

警示

1. 实验报告如有雷同，雷同各方当次实验成绩均以 0 分计。
2. 当次小组成员成绩只计学号、姓名登录在下表中的。
3. 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。
4. 实验报告文件以 PDF 格式提交。

院系	数据科学与计算机实验		班 级	14M3, 14C1		组长	白冰
学号	14353355	14353002					
学生	杨金华	白冰					
实验分工							
杨金华	合作完成实验，共同编写实验报告			白冰	合作完成实验，共同编写实验报告		

实验 5 防火墙扫描实验

【实验目的】

通过 Nmap 强有力的防火墙扫描命令，判断防火墙存在性。

【实验原理】

Nmap 对防火墙的探测包括发送 ACK 包、SYN 包、TCP 包等手段，根据回应包分析防火墙的情况，防火墙有四种类型的响应：

- (1) Open port (防火墙允许少数端口打开)
- (2) Closed Port (由于防火墙的缘故，大部分的端口被关闭)
- (3) Filtered (Nmap 不确定端口是否打开或者关闭)
- (4) Unfiltered (Nmap 能够访问这个端口，但是不清楚这个端口打开的状态)

根据不同的回应信息，可给出大致的判断。

【实验环境】

操作系统：Windows7

IP 地址：扫描机 IP：192.168.1.10，目标机：192.168.1.20 （按实际情况更改）

防火墙：Windows7 自带防火墙

【实验过程】

实验一、TCP ACK Scan (-sA)

- (1) 关闭目标机防火墙，命令：netsh firewall set opmode=disable
- (2) 在扫描机上执行 nmap -sA 192.168.1.20 记录扫描结果(探测该主机是否使用了包过滤器或防火墙)



- (3) 开启目标机防火墙 netsh firewall reset
- (4) 在扫描机上执行 nmap -sA 192.168.1.20 记录扫描结果
- (5) 将前后两次扫描结果填入表 2-18:

表 2-18 ACK 扫描结果

关闭目标机防火墙后	开启目标机防火墙后
nmap -sA 192.168.1.20	nmap -sA 192.168.1.20
<pre>nmap -sA 172.16.11.3 Starting Nmap 6.00 (http://nmap.org) at 2017-04-19 20:03 中国标准时间 Nmap scan report for 172.16.11.3 Host is up (0.0050s latency). All 1000 scanned ports on 172.16.11.3 are unfiltered MAC Address: <u>44:33:4C:0E</u>:C8:58 (Unknown) Nmap done: 1 IP address (1 host up) scanned in 1.95 seconds</pre>	<pre>nmap -sA 172.16.11.3 Starting Nmap 6.00 (http://nmap.org) at 2017-04-19 20:04 中国标准时间 Nmap scan report for 172.16.11.3 Host is up (0.0010s latency). All 1000 scanned ports on 172.16.11.3 are filtered MAC Address: <u>44:33:4C:0E</u>:C8:58 (Unknown) Nmap done: 1 IP address (1 host up) scanned in 21.55 seconds</pre>

- (6) 用 Wireshark 抓取数据包，Nmap 发出了什么探测包？

发出的是 ACK 探测包。截图如下：

365	37.7754780	172.16.26.3	172.16.255.255	NBNS	92	Name query NB WPAD<00>
366	37.7828350	172.16.12.3	172.16.11.3	TCP	54	44898 > 801 [ACK] Seq=1 Ack=1 win=1024 Len=0
367	37.7829160	172.16.12.3	172.16.11.3	TCP	54	44898 > xmpp-client [ACK] Seq=1 Ack=1 win=1024 Len=0
368	37.7877980	172.16.12.3	172.16.11.3	TCP	54	44898 > 16113 [ACK] Seq=1 Ack=1 win=1024 Len=0
369	37.7878720	172.16.12.3	172.16.11.3	TCP	54	44898 > 50389 [ACK] Seq=1 Ack=1 win=1024 Len=0
370	37.7897510	172.16.12.3	172.16.11.3	TCP	54	44898 > sixtrak [ACK] Seq=1 Ack=1 win=1024 Len=0
371	37.7897970	172.16.12.3	172.16.11.3	TCP	54	44898 > 3325 [ACK] Seq=1 Ack=1 win=1024 Len=0
372	37.7937970	172.16.12.3	172.16.11.3	TCP	54	44898 > 3367 [ACK] Seq=1 Ack=1 win=1024 Len=0
373	37.8037920	172.16.12.3	172.16.11.3	TCP	54	44898 > isbconferencel [ACK] Seq=1 Ack=1 win=1024 Len=0
374	37.8038630	172.16.12.3	172.16.11.3	TCP	54	44898 > filenet-cm [ACK] Seq=1 Ack=1 win=1024 Len=0
375	37.8077900	172.16.12.3	172.16.11.3	TCP	54	44898 > 32 [ACK] Seq=1 Ack=1 win=1024 Len=0
376	37.8838170	172.16.12.3	172.16.11.3	TCP	54	44897 > 4 [ACK] Seq=1 Ack=1 win=1024 Len=0
377	37.8838920	172.16.12.3	172.16.11.3	TCP	54	44897 > sip-tls [ACK] Seq=1 Ack=1 win=1024 Len=0
378	37.8897480	172.16.12.3	172.16.11.3	TCP	54	44897 > lmsocialserver [ACK] Seq=1 Ack=1 win=1024 Len=0
379	37.8897920	172.16.12.3	172.16.11.3	TCP	54	44897 > 27356 [ACK] Seq=1 Ack=1 win=1024 Len=0
380	37.8917520	172.16.12.3	172.16.11.3	TCP	54	44897 > cgms [ACK] Seq=1 Ack=1 win=1024 Len=0
381	37.8918000	172.16.12.3	172.16.11.3	TCP	54	44897 > netsupport [ACK] Seq=1 Ack=1 win=1024 Len=0
382	37.8957430	172.16.12.3	172.16.11.3	TCP	54	44897 > warmspotMgmt [ACK] Seq=1 Ack=1 win=1024 Len=0

- (7) 分析扫描结果，得出结论：

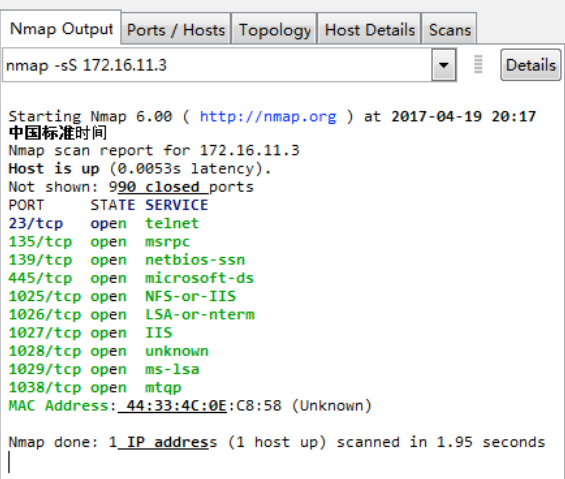
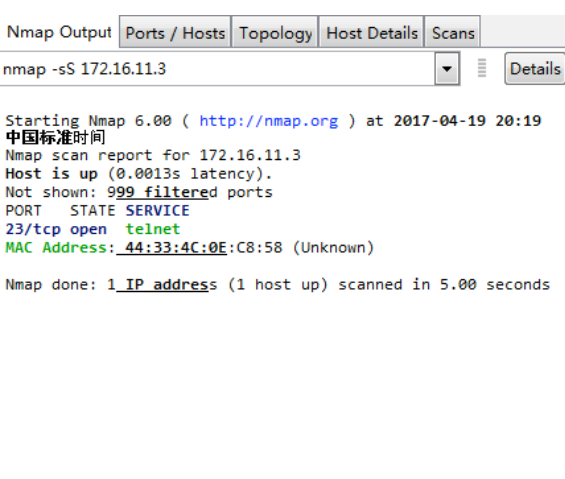
由表 2-18 的结果以及实验原理可知，ACK 扫描不能有计划地发现打开的端口，但是可以有效的划分过滤和未过滤响应，发现防火墙规则。

实验二、SYN 扫描（-sS）

- (1) 关闭目标机防火墙，命令：netsh firewall set opmode=disable
- (2) 在扫描机上执行 nmap -sS 192.168.1.20 记录扫描结果
- (3) 开启目标机防火墙 netsh firewall reset
- (4) 在扫描机上执行 nmap -sS 192.168.1.20 记录扫描结果
- (5) 将前后两次扫描结果填入表 2-19:

表 2-19 SYN 扫描结果



关闭目标机防火墙	开启目标机防火墙
nmap -sS 192.168.1.20	nmap -sS 192.168.1.20
	

(6) 用 Wireshark 抓取数据包, Nmap 发出了什么探测包?

SYN 探测包

2401	20.6900480	172.16.12.3	169.10.133.34	UDP	44	Source port: 19203	Destination port: 19603
2402	20.6903980	172.16.12.3	172.16.11.3	TCP	58	46968 > 16018 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2403	20.6911600	172.16.12.3	172.16.11.3	TCP	58	46968 > brvread [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2404	20.6973370	172.16.12.3	172.16.11.3	TCP	58	46968 > xfer [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2405	20.6973800	172.16.12.3	172.16.11.3	TCP	58	46968 > 6666 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2406	20.6993350	172.16.12.3	172.16.11.3	TCP	58	46968 > wag-service [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2407	20.6993770	172.16.12.3	172.16.11.3	TCP	58	46968 > 50001 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2408	20.7001070	172.16.12.3	172.16.11.3	TCP	58	46968 > 5001 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2409	20.7023390	172.16.12.3	172.16.11.3	TCP	58	46968 > 35500 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2410	20.7043370	172.16.12.3	172.16.11.3	TCP	58	46968 > amiganetfs [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2411	20.7043810	172.16.12.3	172.16.11.3	TCP	58	46968 > writesrv [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2412	20.7051120	172.16.12.3	172.16.11.3	TCP	58	46968 > 40911 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2413	20.7058400	172.16.12.3	172.16.11.3	TCP	58	46968 > fpitp [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2414	20.7083470	172.16.12.3	172.16.11.3	TCP	58	46968 > ms-olap4 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2415	20.7083960	172.16.12.3	172.16.11.3	TCP	58	46968 > 1027 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2416	20.7091240	172.16.12.3	172.16.11.3	TCP	58	46968 > 2005 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2417	20.7098580	172.16.12.3	172.16.11.3	TCP	58	46968 > 880 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2418	20.7123380	172.16.12.3	172.16.11.3	TCP	58	46968 > 7911 [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2419	20.7123800	172.16.12.3	172.16.11.3	TCP	58	46968 > ams [SYN] Seq=0 win=1024 Len=0 MSS=1460	
2420	20.7143350	172.16.12.3	172.16.11.3	TCP	58	46968 > drp [SYN] Seq=0 win=1024 Len=0 MSS=1460	

(7) 分析扫描结果, 得出结论:

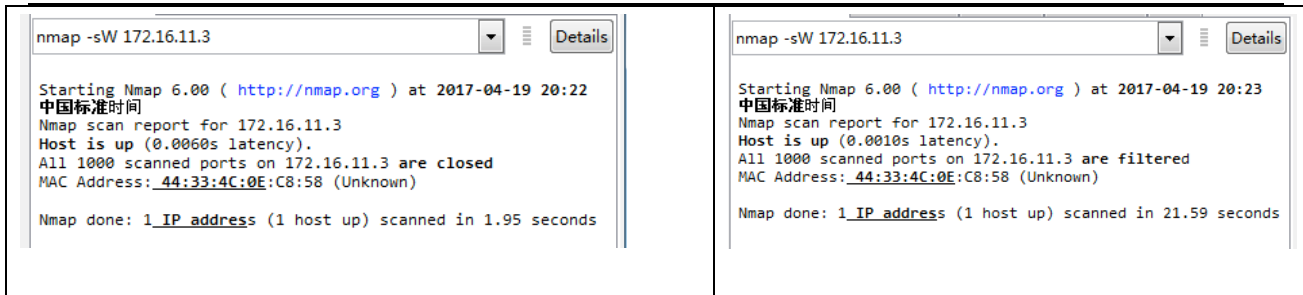
SYN 扫描可以发现端口的状态是打开还是关闭, 但防火墙开启时, SYN 包会被过滤。

实验三、TCP Window Scan (-sW) 扫描

- (1) 关闭目标机防火墙, 命令: netsh firewall set opmode=disable
- (2) 在扫描机上执行 nmap -sW 192.168.1.20 记录扫描结果
- (3) 开启目标机防火墙 netsh firewall reset
- (4) 在扫描机上执行 nmap -sW 192.168.1.20 记录扫描结果
- (5) 将前后两次扫描结果填入表 2-20:

表 2-20 TCP 扫描结果

关闭目标机防火墙	开启目标机防火墙
nmap -sW 192.168.1.20	nmap -sW 192.168.1.20



(6) 用 Wireshark 抓取数据包，Nmap 发出了什么探测包？

ACK 探测包。

45	12.8370550	172.16.12.3	172.16.11.3	TCP	54	51355	>	5510 [ACK] Seq=1 Ack=1 win=1024 Len=0
46	12.8410440	172.16.12.3	172.16.11.3	TCP	54	51355	>	gopher [ACK] Seq=1 Ack=1 win=1024 Len=0
47	12.8410860	172.16.12.3	172.16.11.3	TCP	54	51355	>	rsh-spx [ACK] Seq=1 Ack=1 win=1024 Len=0
48	12.8450470	172.16.12.3	172.16.11.3	TCP	54	51355	>	synchronet-rtc [ACK] Seq=1 Ack=1 win=1024 Len=0
49	12.8450910	172.16.12.3	172.16.11.3	TCP	54	51355	>	dnsix [ACK] Seq=1 Ack=1 win=1024 Len=0
50	12.8458200	172.16.12.3	172.16.11.3	TCP	54	51355	>	sixnetudr [ACK] Seq=1 Ack=1 win=1024 Len=0
51	12.8480440	172.16.12.3	172.16.11.3	TCP	54	51355	>	boinc-client [ACK] Seq=1 Ack=1 win=1024 Len=0
52	12.9321260	172.16.12.3	172.16.11.3	TCP	54	51354	>	remote-as [ACK] Seq=1 Ack=1 win=1024 Len=0
53	12.9322060	172.16.12.3	172.16.11.3	TCP	54	51354	>	beserver-msg-q [ACK] Seq=1 Ack=1 win=1024 Len=0
54	12.9360560	172.16.12.3	172.16.11.3	TCP	54	51354	>	alias [ACK] Seq=1 Ack=1 win=1024 Len=0
55	12.9380530	172.16.12.3	172.16.11.3	TCP	54	51354	>	esro-gen [ACK] Seq=1 Ack=1 win=1024 Len=0
56	12.9420510	172.16.12.3	172.16.11.3	TCP	54	51354	>	255 [ACK] Seq=1 Ack=1 win=1024 Len=0
57	12.9420940	172.16.12.3	172.16.11.3	TCP	54	51354	>	bacula-fd [ACK] Seq=1 Ack=1 win=1024 Len=0
58	12.9460560	172.16.12.3	172.16.11.3	TCP	54	51354	>	2021 [ACK] Seq=1 Ack=1 win=1024 Len=0
59	12.9461000	172.16.12.3	172.16.11.3	TCP	54	51354	>	3323 [ACK] Seq=1 Ack=1 win=1024 Len=0
60	12.9468290	172.16.12.3	172.16.11.3	TCP	54	51354	>	avt-profile-1 [ACK] Seq=1 Ack=1 win=1024 Len=0
61	12.9490650	172.16.12.3	172.16.11.3	TCP	54	51354	>	vmvc-2 [ACK] Seq=1 Ack=1 win=1024 Len=0

(7) 分析扫描结果，得出结论：

相对于 ACK 扫描，TCP window 扫描可以区分未被过滤端口的打开或者关闭，其他与 ACK 扫描一致。

实验四、根据实验一～实验三的扫描特点，对三种扫描方式如何发现防火墙进行综合分析。

ACK 扫描：发送一个只有 ACK 标志的 TCP 数据报给主机，如果主机反馈一个 TCP RST 数据报来，那么这个主机是存在的。也可以通过这种技术来确定对方防火墙是否是简单的分组过滤，还是一个基于状态的防火墙。

SYN 扫描为半开放式扫描。它向目标端口发送 SYN 包，一个 SYN|ACK 的返回信息表示端口处于侦听状态：返回 RST 表示端口没有处于侦听态。如果收到一个 SYN|ACK，则扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。

TCP Window 扫描的流程类似于 ACK 扫描，都是向服务端发送带有 ACK 标识的数据包，不同的在于 TCP 窗口扫描会检查收到的 RST 数据包中的窗口大小，如果 RST 数据包中的窗口大小不为零，则说明目标端口是开放的。

【交实验报告】



中山大學
SUN YAT-SEN UNIVERSITY

信息安全实验报告

上传实验报告：<ftp://222.200.180.109/>

截止日期：一周完成

上传小组实验报告。上传文件名格式：小组号_防火墙分析实验.pdf （由组长负责上传）

例如：文件名“6_防火墙管理实验.pdf”表示第 6 组的防火墙分析实验报告。

注意：不要打包上传！