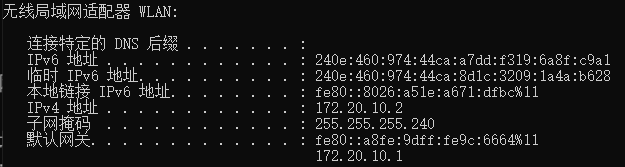
三、实验步骤

**1.对本地主机进行端口扫描**

先要查看本机IP地址，可通过ipconfig命令查看，如下例中本机地址为172.20.10.2

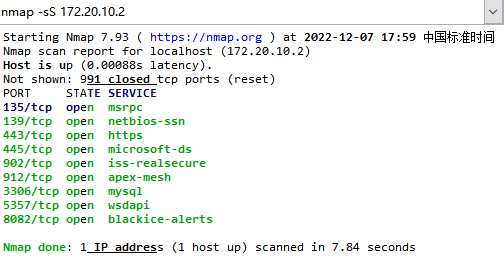
通过ifconfig命令找到本机ip地址为：172.20.10.2



通过Nmap工具使用不发ICMP包并且通过SYN包扫描的命令：

Nmap -sS 172.20.10.2

扫描得到结果：



172.20.10.2这台电脑打开了8个端口，分别是：

135/tcp msrpc服务

139/tcp netbios-ssn服务端口

443/tcp Https服务端口

445/tcp microsofy-ds服务端口

902/tcp iss-realsecure服务端口

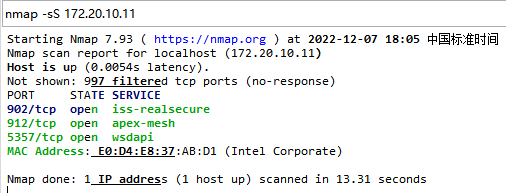
912/tcp apex-mesh服务端口

3306/tcp mysql服务端口

5357/tcp wsdapi服务端口

**2.对局域网的特定的主机进行端口扫描**

如，可对同一网段的172.20.10.11进行扫描:



172.20.10.11主机打开了五个端口，分别是：

902/tcp iss-realsecure服务端口

912/tcp apex-mesh

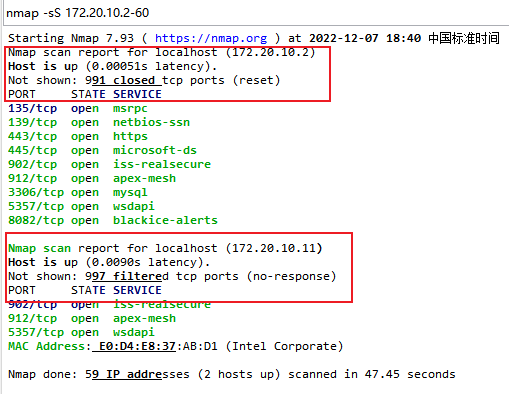
5357/tcp wsdapi服务端口

**3.对局域网的某些特定主机（如某一子网段）进行端口扫描**

如，对172.20.10.2-172.20.10.60这一网段内的58个IP进行系列扫描

使用如下命令：

Nmap -sS 172.20.10.2-60



如图，一共扫出两个IP：  
172.20.10.2

172.20.10.11