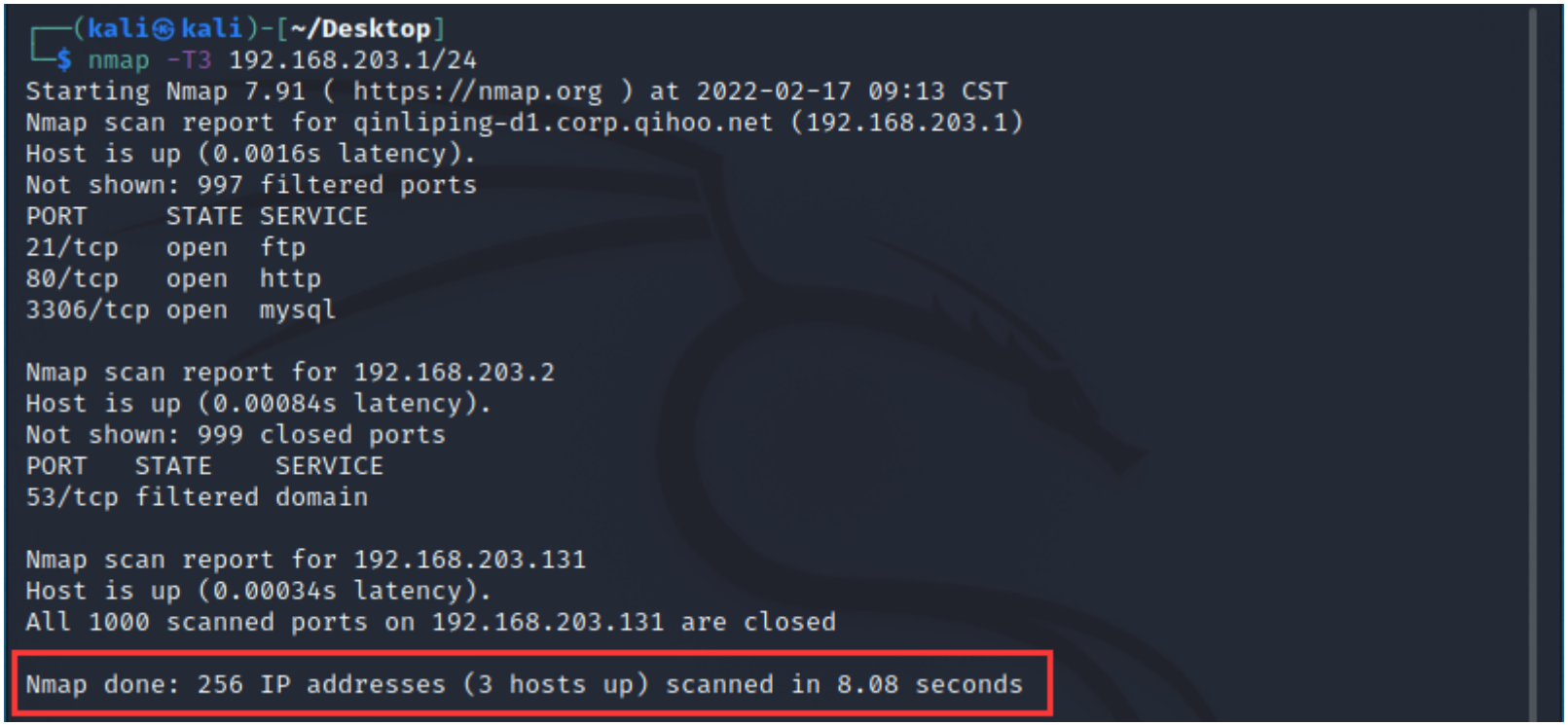
探索网络实战 实验步骤

探索网络命令实践

1、-T



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -T5 192.168.203.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:15 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0010s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql

Nmap scan report for 192.168.203.2
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT   STATE    SERVICE
53/tcp filtered domain

Nmap scan report for 192.168.203.131
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.203.131 are closed

Nmap done: 256 IP addresses (3 hosts up) scanned in 4.51 seconds
```

时序选项

结果:可以很明显地看到T3耗时8.08s，T5耗时4.51s。

2、-p

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -p 3306 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:18 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00041s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

结果:扫描到192.168.203.1主机的3306端口开放，且运行服务为MySQL

指定端口进行扫描，可加参数，设定扫描TCP或者UDP端口如：

```
┌──(root💀kali)-[~]
└─# nmap -sS -p T:80,U:445 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:19 CST
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00027s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

指定扫描TCP的80端口和UDP的445端口

结果80端口开放，运行服务为http

3、-sS

```
┌──(root💀kali)-[~]
└─# nmap -sS 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:22 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00043s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

对192.168.203.1进行TCP SYN扫描

结果：显示主机存活，开放端口为21、80、3306，运行服务分别为ftp、http、mysql，并且获得其MAC地址。

4、-sT

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sT 192.168.203.1                                                    1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:23 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0010s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
```

对192.168.203.1进行TCP连接扫描

结果：显示主机存活，开放端口为21、80、3306，运行服务分别为ftp、http、mysql。

5、-sU UDP扫描

```
┌──(root💀kali)-[~]
└─# nmap -sU -p 80-500 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:24 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00016s latency).
All 421 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 10.02 seconds
```

对192.168.203.1进行UDP扫描

结果：所有UDP端口均为open|filtered状态，但获得了MAC地址。

6、-sN;-sF;-sX

```
┌──(root💀kali)-[~]
└─# nmap -sN 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:25 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00037s latency).
All 1000 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.72 seconds
```

```
┌──(root💀kali)-[~]
└─# nmap -sF 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:26 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00023s latency).
All 1000 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.80 seconds
```

```
┌──(root💀kali)-[~]
└─# nmap -sX 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:27 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00026s latency).
All 1000 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
```

隐蔽扫描——-sN为Null扫描，-sF为FIN扫描，-sX为Xmas扫描

结果：在面对windows个人PC防火墙时，隐蔽扫描效果都不是很好，很明显都被防火墙拦截了。

7、-sA

```
┌──(root💀kali)-[~]
└─# nmap -sA -v 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:29 CST
Initiating ARP Ping Scan at 09:29
Scanning 192.168.203.1 [1 port]
Completed ARP Ping Scan at 09:29, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:29
Completed Parallel DNS resolution of 1 host. at 09:29, 0.01s elapsed
Initiating ACK Scan at 09:29
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [1000 ports]
Completed ACK Scan at 09:30, 21.55s elapsed (1000 total ports)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00016s latency).
All 1000 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.70 seconds
           Raw packets sent: 2001 (80.028KB) | Rcvd: 1 (28B)
```

对192.168.203.1进行TCP ACK扫描

结果：被防火墙拦截。

8、-sW

```
┌──(root💀kali)-[~]
└─# nmap -sW -v -F 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:31 CST
Initiating ARP Ping Scan at 09:31
Scanning 192.168.203.1 [1 port]
Completed ARP Ping Scan at 09:31, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:31
Completed Parallel DNS resolution of 1 host. at 09:31, 0.01s elapsed
Initiating Window Scan at 09:31
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [100 ports]
Completed Window Scan at 09:31, 3.08s elapsed (100 total ports)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00013s latency).
All 100 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.24 seconds
           Raw packets sent: 201 (8.028KB) | Rcvd: 1 (28B)
```

对192.168.203.1进行TCP窗口扫描。

结果：首先是这种扫描方式的结果可信度很低，其次并未绕过防火墙。

9、-sM

```
┌──(root💀kali)-[~]
└─# nmap -sM -T4 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:34 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00022s latency).
All 1000 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.68 seconds
```

对192.168.203.1进行TCP Maimon扫描

结果：被防火墙拦截。

10、--scanflags

```
┌──(root💀kali)-[~]
└─# nmap -sT --scanflags SYNURG 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:43 CST
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00089s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
```

对192.168.203.1进行自定义TCP扫描，该命令中TCP报文标志位SYNURG均为1

结果：显示主机存活，开放端口为21、80、3306，运行服务分别为ftp、http、mysql。

11、-sO

```
┌──(root💀kali)-[~]
└─# nmap -sO -T4 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 09:44 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00023s latency).
All 256 scanned ports on qinliping-d1.corp.qihoo.net (192.168.203.1) are open|filtered
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.50 seconds
```

对192.168.203.1进行IP协议扫描

结果:主机IP协议端口均处于open|filtered状态，大概率被防火墙拦截。