

信息安全实验报告

Nmap

实验名称

丁瑞

学生姓名

2016217676

学 号

物联网16-01班

专业班级

**2019**年 12月 30日

1. 实验目的

1、掌握端口扫描这种信息探测技术的原理；

2、学会使用常见端口扫描工具；

3、了解各种常用网络服务所对应的端口号。

1. 实验原理

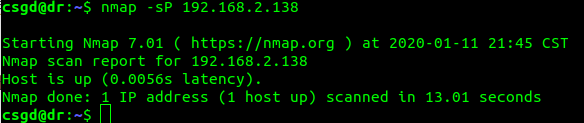
利用 Nmap 是一款开放源代码的网络探测和安全审核的工具。其设计目标是快速地扫描大型网络，也可以扫描单个主机。Nmap 使用原始 IP 报文来发现网络上的主机及其提供的服务，包括其应用程序名称和版本，这些服务运行的操作系统包括版本信息，它们使用什么类型的报文过滤器/防火墙，以及一些其它功能。虽然 Nmap 通常用于安全审核，但也可以利用来做一些日常管理维护的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

1. 实验步骤

**3.1主机发现**

进行连通性检测，来判断目标主机（IP 地址为 192.168.2.138）是否连通。

主机发现发现的原理与Ping命令类似，发送探测包到目标主机，如果收到回复，那么说明目标主机是开启的。Nmap支持十多种不同的主机探测方式，比如发送ICMP ECHO/TIMESTAMP/NETMASK报文、发送TCPSYN/ACK包、发送SCTP INIT/COOKIE-ECHO包，用户可以在不同的条件下灵活选用不同的方式来探测目标机。

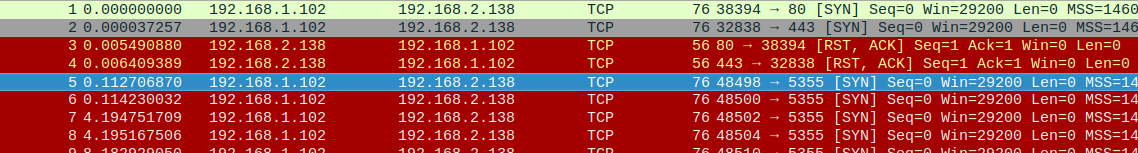


采用namp -sP指令判断对方主机是否在线，用wireshark抓包

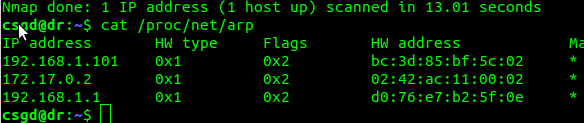
在执行命令后 本机向目标主机的80端口发送同步位SYN=1，序列号seq=0的请求连接报文段。

目标主机接收到连接请求报文后同意连接，返回报文SYN=1，ACK=1,确认序列号ack=0+1=1，自己的序列号为seq=1。

下图表示连接过程



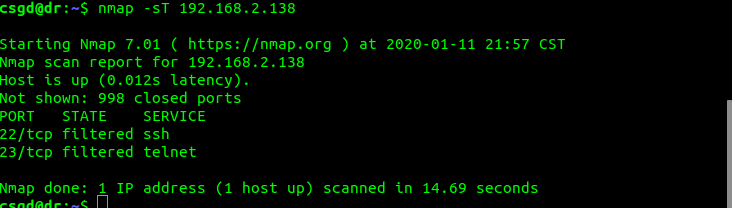
查看mac地址



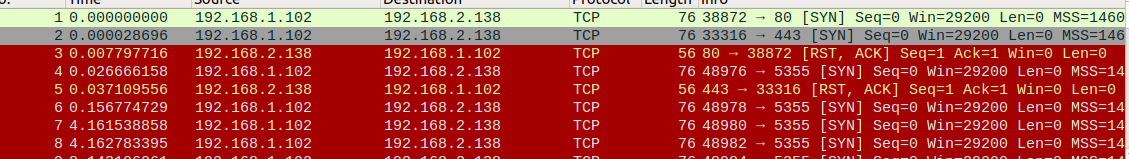
**3.2使用常规扫描**

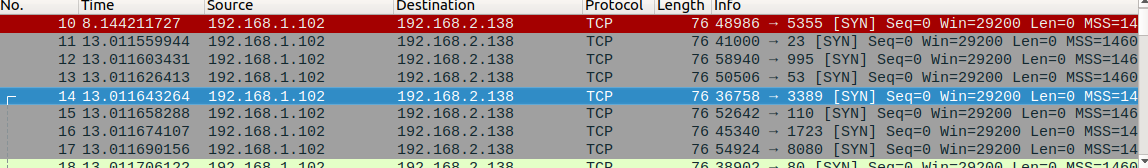
常规扫描方式对目标主机进行 TCP 扫描。

全连接。这种扫描方式是使用connect()系统调用打开目标机上相关端口的连接，并完成三次TCP握手

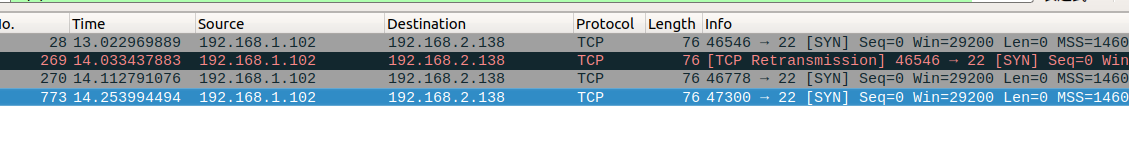


抓取报文的信息



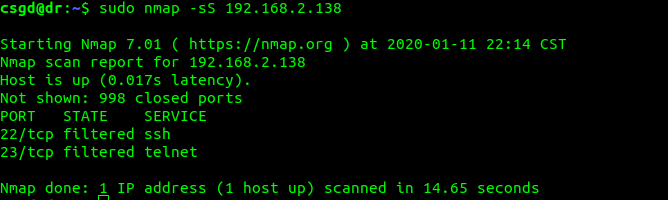


22号端口情况



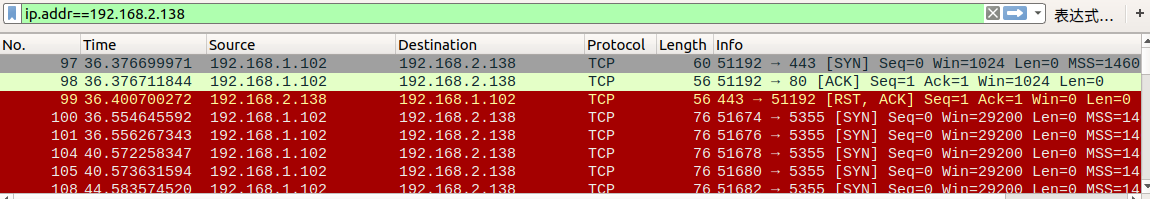
**3.3 SYN半扫描**

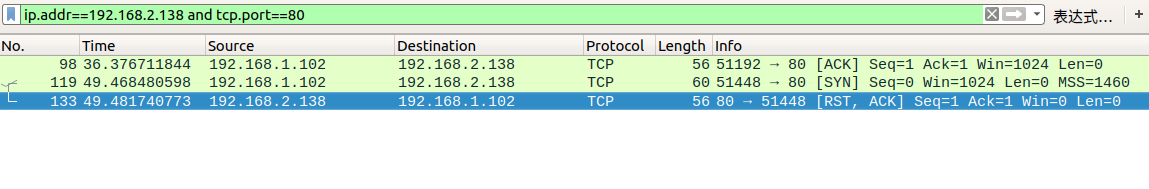
使用 SYN 半扫描方式对目标主机进行 TCP 端口扫描。



半连接的时间相比于全连接更短

半开扫描的原理是Nmap发送SYN包到远程主机，但是它不会产生任何会话，不需要通过完整的握手获得远程主机的信息，因此不会在目标主机上产生任何日志记录。



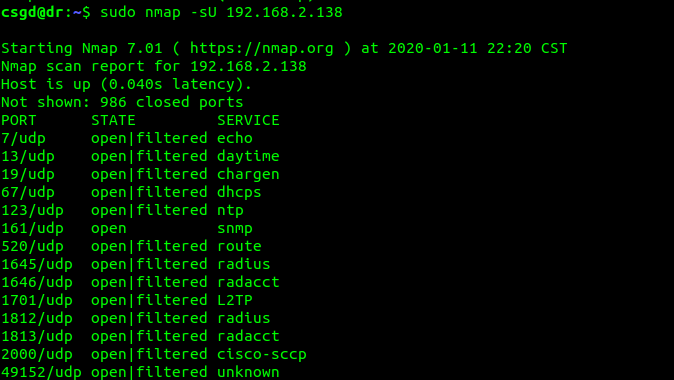


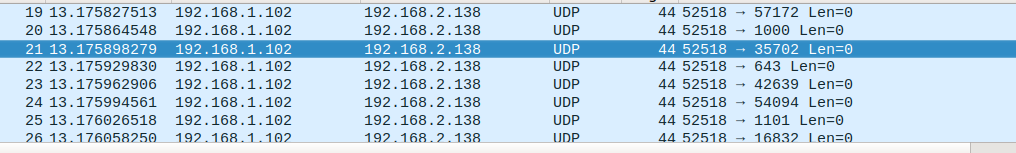
可见没有建立完整的连接就终止了

**3.4 UDP端口扫描**

对目标主机进行 UDP 端口扫描。

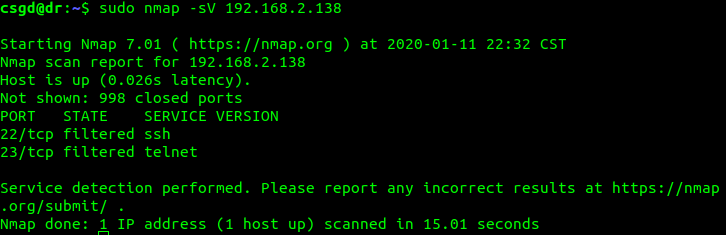
UDP Ping 扫描是发送一个空的UDP报文到指定的端口，如果不指定端口则默认40125，使用UDP ping扫描时Nmap会发送一个空的UDP包到目标主机，如果目标主机响应则返回一个ICMP端口不可达错误，如果目标主机不是存活状态则会返回各种ICMP错误信息。

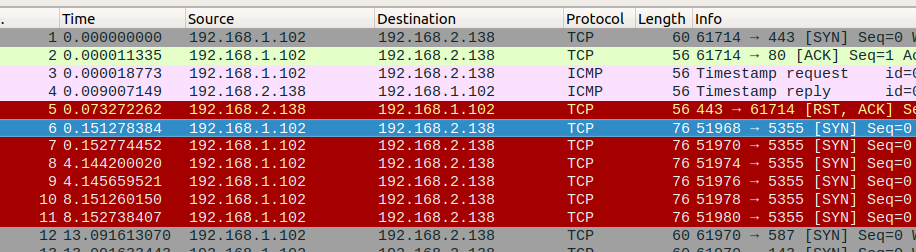




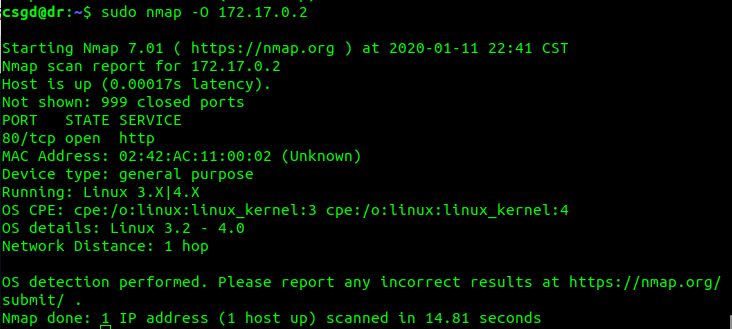
**3.5 目标主机扫描**

检测目标主机开放端口所提供的服务及其类型和版本信息。





**3.6 探测目标主机的操作系统类型。**



1. 实验总结

通过本次实验我学会了利用 Nmap 配合 Wireshark 的使用，对目标主机进行扫描，并获取到包括端口、操作系统、协议在内的有效信息。初步掌握了软件的使用。