Nmap主机发现实战 实验步骤

Nmap主机发现

1、-sP

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:27 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0013s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

对192.168.203.1进行Ping扫描

结果：发现主机存活。（`host is up`）

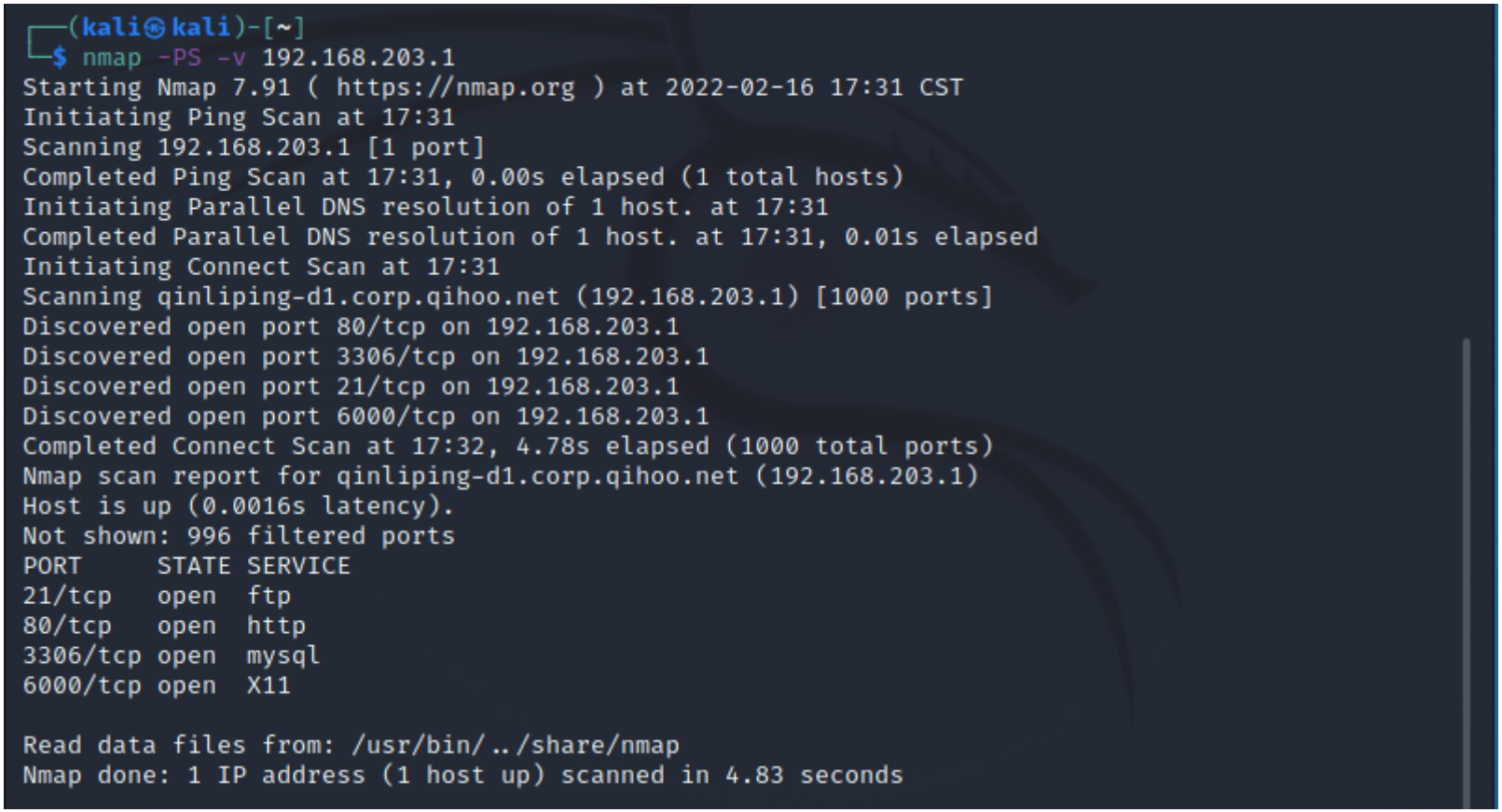
2、-P0

```
┌──(kali㉿kali)-[~]
└─$ nmap -P0 192.168.203.1
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:30 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
6000/tcp open  X11

Nmap done: 1 IP address (1 host up) scanned in 4.63 seconds
```

对192.168.203.1进行无Ping扫描

结果：发现主机存活，并开放了21、80、3306、6000端口及其开放的服务。

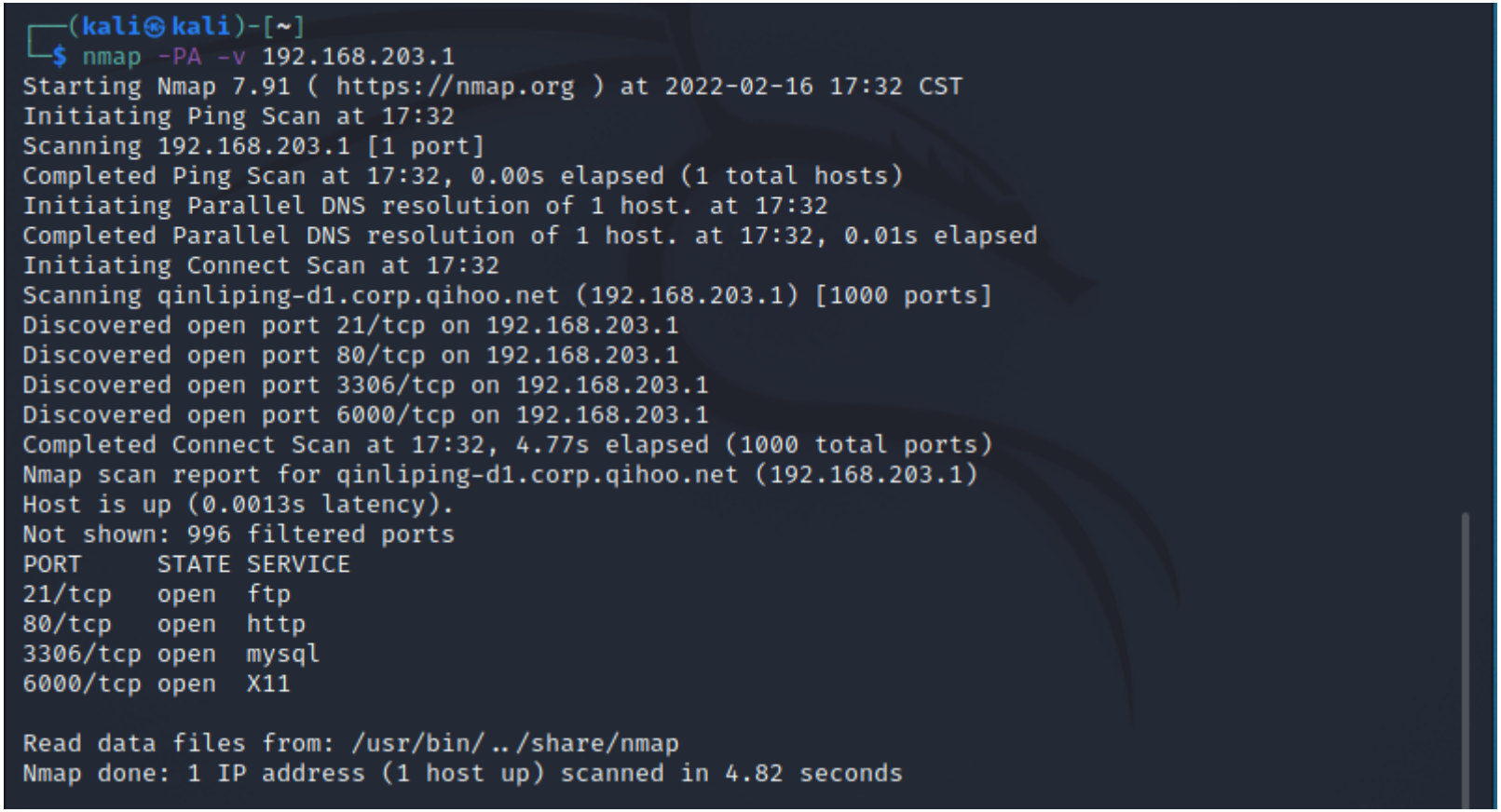
3、-PS



对192.168.203.1进行TCP SYN Ping扫描

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

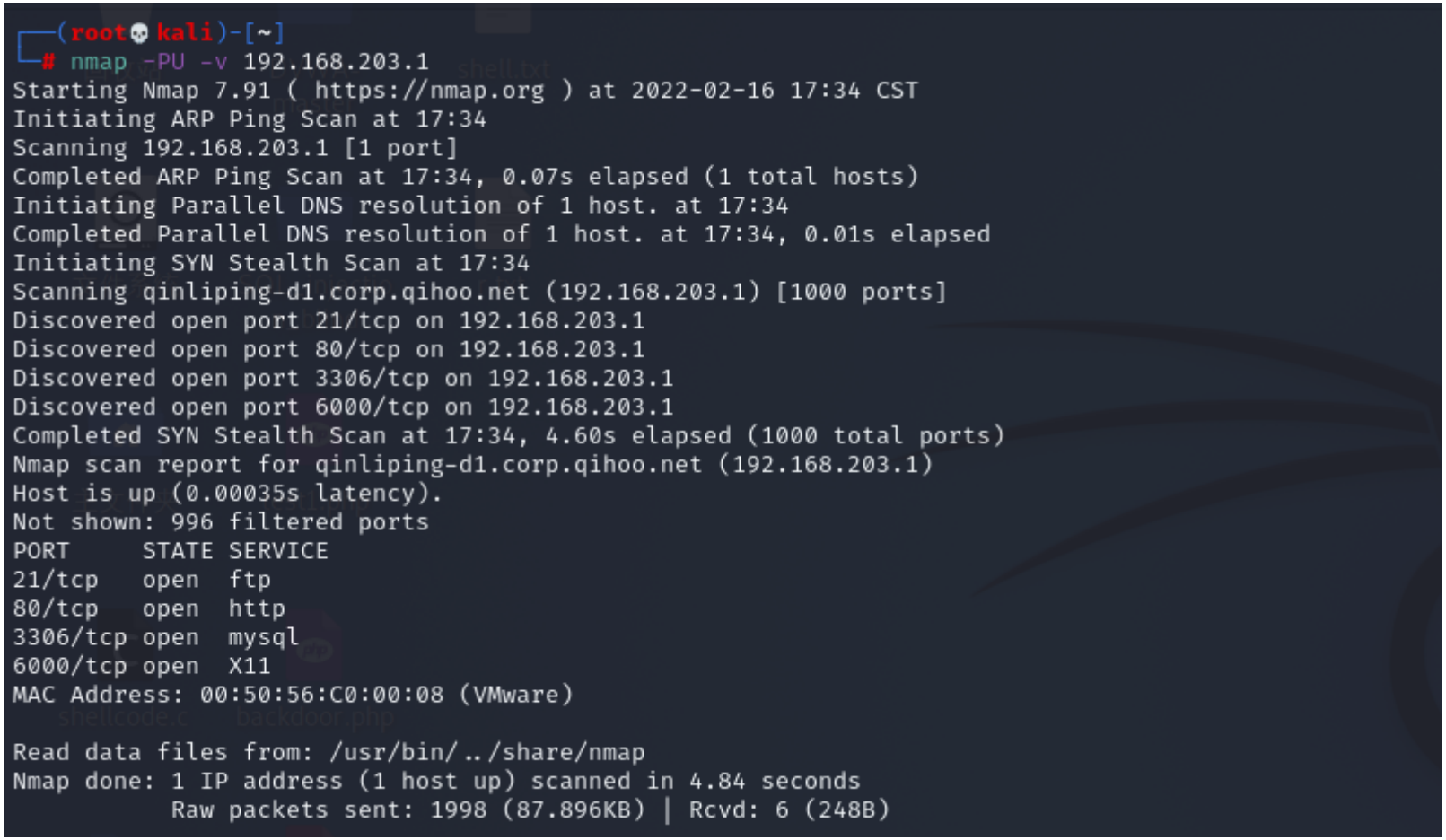
4、-PA



对192.168.203.1进行TCP ACK Ping扫描

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

5、-PU(该命令需要root权限)



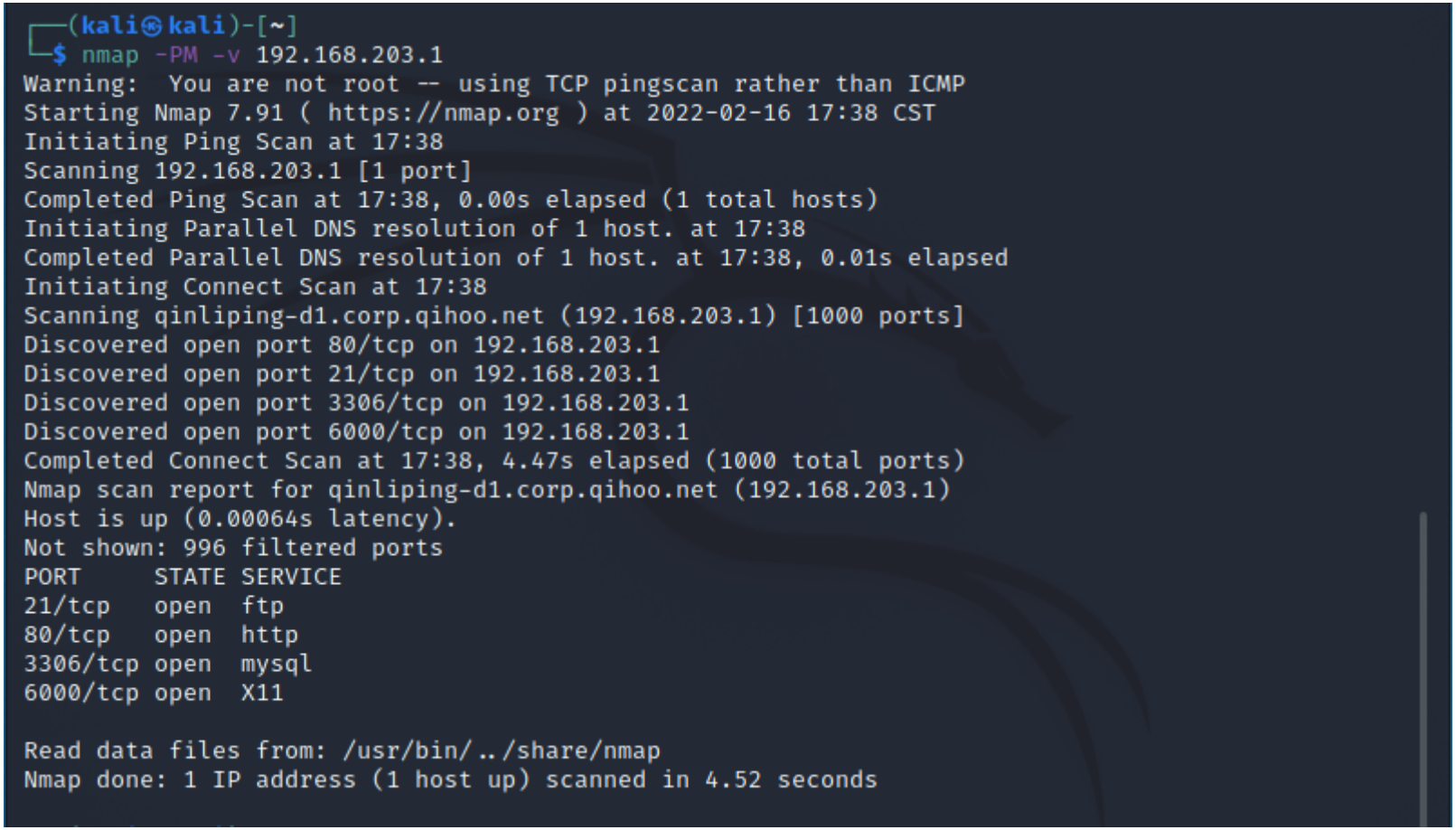
对192.168.203.1进行UDP Ping扫描

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

6、-PE;-PP;-PM

```
┌──(kali㉿kali)-[~]
└─$ nmap -PE -v 192.168.203.1
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:36 CST
Initiating Ping Scan at 17:36
Scanning 192.168.203.1 [1 port]
Completed Ping Scan at 17:36, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:36
Completed Parallel DNS resolution of 1 host. at 17:36, 0.01s elapsed
Initiating Connect Scan at 17:36
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [1000 ports]
Discovered open port 21/tcp on 192.168.203.1
Discovered open port 80/tcp on 192.168.203.1
Discovered open port 3306/tcp on 192.168.203.1
Discovered open port 6000/tcp on 192.168.203.1
Completed Connect Scan at 17:36, 4.59s elapsed (1000 total ports)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00090s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
6000/tcp open  X11

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.64 seconds
```

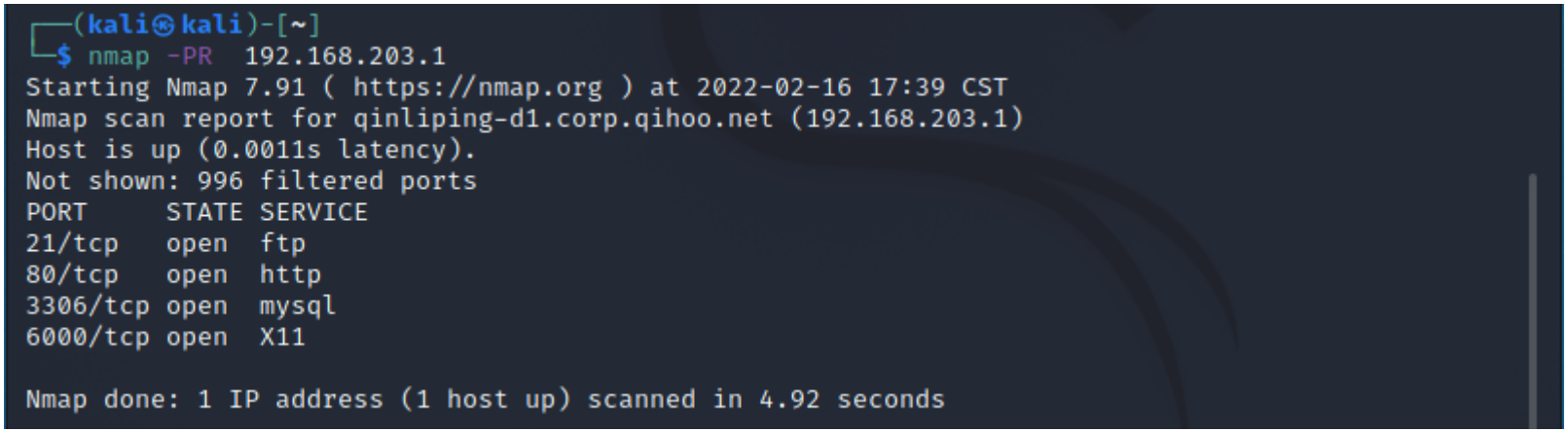
```
┌──(kali㉿kali)-[~]
└─$ nmap -PP -v 192.168.203.1
Warning:  You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:37 CST
Initiating Ping Scan at 17:37
Scanning 192.168.203.1 [1 port]
Completed Ping Scan at 17:37, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:37
Completed Parallel DNS resolution of 1 host. at 17:37, 0.01s elapsed
Initiating Connect Scan at 17:37
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [1000 ports]
Discovered open port 21/tcp on 192.168.203.1
Discovered open port 3306/tcp on 192.168.203.1
Discovered open port 80/tcp on 192.168.203.1
Discovered open port 6000/tcp on 192.168.203.1
Completed Connect Scan at 17:37, 3.97s elapsed (1000 total ports)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00083s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
6000/tcp open  X11

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.02 seconds
```



均对192.168.203.1进行ICMP Ping扫描，分别为ICMP Echo、ICMP时间戳Ping、ICMP地址掩码Ping

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

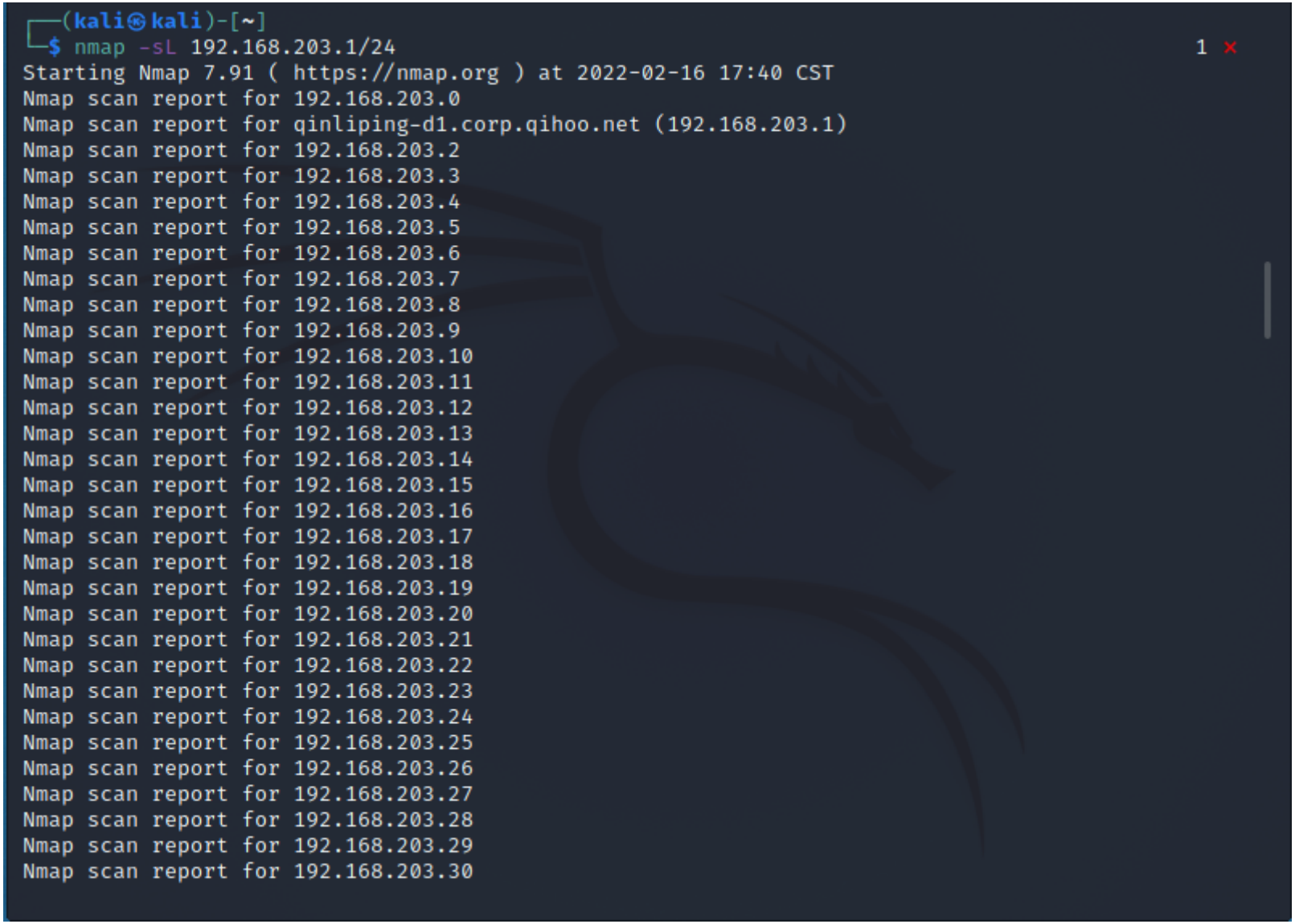
7、-PR



对192.168.203.1进行ARP Ping扫描

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

8、-sL



对192.168.203.*共256个IP地址进行列表扫描

结果:获取到192.168.203.1主机名。

9、--system-dns

```
┌──(kali㉿kali)-[~]
└─$ nmap --system-dns 192.168.203.2 192.168.203.1                    148 ✕ 1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:47 CST
Nmap scan report for 192.168.203.2
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain

Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0022s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
6000/tcp open  X11

Nmap done: 2 IP addresses (2 hosts up) scanned in 4.23 seconds
```

使用系统域名解析器

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。

10、-6

```
┌──(kali㉿kali)-[~]
└─$ nmap -6 fe80::d0c7:d778:c9dd:b29c%4                                1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:51 CST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds
```

扫描一个IPv6地址

结果:回显提示主机未存活，或者Ping请求被防火墙拦截。

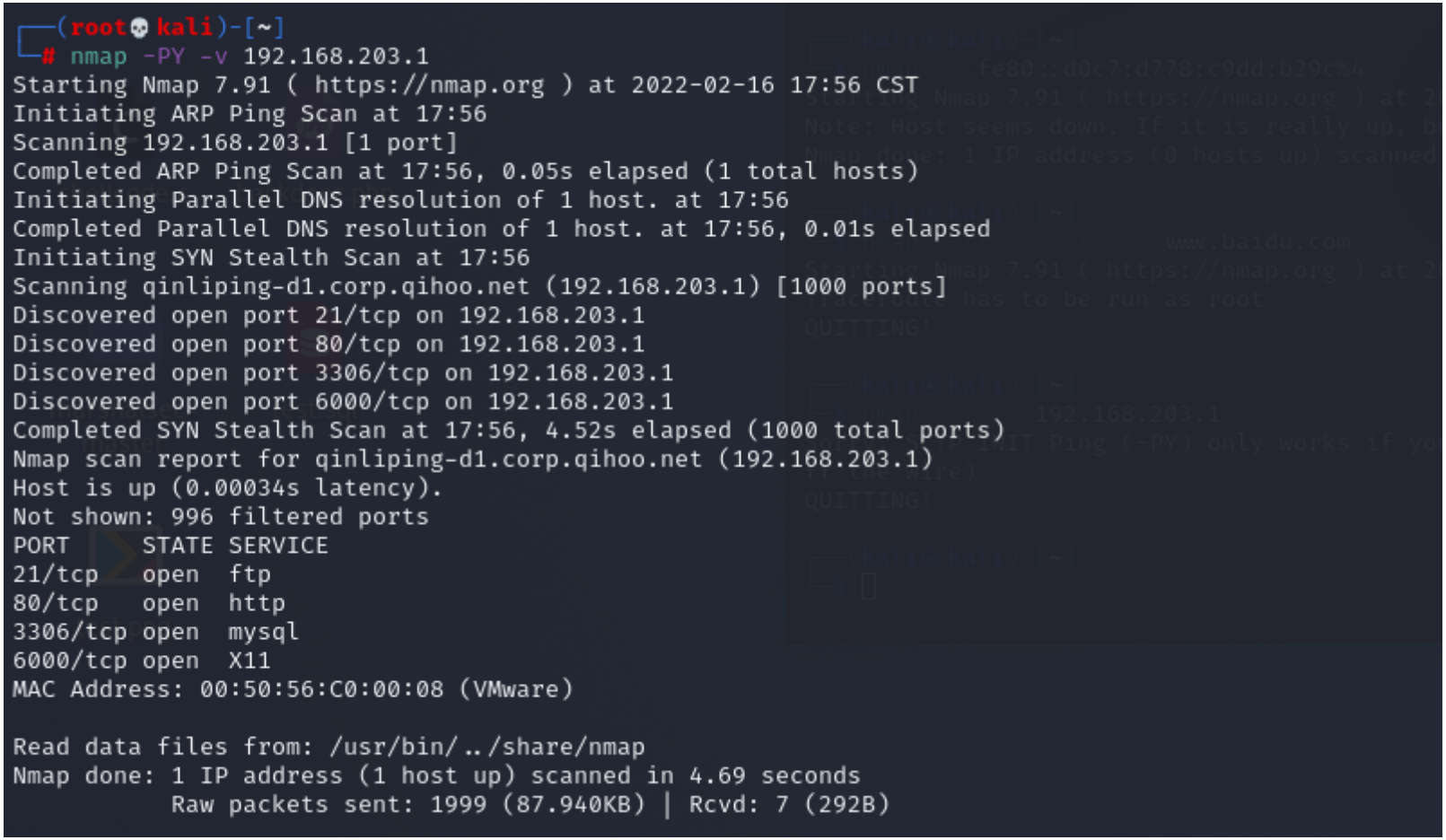
11、-traceroute

```
┌──(root💀kali)-[~]
└─# nmap --traceroute -v www.baidu.com
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-16 17:53 CST
Initiating Ping Scan at 17:53
Scanning www.baidu.com (220.181.38.149) [4 ports]
Completed Ping Scan at 17:53, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:53
Completed Parallel DNS resolution of 1 host. at 17:53, 0.02s elapsed
Initiating SYN Stealth Scan at 17:53
Scanning www.baidu.com (220.181.38.149) [1000 ports]
Discovered open port 443/tcp on 220.181.38.149
Discovered open port 80/tcp on 220.181.38.149
Increasing send delay for 220.181.38.149 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 220.181.38.149 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 17:54, 48.60s elapsed (1000 total ports)
Initiating Traceroute at 17:54
Completed Traceroute at 17:54, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 17:54
Completed Parallel DNS resolution of 2 hosts. at 17:54, 0.02s elapsed
Nmap scan report for www.baidu.com (220.181.38.149)
Host is up (0.019s latency).
Other addresses for www.baidu.com (not scanned): 220.181.38.150
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.04 ms 192.168.203.2
2   0.05 ms 220.181.38.149

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 48.92 seconds
           Raw packets sent: 2047 (89.864KB) | Rcvd: 816 (32.676KB)
```

解析访问网址www.baidu.com的路由状况

结果：经过局域网路由192.168.203.2，到达百度服务器220.181.38.149

12、-PY



对192.168.203.1进行SCTP INIT Ping扫描

结果：发现主机存活，共扫描了1000个端口，未显示996个状态为filtered的端口，开放了21、80、3306、6000端口，并显示了其开放的服务。