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	软件工程教务一班	学号	17343094	姓名	彭湃
完成日期： 2019 年 12 月 24 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：172.19.58.50

目标机操作系统：windows10 IP地址：222.200.172.78

网络环境：无线局域网(SYSU-SECURE)

【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】

1. 主机发现：进行连通性监测，判断目标主机：

① **我们首先在关闭目标主机防火墙的条件下进行试验：**

- 首先我们使用 ping 命令进行测试：指令为：ping 222.200.172.78

```
C:\Users\lenovo>ping 222.200.172.78

正在 Ping 222.200.172.78 具有 32 字节的数据:
来自 222.200.172.78 的回复: 字节=32 时间=10ms TTL=60
来自 222.200.172.78 的回复: 字节=32 时间=2ms TTL=60
来自 222.200.172.78 的回复: 字节=32 时间=3ms TTL=60
来自 222.200.172.78 的回复: 字节=32 时间=3ms TTL=60

222.200.172.78 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 = 2ms，最长 = 10ms，平均 = 4ms

C:\Users\lenovo>
```

可以看得到在关闭防火墙的状态下，我们是能够 ping 通目标主机的，0%的丢包率，即连通性没有任何问题。

➢ 然后我们使用 Nmap 命令进行测试：指令为：Nmap -sP 222.200.172.78

```
C:\Users\lenovo>nmap -sP 222.200.172.78
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 20:59 ?D1ú±ê×?ê±??
Nmap scan report for 222.200.172.78
Host is up (0.010s latency).
Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds

C:\Users\lenovo>
```

和上面的差不多，Nmap 中的 ping 指令(即 sP)只是用来对目标主机进行 ping 测试，看其是否存活在网络中。这里面显示扫描这个 ip 地址花了 12.23 秒，同时这个主机是联通的。

② **然后我们在开启目标主机防火墙的条件下进行试验：**

这……肯定是 ping 不通的，真当防火墙是摆设？

➢ 同上，我们先用 ping 指令进行连通性测试，指令和上面的第一步一样：

```
C:\Users\lenovo>ping 222.200.172.78

正在 Ping 222.200.172.78 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

果然……请求超时，丢包率 100%。

➢ 然后和上面一样，我们再在 Nmap 里面用 ping 指令进行测试，指令同上面第二步：

```
C:\Users\lenovo>nmap -sP 222.200.172.78
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 21:02 ?D1ú±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 9.69 seconds
```

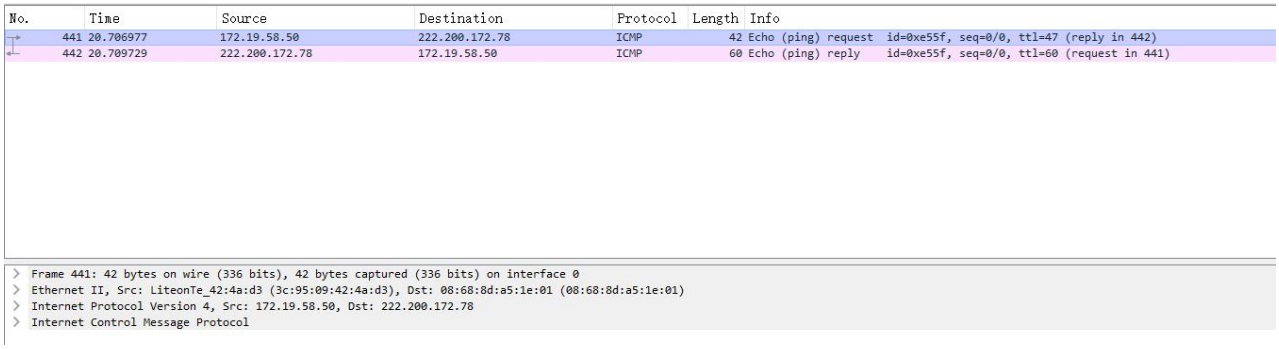
在 9.69s 内完成了扫描，显示这台目标主机挂掉了。事实上当然不是……解决这个问题的方法是我们使用 TCP SYN Ping 绕过防火墙。

③ **测试结果不连通，但实际上是物理联通的，什么原因？**

我们在 ping 的过程中使用 wireshark 监测流量，不难可以看出 ping 的运作原理其实就是向目标主机传出一个 ICMP echo@要求数据包，并等待接收 echo 回应数据包，以此来检测目标主机是否存活。

No.	Time	Source	Destination	Protocol	Length	Info
439	16.145913	172.19.58.50	222.200.172.78	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 441)
441	16.148606	222.200.172.78	172.19.58.50	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=60 (request in 439)
472	17.151505	172.19.58.50	222.200.172.78	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 473)
473	17.163927	222.200.172.78	172.19.58.50	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=60 (request in 472)
505	18.156503	172.19.58.50	222.200.172.78	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 507)
507	18.159594	222.200.172.78	172.19.58.50	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=60 (request in 505)
526	19.162728	172.19.58.50	222.200.172.78	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 527)
527	19.165437	222.200.172.78	172.19.58.50	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=60 (request in 526)

Cmd 下 ping 时的 wireshark 流量分析



Nmap 下 ping 时的 wireshark 流量分析

而 windows 防火墙的一个主要功能就是过滤 ping 发出的 ICMP 数据包,防止被大流量攻击使系统瘫痪，所以就会造成了即使是物理联通的，但是我们使用 ping 相关指令的时候测试结果显示不连通。

2. 对目标主机进行 TCP 端口扫描。

① 使用常规扫描方式

我们直接使用常规的 Nmap -sT 进行主机的 TCP 端口扫描，指令为：Nmap -sT 222.200.172.78

```
C:\Users\lenovo>nmap -sT 222.200.172.78
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 21:05 ?D1ú±ê×?ê±??
Nmap scan report for 222.200.172.78
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 57.30 seconds
```

Nmap 花费 57.30s 完成整个目标主机的端口扫描，首先可以确定的是主机是可以联通的，有 999 个 filtered 端口没有展示出来，filtered 端口也就是被过滤的端口，因为包过滤阻止探测报文到达端口，所以 Nmap 无法确定端口是否开放，所以我们无法获取任何信息。

唯一扫描到的一个开放端口是：5537 端口，它提供的是 wsdapi 服务。

② 使用 SYN 半扫描方式

使用 Nmap -sS 对目标主机进行 SYN 半扫描，指令为：Nmap -sS 222.200.172.78

```
C:\Users\lenovo>nmap -sS 222.200.172.78
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-23 21:06 ?D1ú±ê×?ê±??
Nmap scan report for 222.200.172.78
Host is up (0.015s latency).
Not shown: 992 closed ports
PORT      STATE    SERVICE
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1521/tcp  filtered oracle
3306/tcp  filtered mysql
5000/tcp  filtered upnp
5357/tcp  open     wsdapi
50000/tcp filtered ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 16.75 seconds
```

这次扫描花费了 16.75s，显示主机是可以联通的，延迟为 0.15s，这次显示：有 992 个端口是关闭的，直接就没有显示了，有一个端口是开放的，这个端口是：5537/tcp 端口，它的服务是 wsapi，另外列举出了七个被过滤的端口，分别是：

端口	服务
135/tcp	msrpc
139/tcp	netbios-ssn
445/tcp	microsoft-ds
1521/tcp	oracle
3306/tcp	mysql
5000/tcp	upnp
50000/tcp	ibm-db2

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。

- 从扫描结果的角度看：

  采用常规的扫描方式，直接将所有无法确定的 999 个端口认定为被过滤的 filtered 端口，同时不展示具体的端口和服务；而采用 SYN 半扫描的方式，则可以确定这 999 个端口中有 992 个是关闭的，另外七个过滤端口和一个开放端口显示了详细的端口信息；可见采用第二种方式，端口扫描出的信息更详细更具体。

- 从扫描花费时间的角度看：

  采用常规的扫描方式，花费了 57.30 秒才扫描完目标主机，而采用 SYN 半扫描的方式，则花费 16.75 秒就可以扫描完，很明显第二种的效率要高很多。

解释：

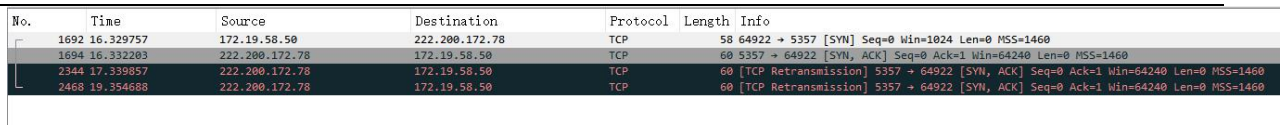
扫描过程都是我们自己的主机向目标主机的一个端口发送请求连接的 SYN 包

- 如果目标主机端返回 SYN/ACK，表明端口开放；区别在于我们的主机在收到 SYN/ACK 后，常规的扫描方式会发送 ACK 应答完成三次握手，而 SYN 半扫描则是发送 RST 包断开连接，这样，三次握手就没有完成，无法建立正常的 TCP 连接，因此，这次扫描就不会被记录到系统日志中。
- 如果目标主机返回 RST/ACK，则显示端口是关闭状态。

所以采用 SYN 半扫描所需要的时间比较短，效率更高，同时隐蔽性也会强得多。

3352	39.881451	172.19.58.50	222.200.172.78	TCP	66 54211 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3355	39.887735	222.200.172.78	172.19.58.50	TCP	66 5357 → 54211 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3356	39.887804	172.19.58.50	222.200.172.78	TCP	54 54211 → 5357 [ACK] Seq=1 Ack=1 Win=131328 Len=0
3357	39.887928	172.19.58.50	222.200.172.78	TCP	54 54211 → 5357 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3499	41.196335	172.19.58.50	222.200.172.78	TCP	66 54277 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3501	41.199067	222.200.172.78	172.19.58.50	TCP	66 5357 → 54277 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3502	41.199173	172.19.58.50	222.200.172.78	TCP	54 54277 → 5357 [ACK] Seq=1 Ack=1 Win=131328 Len=0
3504	41.208856	172.19.58.50	222.200.172.78	TCP	54 54277 → 5357 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3681	42.512528	172.19.58.50	222.200.172.78	TCP	66 54345 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3682	42.515245	222.200.172.78	172.19.58.50	TCP	66 5357 → 54345 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
3683	42.515352	172.19.58.50	222.200.172.78	TCP	54 54345 → 5357 [ACK] Seq=1 Ack=1 Win=131328 Len=0
3684	42.515408	172.19.58.50	222.200.172.78	TCP	54 54345 → 5357 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
3859	43.827924	172.19.58.50	222.200.172.78	TCP	66 54411 → 5357 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3860	43.833894	222.200.172.78	172.19.58.50	TCP	66 5357 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

常规的 connect 扫描 wireshark 解析



No.	Time	Source	Destination	Protocol	Length	Info
1692	16.329757	172.19.58.50	222.200.172.78	TCP	58	64922 → 5357 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1694	16.332203	222.200.172.78	172.19.58.50	TCP	60	5357 → 64922 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2344	17.339857	222.200.172.78	172.19.58.50	TCP	60	[TCP Retransmission] 5357 → 64922 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2468	19.354688	222.200.172.78	172.19.58.50	TCP	60	[TCP Retransmission] 5357 → 64922 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

SYN 半扫描 wireshark 解析

【实验体会】

感觉又回到了上学期计网实验的感觉，总的来说，这次的实验并不难，最重要的是熟悉了 Nmap 这个开源的检测扫描工具的使用，这是之前没有接触过的。同时对电脑防火墙下外机不能 ping 通主机，传统 coneect 扫描和 SYN 半扫描的区别等进行了进一步的了解，以及熟悉了 Nmap 常用的一些指令。总的来说，收获还是比较大的。

但是也反映出了很大的问题，Nmap 作为信息安全的一个基础工具，然而已经大三上了，要不是这次作业，我竟然听都没听过，想想让我感到有些汗颜，也希望自己以后能够在日常的课程学习中不要拘泥于课本上的知识，而应该多做多了解，计算机学科本身就是一个应用的学科，好的工具的使用能够大大提高我们的效率。

提前祝老师和 TA 师兄圣诞快乐！