**实验 2：端口扫描  
姓名：潘韵泽 学号：2023141530019  
完成日期：2025-09-24**

1. **SYN端口扫描基本原理**
2. **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）
3. **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）

1. **优点**

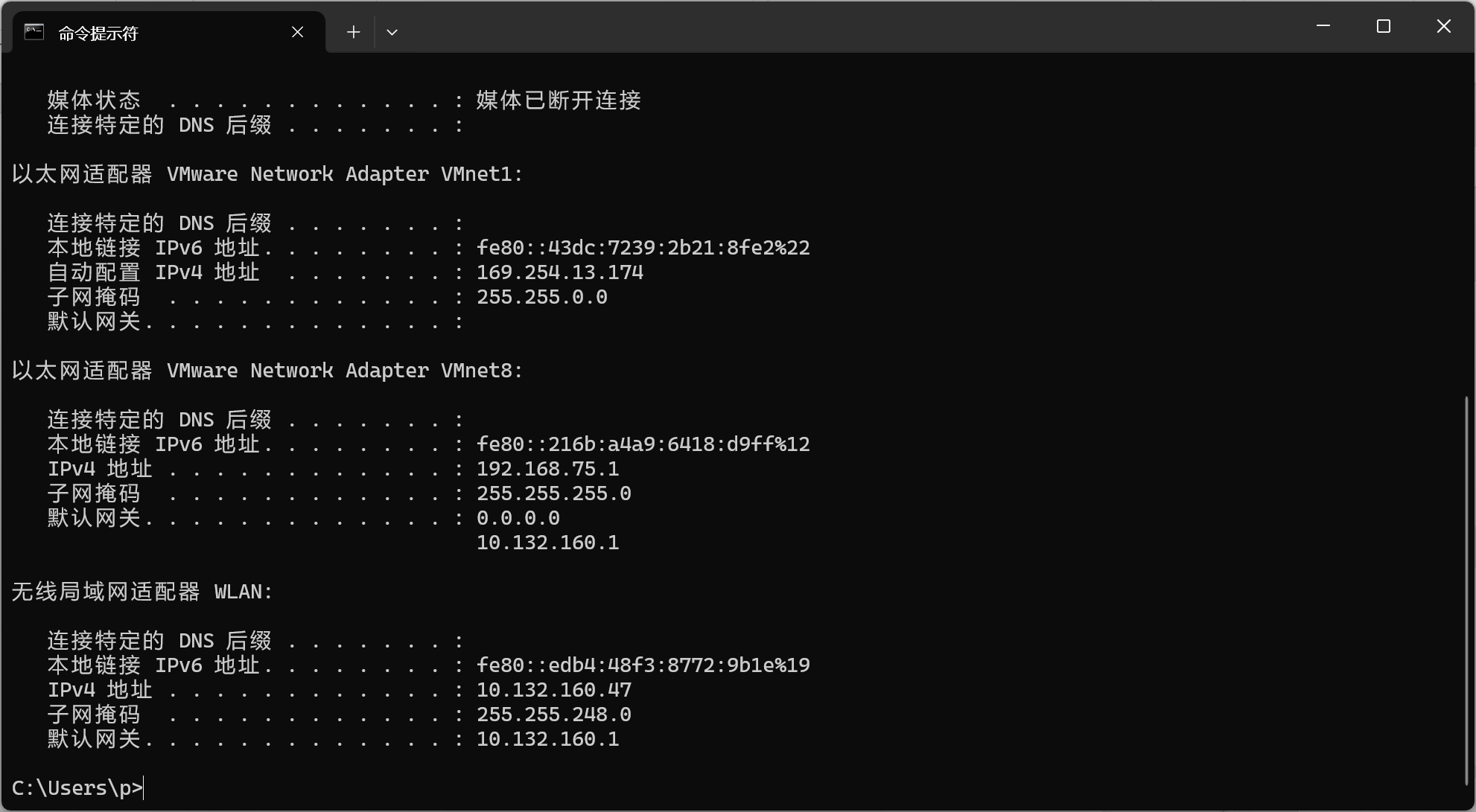
操作系统****不会记录完整连接****（/proc/net/tcp 无条目），日志极少。

可在****非 root**** 用户空间通过 Raw-Socket（Scapy）构造包实现。

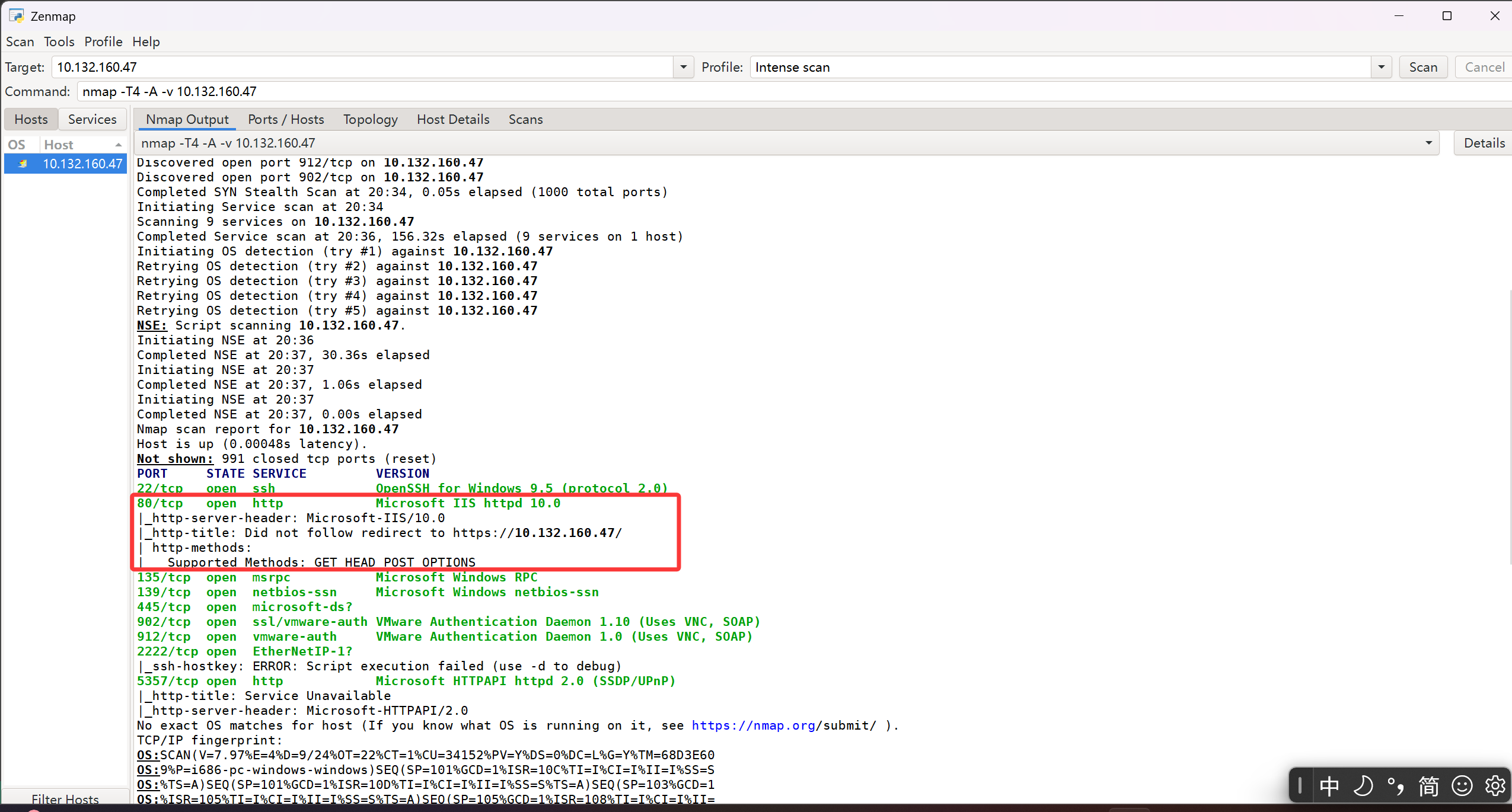
扫描速度高，适用于大段端口。

1. **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。

