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： | 马玉坤 |
| 组 号： | 3-19 |
| 实验日期： | 2018年4月20日-2018年4月21日 |
| 实验地点： | 哈尔滨工业大学 |
| 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

本实验的实验环境为一台Windows主机。

三、实验内容与实验要求

实验内容

1. 安装Nmap

实验目的：掌握windows下nmap的安装方法。

* 1. 查找本机网关
  2. 等待返回扫描结果
  3. 整网段扫描

1. Zenmap图形基本应用

实验目的：通过扫描本机网关熟悉nmap基本运行环境

1. nmap命令行的使用

实验目的：掌握nmap命令行下常用的参数

****预备知识****

1. **TCP与UDP**

      TCP是一种面向连接（连接导向）的、可靠的、基于字节流的运输层通信协议；UDP协议的全称是用户数据报协议，在网络中它与TCP协议一样用于处理数据包，是一种无连接的协议。

1. **建立TCP连接的三次握手：**

      第一次握手：建立连接时，客户端发送syn包（syn=j）到服务器，并进入SYN\_SENT状态，等待服务器确认；SYN：同步序列编号（Synchronize Sequence Numbers）。

      第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入SYN\_RECV状态；

      第三次握手：客户端收到服务器的SYN+ACK包，向服务器发送确认包ACK(ack=k+1），此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

      完成三次握手，客户端与服务器开始传送数据。

1. **扫描的分类**

      常规扫描，通过TCP的三次连接进行扫描；

      半打开扫描，没有完成三次连接进行扫描；

      UDP扫描，由扫描主机发出 UDP 数据包给目标主机的UDP Port ，并等待目标主机 Port 送回ICMP Unreachable信息。

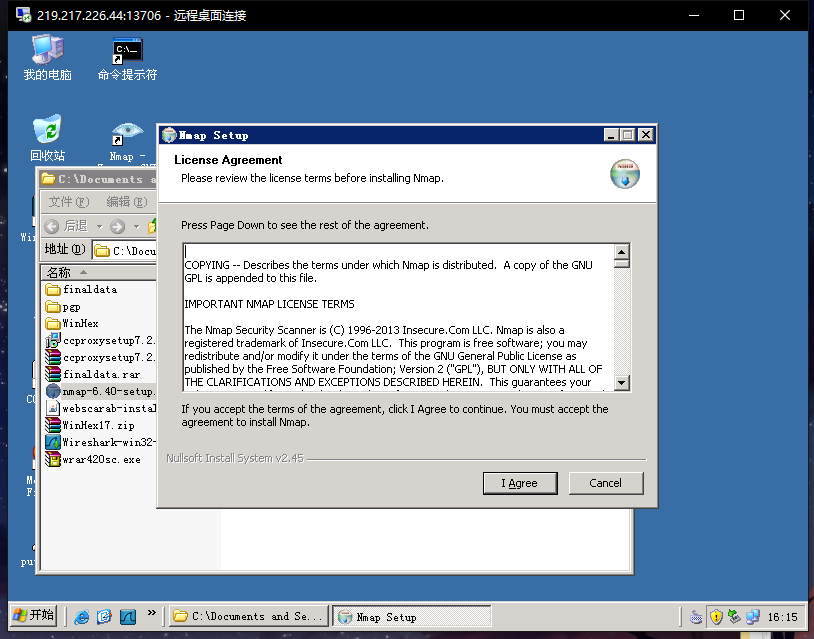
1. **nmap简介**

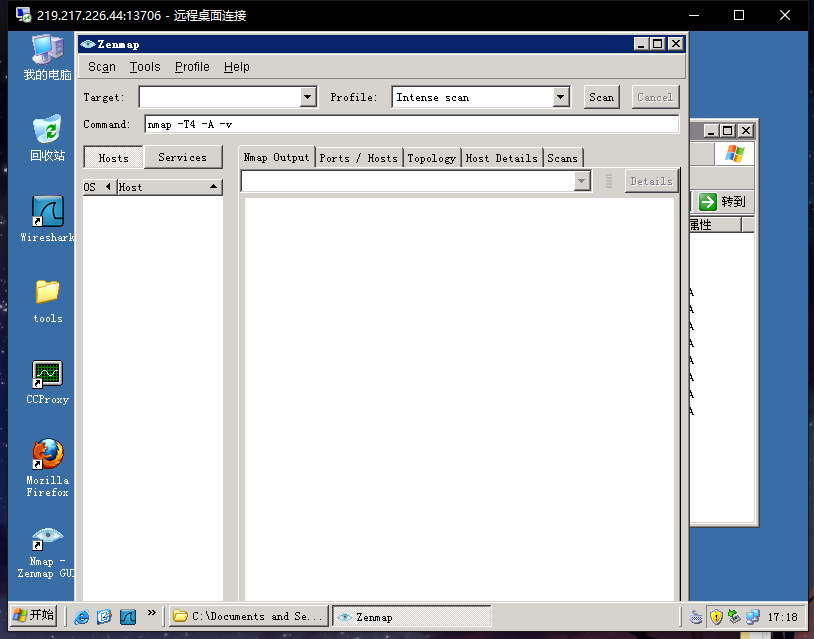
      nmap是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取主机正在运行以及提供什么服务等信息。nmap支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。从扫描类型一节可以得到细节。nmap还提供了一些高级的特征，例如：通过TCP/IP协议栈特征探测操作系统类型，秘密扫描，动态延时和重传计算，并行扫描，通过并行ping扫描探测关闭的主机，诱饵扫描，避开端口过滤检测，直接RPC扫描(无须端口影射)，碎片扫描，以及灵活的目标和端口设定。

四、实验过程与分析

任务一：安装Nmap

1. 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。

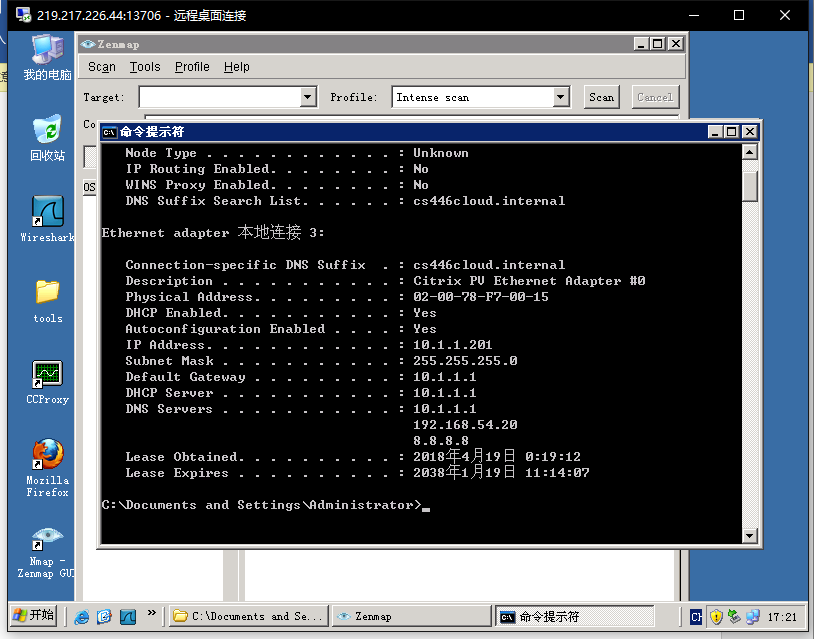




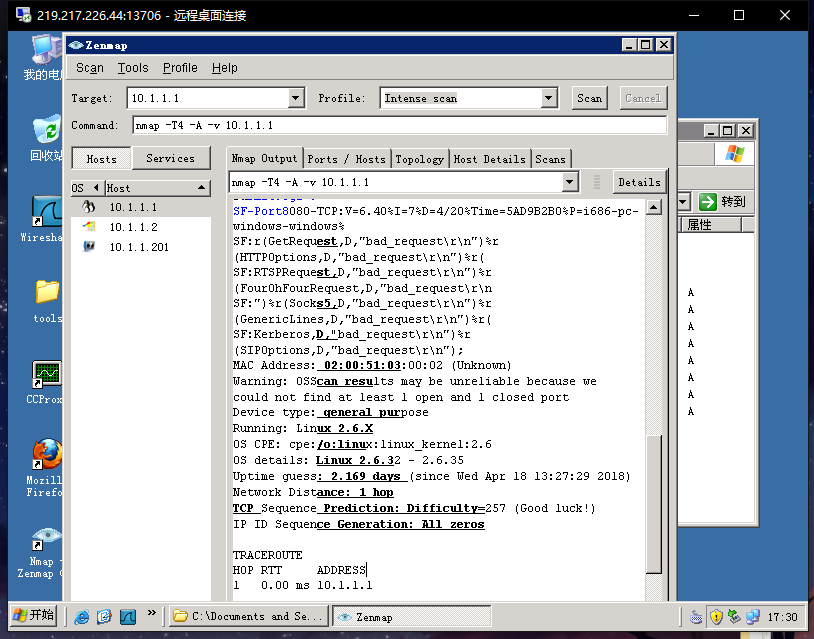
任务二：Zenmap图形基本应用

1. 查找本机网关

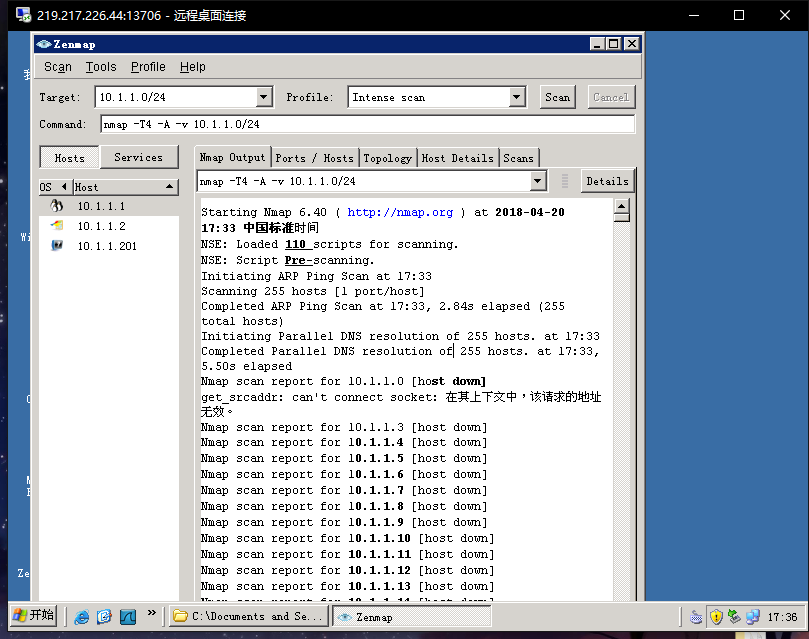
打开cmd控制台，在控制台中输入ipconfig /all，查看本机网关信息。从下图中可以看到，本机的IP地址为：10.1.1.201，网关地址为：10.1.1.1：



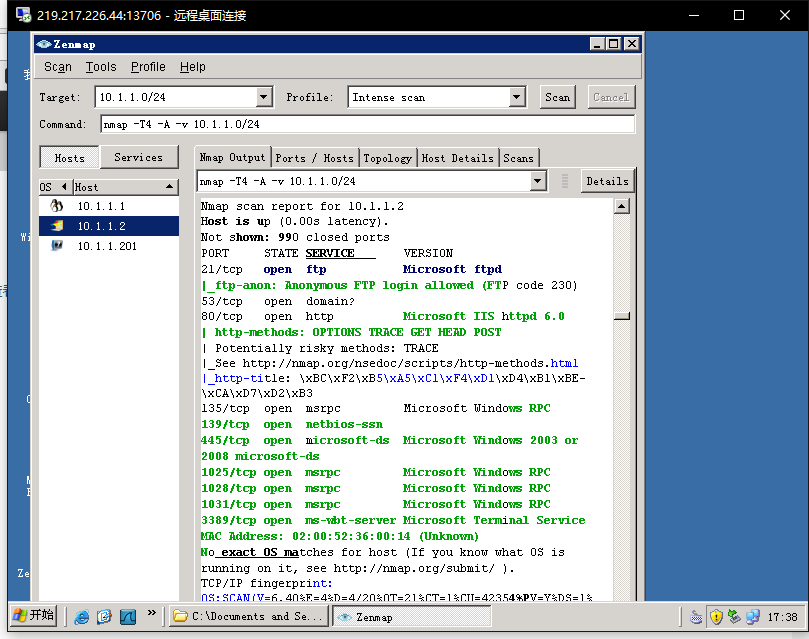
1. 在zenmap界面中将扫描目标10.1.1.1填写入targe项，不修改参数直接点击scan，等待返回扫描结果。



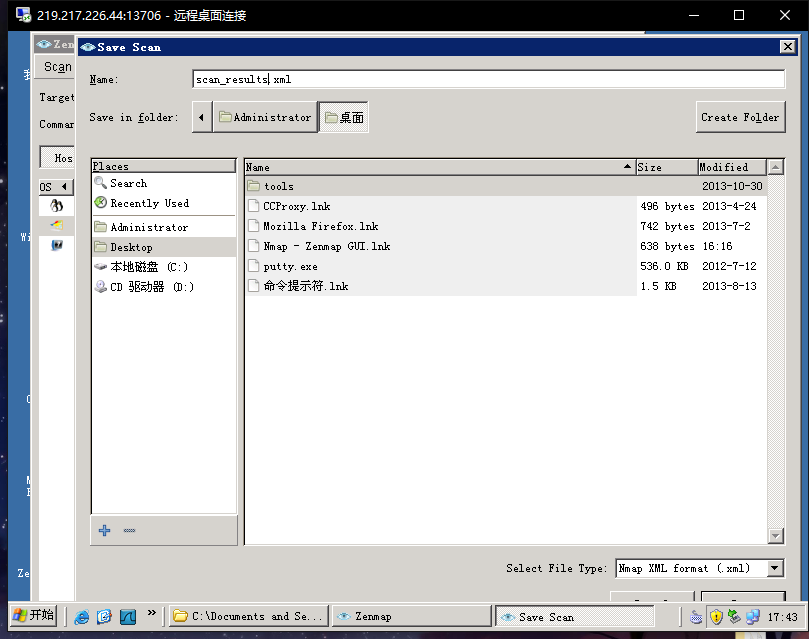
1. 对本机所处网段进行扫描，分析本网段环境，使用方法：在扫描目标中输入：10.1.1.0/24，然后运行扫描任务。扫描任务停止后查看返回结果。



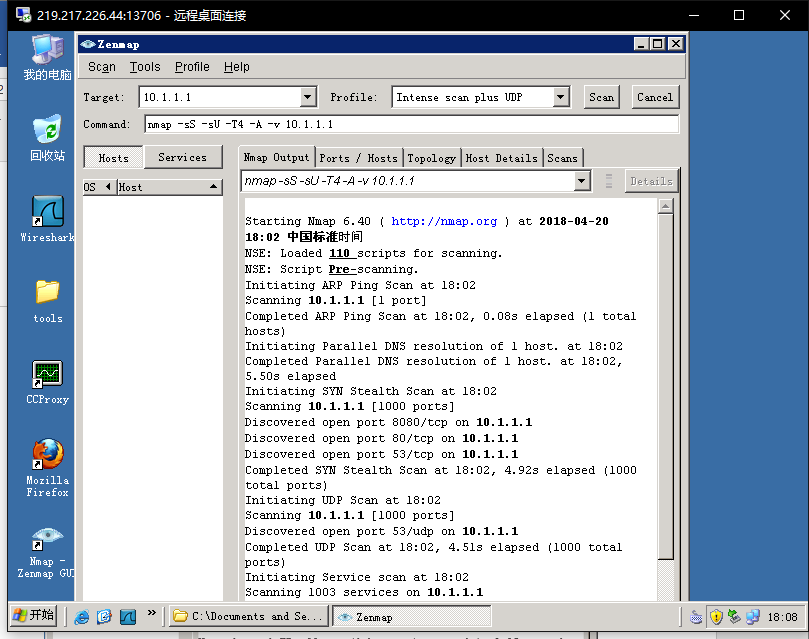
在host中列举本网段中所有存活主机，OS项指明该主机的操作系统，点击相关主机即可查看主机的详细信息。

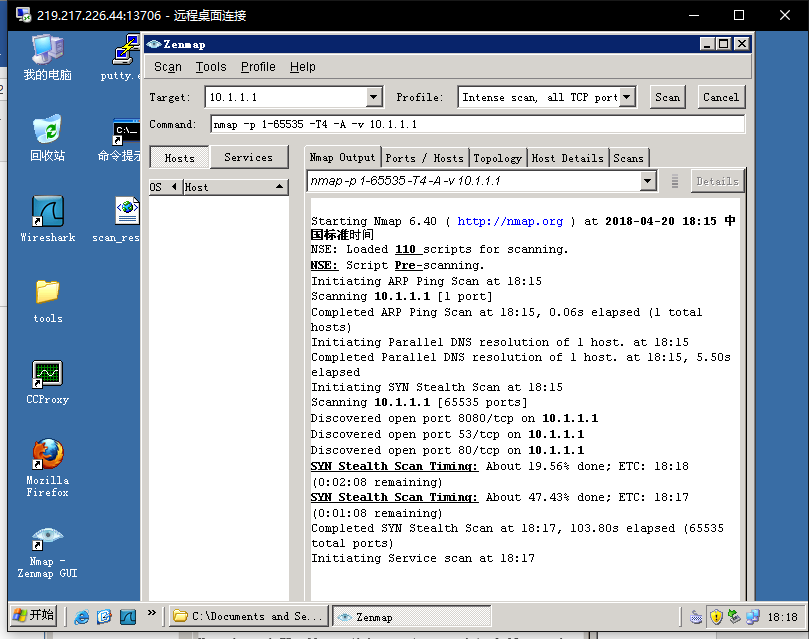


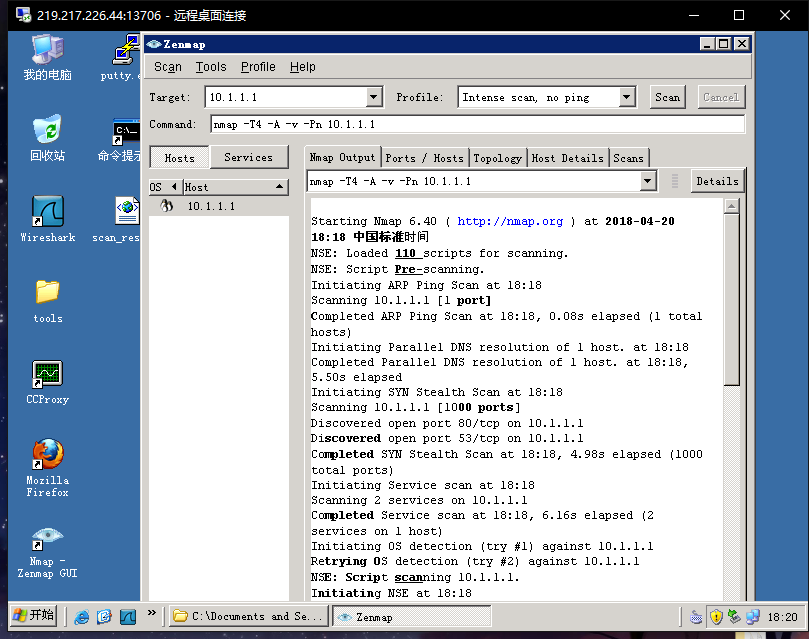
选择“scan”菜单中“Save Scan”选项保存扫描结果，保存类型选用默认的XML格式。

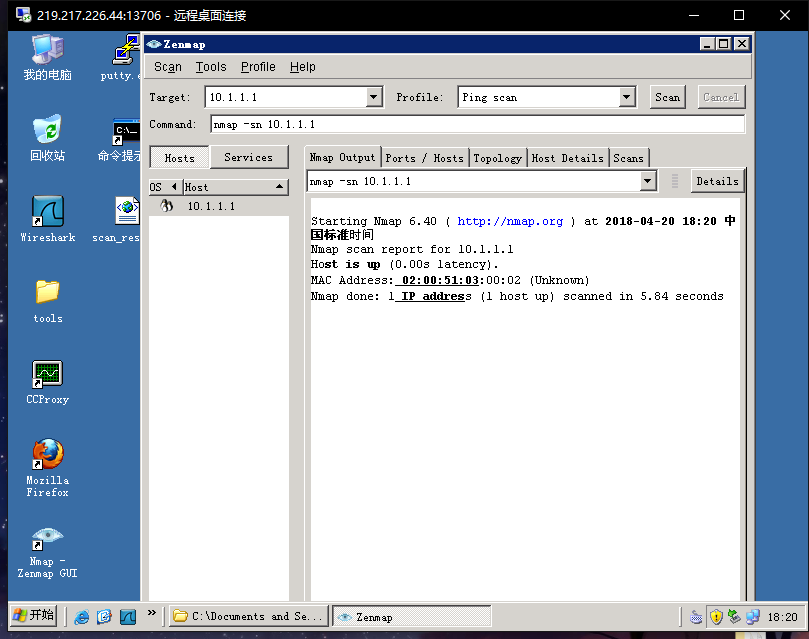


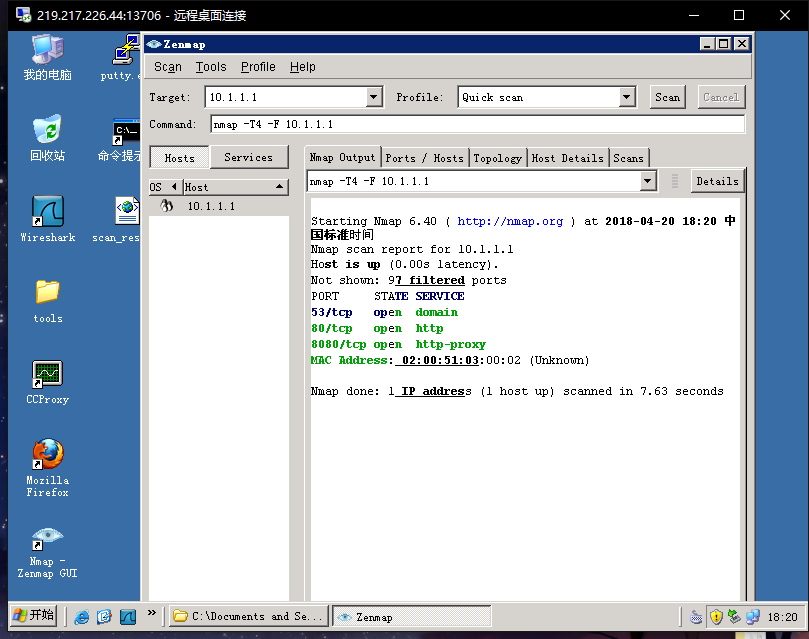
1. 在zenamp界面选择不同的profile重新对目标10.1.1.1进行扫描

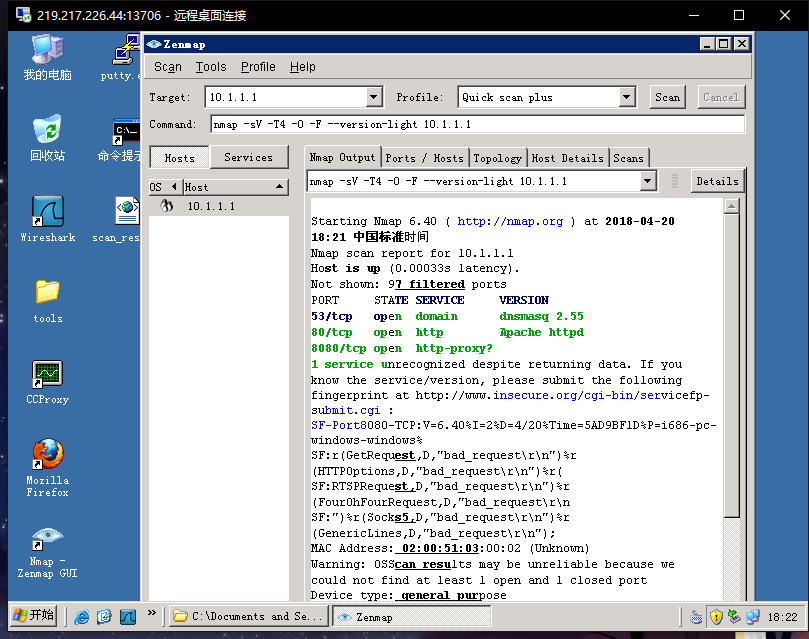


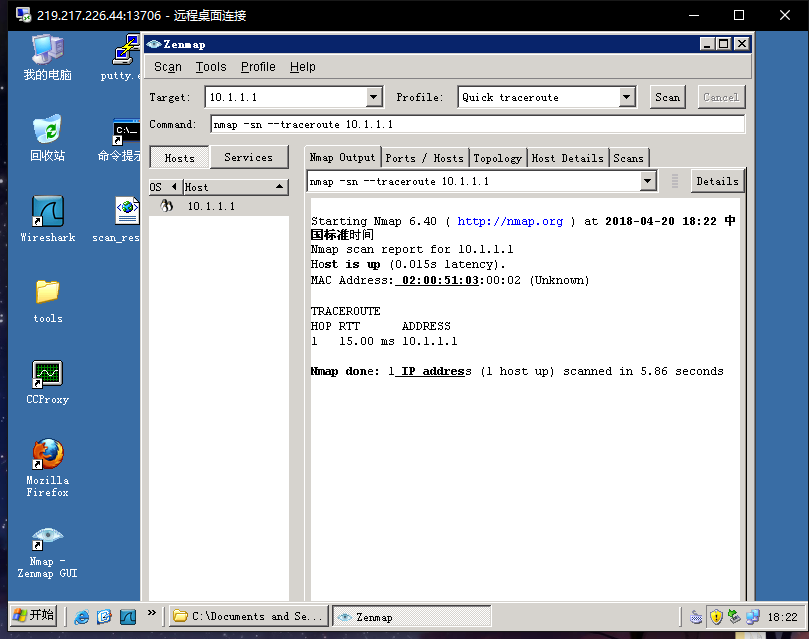


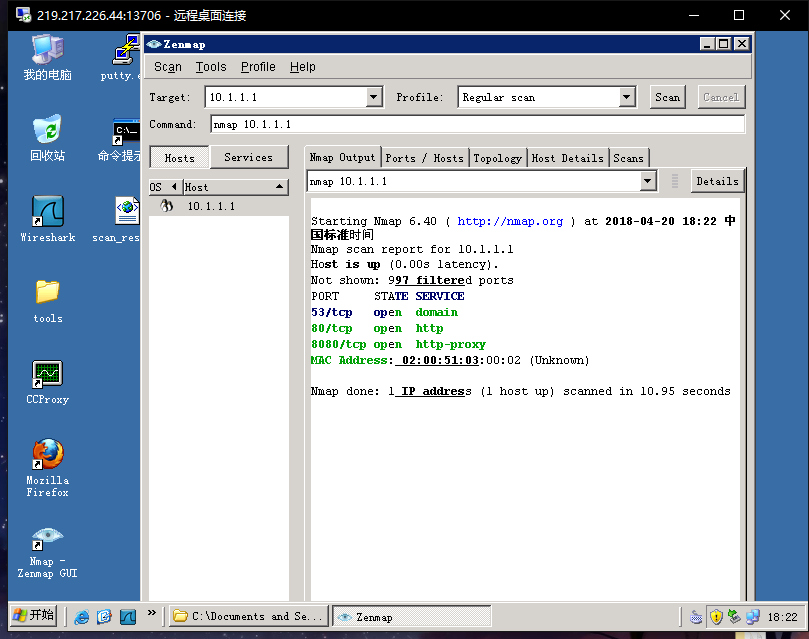


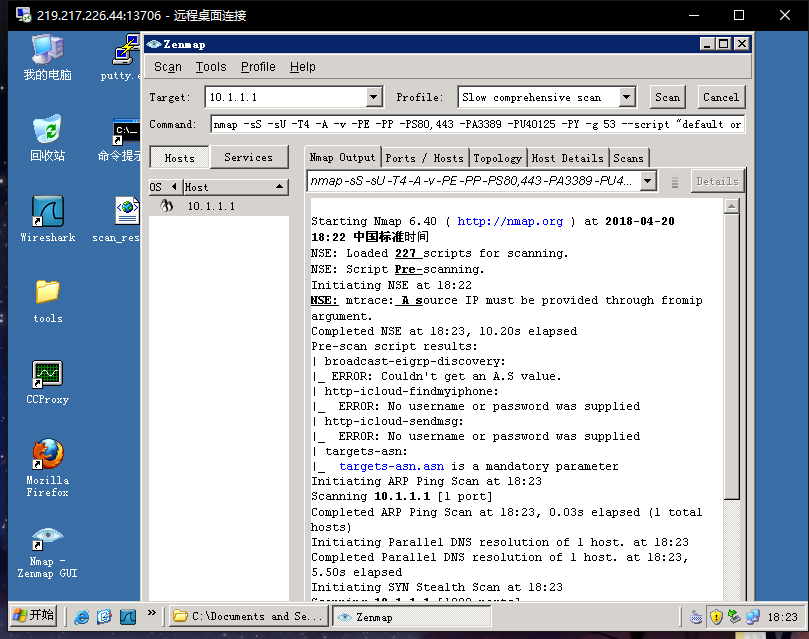






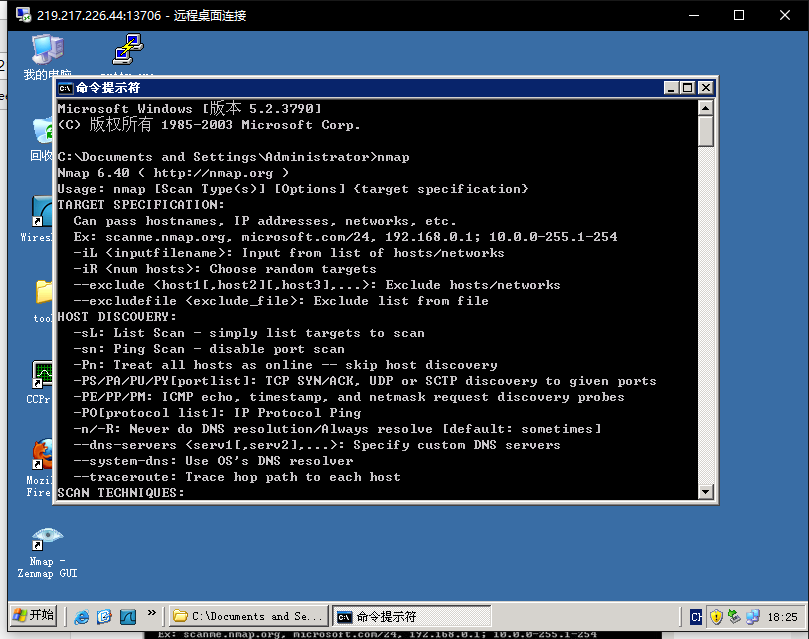


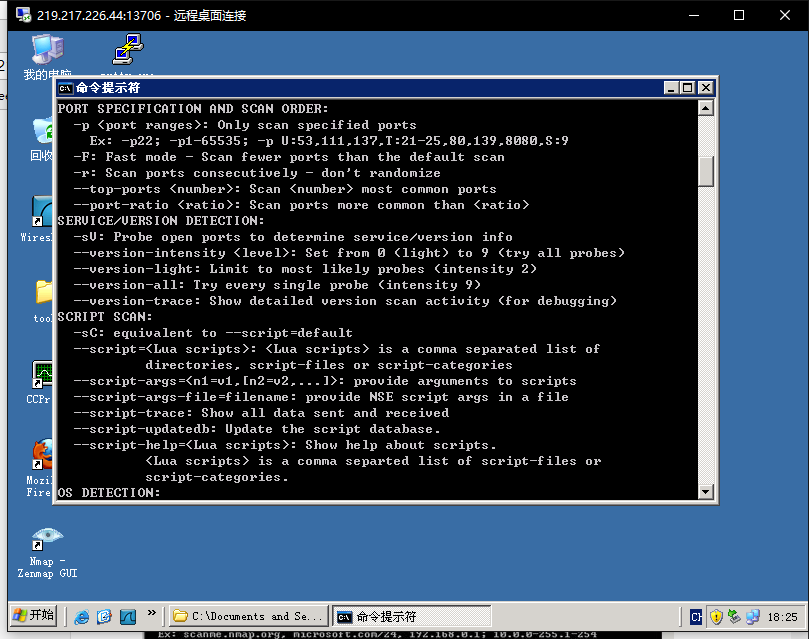




任务三：nmap命令行的使用

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。

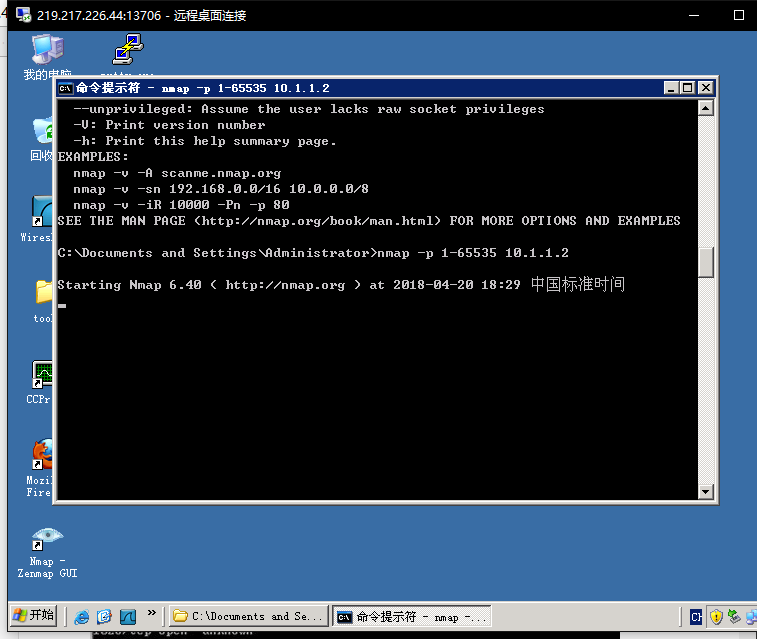




1. 扫描类型及参数

|  |  |
| --- | --- |
| -sT | TCP connect()扫描：这是最基本的TCP扫描方式。如果目标端口有程序监听，connect()就会成功返回，否则这个端口是不可达的。这种扫描很容易被检测到，在目标主机的日志中会记录大批的连接请求以及错误信息。 |
| -sS | TCP同步扫描(TCP SYN)：因为不必全部打开一个TCP连接，所以这项技术通常称为半开扫描(half-open)。你可以发出一个TCP同步包(SYN)，然后等待回应。如果对方返回SYN|ACK(响应)包就表示目标端口正在监听；如果返回RST数据包，就表示目标端口没有监听程序；如果收到一个SYN|ACK包，源主机就会马上发出一个RST(复位)数据包断开和目标主机的连接，这实际上有我们的操作系统内核自动完成的。这项技术最大的好处是，很少有系统能够把这记入系统日志。 |
| -sA | ACK扫描：这项高级的扫描方法通常用来穿过防火墙的规则集。通常情况下，这有助于确定一个防火墙是功能比较完善的或者是一个简单的包过滤程序，只是阻塞进入的SYN包。 |
| -sU | UDP扫描，如果你想知道在某台主机上提供哪些UDP服务，可以使用这种扫描方法。 |
| -O | 这个选项激活对TCP/IP指纹特征(fingerprinting)的扫描，获得远程主机的标志，可以识别目标主机的操作系统。 |
| -S | 伪造本扫描主机的源IP地址。 |
| -T | 每次扫描的间隔时间。 |
| -p | 选择要进行扫描的端口号的范围。例如，-p 23表示：只扫描目标主机的23号端口。-p 20-30,139,60000-表示：扫描20到30号端口，139号端口以及所有大于60000的端口。在默认情况下，nmap扫描从1到1024号。 |

1. 扫描目标主机10.1.1.2所有端口（1-65535）

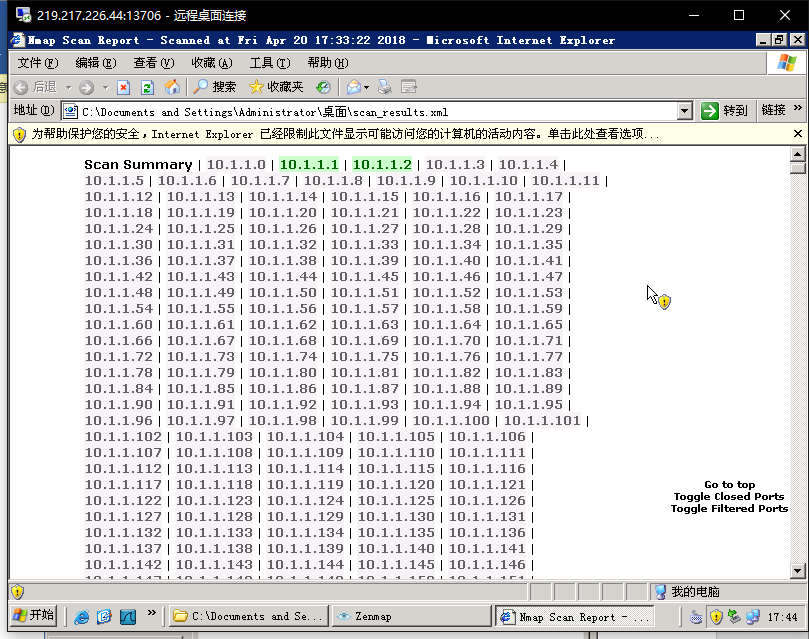


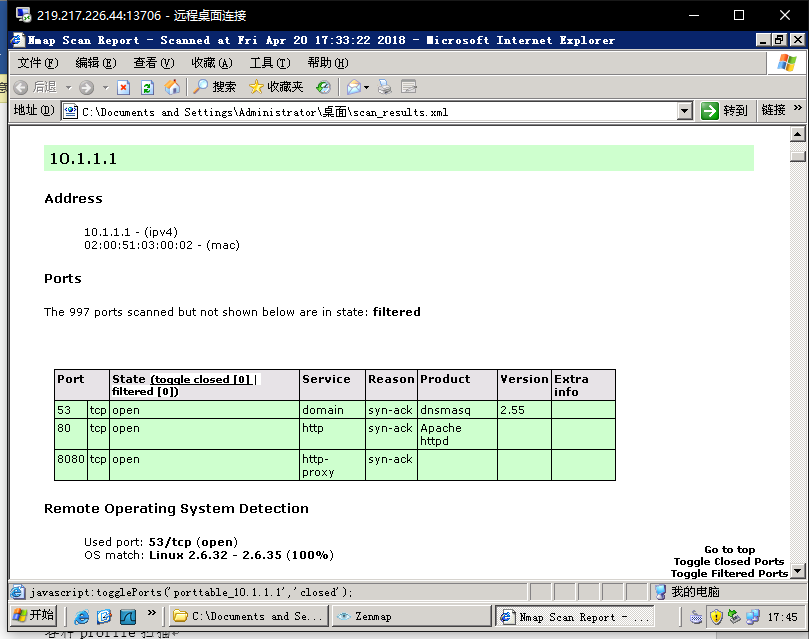
五、实验结果总结

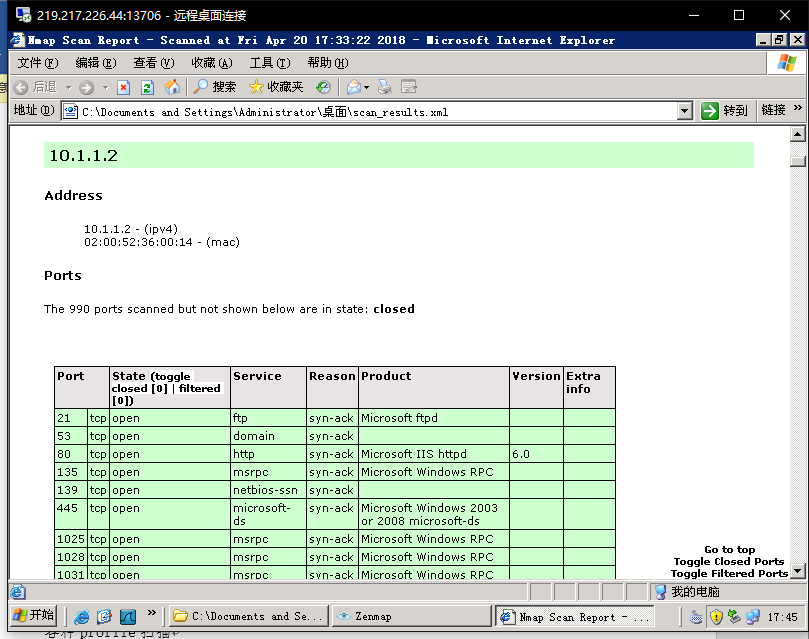
实验结果分析

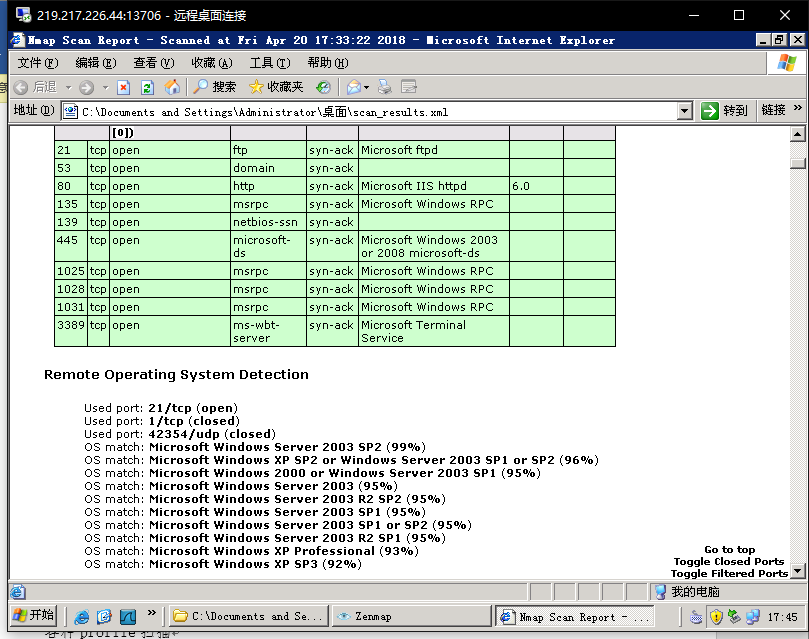
1. 对“任务二：Zenmap图形基本应用”中的第3步结果进行分析。

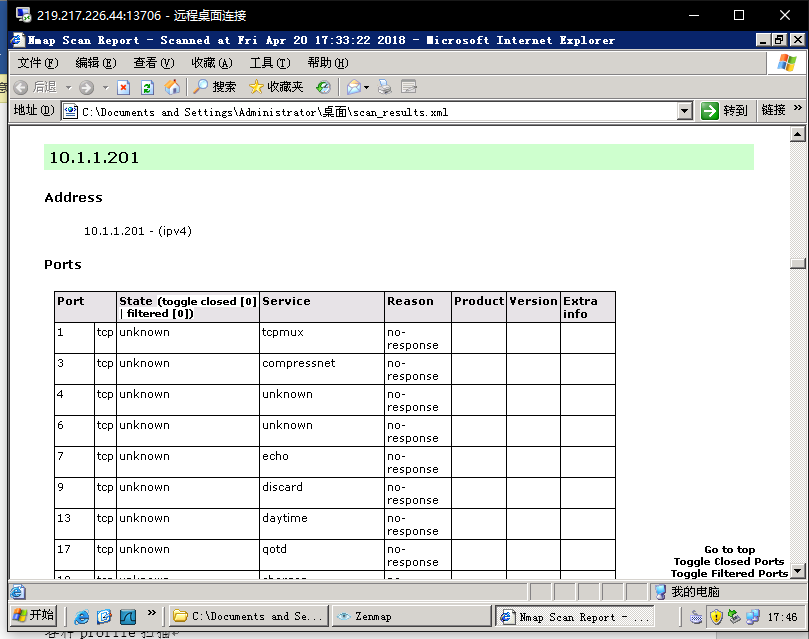
扫描结果一部分如图所示：

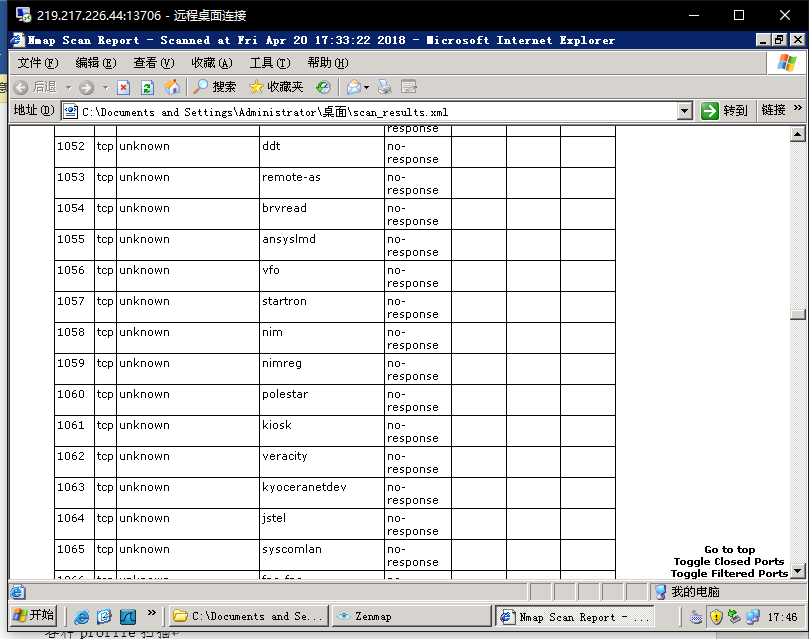












可以看出：

1. 10.1.1.1使用Linux操作系统，开放了53,80,8080三个端口。
2. 10.1.1.2使用Windows Server 2003 SP2操作系统，开放了21,53,80等端口。
3. 10.1.1.201无法检查到有用的信息。
4. 对“任务二：Zenmap图形基本应用”中的不同profile测试结果分析：
5. Intense Scan：扫描最常见的TCP端口。将确定操作系统类型以及运行哪些服务及其版本。
6. Intense Scan, plus UDP：加上UDP协议的intense scan。
7. 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。
8. 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。
9. Ping scan：只对目标执行ping操作，不进行端口扫描。
10. Quick Scan：通过将扫描的TCP端口数量限制为仅排名前100个最常用的TCP端口，可以扫描比密集扫描更快的速度。
11. Quick scan plus：Quick scan的加强模式, 添加了版本和操作系统检测。
12. Quick traceroute：跟踪路由和ping目标中定义的所有主机。
13. Regular scan：使用默认值。这意味着它将为最常见的1000个TCP端口发出TCP SYN扫描，并使用ICMP Echo请求（ping）进行主机检测。
14. 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。
15. 对图形界面proflie中选项对应的命令行参数进行分析。

|  |  |  |
| --- | --- | --- |
| Profile | 对应的命令行参数 | 对参数的分析 |
| Intense scan | Nmap -T4 -A -v | -T4 加快执行速度  -A 操作系统及版本探测  -v 显示详细的输出  特点: 适用于局域网，可靠性网络进行扫描，略带侵略性，能实现操作系统及版本检测，系统脚本运行，路由显示扫描过程中的详细信息 |
| Intense scan plus UDP | Nmap -sS -sU -T4 -A -v | -Pn 非ping扫描  特点: 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 |
| Intense scan, all TCP port | Nmap -p 1-65535 -T4 -A -v | -p指定要扫描的端口范围，否则扫描最有可能的top1000端口  在Intense scan的基础上要求了对完整1-65535端口的扫描 |
| Intense scan, no ping | Nmap -T4 -A -v -Pn | -Pn将所指定的主机视作开启的，跳过使用ping的主机发现的过程  当我们确定10.1.1.1主机是开启的时候可以使用这个参数 |
| Ping scan | Nmap -sn | -sn ping扫描  特点: 在发现主机后，不进行端口扫描 |
| Quick scan | Nmap -T4 -F | -F 快速模式 |
| Quick scan plus | Nmap -sV -T4 -O -F --version-light | -sV 探测端口及版本服务信息  -O 操作系统检测  --version-light 设定侦测等级为2 |
| Quick traceroute | Nmap -sn --traceroute | -sn ping扫描，关闭端口扫描  -traceroute 显示本机到目标的路由跃点  特点：快速扫描，不扫端口，返回每一跳的主机ip |
| Regular scan | nmap | 默认扫描，扫描主机和主机端口 |
| Slow comprehensive scan | nmap -sS -sU -T4 -A -v -PE -PP -PS80,443,-PA3389,PU40125 -PY -g 53 --script all | 特点: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。 |

思考问题

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？
   1. 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。例如扫描局域网192.168.1.100-192.168.1.120范围内哪些IP的主机是活动的命令如下：  
      nmap –sn 192.168.1.100-120
   2. 而对于互联网的扫描，则需要对扫描时序等参数进行仔细的优化。

例如随机地产生10万个IP地址，对其80端口进行扫描。将扫描结果以greppable（可用grep命令提取）格式输出到nmap.txt文件。

nmap -iR 100000 -sS -PS80 -p 80 -oG nmap.txt

还需要产生随机IP地址，这里可以使用如下命令：

nmap -iR 1200000 -sL -n | grep “not scanned” | awk „{print $2}‟ | sort -n | uniq >! tp; head -25000000 tp >! tcp-allports-1M-IPs; rm tp

1. 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？
   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

心得与体会

通过本次实验，我对TCP、UDP协议以及nmap的基本原理和使用方法有了初步的了解。我现在可以使用nmap进行不同网络环境下的端口扫描。同时，我对互联网安全也有了更深刻的认识，通过对扫描攻击的了解了来提高防御的能力。