南昌大学软件学院

实验报告书

课 程 名 ： 网络安全技术

题　　目： Nmap 扫描试验

实验类别 【验证】

班　　级： 信息安全 193 班

学　　号： 8003119100

姓　　名： 丁俊

评语：

实验态度：认真（　）　一般（　）　较差（　）
实验结果：正确（　）　部分正确（　）错（　）
实验理论：掌握（　）　熟悉（　）　了解（　）生疏（　）
操作技能：较强（　）　一般（　）　较差（　）
实验报告：较好（　）　一般（　）　较差（　）

成绩：＿＿＿＿＿＿　　指导教师： 鄢志辉

一、实验目的

掌握主机、端口扫描的原理

掌握Nmap扫描器的使用

掌握Nmap进行远程OS检测的原理

二、实训内容

Nmap 四项基本功能：1 主机发现（Host Discovery）2 端口扫描（Port Scanning）3 版本侦测（Version Detection）4 操作系统侦测（Operating System Detection）。实验中操作和验证以上功能

1、实验任务

（1）安装和运行网络扫描软件。

（2）进行典型的探测，如主机探测、系统探测、TCP 扫描等。

（3）记录并分析实验结果。

3、实验报告

（1）简要描述实验过程。

（2）实验中遇到了什么问题，如何解决的。

（3）分析网络扫描器在网络管理和网络安全方面的作用。

（4）实验收获与体会。

三、实验环境（本次上机实践所使用的平台和相关软件）

操作系统 :Microsoft Windows 2003虚拟机

网络平台：TCP/IP网络

Nmap版本：6.40

四、实验背景

1 基础知识

扫描的目的是收集被扫描系统或网络的信息。通常，扫描是利用一些程序或专用的扫描器来实现，扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用扫描器，可以发现远程服务器是否存活、对外开放的各种 TCP 端口的分配及提供的服务、所使用的软件版本，如操作系统或其他应用软件的版本，以及可能被利用的系统漏洞。根据这些信息，可以使用户了解目标主机所存在的安全漏洞。

扫描器不仅是黑客用作网络攻击的工具，也是网络安全管理员维护网络安全的重要工具。网络安全管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误。

2 网络扫描工具 Nmap 简介

Nmap 是一款开放源代码的网络探测和安全审核的工具，基本包括了常用的扫描方式，并且提供了许多非常实用的辅助功能，以对目标主机做出进一步的侦测，如操作系统识别、进程用户分析以及众多可选的方式来逃避目标系统的监测等。Nmap 可任意指定主机、网段甚至是整个网络作为扫描目标，扫描方式亦可通过添加合适的选项按需组合。

本实验使用基于 Windows 的 Nmap 软件，其命令语法如下：

nmap [扫描类型] [选项] <主机或网络 #1……[#N]>

在 Nmap 的所有参数中，只在目标参数是必须给出的，其最简单的形式是在命令行直接输入一个主机名或者一个 IP 地址。如果希望扫描某个 IP 地址的一个子网，可以在主机名或者 IP 地址的后面加上/掩码。掩码的范围是 0（扫描整个网络）~32（只扫描这个主机）。使用/24 扫描 C 类地址，/16 扫描 B 类地址。

可以使用 nmap –h 快速列出 Nmap 选项参数的说明，下面列举出一些常用的扫描类型：

-sT 表示 TCP 全连接扫描（TCP connect（））。

-sS 表示 TCP 半开扫描。

-sF 表示隐蔽 FIN 数据包扫描。

-sA 表示 Xmas Tree 扫描。

-sN 表示空（Null）扫描。

-sP 表示 ping 扫描。

-sU 表示 UDP 扫描。

-sA 表示 ACK 扫描。

-sW 表示对滑动窗口的扫描。

-sR 表示 RPC 扫描。

-b 表示 FTP 反弹攻击（bounce attack）。

功能选项可以组使用，有些功能选项只能在扫描模式下使用，Nmap 会自动识别无效或者不支持的功能选项组合，并向用户发出警告信息。下面列举出一些常用的选项：

-P0 表示在扫描之前，不必 ping 主机。

-PT 表示扫描之前，使用 TCP ping 确定哪些主机正在运行。

-PS 表示使用 SYN 包而不是 ACK 包来对目标主机进行扫描（需要 Root 权限）。

-PI 表示使用真正的 ping（ICMP echo 请求）来扫描目标主机是否正在运行。

-PB 表示这是默认的 ping 扫描选项。它使用 ACK（-PT）和 ICMP（-PI）两种扫描类型并行扫描。

-O 表示对 TCP/IP 指纹特征（fingerprinting）的扫描，获得远程主机的标志。

-I 表示反向标志扫描。

-f 表示使用碎片 IP 数据包发送 SYN、FIN、XMAS、NULL 扫描。

-v 表示冗余模式。它会给出扫描过程中的详细信息。使用-d 选项可以得到更加详细的信息。

-h 表示快速参考选项。

-oN 表示把扫描结果重定向到一个可读的文件 logfilename 中。

-oS 表示把扫描结果重定向到标准输出上。

-resume 表示可以使扫描接着以前的扫描进行。

-iL 表示从 inputfilename 文件中读取扫描的目标。

-iR 表示让 nmap 自己随机挑选主机进行扫描。

-p <端口范围> 表示选择要进行扫描的端口号的范围。

-F 表示快速扫描模式。

-D 表示使用诱饵扫描方法对目标网络/主机进行扫描。

-S <IP-Address>表示指定 IP 源地址。

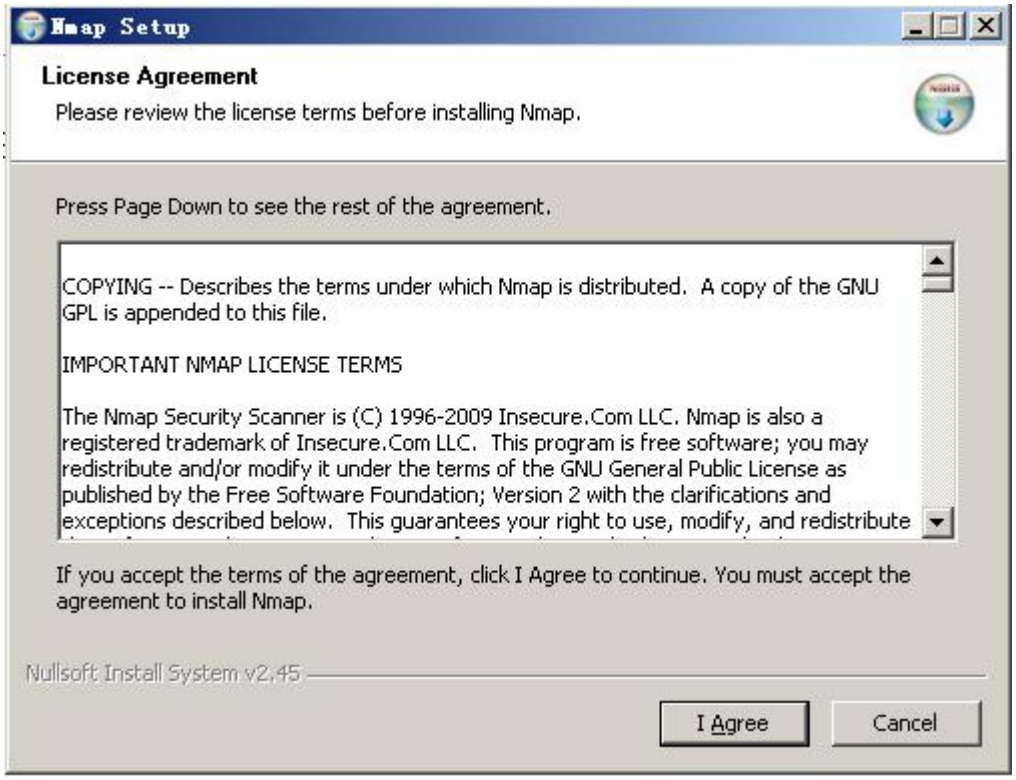
-e 表示使用哪个接口发送和接受数据包。

-g 表示设置扫描的源端口。

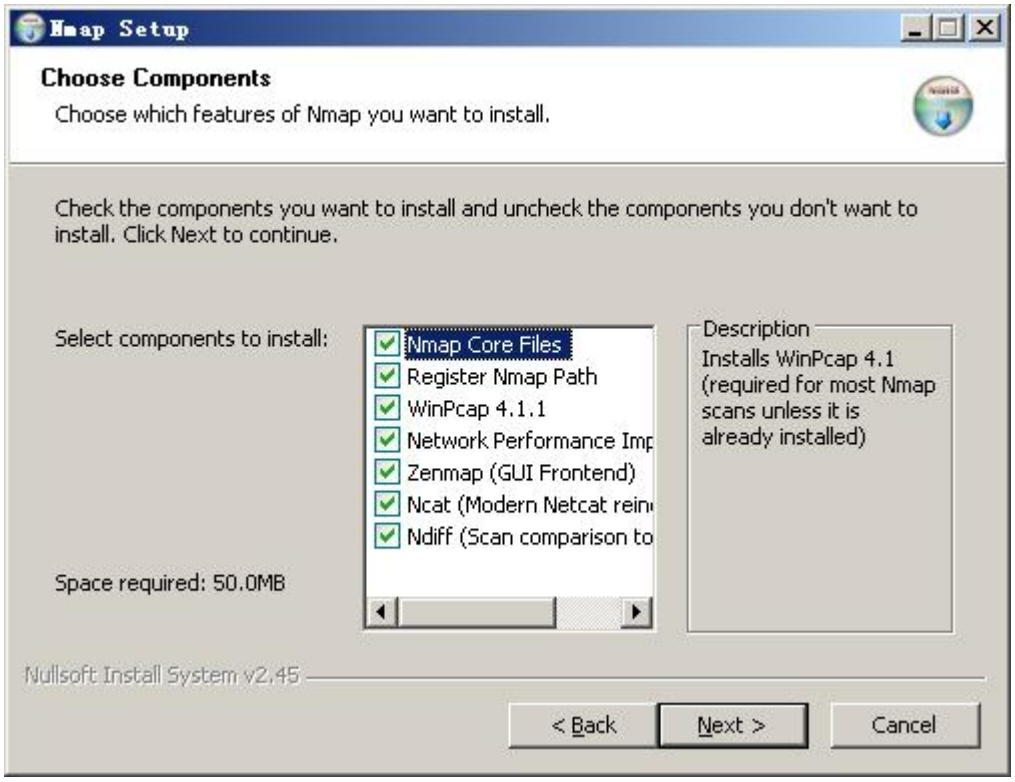
Nmap运行通常会得到被扫描主机端口的列表、Well-known端口的服务名（如果可能）、端口号、状态和协议等信息。每个端口有Open、Filtered和Unfiltered三种状态。Open状态意味着目标主机能够在这个端口使用Accept（）系统调用接受连接；Filtered状态表示防火墙、包过滤和其他的网络安全软件掩盖了这个端口，禁止Nmap探测其是否打开；Unfiltered表示这个端口关闭，并且没有防火墙/包过

滤软件来隔离Nmap的探测企图。

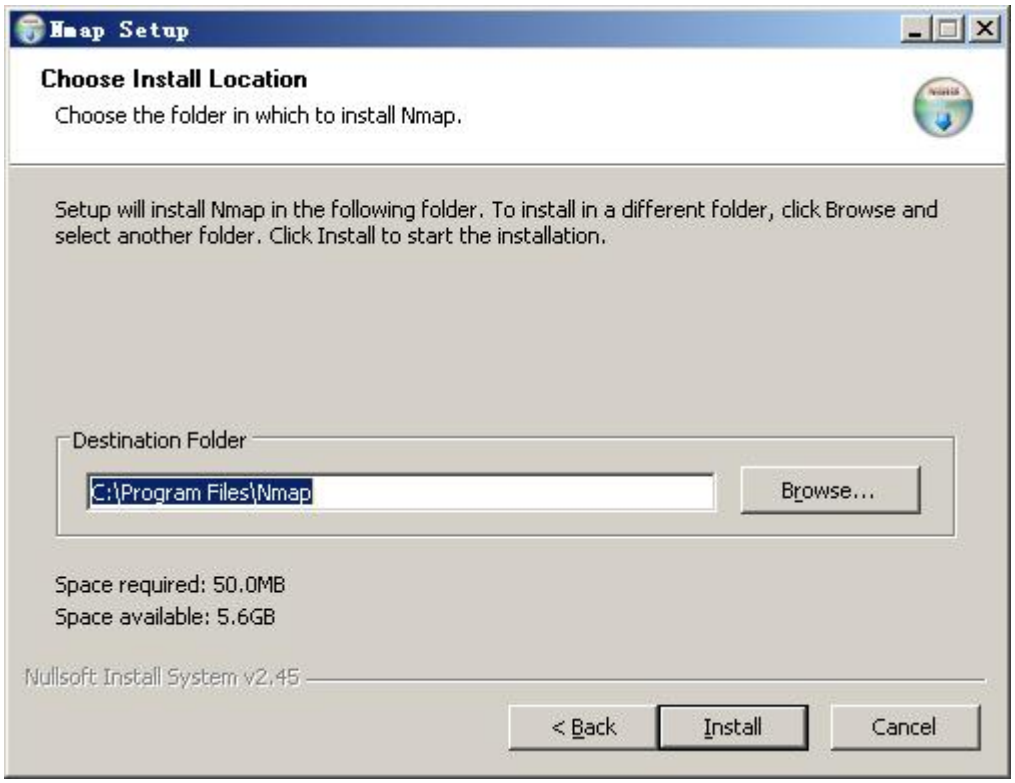
四、实验步骤



单击 IAgree

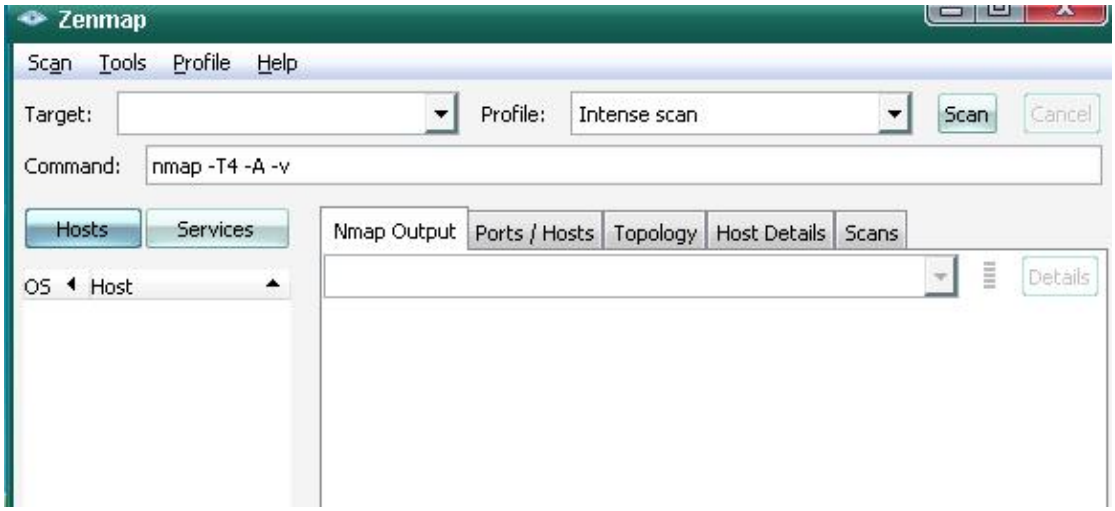


默认安装，单击“Next”



单击 Install 完成安装

软件界面



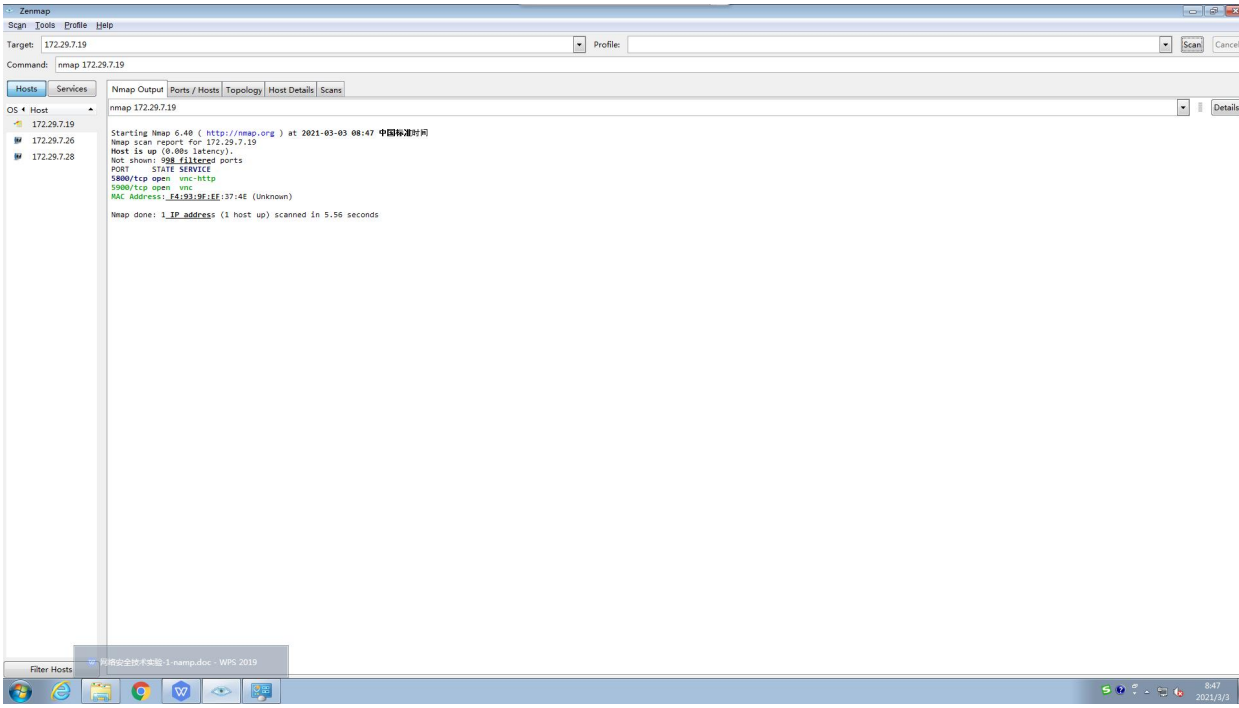
也可以在命令提示符中

1.利用 Nmap 扫描

1.1 扫描整个子网命令如下

命令形式:nmap targethost 可以确定目标主机在线情况及端口基本状况

命令为：nmap 210.40.2.253

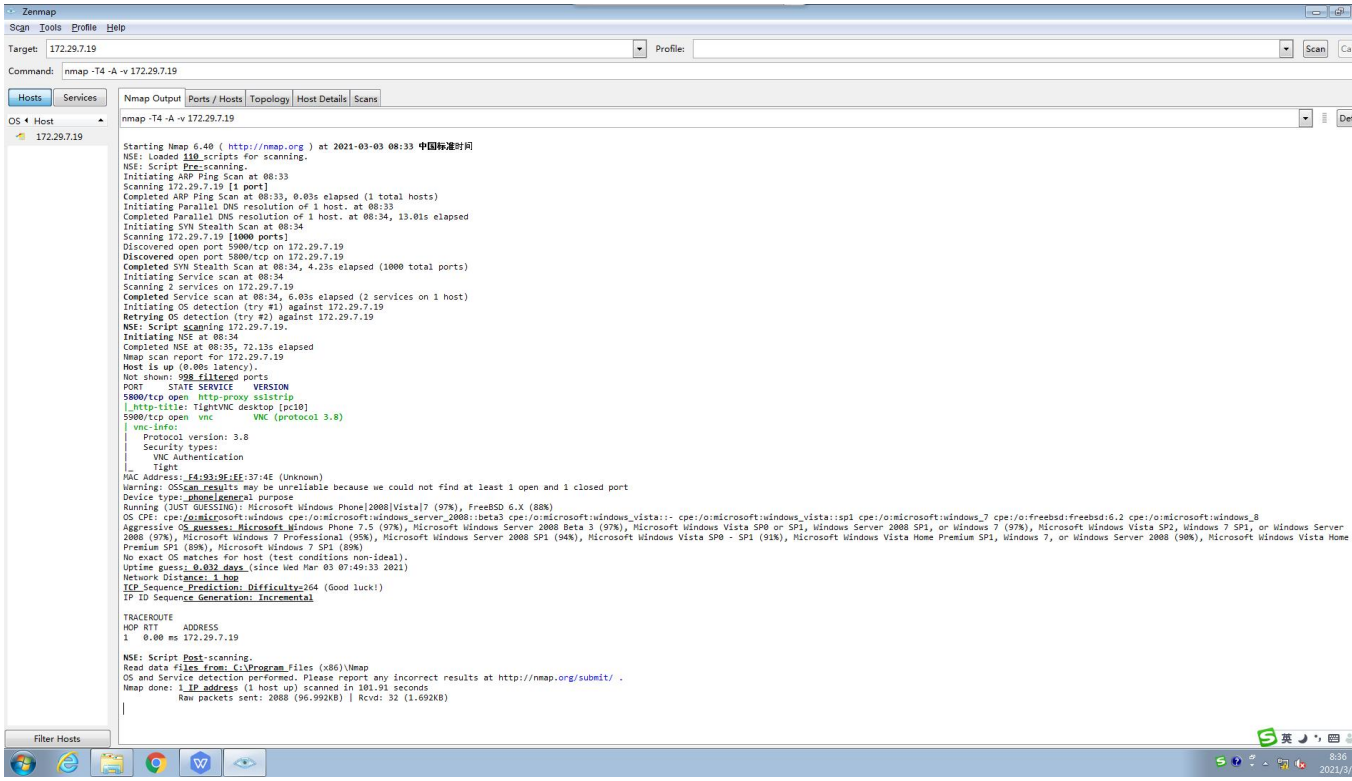


主机处于打开状态，996 个端口处于关闭状态。22 端口打开，ASH 服务，且基于 tcp，1720 端口打开，Http 服务，且基于 TCP 服务。

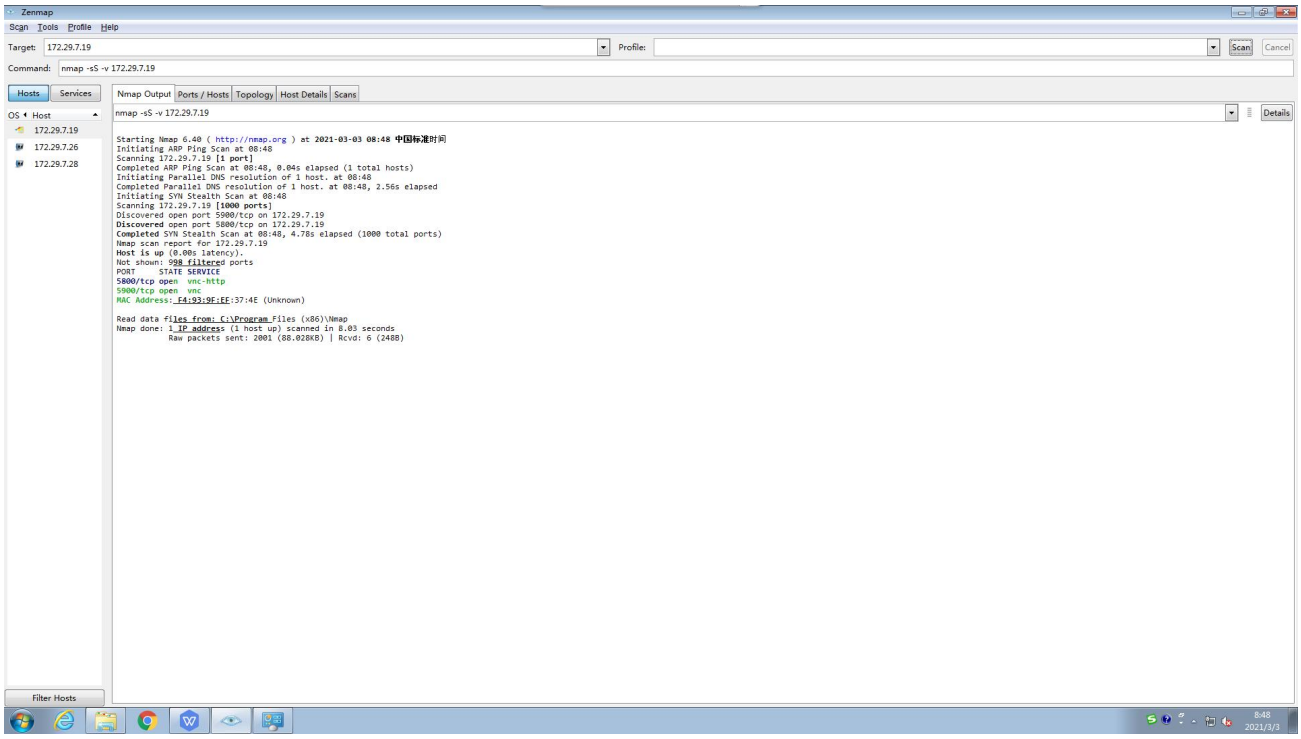
1.2 完整全面的扫描

命令形式：nmap –T4 –A –v targethost

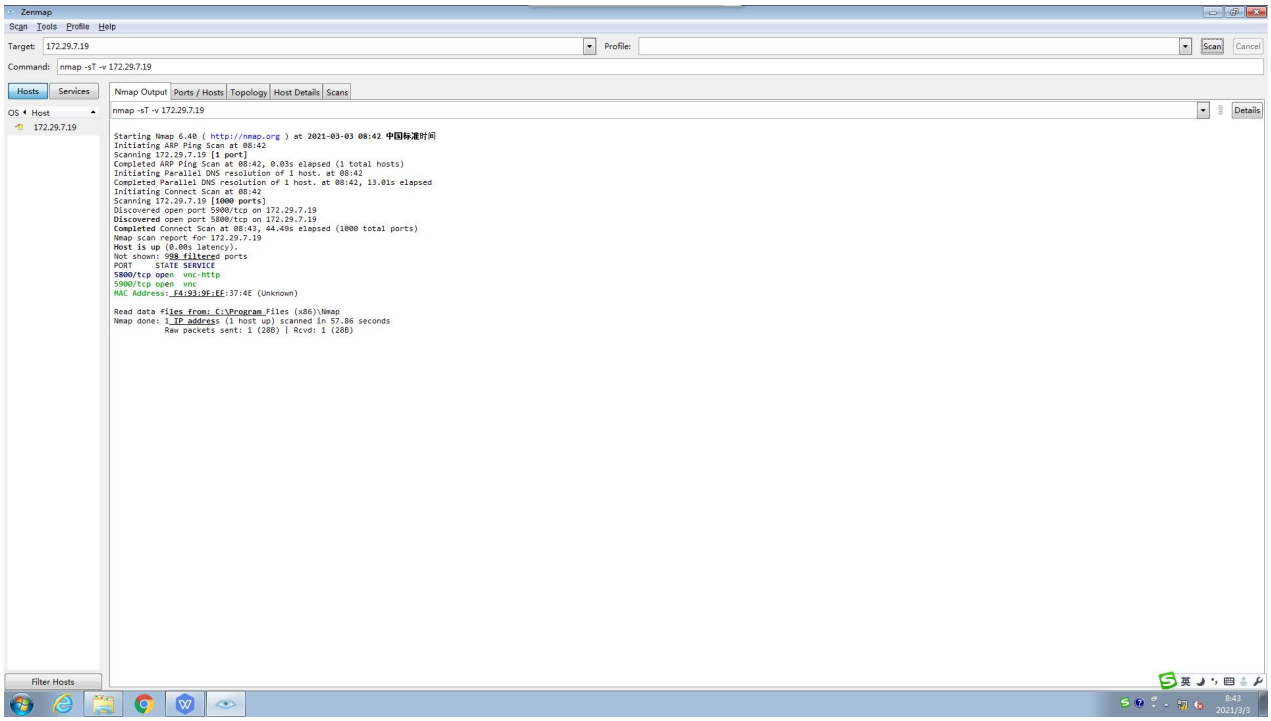
nmap –T4 –A –v 192.168.0.28



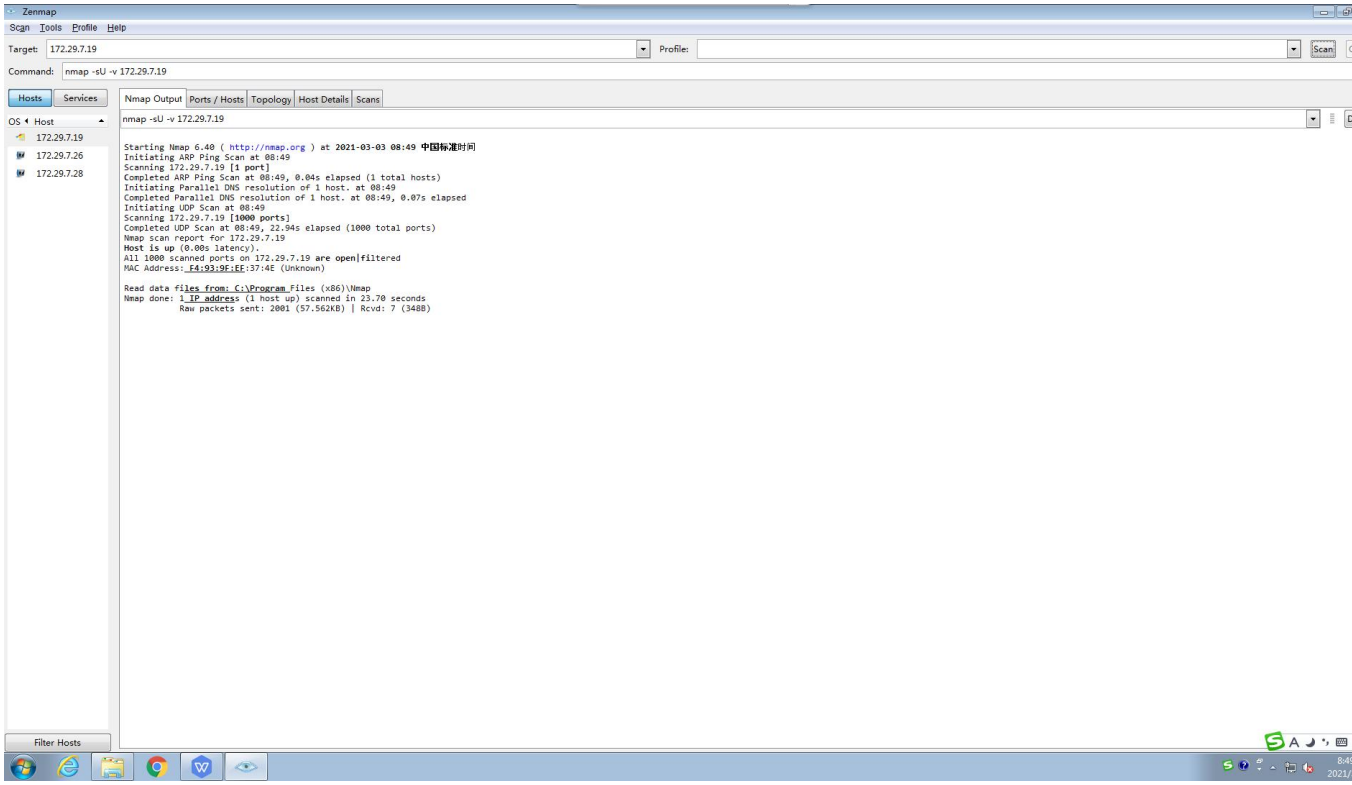
2、命令为：nmap -sS -v 210.40.2.254



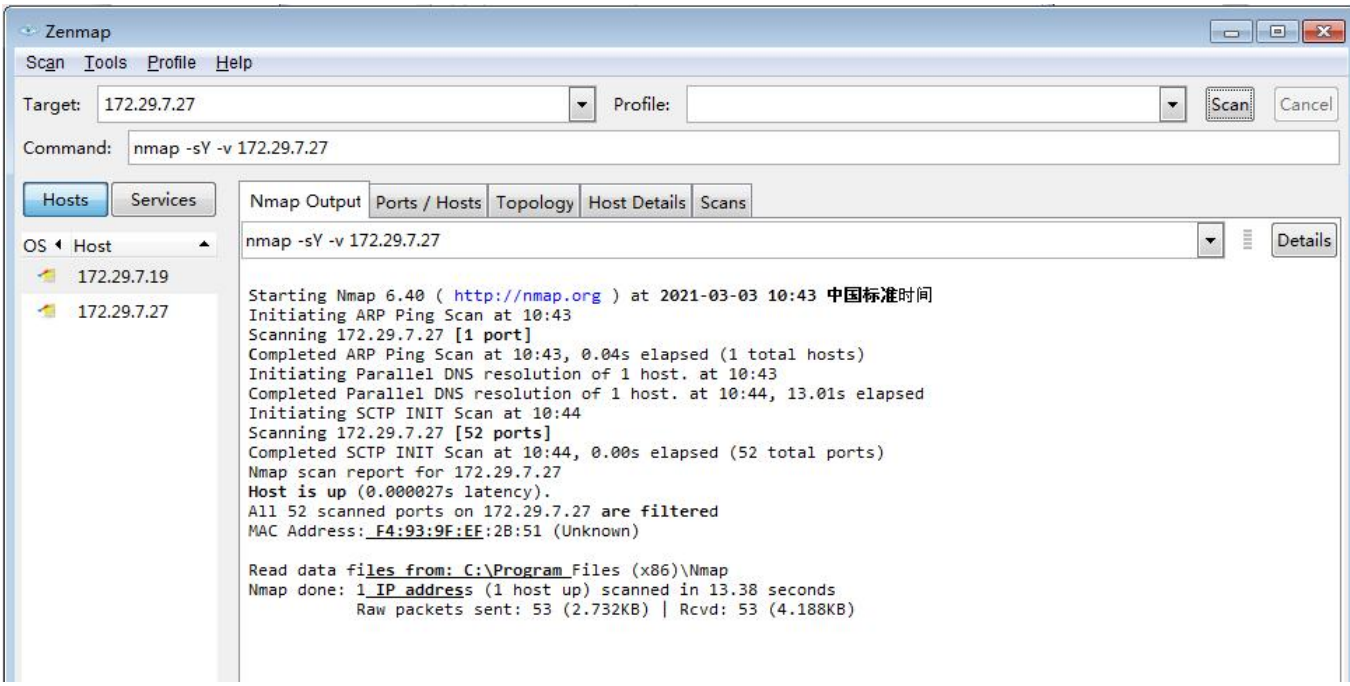
3、命令为：nmap　-sT -v 210.40.2.254



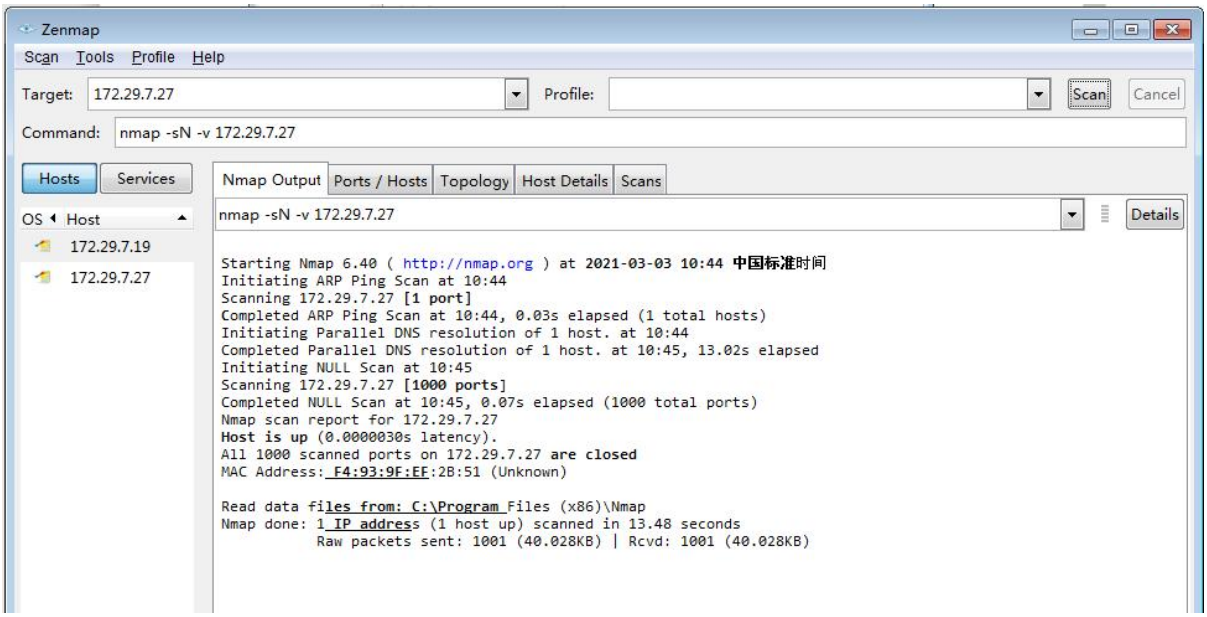
4、-sU: 指定使用 UDP 扫描方式确定目标主机的 UDP 端口状况。
命令为：nmap　-sU　-v 210.40.2.254



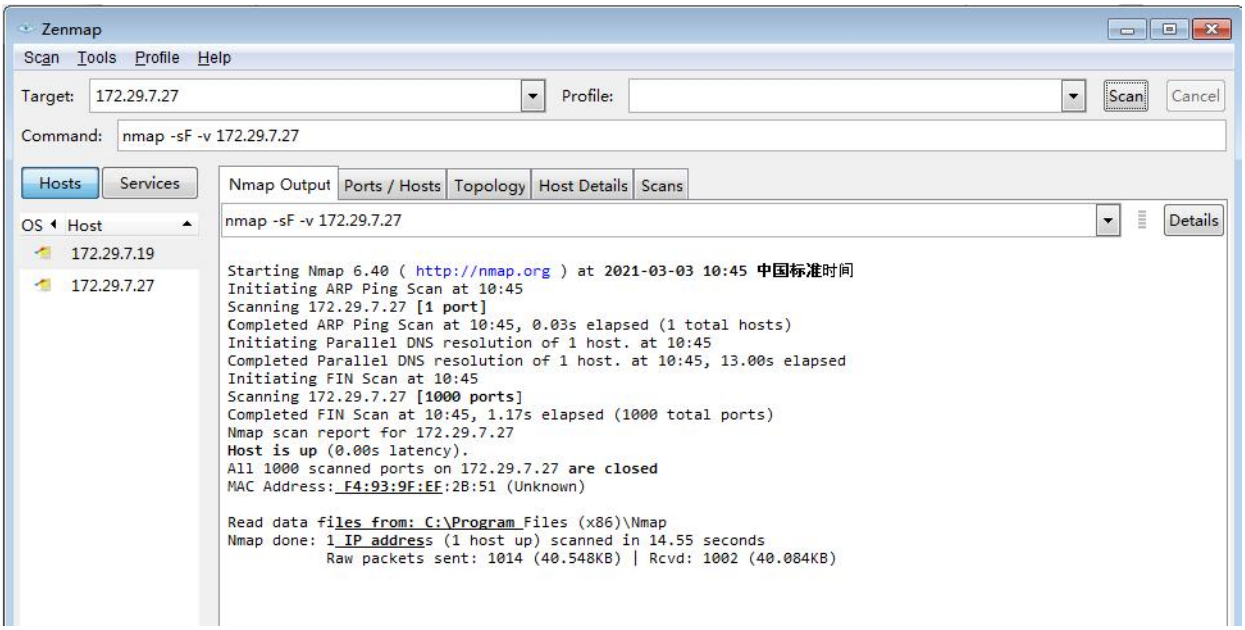
5、命令为：nmap　-sY　-v 210.40.2.254



6、命令为：nmap　-sN -v 210.40.2.254

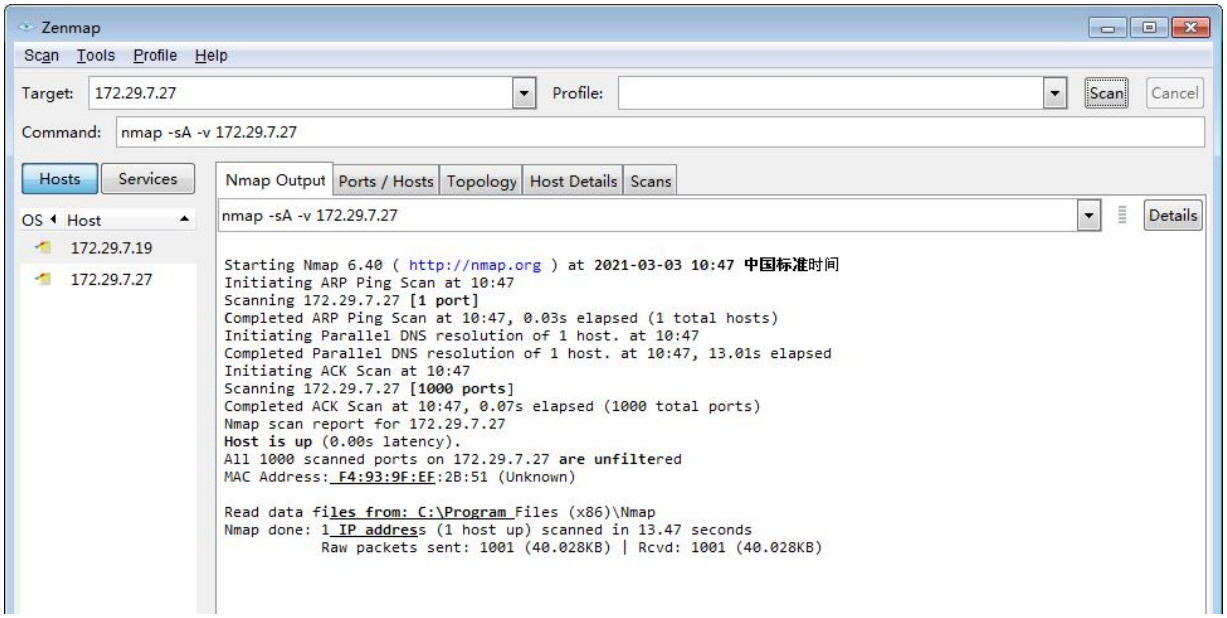


7、命令为：nmap　-sF　-v 172.29.7.27

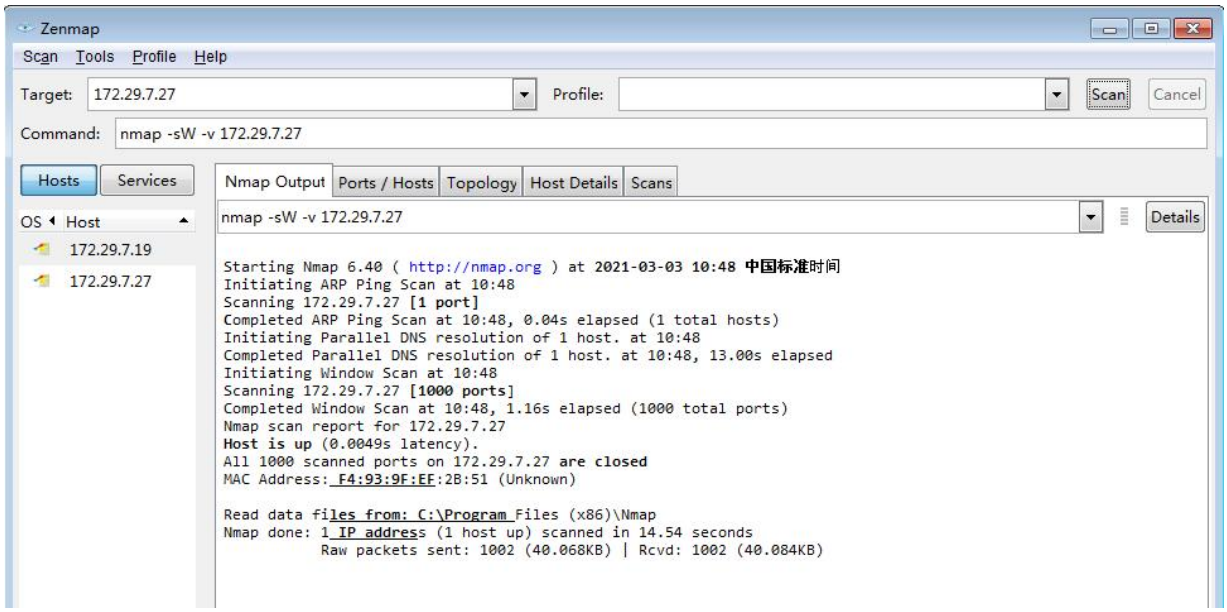


8、命令为：nmap　-sX　-v172.29.7.27

9、命令为：nmap　-sA　-v 172.29.7.27



10、命令为：nmap　-sW　-v 172.29.7.27

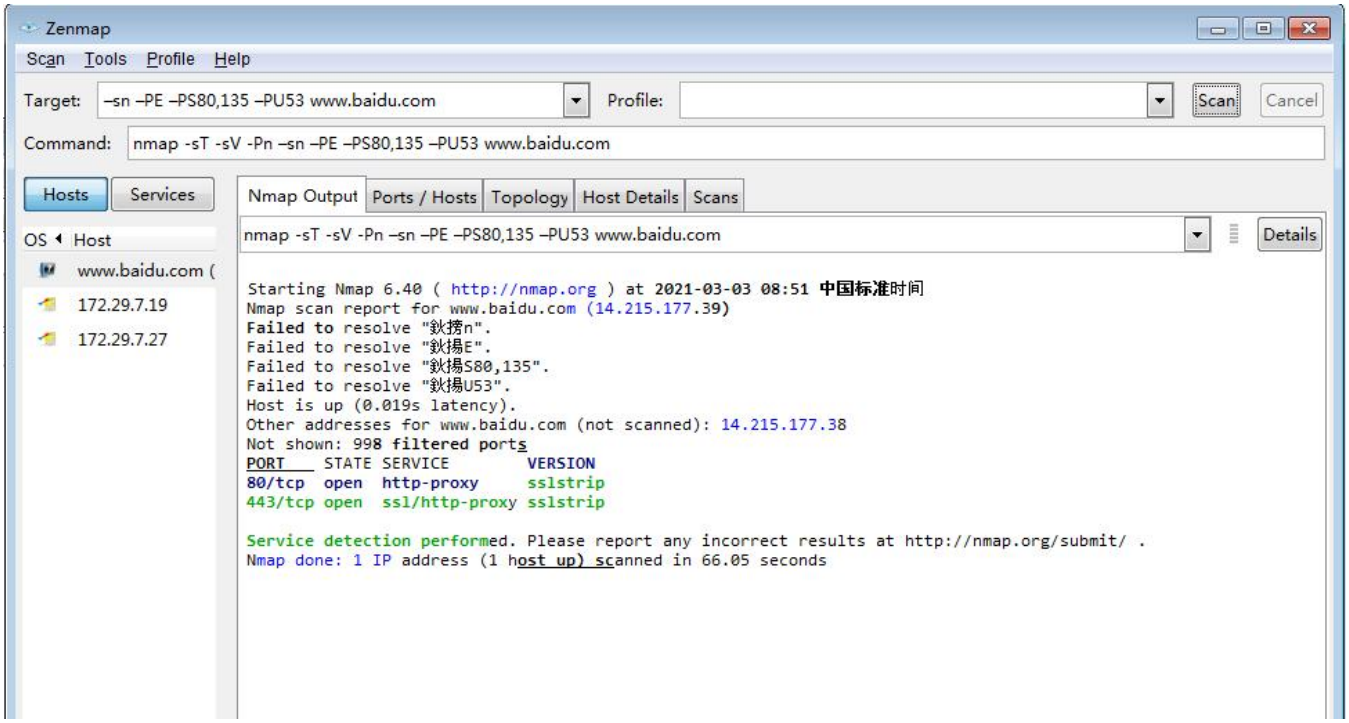


11、探测 www.baidu.com

下面以探测 www.baidu.com 的主机为例，简单演示主机发现的用法。

命令：nmap –sn –PE –PS80,135 –PU53 www.baidu.com

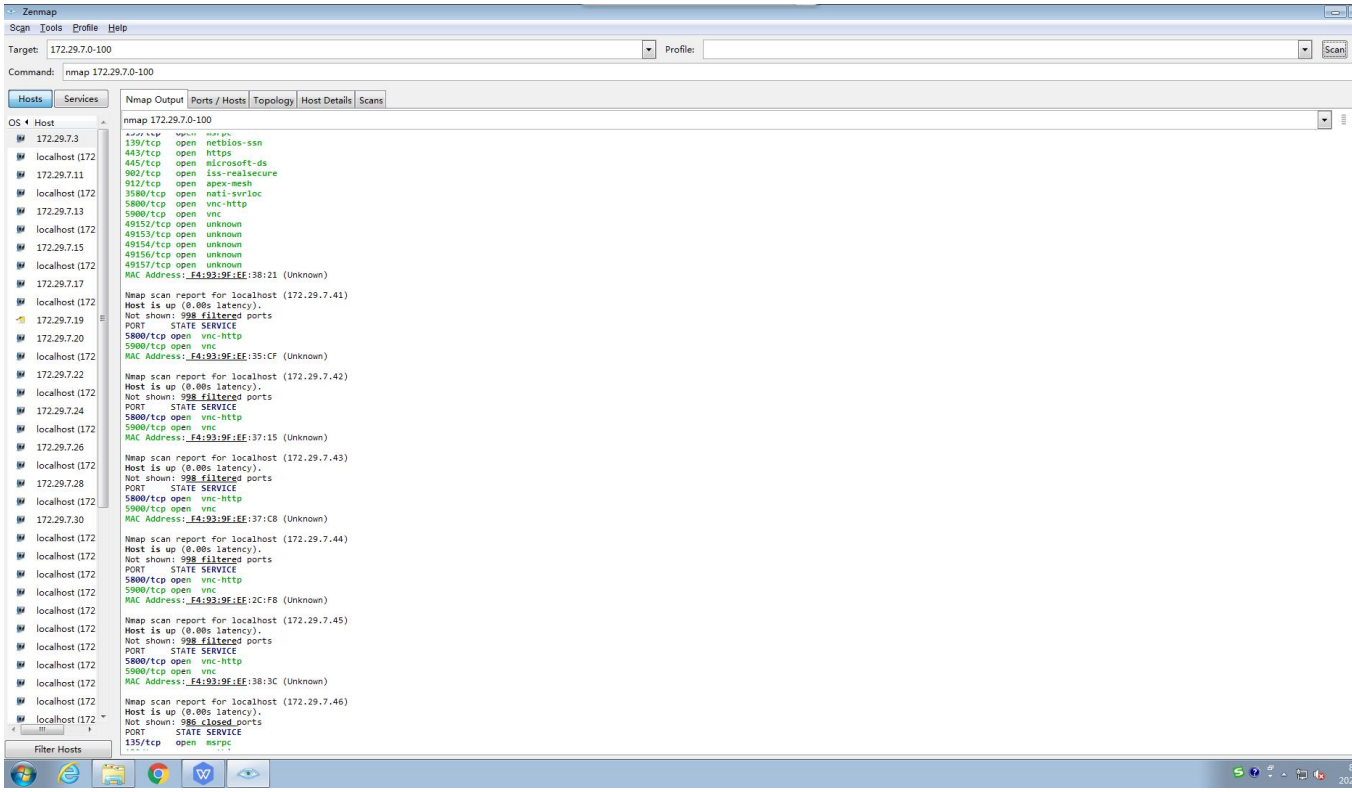
注：使用 nmap –sn –PE –PS80,135 –PU53 www.baidu.com 命令扫描不出来，原因是使用拨号上网，协议使用的是 ppp，nmap 不识别。解决方法：加上 -sT -Pn 两个参数即可。




```
Nmap scan report for www.baidu.com (180.97.33.107)
Failed to resolve "鈥撴n".
Failed to resolve "鈥撴E".
Failed to resolve "鈥撴S80,135".
Failed to resolve "鈥撴U53".
Host is up (0.13s latency).
Other addresses for www.baidu.com (not scanned): 180.97.33.108
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

主机处于打开状态。

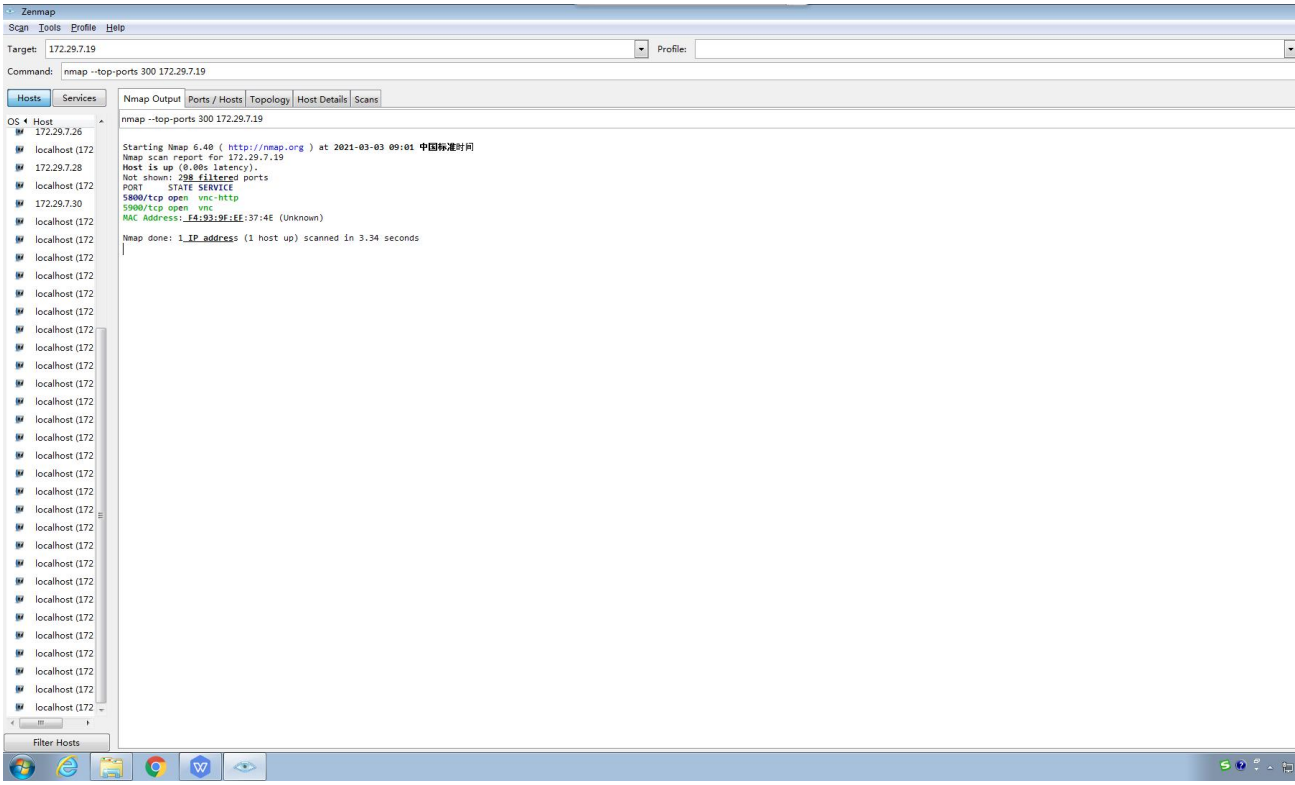
12、nmap 192.168.0.28-100



13、--top-ports <number>:扫描开放概率最高的 number 个端口（nmap 的作者曾经做过大规模地互联网扫描，以此统计出网络上各种端口可能开放的概率。

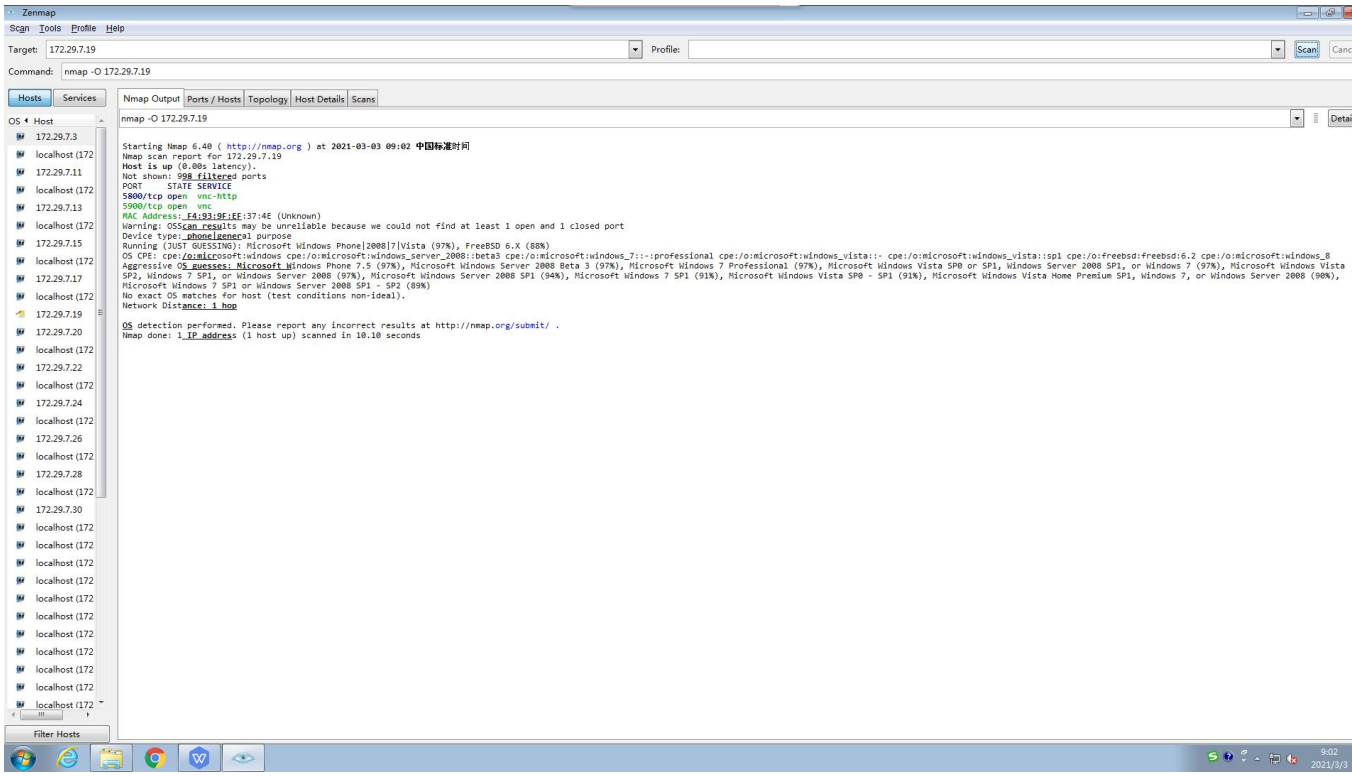
以扫描局域网内 192.168.0.28 主机为例

命令如下： nmap --top-ports 300 192.168.0.28



14、-sO: 使用 IP protocol 扫描确定目标机支持的协议类型。

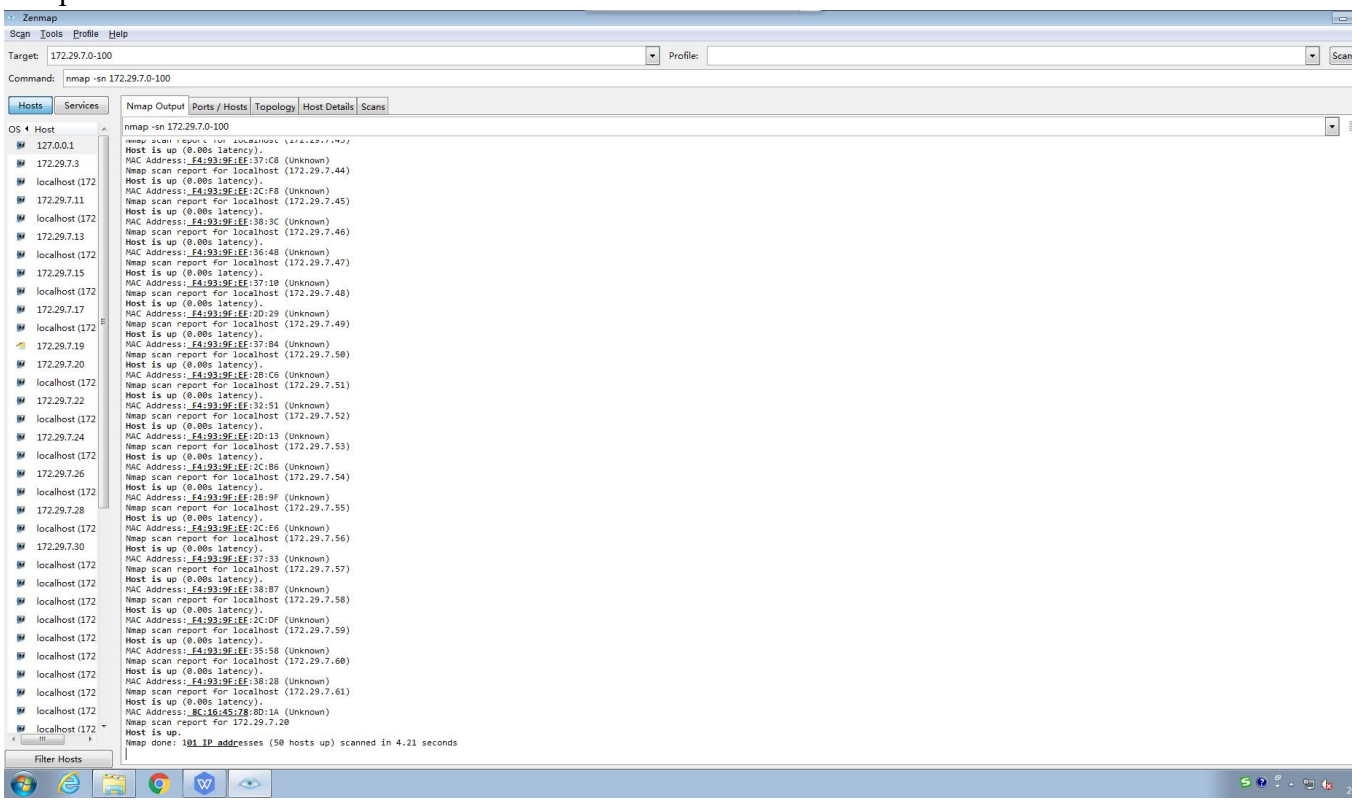
命令为：nmap -O 192.168.0.28



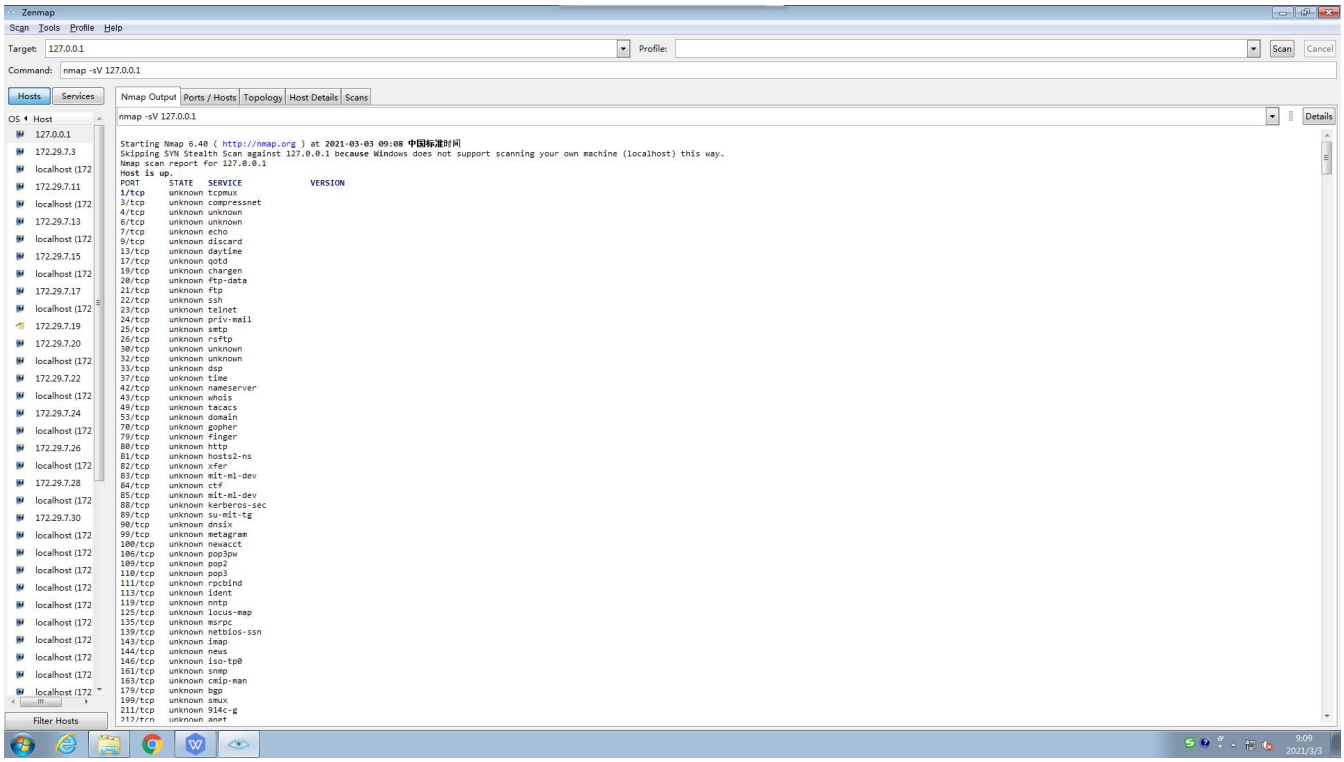
```
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.0.28 are filtered
MAC Address: 48:5A:B6:64:ED:B9 (Hon Hai Precision Ind. Co.)
```

15、扫描局域网 192.168.0.28-192.168.0.100 范围内哪些 IP 的主机是活动的。

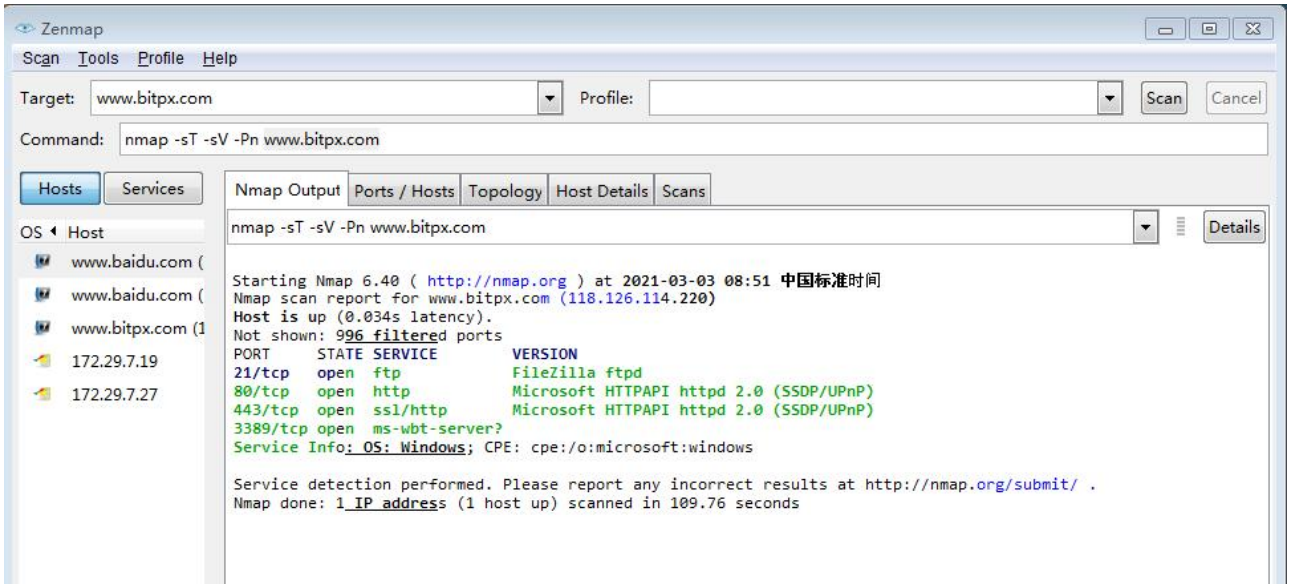
namp -sn 192.168.0.28-100



16、nmap -sV 127.0.0.1



17.Nmap -sV www.bitpx.com



```
Starting Nmap 6.40 ( http://nmap.org ) at 2021-03-03 08:51 中国标准时间
Nmap scan report for www.bitpx.com (118.126.114.220)
Host is up (0.034s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            FileZilla ftpd
80/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp  open  ssl/http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server?
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 109.76 seconds
```

五、**结果分析与实验体会**（试验中遇到的问题及解决过程，产生的错误及原因分析，试验体会和收获）

Nmap 是一个网络探测和漏洞扫描程序

安全管理人员可以使用 Nmap 软件对系统和网络进行扫描，获取网络中正在运行的主机以及主机提供的服务等信息。

Nmap 通过探测将端口划分为 6 个状态 1. open：端口是开放的。2. closed：端口是关闭的。3. filtered：端口被防火墙 IDS/IPS 屏蔽，无法确定其状态。4. unfiltered：端口没有被屏蔽，但是否开放需要进一步确定。5. open|filtered：端口是开放的或被屏蔽。6. closed|filtered ：端口是关闭的或被屏蔽。