

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		班级		学号		姓名	
完成日期：							

网络扫描实验

【实验目的】

1. 掌握网络扫描技术的原理。
2. 学会使用 Nmap 扫描工具。

【实验环境】

实验主机操作系统：Linux IP地址：192.168.199.100
目标机操作系统：Windows IP地址：192.168.199.104
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）

假设以下测试命令假设目标机 IP 是 172.16.1.101。

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。

1. 主机发现：进行连通性监测，判断目标主机。

假设本地目标 IP 地址为 172.16.1.101，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 Windows 命令

ping 172.16.1.101

和 Nmap 命令

nmap -sP 172.16.1.101

进行测试，记录测试情况。简要说明测试差别。

```
jskyzero@MOONS: ~  
~ ping 192.168.199.171  
PING 192.168.199.171 (192.168.199.171) 56(84) bytes of data.  
64 bytes from 192.168.199.171: icmp_seq=1 ttl=64 time=0.019 ms  
64 bytes from 192.168.199.171: icmp_seq=2 ttl=64 time=0.018 ms  
64 bytes from 192.168.199.171: icmp_seq=3 ttl=64 time=0.019 ms  
64 bytes from 192.168.199.171: icmp_seq=4 ttl=64 time=0.018 ms  
64 bytes from 192.168.199.171: icmp_seq=5 ttl=64 time=0.019 ms  
64 bytes from 192.168.199.171: icmp_seq=6 ttl=64 time=0.015 ms  
^C  
--- 192.168.199.171 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5101ms  
rtt min/avg/max/mdev = 0.015/0.018/0.019/0.001 ms  
~ nmap -sP 192.168.199.171  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:00 HKT  
Nmap scan report for MOONS.lan (192.168.199.171)  
Host is up (0.000050s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds  
~
```

差别：ping 指令会显示一些额外信息，而 Nmap 则只会检查主机是否开启。

② 开启目标机的防火墙，重复①，结果有什么不同？请说明因。

没有不同，目标机一直处于开启防火墙状态，同时对网络设置为专用网络。

按照题意，推测这里开启防火墙以后会无法 ping 通 / Scan 显示目标主机 down，原因是目标主机的防火墙的过滤作用。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

上面测试连接是接通的，两台主机之间通过路由器无线链接。

按照题意，推测这里应该回答由于目标主机防火墙的过滤作用导致无法连接。

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。

② 使用 SYN 半扫描方式

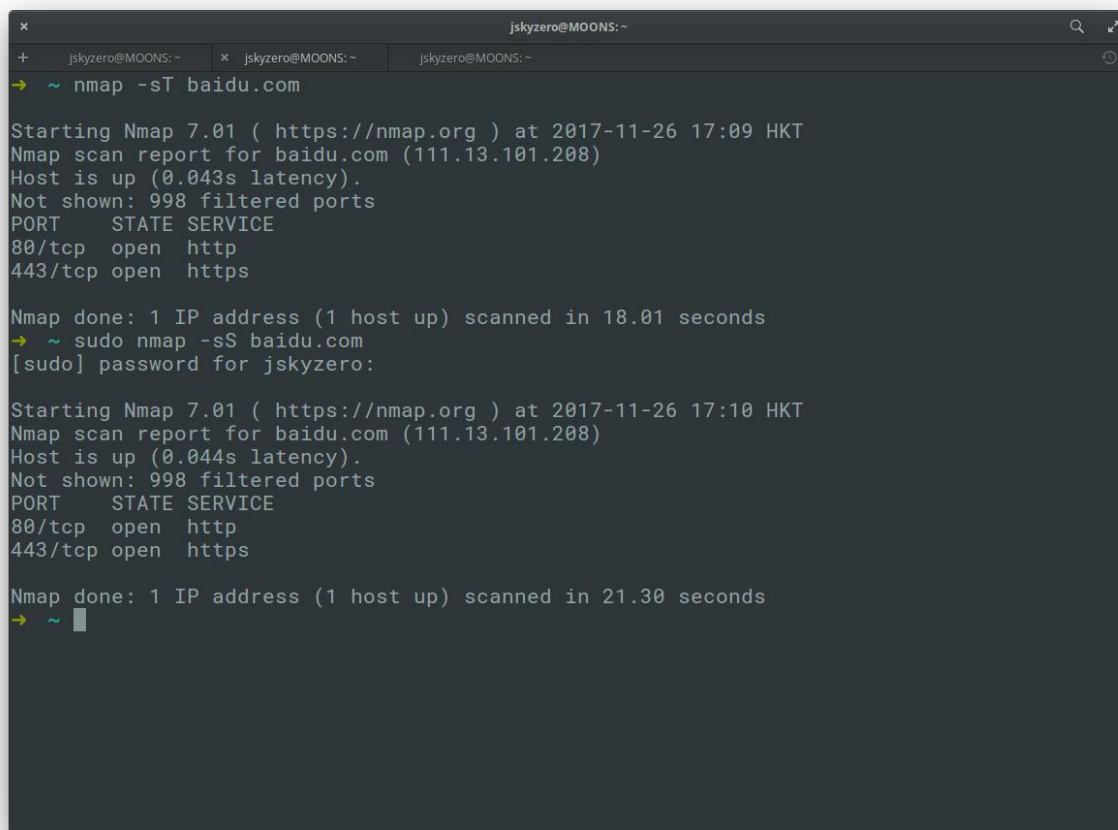
Nmap -sS 172.16.1.101

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。

③ 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。

```
jskyzero@MOONS: ~  
→ ~ nmap -sT 192.168.199.171  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:05 HKT  
Nmap scan report for MOONS.lan (192.168.199.171)  
Host is up (0.000035s latency).  
All 1000 scanned ports on MOONS.lan (192.168.199.171) are closed  
  
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds  
→ ~ nmap -sS 192.168.199.171  
You requested a scan type which requires root privileges.  
QUITTING!  
→ ~ sudo nmap -sS 192.168.199.171  
[sudo] password for jskyzero:  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:05 HKT  
Nmap scan report for MOONS.lan (192.168.199.171)  
Host is up (0.000030s latency).  
All 1000 scanned ports on MOONS.lan (192.168.199.171) are closed  
  
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds  
→ ~ █
```

```
jskyzero@MOONS: ~  
+ jskyzero@MOONS: ~ ... nmap -sS.baidu.com x jskyzero@MOONS: ~  
PING qq.com (125.39.240.113) 56(84) bytes of data.  
^C  
--- qq.com ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms  
  
→ ~ nmap -sT 125.39.240.113  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:09 HKT  
Nmap scan report for no-data (125.39.240.113)  
Host is up (0.036s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
843/tcp    open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 9.62 seconds  
→ ~ nmap -sS 125.39.240.113  
You requested a scan type which requires root privileges.  
QUITTING!  
→ ~ sudo nmap -sS 125.39.240.113  
[sudo] password for jskyzero:  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:10 HKT  
Nmap scan report for no-data (125.39.240.113)  
Host is up (0.035s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
843/tcp    open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 20.19 seconds  
→ ~ █
```



```
jskyzero@MOONS: ~  
→ ~ nmap -sT baidu.com  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:09 HKT  
Nmap scan report for baidu.com (111.13.101.208)  
Host is up (0.043s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp    open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 18.01 seconds  
→ ~ sudo nmap -sS baidu.com  
[sudo] password for jskyzero:  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2017-11-26 17:10 HKT  
Nmap scan report for baidu.com (111.13.101.208)  
Host is up (0.044s latency).  
Not shown: 998 filtered ports  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp    open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 21.30 seconds  
→ ~ █
```

情况如图，从结果来看两种扫描基本一样，第二种 SYN 扫描需要系统权限发送特殊的 IP 包，从耗时来看，第二种似乎耗时更长，但是就感觉上来说常规扫描建立链接应该耗时更长。查了一下似乎，大部分人是常规扫描耗时更长，至于上面的测试情况可能有多种环境的因素因而结果可能不准确。

【实验体会】

总感觉，实际经历的和实验本来希望经历的有点区别，不过实验本身并不难，而且很有趣，试着扫描了 Tencent / Baidu / Bing 的 IP，其中 Bing 打开了非常多的端口，扫了一下只能大概认懂一些比如 POP3S 的，总的来说本次实验还是很有趣的。