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	周二 3-4 节	学号	15331416	姓名	赵寒旭
完成日期： 2017 年 12 月 2 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：windows10 IP地址：172.18.136.220

目标机操作系统：windows10 IP地址：172.18.139.60

网络环境：校园网（以太网）。

【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。

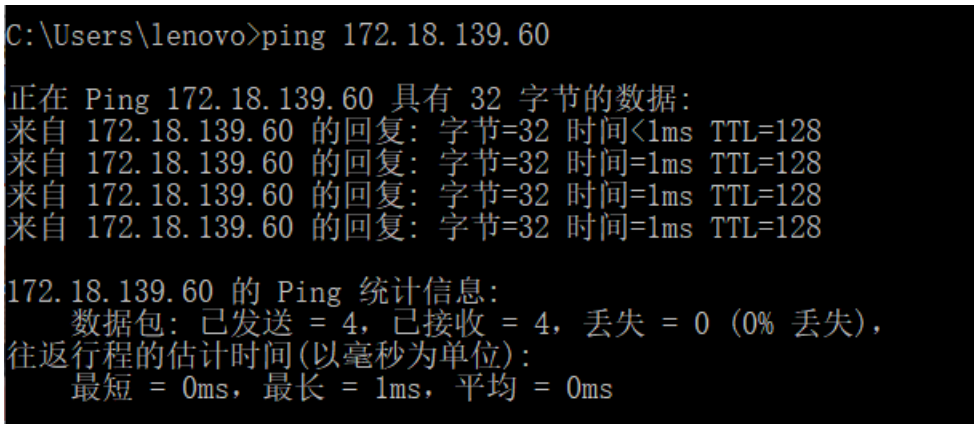
1．主机发现：进行连通性监测，判断目标主机。

以下测试命令目标机 IP 是 172.18.139.60。

本地目标 IP 地址为 172.18.139.60，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 172.18.139.60



和 Nmap 命令

nmap -sP 172.18.139.60

```
C:\Users\lenovo>nmap -sP 172.18.139.60

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-02 11:13 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.139.60
Host is up (0.0010s latency).
MAC Address: D8:CB:8A:7D:AF:07 (Micro-star Intl)
Nmap done: 1 IP address (1 host up) scanned in 7.83 seconds
```

nmap 命令运行时，wireshark 抓包结果：

ip.dst == 172.18.139.60

No.	Time	Source	Destination	Protocol
1138	23.046678	172.18.136.220	172.18.139.60	TCP
1139	23.046704	172.18.136.220	172.18.139.60	TCP
1141	23.047457	172.18.136.220	172.18.139.60	TCP
1142	23.047489	172.18.136.220	172.18.139.60	TCP
1143	23.047669	172.18.136.220	172.18.139.60	TCP
1144	23.047692	172.18.136.220	172.18.139.60	TCP
1145	23.047801	172.18.136.220	172.18.139.60	HTTP/X…
1146	23.047821	172.18.136.220	172.18.139.60	TCP
1153	23.079659	172.18.136.220	172.18.139.60	TCP
1154	23.079701	172.18.136.220	172.18.139.60	TCP
1157	23.092376	172.18.136.220	172.18.139.60	TCP
1158	23.092409	172.18.136.220	172.18.139.60	TCP
1160	23.093704	172.18.136.220	172.18.139.60	TCP
1161	23.093744	172.18.136.220	172.18.139.60	TCP
1183	23.137703	172.18.136.220	172.18.139.60	TCP

Nmap 采用 TCP 探测包。

进行测试，记录测试情况。简要说明测试差别。

测试差别：

nmap -sP 命令告诉 Nmap 仅仅进行 ping 扫描 (主机发现)，然后打印出对扫描做出响应的主机。没有进一步的测试 (如端口扫描或者操作系统探测)。 这比列表扫描更积极，常常用于和列表扫描相同的目的。它可以得到些许目标网络的信息而不被特别注意到。 对于攻击者来说，了解多少主机正在运行比列表扫描提供的一列 IP 和主机名往往更有价值。

系统管理员往往也很喜欢这个选项。 它可以很方便地得出网络上有多少机器正在运行或者监视服务器是否正常运行。常常有人称它为地毯式 ping，它比 ping 广播地址更可靠，因为许多主机对广播请求不响应。

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\lenovo>ping 172.18.139.60

正在 Ping 172.18.139.60 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

C:\Users\lenovo>_
```

```
C:\Users\lenovo>nmap -sP 172.18.139.60

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-02 11:17 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.139.60
Host is up (0.0010s latency).
MAC Address: D8:CB:8A:7D:AF:07 (Micro-star Intl)
Nmap done: 1 IP address (1 host up) scanned in 8.08 seconds

C:\Users\lenovo>_
```

nmap 命令运行时，wireshark 抓包结果：

ip.dst == 172.18.139.60

No.	Time	Source	Destination	Protocol	Ler
2764	34.267145	172.18.136.220	172.18.139.60	TCP	
2765	34.267176	172.18.136.220	172.18.139.60	TCP	
2770	34.268568	172.18.136.220	172.18.139.60	TCP	
2771	34.268605	172.18.136.220	172.18.139.60	TCP	
2774	34.268814	172.18.136.220	172.18.139.60	TCP	
2775	34.268854	172.18.136.220	172.18.139.60	TCP	
2776	34.269005	172.18.136.220	172.18.139.60	HTTP/X…	
2777	34.269028	172.18.136.220	172.18.139.60	TCP	
2806	34.318336	172.18.136.220	172.18.139.60	TCP	
2807	34.318391	172.18.136.220	172.18.139.60	TCP	
2809	34.328598	172.18.136.220	172.18.139.60	TCP	
2810	34.328632	172.18.136.220	172.18.139.60	TCP	
2812	34.329449	172.18.136.220	172.18.139.60	TCP	
2814	34.329484	172.18.136.220	172.18.139.60	TCP	

结果的不同之处：

ping 命令显示请求超时，无法 ping 通。

nmap 命令运行情况与之前并无不同。

下图为防火墙打开和防火墙关闭状态下对 namp 命令抓包结果的对比：

Destination	Protocol	Length	Info
172.18.139.60	TCP	66	59631 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.18.139.60	TCP	66	[TCP Out-Of-Order] 59631 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.18.139.60	TCP	54	59631 → 5357 [ACK] Seq=1 Ack=1 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Dup ACK 2770#1] 59631 → 5357 [ACK] Seq=1 Ack=1 Win=65536 Len=0
172.18.139.60	TCP	280	59631 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=226 [TCP segment of a reassembled PDU]
172.18.139.60	TCP	280	[TCP Retransmission] 59631 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=226
172.18.139.60	HTTP/X…	787	POST /07bb0d67-080f-4837-b22f-ce4350f3017d/ HTTP/1.1
172.18.139.60	TCP	787	[TCP Retransmission] 59631 → 5357 [PSH, ACK] Seq=227 Ack=1 Win=65536 Len=733
172.18.139.60	TCP	54	59631 → 5357 [ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Dup ACK 2806#1] 59631 → 5357 [ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	59631 → 5357 [FIN, ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Out-Of-Order] 59631 → 5357 [FIN, ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	59631 → 5357 [ACK] Seq=961 Ack=2353 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Dup ACK 2812#1] 59631 → 5357 [ACK] Seq=961 Ack=2353 Win=65536 Len=0

计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

Destination	Protocol	Length	Info
172.18.139.60	TCP	66	60240 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.18.139.60	TCP	66	[TCP Out-Of-Order] 60240 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
172.18.139.60	TCP	54	60240 → 5357 [ACK] Seq=1 Ack=1 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Dup ACK 1793#1] 60240 → 5357 [ACK] Seq=1 Ack=1 Win=65536 Len=0
172.18.139.60	TCP	280	60240 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=226 [TCP segment of a reassembled PDU]
172.18.139.60	TCP	280	[TCP Retransmission] 60240 → 5357 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=226
172.18.139.60	HTTP/X…	787	POST /07bb0d67-080f-4837-b22f-ce4350f3017d/ HTTP/1.1
172.18.139.60	TCP	787	[TCP Retransmission] 60240 → 5357 [PSH, ACK] Seq=227 Ack=1 Win=65536 Len=733
172.18.139.60	TCP	54	60240 → 5357 [ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	[TCP Dup ACK 1812#1] 60240 → 5357 [ACK] Seq=960 Ack=2352 Win=65536 Len=0
172.18.139.60	TCP	54	60240 → 5357 [FIN, ACK] Seq=960 Ack=2352 Win=65536 Len=0

结果不同的原因：

防火墙打开之后无法 ping 通，原因是防火墙捕获并丢弃探测包或者响应包时，主机就不能被探测到。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

```
C:\Windows\system32>ping -a 172.18.139.60

正在 Ping DESKTOP-A4U1R93 [172.18.139.60] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

ping 命令添加参数-a，将地址解析为主机名，可以正常显示，但是请求超时，测试结果不联通原因是目标主机开启了防火墙，捕获并丢弃探测包或者响应包，使数据包不能得到正确的接收和响应。

2．对目标主机进行 TCP 端口扫描（以下命令均在防火墙关闭时运行）

以下测试命令目标机 IP 是 172.18.136.68

① 使用常规扫描方式

Nmap -sT 172.18.136.68

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 -sT 172.18.136.68

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-02 17:25 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.136.68
Host is up (1.0s latency).
Not shown: 920 closed ports, 70 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
6000/tcp  open  X11
8082/tcp  open  blackice-alerts
49152/tcp open  unknown
MAC Address: 68:F7:28:EF:B1:BA (Lcfc(hefei) Electronics Technology)

Nmap done: 1 IP address (1 host up) scanned in 521.63 seconds

C:\Windows\system32>
```

列出端口显示为 open（开放的），应用程序正在该端口接收 TCP 连接或者 UDP 报文。

② 使用 SYN 半扫描方式

Nmap －sS 172.18.136.68

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 172.18.136.68

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-02 17:25 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.136.68
Host is up (0.0058s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
6000/tcp  open  X11
8082/tcp  open  blackice-alerts
49152/tcp open  unknown
MAC Address: 68:F7:28:EF:B1:BA (Lcfc(hefei) Electronics Technology)

Nmap done: 1 IP address (1 host up) scanned in 8.62 seconds
```

列出端口显示为 open（开放的）

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。

扫描结果差异：

扫描方式	open 端口个数	filtered 端口个数	closed 端口个数
常规扫描	10	70	920
SYN 半扫描	10	0	990

扫描花费的时间：

SYN 半扫描方式时间（9.58s）远低于常规扫描方式（54.29s）。

TCP connect 方式使用系统网络 API connect 向目标主机的端口发起连接，如果无法连接，说明该端口关闭。该方式扫描速度比较慢，而且由于建立完整的 TCP 连接会在目标机上留下记录信息，不够隐蔽。（TCP connect 是 TCP SYN 无法使用才考虑选择的方式）

SYN 半扫描方式发送 SYN 到目标端口，如果收到 SYN/ACK 回复，那么判断端口是开放的；如果收到 RST 包，说明该端口是关闭的。如果没有收到回复，那么判断该端口被屏蔽（Filtered）。因为该方式仅发送 SYN 包对目标主机的特定端口，但不建立的完整的 TCP 连接，所以相对比较隐蔽，而且效率比较高，适用范围广。

SYN 扫描它执行得很快，在一个没有入侵防火墙的快速网络上，每秒钟可以扫描数千个 端口。SYN 扫描更加隐蔽，因为它从来不完成 TCP 连接，还可以明确可靠地区分 open(开放的)， closed(关闭的)，和 filtered(被过滤的) 状态

SYN 半扫描不打开一个完全的 TCP 连接。它发送一个 SYN 报文， 就像真的要打开一个连接，然后等待响应。 SYN/ACK 表示端口在监听 (开放)，而 RST (复位)表示没有监听者。如果数次重发后仍没响应， 该端口就被标记为被过滤。如果收到 ICMP 不可到达错误 (类型 3，代码 1，2，3，9，10，或者 13)，该端口也被标记为被过滤。

【实验体会】

本次实验初步了解了 nmap 的功能，主要任务是测试了主机发现和端口扫描的几个简单命令的运行，加深了对 nmap 机制的理解。

1. 主机发现理解

由于主机发现的需求各不相同，Nmap 提供了许多选项来定制需求。 主机发现有时候也叫做 ping 扫描，但它远远超越用世人皆知的 ping 工具发送简单的 ICMP 回声请求报文。（wireshark 在 ping 命令执行时捕捉到 icmp 包）用户完全可以通过使用列表扫描(-sL)或者 通过关闭 ping (-P0)跳过 ping 的步骤，也可以使用多个端口把 TCP SYN/ACK，UDP 和 ICMP 任意组合起来。这些探测的目的是获得响应以显示某个 IP 地址是否是活动的(正在被某主机或者网络设备使用)。 在许多网络上，在给定的时间，往往只有小部分的 IP 地址是活动的。

2. 端口扫描理解

nmap 功能是从一个高效的端口扫描器开始的，并且到目前为止端口扫描仍然是它的核心功能。nmap <target>这个简单的命令扫描主机<target>上的超过 1660 个 TCP 端口。许多传统的端口扫描器只列出所有端口是开放还是关闭的，Nmap 检测出的端口信息要详细得多。它把端口分成六个状态: open(开放的)，closed(关闭的)，filtered(被过滤的)，unfiltered(未被过滤的)，open|filtered(开放或者被过滤的)，或者

closed|filtered(关闭或者被过滤的)。

这些状态并非端口本身的性质，而是描述 Nmap 怎样看待它们。例如，对于同样的目标机器的 135/tcp 端口，从同网络扫描显示它是开放的，而跨网络作完全相同的扫描则可能显示它是 filtered(被过滤的)。

3. 关于防火墙

在打开防火墙时，ping 命令无法在源主机和目的主机直接传送数据包。

ping 程序的原理是首先发送一个 ICMP echo 类型的包到目标主机，如果目标主机返回一个 ICMP echo replay 包的话,那么就代表主机存活，然后根据时间差，以及 IP 报头的 TTL 把信息打印出来.在防火墙开启时我们使用 ping 命令的时候会发现这样的现象,比如 ping 返回的是 timeout，但是事实上目标主机却是存活的，这是因为防火墙把 ICMP echo 包给阻挡了。

本以为 nmap 在防火墙开启时也无法正常运行，发现 nmap －sP 实验中未受防火墙影响，wireshark 抓包显示 nmap 通过 TCP 检测包，可以通过防火墙。