	Découvrez les atouts du 1er groupe d'écoles d'ingénieur et de management en France. Accès rapide à l'emploi, cursus innovants, double-diplôme, mobilité, ambiance start-up.	Primary language	French

Network

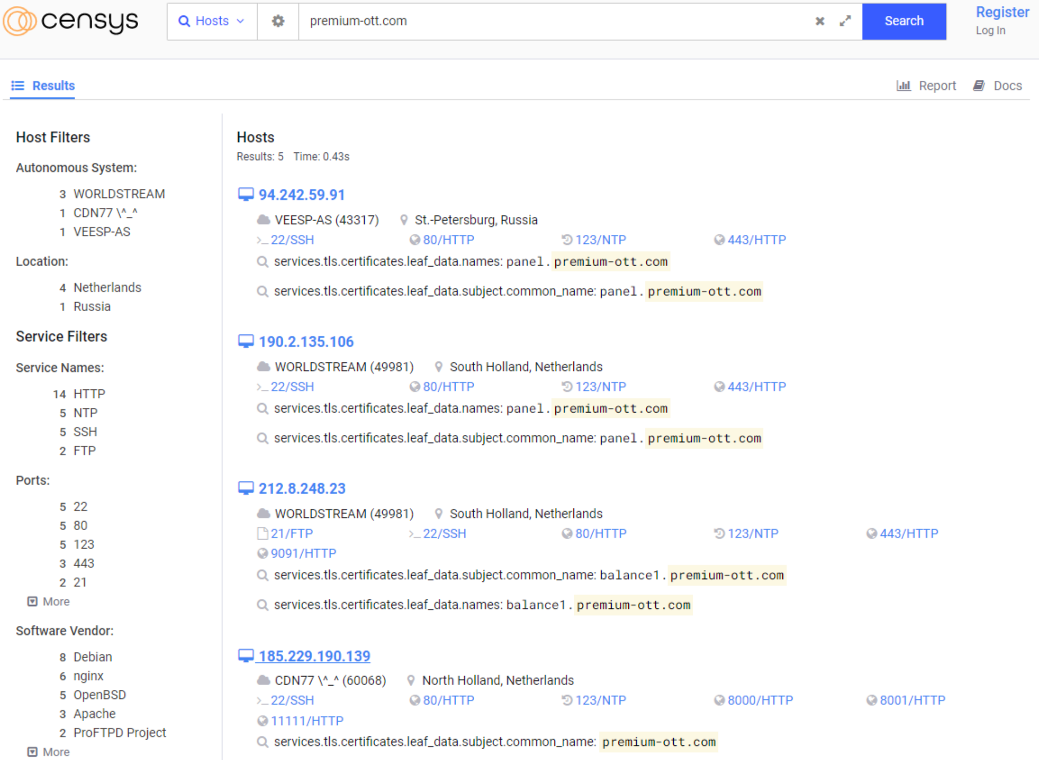
Site	https://www.imt-mines-ales.fr	Domain	imt-mines-ales.fr
Netblock Owner	OVH SAS	Nameserver	soleil.mines-ales.fr
Hosting company	OVH	Domain registrar	unknown
Hosting country	FR	Nameserver organisation	whois.nic.fr
IPv4 address	51.83.108.215 (VirusTotal)	Organisation	unknown
IPv4 autonomous systems	AS16276	DNS admin	postmaster@soleil.mines-ales.fr
IPv6 address	Not Present	Top Level Domain	France (.fr)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	unknown		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
OVH SAS	51.83.108.215	Linux	nginx/1.14.2	24-Apr-2022

Censys

- Censys is similar to Netcraft. It can monitors the infrastructure and discovers unknown assets anywhere on the internet.



premium-ott.com

Host Filters

Autonomous System:

3	WORLDSTREAM
1	CDN77 \^_^
1	VEESP-AS

Location:

4	Netherlands
1	Russia

Service Filters

Service Names:

14	HTTP
5	NTP
5	SSH
2	FTP

Ports:

5	22
5	80
5	123
3	443
2	21

More

Software Vendor:

8	Debian
6	nginx
5	OpenBSD
3	Apache
2	ProFTPD Project

More

Hosts

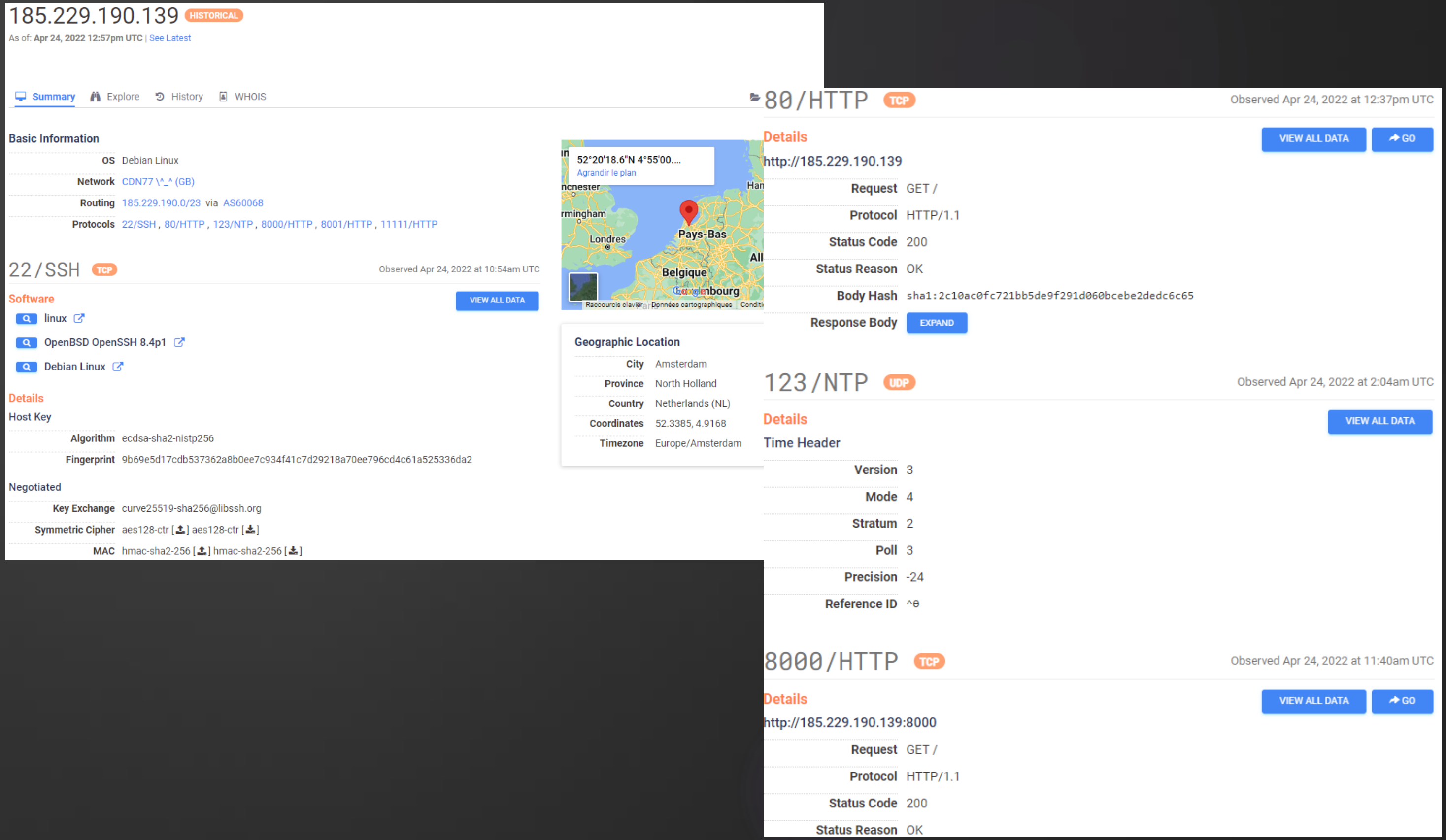
Results: 5 Time: 0.43s

94.242.59.91
VEESP-AS (43317) St.-Petersburg, Russia
22/SSH 80/HTTP 123/NTP 443/HTTP
services.tls.certificates.leaf_data.names: panel.premium-ott.com
services.tls.certificates.leaf_data.subject.common_name: panel.premium-ott.com

190.2.135.106
WORLDSTREAM (49981) South Holland, Netherlands
22/SSH 80/HTTP 123/NTP 443/HTTP
services.tls.certificates.leaf_data.names: panel.premium-ott.com
services.tls.certificates.leaf_data.subject.common_name: panel.premium-ott.com

212.8.248.23
WORLDSTREAM (49981) South Holland, Netherlands
21/FTP 22/SSH 80/HTTP 123/NTP 443/HTTP
9091/HTTP
services.tls.certificates.leaf_data.subject.common_name: balance1.premium-ott.com
services.tls.certificates.leaf_data.names: balance1.premium-ott.com

185.229.190.139
CDN77 \^_^ (60068) North Holland, Netherlands
22/SSH 80/HTTP 123/NTP 8000/HTTP 8001/HTTP
11111/HTTP
services.tls.certificates.leaf_data.subject.common_name: premium-ott.com



185.229.190.139

As of: Apr 24, 2022 12:57pm UTC | See Latest

Basic Information

OS	Debian Linux
Network	CDN77 \^_^ (GB)
Routing	185.229.190.0/23 via AS60068
Protocols	22/SSH, 80/HTTP, 123/NTP, 8000/HTTP, 8001/HTTP, 11111/HTTP

Geographic Location

City	Amsterdam
Province	North Holland
Country	Netherlands (NL)
Coordinates	52.3385, 4.9168
Timezone	Europe/Amsterdam

22/SSH — Observed Apr 24, 2022 at 10:54am UTC

Software
- linux
- OpenBSD OpenSSH 8.4p1
- Debian Linux

Details

Host Key

Algorithm	ecdsa-sha2-nistp256
Fingerprint	9b69e5d17cdb537362a8b0ee7c934f41c7d29218a70ee796cd4c61a525336da2

Negotiated

Key Exchange	curve25519-sha256@libssh.org
Symmetric Cipher	aes128-ctr [⬆] aes128-ctr [⬇]
MAC	hmac-sha2-256 [⬆] hmac-sha2-256 [⬇]

80/HTTP — Observed Apr 24, 2022 at 12:37pm UTC

Details

http://185.229.190.139

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:2c10ac0fc721bb5de9f291d060bcebe2dedc6c65
Response Body	EXPAND

123/NTP — Observed Apr 24, 2022 at 2:04am UTC

Details

Time Header

Version	3
Mode	4
Stratum	2
Poll	3
Precision	-24
Reference ID	^0

8000/HTTP — Observed Apr 24, 2022 at 11:40am UTC

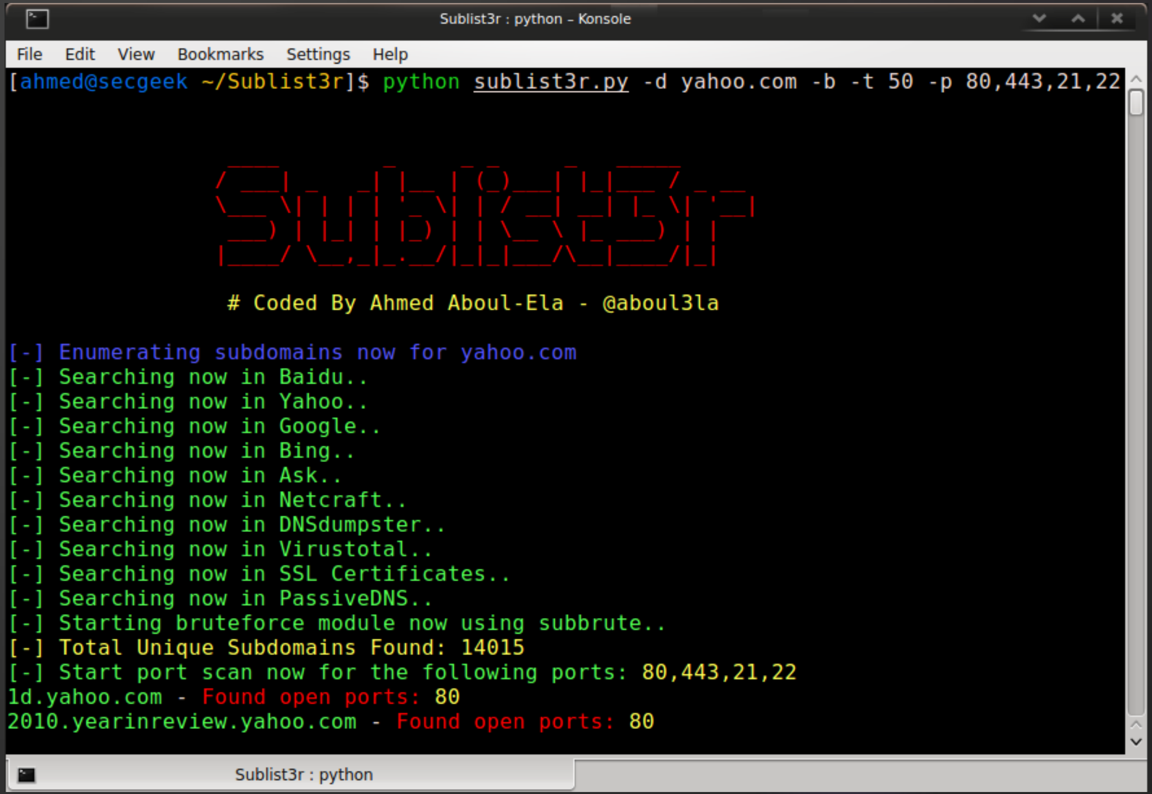
Details

http://185.229.190.139:8000

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK

Sublist3r

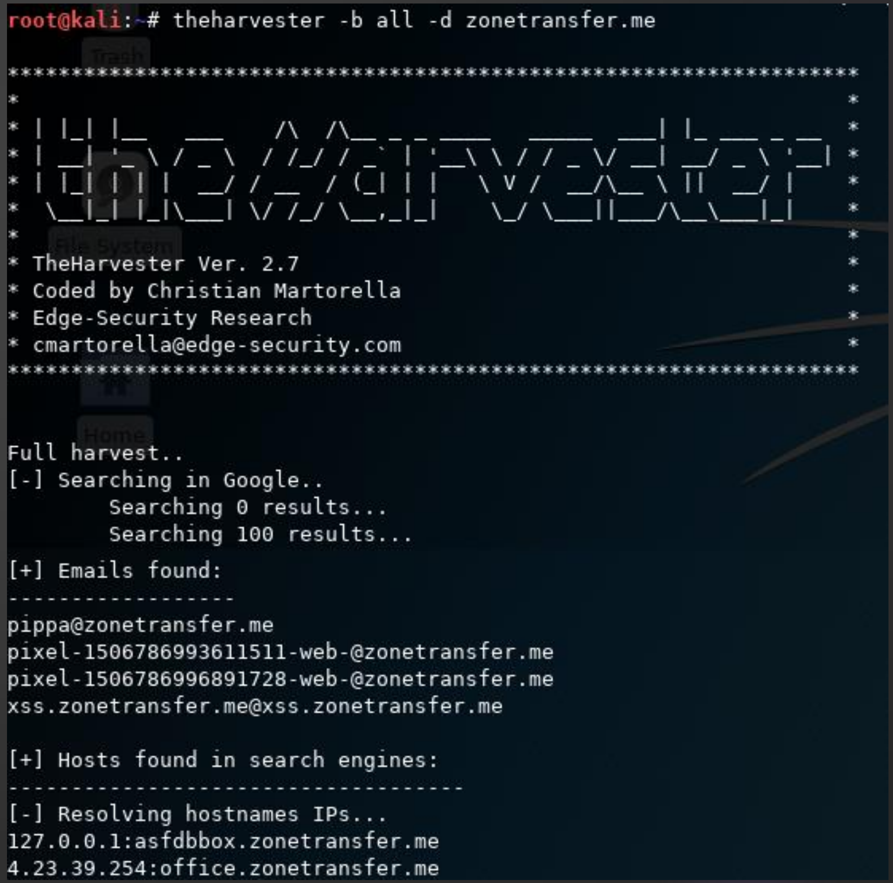
- **Sublist3r** is a python tool designed to enumerate subdomains of websites using OSINT with many search engines such as Google, Yahoo, Bing, Netcraft, Virustotal, ReverseDNS, etc.
- **subbrute** was integrated with **Sublist3r** to increase the possibility of finding more subdomains using bruteforce with an improved wordlist (active reconnaissance).



```
[ahmed@secgeek ~/Sublist3r]$ python sublist3r.py -d yahoo.com -b -t 50 -p 80,443,21,22

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for yahoo.com
[-] 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 SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Starting bruteforce module now using subbrute..
[-] Total Unique Subdomains Found: 14015
[-] Start port scan now for the following ports: 80,443,21,22
1d.yahoo.com - Found open ports: 80
2010.yearinreview.yahoo.com - Found open ports: 80
```

TheHarvester

- **TheHarvester** is a tool for gathering e-mail accounts and subdomain names from public sources.



```
root@kali:~# theharvester -b all -d zonetransfer.me

*******************************************************************
*                                                                 *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* TheHarvester Ver. 2.7                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************


Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[+] Emails found:
------------------
pippa@zonetransfer.me
pixel-1506786993611511-web-@zonetransfer.me
pixel-1506786996891728-web-@zonetransfer.me
xss.zonetransfer.me@xss.zonetransfer.me

[+] Hosts found in search engines:
------------------------------------
[-] Resolving hostnames IPs...
127.0.0.1:asfdbbox.zonetransfer.me
4.23.39.254:office.zonetransfer.me
```

Deep and Dark Web Footprinting

- **Deep web:**
  - it consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines.
  - Example is that of a banking website which has a public part, referenced by search engines, and a private part, which concerns the customer's banking information and is behind an authentication mechanism. The second is accessible to the client but not to the search engine.
- **Dark web / Darknet:**
  - Isn’t indexed and not accessible the web by standard means.
  - It’s generally used to refer to the criminal web and it’s accessible only with TOR Browser.
- **TOR Browser:**
  - it’s used to access the deep and dark web where it acts as default VPN fot the user and bounces the network IP address through several servers before interacting with the web.

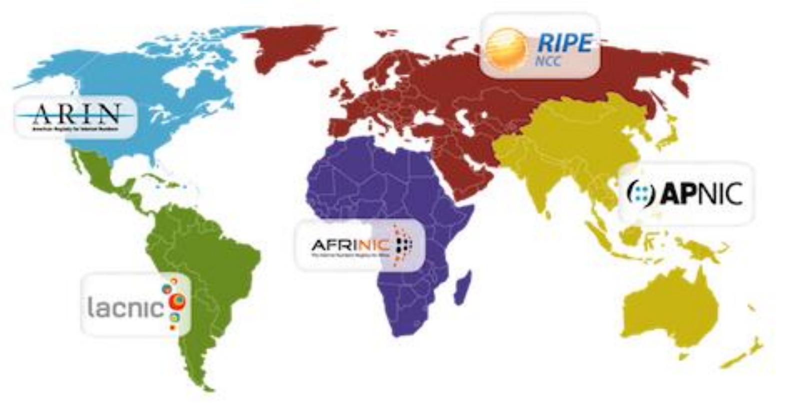
TODO Fingerprint with Burp

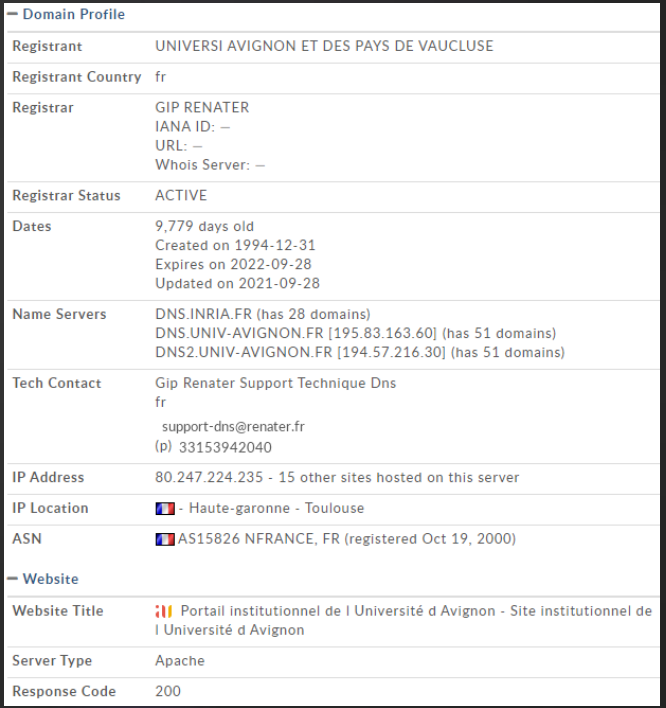
Nslookup, Whois, DNSStuff, etc.

- Nslookup is a tool for querying the DNS to obtain domain name or IP address mapping, or other DNS records.
- Whois is a query and response protocol that is widely used for querying databases that store multiple records :
  - the registered users ;
  - domain name ;
  - IP address block ;
  - Etc.
- Many command line tools exist, but other tools have been created to make life easier for attackers (they concatenate manual tools).

Whois Lookup

- IANA (Internet Assigned Numbers Authority) is a standards organization that oversees global IP address allocation.
- Following the Internet's rapid expansion across the world, IANA was no longer able to respond to all requests.
- In 1992, the Internet Engineering Task Force (IETF) recommended that Internet number resources be managed by subsidiary organizations at a regional level.
- Whois databases are maintained by RIR (Regional Internet Registries) and contain personal information of domain owners.
- Whois query returns:
  - Domain name details
  - Contact details of domain owners
  - Domain name servers
  - Netrange
  - When a domain was created
  - Expiry records
  - Last updated record





Domain Profile

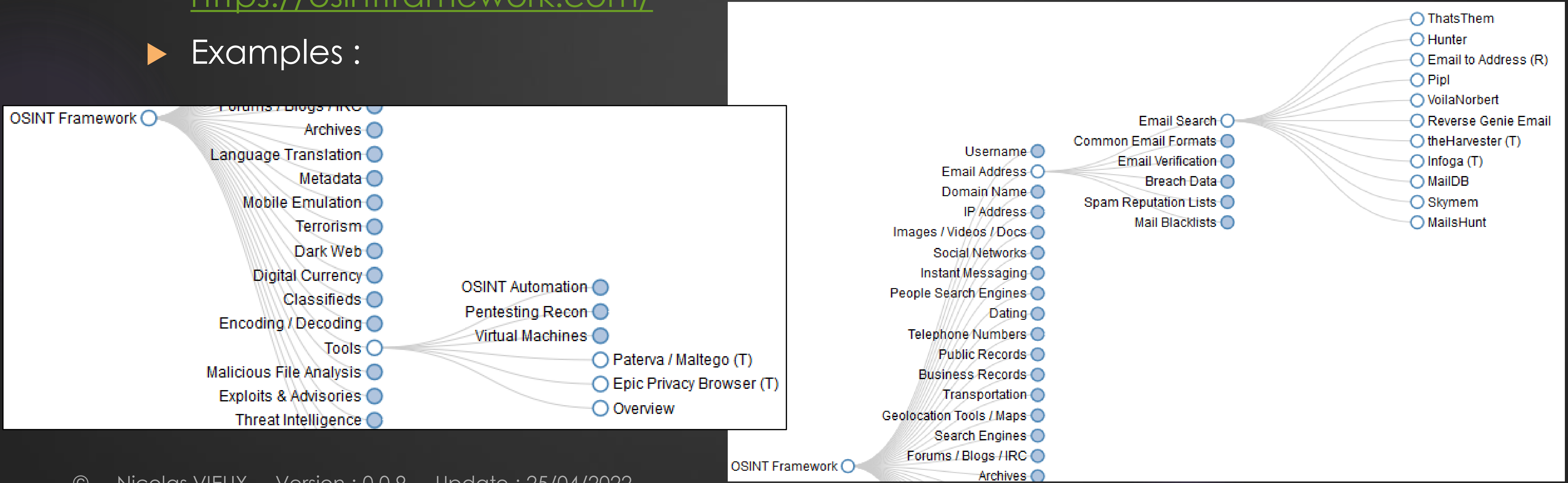
Registrant	UNIVERSI AVIGNON ET DES PAYS DE VAUCLUSE
Registrant Country	fr
Registrar	GIP RENATER IANA ID: – URL: – Whois Server: –
Registrar Status	ACTIVE
Dates	9,779 days old Created on 1994-12-31 Expires on 2022-09-28 Updated on 2021-09-28
Name Servers	DNS.INRIA.FR (has 28 domains) DNS.UNIV-AVIGNON.FR [195.83.163.60] (has 51 domains) DNS2.UNIV-AVIGNON.FR [194.57.216.30] (has 51 domains)
Tech Contact	Gip Renater Support Technique Dns fr support-dns@renater.fr (p) 33153942040
IP Address	80.247.224.235 - 15 other sites hosted on this server
IP Location	- Haute-garonne - Toulouse
ASN	AS15826 NFRANCE, FR (registered Oct 19, 2000)

Website

Website Title	Portail institutionnel de l Université d Avignon - Site institutionnel de l Université d Avignon
Server Type	Apache
Response Code	200

OSINT

- OSINT (Open-source intelligence) is a framework focused on gathering information from free tools or resources: https://osintframework.com/
- Examples :



OSINT Framework

Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence

OSINT Automation
Pentesting Recon
Virtual Machines
Paterva / Maltego (T)
Epic Privacy Browser (T)
Overview

OSINT Framework

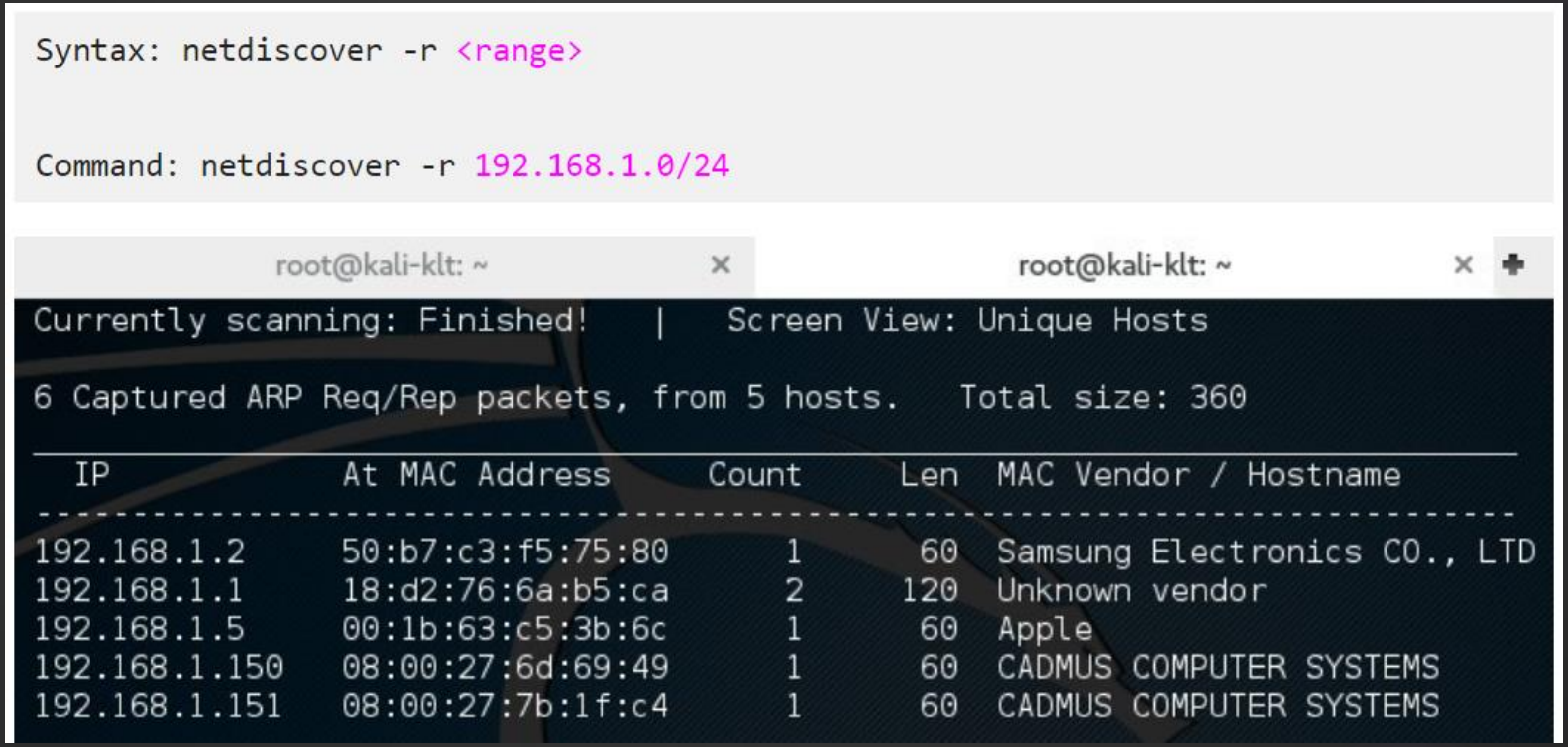
Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives

Email Search
Common Email Formats
Email Verification
Breach Data
Spam Reputation Lists
Mail Blacklists

ThatsThem
Hunter
Email to Address (R)
Pipl
VoilaNorbert
Reverse Genie Email
theHarvester (T)
Infoga (T)
MailDB
Skymem
MailsHunt

Netdiscover

- Netdiscover is a network address discovering tool.

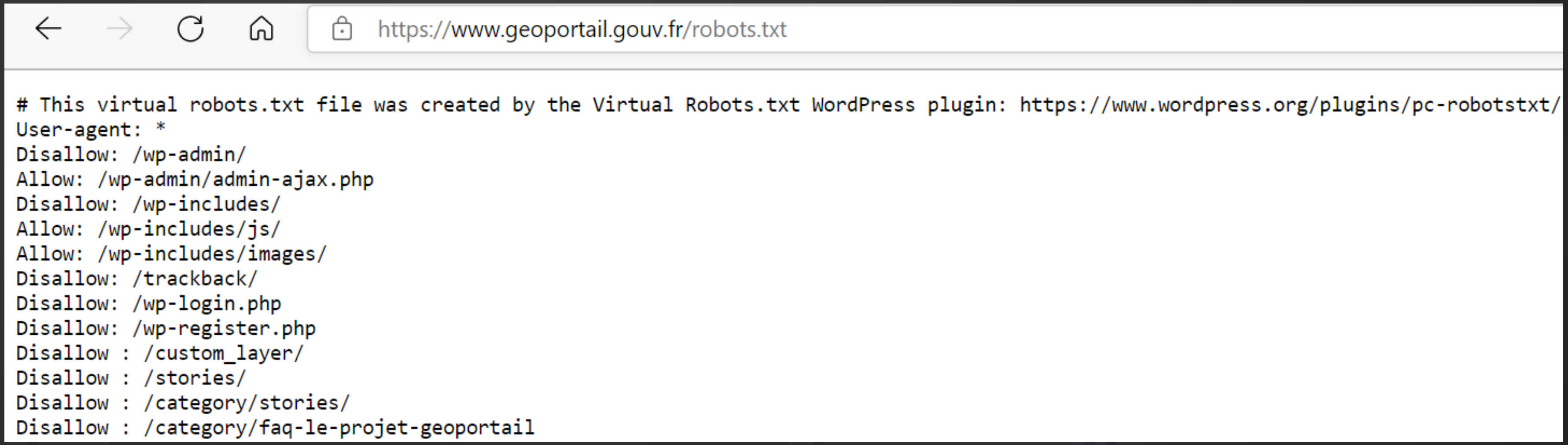


```
Syntax: netdiscover -r <range>


Command: netdiscover -r 192.168.1.0/24
```

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 360
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.2     50:b7:c3:f5:75:80      1      60  Samsung Electronics CO., LTD
192.168.1.1     18:d2:76:6a:b5:ca      2     120  Unknown vendor
192.168.1.5     00:1b:63:c5:3b:6c      1      60  Apple
192.168.1.150   08:00:27:6d:69:49      1      60  CADMUS COMPUTER SYSTEMS
192.168.1.151   08:00:27:7b:1f:c4      1      60  CADMUS COMPUTER SYSTEMS
```

robots.txt file

- The robots.txt file contains the list of the web server directories and files that the web site owner wants to hide from web crawlers.
- An attacker can simply request the robots.txt file from the URL and retrieve sensitive information such as the root directory structure and content management system information about the target.
- Example:



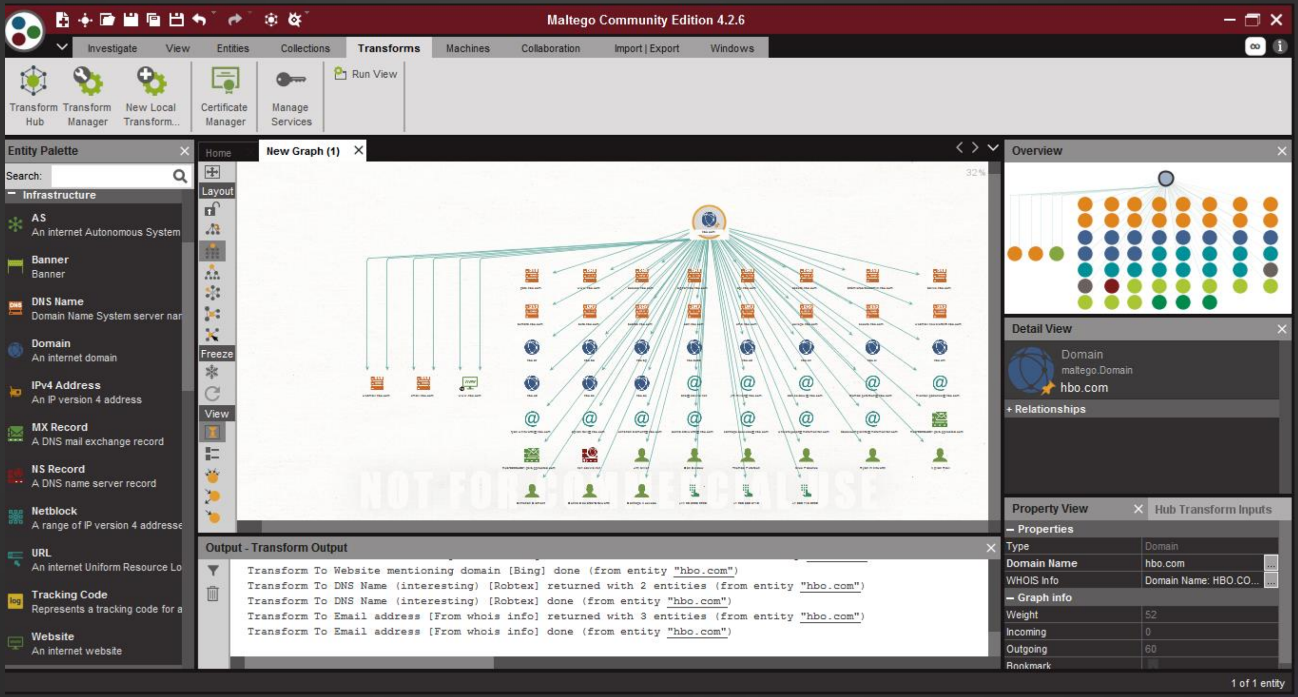
```
# This virtual robots.txt file was created by the Virtual Robots.txt WordPress plugin: https://www.wordpress.org/plugins/pc-robotstxt/
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
Disallow: /wp-includes/
Allow: /wp-includes/js/
Allow: /wp-includes/images/
Disallow: /trackback/
Disallow: /wp-login.php
Disallow: /wp-register.php
Disallow : /custom_layer/
Disallow : /stories/
Disallow : /category/stories/
Disallow : /category/faq-le-projet-geoportail
```

Web Server Footprinting / Banner Grabing

- Telnet is a protocol that can be used to footprint an asset (and therefore a web server):
  - Server name;
  - Server type;
  - OS;
  - Application;
  - Application version;
  - Etc.
- Use tools such as Netcraft, httprecon, ID Serve and other to automate footprinting.

Maltego

- **Maltego** is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks. Website : https://www.maltego.com/



AS
An internet Autonomous System

Banner
Banner

DNS Name
Domain Name System server nar

Domain
An internet domain

IPv4 Address
An IP version 4 address

MX Record
A DNS mail exchange record

NS Record
A DNS name server record

Netblock
A range of IP version 4 addresse

URL
An internet Uniform Resource Lo

Tracking Code
Represents a tracking code for a

Website
An internet website

Output - Transform Output

```
Transform To Website mentioning domain [Bing] done (from entity "hbo.com")
Transform To DNS Name (interesting) [Robtex] returned with 2 entities (from entity "hbo.com")
Transform To DNS Name (interesting) [Robtex] done (from entity "hbo.com")
Transform To Email address [From whois info] returned with 3 entities (from entity "hbo.com")
Transform To Email address [From whois info] done (from entity "hbo.com")
```

Detail View

Domain
maltego.Domain
hbo.com

+ Relationships

Property View | Hub Transform Inputs

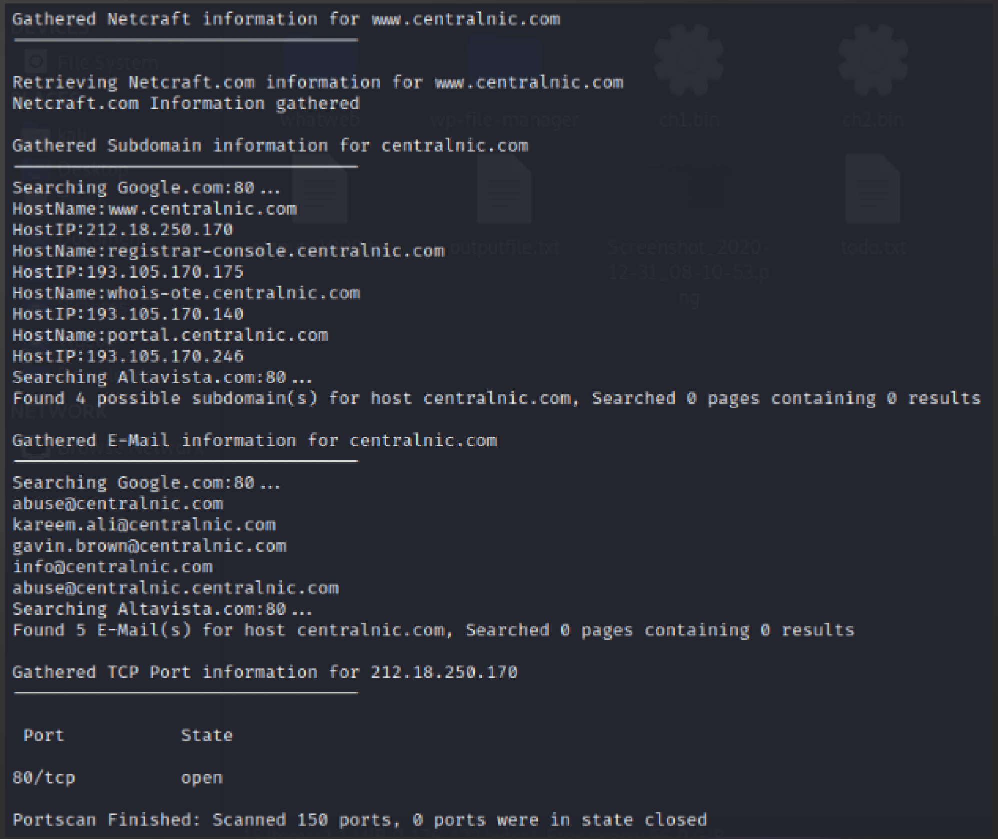
– Properties	
Type	Domain
Domain Name	hbo.com
WHOIS Info	Domain Name: HBO.CO...
– Graph info	
Weight	52
Incoming	0
Outgoing	60
Bookmark	

1 of 1 entity

DMitry

- **Dmitry** has the ability to gather as much information as possible about a host (subdomains, email addresses, uptime information, whois lookups, , tcp port scan etc.).

- Port scan is active reconnaissance.



```
Gathered Netcraft information for www.centralnic.com
---------------------------------

Retrieving Netcraft.com information for www.centralnic.com
Netcraft.com Information gathered

Gathered Subdomain information for centralnic.com
---------------------------------
Searching Google.com:80...
HostName:www.centralnic.com
HostIP:212.18.250.170
HostName:registrar-console.centralnic.com
HostIP:193.105.170.175
HostName:whois-ote.centralnic.com
HostIP:193.105.170.140
HostName:portal.centralnic.com
HostIP:193.105.170.246
Searching Altavista.com:80...
Found 4 possible subdomain(s) for host centralnic.com, Searched 0 pages containing 0 results

Gathered E-Mail information for centralnic.com
---------------------------------
Searching Google.com:80...
abuse@centralnic.com
kareem.ali@centralnic.com
gavin.brown@centralnic.com
info@centralnic.com
abuse@centralnic.centralnic.com
Searching Altavista.com:80...
Found 5 E-Mail(s) for host centralnic.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 212.18.250.170
---------------------------------

 Port           State

80/tcp          open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed
```

Website mirroring

- Mirror a website to create a complete profile of the site's directory structure, file structures, external links, etc.
- Search for comments and other items in the HTML source code to make footprinting activities more efficient.
- Use tools such as NCollector Studio, HTTrack Web Site Copier, WebCopier Pro, etc. to mirror a website.

Other tools list

- Recon-ng;
- Uniscan;
- Nmap;
- Ghost Eye;
- Skip fish;
- Etc.