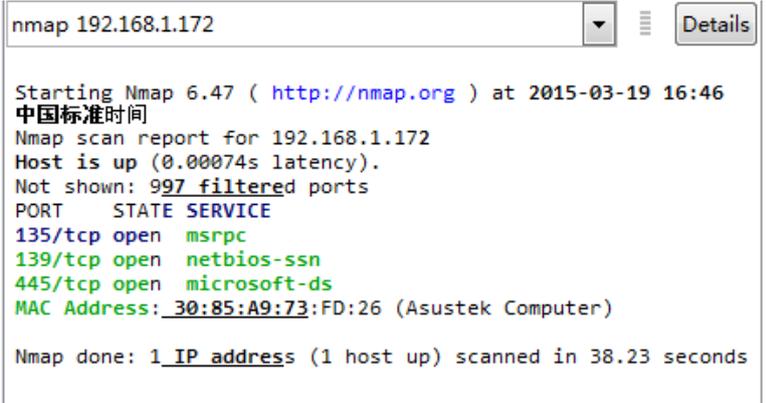


## 贵州大学实验报告

学院：计算机科学与技术      专业：XXX      班级：网络 XXX

姓名	XXX	学号	XXX	实验组	
实验时间	2015.3.13	指导教师	XXX	成绩	
实验项目名称	<b>Nmap 扫描器使用和分析</b>				
实验目的	1、掌握主机、端口扫描的原理 2、掌握 Nmap 扫描器的使用 3、掌握 Nmap 进行远程 OS 检测的原理				
实验内容	<p>1 主机发现 (Host Discovery)</p> <p>默认情况下, Nmap 会发送四种不同类型的数据包来探测目标主机是否在线。</p> <ol style="list-style-type: none"> <li>1. ICMP echo request</li> <li>2. a TCP SYN packet to port 443(网页浏览端口)</li> <li>3. a TCP ACK packet to port 80</li> <li>4. an ICMP timestamp request</li> </ol> <p>依次发送四个报文探测目标机是否开启。只要收到其中一个包的回复, 那就证明目标机开启。使用四种不同类型的数据包可以避免因防火墙或丢包造成的判断错误。</p> <ul style="list-style-type: none"> <li>● -sL: List Scan 列表扫描, 仅将指定的目标的 IP 列举出来, 不进行主机发现。</li> <li>● -sn: Ping Scan 只进行主机发现, 不进行端口扫描。</li> <li>● -Pn: 将所有指定的主机视作开启的, 跳过主机发现的过程。</li> <li>● -PS/PA/PU/PY[portlist]: 使用 TCP SYN/ACK 或 SCTP INIT/ECHO 方式进行发现。</li> <li>● -PE/PP/PM: 使用 ICMP echo, timestamp, and netmask 请求包发现主机。</li> <li>● -sn: 表示只单独进行主机发现过程;</li> <li>● -Pn : 表示直接跳过主机发现而进行端口扫描等高级操作 (如果已经确知目标主机已经开启, 可用该选项);</li> <li>● -n: 如果不想使用 DNS 或 reverse DNS 解析, 那么可以使用该选项。</li> </ul> <p>2 端口扫描 (Port Scanning)</p> <p>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。</p> <p>默认情况下, Nmap 会扫描 1000 个最有可能开放的 TCP 端口。</p>				

	<p>Nmap 在端口扫描方面非常强大，提供了十多种探测方式。</p> <ul style="list-style-type: none"> <li>● 1. <b>TCP SYN(synchronize) scanning(默认)</b></li> <li>● 2. <b>TCP connect scanning</b></li> <li>● 3. <b>TCPACK (Acknowledgement) scanning</b></li> <li>● 4. <b>UDP scanning</b></li> <li>● .....</li> </ul> <p>3 版本侦测 (Version Detection)</p> <p>用于确定目标主机开放端口上运行的具体的应用程序及版本信息。</p> <ul style="list-style-type: none"> <li>● -sV: 指定让 Nmap 进行版本侦测</li> <li>● --version-intensity &lt;level&gt;: 指定版本侦测强度 (0-9)，默认为 7。数值越高，探测出的服务越准确，但是运行时间会比较长。</li> <li>● --version-light: 指定使用轻量侦测方式 (intensity 2)</li> <li>● --version-all: 尝试使用所有的 probes 进行侦测 (intensity 9)</li> <li>● --version-trace: 显示出详细的版本侦测过程信息。</li> </ul> <p>4 操作系统侦测 (Operating System Detection)</p> <ul style="list-style-type: none"> <li>● 操作系统侦测用于检测目标主机运行的操作系统类型及设备类型等信息。</li> <li>● Nmap 使用 TCP/IP 协议栈指纹来识别不同的操作系统和设备。</li> </ul>
<p>实验环境</p>	<p>Win7 TCP/IP 网络 Nmap 6.47</p>
<p>实验步骤及结果</p>	<p>Nmap 的典型用法</p> <p>1、确定端口状况</p> <pre>nmap targethost nmap 192.168.1.172</pre>  <p>扫描发现该主机是存在的，而且默认扫描了 1000 个端口，其中有 997 个关闭的，135, 139, 445 三个端口是打开的</p> <p>跳过主机发现扫描端口</p> <pre>Nmap -Pn 192.168.1.172</pre>

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

nmap -Pn 192.168.1.172

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19 16:41
中国标准时间
Nmap scan report for 192.168.1.172
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 38.63 seconds
```

2、完整全面的扫描

```
nmap -T4 -A -v targethost
nmap -T4 -A -v 172.168.1.172
```

nmap -T4 -A -v 192.168.1.172

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19
17:04 中国标准时间
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 17:04
Scanning 192.168.1.172 [1 port]
Completed ARP Ping Scan at 17:04, 0.99s elapsed (1 total
hosts)
Initiating Parallel DNS resolution of 1 host. at 17:04
Completed Parallel DNS resolution of 1 host. at 17:04,
16.50s elapsed
Initiating SYN Stealth Scan at 17:04
Scanning 192.168.1.172 [1000 ports]
Discovered open port 135/tcp on 192.168.1.172
Discovered open port 445/tcp on 192.168.1.172
Discovered open port 139/tcp on 192.168.1.172
Completed SYN Stealth Scan at 17:04, 4.68s elapsed (1000
total ports)
Initiating Service scan at 17:04
Scanning 3 services on 192.168.1.172
Completed Service scan at 17:04, 6.00s elapsed (3
services on 1 host)
Initiating OS detection (try #1) against 192.168.1.172
Retrying OS detection (try #2) against 192.168.1.172
NSE: Script scanning 192.168.1.172.
Initiating NSE at 17:04
Completed NSE at 17:05, 40.16s elapsed
Nmap scan report for 192.168.1.172
Host is up (0.00063s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
```

```
135/tcp open  msrpc      Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  netbios-ssn
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)
Warning: OSscan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows Vista|2008|7|
Phone|2012 (97%)
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/
o:microsoft:windows_vista::sp1 cpe:/
o:microsoft:windows_server_2008::sp1 cpe:/
o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/
o:microsoft:windows_8 cpe:/
o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows Vista SP0 or
SP1, Windows Server 2008 SP1, or Windows 7 (97%),
Microsoft Windows Vista SP2, Windows 7 SP1, or Windows
Server 2008 (96%), Microsoft Windows Phone 7.5 or 8.0
(95%), Windows Server 2008 R2 (95%), Microsoft Windows 7
Professional or Windows 8 (95%), Microsoft Windows
Server 2008 SP1 (93%), Microsoft Windows 7 SP1 (92%),
Microsoft Windows 8 Enterprise (90%), Microsoft Windows
Vista SP0 - SP1 (90%), Microsoft Windows 7 SP1 or
Windows Server 2008 SP1 - SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.417 days (since Thu Mar 19 07:04:48 2015)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=250 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Host script results:

```
| nbstat: NetBIOS name: ASUS-DN, NetBIOS user:
<unknown>, NetBIOS MAC: 30:85:a9:73:fd:26 (Asustek
Computer)
| Names:
|   ASUS-DN<20>           Flags: <unique><active>
|   ASUS-DN<00>           Flags: <unique><active>
|_  WORKGROUP<00>        Flags: <group><active>
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_ smbv2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

```
HOP RTT    ADDRESS
1   0.63 ms 192.168.1.172
```

NSE: Script Post-scanning.

```
Read data files from: D:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any
incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 90.78
seconds
```

```
Raw packets sent: 2075 (94.992KB) | Rcvd: 38
(2.432KB)
```

使用了该选项，nmap 对目标主机进行主机发现、端口扫描、应用程序与版本侦测、操作系统侦测及调用默认 NSE 脚本扫

描。

### 3、探测 [www.baidu.com](http://www.baidu.com)

Target:  Profile:

Command:

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.baidu.com (192.168.1.8)

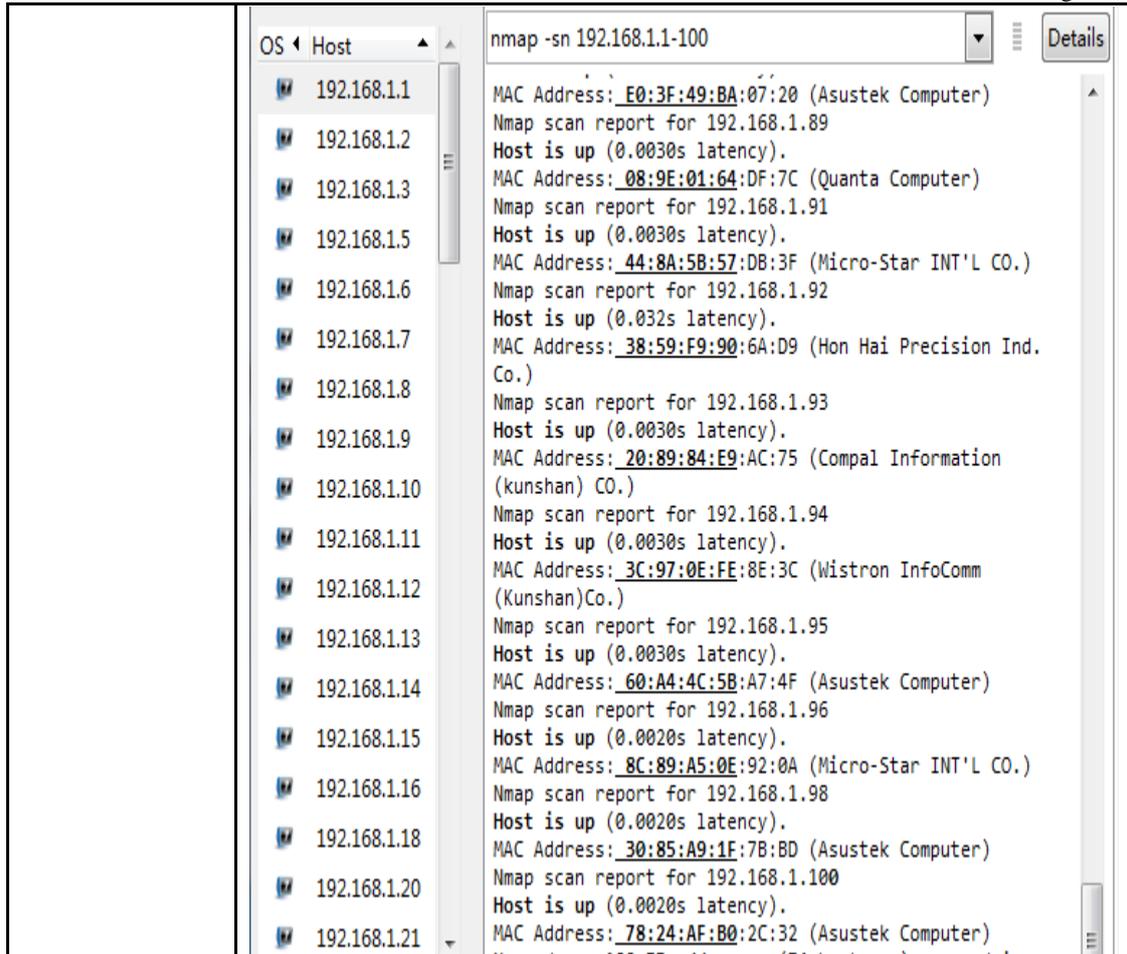
```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-13 11:17 中国标准时间
Nmap scan report for www.baidu.com (61.135.169.125)
Host is up (0.016s latency).
Other addresses for www.baidu.com (not scanned):
61.135.169.121
Nmap done: 1 IP address (1 host up) scanned in 12.70 seconds
```

### 4、扫面局域网内活动主机

`nmap -sn 192.168.1.1-100`

OS Host

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19 17:00 中国标准时间
Nmap scan report for 192.168.1.1
Host is up (0.0020s latency).
MAC Address: 04:5F:A7:09:32:CE (Shenzhen Yichen Technology Development Co.)
Nmap scan report for 192.168.1.2
Host is up (0.0010s latency).
MAC Address: 74:86:7A:24:FE:DC (Dell)
Nmap scan report for 192.168.1.3
Host is up (0.0010s latency).
MAC Address: 74:86:7A:28:7C:A4 (Dell)
Nmap scan report for 192.168.1.5
Host is up (0.0020s latency).
MAC Address: 2C:27:D7:C9:B5:A8 (Hewlett-Packard Company)
Nmap scan report for 192.168.1.6
Host is up (0.0020s latency).
MAC Address: 74:86:7A:5C:71:CC (Dell)
Nmap scan report for 192.168.1.7
Host is up (0.0020s latency).
MAC Address: 00:1B:77:97:54:09 (Intel Corporate)
Nmap scan report for 192.168.1.8
Host is up (0.0040s latency).
MAC Address: 44:6D:57:A8:92:3B (Liteon Technology)
Nmap scan report for 192.168.1.9
Host is up (0.0010s latency).
MAC Address: BC:5F:F4:05:70:60 (ASRock Incorporation)
Nmap scan report for 192.168.1.10
Host is up (0.0010s latency).
MAC Address: 00:90:F5:E5:E2:AC (Clevo CO.)
Nmap scan report for 192.168.1.11
Host is up (0.0010s latency).
MAC Address: 00:0C:29:15:70:00 (Hewlett-Packard)
```



OS Host nmap -sn 192.168.1.1-100

Host	MAC Address	Company
192.168.1.1	E0:3F:49:BA:07:20	Asustek Computer
192.168.1.2		
192.168.1.3	08:9E:01:64:DF:7C	Quanta Computer
192.168.1.5		
192.168.1.6	44:8A:5B:57:DB:3F	Micro-Star INT'L CO.
192.168.1.7	38:59:F9:90:6A:D9	Hon Hai Precision Ind. Co.)
192.168.1.8		
192.168.1.9	20:89:84:E9:AC:75	Compal Information (kunshan) CO.)
192.168.1.10		
192.168.1.11	3C:97:0E:FE:8E:3C	Wistron InfoComm (Kunshan)Co.)
192.168.1.13		
192.168.1.14	60:A4:4C:5B:A7:4F	Asustek Computer
192.168.1.15		
192.168.1.16	8C:89:A5:0E:92:0A	Micro-Star INT'L CO.)
192.168.1.18	30:85:A9:1F:7B:BD	Asustek Computer
192.168.1.20		
192.168.1.21	78:24:AF:80:2C:32	Asustek Computer

在局域网内，Nmap 是通过 ARP 包来询问 IP 地址上的主机是否活动的，如果收到 ARP 回复包，那么说明主机在线。

5、使用 TCP SYN 方式扫描 TCP 端口；-sU 表示扫描 UDP 端口；-T4 表示时间级别配置 4 级；--top-ports 300 表示扫描最有可能开放的 300 个端口（TCP 和 UDP 分别有 300 个端口）。

nmap -sS -sU -T4 --top-ports 300 192.168.1.172



nmap -sS -sU -T4 --top-ports 300 192.168.1.172

```

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19 16:59
中国标准时间
Nmap scan report for 192.168.1.172
Host is up (0.0012s latency).
Not shown: 299 open|filtered ports, 297 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
137/udp   open  netbios-ns
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)

Nmap done: 1 IP address (1 host up) scanned in 39.01 seconds
  
```

有三个 tcp 端口打开的，分别是 135，139，445，还有一个 udp 端口打

开的, 137

### 6、版本侦测

Nmap -sV 192.168.1.172

```
nmap -sV 192.168.1.172
```

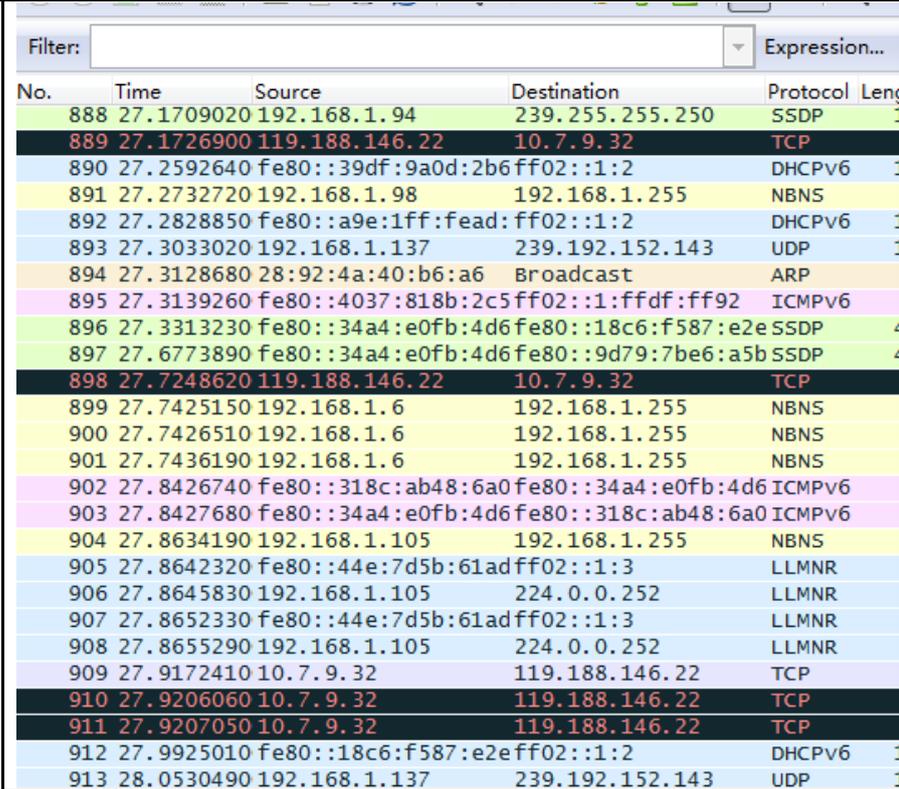
```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19 16:52  
中国标准时间  
Nmap scan report for 192.168.1.172  
Host is up (0.0016s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows RPC  
445/tcp   open  netbios-ssn  Microsoft Windows RPC  
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Service detection performed. Please report any incorrect  
results at http://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 46.03 seconds
```

### 7、OS 侦测

```
nmap -O 192.168.1.172
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-19  
16:39 中国标准时间  
Nmap scan report for 192.168.1.172  
Host is up (0.0021s latency).  
Not shown: 997 filtered ports  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)  
Warning: OSScan results may be unreliable because we  
could not find at least 1 open and 1 closed port  
Device type: phone | general purpose  
Running (JUST GUESSING): Microsoft Windows Phone|2008|7|  
Vista|2012 (97%)  
OS CPE: cpe:/o:microsoft:windows cpe:/  
o:microsoft:windows_server_2008:r2 cpe:/  
o:microsoft:windows_7::-:professional cpe:/  
o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::-  
cpe:/o:microsoft:windows_vista:::sp1 cpe:/  
o:microsoft:windows_server_2012  
Aggressive OS guesses: Microsoft Windows Phone 7.5 or  
8.0 (97%), Windows Server 2008 R2 (97%), Microsoft  
Windows 7 Professional or Windows 8 (97%), Microsoft  
Windows Vista SP0 or SP1, Windows Server 2008 SP1, or  
Windows 7 (97%), Microsoft Windows Vista SP2, Windows 7  
SP1, or Windows Server 2008 (96%), Microsoft Windows  
Server 2008 SP1 (94%), Microsoft Windows 8 Enterprise  
(92%), Microsoft Windows Vista SP0 - SP1 (92%),  
Microsoft Windows Server 2012 (91%), Microsoft Windows  
Vista Home Premium SP1, Windows 7, or Windows Server  
2008 (91%)  
No exact OS matches for host (test conditions non-ideal).
```

使用 wireshark 抓包

	 <table border="1"> <thead> <tr> <th>No.</th> <th>Time</th> <th>Source</th> <th>Destination</th> <th>Protocol</th> <th>Length</th> <th>Info</th> </tr> </thead> <tbody> <tr><td>888</td><td>27.1709020</td><td>192.168.1.94</td><td>239.255.255.250</td><td>SSDP</td><td>175</td><td>M-SEARCH * HTTP</td></tr> <tr><td>889</td><td>27.1726900</td><td>119.188.146.22</td><td>10.7.9.32</td><td>TCP</td><td>62</td><td>[TCP Retransmi</td></tr> <tr><td>890</td><td>27.2592640</td><td>fe80::39df:9a0d:2b6ff02::1:2</td><td></td><td>DHCPv6</td><td>149</td><td>solicit XID: 0</td></tr> <tr><td>891</td><td>27.2732720</td><td>192.168.1.98</td><td>192.168.1.255</td><td>NBNS</td><td>92</td><td>Name query NB</td></tr> <tr><td>892</td><td>27.2828850</td><td>fe80::a9e:1ff:fead:ff02::1:2</td><td></td><td>DHCPv6</td><td>114</td><td>solicit XID: 0</td></tr> <tr><td>893</td><td>27.3033020</td><td>192.168.1.137</td><td>239.192.152.143</td><td>UDP</td><td>161</td><td>Source port: 6</td></tr> <tr><td>894</td><td>27.3128680</td><td>28:92:4a:40:b6:a6</td><td>Broadcast</td><td>ARP</td><td>60</td><td>who has 192.16</td></tr> <tr><td>895</td><td>27.3139260</td><td>fe80::4037:818b:2c5ff02::1:ffdf:ff92</td><td></td><td>ICMPv6</td><td>86</td><td>Neighbor Solic</td></tr> <tr><td>896</td><td>27.3313230</td><td>fe80::34a4:e0fb:4d6fe80::18c6:f587:e2e</td><td></td><td>SSDP</td><td>453</td><td>HTTP/1.1 200 O</td></tr> <tr><td>897</td><td>27.6773890</td><td>fe80::34a4:e0fb:4d6fe80::9d79:7be6:a5b</td><td></td><td>SSDP</td><td>453</td><td>HTTP/1.1 200 O</td></tr> <tr><td>898</td><td>27.7248620</td><td>119.188.146.22</td><td>10.7.9.32</td><td>TCP</td><td>62</td><td>[TCP Retransmi</td></tr> <tr><td>899</td><td>27.7425150</td><td>192.168.1.6</td><td>192.168.1.255</td><td>NBNS</td><td>92</td><td>Name query NB</td></tr> <tr><td>900</td><td>27.7426510</td><td>192.168.1.6</td><td>192.168.1.255</td><td>NBNS</td><td>92</td><td>Name query NB</td></tr> <tr><td>901</td><td>27.7436190</td><td>192.168.1.6</td><td>192.168.1.255</td><td>NBNS</td><td>92</td><td>Name query NB</td></tr> <tr><td>902</td><td>27.8426740</td><td>fe80::318c:ab48:6a0fe80::34a4:e0fb:4d6</td><td></td><td>ICMPv6</td><td>86</td><td>Neighbor Solic</td></tr> <tr><td>903</td><td>27.8427680</td><td>fe80::34a4:e0fb:4d6fe80::318c:ab48:6a0</td><td></td><td>ICMPv6</td><td>86</td><td>Neighbor Adver</td></tr> <tr><td>904</td><td>27.8634190</td><td>192.168.1.105</td><td>192.168.1.255</td><td>NBNS</td><td>92</td><td>Name query NB</td></tr> <tr><td>905</td><td>27.8642320</td><td>fe80::44e:7d5b:61adff02::1:3</td><td></td><td>LLMNR</td><td>84</td><td>Standard query</td></tr> <tr><td>906</td><td>27.8645830</td><td>192.168.1.105</td><td>224.0.0.252</td><td>LLMNR</td><td>64</td><td>Standard query</td></tr> <tr><td>907</td><td>27.8652330</td><td>fe80::44e:7d5b:61adff02::1:3</td><td></td><td>LLMNR</td><td>84</td><td>Standard query</td></tr> <tr><td>908</td><td>27.8655290</td><td>192.168.1.105</td><td>224.0.0.252</td><td>LLMNR</td><td>64</td><td>Standard query</td></tr> <tr><td>909</td><td>27.9172410</td><td>10.7.9.32</td><td>119.188.146.22</td><td>TCP</td><td>62</td><td>16106-7533 [AC</td></tr> <tr><td>910</td><td>27.9206060</td><td>10.7.9.32</td><td>119.188.146.22</td><td>TCP</td><td>74</td><td>[TCP Dup ACK 9</td></tr> <tr><td>911</td><td>27.9207050</td><td>10.7.9.32</td><td>119.188.146.22</td><td>TCP</td><td>74</td><td>[TCP Dup ACK 9</td></tr> <tr><td>912</td><td>27.9925010</td><td>fe80::18c6:f587:e2eff02::1:2</td><td></td><td>DHCPv6</td><td>148</td><td>solicit XID: 0</td></tr> <tr><td>913</td><td>28.0530490</td><td>192.168.1.137</td><td>239.192.152.143</td><td>UDP</td><td>161</td><td>Source port: 6</td></tr> </tbody> </table>	No.	Time	Source	Destination	Protocol	Length	Info	888	27.1709020	192.168.1.94	239.255.255.250	SSDP	175	M-SEARCH * HTTP	889	27.1726900	119.188.146.22	10.7.9.32	TCP	62	[TCP Retransmi	890	27.2592640	fe80::39df:9a0d:2b6ff02::1:2		DHCPv6	149	solicit XID: 0	891	27.2732720	192.168.1.98	192.168.1.255	NBNS	92	Name query NB	892	27.2828850	fe80::a9e:1ff:fead:ff02::1:2		DHCPv6	114	solicit XID: 0	893	27.3033020	192.168.1.137	239.192.152.143	UDP	161	Source port: 6	894	27.3128680	28:92:4a:40:b6:a6	Broadcast	ARP	60	who has 192.16	895	27.3139260	fe80::4037:818b:2c5ff02::1:ffdf:ff92		ICMPv6	86	Neighbor Solic	896	27.3313230	fe80::34a4:e0fb:4d6fe80::18c6:f587:e2e		SSDP	453	HTTP/1.1 200 O	897	27.6773890	fe80::34a4:e0fb:4d6fe80::9d79:7be6:a5b		SSDP	453	HTTP/1.1 200 O	898	27.7248620	119.188.146.22	10.7.9.32	TCP	62	[TCP Retransmi	899	27.7425150	192.168.1.6	192.168.1.255	NBNS	92	Name query NB	900	27.7426510	192.168.1.6	192.168.1.255	NBNS	92	Name query NB	901	27.7436190	192.168.1.6	192.168.1.255	NBNS	92	Name query NB	902	27.8426740	fe80::318c:ab48:6a0fe80::34a4:e0fb:4d6		ICMPv6	86	Neighbor Solic	903	27.8427680	fe80::34a4:e0fb:4d6fe80::318c:ab48:6a0		ICMPv6	86	Neighbor Adver	904	27.8634190	192.168.1.105	192.168.1.255	NBNS	92	Name query NB	905	27.8642320	fe80::44e:7d5b:61adff02::1:3		LLMNR	84	Standard query	906	27.8645830	192.168.1.105	224.0.0.252	LLMNR	64	Standard query	907	27.8652330	fe80::44e:7d5b:61adff02::1:3		LLMNR	84	Standard query	908	27.8655290	192.168.1.105	224.0.0.252	LLMNR	64	Standard query	909	27.9172410	10.7.9.32	119.188.146.22	TCP	62	16106-7533 [AC	910	27.9206060	10.7.9.32	119.188.146.22	TCP	74	[TCP Dup ACK 9	911	27.9207050	10.7.9.32	119.188.146.22	TCP	74	[TCP Dup ACK 9	912	27.9925010	fe80::18c6:f587:e2eff02::1:2		DHCPv6	148	solicit XID: 0	913	28.0530490	192.168.1.137	239.192.152.143	UDP	161	Source port: 6
No.	Time	Source	Destination	Protocol	Length	Info																																																																																																																																																																																								
888	27.1709020	192.168.1.94	239.255.255.250	SSDP	175	M-SEARCH * HTTP																																																																																																																																																																																								
889	27.1726900	119.188.146.22	10.7.9.32	TCP	62	[TCP Retransmi																																																																																																																																																																																								
890	27.2592640	fe80::39df:9a0d:2b6ff02::1:2		DHCPv6	149	solicit XID: 0																																																																																																																																																																																								
891	27.2732720	192.168.1.98	192.168.1.255	NBNS	92	Name query NB																																																																																																																																																																																								
892	27.2828850	fe80::a9e:1ff:fead:ff02::1:2		DHCPv6	114	solicit XID: 0																																																																																																																																																																																								
893	27.3033020	192.168.1.137	239.192.152.143	UDP	161	Source port: 6																																																																																																																																																																																								
894	27.3128680	28:92:4a:40:b6:a6	Broadcast	ARP	60	who has 192.16																																																																																																																																																																																								
895	27.3139260	fe80::4037:818b:2c5ff02::1:ffdf:ff92		ICMPv6	86	Neighbor Solic																																																																																																																																																																																								
896	27.3313230	fe80::34a4:e0fb:4d6fe80::18c6:f587:e2e		SSDP	453	HTTP/1.1 200 O																																																																																																																																																																																								
897	27.6773890	fe80::34a4:e0fb:4d6fe80::9d79:7be6:a5b		SSDP	453	HTTP/1.1 200 O																																																																																																																																																																																								
898	27.7248620	119.188.146.22	10.7.9.32	TCP	62	[TCP Retransmi																																																																																																																																																																																								
899	27.7425150	192.168.1.6	192.168.1.255	NBNS	92	Name query NB																																																																																																																																																																																								
900	27.7426510	192.168.1.6	192.168.1.255	NBNS	92	Name query NB																																																																																																																																																																																								
901	27.7436190	192.168.1.6	192.168.1.255	NBNS	92	Name query NB																																																																																																																																																																																								
902	27.8426740	fe80::318c:ab48:6a0fe80::34a4:e0fb:4d6		ICMPv6	86	Neighbor Solic																																																																																																																																																																																								
903	27.8427680	fe80::34a4:e0fb:4d6fe80::318c:ab48:6a0		ICMPv6	86	Neighbor Adver																																																																																																																																																																																								
904	27.8634190	192.168.1.105	192.168.1.255	NBNS	92	Name query NB																																																																																																																																																																																								
905	27.8642320	fe80::44e:7d5b:61adff02::1:3		LLMNR	84	Standard query																																																																																																																																																																																								
906	27.8645830	192.168.1.105	224.0.0.252	LLMNR	64	Standard query																																																																																																																																																																																								
907	27.8652330	fe80::44e:7d5b:61adff02::1:3		LLMNR	84	Standard query																																																																																																																																																																																								
908	27.8655290	192.168.1.105	224.0.0.252	LLMNR	64	Standard query																																																																																																																																																																																								
909	27.9172410	10.7.9.32	119.188.146.22	TCP	62	16106-7533 [AC																																																																																																																																																																																								
910	27.9206060	10.7.9.32	119.188.146.22	TCP	74	[TCP Dup ACK 9																																																																																																																																																																																								
911	27.9207050	10.7.9.32	119.188.146.22	TCP	74	[TCP Dup ACK 9																																																																																																																																																																																								
912	27.9925010	fe80::18c6:f587:e2eff02::1:2		DHCPv6	148	solicit XID: 0																																																																																																																																																																																								
913	28.0530490	192.168.1.137	239.192.152.143	UDP	161	Source port: 6																																																																																																																																																																																								
<p>实验总结</p>	<ol style="list-style-type: none"> <li>1、了解了主机、端口扫描的原理</li> <li>2、基本掌握 Nmap 扫描器的使用</li> <li>3、掌握 Nmap 进行远程 OS 检测的原理</li> </ol>																																																																																																																																																																																													
<p>指导教师意见</p>	<p style="text-align: right;">签名:</p> <p style="text-align: right;">年 月 日</p>																																																																																																																																																																																													