# Attack Methodology

PASSIVE RECONNAISSANCE DURATION: 0'30

### OSINT



ThatsThem

OSINT (Open-source intelligence) is a framework focused on gathering information from free tools or resources:

https://osintframework.com/

Examples:



### Netdiscover



▶ Netdiscover is a network address discovering tool.

Syntax: netdiscover -r <range></range>					
Command: netdis	cover -r 192.168.1.0	/24			
roc	ot@kali-klt: ~	×	root@kali-klt: ~	× +	
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 / Hos	tname	
192.168.1.2	50:b7:c3:f5:75:80	1	60 Samsung Electron	ics CO., LTD	
192.168.1.1	18:d2:76:6a:b5:ca		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	

## 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, it became clear that even IANA would be unable to scale to meet the demand for addresses or be able to service the wide range of different regional needs. 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





<ul> <li>Domain Profile</li> </ul>	
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 - Website	AS15826 NFRANCE, FR (registered Oct 19, 2000)
Website Title	;     Portail institutionnel de l'Université d'Avignon - Site institutionnel de l'Université d'Avignon
Server Type	Apache
Response Code	200

#### 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/
Allow: /wp-includes/is/
Allow: /wp-includes/images/
Disallow: /trackback/
Disallow: /wp-login.php
Disallow: /wp-register.php
Disallow: /wp-register.php
Disallow: /custom_layer/
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.



# Google Hacking Database (GHDB) 1/2



- 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: <a href="https://www.exploit-db.com/google-hacking-database">https://www.exploit-db.com/google-hacking-database</a>
- 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 ('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');
```

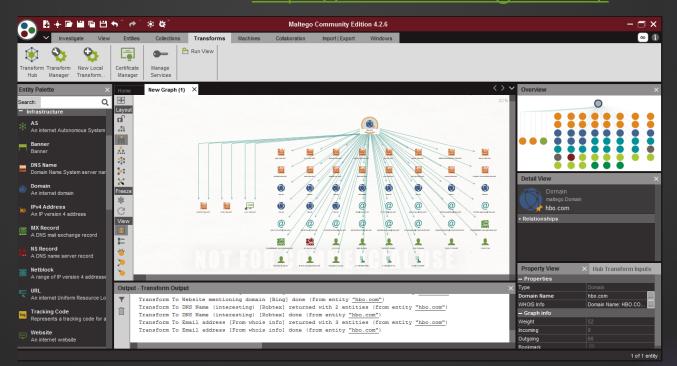
# Google Hacking Database (GHDB)



- 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:]  $\rightarrow$  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.

## Maltego

Maltego is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks. Website: <a href="https://www.maltego.com/">https://www.maltego.com/</a>



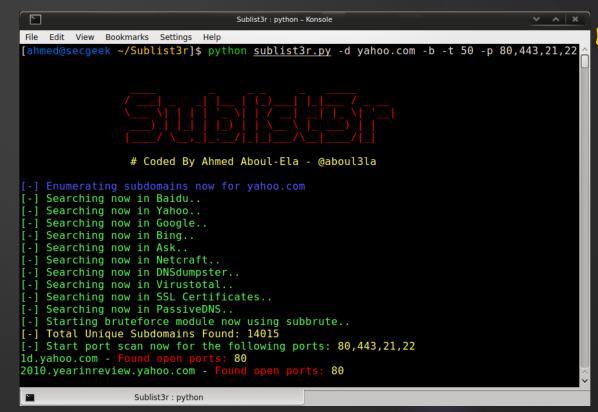


### Sublist3r

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.

with **Sublist3r** to increase the possibility of finding more subdomains using bruteforce with an improved wordlist (active reconnaissance).



### TheHarvester

▶ **TheHarvester** is a tool for gathering e-mail accounts and subdomain

names from public sources.





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

### Other tools list

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

## 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.