

**警示:** 实验报告如有雷同, 雷同各方当次实验成绩均以 0 分计; 在规定时间内未上交实验报告的, 不得以其他方式补交, 当次成绩按 0 分计; 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机学院	班级	周五选修班	学号	13331233	姓名	孙中阳
完成日期: 2016 年 11 月 4 日							

## 网络扫描实验

### 【实验目的】

- 掌握网络扫描技术的原理。
- 学会使用 Nmap 扫描工具。

### 【实验环境】

实验主机操作系统: Mac OS Yosemite 10.10.5 IP 地址: 192.168.199.112  
目标机操作系统: Microsoft Windows 10 10586 IP 地址: 192.168.199.179  
网络环境: 局域网。

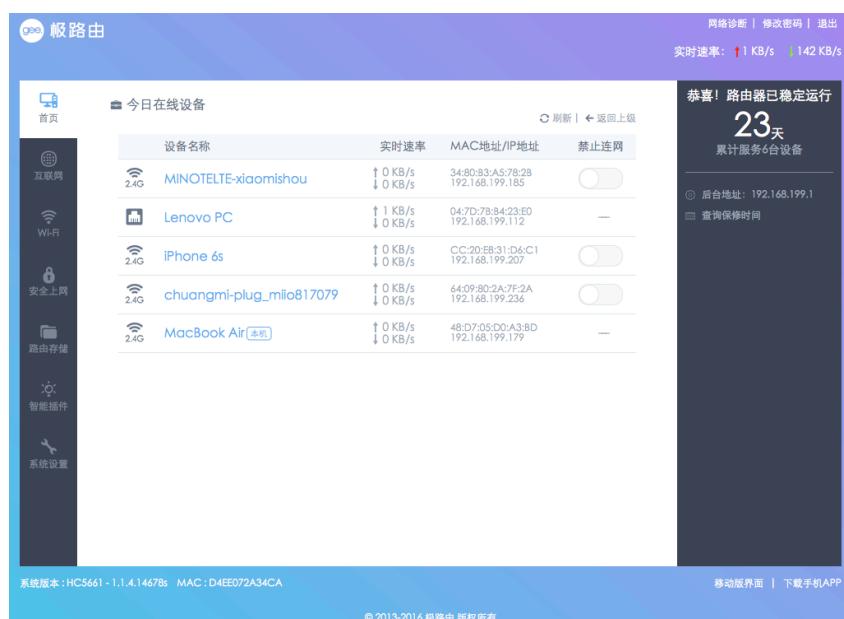
### 【实验工具】

Nmap (Network Mapper, 网络映射器) 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 以新颖的方式使用原始 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, 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。

### 【实验过程】(要有实验截图)

在实验过程中, 可通过 Wireshark 捕获数据包, 分析 Nmap 采用什么探测包。

本地网络状况





## 1. 主机发现：进行连通性监测，判断目标主机。

本地目标 IP 地址为 192.168.199.112，首先确定测试机与目标机物理连接是连通的。

### ① 关闭目标机的防火墙，分别命令行窗口用 Linux 命令

```
ping 192.168.199.112
```

```
1. ping 192.168.199.112 (ping)
Last login: Fri Nov  4 00:33:04 on ttys000
SJD@SJDdeAir ~ ping 192.168.199.112
PING 192.168.199.112 (192.168.199.112): 56 data bytes
64 bytes from 192.168.199.112: icmp_seq=0 ttl=64 time=13.471 ms
64 bytes from 192.168.199.112: icmp_seq=1 ttl=64 time=3.864 ms
64 bytes from 192.168.199.112: icmp_seq=2 ttl=64 time=4.259 ms
64 bytes from 192.168.199.112: icmp_seq=3 ttl=64 time=8.220 ms
64 bytes from 192.168.199.112: icmp_seq=4 ttl=64 time=10.464 ms
64 bytes from 192.168.199.112: icmp_seq=5 ttl=64 time=7.087 ms
64 bytes from 192.168.199.112: icmp_seq=6 ttl=64 time=3.838 ms
64 bytes from 192.168.199.112: icmp_seq=7 ttl=64 time=3.626 ms
64 bytes from 192.168.199.112: icmp_seq=8 ttl=64 time=4.176 ms
64 bytes from 192.168.199.112: icmp_seq=9 ttl=64 time=10.021 ms
64 bytes from 192.168.199.112: icmp_seq=10 ttl=64 time=5.881 ms
64 bytes from 192.168.199.112: icmp_seq=11 ttl=64 time=4.161 ms
```

和 Nmap 命令

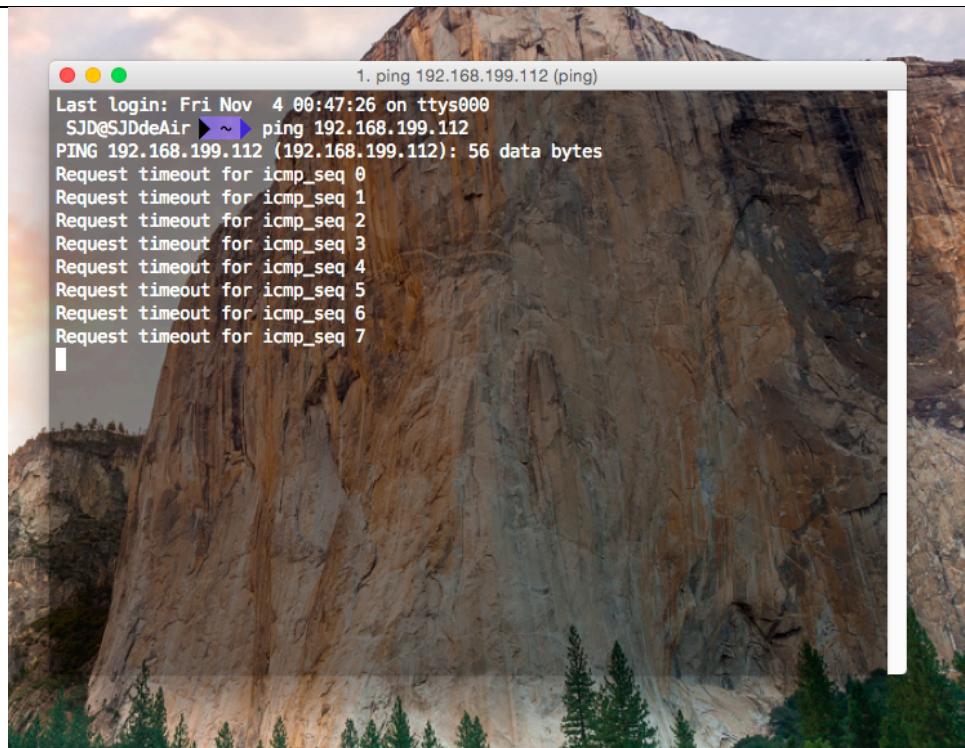
```
nmap -sP 192.168.199.112
```

```
1. SJD@SJDdeAir: ~ (zsh)
Last login: Fri Nov  4 00:49:07 on ttys000
SJD@SJDdeAir ~ nmap -sP 192.168.199.112
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-04 00:50 CST
Nmap scan report for SJD.lan (192.168.199.112)
Host is up (0.00032s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds
SJD@SJDdeAir ~
```

进行测试，记录测试情况。简要说明测试差别。

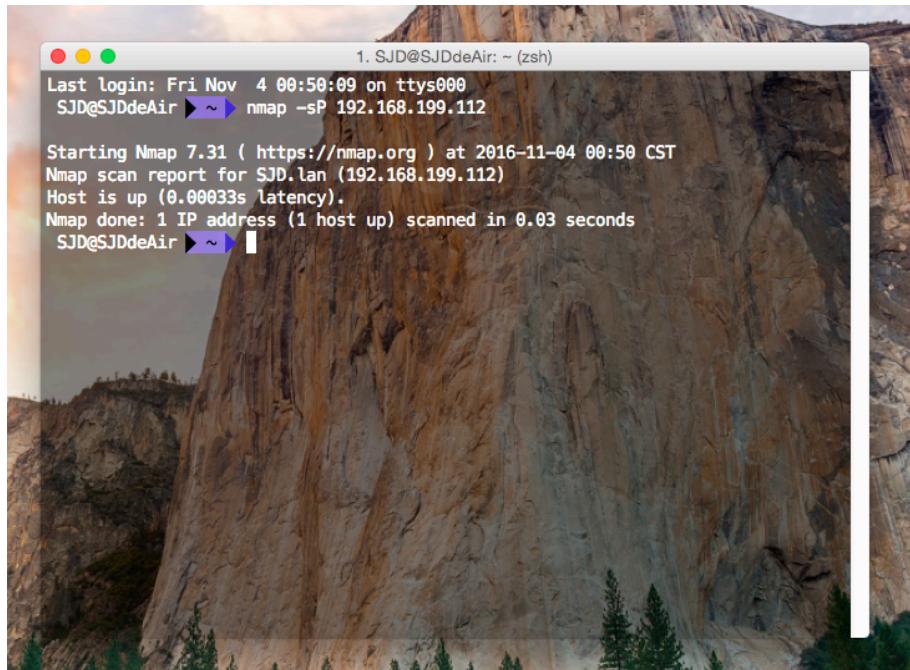
### ② 开启目标机的防火墙，重复①，结果有什么不同？请说明原因。

```
ping 192.168.199.112
```



和 Nmap 命令

```
nmap -sP 192.168.199.112
```



③ 测试结果不连通，但实际上是物理连通的，什么原因？

根据推测，物理上本地机器和目标机器是联通的，在有防火墙时，可进行一定范围的通信，但其中 ping 操作发送的数据包被目标机器防火墙拦截。而没有防火墙时，仍可进行一定范围的通信，这一范围可能更广，ping 操作发送的数据包并没有被拦截，返回了正常的结果。

## 2. 对目标主机进行 TCP 端口扫描

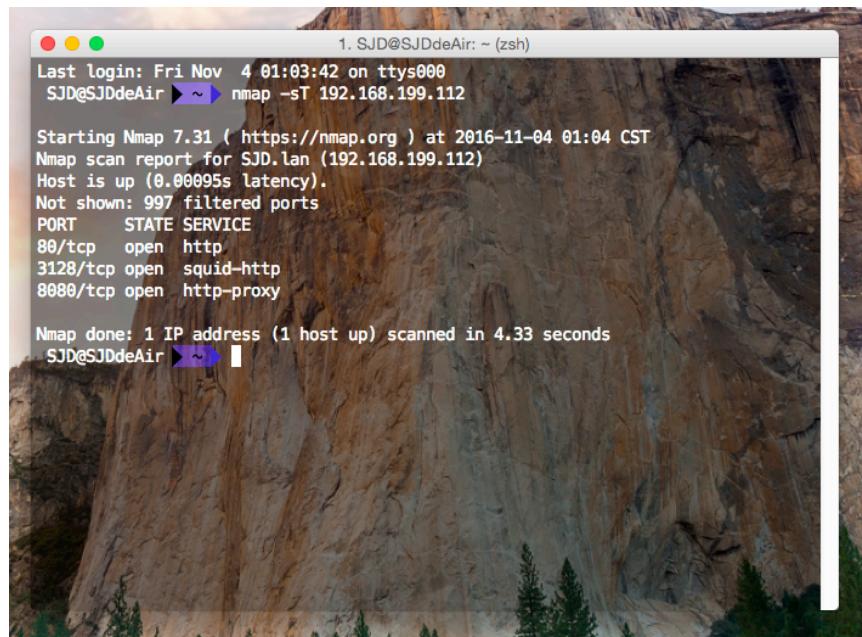
### ① 使用常规扫描方式

```
Nmap -sT 172.16.1.101
```

请将扫描检测结果截图写入实验报告，包括所有的端口及开放情况。

这部分测试过程中发现，目标机器防火墙会对计划操作产生影响

防火墙开启状态

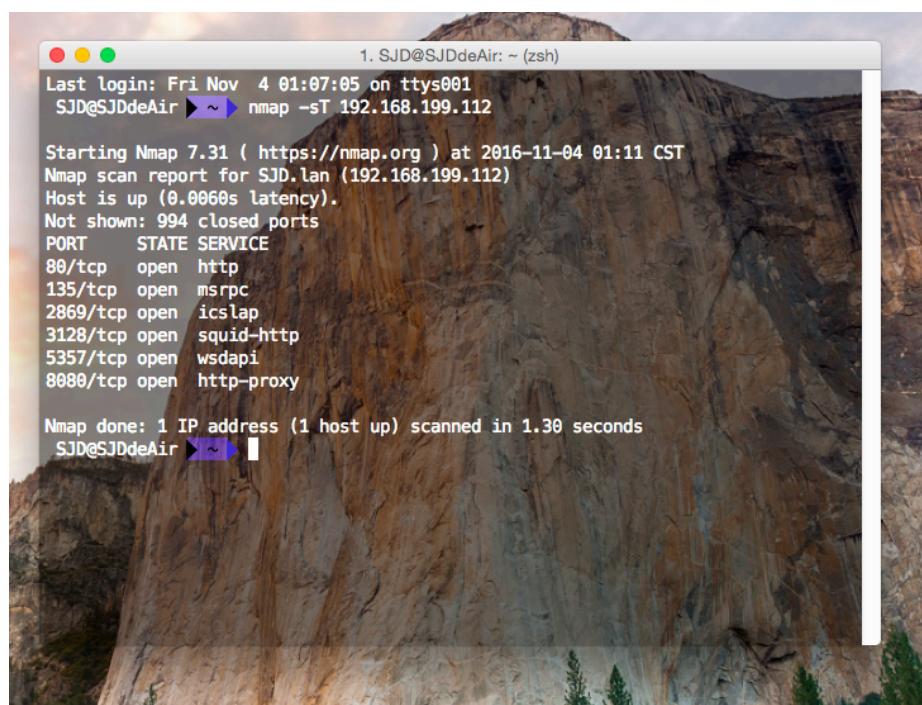


```
1. SJD@SJDdeAir: ~ (zsh)
Last login: Fri Nov  4 01:03:42 on ttys000
SJD@SJDdeAir ➤ ~▶ nmap -sT 192.168.199.112

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-04 01:04 CST
Nmap scan report for SJD.lan (192.168.199.112)
Host is up (0.00095s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
3128/tcp  open  squid-http
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
SJD@SJDdeAir ➤ ~▶
```

防火墙关闭状态



```
1. SJD@SJDdeAir: ~ (zsh)
Last login: Fri Nov  4 01:07:05 on ttys001
SJD@SJDdeAir ➤ ~▶ nmap -sT 192.168.199.112

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-04 01:11 CST
Nmap scan report for SJD.lan (192.168.199.112)
Host is up (0.0060s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
2869/tcp  open  icslap
3128/tcp  open  squid-http
5357/tcp  open  wsdapi
8080/tcp  open  http-proxy

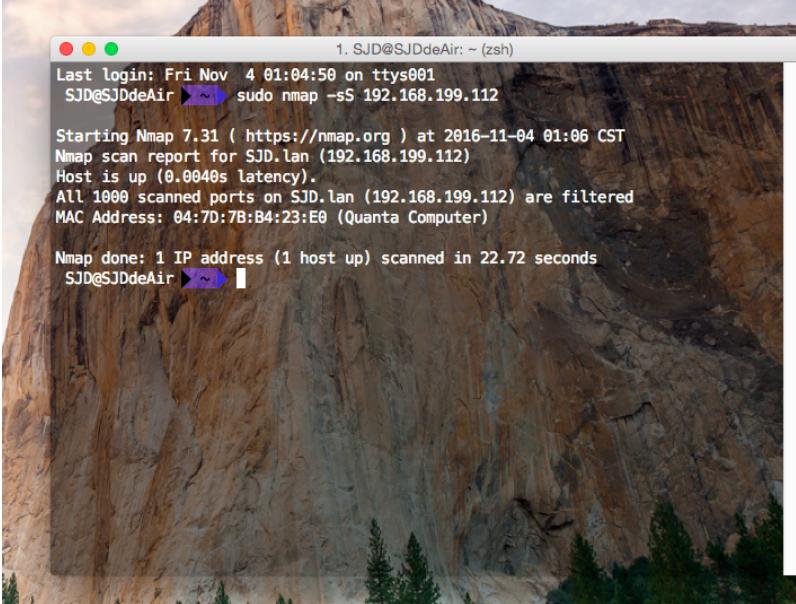
Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
SJD@SJDdeAir ➤ ~▶
```

② 使用 SYN 半扫描方式

Nmap -sS 172.16.1.101

请将扫描检测结果截图写入实验报告，包括所有的端口及开放情况。

防火墙开启状态

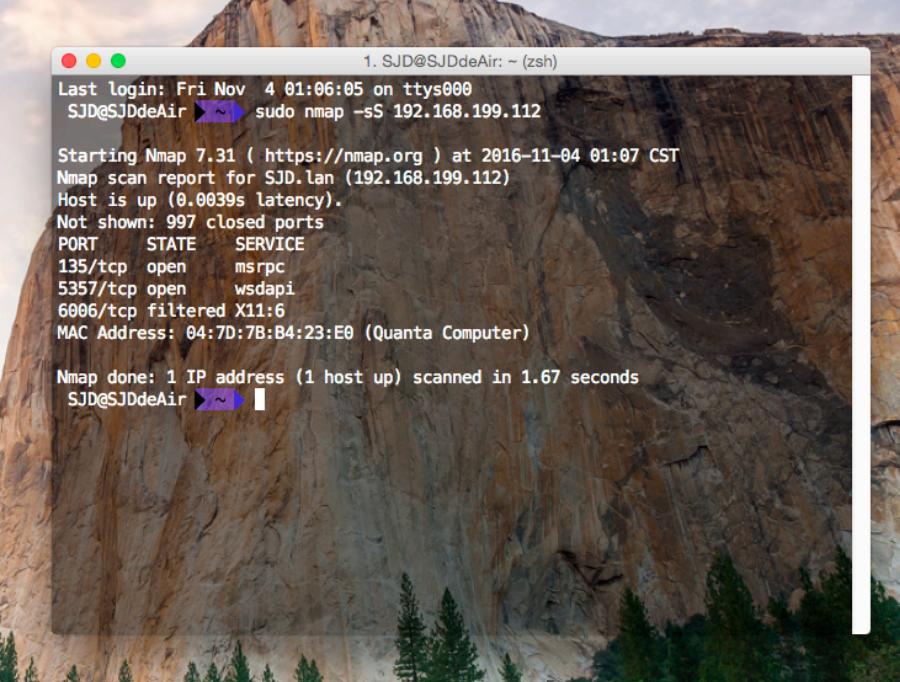


```
1. SJD@SJDdeAir: ~ (zsh)
Last login: Fri Nov  4 01:04:50 on ttys001
SJD@SJDdeAir [~] ~▶ sudo nmap -sS 192.168.199.112

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-04 01:06 CST
Nmap scan report for SJD.lan (192.168.199.112)
Host is up (0.0040s latency).
All 1000 scanned ports on SJD.lan (192.168.199.112) are filtered
MAC Address: 04:7D:7B:B4:23:E0 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 22.72 seconds
SJD@SJDdeAir [~] ~▶
```

防火墙关闭状态



```
1. SJD@SJDdeAir: ~ (zsh)
Last login: Fri Nov  4 01:06:05 on ttys001
SJD@SJDdeAir [~] ~▶ sudo nmap -sS 192.168.199.112

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-04 01:07 CST
Nmap scan report for SJD.lan (192.168.199.112)
Host is up (0.0039s latency).
Not shown: 997 closed ports
PORT      STATE     SERVICE
135/tcp    open      msrpc
5357/tcp   open      wsddapi
6006/tcp   filtered X11:6
MAC Address: 04:7D:7B:B4:23:E0 (Quanta Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
SJD@SJDdeAir [~] ~▶
```

④ 比较上述两次扫描结果差异、扫描所花费的时间。并进行解释。



首先，扫描到的端口有所不同，总体来讲，前者更多一些。耗时方面，前者却更少。这和我查找到的资料并不相同，理论上来讲，SYN 半扫描只建立两次握手，速度快而且能扫描更多的端口。常规扫描主要建立 TCP 连接，速度更慢而且不一定能扫描很多端口。本例出现的情况可能的原因是网络干扰，目标主机正在下载等等，造成扫描时间较长。

## 【实验体会】

感觉 nmap 还是非常有实际作用的，不仅可以用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统，使用了哪些软件，方便进行统一的查询和管理。