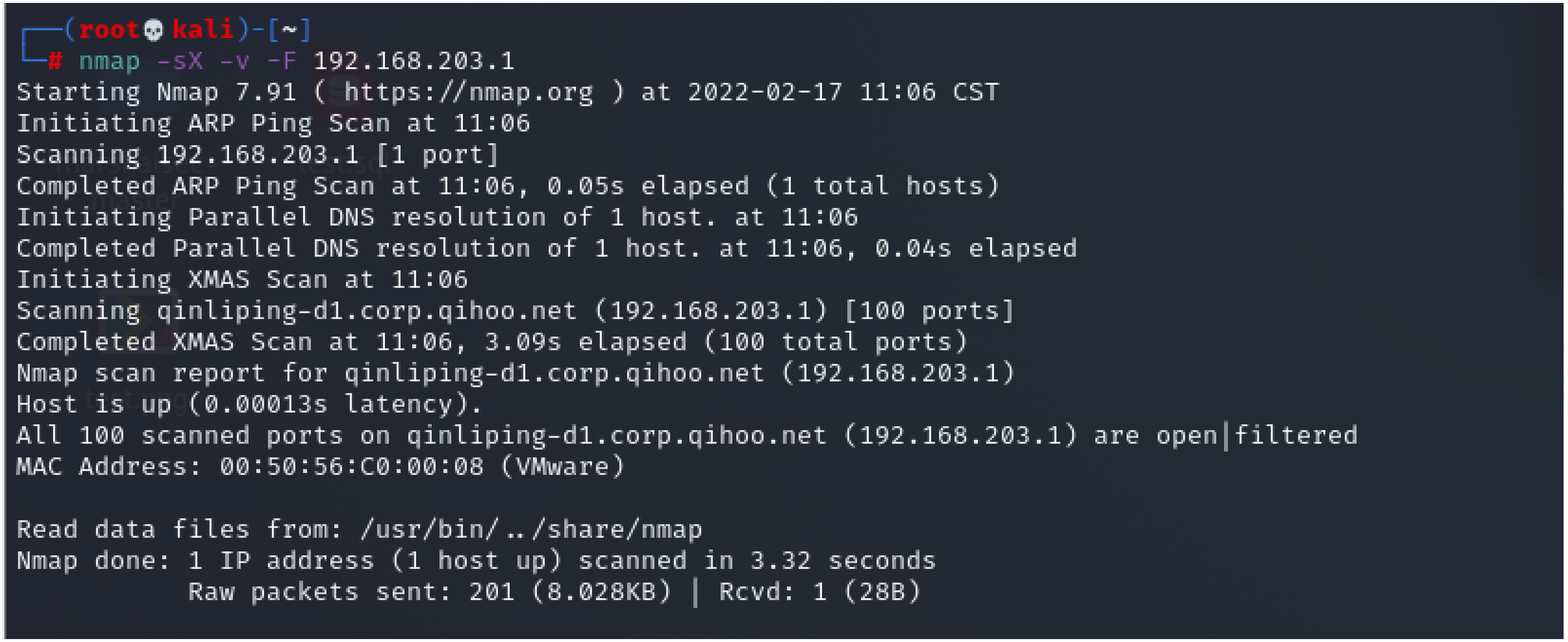
防火墙/IDS逃逸实战 实验步骤

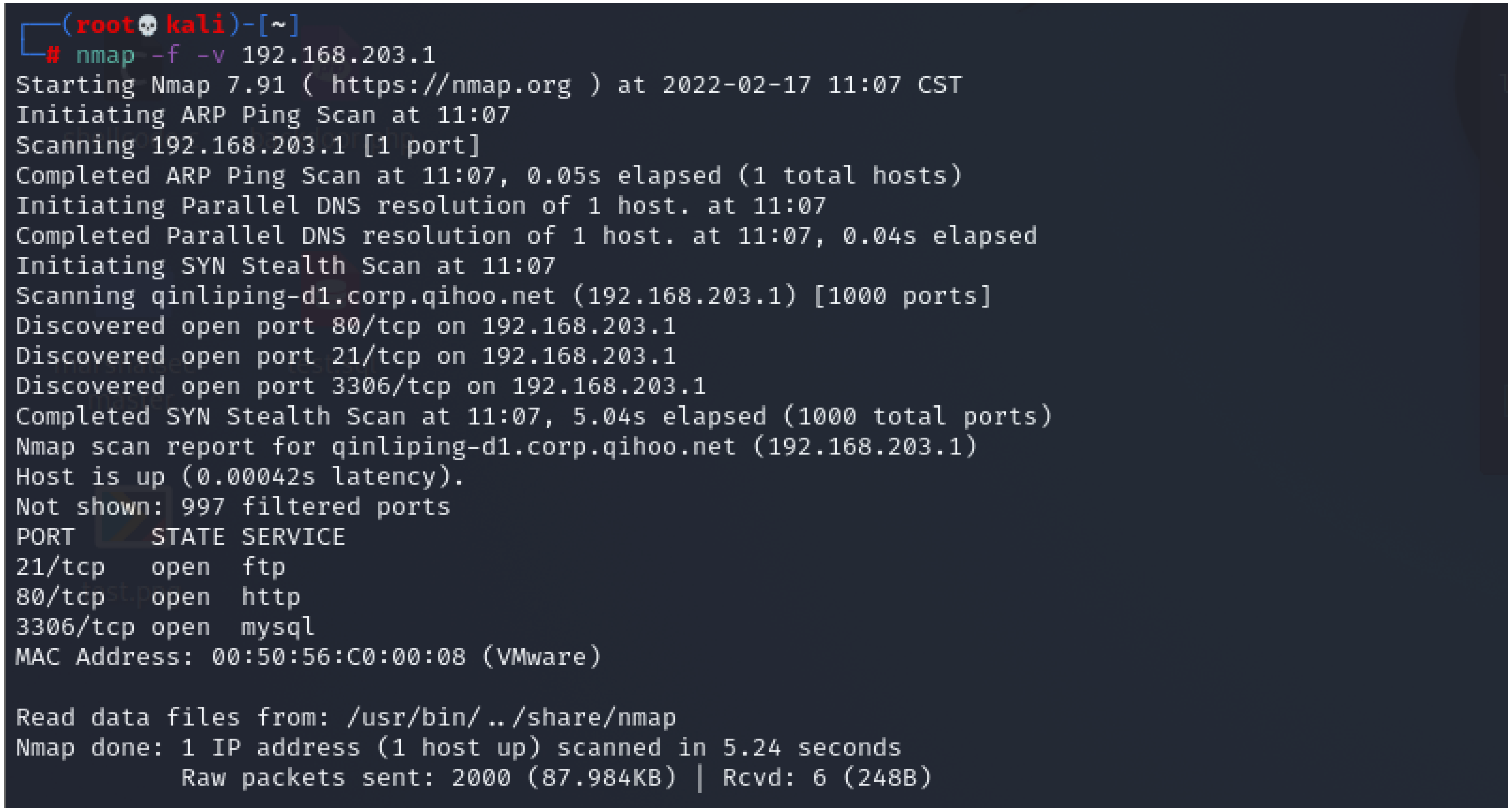
防火墙/IDS逃逸基础命令实践

1、-f



```
┌──(root💀kali)-[~]
└─# nmap -sX -v -F 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:06 CST
Initiating ARP Ping Scan at 11:06
Scanning 192.168.203.1 [1 port]
Completed ARP Ping Scan at 11:06, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:06
Completed Parallel DNS resolution of 1 host. at 11:06, 0.04s elapsed
Initiating XMAS Scan at 11:06
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [100 ports]
Completed XMAS Scan at 11:06, 3.09s 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 open|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 3.32 seconds
           Raw packets sent: 201 (8.028KB) | Rcvd: 1 (28B)
```



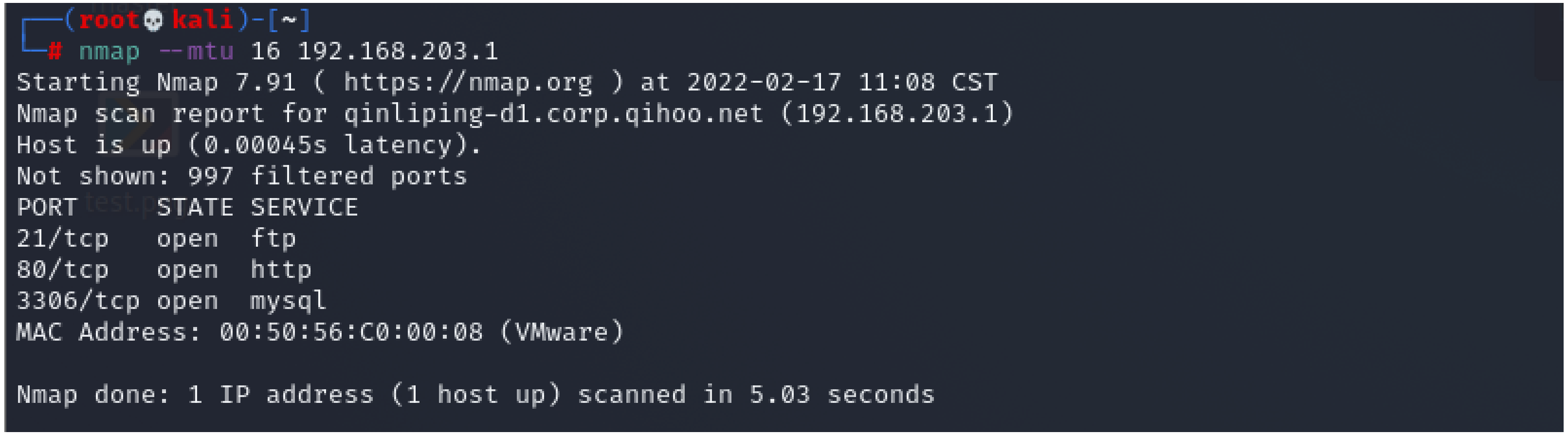
```
┌──(root💀kali)-[~]
└─# nmap -f -v 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:07 CST
Initiating ARP Ping Scan at 11:07
Scanning 192.168.203.1 [1 port]
Completed ARP Ping Scan at 11:07, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.04s elapsed
Initiating SYN Stealth Scan at 11:07
Scanning qinliping-d1.corp.qihoo.net (192.168.203.1) [1000 ports]
Discovered open port 80/tcp on 192.168.203.1
Discovered open port 21/tcp on 192.168.203.1
Discovered open port 3306/tcp on 192.168.203.1
Completed SYN Stealth Scan at 11:07, 5.04s elapsed (1000 total ports)
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00042s 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)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.24 seconds
           Raw packets sent: 2000 (87.984KB) | Rcvd: 6 (248B)
```

利用报文分段，绕过windows防火墙

结果：第一次的命令中很明显被拦截了，第二次使用参数-f之后获取到了主机端口开放情况。

2、--mtu



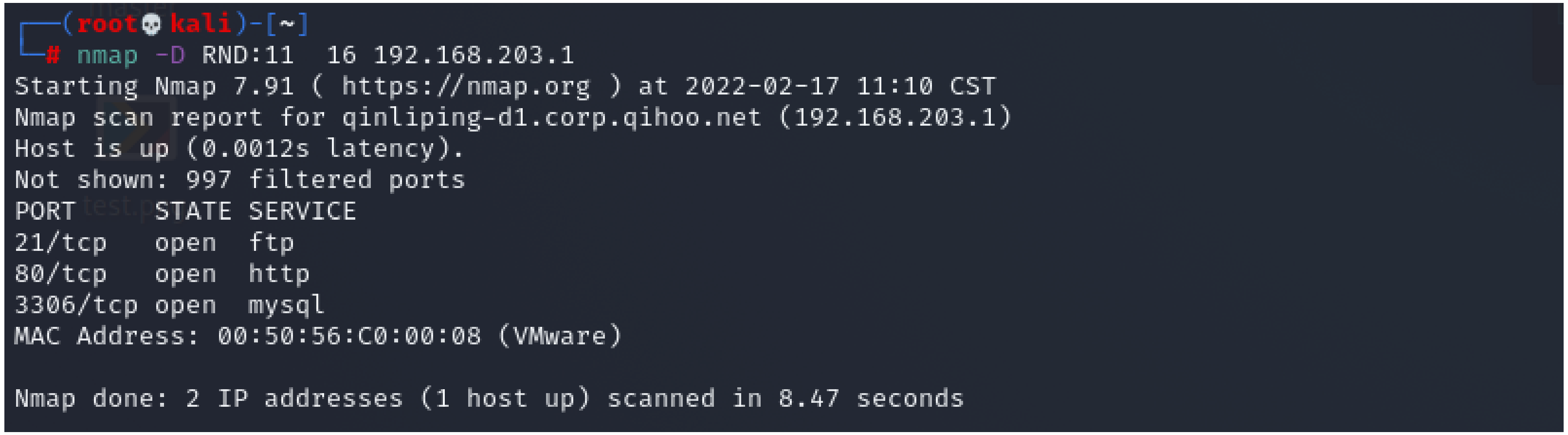
```
┌──(root💀kali)-[~]
└─# nmap --mtu 16 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:08 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00045s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds
```

对192.168.203.1进行扫描，并指定偏移大小为16(偏移量必须为8的倍数)

结果：获取到主机端口开放以及运行服务的信息。

3、-D



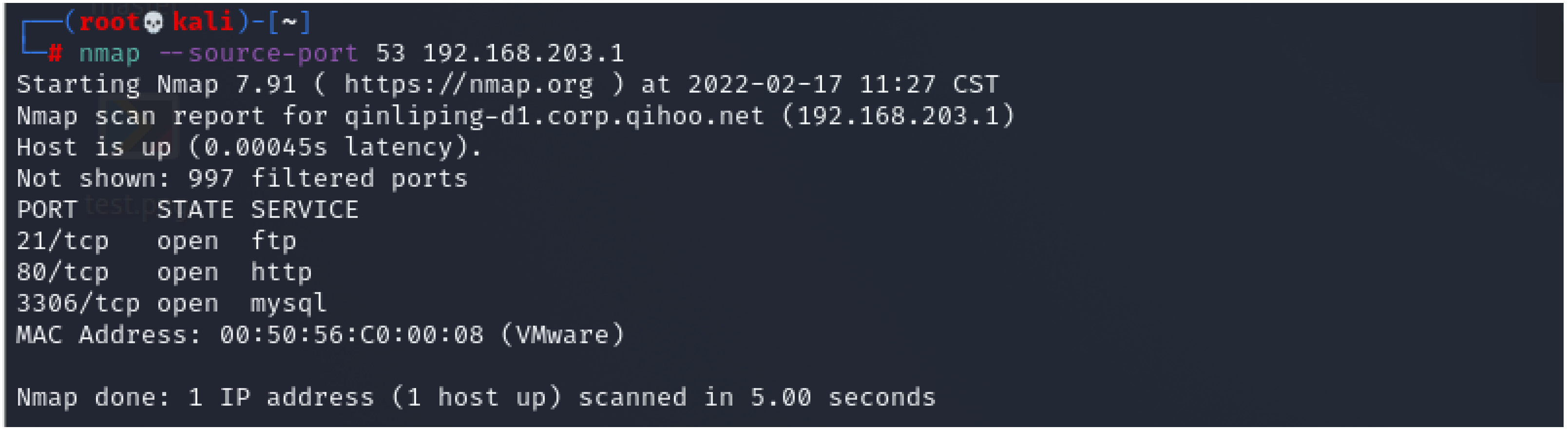
```
┌──(root💀kali)-[~]
└─# nmap -D RND:11  16 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:10 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap done: 2 IP addresses (1 host up) scanned in 8.47 seconds
```

使用IP地址欺骗，对192.168.203.1进行扫描

结果：获取到主机端口开放以及运行服务的信息。

4、--sourec-port



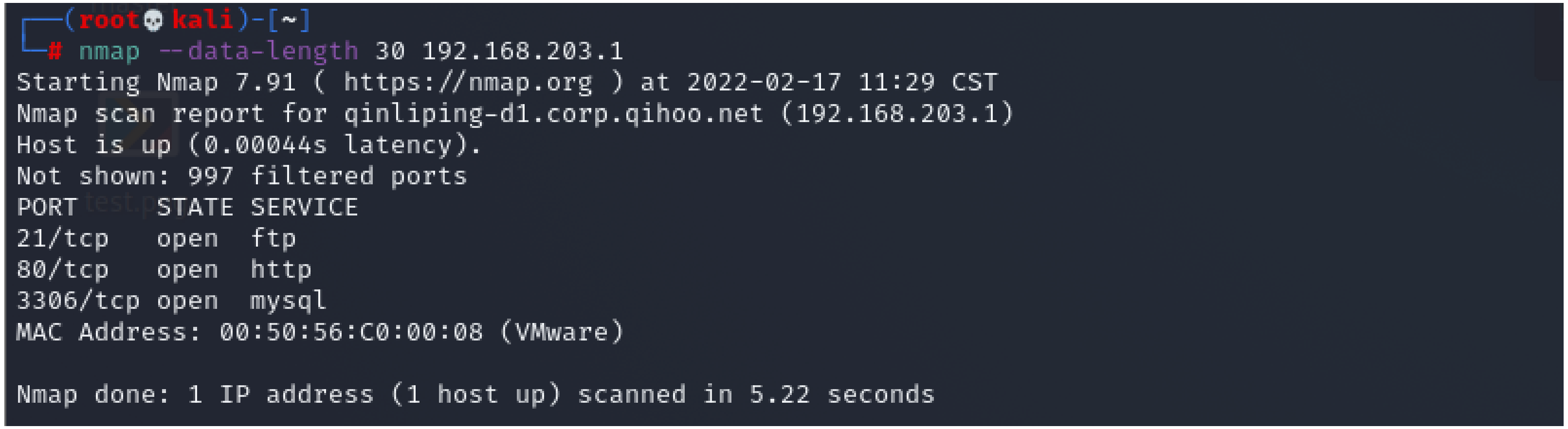
```
┌──(root💀kali)-[~]
└─# nmap --source-port 53 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:27 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00045s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   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 5.00 seconds
```

指定53端口为发送端口对192.168.203.1进行主机扫描

结果：获取到主机端口开放以及运行服务的信息。

5、--data-length



```
┌──(root💀kali)-[~]
└─# nmap --data-length 30 192.168.203.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-17 11:29 CST
Nmap scan report for qinliping-d1.corp.qihoo.net (192.168.203.1)
Host is up (0.00044s 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
```

指定发包长度，对192.168.203.1进行主机扫描

结果：获取到主机端口开放以及运行服务的信息。