

合肥工业大学

信息安全实验报告

实验 Nmap

学生 丁瑞

学 2016217676

专业 物联网 16-01 班

2019 年 12 月 30 日

一、 实验目的

- 1、掌握端口扫描这种信息探测技术的原理；
- 2、学会使用常见端口扫描工具；
- 3、了解各种常用网络服务所对应的端口号。

二、 实验原理

利用 Nmap 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 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，但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。

三、 实验步骤

3.1 主机发现

进行连通性检测，来判断目标主机（IP 地址为 192.168.2.138）是否连通。

主机发现发现的原理与 Ping 命令类似，发送探测包到目标主机，如果收到回复，那么说明目标主机是开启的。Nmap 支持十多种不同的主机探测方式，比如发送 ICMP ECHO/TIMESTAMP/NETMASK 报文、发送 TCPSYN/ACK 包、发送 SCTP INIT/COOKIE-ECHO 包，用户可以在不同的条件下灵活选用不同的方式来探测目标机。

```

csgd@dr:~$ nmap -sP 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 21:45 CST
Nmap scan report for 192.168.2.138
Host is up (0.0056s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
csgd@dr:~$ 

```

采用 nmap -sP 指令判断对方主机是否在线，用 wireshark 抓包

在执行命令后 本机向目标主机的 80 端口发送同步位 SYN=1，序列号 seq=0 的请求连接报文段。

目标主机接收到连接请求报文后同意连接，返回报文 SYN=1，ACK=1，确认序列号 ack=0+1=1，自己的序列号为 seq=1。

下图表示连接过程

1 0.000000000	192.168.1.102	192.168.2.138	TCP	76 38394 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
2 0.000037257	192.168.1.102	192.168.2.138	TCP	76 32838 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
3 0.005490880	192.168.2.138	192.168.1.102	TCP	56 80 → 38394 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4 0.006409389	192.168.2.138	192.168.1.102	TCP	56 443 → 32838 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
5 0.112706870	192.168.1.102	192.168.2.138	TCP	76 48498 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
6 0.114230032	192.168.1.102	192.168.2.138	TCP	76 48500 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
7 4.194751709	192.168.1.102	192.168.2.138	TCP	76 48502 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
8 4.195167506	192.168.1.102	192.168.2.138	TCP	76 48504 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
9 8.182990050	192.168.1.102	192.168.2.138	TCP	76 48510 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460

查看 mac 地址

```

Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
csgd@dr:~$ cat /proc/net/arp
IP address      HW type    Flags       HW address    Ma
192.168.1.101   0x1        0x2        bc:3d:85:bf:5c:02  *
172.17.0.2     0x1        0x2        02:42:ac:11:00:02  *
192.168.1.1     0x1        0x2        d0:76:e7:b2:5f:0e  *
csgd@dr:~$ 

```

3.2 使用常规扫描

常规扫描方式对目标主机进行 TCP 扫描。

全连接。这种扫描方式是使用 connect()系统调用打开目标机上相关端口的连接，并完成三次 TCP 握手

```

csgd@dr:~$ nmap -sT 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 21:57 CST
Nmap scan report for 192.168.2.138
Host is up (0.012s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    filtered  telnet

Nmap done: 1 IP address (1 host up) scanned in 14.69 seconds
csgd@dr:~$

```

抓取报文的信息

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.102	192.168.2.138	TCP	76	38872 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
2	0.000028696	192.168.1.102	192.168.2.138	TCP	76	33316 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
3	0.007797716	192.168.2.138	192.168.1.102	TCP	56	80 → 38872 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	0.026666158	192.168.1.102	192.168.2.138	TCP	76	48976 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
5	0.037109556	192.168.2.138	192.168.1.102	TCP	56	443 → 33316 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	0.156774729	192.168.1.102	192.168.2.138	TCP	76	48978 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
7	4.161538858	192.168.1.102	192.168.2.138	TCP	76	48980 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
8	4.162783395	192.168.1.102	192.168.2.138	TCP	76	48982 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
9	0.415666864	192.168.2.138	192.168.1.102	TCP	76	48984 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
10	8.144211727	192.168.1.102	192.168.2.138	TCP	76	48986 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
11	13.011559944	192.168.1.102	192.168.2.138	TCP	76	41000 → 23 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
12	13.011603431	192.168.1.102	192.168.2.138	TCP	76	58940 → 995 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
13	13.011626413	192.168.1.102	192.168.2.138	TCP	76	50506 → 53 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
14	13.011643264	192.168.1.102	192.168.2.138	TCP	76	36758 → 3389 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
15	13.011658288	192.168.1.102	192.168.2.138	TCP	76	52642 → 110 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
16	13.011674107	192.168.1.102	192.168.2.138	TCP	76	45340 → 1723 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
17	13.011690156	192.168.1.102	192.168.2.138	TCP	76	54924 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
18	13.011706122	192.168.1.102	192.168.2.138	TCP	76	38882 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460

22 号端口情况

No.	Time	Source	Destination	Protocol	Length	Info
28	13.022969889	192.168.1.102	192.168.2.138	TCP	76	46546 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
269	14.033437883	192.168.1.102	192.168.2.138	TCP	76	[TCP Retransmission] 46546 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
270	14.112791076	192.168.1.102	192.168.2.138	TCP	76	46778 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
773	14.253994494	192.168.1.102	192.168.2.138	TCP	76	47300 → 22 [SYN] Seq=0 Win=29200 Len=0 MSS=1460

3.3 SYN 半扫描

使用 SYN 半扫描方式对目标主机进行 TCP 端口扫描。

```

csgd@dr:~$ sudo nmap -sS 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 22:14 CST
Nmap scan report for 192.168.2.138
Host is up (0.017s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
22/tcp    filtered  ssh
23/tcp    filtered  telnet

Nmap done: 1 IP address (1 host up) scanned in 14.65 seconds
csgd@dr:~$

```

半连接的时间相比于全连接更短

半开扫描的原理是 Nmap 发送 SYN 包到远程主机，但是它不会产生任何会话，不需要通过完整的握手获得远程主机的信息，因此不会在目标主机上产生任何日志记录。

ip.addr==192.168.2.138							表达式...	+
No.	Time	Source	Destination	Protocol	Length	Info		
97	36.376699971	192.168.1.102	192.168.2.138	TCP	60	51192 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
98	36.376711844	192.168.1.102	192.168.2.138	TCP	56	51192 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0		
99	36.400700272	192.168.2.138	192.168.1.102	TCP	56	443 → 51192 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		
100	36.554645592	192.168.1.102	192.168.2.138	TCP	76	51674 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14		
101	36.556267343	192.168.1.102	192.168.2.138	TCP	76	51676 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14		
104	40.572258347	192.168.1.102	192.168.2.138	TCP	76	51678 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14		
105	40.573631594	192.168.1.102	192.168.2.138	TCP	76	51680 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14		
108	44.583574520	192.168.1.102	192.168.2.138	TCP	76	51682 → 5355 [SYN] Seq=0 Win=29200 Len=0 MSS=14		

ip.addr==192.168.2.138 and tcp.port==80							表达式...	+
No.	Time	Source	Destination	Protocol	Length	Info		
98	36.376711844	192.168.1.102	192.168.2.138	TCP	56	51192 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0		
119	49.468480598	192.168.1.102	192.168.2.138	TCP	60	51448 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460		
133	49.481740773	192.168.2.138	192.168.1.102	TCP	56	80 → 51448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0		

可见没有建立完整的连接就终止了

3.4 UDP 端口扫描

对目标主机进行 UDP 端口扫描。

UDP Ping 扫描是发送一个空的 UDP 报文到指定的端口，如果不指定端口则默认 40125，使用 UDP ping 扫描时 Nmap 会发送一个空的 UDP 包到目标主机，如果目标主机响应则返回一个 ICMP 端口不可达错误，如果目标主机不是存活状态则会返回各种 ICMP 错误信息。

```

csgd@dr:~$ sudo nmap -sU 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 22:20 CST
Nmap scan report for 192.168.2.138
Host is up (0.040s latency).
Not shown: 986 closed ports
PORT      STATE      SERVICE
7/udp     open|filtered echo
13/udp    open|filtered daytime
19/udp    open|filtered chargen
67/udp    open|filtered dhcps
123/udp   open|filtered ntp
161/udp   open       snmp
520/udp   open|filtered route
1645/udp  open|filtered radius
1646/udp  open|filtered radacct
1701/udp  open|filtered L2TP
1812/udp  open|filtered radius
1813/udp  open|filtered radacct
2000/udp  open|filtered cisco-sccp
49152/udp open|filtered unknown

```

19	13.175827513	192.168.1.102	192.168.2.138	UDP	44	52518 → 57172 Len=0
20	13.175864548	192.168.1.102	192.168.2.138	UDP	44	52518 → 1000 Len=0
21	13.175898279	192.168.1.102	192.168.2.138	UDP	44	52518 → 35702 Len=0
22	13.175929830	192.168.1.102	192.168.2.138	UDP	44	52518 → 643 Len=0
23	13.175962906	192.168.1.102	192.168.2.138	UDP	44	52518 → 42639 Len=0
24	13.175994561	192.168.1.102	192.168.2.138	UDP	44	52518 → 54094 Len=0
25	13.176026518	192.168.1.102	192.168.2.138	UDP	44	52518 → 1101 Len=0
26	13.176058250	192.168.1.102	192.168.2.138	UDP	44	52518 → 16832 Len=0

3.5 目标主机扫描

检测目标主机开放端口所提供的服务及其类型和版本信息。

```
csgd@dr:~$ sudo nmap -sV 192.168.2.138

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 22:32 CST
Nmap scan report for 192.168.2.138
Host is up (0.026s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    filtered ssh
23/tcp    filtered telnet

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.01 seconds
```

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.102	192.168.2.138	TCP	60	61714 → 443 [SYN] Seq=0 W
2	0.000011335	192.168.1.102	192.168.2.138	TCP	56	61714 → 80 [ACK] Seq=1 Ar
3	0.000018773	192.168.1.102	192.168.2.138	ICMP	56	Timestamp request id=(
4	0.009007149	192.168.2.138	192.168.1.102	ICMP	56	Timestamp reply id=(
5	0.073272262	192.168.2.138	192.168.1.102	TCP	56	443 → 61714 [RST, ACK] Sd
6	0.151278384	192.168.1.102	192.168.2.138	TCP	76	51968 → 5355 [SYN] Seq=0
7	0.152774452	192.168.1.102	192.168.2.138	TCP	76	51970 → 5355 [SYN] Seq=0
8	4.144200020	192.168.1.102	192.168.2.138	TCP	76	51974 → 5355 [SYN] Seq=0
9	4.145659521	192.168.1.102	192.168.2.138	TCP	76	51976 → 5355 [SYN] Seq=0
10	8.151260150	192.168.1.102	192.168.2.138	TCP	76	51978 → 5355 [SYN] Seq=0
11	8.152738407	192.168.1.102	192.168.2.138	TCP	76	51980 → 5355 [SYN] Seq=0
12	13.091613070	192.168.1.102	192.168.2.138	TCP	60	61970 → 587 [SYN] Seq=0 W
13	13.091633412	192.168.1.102	192.168.2.138	TCP	60	61972 → 443 [SYN] Seq=0 W

3.6 探测目标主机的操作系统类型。

```
csgd@dr:~$ sudo nmap -O 172.17.0.2

Starting Nmap 7.01 ( https://nmap.org ) at 2020-01-11 22:41 CST
Nmap scan report for 172.17.0.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds
```

四、实验总结

通过本次实验我学会了利用 Nmap 配合 Wireshark 的使用，对目标主机进行扫描，并获取到包括端口、操作系统、协议在内的有效信息。初步掌握了软件的使用。

