哈尔滨工业大学计算机学院

《基于nmap的网络信息扫描原理与设计》

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： | 韩越 |
| 组 号： | 第二组11号 |
| 实验日期： | 2018-04-19 |
| 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

*实验所使用的设备名称及规格，网络管理工具简介、版本等。*

本实验的实验环境为一台Windows主机。和它所在的局域网，和局域网内ip为10.1.1.1的linux主机和ip为10.1.1.2的windows主机。

三、实验内容与实验要求

**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。

**2. 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。

**3. 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。

**4. nmap简介**

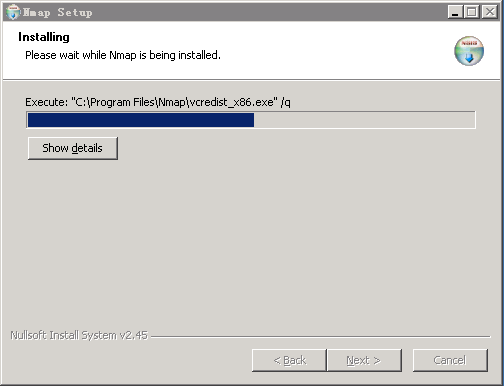
      nmap是一个网络探测和安全扫描程序，系统管理者和个人可以使用这个软件扫描大型的网络，获取主机正在运行以及提供什么服务等信息。nmap支持很多扫描技术，例如：UDP、TCP connect()、TCP SYN(半开扫描)、ftp代理(bounce攻击)、反向标志、ICMP、FIN、ACK扫描、圣诞树(Xmas Tree)、SYN扫描和null扫描。从扫描类型一节可以得到细节。nmap还提供了一些高级的特征，例如：通过TCP/IP协议栈特征探测操作系统类型，秘密扫描，动态延时和重传计算，并行扫描，通过并行ping扫描探测关闭的主机，诱饵扫描，避开端口过滤检测，直接RPC扫描(无须端口影射)，碎片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

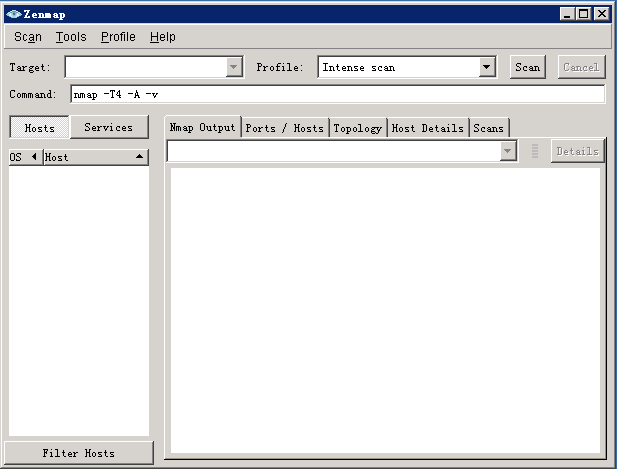
四、实验过程与分析

*实验内容、原理分析及具体实验要求。*

# 任务一：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。





# 任务二：Zenmap图形基本应用

      1）查找本机网关

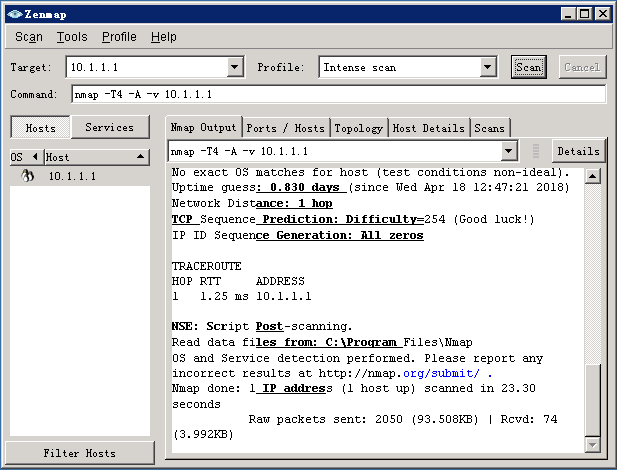
      打开cmd控制台，在控制台中输入ipconfig /all，查看本机网关信息。

      实验目的：通过扫描本机网关熟悉nmap基本运行环境

      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：10.1.1.243，网关地址为：10.1.1.1：

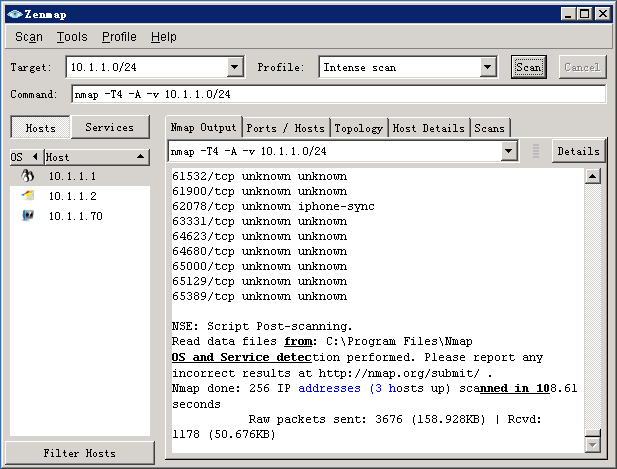


 2）在zenmap界面中将扫描目标10.1.1.1填写入targe项，不修改参数直接点击scan，等待返回扫描结果。

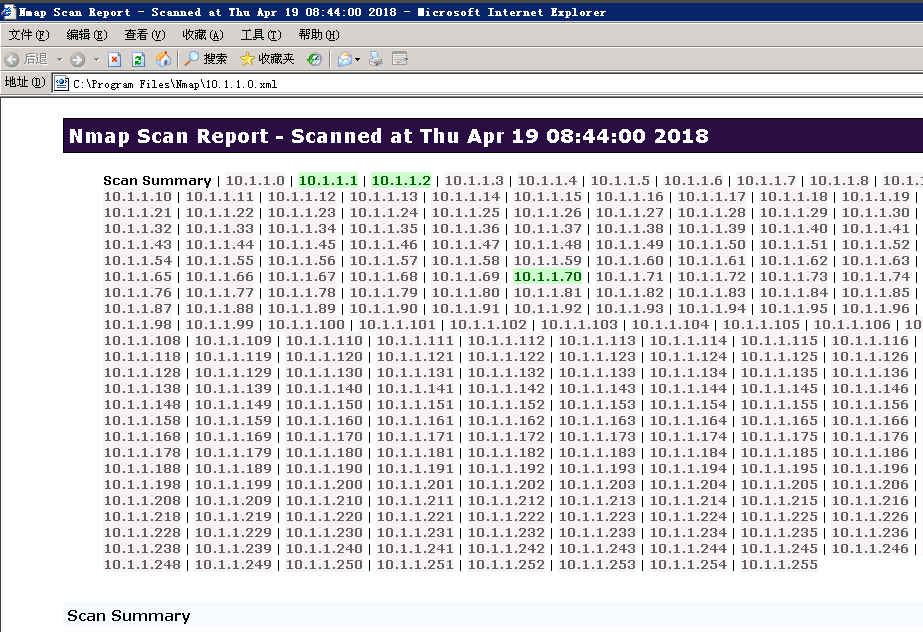


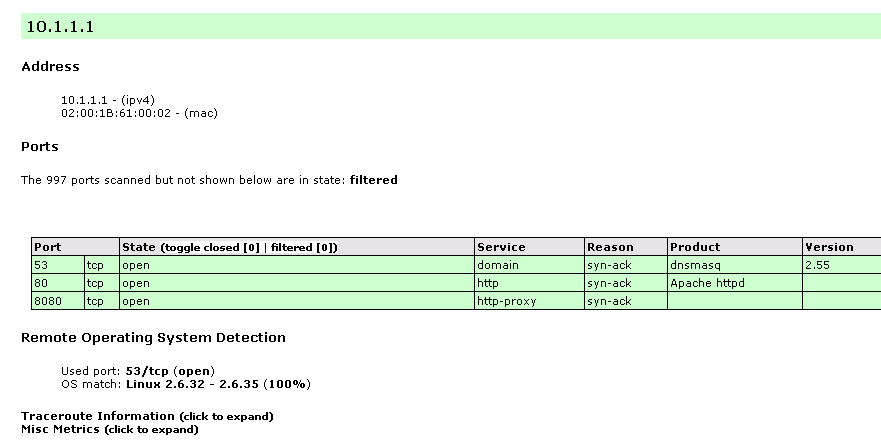
 3）整网段扫描

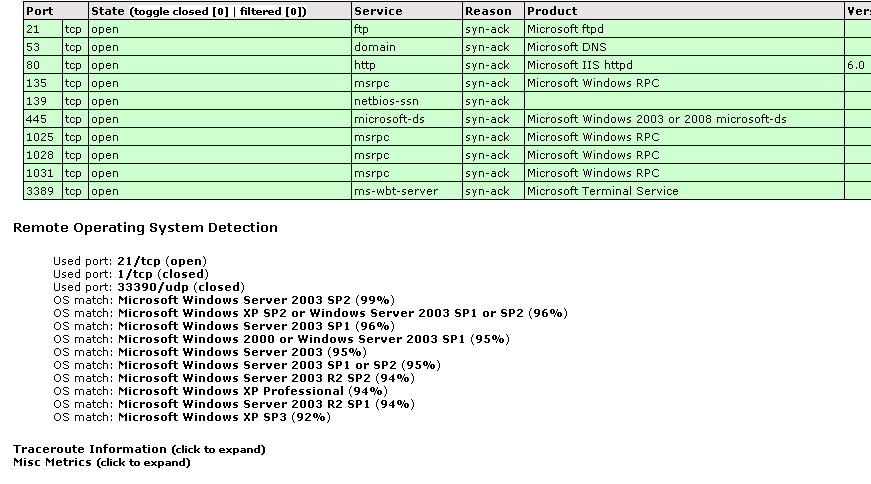
      对本机所处网段进行扫描，分析本网段环境，使用方法：在扫描目标中输入：10.1.1.0/24，然后运行扫描任务。扫描任务停止后查看返回结果。

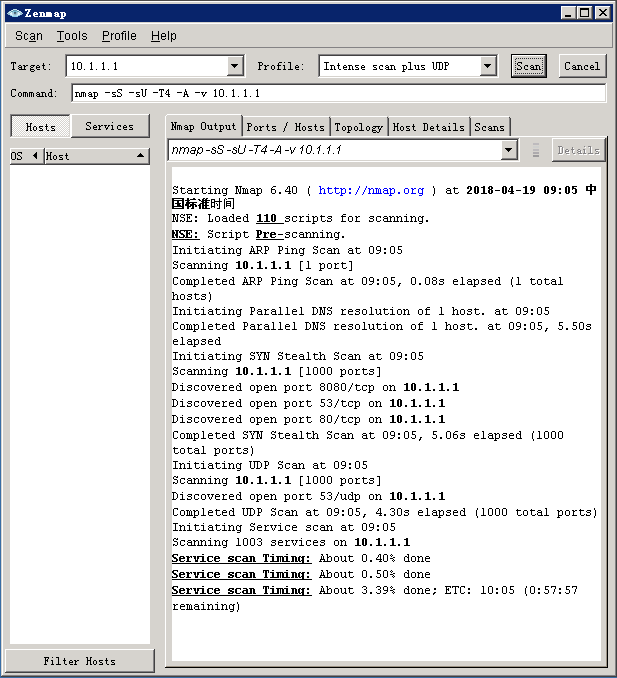


选择“scan”菜单中“Save Scan”选项保存扫描结果，保存类型选用默认的XML格式。

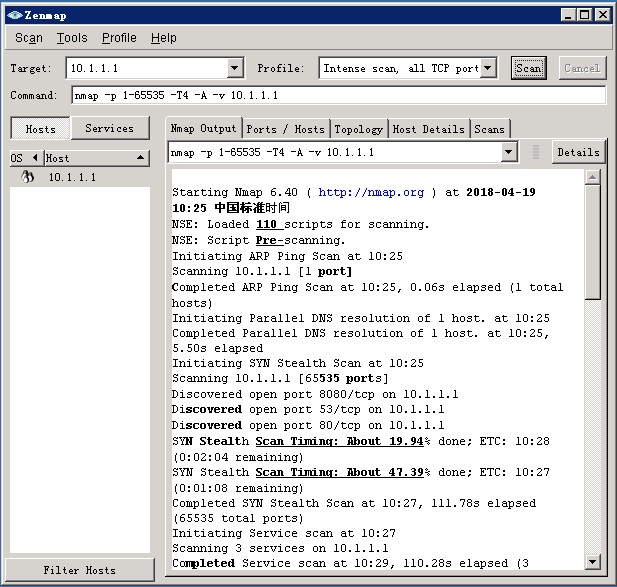


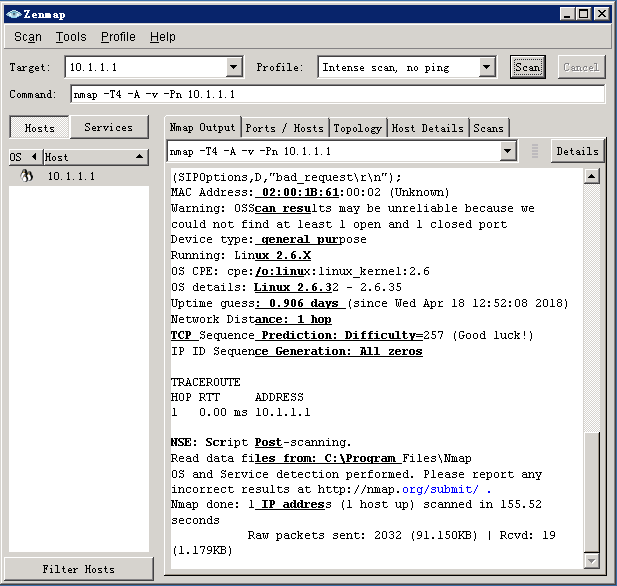


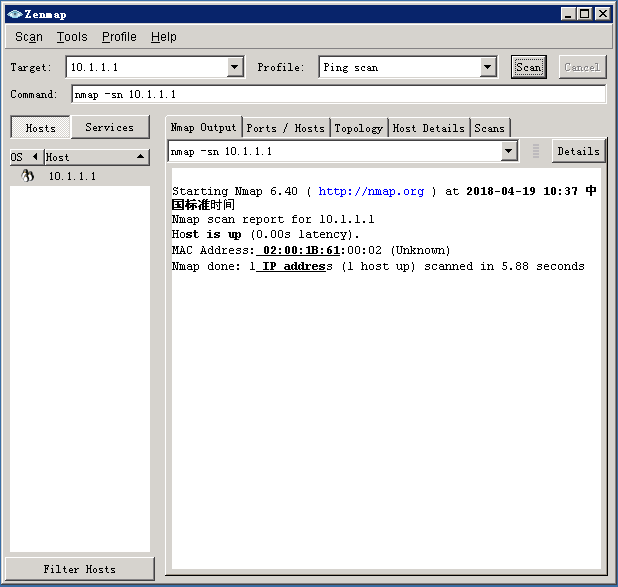


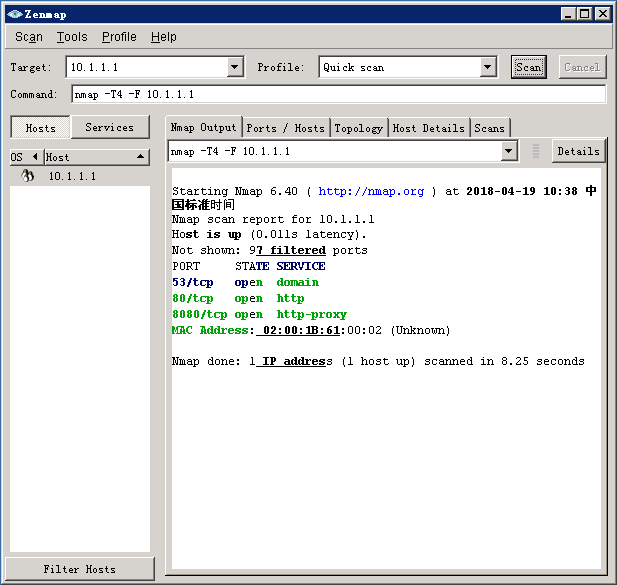


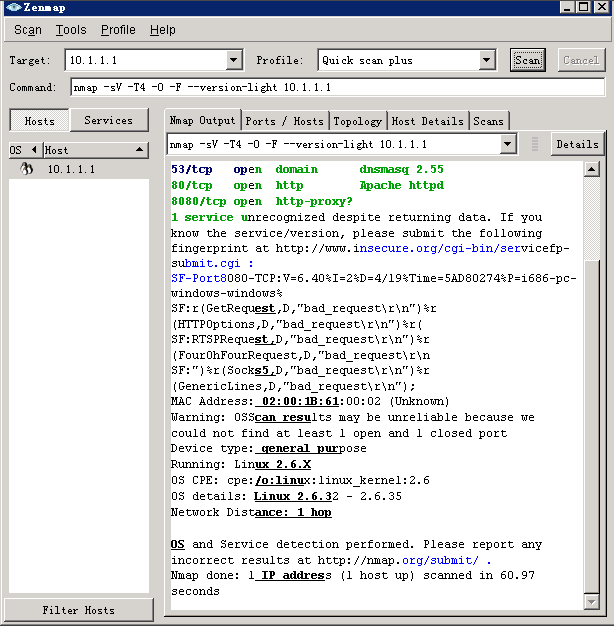
各种profile扫描

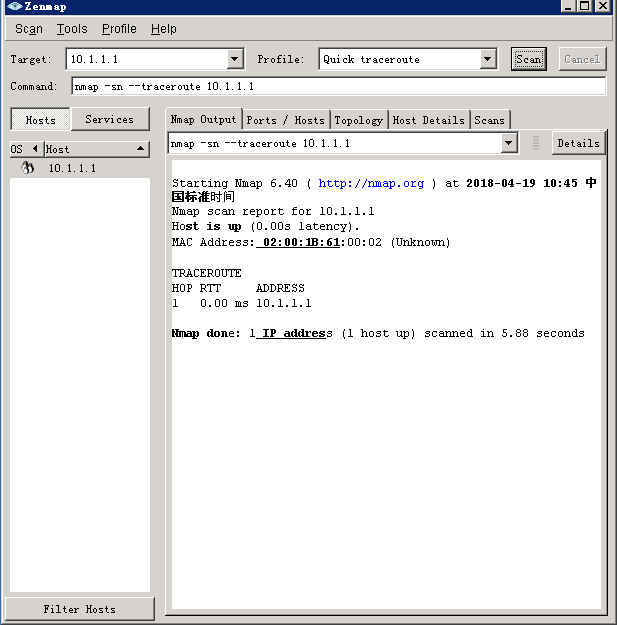


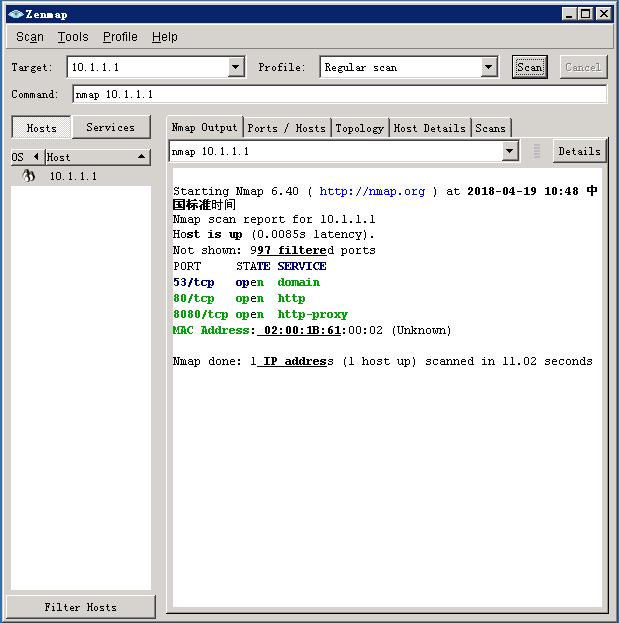


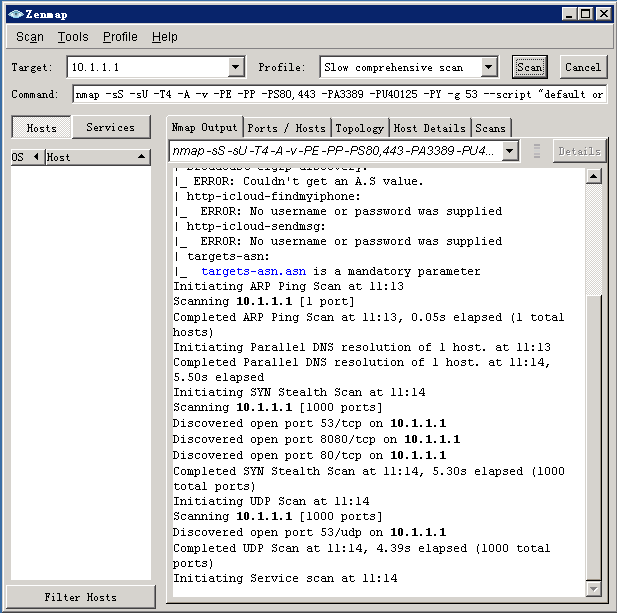






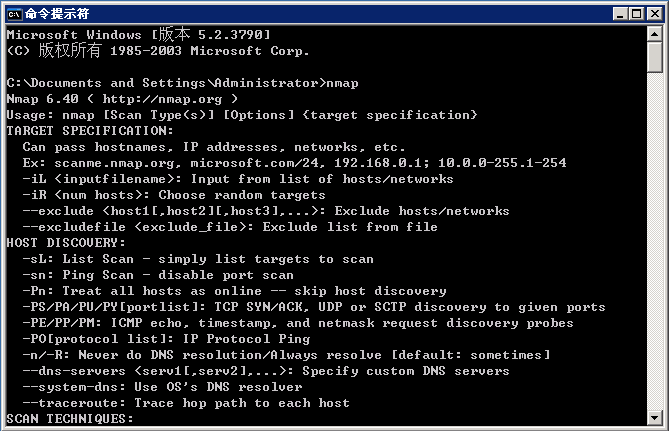


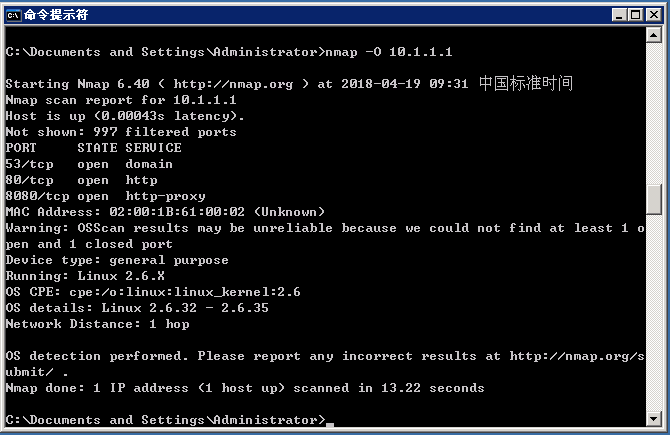


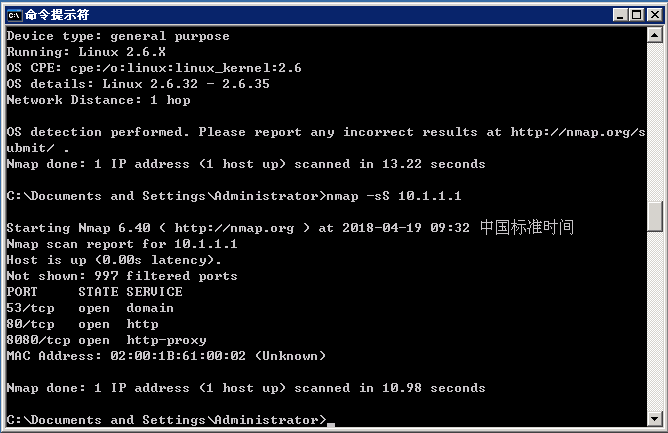


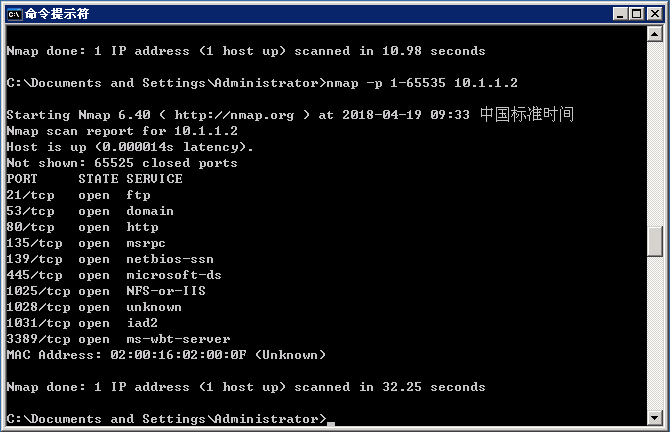
**任务三：nmap命令行的使用**

 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。









最基本的模式Intense scan

主机检测阶段可以得到主机的打开情况；

端口扫描阶段得到主机哪些端口的开启状态，例如53,80，8080；每个端口上运行的服务类型，如domain, http, http-proxy；

版本侦测阶段得到运行服务的软件名称；软件版本等。

系统侦测阶段猜测运行的系统类型，猜测出系统名称和确信概率。

Intense scan plus UDP

增加了使用UDP协议扫描1000个端口的结果。

Intense scan, all TCP port

扫描了所有端口，端口结果上差异不大，系统猜测变成100%的linux2.6.32-2.6.35。

Intense scan, no ping

没有了主机发现阶段的内容。

Ping scan

结果得到了主机10.1.1.1的开放情况和连接延迟，没有端口信息。

Quick scan

得到了主机端口扫描结果和端口上运行的服务类型。

Quick scan plus

Quick scan的结果上增加了软件名称和版本信息，系统类型和版本信息猜测。

Quick traceeoute

由于是在局域网内，路径追踪只有HOP 1, RTT 0.00ms, ADDRESS 10.1.1.1

Regular scan

得到了主机和主机的端口信息。

Slow comprehensive scan

非常完整的信息。

**参数和结果分析**

|  |  |  |
| --- | --- | --- |
| Profile | 参数 | 分析 |
| Intense scan | Nmap -T4 -A -v | -T4设置时序，范围0-5，越高越快；  -A使用进攻性扫描，一次扫描包含系统探测、版本探测、脚本扫描和跟踪扫描。  -v显示扫描过程中的冗余信息  Intense scan可以快速得到扫描对象的大部分信息 |
| Intense scan plus UDP | Nmap -sS -sU -T4 -A -v | -sS使用TCP SYN半连接扫描，由于不建立完整的TCP连接，速度较快，隐蔽好  -sU使用UDP扫描确定目的主机UDP端口情况  Intense scan plus UDP增加了UDP端口的UDP方式扫描 |
| 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只用ping进行主机发现，不进行端口扫描  得到的结果只是知道主机是否开启和连接延迟情况 |
| Quick scan | Nmap -T4 -F | -F fast mode快速模式，仅扫描TOP 100的端口  使用较快的速度扫描最有可能的100个端口，特点是速度快 |
| Quick scan plus | Nmap -sV -T4 -O -F --version-light | -sV指定让Nmap进行版本侦测  -O指定Nmap进行OS侦测  --version-light指定使用轻量侦测方式 (intensity 2)  在quick scan的基础上增加了2级的版本侦测和系统侦测 |
| Quick traceeoute | Nmap -sn --traceroute | --traceroute追踪每个路由节点  使用ping扫描主机并且跟踪路由节点 |
| 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 | 全面扫描，很慢，很容易崩 |

五、实验结果总结

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？

局域网中的机器比互联网中的机器数量少，通信速率高，对局域网中的机器扫描时可以暴力一些。局域网中还可以使用发ARP包的方式来较快速地扫描局域网机器。

对互联网中的机器扫描时要注意网络延迟，对方防火墙等级，是否能访问到对方局域网内等问题，所以就不能加入-p 1-65535这种非常消耗资源的参数，使用-T（0-5）参数时也要注意速度是否太快而被对方防火墙屏蔽，谨慎使用Slow comprehensive scan方式。对于防火墙的规避nmap也提供了一些方法。例如使用-f； –mtu <val>；-D；-S；-e等参数来完成分片，IP诱骗等操作。

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？

设置防火墙检测扫描行为。例如屏蔽短时间同一个源对多个端口的访问行为，屏蔽反复的TCP SYN握手操作。修复防火墙漏洞。关闭不必要的端口，监视重要的端口例如FTP21端口。经常更新防火墙。

**心得体会：**

通过这次实验我学会了nmap软件的使用，对网络中各种连接方式有了更深的了解，例如TCP三次握手操作。对于局域网，互联网的架构有了更深更形象的理解。受益匪浅。