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	软工五班	学号	17343153	姓名	张淇
完成日期： 2019 年 12 月 16 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：Win10 IP地址：192.168.199.155

目标机操作系统：Win10 IP地址：192.168.199.147

网络环境：无线局域网

【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】

1. 主机发现：进行连通性监测，判断目标主机。

实验主机 cmd 中输入 ipconfig 得到的 WLAN 部分：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : lan
   IPv6 地址 . . . . . : 2001:250:3002:4470:49c6:126d:37b1:34e
   临时 IPv6 地址. . . . . : 2001:250:3002:4470:503f:334f:a96a:d927
   本地链接 IPv6 地址. . . . . : fe80::49c6:126d:37b1:34e%17
   IPv4 地址 . . . . . : 192.168.199.155
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . : fe80::d6ee:7ff:fe50:5e70%17
                       192.168.199.1
```

目标机 cmd 中输入 ipconfig 得到的 WLAN 部分：

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : lan
   IPv6 地址 . . . . . : 2001:250:3002:4470:21f7:e194:9f9d:d5b7
   临时 IPv6 地址. . . . . : 2001:250:3002:4470:e89e:2b51:d66b:6360
   本地链接 IPv6 地址. . . . . : fe80::21f7:e194:9f9d:d5b7%13
   IPv4 地址 . . . . . : 192.168.199.147
   子网掩码 . . . . . : 255.255.255.0
   默认网关. . . . . : fe80::d6ee:7ff:fe50:5e70%13
                       192.168.199.1
```

所以实验主机与目标机处于“物理联通”的状态。

① 关闭目标机的防火墙

- 使用实验主机 Ping 目标机：

```
C:\Users\54603>ping 192.168.199.147

正在 Ping 192.168.199.147 具有 32 字节的数据:
来自 192.168.199.147 的回复: 字节=32 时间=45ms TTL=64
来自 192.168.199.147 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.199.147 的回复: 字节=32 时间=36ms TTL=64
来自 192.168.199.147 的回复: 字节=32 时间=45ms TTL=64

192.168.199.147 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 = 3ms, 最长 = 45ms, 平均 = 32ms
```

与此同时，使用 Wireshark 进行抓包：

8	0.972001	192.168.199.155	192.168.199.147	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 9)
54	1.983775	192.168.199.155	192.168.199.147	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 55)
57	2.999353	192.168.199.155	192.168.199.147	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 58)
62	4.030503	192.168.199.155	192.168.199.147	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 63)
2	0.022397	117.18.237.29	192.168.199.155	TCP	54	80 → 31022 [FIN, ACK] Seq=1 Ack=2 Win=288 Len=0
5	0.445086	23.198.124.11	192.168.199.155	TLSv1.2	584	Application Data
9	1.001201	192.168.199.147	192.168.199.155	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=64 (request in 8)
55	1.990025	192.168.199.147	192.168.199.155	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=64 (request in 54)
58	3.005101	192.168.199.147	192.168.199.155	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=64 (request in 57)
60	3.354519	183.232.127.124	192.168.199.155	OICQ	89	OICQ Protocol
63	4.036038	192.168.199.147	192.168.199.155	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=64 (request in 62)

可以看到 Ping 操作采用的探测包类型为 ICMP。

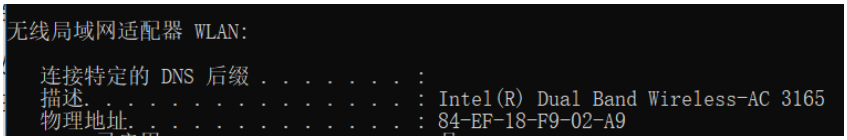
- 使用实验主机执行 Nmap 命令 nmap -sP 192.168.199.147

多次测试均无法用 Wireshark 捕捉到 nmap 采用的探测包。

- 测试差别

nmap -sP 首先会进行判断对方 IP 是否“存活”，以及会返回对方 IP 的 Mac 地址。

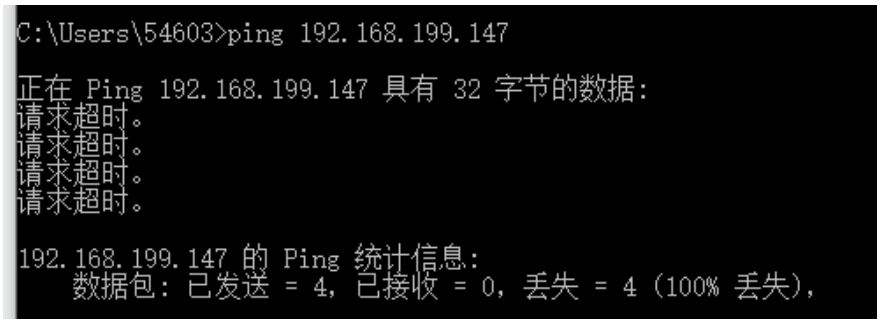
我在目标机上执行 ipconfig /all 得到的网卡地址：



可以发现，与 nmap -sP 得到的结果一致。

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。

- 使用实验主机 Ping 目标机：



- 使用实验主机执行 Nmap 命令 nmap -sP 192.168.199.147

- 不同之处及原因：

实验主机无法 Ping 通目标机，因为目标机的防火墙已经开启，防火墙为了防止 DOS 攻击而禁止了外部 IP 对本机进行 Ping。

③ 测试结果不连通，但实际上是物理连通的，什么原因？

见上文解析。

2. 对目标主机进行 TCP 端口扫描

① 使用常规扫描方式 Nmap -sT 192.168.199.147

- 目标机防火墙关闭时：

Nmap Scan Report - Scanned at Mon Dec 16 13:58:08 2019

Scan Summary | DESKTOP-1G1VAAU.lan (192.168.199.147)

Scan Summary

Nmap 7.80 was initiated at Mon Dec 16 13:58:08 2019 with these arguments:
Nmap -sT 192.168.199.147

Verbosity: 0; Debug level 0

192.168.199.147 / DESKTOP-1G1VAAU.lan

Address

- 192.168.199.147 - (ipv4)
- 84:EF:18:F9:02:A9 - Intel Corporate (mac)

Hostnames

- DESKTOP-1G1VAAU.lan (PTR)

Ports

The 994 ports scanned but not shown below are in state: **filtered**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
443	tcp	open	https	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	iss-realsecure	syn-ack			
912	tcp	open	apex-mesh	syn-ack			

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

- 目标机防火墙打开时：

Nmap Scan Report - Scanned at Mon Dec 16 13:45:04 2019

Scan Summary | DESKTOP-1G1VAAU.lan (192.168.199.147)

Scan Summary

Nmap 7.80 was initiated at Mon Dec 16 13:45:04 2019 with these arguments:
Nmap -sT 192.168.199.147

Verbosity: 0; Debug level 0

192.168.199.147 / DESKTOP-1G1VAAU.lan

Address

- 192.168.199.147 - (ipv4)
- 84:EF:18:F9:02:A9 - Intel Corporate (mac)

Hostnames

- DESKTOP-1G1VAAU.lan (PTR)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

可以看到，当目标机防火墙打开时，扫描目标机的端口得到的结果全是“filtered”（过滤的），表示端口没有对探测做出响应；同时告诉我们探针可能被一些过滤器（防火墙）终止了。而当防火墙关闭时，我们可以检测到一些目标端口是处于“Open”(开放的)。

② 使用 SYN 半扫描方式 Nmap -sS 192.168.199.147

- 目标机防火墙关闭时：

Nmap Scan Report - Scanned at Mon Dec 16 13:53:33 2019

Scan Summary | DESKTOP-1G1VAAU.lan (192.168.199.147)

Scan Summary

Nmap 7.80 was initiated at Mon Dec 16 13:53:33 2019 with these arguments:
Nmap -sS 192.168.199.147

Verbosity: 0; Debug level 0

192.168.199.147 / DESKTOP-1G1VAAU.lan

Address

- 192.168.199.147 - (ipv4)
- 84:EF:18:F9:02:A9 - Intel Corporate (mac)

Hostnames

- DESKTOP-1G1VAAU.lan (PTR)

Ports

The 994 ports scanned but not shown below are in state: **closed**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
135	tcp	open	msrpc	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
443	tcp	open	https	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
902	tcp	open	iss-realsecure	syn-ack			
912	tcp	open	apex-mesh	syn-ack			

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

- 目标机防火墙开放时：

Nmap Scan Report - Scanned at Mon Dec 16 13:51:43 2019

Scan Summary | DESKTOP-1G1VAAU.lan (192.168.199.147)

Scan Summary

Nmap 7.80 was initiated at Mon Dec 16 13:51:43 2019 with these arguments:
Nmap -sS 192.168.199.147

Verbosity: 0; Debug level 0

192.168.199.147 / DESKTOP-1G1VAAU.lan

Address

- 192.168.199.147 - (ipv4)
- 84:EF:18:F9:02:A9 - Intel Corporate (mac)

Hostnames

- DESKTOP-1G1VAAU.lan (PTR)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

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。

从面可以看到使用常规扫描方式（-sT）时所耗费的时间是多余半扫描方式（-sY）的，这是因为常规扫描需要建立完整的 TCP 连接（三次握手），并且这种方式会在目标主机的日志中记录大批连接请求和错误信息，所以需要耗费更多的时间。

【实验体会】

本次实验让我了解到了一种新的网络工具 Nmap 的基本功能，在网上进行查阅相关资料的时候发现这个工具能够做到的事情“超乎我的想象”。如果能够恰到好处地使用地话能够为我们提供很大的方便，但是反过来如果被居心叵测的人使用的话那么后果可能…但是无论如何，技术本身是无罪的。