BabyPass-MJ

1.信息收集

初步信息探测

```
┌──(root㉿kali)-[/tmp/test]
└─# nmap --min-rate 10000 -p- 192.168.2.58
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 06:09 EST
Nmap scan report for 192.168.2.58
Host is up (0.00056s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:0A:76:0B (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.05 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sV -sC -O -p22,80 192.168.2.58
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 06:09 EST
Nmap scan report for 192.168.2.58
Host is up (0.00029s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:0A:76:0B (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
```

```
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap --script=vuln -p22,80 192.168.2.58
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 06:10 EST
Nmap scan report for 192.168.2.58
Host is up (0.00020s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 08:00:27:0A:76:0B (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 37.39 seconds

┌──(root㉿kali)-[/tmp/test]
└─# nmap -sU --top-ports 20 192.168.2.58
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 06:10 EST
Nmap scan report for 192.168.2.58
Host is up (0.00048s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   open|filtered snmp
162/udp   closed        snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
```

```
514/udp   open|filtered syslog
520/udp   open|filtered route
631/udp   closed        ipp
1434/udp  closed        ms-sql-m
1900/udp  open|filtered upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:0A:76:0B (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.51 seconds
```

开放22，80端口，udp发现tftp可能开放，udp协议端口不好做扫描，大多扫描并不准确，且每次扫描结果大概率不相同

web信息收集

curl一下web发现隐藏信息

```
┌──(root㉿kali)-[/tmp/test]
└─# curl http://192.168.2.58/
hello world
<!-- tms -->
<!-- Do not use same password in different account.  -->
```

目录爆破，发现部分有用信息

```
┌──(root㉿kali)-[/tmp/test]
└─# dirsearch -u http://192.168.2.58/tms/
Target: http://192.168.2.58/

[06:14:40] Starting: tms/
[06:14:41] 301 -  313B  - /tms/js  ->  http://192.168.2.58/tms/js/
[06:14:48] 301 -  316B  - /tms/admin  ->  http://192.168.2.58/tms/admin/
[06:14:49] 200 -  820B  - /tms/admin/
[06:14:49] 200 -  820B  - /tms/admin/index.php
[06:15:01] 301 -  314B  - /tms/css  ->  http://192.168.2.58/tms/css/
[06:15:05] 301 -  316B  - /tms/fonts  ->  http://192.168.2.58/tms/fonts/
[06:15:07] 301 -  317B  - /tms/images  ->  http://192.168.2.58/tms/images/
[06:15:08] 200 -  820B  - /tms/images/
[06:15:08] 301 -  319B  - /tms/includes  ->  http://192.168.2.58/tms/includes/
[06:15:08] 200 -  551B  - /tms/includes/
[06:15:08] 200 -    4KB - /tms/index.php
[06:15:09] 200 -    4KB - /tms/index.php/login/
[06:15:10] 200 -  516B  - /tms/js/
```

```
[06:15:12] 302 -    1B  - /tms/logout.php  ->  index.php
[06:15:16] 200 -    3KB - /tms/page.php
[06:15:21] 302 -    0B  - /tms/profile.php  ->  index.php
[06:15:22] 200 -    2KB - /tms/README.md
[06:15:22] 200 -  336B  - /tms/Readme.txt
[06:15:30] 200 -    3KB - /tms/thankyou.php
```

敏感文件发现可能的密码

```
┌──(root㉿kali)-[/tmp/test]
└─# curl http://192.168.2.58/tms/Readme.txt
Installation Steps(Configuration)
1. Download and Unzip file on your local system.
2.Copy tms folder and tms folder inside root directory (for xampp
xampp/htdocs, for wamp wamp/www, for lamp var/www/html)

Database Configuration

Open phpmyadmin
Create Database tms
Import database tms.sql (available inside zip package)
Open Your browser put inside browser ⋄http://localhost/tms⋄

Login Details for admin :
Open Your browser put inside browser ⋄http://localhost/tms/admin⋄
Username : admin
Password : Test@123

Login Details for user:
Open Your browser put inside browser ⋄http://localhost/tms/⋄
Username : anuj@gmail.com
Password : Test@123
```

进入admin登录页面登录发现页面崩了，点几个也没发现有什么变化，感觉像是死页面，因为首页提示不要密码复用，换方向到ssh登录，感觉anuj可能是用户

2.立足点

成功登录

```
┌──(root㉿kali)-[/tmp/test]
└─# ssh anuj@192.168.2.58
anuj@192.168.2.58's password:
Linux BabyPass 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Nov 11 04:44:50 2025 from 192.168.2.55
anuj@BabyPass:~$ sudo -l
[sudo] password for anuj:
Sorry, user anuj may not run sudo on BabyPass.
anuj@BabyPass:~$
```

发现有这几个非特权用户

```
anuj:x:1001:1001:,,,:/home/anuj:/bin/bash
admin:x:1002:1002:,,,:/home/admin:/bin/bash
welcome:x:1000:1000:,,,:/home/welcome:/bin/bash
```

welcome家目录下发现user.txt

```
anuj@BabyPass:/home/welcome$ cat user.txt
flag{user-0bb3c30dc72e63881db5005f1aa19ac3}
```

3.root

经过尝试发现admin与anuj密码相同，都没有sudo权限，web架构挺大，可以考虑是否存在数据库配置文件

```
anuj@BabyPass:/var/www/html/tms$ find ./ -iname "*config*" 2>/dev/null
./includes/config.php
./admin/includes/config.php
anuj@BabyPass:/var/www/html/tms$ cat $(find ./ -iname "*config*" 2>/dev/null)
<?php
// DB credentials.
define('DB_HOST','localhost');
define('DB_USER','tms_user');
define('DB_PASS','secure_password');
define('DB_NAME','tms');
// Establish database connection.
try
{
```

```
$dbh = new PDO("mysql:host=".DB_HOST.";dbname=".DB_NAME,DB_USER,
DB_PASS,array(PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES 'utf8'"));
}
catch (PDOException $e)
{
exit("Error: " . $e->getMessage());
}
?>
<?php
// DB credentials.
define('DB_HOST','localhost');
define('DB_USER','tms_user');
define('DB_PASS','secure_password');
define('DB_NAME','tms');
// Establish database connection.
try
{
$dbh = new PDO("mysql:host=".DB_HOST.";dbname=".DB_NAME,DB_USER,
DB_PASS,array(PDO::MYSQL_ATTR_INIT_COMMAND => "SET NAMES 'utf8'"));
}
catch (PDOException $e)
{
exit("Error: " . $e->getMessage());
}
?>
```

找到数据库凭据tms_user:secure_password
登录查到root加密hash

```
anuj@BabyPass:/var/www/html/tms$ mysql -utms_user -psecure_password
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tms                |
+--------------------+
2 rows in set (0.000 sec)

MariaDB [(none)]> use tms;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [tms]> show tables;
```

```
+-----------------+
| Tables_in_tms   |
+-----------------+
| admin           |
| tblbooking      |
| tblenquiry      |
| tblissues       |
| tblpages        |
| tbltourpackages |
| tblusers        |
+-----------------+
7 rows in set (0.000 sec)
MariaDB [tms]> select * from tblusers \G ;
*************************** 1. row ***************************
          id: 1
    FullName: Manju Srivatav
MobileNumber: 4456464654
     EmailId: manju@gmail.com
    Password: 202cb962ac59075b964b07152d234b70
     RegDate: 2020-07-08 02:33:20
UpdationDate: NULL
*************************** 2. row ***************************
          id: 2
    FullName: Kishan
MobileNumber: 9871987979
     EmailId: kishan@gmail.com
    Password: 202cb962ac59075b964b07152d234b70
     RegDate: 2020-07-08 02:33:56
UpdationDate: NULL
*************************** 3. row ***************************
          id: 3
    FullName: Salvi Chandra
MobileNumber: 1398756416
     EmailId: salvi@gmail.com
    Password: 202cb962ac59075b964b07152d234b70
     RegDate: 2020-07-08 02:34:20
UpdationDate: NULL
*************************** 4. row ***************************
          id: 4
    FullName: Abir
MobileNumber: 4789756456
     EmailId: abir@gmail.com
    Password: 202cb962ac59075b964b07152d234b70
     RegDate: 2020-07-08 02:34:38
UpdationDate: NULL
*************************** 5. row ***************************
```

```
          id: 5
    FullName: Test
MobileNumber: 1987894654
     EmailId: anuj@gmail.com
    Password: f925916e2754e5e03f75dd58a5733251
     RegDate: 2020-07-08 02:35:06
UpdationDate: 2021-05-11 00:37:41
*************************** 6. row ***************************
          id: 6
    FullName: root
MobileNumber: 123456789
     EmailId: root@gmail.com
    Password: fd50619cd7026f0f32272f77f4da6e92
     RegDate: 2020-07-08 02:35:06
UpdationDate: 2021-05-11 00:37:41
6 rows in set (0.000 sec)
```

破解hash得到

```
fd50619cd7026f0f32272f77f4da6e92:Root@456
```

提权得到root

```
anuj@BabyPass:/var/www/html/tms$ su
Password:
root@BabyPass:/var/www/html/tms# cat /root/root.txt
flag{root-bb289959b86dd81869df2eb9a7f3602a}
```