

**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	周一3-4 节	学号	15331151	姓名	李佳
完成日期： 2017 年 11 月 20 日							

## 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： Win 10 IP地址： 172.18.158.60

目标机操作系统： Win 10 IP地址： 172.18.157.178

网络环境： 中山大学校园网。

### 【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。

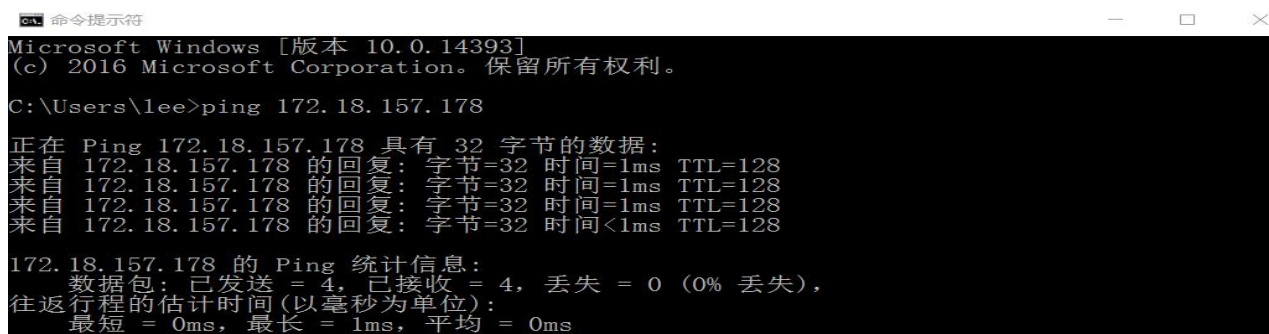
- ① 关闭目标机的防火墙，分别命令行窗口用 Windows 命令

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。



```
命令提示符
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Users\lee>ping 172.18.157.178

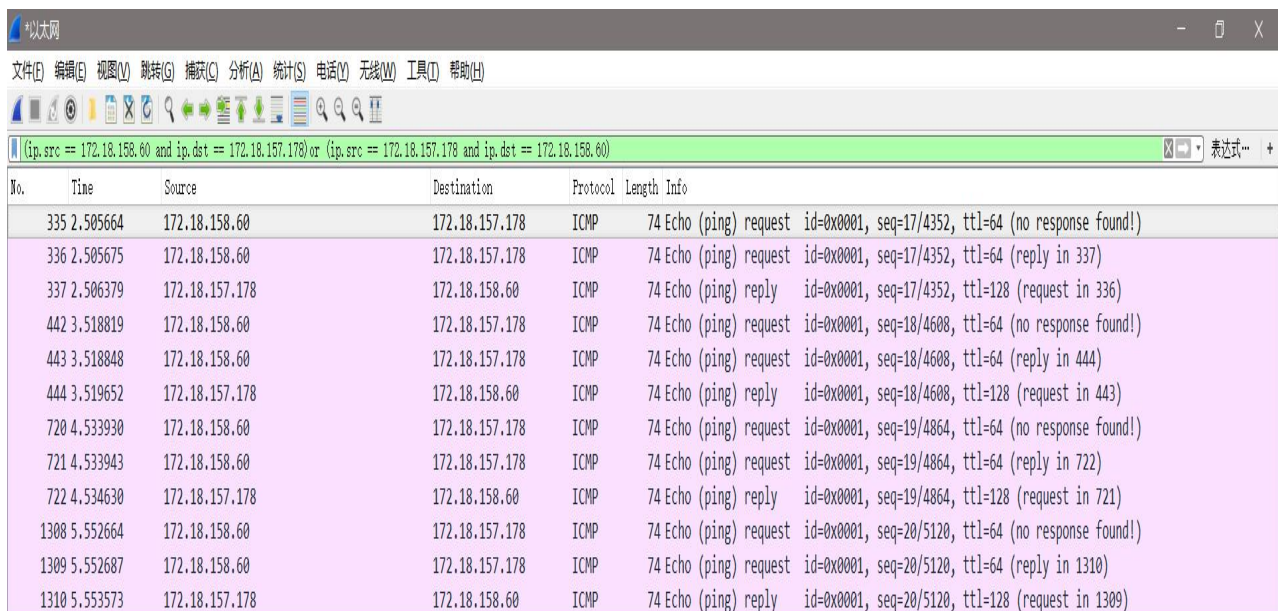
正在 Ping 172.18.157.178 具有 32 字节的数据:
来自 172.18.157.178 的回复: 字节=32 时间=1ms TTL=128
来自 172.18.157.178 的回复: 字节=32 时间=1ms TTL=128
来自 172.18.157.178 的回复: 字节=32 时间=1ms TTL=128
来自 172.18.157.178 的回复: 字节=32 时间<1ms TTL=128

172.18.157.178 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

```
C:\Users\lee>nmap -sP 172.18.157.178

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-20 18:45 ?Dlú±ê×?ê±??
Nmap scan report for 172.18.157.178
Host is up (0.00s latency).
MAC Address: F8:A9:63:B9:4D:03 (Compal Information (kunshan))
Nmap done: 1 IP address (1 host up) scanned in 8.82 seconds
```

ping 指令会向目标机发送报文，并且反馈每个报文是否送达并计算 RTT 时间，通过查看包是否顺利达到测试本机与目标机的连通性。而 nmap 的反馈结果中显示了扫描目标机的 IP 地址，以及目标机的状态，同时有目标机的 MAC 地址及所使用的网卡以及扫描目标机所用的时间 8.82s。从时间上来说，nmap 扫描所需要的时间更多，但是 nmap 所显示的信息更加简洁。



Wireshark interface showing a packet capture on the interface \*以太网. The filter is set to (ip.src == 172.18.158.60 and ip.dst == 172.18.157.178) or (ip.src == 172.18.157.178 and ip.dst == 172.18.158.60). The capture shows 12 ICMP Echo (ping) requests and replies between 172.18.158.60 and 172.18.157.178. Requests 335, 442, 720, and 1308 resulted in 'no response found!', while the others received replies.

No.	Time	Source	Destination	Protocol	Length	Info
335	2.505664	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
336	2.505675	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 337)
337	2.506379	172.18.157.178	172.18.158.60	ICMP	74	Echo (ping) reply id=0x0001, seq=17/4352, ttl=128 (request in 336)
442	3.518819	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
443	3.518848	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 444)
444	3.519652	172.18.157.178	172.18.158.60	ICMP	74	Echo (ping) reply id=0x0001, seq=18/4608, ttl=128 (request in 443)
720	4.533930	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
721	4.533943	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 722)
722	4.534630	172.18.157.178	172.18.158.60	ICMP	74	Echo (ping) reply id=0x0001, seq=19/4864, ttl=128 (request in 721)
1308	5.552664	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
1309	5.552687	172.18.158.60	172.18.157.178	ICMP	74	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 1310)
1310	5.553573	172.18.157.178	172.18.158.60	ICMP	74	Echo (ping) reply id=0x0001, seq=20/5120, ttl=128 (request in 1309)

通过 wireshark 抓包结果看到可得：ping 指令会向目标机发送数据包，而 nmap -sP 指令不会对目标机发送报文，只是列出主机的相关信息。有 12 个报文传输与源主机和目标主机之间。

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。

```
C:\Users\lee>ping 172.18.157.178

正在 Ping 172.18.157.178 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

172.18.157.178 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-20 19:02 ?Dlú±ê×?ê±??
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.99 seconds

C:\Users\lee>.
```

ping 命令显示请求超时，nmap -sP 命令显示主机 down 掉了。所有的传入都被目标主机防火墙阻止。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

网络上的机器都会被分配到一个确定的 IP 地址，当我们用本机给目标 IP 地址发送一个数据包时，对方就要返回一个同样大小的数据包，本机根据是否有返回的数据包来确定目标主机的存在以及在线状态，并且可以初步判断目标主机的操作系统等信息。

但是当开启防火墙后，目标主机拒绝接收源主机发送的数据包并且不做响应，从而造成不连通，但是物理上，两台主机是有网络线缆相连的，所以物理连通。

## 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。

```
C:\Users\lee>nmap -sT 172.18.157.178

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-20 19:04 ?Dlú±ê×?ê±??
Nmap scan report for 172.18.157.178
Host is up (1.0s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
MAC Address: F8:A9:63:B9:4D:03 (Compal Information (kunshan))

Nmap done: 1 IP address (1 host up) scanned in 236.15 seconds

C:\Users\lee>.
```

首先再次关闭防火墙。扫描用时 236.15s。

可以看到有 995 个关闭端口；目标机使用的端口有 5 个处于开放状态（135、139、445、5357、5432），且扫描结果只有使用 TCP 协议的端口使用情况。开放的端口所提供的服务也可以在扫描结果中看出。

## 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。

```
C:\WINDOWS\system32>nmap -sS 172.18.157.178

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-20 19:06 ?Dlú±ê×?ê±??
Nmap scan report for 172.18.157.178
Host is up (0.00096s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5357/tcp   open  wsapi
5432/tcp   open  postgresql
MAC Address: F8:A9:63:B9:4D:03 (Compal Information (kunshan))

Nmap done: 1 IP address (1 host up) scanned in 9.57 seconds

C:\WINDOWS\system32>_
```

继续关闭防火墙。扫描用时 9.57s。

可以看到还是有 995 个关闭端口；目标机使用的端口有 5 个处于开放状态（135、139、445、5357、5432），且扫描结果只有使用 TCP 协议的端口使用情况。开放的端口所提供的服务也可以在扫描结果中看出。

## 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。

Nmap -sT 扫描所花费的时间为 236.15s，而 nmap -sS 扫描所花费的时间仅为 9.57s，半扫描的速度明显要高于完整的 TCP 扫描模式。经过查阅资料得知，这是由于半开扫描的原理导致的，半开扫描由本机发送一个 SYN 包到目标机，目标机若返回一个 SYN-ACK 的包，本机再发送一个 RST 包，在双方达成握手协议前，就断开连接，这就意味着双方并没有真正意义上建立起连接，而全开放 TCP 扫描则是在双方之间建立起了 TCP 链接，对于每一个端口，都要尝试三次握手。

## 【实验体会】

说实话到现在还不是很懂，为什么打开防火墙且选择阻止所有的时候，刚开始的 nmap -sP 指令依然可以得到和关闭防火墙时一样的结果，依然显示主机端口是开放的。我在网上查了一些资料，也不是很懂到底是什么。

这次实验通过网络扫描过程以及自己的学习和老师的讲解，了解了一些网络安全基础方面的知识，也认识到了电脑上防火墙的作用，能阻止部分传入攻击，倘若不打开防火墙，对于黑客们来说，可以很轻松的扫描主机的不安全的端口，进而发现漏洞而入侵主机，造成我们的损失。也体会到了全扫描是真的慢，等了四分钟，而 SYN 半扫描相比之下就很快了，而且效果无很大差异（在一些资料看到有一些端口用半扫描无法显示，但是我们的实验两个结果一致）。总之收获还是很多的。