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	软件工程	班级	4	学号	17343105	姓名	田皓
完成日期： 2019 年 月 12 日 20							

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：172.18.61.253

目标机操作系统：windows10 IP地址：172.18.63.254

网络环境：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。

1. 在 cmd 窗口 ping：

很普通的响应，连接正常。

```
C:\Users\TIFINITY>ping 172.18.63.254

正在 Ping 172.18.63.254 具有 32 字节的数据:
来自 172.18.63.254 的回复: 字节=32 时间<1ms TTL=255
来自 172.18.63.254 的回复: 字节=32 时间=1ms TTL=255
来自 172.18.63.254 的回复: 字节=32 时间=1ms TTL=255
来自 172.18.63.254 的回复: 字节=32 时间<1ms TTL=255

172.18.63.254 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\TIFINITY>
```

2. 使用 Nmap：

在 Nmap 上执行 nmap -sP 172.16.1.101.

用 ping 扫描判断主机是否存活，只有主机存活，nmap 才会继续扫描，一般最好不加，因为有的主机会禁止 ping。

只返回了 MAC 地址，没有端口信息 。

```
C:\Users\TIFINITY>nmap -sP 172.18.63.254
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 23:37 ?D1ú±ê×?ê±
Nmap scan report for 172.18.63.254
Host is up (0.0030s latency).
MAC Address: 38:22:D6:E7:2E:C9 (Hangzhou H3C Technologies, Limited)
Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

在 Nmap 上执行 nmap 172.16.1.101.

可以看到有了一些端口的信息，23 是 open 的，另外三个被防火墙屏蔽。

```
C:\Users\TIFINITY>nmap 172.18.63.254
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 23:36 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.63.254
Host is up (0.0019s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
23/tcp    open     telnet
50300/tcp filtered unknown
50389/tcp filtered unknown
50500/tcp filtered unknown
MAC Address: 38:22:D6:E7:2E:C9 (Hangzhou H3C Technologies, Limited)

Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

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。

Cmd 中还是可以 ping 通。

在 Nmap 上执行 nmap -sP 172.16.1.101.

没有端口信息。

```
C:\Users\TIFINITY>nmap -sP 172.18.63.254
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 23:37 ?D1ú±ê×?ê±
Nmap scan report for 172.18.63.254
Host is up (0.0030s latency).
MAC Address: 38:22:D6:E7:2E:C9 (Hangzhou H3C Technologies, Limited)
Nmap done: 1 IP address (1 host up) scanned in 2.11 seconds
```

在 Nmap 上执行 nmap 172.16.1.101.

部分端口被防火墙屏蔽。

```
C:\Users\TIFINITY>nmap 172.18.63.254
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 23:36 ?D1ú±ê×?ê±??
Nmap scan report for 172.18.63.254
Host is up (0.0019s latency).
Not shown: 996 closed ports
PORT      STATE    SERVICE
23/tcp    open     telnet
50300/tcp filtered unknown
50389/tcp filtered unknown
50500/tcp filtered unknown
MAC Address: 38:22:D6:E7:2E:C9 (Hangzhou H3C Technologies, Limited)

Nmap done: 1 IP address (1 host up) scanned in 7.76 seconds
```

使用 wireshark 抓包：

691	3.671688	172.18.63.254	172.18.61.253	TCP	60 2222 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1558	4.891686	172.18.63.254	172.18.61.253	TCP	60 2251 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3536	7.281991	172.18.63.254	172.18.61.253	TCP	60 2260 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
676	3.668288	172.18.63.254	172.18.61.253	TCP	60 2288 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2025	4.962524	172.18.63.254	172.18.61.253	TCP	60 22939 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
145	3.583005	172.18.63.254	172.18.61.253	TCP	60 23 → 51464 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
3531	7.280871	172.18.63.254	172.18.61.253	TCP	60 2301 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
727	3.679953	172.18.63.254	172.18.61.253	TCP	60 2323 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2188	4.987120	172.18.63.254	172.18.61.253	TCP	60 23502 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2909	6.180912	172.18.63.254	172.18.61.253	TCP	60 2366 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
912	3.715229	172.18.63.254	172.18.61.253	TCP	60 2381 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
480	3.631853	172.18.63.254	172.18.61.253	TCP	60 2382 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2804	6.164977	172.18.63.254	172.18.61.253	TCP	60 2383 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1524	4.883973	172.18.63.254	172.18.61.253	TCP	60 2393 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
731	3.680849	172.18.63.254	172.18.61.253	TCP	60 2394 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2677	6.144219	172.18.63.254	172.18.61.253	TCP	60 2399 → 51466 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1864	4.938095	172.18.63.254	172.18.61.253	TCP	60 24 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1393	4.865675	172.18.63.254	172.18.61.253	TCP	60 2401 → 51465 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
164	3.587321	172.18.63.254	172.18.61.253	TCP	60 24444 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3323	7.245956	172.18.63.254	172.18.61.253	TCP	60 24800 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
964	3.727060	172.18.63.254	172.18.61.253	TCP	60 2492 → 51464 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```
Flags: 0x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  > .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A··S·]
```

23 号端口收到 ACK/SYN 回复，所以 Nmap 判断其开放；

```
Flags: 0x014 (RST, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
  > .... .... .1.. = Reset: Set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
```

其他端口仅有 ACK 表示收到了发过去的包但没有 SYN，所以 Nmap 判断其被屏蔽。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

端口扫描是 Nmap 最基本最核心的功能，用于确定目标主机的 TCP/UDP 端口的开放情况。Nmap 通过探测将端口划分为 6 个状态：

open：端口是开放的。

closed：端口是关闭的。

filtered：端口被防火墙 IDS/IPS 屏蔽，无法确定其状态。

unfiltered：端口没有被屏蔽，但是否开放需要进一步确定。

open|filtered：端口是开放的或被屏蔽，Nmap 不能识别。

closed|filtered ：端口是关闭的或被屏蔽，Nmap 不能识别。

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。

```
Host is up (1.0s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 205.32 seconds
```

扫描用时 205 秒。

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。

```
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 2.30 seconds
```

只需要 2 秒。

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。

TCP SYN 扫描(-sS)

这是 Nmap 默认的扫描方式，通常被称作半开放扫描。该方式发送 SYN 到目标端口，如果收到 SYN/ACK 回复，那么可以判断端口是开放的；如果收到 RST 包，说明该端口是关闭的。如果没有收到回复，那么可以判断该端口被屏蔽了。因为该方式仅发送 SYN 包对目标主机的特定端口，但不建立完整的 TCP 连接，所以相对比较隐蔽，而且效率比较高，适用范围广。

TCP connent 扫描(-sT)

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 连接会在目标主机上留下记录信息，不够隐蔽。所以，TCP connect 是 TCP SYN 无法使用才考虑使用的方式。

【实验体会】

本次实验内容不多，过程也比较顺利，使用了 Nmap 进行端口扫描，了解了端口扫描的不同方式以及各种方式的特点，也顺便复习了一下 wireshark 抓包以及 TCP 包的一些字段代表什么意思。总体感觉有点像以前做计网实验，希望以后继续努力。