一、TCP知识

1、TCP字段

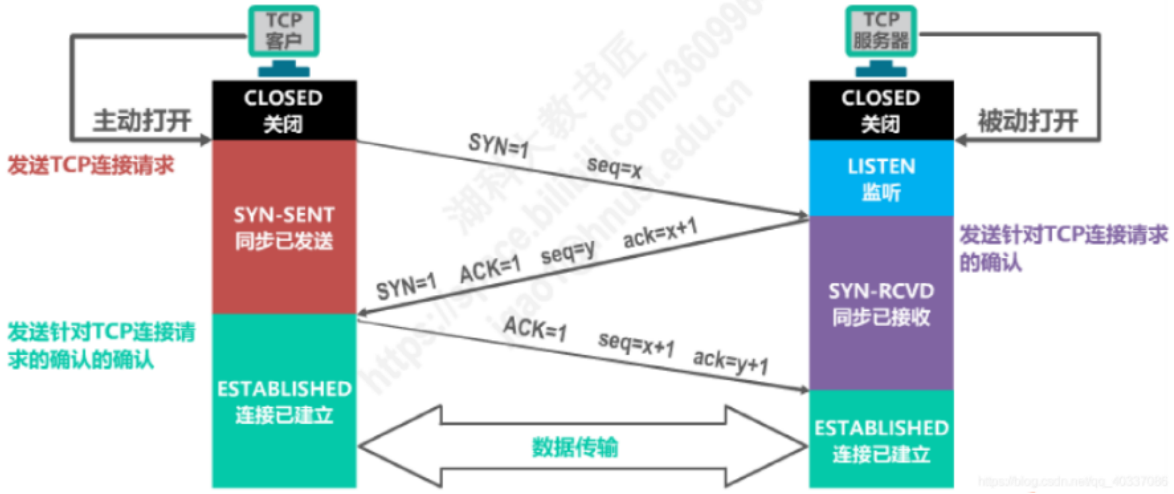
```
    Source Port：源端口
    Destination Port：目的端口
    Sequence Number：序列号
    Acknowledgment Number：确认号
```

```
    URG：紧急指针是否有效
    ACK：确认号是否有效
    PSH：强制将数据压入缓冲区
    RST：连接重置
    SYN：表示建立连接
    FIN：表示关闭连接
```

2、TCP握手

```
    一次握手：客户端发送带有 SYN 标志的连接请求数据包给服务端
    二次握手：服务端发送带有 SYN + ACK 标志的连接请求和应答数据包给客户端
    三次握手：客户端发送带有 ACK 标志的应答数据包给服务端
```

■ TCP使用“三报文握手”建立连接

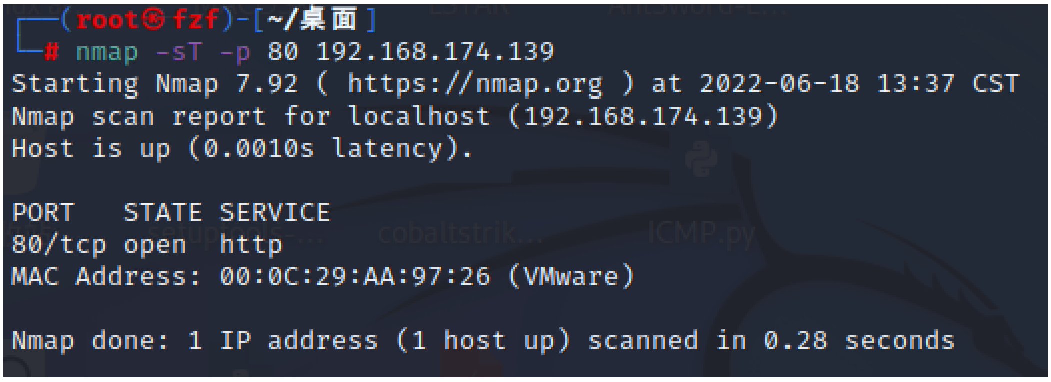


二、Nmap扫描

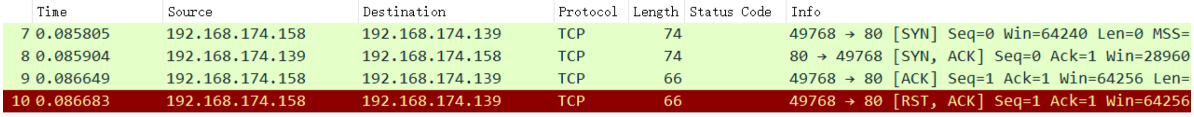
1、TCP扫描

```
# 扫描语法
    nmap -sT -p [端口] [IP]
    TCP扫描将扫描TCP端口，并通过源端口和目标端口之间的三次握手连接确保端口开放
```

```
# 端口开放
	1、源发出带有SYN数据包的请求
	2、目标响应SYN、ACK数据包
	3、源发送ACK数据包
	4、源再次发送RST、ACK数据包
```

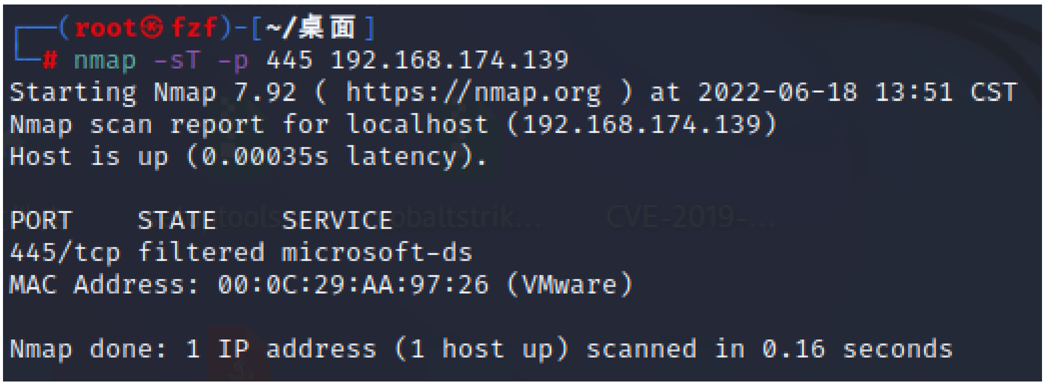


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sT -p 80 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 13:37 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.0010s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

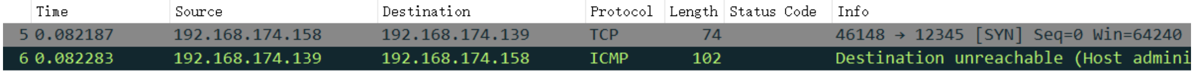


	Time	Source	Destination	Protocol	Length	Status Code	Info
7	0.085805	192.168.174.158	192.168.174.139	TCP	74		49768 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=
8	0.085904	192.168.174.139	192.168.174.158	TCP	74		80 → 49768 [SYN, ACK] Seq=0 Ack=1 Win=28960
9	0.086649	192.168.174.158	192.168.174.139	TCP	66		49768 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=
10	0.086683	192.168.174.158	192.168.174.139	TCP	66		49768 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256

```
# 端口不开放
	1、源发出带有SYN数据包的请求
	2、目标响应ICMP数据包Destnation unreachable（无法到达目的地）
```



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sT -p 445 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 13:51 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00035s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

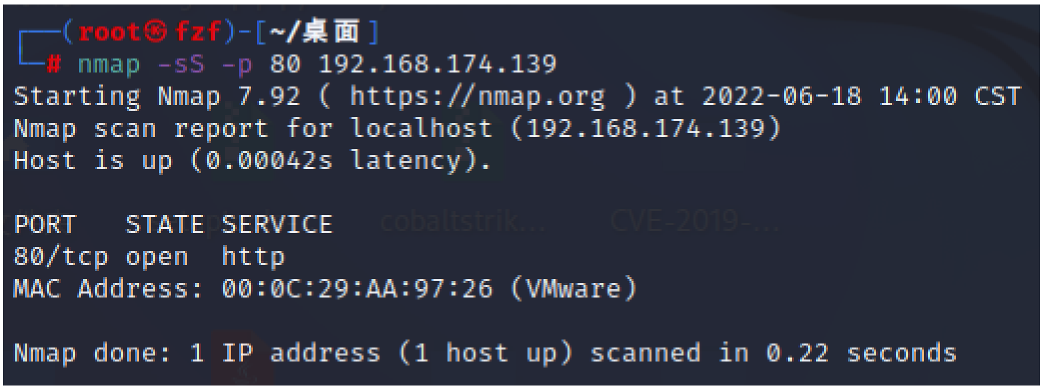


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.082187	192.168.174.158	192.168.174.139	TCP	74		46148 → 12345 [SYN] Seq=0 Win=64240
6	0.082283	192.168.174.139	192.168.174.158	ICMP	102		Destination unreachable (Host admini

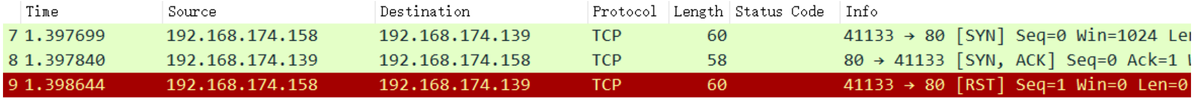
2、Stealth扫描

```
# 扫描语法
	nmap -sS -p [端口] [IP]
	SYN扫描是默认的也是最受欢迎的扫描选项。它可以快速执行，在不受防火墙限制的情况下，以每秒数千个的速度扫描网站端口
```

# 端口开放
　　1、源将SYN数据包发送到目标
　　2、目标向源发送SYN、ACK数据包
　　3、源将RST数据包发送到目标

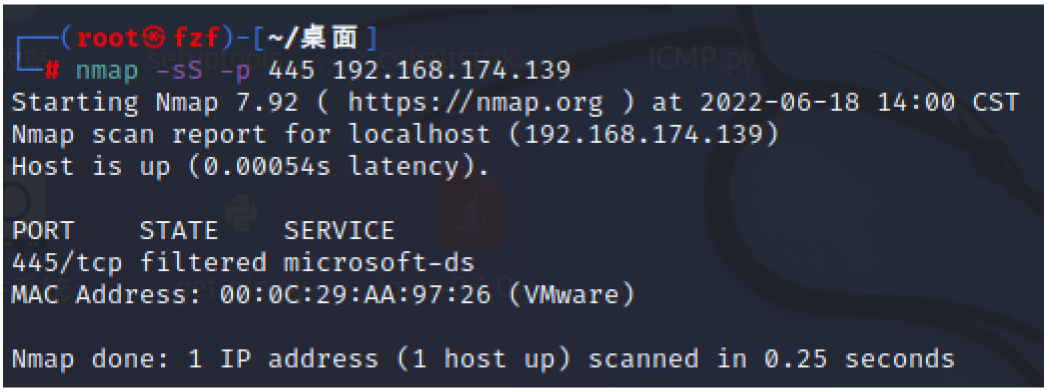


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sS -p 80 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:00 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00042s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

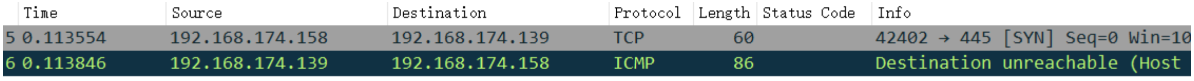


	Time	Source	Destination	Protocol	Length	Status Code	Info
7	1.397699	192.168.174.158	192.168.174.139	TCP	60		41133 → 80 [SYN] Seq=0 Win=1024 Le
8	1.397840	192.168.174.139	192.168.174.158	TCP	58		80 → 41133 [SYN, ACK] Seq=0 Ack=1
9	1.398644	192.168.174.158	192.168.174.139	TCP	60		41133 → 80 [RST] Seq=1 Win=0 Len=0

# 端口不开放
　　1、源将SYN数据包发送到目标
　　2、目标响应ICMP数据包Destnation unreachable（无法到达目的地）



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sS -p 445 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:00 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00054s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

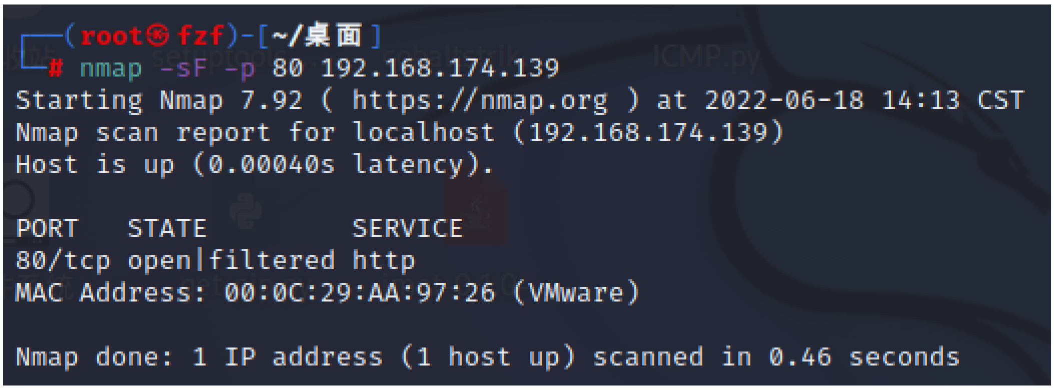


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.113554	192.168.174.158	192.168.174.139	TCP	60		42402 → 445 [SYN] Seq=0 Win=10
6	0.113846	192.168.174.139	192.168.174.158	ICMP	86		Destination unreachable (Host

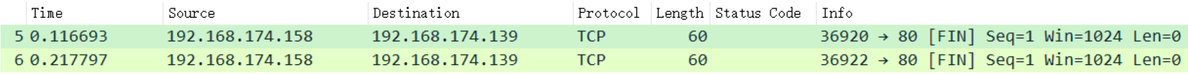
3、Fin扫描

# 扫描语法（误报严重）
　　nmap -sF -p [端口] [IP]
　　通常在数据传输完成后，使用FIN数据包终止源端口和目标端口之间的TCP连接。Nmap通过发送FIN数据包进行扫描，如果端口是开放的，则发送FIN数据包时，目标端口没有响应

```
# 端口开放
        1、源将FIN数据包发送到目标
        2、目标未回复
```

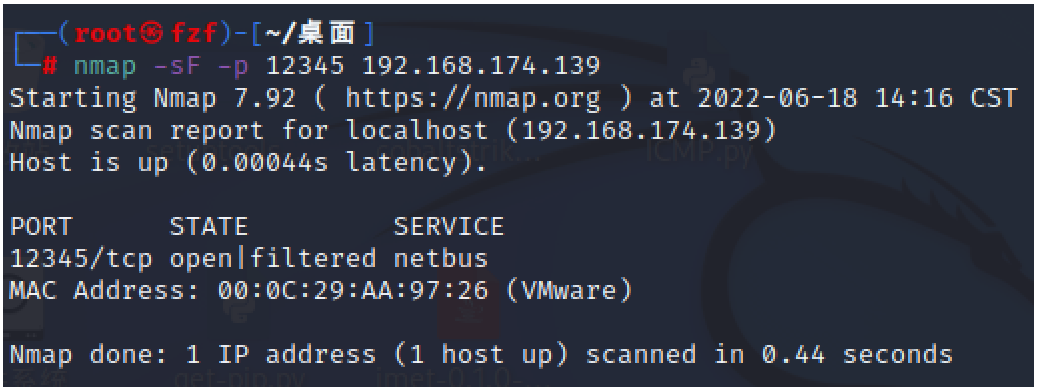


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sF -p 80 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:13 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00040s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

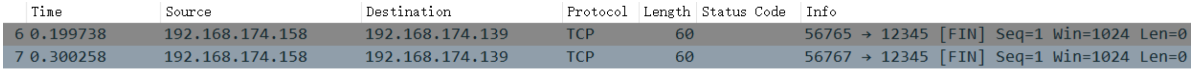


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.116693	192.168.174.158	192.168.174.139	TCP	60		36920 → 80 [FIN] Seq=1 Win=1024 Len=0
6	0.217797	192.168.174.158	192.168.174.139	TCP	60		36922 → 80 [FIN] Seq=1 Win=1024 Len=0

```
# 端口不开放
        1、源将FIN数据包发送到目标
        2、目标未回复（本应该回复RST包）
```



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sF -p 12345 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:16 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00044s latency).

PORT      STATE         SERVICE
12345/tcp open|filtered netbus
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

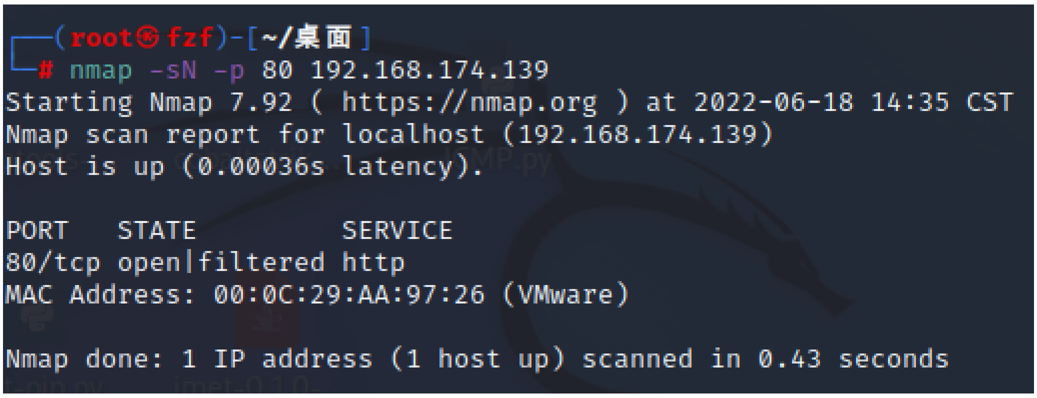


	Time	Source	Destination	Protocol	Length	Status Code	Info
6	0.199738	192.168.174.158	192.168.174.139	TCP	60		56765 → 12345 [FIN] Seq=1 Win=1024 Len=0
7	0.300258	192.168.174.158	192.168.174.139	TCP	60		56767 → 12345 [FIN] Seq=1 Win=1024 Len=0

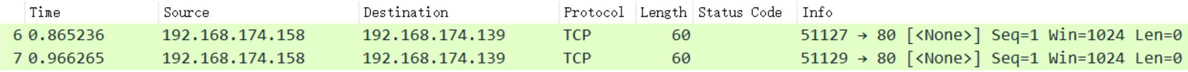
4、Null扫描

```
# 扫描语法（误报严重）
        nmap -sN -p [端口] [IP]
        空扫描是一系列TCP数据包，序列号为"零"（0000000），并且由于未设置任何标志，因此目的地将不知道如何回复请求。将丢弃该数据包，并不会发送任何答复，表明该端口开放
```

```
# 端口开放
        1、源将Null数据包发送到目标
        2、目标不回复源
```

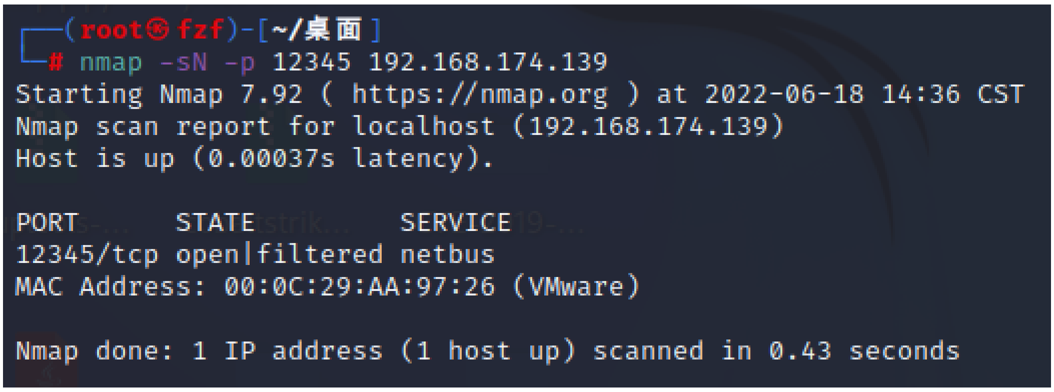


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sN -p 80 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:35 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00036s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

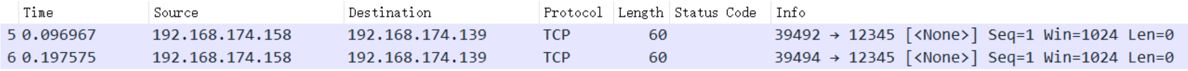


	Time	Source	Destination	Protocol	Length	Status Code	Info
6	0.865236	192.168.174.158	192.168.174.139	TCP	60		51127 → 80 [<None>] Seq=1 Win=1024 Len=0
7	0.966265	192.168.174.158	192.168.174.139	TCP	60		51129 → 80 [<None>] Seq=1 Win=1024 Len=0

```
# 端口不开放
	1、源将Null数据包发送到目标
	2、目标将RST、ACK发送到源
```



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sN -p 12345 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 14:36 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00037s latency).

PORT      STATE         SERVICE
12345/tcp open|filtered netbus
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

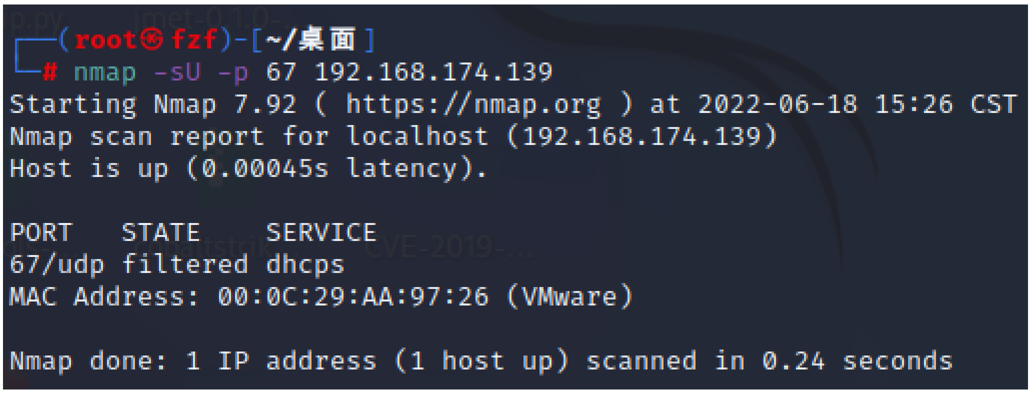


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.096967	192.168.174.158	192.168.174.139	TCP	60		39492 → 12345 [<None>] Seq=1 Win=1024 Len=0
6	0.197575	192.168.174.158	192.168.174.139	TCP	60		39494 → 12345 [<None>] Seq=1 Win=1024 Len=0

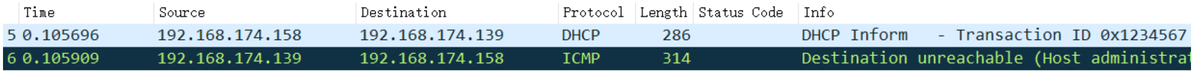
5、UDP扫描

```
# 扫描语法（误报严重）
	nmap -sU -p [端口] [IP]
	UDP扫描通过将UDP数据包发送到每个目标端口来进行。这是一个无连接协议。对于某些常见端口，将发送协议特定的有效负载以提高响应速度，服务将使用UDP数据包进行响应，证明其开放
```

```
# 端口开放
	1、源将UDP数据包发送到目标
	2、发送ICMP数据包Destnation unreachable（本该不回复）
```

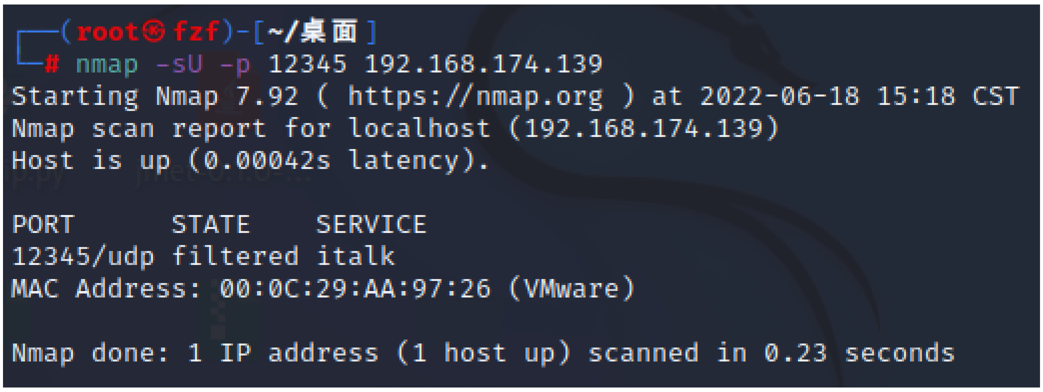


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sU -p 67 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 15:26 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00045s latency).

PORT   STATE    SERVICE
67/udp filtered dhcps
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

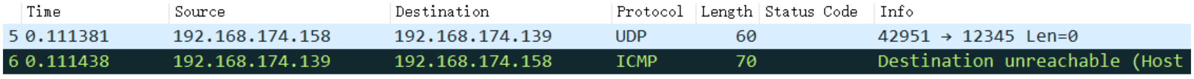


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.105696	192.168.174.158	192.168.174.139	DHCP	286		DHCP Inform - Transaction ID 0x1234567
6	0.105909	192.168.174.139	192.168.174.158	ICMP	314		Destination unreachable (Host administrat

```
# 端口不开放
    1、源将UDP数据包发送到目标
    2、目标发送ICMP数据包Destnation unreachable（无法到达目的地）
```



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sU -p 12345 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 15:18 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00042s latency).

PORT      STATE    SERVICE
12345/udp filtered italk
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

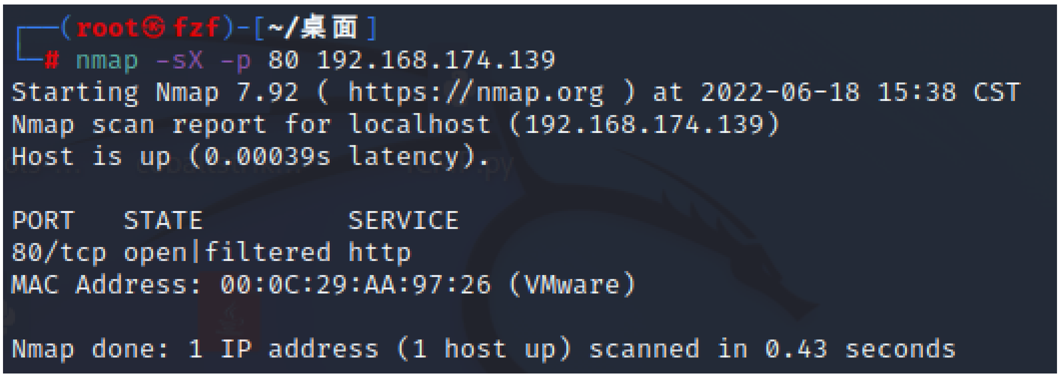


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.111381	192.168.174.158	192.168.174.139	UDP	60		42951 → 12345 Len=0
6	0.111438	192.168.174.139	192.168.174.158	ICMP	70		Destination unreachable (Host

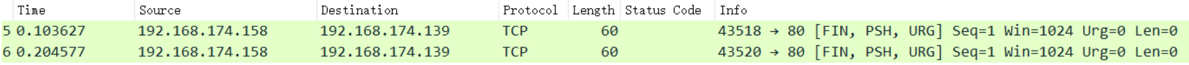
6、Xmas扫描

```
# 扫描语法（误报严重）
    nmap -sX -p [端口] [IP]
    当源将FIN、PUSH和URG数据包发送到特定端口时，如果该端口已开放，则目标丢弃该数据包，并且将不向源发送任何答复
```

```
# 端口开放
    1、源将FIN、PUSH和URG数据包发送给目标
    2、目标未回复源
```

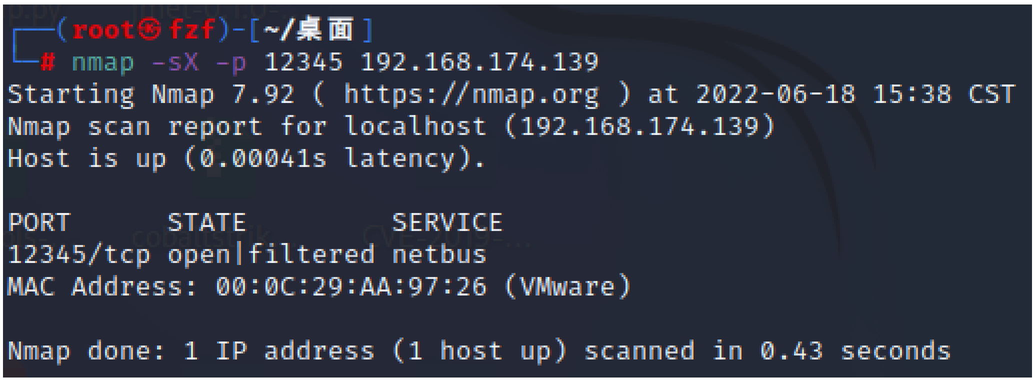


```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sX -p 80 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 15:38 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00039s latency).

PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

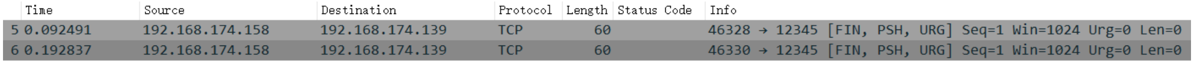


	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.103627	192.168.174.158	192.168.174.139	TCP	60		43518 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
6	0.204577	192.168.174.158	192.168.174.139	TCP	60		43520 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

```
# 端口不开放
    1、源将FIN、PUSH和URG数据包发送到目标
    2、目标未回复源（本应该将RST、ACK数据包发送到源）
```



```
┌──(root㉿fzf)-[~/桌面]
└─# nmap -sX -p 12345 192.168.174.139
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 15:38 CST
Nmap scan report for localhost (192.168.174.139)
Host is up (0.00041s latency).

PORT      STATE         SERVICE
12345/tcp open|filtered netbus
MAC Address: 00:0C:29:AA:97:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```



	Time	Source	Destination	Protocol	Length	Status Code	Info
5	0.092491	192.168.174.158	192.168.174.139	TCP	60		46328 → 12345 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
6	0.192837	192.168.174.158	192.168.174.139	TCP	60		46330 → 12345 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0