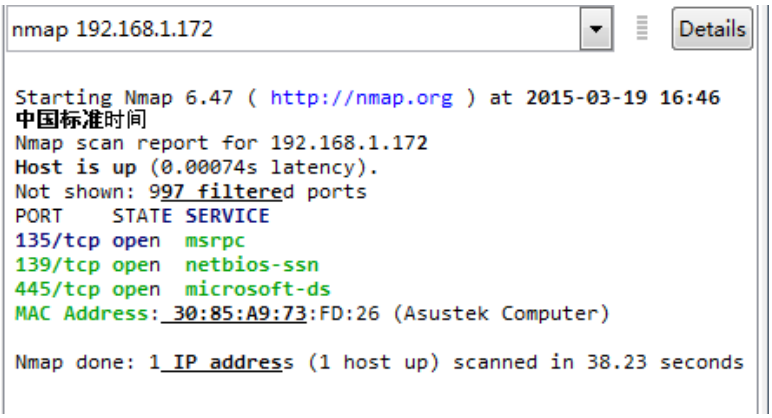
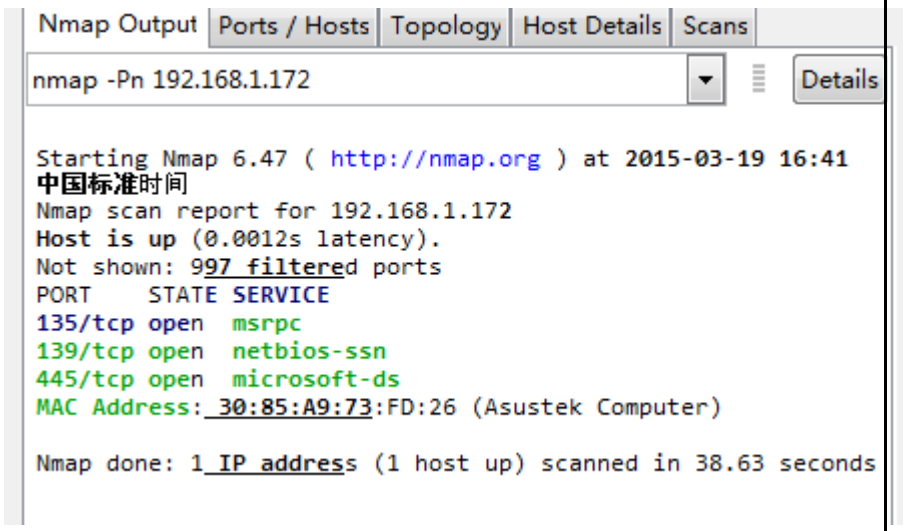
贵州大学实验报告

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	Nmap 扫描器使用和分析				
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	1 主机发现（Host Discovery） 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。 1. ICMP echo request 2. a TCP SYN packet to port 443(网页浏览端口) 3. a TCP ACK packet to port 80 4. an ICMP timestamp request 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。 ● -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。 ● -sn: Ping Scan 只进行主机发现，不进行端口扫描。 ● -Pn: 将所有指定的主机视作开启的，跳过主机发现的过程。 ● -PS/PA/PU/PY[portlist]: 使用 TCP SYN/ACK 或 SCTP INIT/ECHO 方式进行发现。 ● -PE/PP/PM: 使用 ICMP echo, timestamp, and netmask 请求包发现主机。 ● -sn：表示只单独进行主机发现过程； ● -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）； ● -n：如果不想使用 DNS 或 reverse DNS 解析，那么可以使用该选项。 2 端口扫描（Port Scanning） 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。 默认情况下，Nmap 会扫描 1000 个最有可能开放的 TCP 端口。				

<table>
<tr><td></td><td>
Nmap 在端口扫描方面非常强大，提供了十多种探测方式。
● 1.TCP SYN(synchronize) scanning(默认)
● 2.TCP connect scanning
● 3. TCP ACK (Acknowledgement） scanning
● 4.UDP scanning
● ……
3 版本侦测（Version Detection）
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。
● -sV: 指定让 Nmap 进行版本侦测
● --version-intensity <level>: 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。
● --version-light: 指定使用轻量侦测方式 (intensity 2)
● --version-all: 尝试使用所有的 probes 进行侦测 (intensity 9)
● --version-trace: 显示出详细的版本侦测过程信息。
4 操作系统侦测（Operating System Detection）
● 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。
● Nmap 使用 TCP/IP 协议栈指纹来识别不同的操作系统和设备。
</td></tr>
<tr><td>实验环境</td><td>
Win7
TCP/IP 网络
Nmap 6.47
</td></tr>
<tr><td>实验步骤及结果</td><td>
Nmap 的典型用法
1、 确定端口状况
nmap targethost
nmap 192.168.1.172


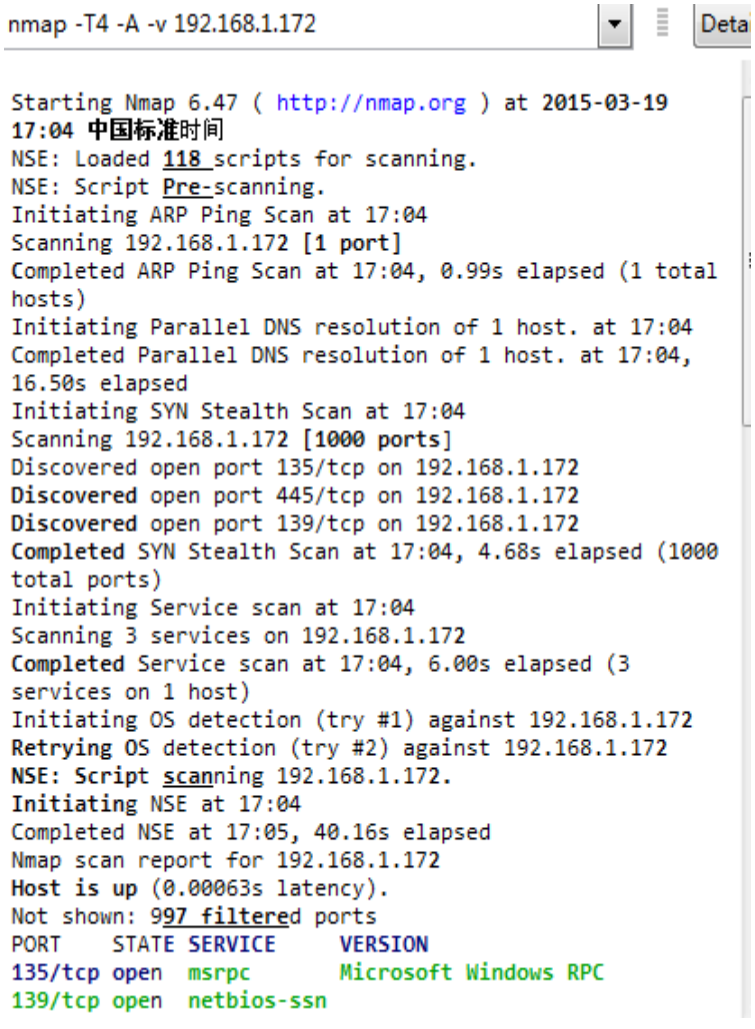
扫描发现该主机是存在的，而且默认扫描了 1000 个端口，其中有 997 个关闭的，135，139，445 三个端口是打开的
跳过主机发现扫描端口
Nmap -Pn 192.168.1.172
</td></tr>
</table>



2、 完整全面的扫描

nmap –T4 –A –v targethost

nmap –T4 –A –v 172.168.1.172

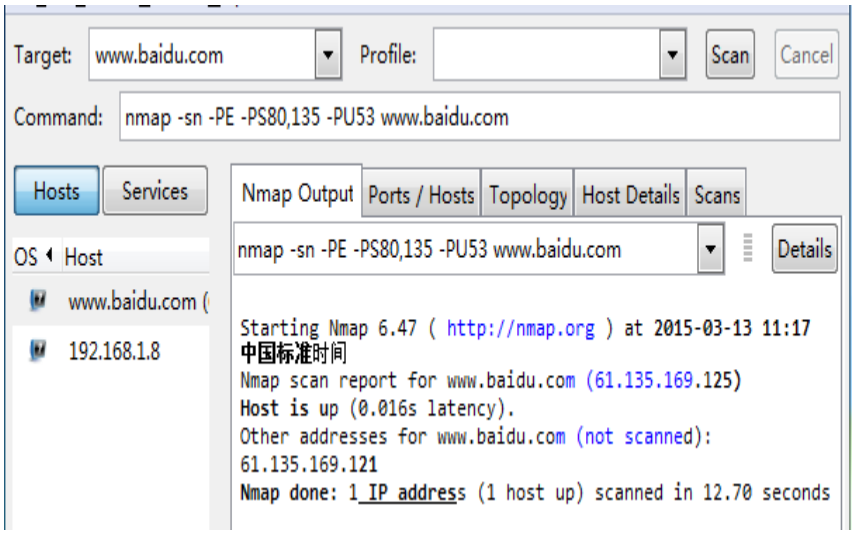


```
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  netbios-ssn
MAC Address: 30:85:A9:73:FD:26 (Asustek Computer)
Warning: OSScan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST 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

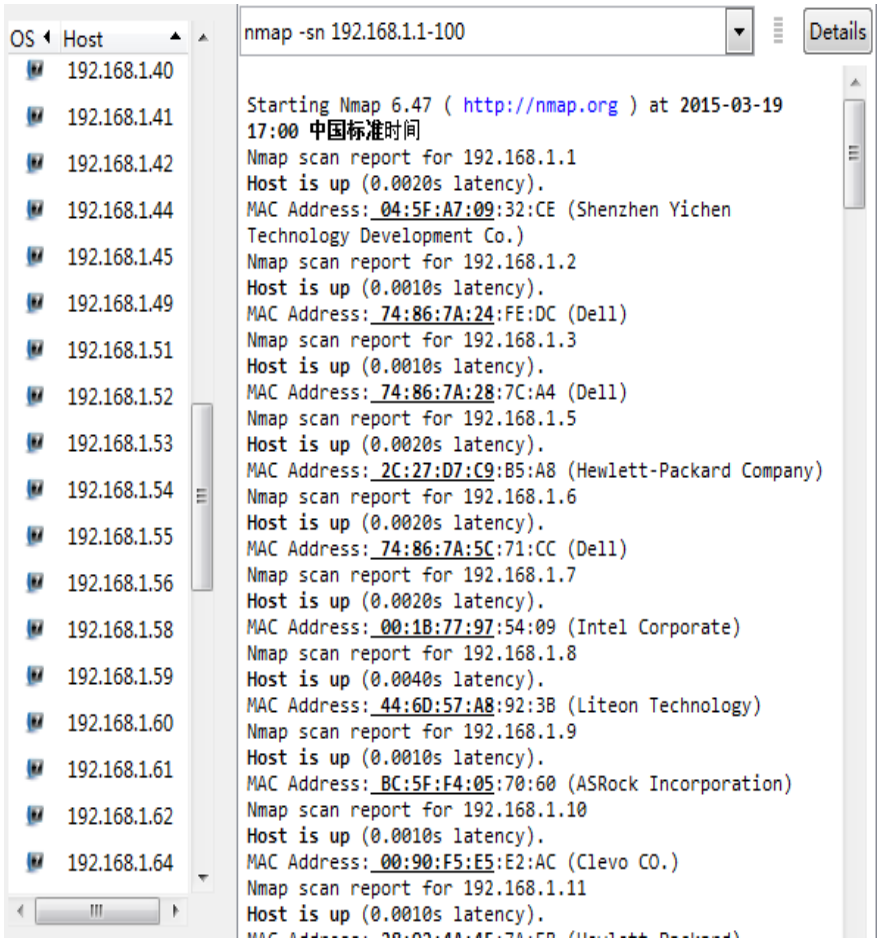
描。

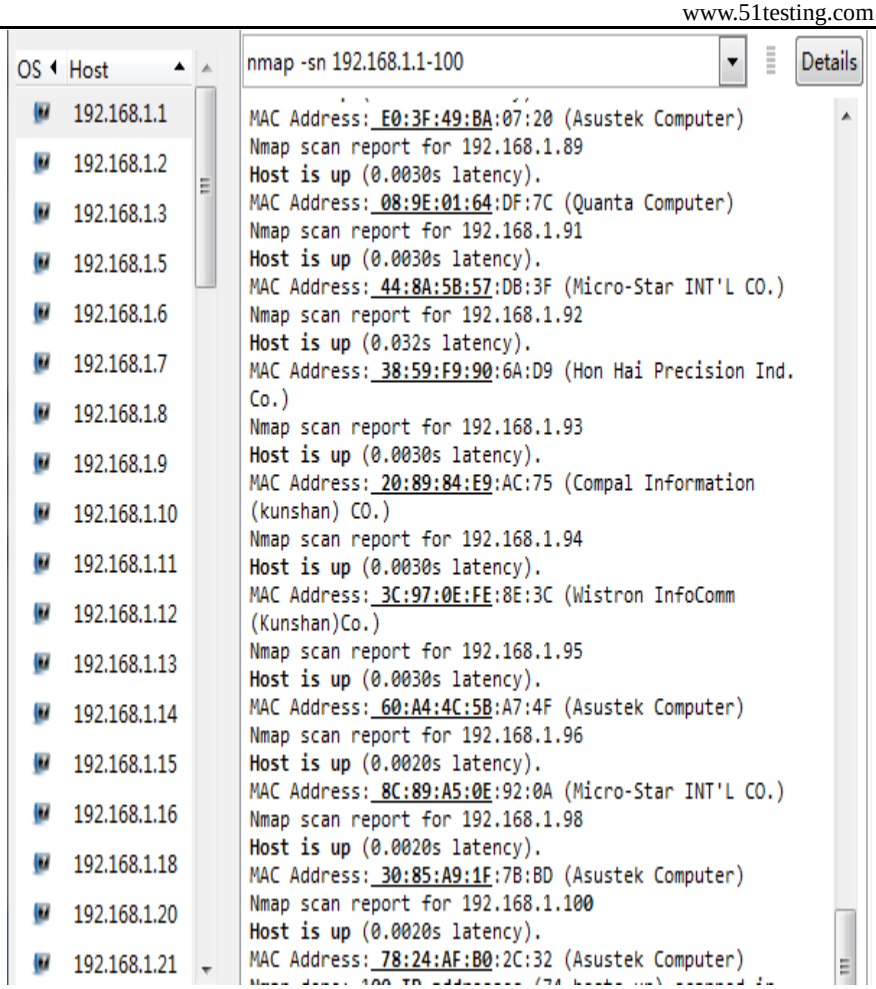
3、探测 www.baidu.com



4、扫面局域网内活动主机

nmap –sn 192.168.1.1-100

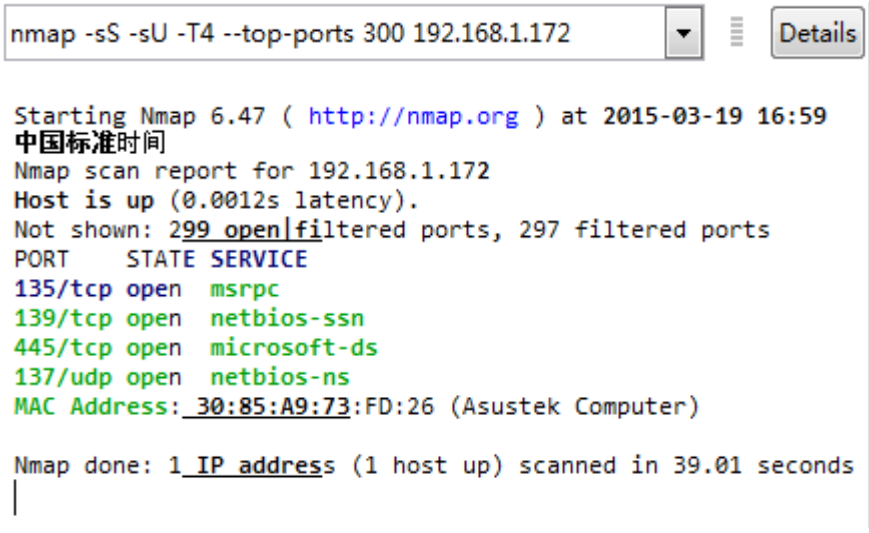




在局域网内，Nmap 是通过 ARP 包来询问 IP 地址上的主机是否活动的，如果收到 ARP 回复包，那么说明主机在线。

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



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

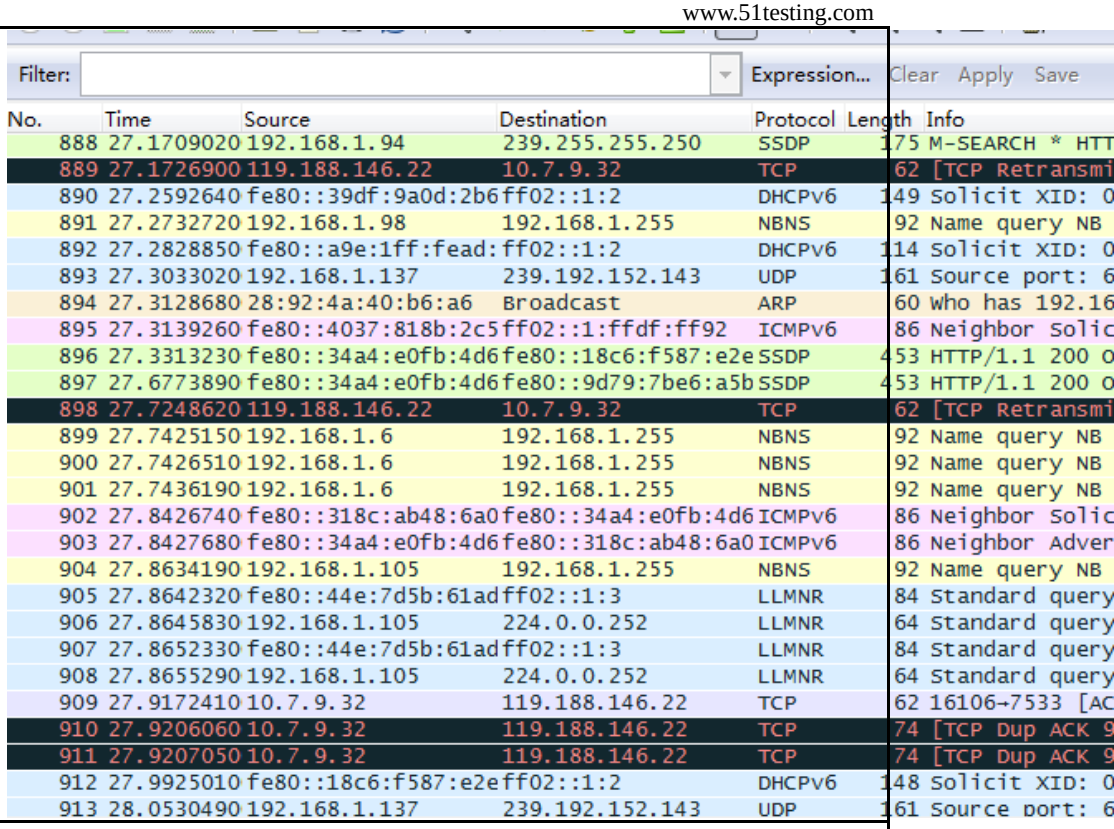
Namp –sV 192.168.1.172

```
nmap -sV 192.168.1.172                                    Details

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
445/tcp open  netbios-ssn
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                                     Details

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



实验总结	1、了解了主机、端口扫描的原理 2、基本掌握 Nmap 扫描器的使用 3、掌握 Nmap 进行远程 OS 检测的原理
指导教师意见	签名： 年　　月　　日