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	2015 级电子政务	学号	15331191	姓名	廖颖泓
完成日期： 2017 年 11 月 27 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：Windows 10　　IP地址：172.18.184.194

目标机操作系统：Windows 10　　IP地址：172.18.184.153

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）

以下测试命令的目标机 IP 是 172.18.184.153。

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。 TCP 探测包。

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 172.18.184.153，首先确定测试机与目标机物理连接是连通的。

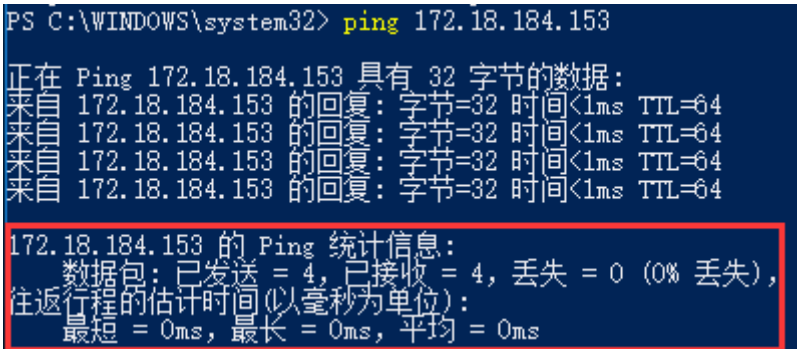
① 关闭目标机的防火墙，分别命令行窗口用 Windows 命令

ping 172.18.184.153

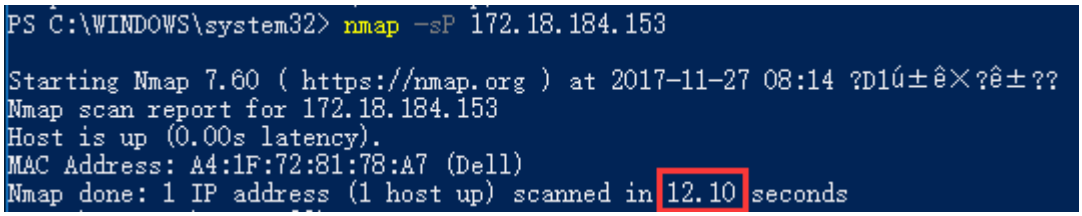
和 Nmap 命令

nmap -sP 172.18.184.153

进行测试，记录测试情况。简要说明测试差别。



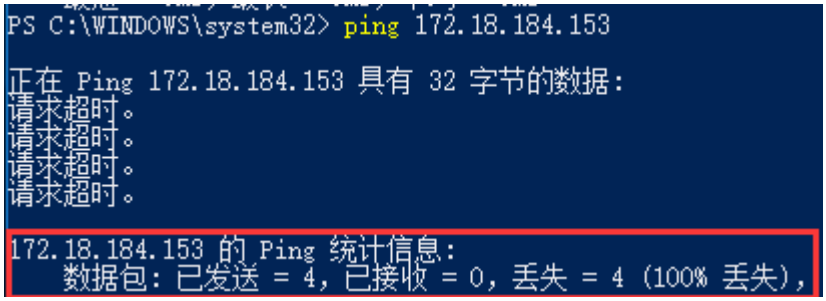
ping 172.18.184.153



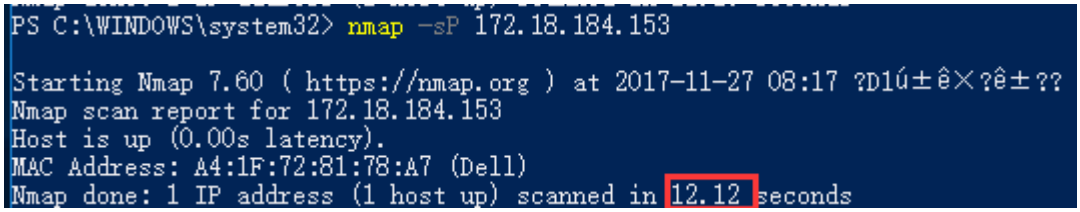
nmap -sP 172.18.184.153

关闭目标主机 Windows 防火墙后，ping 结果显示实验主机和目标主机之间有物理连接，目标主机对实验主机的数据包有响应，而且响应时间平均均小于 1ms；nmap 端口 ping 扫描结果显示目标主机处于运行状态，响应延迟时间是 12.10s。

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 172.18.184.153



nmap -sP 172.18.184.153

开启目标主机 Windows 防火墙后，ping 结果显示目标主机对实验主机的数据包响应超时；nmap 端口 ping 扫描结果显示目标主机处于运行状态，响应延迟时间是 12.12s。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

关闭目标主机 Windows 防火墙之后，ping 结果和 nmap 端口 ping 扫描结果都能表明物理上目标主机和实验主机是连通的，开启目标主机 Windows 防火墙之后就不能连通了，但是目标主机处于运行状态，说明开启防火墙会阻止目标主机和实验主机之间连通。

2．对目标主机进行 TCP 端口扫描

① 使用常规扫描方式

Nmap -sT 172.18.184.153

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。

关闭防火墙的情况下，所有的端口及开放情况如下：

```
PS C:\WINDOWS\system32> nmap -sT 172.18.184.153

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 08:04 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.184.153
Host is up (0.000012s latency).
Not shown: 994 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: A4:1F:72:81:78:A7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 56.62 seconds
```

Wireshark 抓包情况如下：

338	23.826365	172.18.184.194	172.18.184.153	TCP	58 51687 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
339	23.826458	172.18.184.194	172.18.184.153	TCP	58 51687 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
340	23.827125	172.18.184.153	172.18.184.194	TCP	60 143 → 51687 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
341	23.827140	172.18.184.194	172.18.184.153	TCP	58 51687 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
342	23.827882	172.18.184.153	172.18.184.194	TCP	60 3306 → 51687 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
343	23.827888	172.18.184.153	172.18.184.194	TCP	60 5900 → 51687 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
344	23.827908	172.18.184.194	172.18.184.153	TCP	58 51687 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
345	23.828637	172.18.184.153	172.18.184.194	TCP	60 1720 → 51687 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

② 使用 SYN 半扫描方式

Nmap -sS 172.18.184.153

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。

关闭防火墙情况下，所有的端口及开放情况如下：

```
PS C:\WINDOWS\system32> nmap -sS 172.18.184.153

Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-27 08:02 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.184.153
Host is up (0.0092s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: A4:1F:72:81:78:A7 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 12.88 seconds
```

Wireshark 抓包情况如下：

178	13.503479	172.18.184.194	172.18.184.153	TCP	66 63682 → 256 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
179	13.503870	172.18.184.194	172.18.184.153	TCP	66 63683 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
180	13.504184	172.18.184.153	172.18.184.194	TCP	60 256 → 63682 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
181	13.504221	172.18.184.194	172.18.184.153	TCP	66 63684 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
182	13.504528	172.18.184.194	172.18.184.153	TCP	66 63685 → 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
183	13.504846	172.18.184.194	172.18.184.153	TCP	66 63686 → 5900 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
184	13.504866	172.18.184.153	172.18.184.194	TCP	60 8080 → 63683 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
185	13.504881	172.18.184.153	172.18.184.194	TCP	60 3389 → 63684 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
186	13.505573	172.18.184.153	172.18.184.194	TCP	60 111 → 63685 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
187	13.505604	172.18.184.153	172.18.184.194	TCP	60 5900 → 63686 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

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。

扫描方式	时间	开放端口数
常规扫描	56.62	6
半扫描	12.88	6

nmap 端口 TCP 常规扫描和 nmap 端口 SYN 半扫描得到的所有的端口、开放状态以及服务情况是相同的，但不同的是常规扫描所花的时间远大于半扫描时间。

原因如下：

1. 当目标主机的目标端口开放时，常规扫描尝试建立一个完整的 TCP 连接，包括完整的三次握手；当目标端口未完全开放，半扫描会发送 SYN 包尝试建立连接。
2. 当目标主机的目标端口开放时，常规扫描会建立一个不完整的 TCP 连接，即没有三次握手中的第三个连接；当目标端口未完全开放时，会反馈一个 RST 包尝试结束。
3. 常规扫描在每次连接中会发送多个数据包，等待目标主机回复需要更多的时间，故所用时间和发送的数据包均远大于半扫描。

【实验体会】

这次实验通过使用扫描软件 nmap 中的一些简单的扫描命令来获取目标主机的端口信息和系统的一些信息，比如操作系统类型，支持哪些 IP 协议，开启哪些端口，并且对获取的信息进行进一步分析。扫描软件 nmap 可以扫描端口信息，分析各类主机信息，判别出主机的功能，因此一些不法分子利用扫描结果寻找目标主机的安全漏洞。当没被过滤的端口被扫描到的时候，这些端口会被黑客利用作为攻击的入口。因此在计算机的使用中，要注意禁止一些端口的开放，开启防火墙。使用计算机时要养成良好的习惯，不要轻易将一些信息共享在公共网路上，避免黑客侵入。