实验 2：端口扫描

姓名：潘韵泽 学号：2023141530019

完成日期：2025-09-24

一、 SYN 端口扫描基本原理

1. 三次握手

① Client → Server：SYN
② Server → Client：SYN-ACK（端口开放）或 RST（端口关闭）
③ Client → Server：ACK（仅开放时完成连接）

2. 半连接（Stealth / SYN）思想

攻击/扫描方故意不发送第三次 ACK，使连接永远停在第二步：

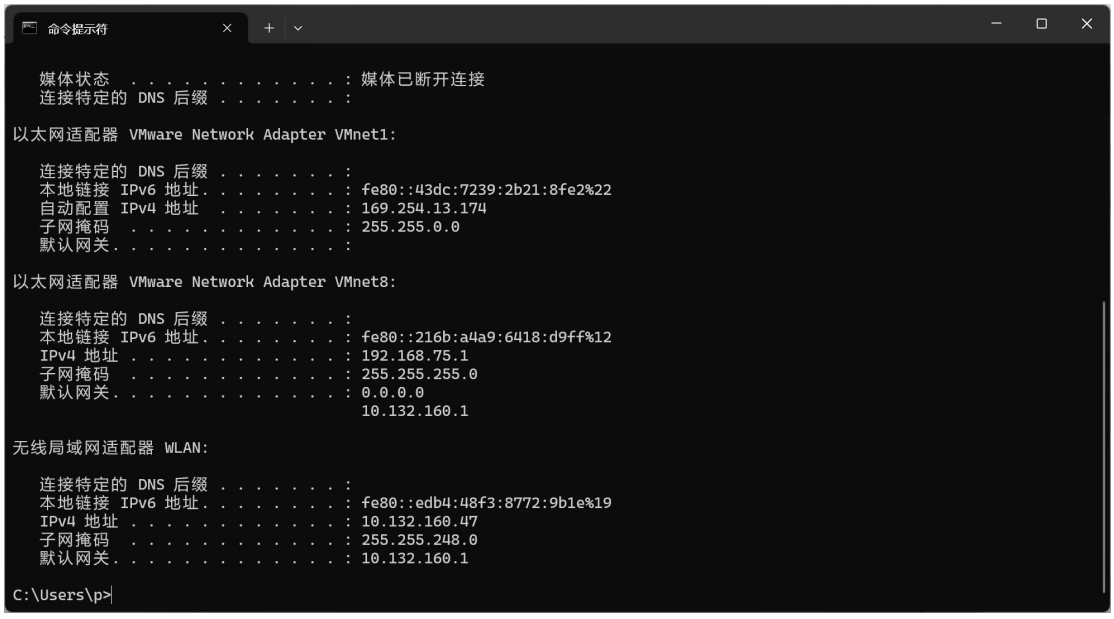
收到 SYN-ACK ⇒ 端口**开放**
收到 RST ⇒ 端口**关闭**
超时无响应 ⇒ 报文被过滤（防火墙丢弃）

3. 优点

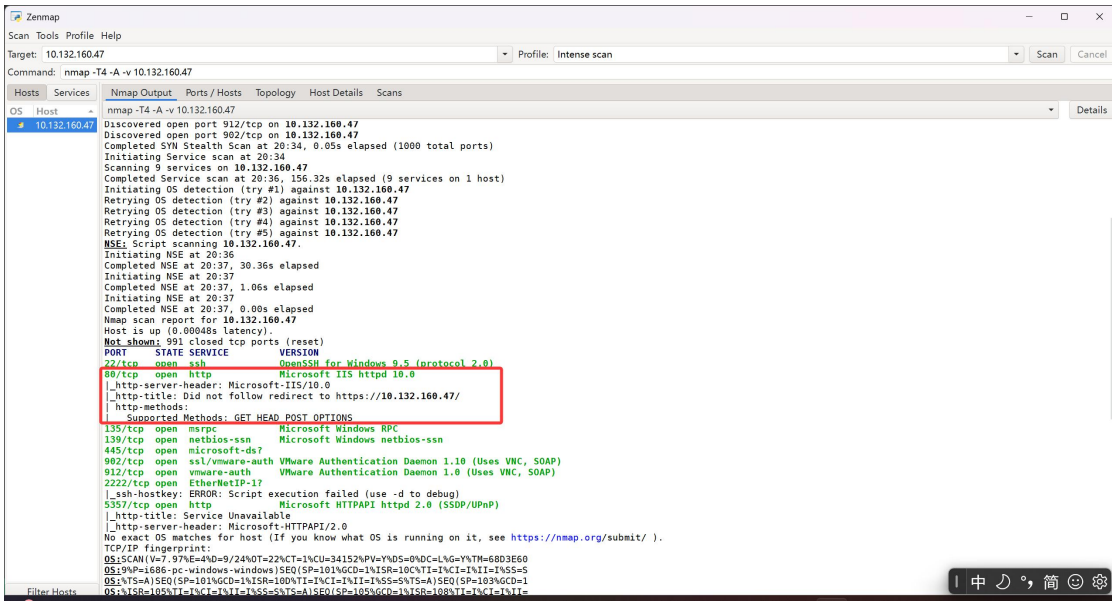
操作系统**不会记录完整连接**（/proc/net/tcp 无条目），日志极少。
可在**非 root** 用户空间通过 Raw-Socket（Scapy）构造包实现。
扫描速度高，适用于大段端口。

二、 端口扫描

使用 IPconfig 指令查找本机 IP 地址



使用 Nmap 对本机进行扫描，发现 80 端口 open



代码使用 SYN 端口扫描

```
dst_ip = "10.132.160.47"

src_port = RandShort()

dst_port = 80



stealth_scan_resp = sr1(IP(dst=dst_ip) / TCP(sport=src_port, dport=dst_port, flags="S"), timeout=10)

if (stealth_scan_resp is None):

    print("Closed")

elif (stealth_scan_resp.haslayer(TCP)):

    if (stealth_scan_resp.getlayer(TCP).flags == "SA"):

        print("Open")

    else:

        print("Closed")
```

代码指定扫描目标主机和接发方端口，构造 SYN 报文发送，在超时等待时间 10s 内等待第一个响应。目标主机在收到 SYN 报文后，若端口开放则会回复 SYN+ACK 报文，若端口关闭，则会回复 RST 报文，如果无返回报文则默认超时，报文被过滤或主机离线。

```
(langchain) C:\Users\p\OneDrive - stu.scu.edu.cn\桌面\作业\大三上\网络攻防\实验二\Lab2_code>python 01-S.py
Begin emission

Finished sending 1 packets
.*
Received 2 packets, got 1 answers, remaining 0 packets
Open

(langchain) C:\Users\p\OneDrive - stu.scu.edu.cn\桌面\作业\大三上\网络攻防\实验二\Lab2_code>
```