OUTILS SOUS KALI

Découvertes des outils de base pour le pentest

SOMMAIRE

- **Nmap**
- Legion
- John
- SqlMap
- Dmitry
- Wireshark
- Burp
- Binwalk
- Versatility
- ExifTools
- Aircrack-ng

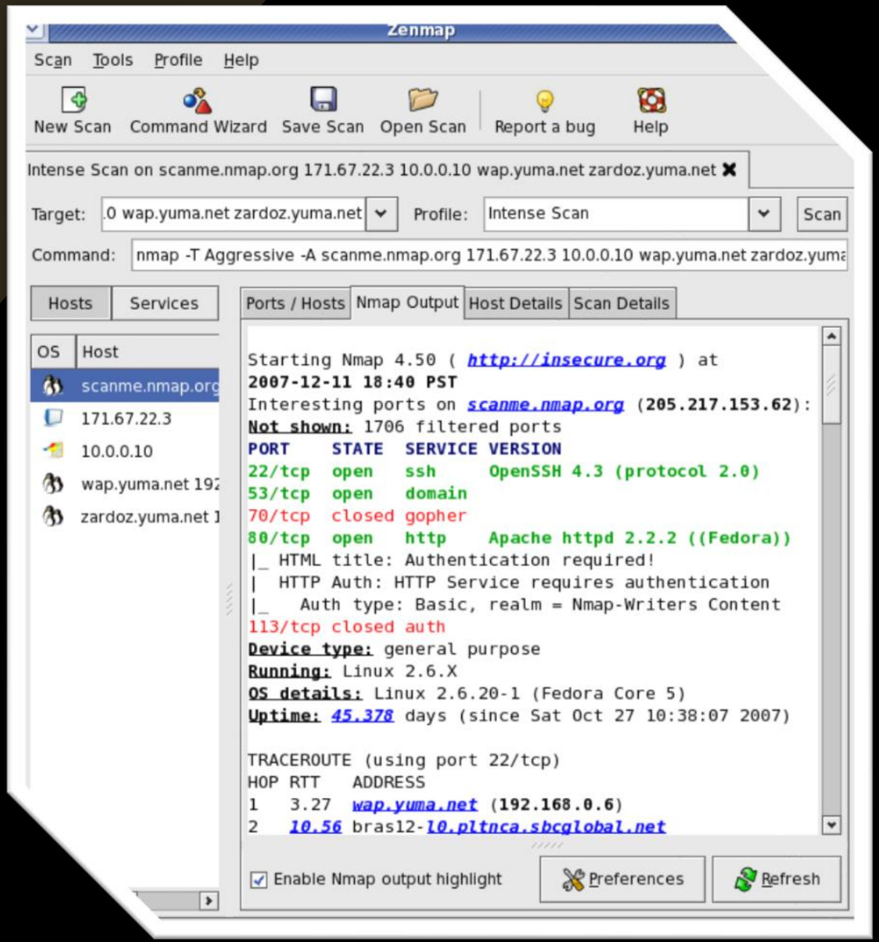
Nmap

Network discovery

- Very modular
- Easy to use but with a great learning curve
- Must
- TCP/UDP/Ports/RangeIp
- « Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant »

https://nmap.org/

NMAP



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net ✖

Target: .0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

OS	Host
	scanme.nmap.org
	171.67.22.3
	10.0.0.10
	wap.yuma.net 192
	zardoz.yuma.net 1

```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

☑ Enable Nmap output highlight

Help

❖ sudo nmap –h

Port-range

❖ sudo nmap ip_addr –pl-3000

TCP SYN

❖ sudo nmap ip_addr -sS

TCP FULL CONNECT (HandShake)

❖ sudo nmap ip_addr –sT

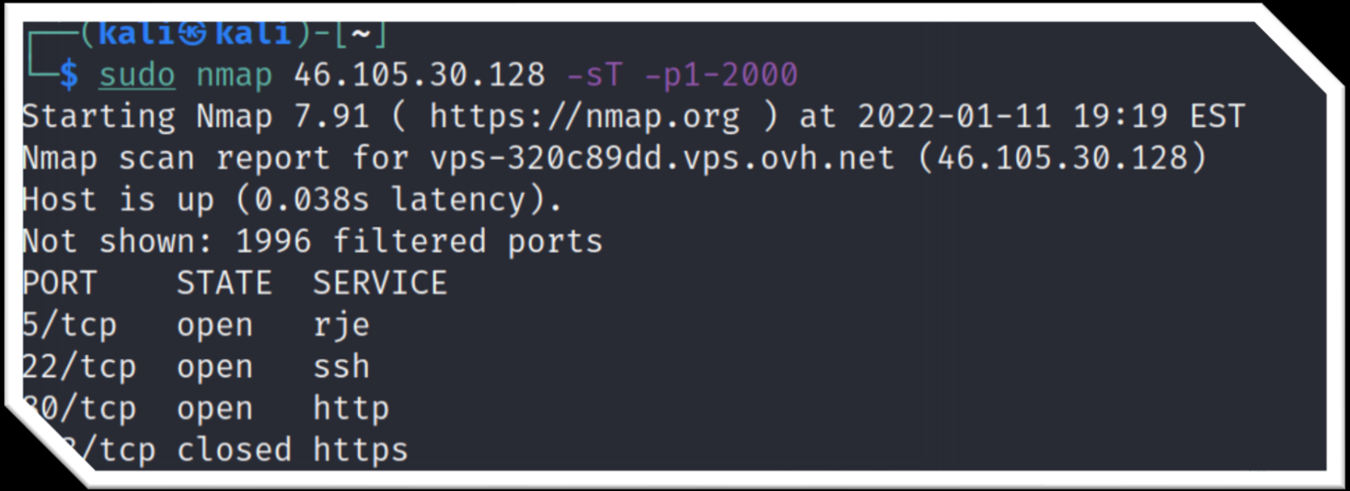
OS

❖ sudo nmap ip_addr –O

A faire : run le nc sur le serveur

Nmap | Your turn

- Trouvez le port ouvert en TCP sur drahoxx.fr (entre 1 et 100)



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 46.105.30.128 -sT -p1-2000
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-11 19:19 EST
Nmap scan report for vps-320c89dd.vps.ovh.net (46.105.30.128)
Host is up (0.038s latency).
Not shown: 1996 filtered ports
PORT     STATE  SERVICE
5/tcp    open   rje
22/tcp   open   ssh
80/tcp   open   http
  3/tcp closed https
```

SOMMAIRE

- Nmap
- **Legion**
- John
- SqlMap
- Dmitry
- Wireshark
- Burp
- Binwalk
- Versatility
- ExifTools
- Aircrack-ng

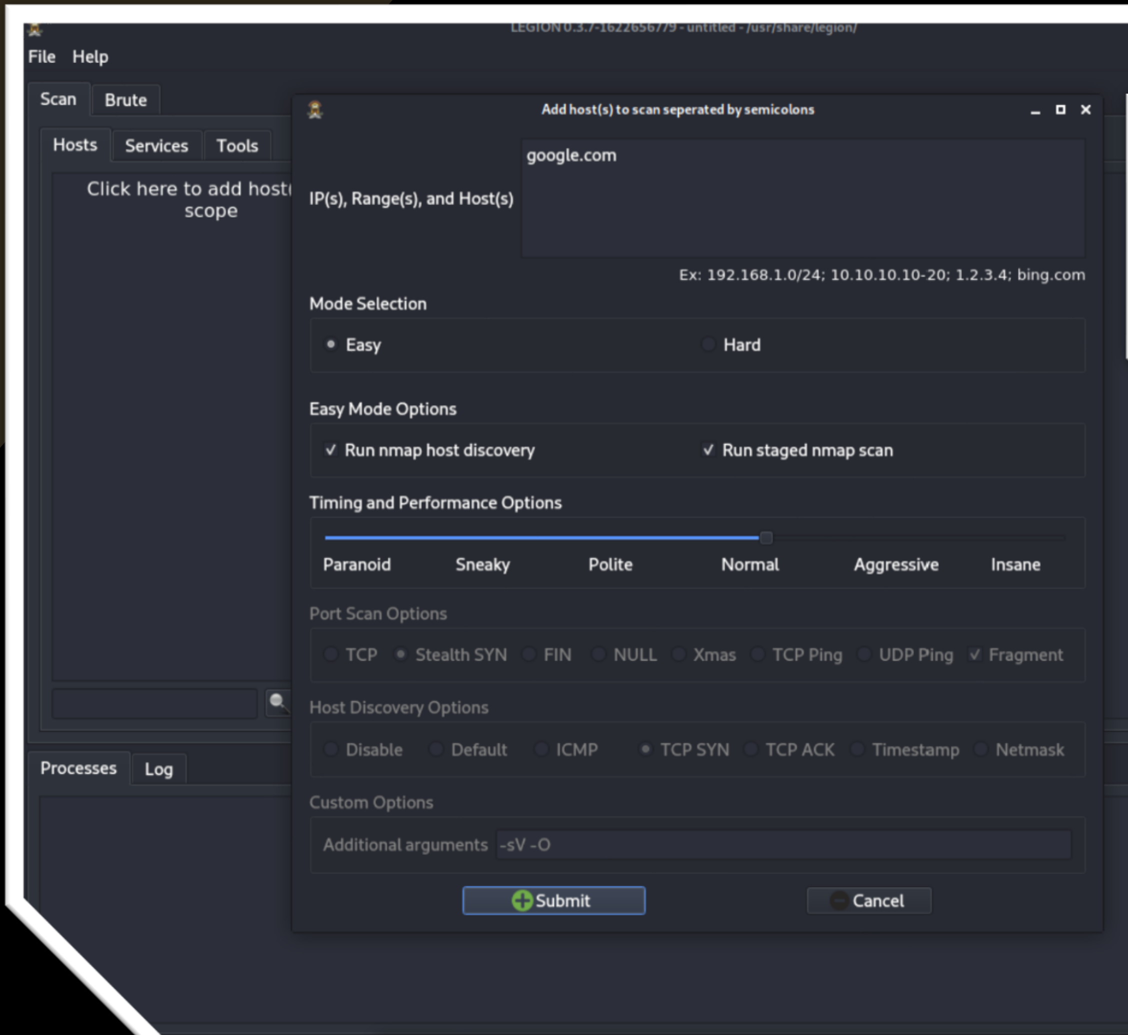
LEGION

Recon, discovery

- NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer
- Graphical interface
- Auto CPEs (Common Platform Enumeration) and CVEs (Common Vulnerabilities and Exposures) discorvery

https://kalilinuxtutorials.com/legion-penetration-testing/

LEGION



LEGION 0.3.7-1622656779 - untitled - /usr/share/legion/
File Help
Scan Brute
Hosts Services Tools
Click here to add host to
scope
Processes Log

Add host(s) to scan seperated by semicolons

IP(s), Range(s), and Host(s): google.com

Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com

Mode Selection

● Easy ○ Hard

Easy Mode Options

✓ Run nmap host discovery ✓ Run staged nmap scan

Timing and Performance Options

Paranoid Sneaky Polite Normal Aggressive Insane

Port Scan Options

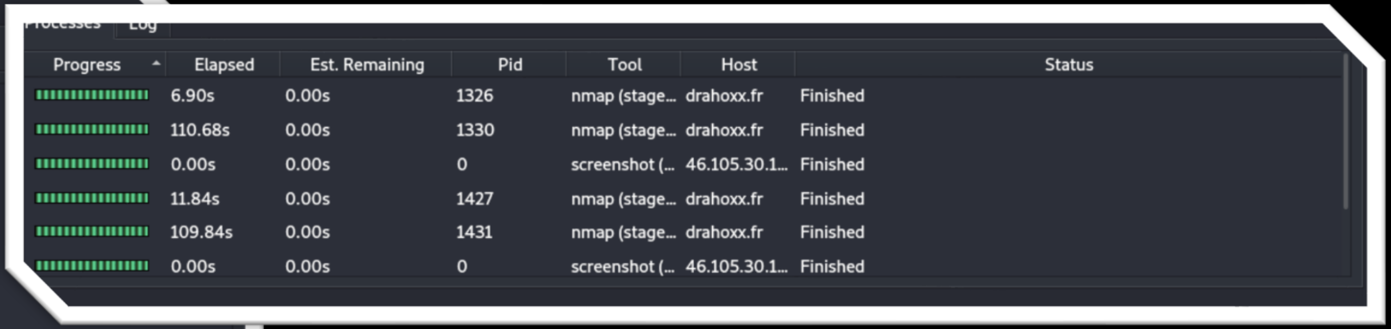
○ TCP ● Stealth SYN ○ FIN ○ NULL ○ Xmas ○ TCP Ping ○ UDP Ping ✓ Fragment

Host Discovery Options

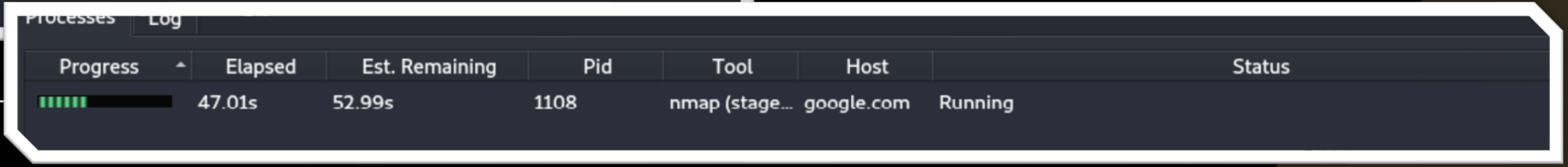
○ Disable ○ Default ○ ICMP ● TCP SYN ○ TCP ACK ○ Timestamp ○ Netmask

Custom Options

Additional arguments -sV -O



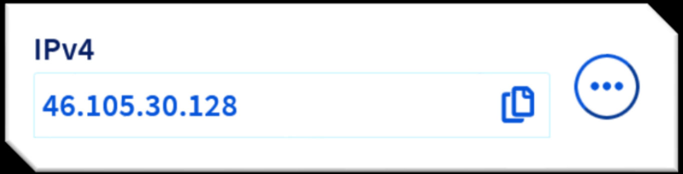
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
▮▮▮▮▮▮▮▮▮▮	6.90s	0.00s	1326	nmap (stage...	drahoxx.fr	Finished
▮▮▮▮▮▮▮▮▮▮	110.68s	0.00s	1330	nmap (stage...	drahoxx.fr	Finished
▮▮▮▮▮▮▮▮▮▮	0.00s	0.00s	0	screenshot (...	46.105.30.1...	Finished
▮▮▮▮▮▮▮▮▮▮	11.84s	0.00s	1427	nmap (stage...	drahoxx.fr	Finished
▮▮▮▮▮▮▮▮▮▮	109.84s	0.00s	1431	nmap (stage...	drahoxx.fr	Finished
▮▮▮▮▮▮▮▮▮▮	0.00s	0.00s	0	screenshot (...	46.105.30.1...	Finished



Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
▮▮▮▮▮▮	47.01s	52.99s	1108	nmap (stage...	google.com	Running

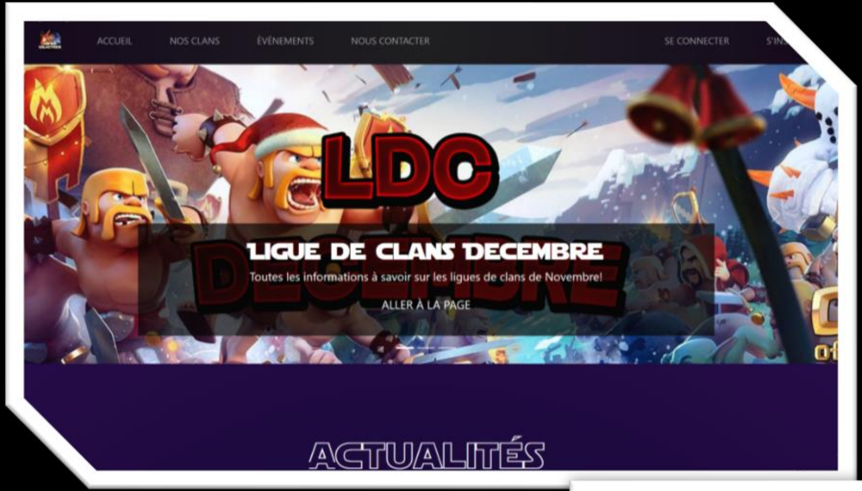
Legion | Your turn

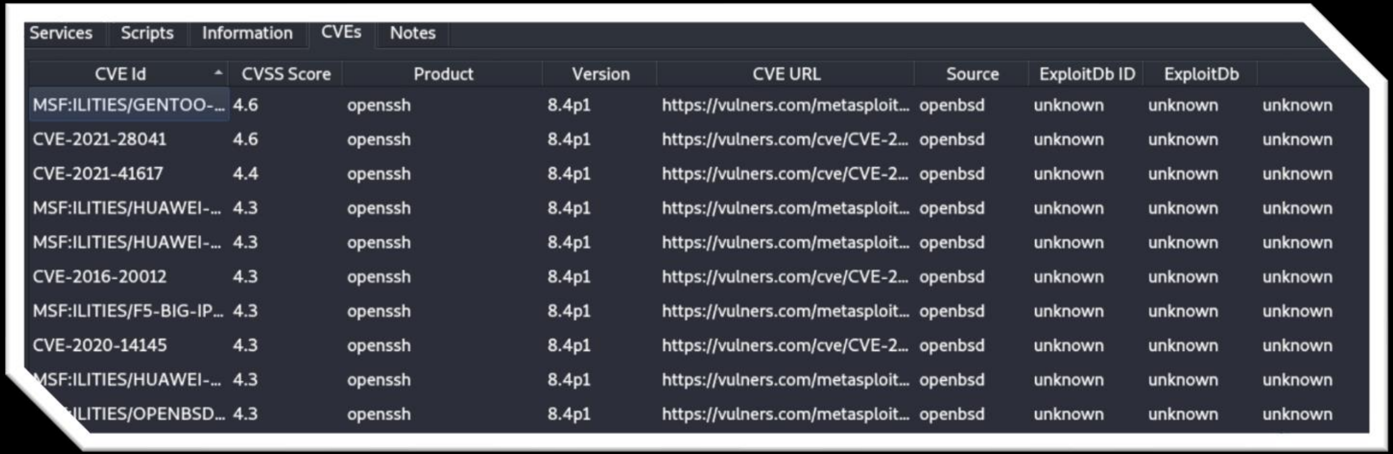
- IP associée à drahoxx.fr
- Screenshot du site caché
- Version du serveur web



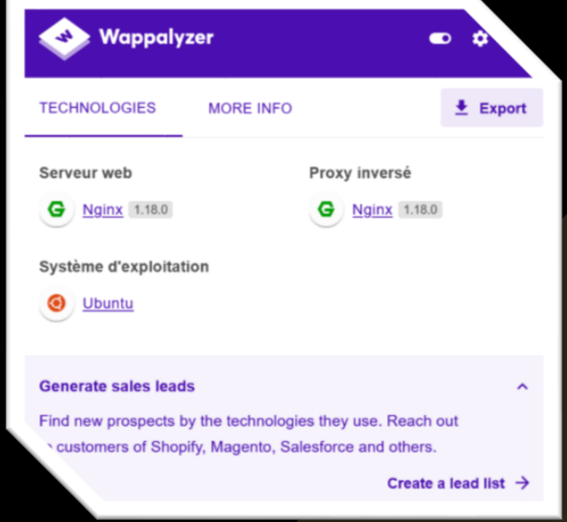
IPv4

46.105.30.128





CVE Id	CVSS Score	Product	Version	CVE URL	Source	ExploitDb ID	ExploitDb	
MSF:ILITIES/GENTOO-...	4.6	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown
CVE-2021-28041	4.6	openssh	8.4p1	https://vulners.com/cve/CVE-2...	openbsd	unknown	unknown	unknown
CVE-2021-41617	4.4	openssh	8.4p1	https://vulners.com/cve/CVE-2...	openbsd	unknown	unknown	unknown
MSF:ILITIES/HUAWEI-...	4.3	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown
MSF:ILITIES/HUAWEI-...	4.3	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown
CVE-2016-20012	4.3	openssh	8.4p1	https://vulners.com/cve/CVE-2...	openbsd	unknown	unknown	unknown
MSF:ILITIES/F5-BIG-IP...	4.3	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown
CVE-2020-14145	4.3	openssh	8.4p1	https://vulners.com/cve/CVE-2...	openbsd	unknown	unknown	unknown
MSF:ILITIES/HUAWEI-...	4.3	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown
ILITIES/OPENBSD...	4.3	openssh	8.4p1	https://vulners.com/metasploit...	openbsd	unknown	unknown	unknown



Serveur web: Nginx 1.18.0

Proxy inversé: Nginx 1.18.0

Système d'exploitation: Ubuntu

Generate sales leads

Find new prospects by the technologies they use. Reach out customers of Shopify, Magento, Salesforce and others.

Create a lead list →

SOMMAIRE

- Nmap
- Legion
- **John**
- WPScan
- Dirbuster
- Wireshark
- Burp
- Binwalk
- Versatility
- ExifTools
- Aircrack-ng

John

Hash cracking

- Rapide, clair, simple
- Moins opti que hashcat pour certains algos
- Outils comme zip2john pour cracker des zips

https://miloserdov.org/?p=5960

John

- Basic use :

```
john file.txt
```

- Wordlist :

```
john file.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

- Format :

```
john file.txt --format=raw-md5
```

- Format lists :

```
john --list=formats
```

- Dynamic Format :

```
john --format=dynamic=‘sha256(md5($p).$cl),$cl=cte' --wordlist=/usr/share/wordlists/rockyou.txt lm.txt
```

> https://miloserdov.org/?p=5960

John | Your turn

- Crackez ces hashs :

  5d41402abc4b2a76b9719d911017c592

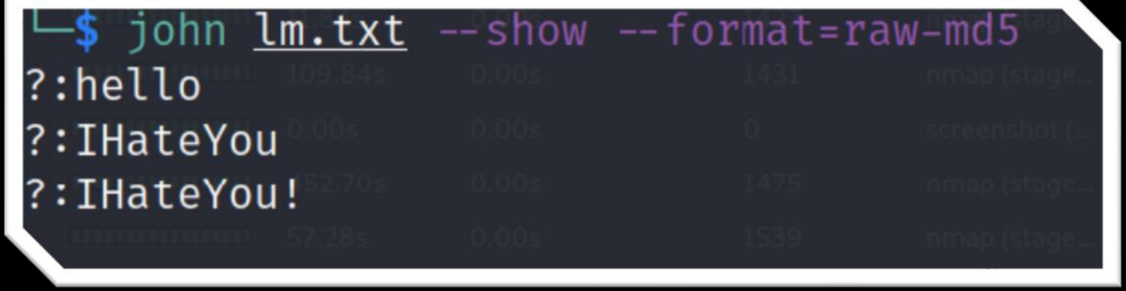
  d30b8241523d7dd29e499d0f6231cfbd

  479b750ad6efefb464b533b2d84416a7

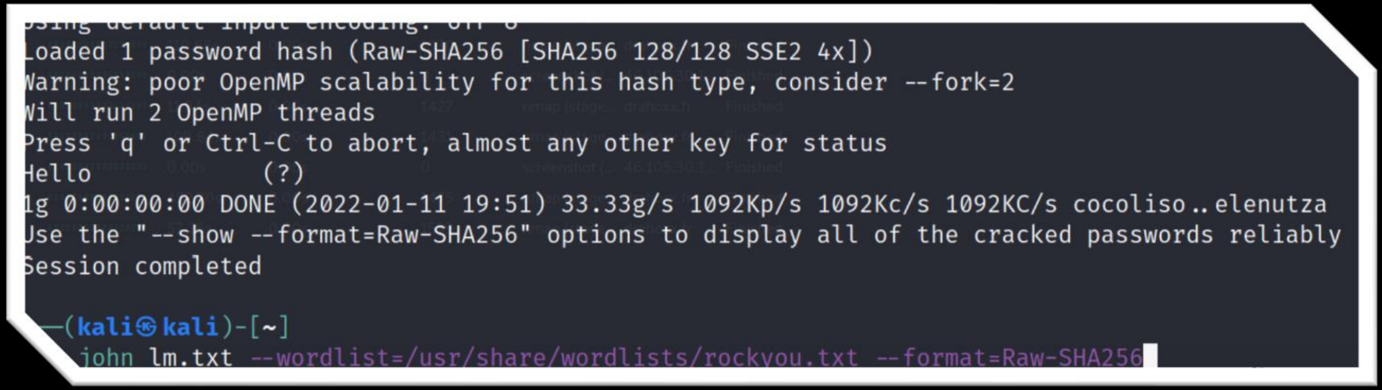
  185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

  f3115e0406b7ad2a0632e50dc2358480

  > md5(sha256(password) + ’lol’)

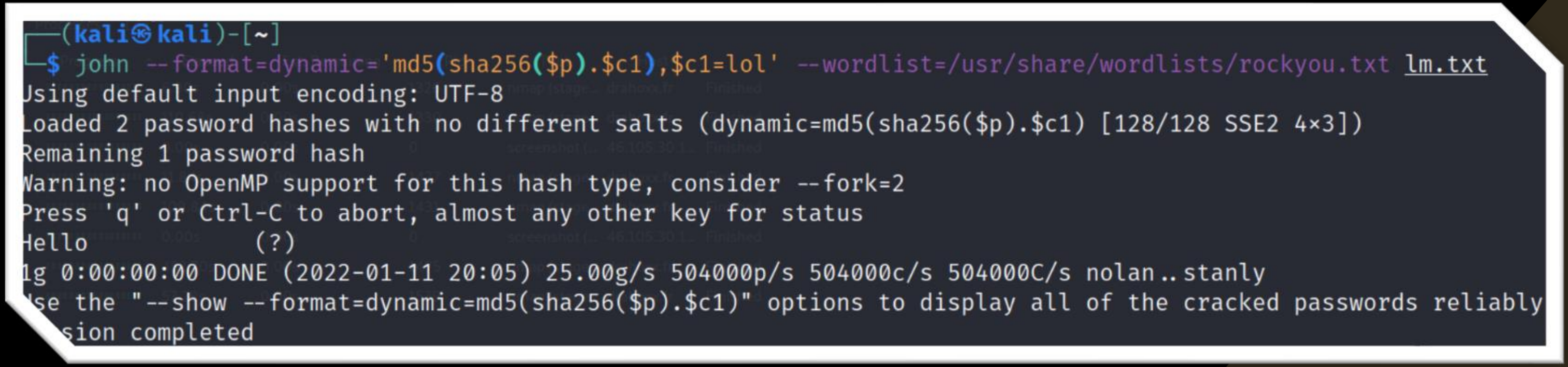


```
└─$ john lm.txt --show --format=raw-md5
?:hello
?:IHateYou
?:IHateYou!
```



```
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 SSE2 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Hello            (?)
1g 0:00:00:00 DONE (2022-01-11 19:51) 33.33g/s 1092Kp/s 1092Kc/s 1092KC/s cocoliso..elenutza
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~]
└─$ john lm.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-SHA256
```



```
┌──(kali㉿kali)-[~]
└─$ john --format=dynamic='md5(sha256($p).$c1),$c1=lol' --wordlist=/usr/share/wordlists/rockyou.txt lm.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (dynamic=md5(sha256($p).$c1) [128/128 SSE2 4x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Hello            (?)
1g 0:00:00:00 DONE (2022-01-11 20:05) 25.00g/s 504000p/s 504000c/s 504000C/s nolan..stanly
se the "--show --format=dynamic=md5(sha256($p).$c1)" options to display all of the cracked passwords reliably
sion completed
```