哈尔滨工业大学

计算机科学与技术学院

《信息安全概论》

实验报告

计算机科学与技术学院

计算机系网络教研室制

|  |  |
| --- | --- |
| 课程名称： | 信息安全概论 |
| 实验名称： | 基于nmap的网络信息扫描原理与设计 |
| 指导教师： | 韩琦 |
| 学生姓名： | 陈三元 |
| 组 号： | 2-28 |
| 实验日期： | 18-04-18 |
| 实验地点： | 校园 |
| 实验成绩： |  |

一、实验目的

1、熟悉TCP、UDP协议基础；

2、掌握nmap扫描原理，能够使用命令行与图形界面进行信息收集；

3、熟练使用nmap常用参数对不同网络环境进行端口扫描，并通过扫描结果对目标进行分析。

二、实验环境

实验环境为一台Windows主机。

三、实验内容与实验要求

1、安装Nmap

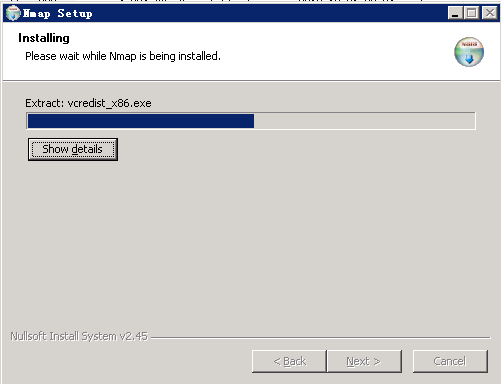
2、Zenmap图形基本应用

3、nmap命令行的使用

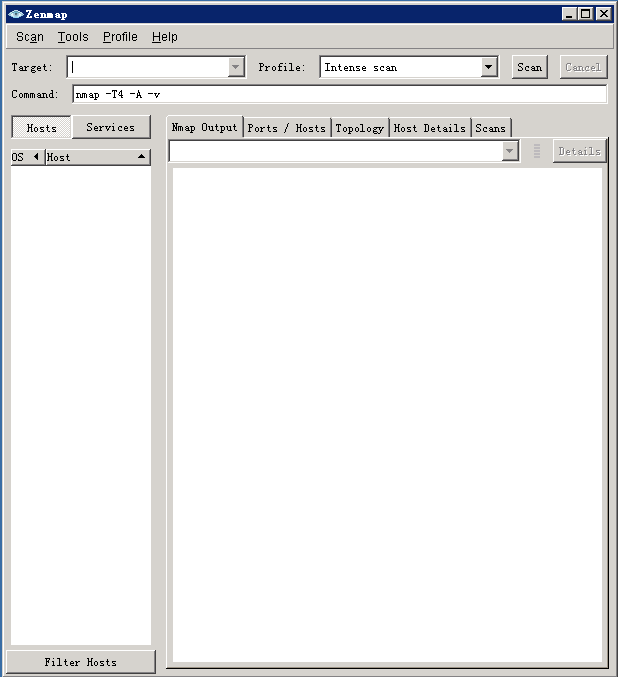
四、实验过程与分析

1、安装Nmap

使用远程桌面登录到实验主机，打开桌面tools文件夹，找到nmap安装文件nmap-6.25-setup.exe，双击进行正常安装。



安装完成后桌面会自动添加一个nmap的快捷方式，双击该图标会出现nmap的主界面：



2、Zenmap图形基本应用

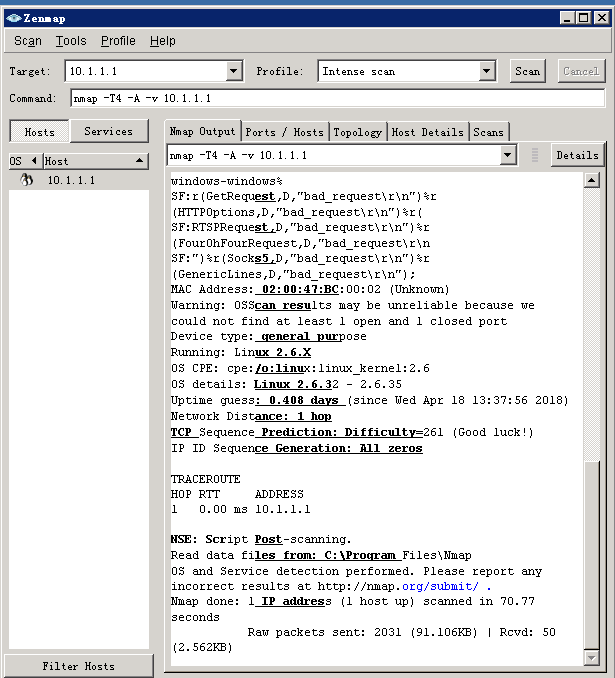
2.1、查找本机网关

打开cmd控制台，在控制台中输入ipconfig /all，查看本机网关信息。



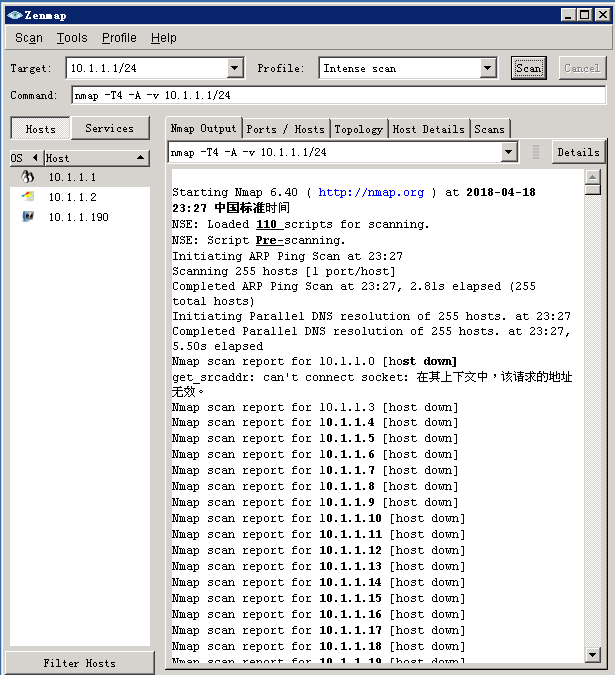
由图可知，本机的IP地址为10.1.1.190，网关地址为10.1.1.1

2.2、在zenmap界面中将扫描目标10.1.1.1填写入targe项，不修改参数直接点击scan，等待返回扫描结果。



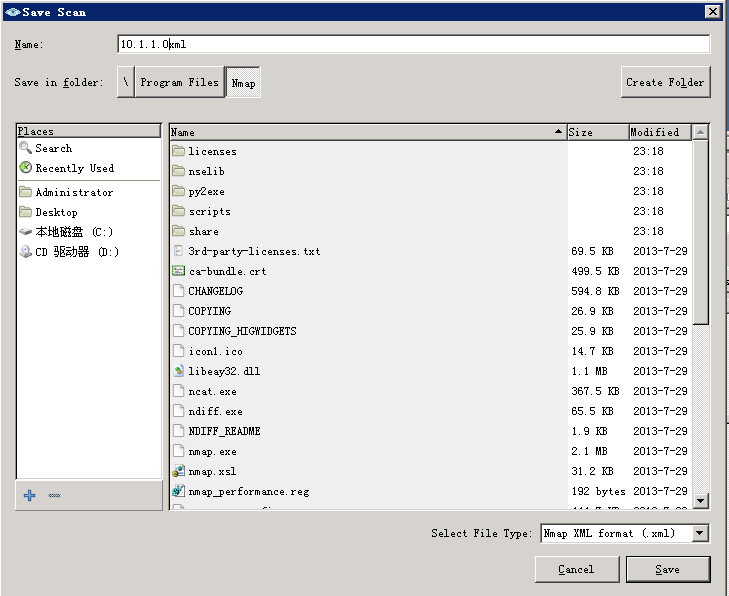
2.3、整网段扫描

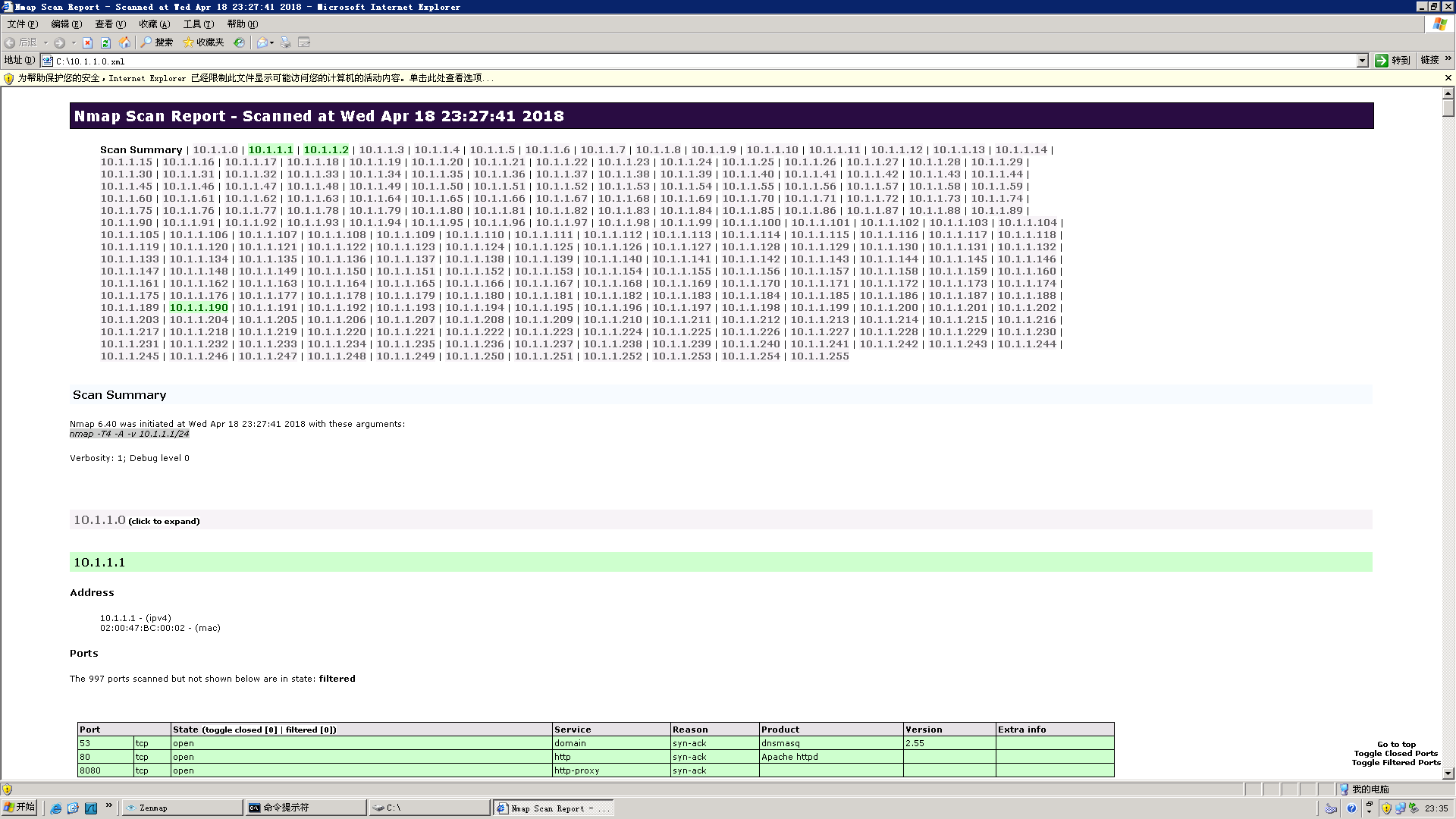
在扫描目标中输入：10.1.1.0/24，然后运行扫描任务。对本机所处网段进行扫描。任务停止后查看返回结果。



在host中列举本网段中所有存活主机，OS项指明该主机的操作系统，点击相关主机即可查看主机的详细信息。

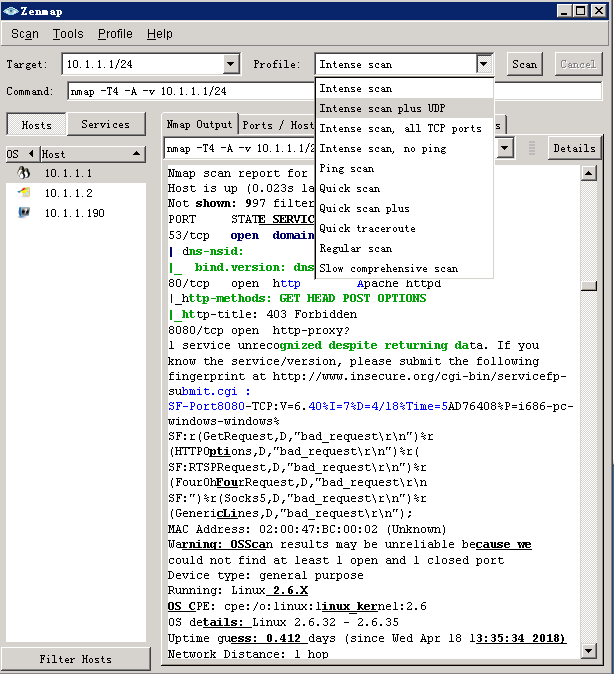
选择“scan”菜单中“Save Scan”选项保存扫描结果，保存类型选用默认的XML格式。



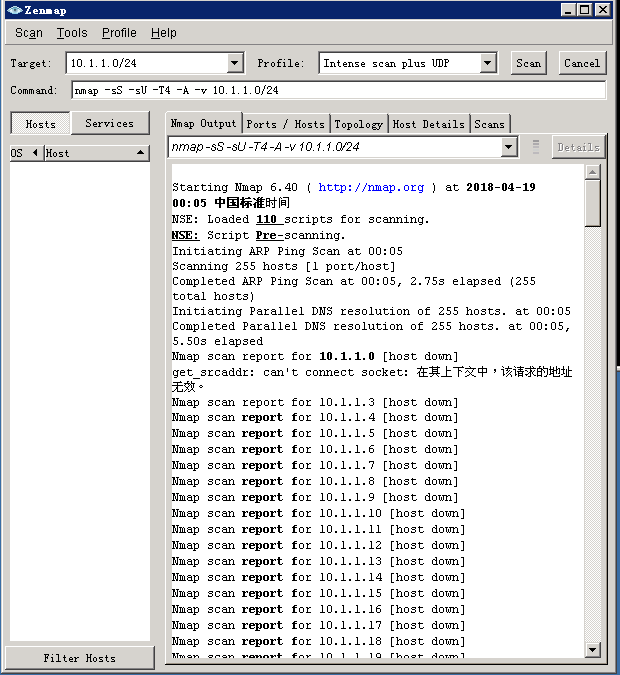


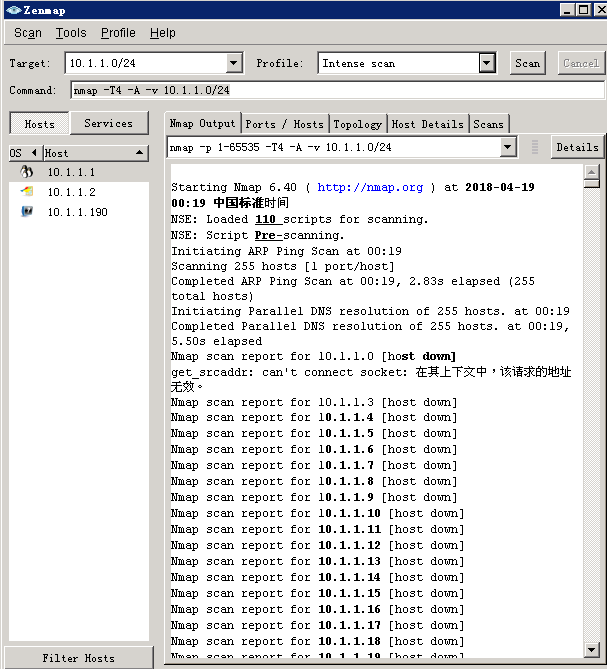
返回的扫描信息进行分析，分析网段中所有主机的相关信息，分析结果见实验结果总结。

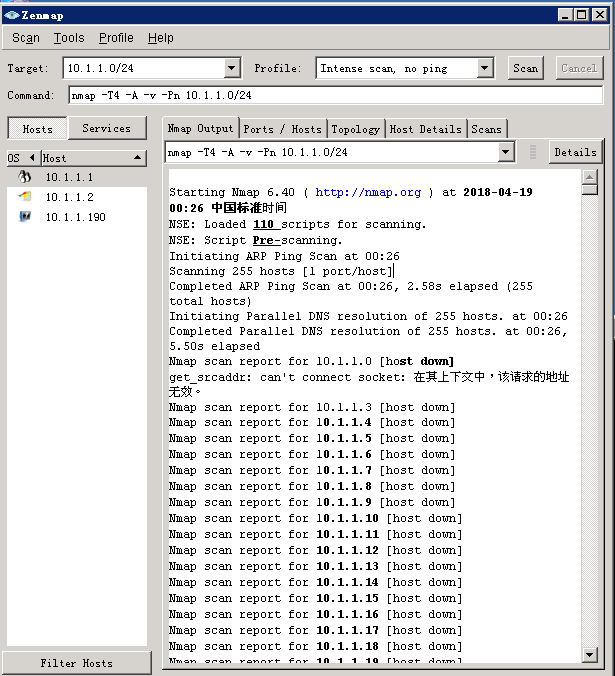
2.4、在zenamp界面选择不同的profile重新对目标10.1.1.1进行扫描：

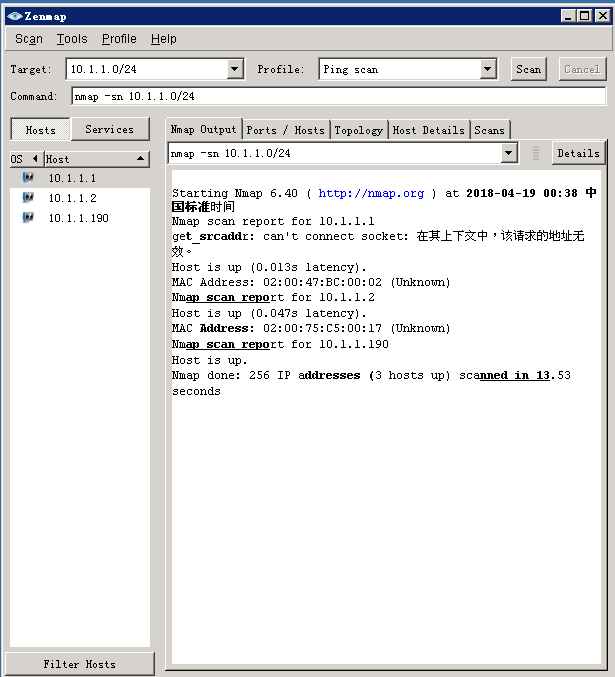


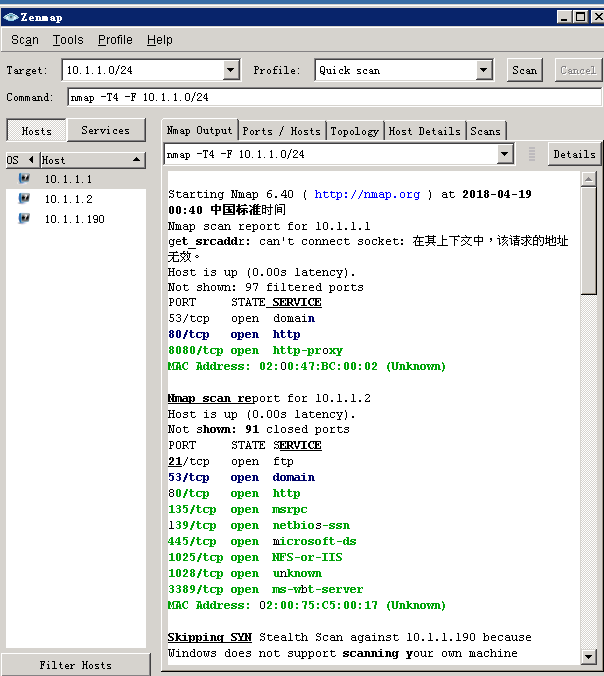
2.5、对每种“Profile”进行测试，观察返回结果有何不同，分析结果见实验结果总结。

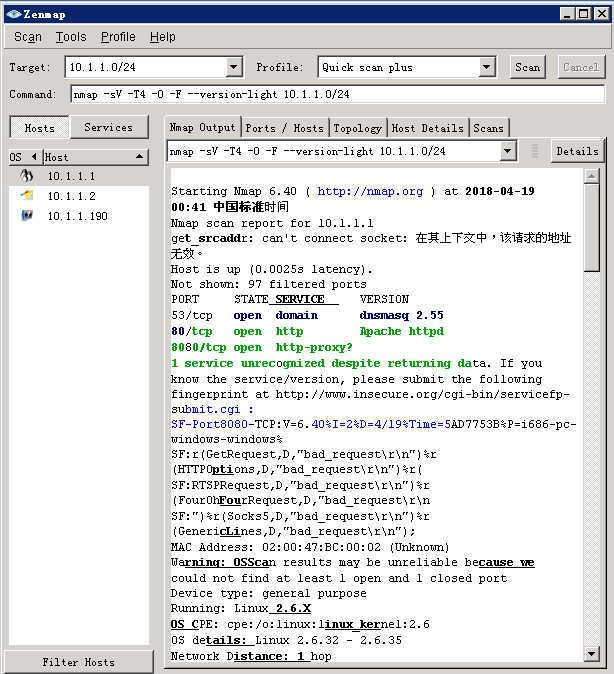


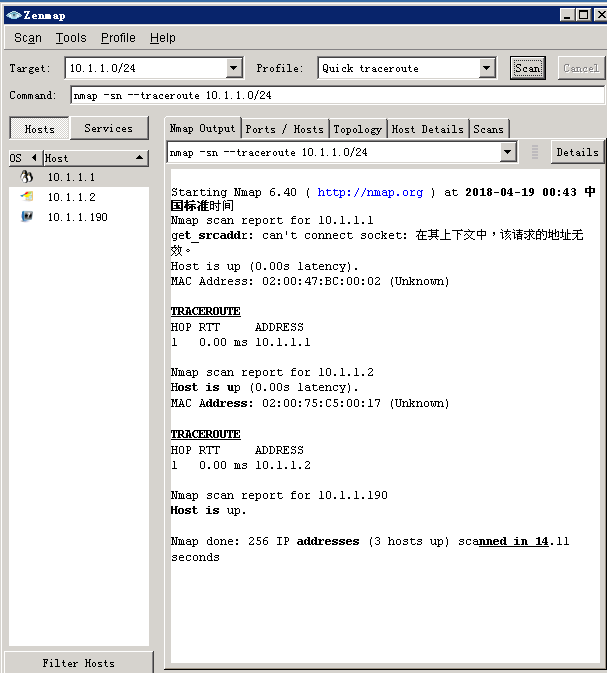


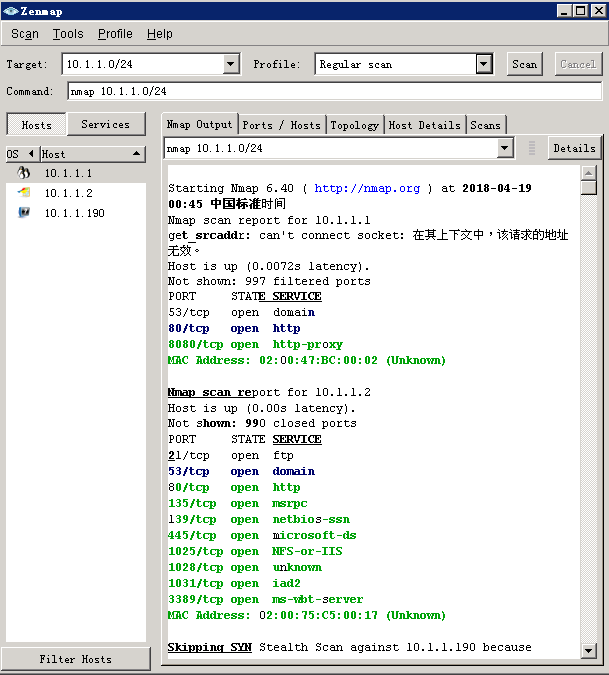


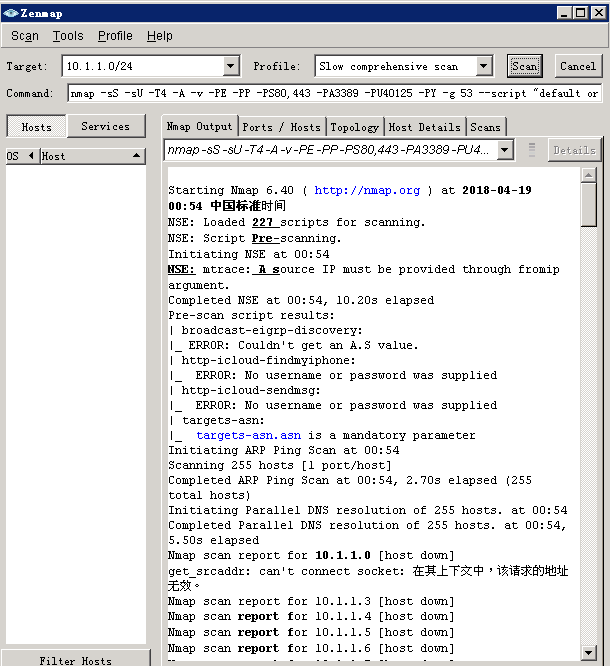






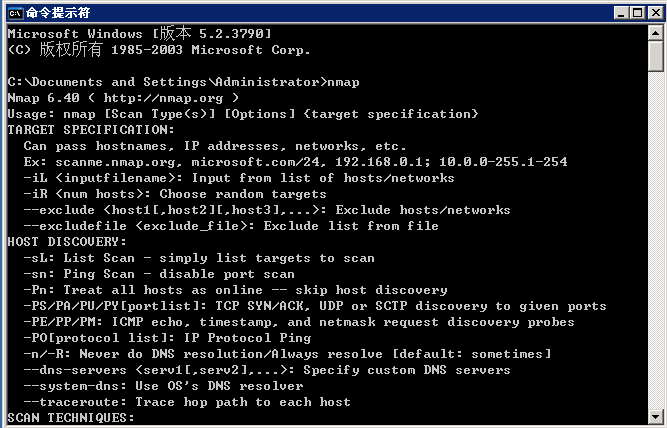






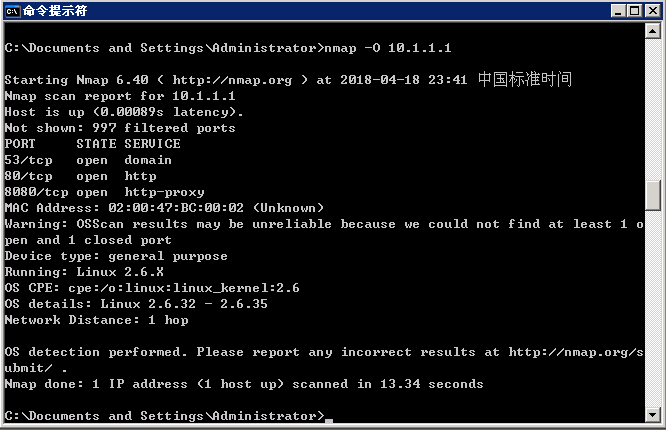
3、nmap命令行的使用

3.1、关闭图形界面的zenmap，打开cmd，在cmd下输入nmap命令，nmap会返回使用说明。



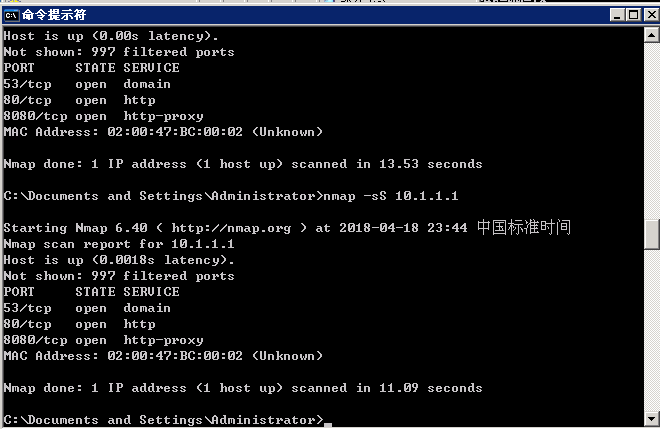
3.2 判断10.1.1.1的操作系统

nmap –O 10.1.1.1



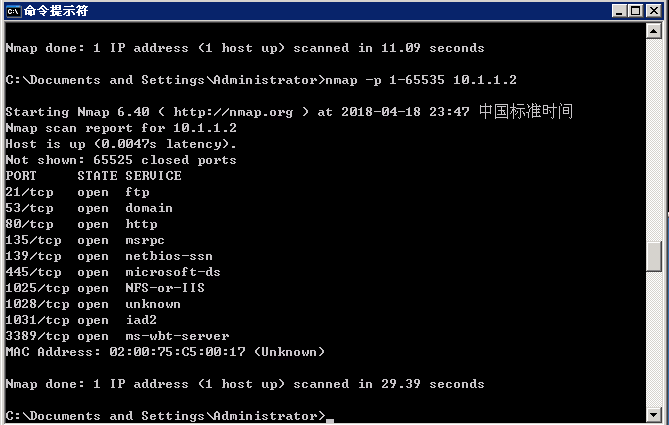
3.3 在测试中为了不在服务器10.1.1.1上留下连接痕迹，采用半开扫描

nmap –sS 10.1.1.1



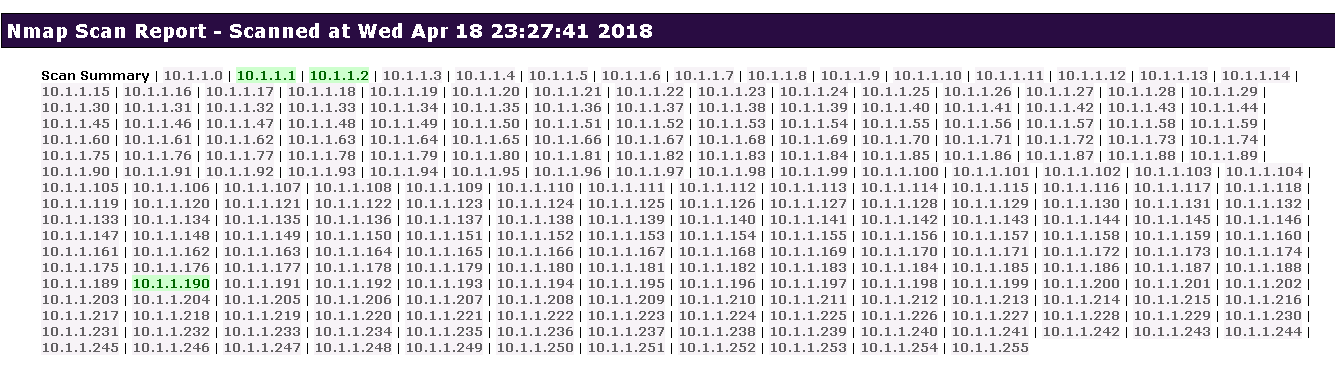
3.4 扫描目标主机10.1.1.2所有端口（1-65535）

nmap –p 1-65535 10.1.1.2



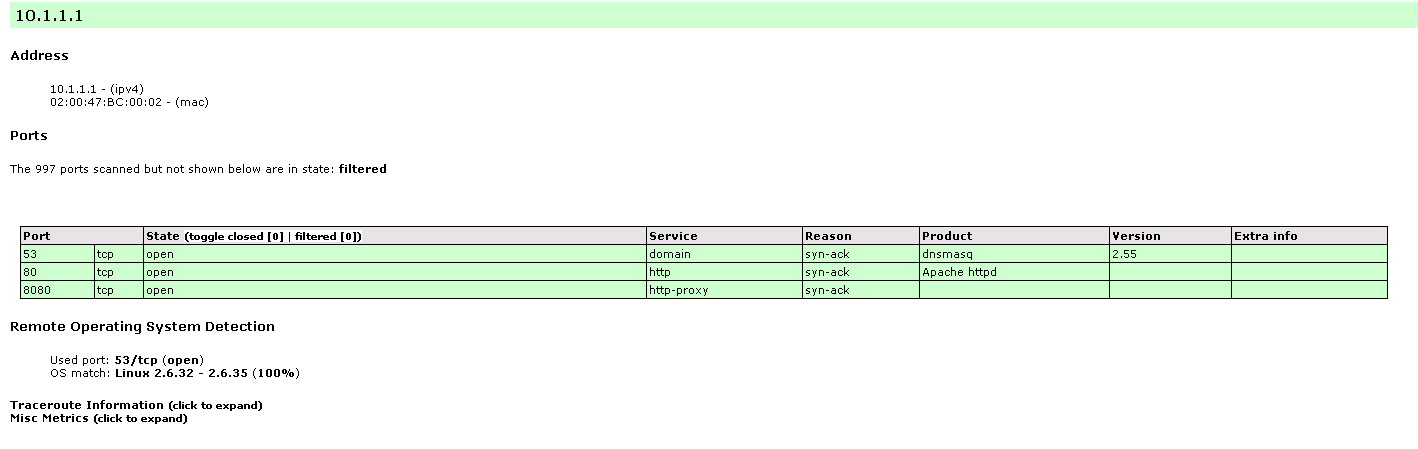
五、实验结果总结

2.3 分析10.1.1.0/24网段中所有主机的相关信息:

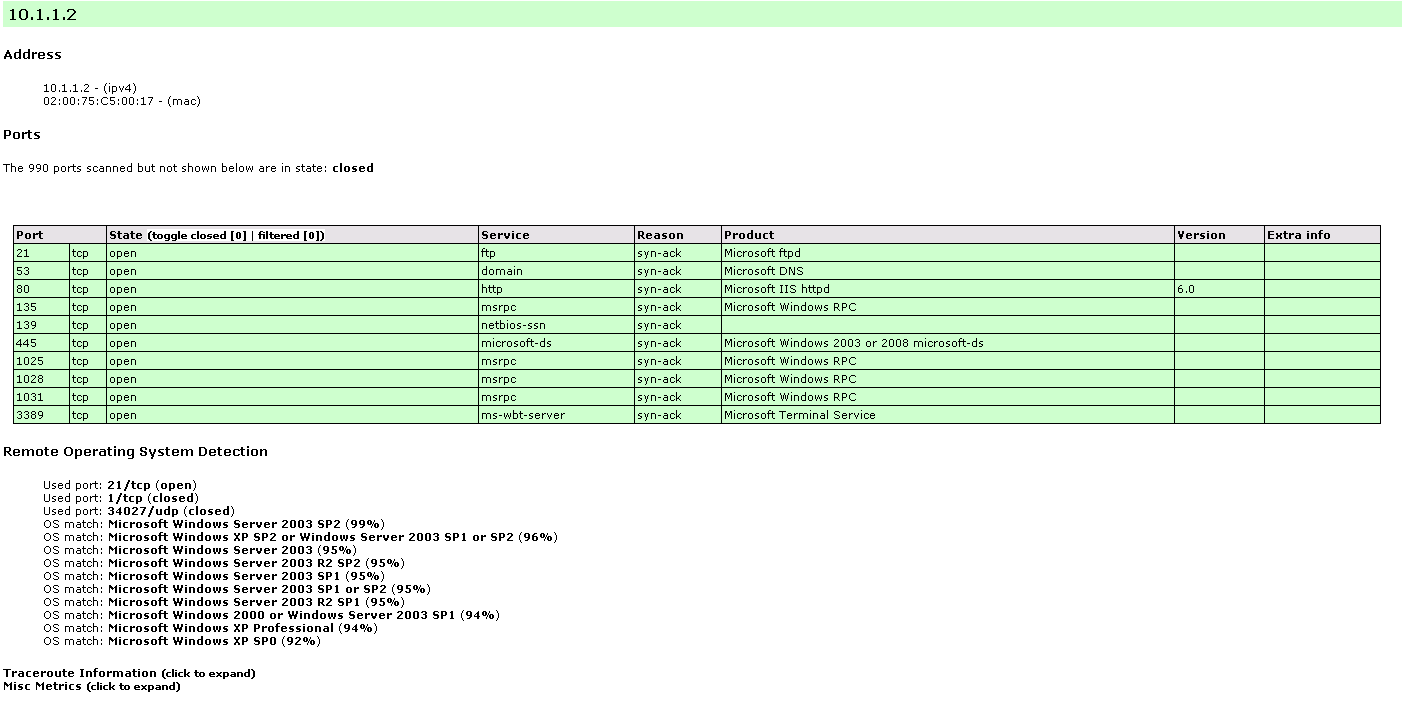


由图扫描结果可知，只有在ip address为10.1.1.1，10.1.1.0和10.1.1.190扫描到主机。

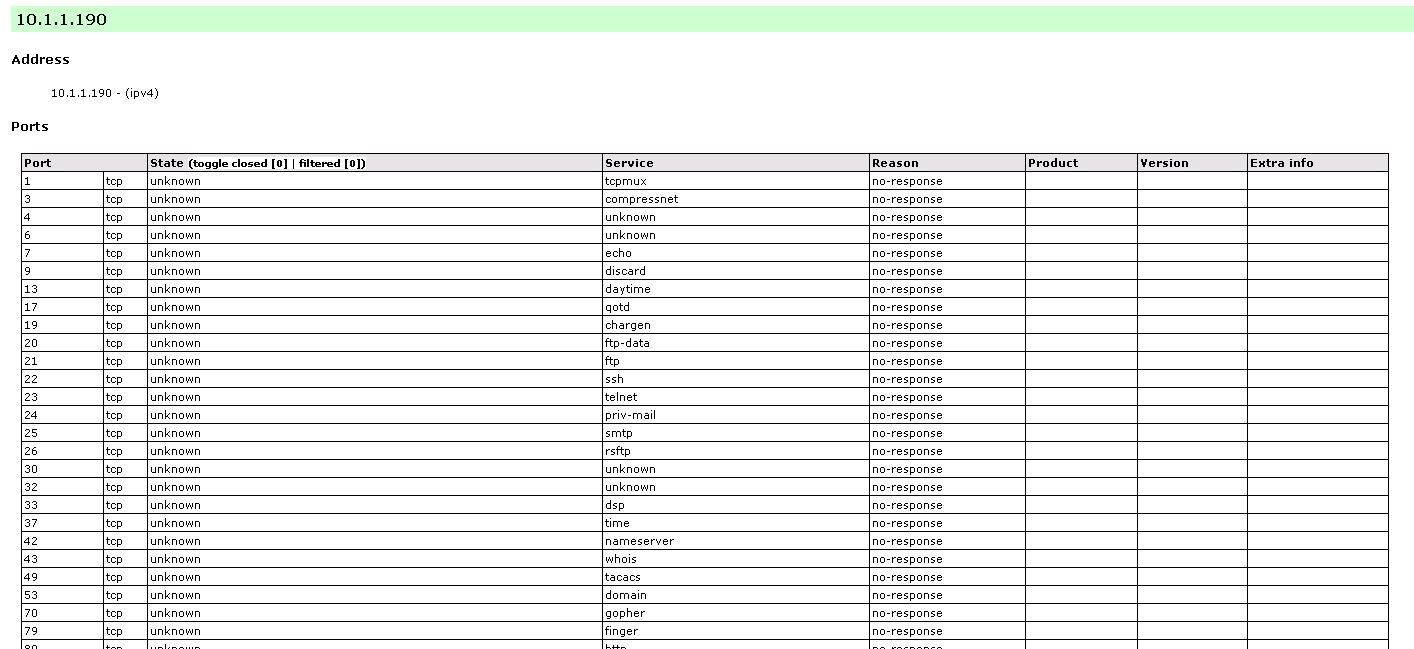
IP address为10.1.1.1中各端口的相关信息如下：



IP address为10.1.1.2中各端口的相关信息如下：



IP address为10.1.1.190中各端口的相关信息如下：



2.5 分析不同profile:

1. Intense Scan：适用在局域网，可靠性网络进行扫描，略带侵略性，扫描一个tcp端口平均耗时10ms，可以满足一般扫描需求。扫描速度较快，输出信息有操作系统及版本探测，有详细的输出信息。
2. Intense Scan, plus UDP：加上UDP协议的intense scan。TCP SYN scan是一种半开方式扫描，并没有完成一个完整真实的tcp连接，运行扫描快，而且隐蔽。发送SYN包，如果收到一个SYN/ACK（或SYN）响应包则说明对方该端口处于打开监听状态；如果是RST,则说明对方端口处于非监听状态；如果未收到任何响应包则标记该端口被过滤。UDP scan的服务主要有DNS,SNMP,DHCP等，由于UDP扫描更困难和耗费时间因此一些审计的时候进行了省略，困难点在于linux和Solaris系统默认限制了每秒不可到达的信息数，Nmap为了避免造成服务器掉包的危害降低发包的速度，因此在扫描时将会耗费非常多的时间，
3. Intense Scan, all TCP: 扫描所有TCP端口，范围在1-65535，试图扫描所有端口的开放情况，速度比较慢。
4. Intense Scan, no ping对目标进行强烈的扫描，不进行主机发现。假设所有主机在线，跳过主机发现过程。
5. Ping scan在发现主机后，不进行端口扫描。速度快，但是容易被防火墙屏蔽，导致无扫描结果。
6. Quick Scan：对常用的1000个端口进行扫描。
7. Quick scan plus：Quick scan的加强模式,可以扫描端口及版本服务信息以及OS检测信息。
8. Quick traceroute：快速扫描，显示本机到目标主机的路由跃点。
9. Regular scan：规则扫描
10. Slow comprehensive scan：慢速全面扫描，会最大限度地避过防火墙等安全设备的检测。

3.5 不同profile对应的参数分析：

Intense scan: nmap -T4 -A -v targethost

-T4: set timing template as 4

-A: enable os detection, version detection, script scanning and traceroute

-v: increase verbosity level

Intense scan plus UDP: nmap -sS -sU -T4 -A -v targethost

-sS: TCP SYN scans

-sU: UDP scans

-T4: set timing template as 4

-A: enable os detection, version detection, script scanning and traceroute

-v: increase verbosity level

Intense scan, all TCP ports: nmap -p 1-65535 –T4 –A –v targethost

-p 1-65535: only scan ports 1-65535

-T4: set timing template as 4

-A: enable os detection, version detection, script scanning and traceroute

-v: increase verbosity level

Intense scan, no pings: nmap -T4 -A -v -Pn targerhost

-T4: set timing template as 4

-A: enable os detection, version detection, script scanning and traceroute

-v: increase verbosity level

-Pn: treat all hosts as online

Ping scan: nmap -sn targethost

-sn: ping scan

Quick scan: nmap -T4 -F targethost

-T4: set timing template as 4

-F: fast mode

Quick scan plus: nmap -sV -T4 -O -F --version-light targethost

-sV: probe open ports to determine service/version info

--version-light: limit to most likely probes

-T4: set timing template as 4

-O: enable os detection

-F: fast mode

Quick traceroute: nmap -sn --traceroute targethost

-sn: Ping scan

--traceroute: trace hop path to each host

Regular scan: nmap targethost

Slow comprehensive scan: nmap -sS -sU -T4 -A -v -PE -PP -PS80.443 -PA3389 -PU40125 -PY -g 53 --script “default or (discovery and safe)” targethost

-sS: TCP SYN scans

-sU: UDP scans

-T4: set timing template as 4

-A: enable os detection, version detection, script scanning and traceroute

-v: increase verbosity level

-PE: ICMP echo

-PP: ICMP timestamp

-PS80.443: TCP SYN/ACK to port 80.443

-PA3389: UDP to port 3389

-PU40125: UDP to port 40125

-PY -g 53: SCTP discovery to port 53

思考题：

1. 对局域网中主机扫描与互联网扫描有什么区别？应该怎样选择相应参数？
2. 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从而进行主机扫描。

如扫描局域网10.1.1.0/24范围内有哪些ip的主机是活动的，命令为: nmap -sn 10.1.1.0/24。

1. 对于互联网扫描，nmap能够通过利用多种不同的扫描方式，扫描主机TCP/UDP端口的开放情况(open/closed/filtered/unfiltered)。

具体有：TCP SYN scanning(发送SYN到目标端口，通过收到的封包类型确定端口的开放情况)、TCP connect scanning（用TCP connect的方式向目标主机发起连接，来判断端口的开放情况）、TCP ACK scanning（发送ACK包到目标端口，通过是否能收到PST包判断端口的开放情况）等。

参数选择有：-sS/sT/sA/sW/sM:指定使用 TCP SYN/Connect()/ACK/Window/Maimon scans的方式来对目标主机进行扫描; -sU: 指定使用UDP扫描方式确定目标主机的UDP端口状况; -sN/sF/sX: 指定使用TCP Null, FIN, and Xmas scans秘密扫描方式来协助探测对方的TCP端口状; --scanflags <flags>: 定制TCP包的flags; -sI <zombiehost[:probeport]>: 指定使用idle scan方式来扫描目标主机（前提需要找到合适的zombie host）; -sY/sZ: 使用SCTP INIT/COOKIE-ECHO来扫描SCTP协议端口的开放的情况; -sO: 使用IP protocol 扫描确定目标机支持的协议类型; -b <FTP relay host>: 使用FTP bounce scan扫描方式。

2）如果你是网络管理员，为了防止其他人扫描你管理的服务器以获取信息，有哪些解决办法？

尽量伪装好自己的服务器上我服务，具体手段有：

1. 禁用ICMP，防止别人通过网络工具获取网络拓扑图
2. 局域网的多台服务器之间禁止公网IP访问
3. 没有必要对外公开的信息就不要给外界权限访问
4. 对外尽量使用代向代理，不要暴露过多端口信息