

《信息对抗技术》课程作业 范例

学号：\_\_\_\_\_ 姓名：\_\_\_\_\_ 成绩：\_\_\_\_\_

---

## 实验 扫描工具的使用

### 一、实验目的

1. 熟悉Nmap使用方法，熟悉扫描工具的原理。
2. 使用 Nmap 扫描网站。

### 二、实验环境

1. 系统环境：Win7
2. 使用软件：NMap

### 三、实验原理

#### 1.NMap

NMap，也就是 Network Mapper，最早是 Linux 下的网络扫描和嗅探工具包。Nmap 是一种目前最强大的信息收集工具，其中综合了各种扫描模式和 OS Fingerprint 技术，以及 TCP 序列号预测难度评估，这种扫描工具不会产生大量的日志记录。它是一款开源的扫描工具，用于系统管理员查看一个大型的网络有哪些主机及其上运行何种服务。它支持多种协议的扫描如 UDP、TCP connect ()、TCP SYN (半连接)、Ftp Proxy (暴力攻击)、Reverse-Ident、ICMP (ping Sweep)、FIN、ACK Sweep、Xmas Tree、SYN Sweep 和 Null 扫描。Nmap 还提供一些实用功能如通过 TCP/IP 来鉴别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 ping 鉴别下属的主机、欺骗扫描、端口过滤探测、直接的 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述。Nmap 的特色在于秘密扫描，操作系统探测，多种扫描模式以及指纹识别技术。

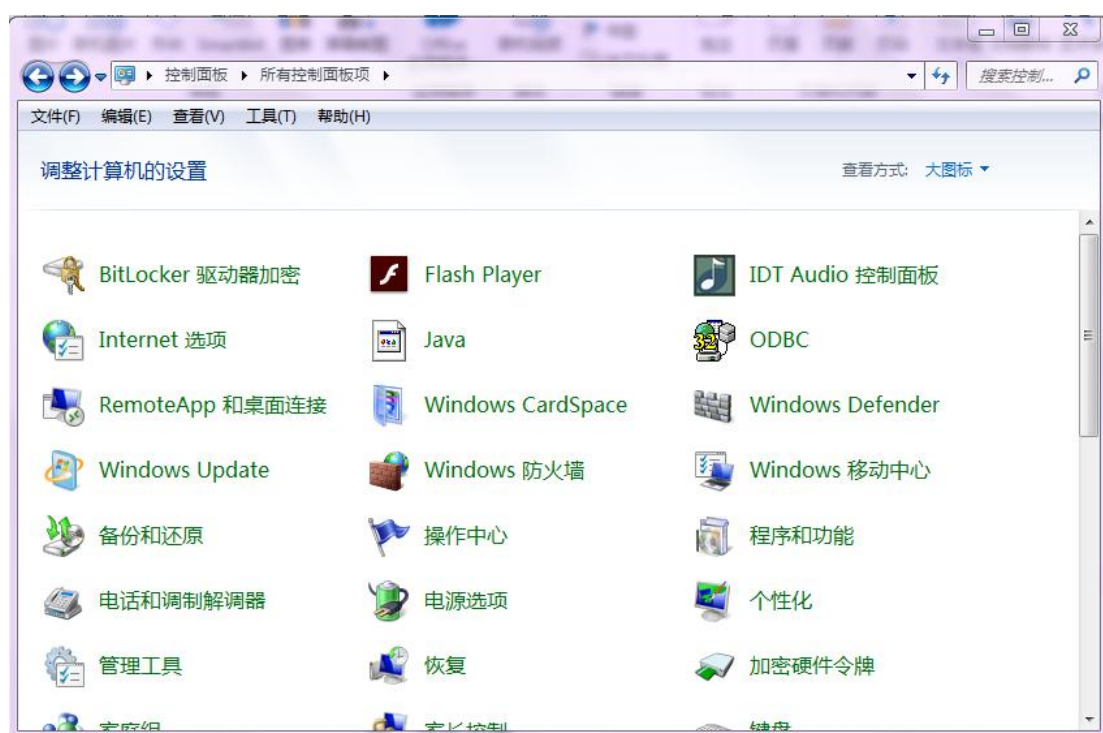
Nmap 输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。

## 四、实验步骤

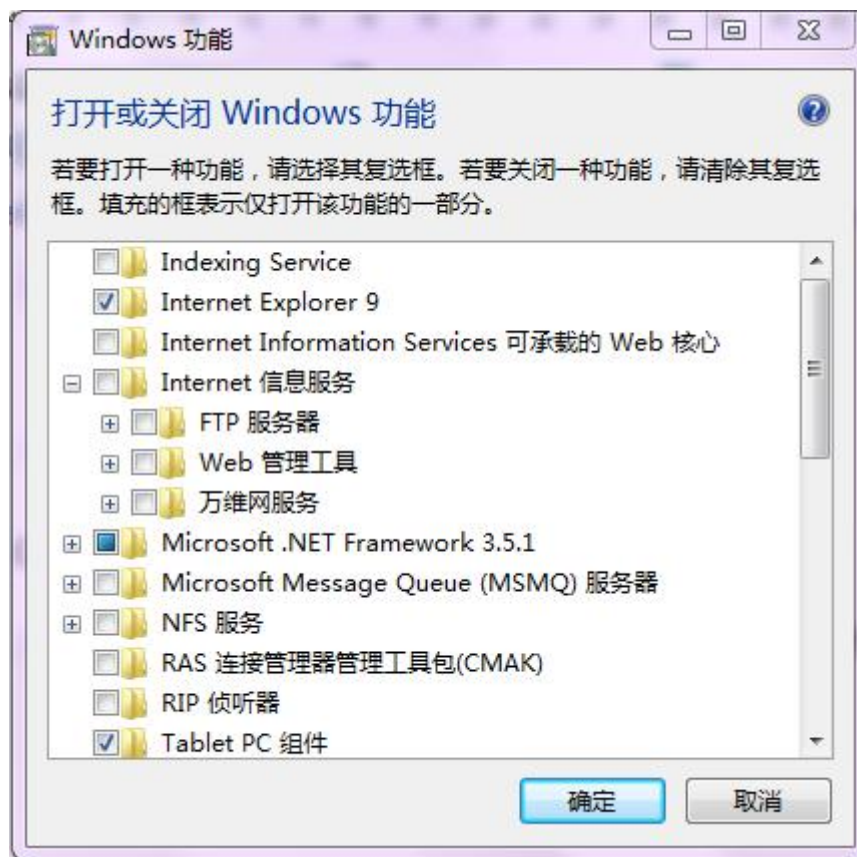
这一部分包含三个内容：配置计算机的相关功能、Nmap 的安装步骤、使用 Nmap 工具扫描实验。

### （a）配置计算机相关功能

#### 1、打开计算机控制面板，找到程序与功能



#### 2、选择<程序与功能>-<打开或关闭 Windows 功能>




















3、勾选 Internet 信息服务下的万维网服务，点击确定



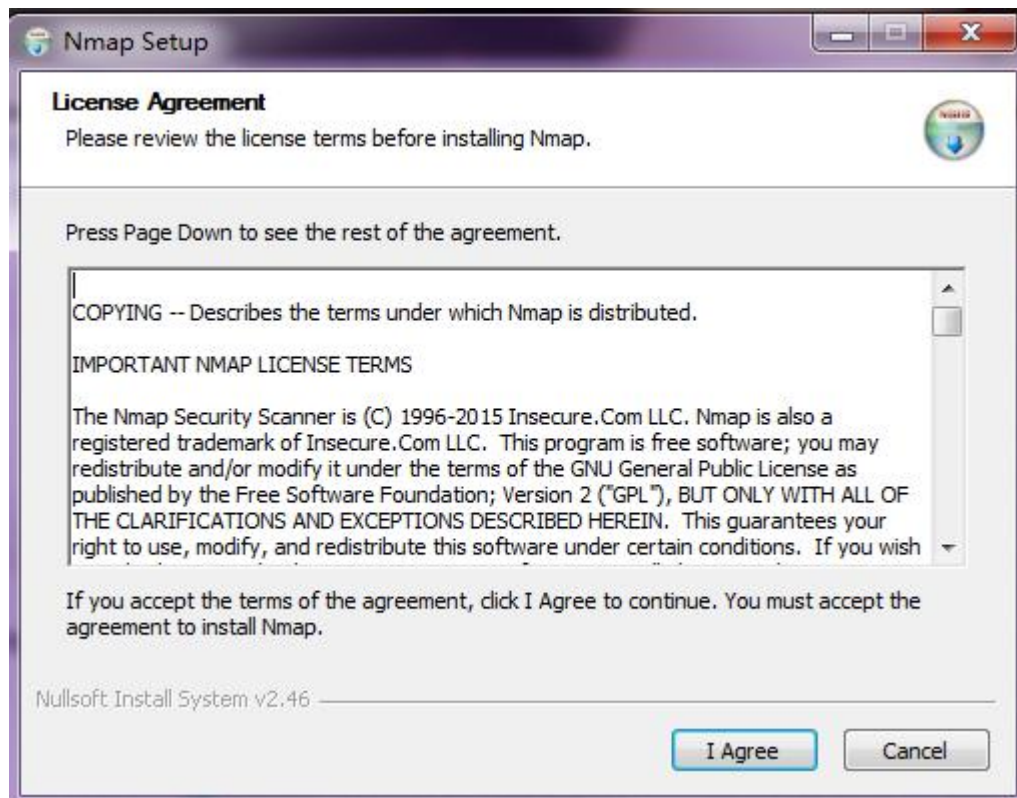
## (b) Nmap 的获取与安装

1、进入网站 <https://nmap.org/dist/?C=M&O=D>，选择自己需要的版本

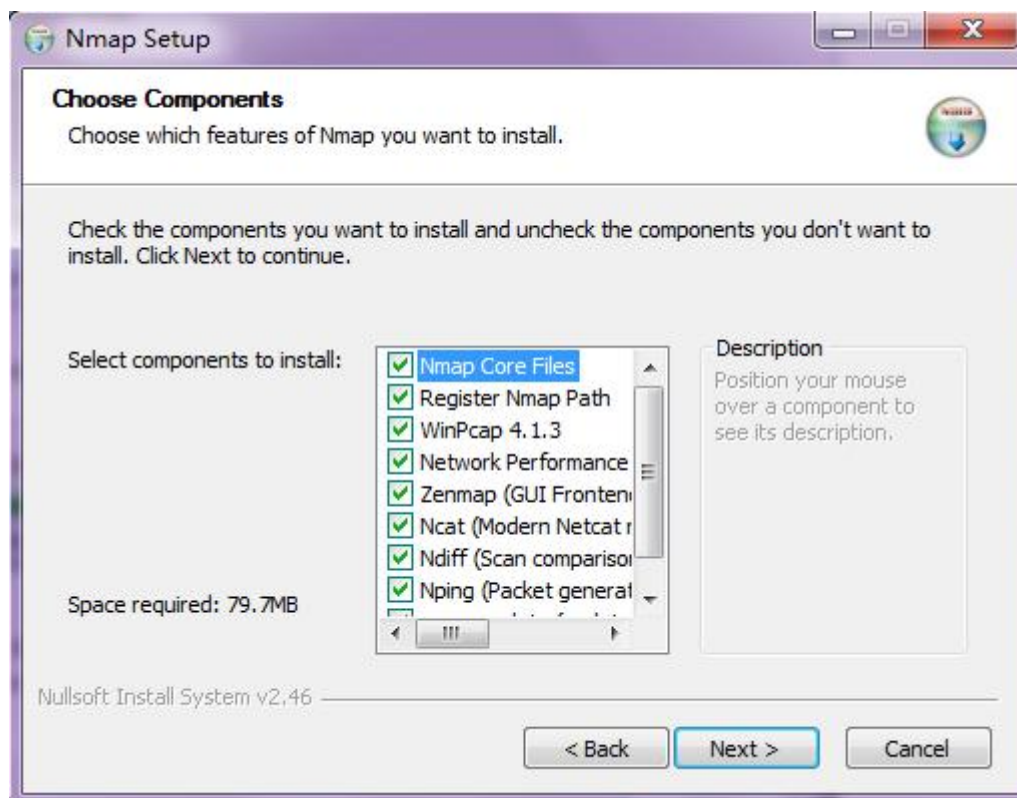


<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">sigs/</a>	2016-03-30 05:26	-	
 <a href="#">zenmap-7.12-1.noarch.rpm</a>	2016-03-29 12:31	691K	
 <a href="#">nping-0.7.12-1.x86_64.rpm</a>	2016-03-29 12:31	1.1M	
 <a href="#">nping-0.7.12-1.i686.rpm</a>	2016-03-29 12:31	822K	
 <a href="#">nmap-update-7.12-1.x86_64.rpm</a>	2016-03-29 12:31	14K	
 <a href="#">nmap-update-7.12-1.i686.rpm</a>	2016-03-29 12:31	13K	
 <a href="#">nmap-7.12-win32.zip</a>	2016-03-29 12:31	14M	
 <a href="#">nmap-7.12.tgz</a>	2016-03-29 12:31	11M	
 <a href="#">nmap-7.12.tar.bz2</a>	2016-03-29 12:31	8.5M	
 <a href="#">nmap-7.12-setup.exe</a>	2016-03-29 12:31	25M	
 <a href="#">nmap-7.12.dmg</a>	2016-03-29 12:31	28M	
 <a href="#">nmap-7.12-1.x86_64.rpm</a>	2016-03-29 12:31	6.0M	
 <a href="#">nmap-7.12-1.src.rpm</a>	2016-03-29 12:31	11M	
 <a href="#">nmap-7.12-1.i686.rpm</a>	2016-03-29 12:31	5.7M	
 <a href="#">ncat-7.12-1.x86_64.rpm</a>	2016-03-29 12:31	1.2M	

2、点击开始安装，选择 I agree。

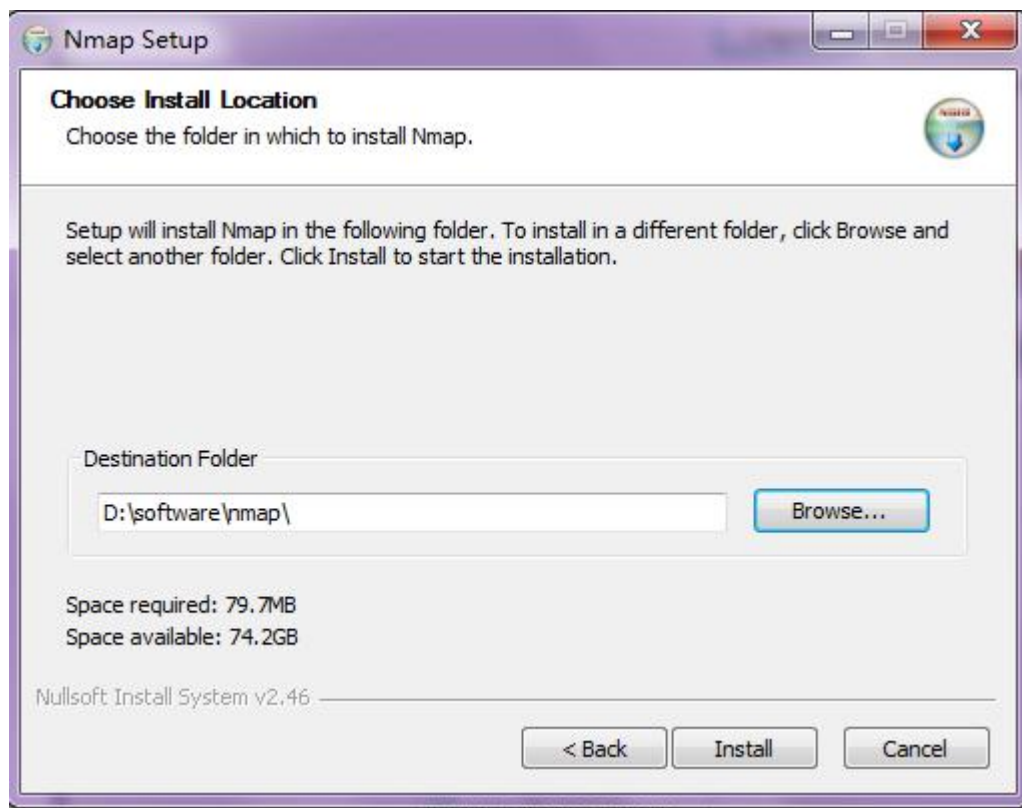


3、next→

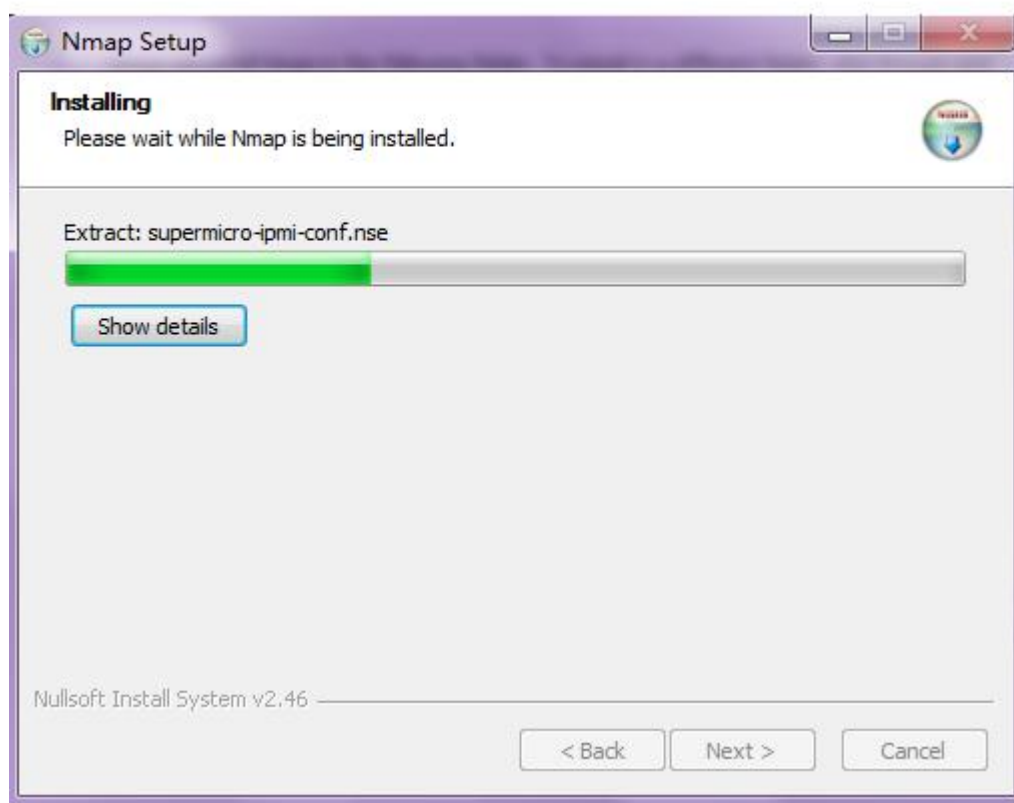




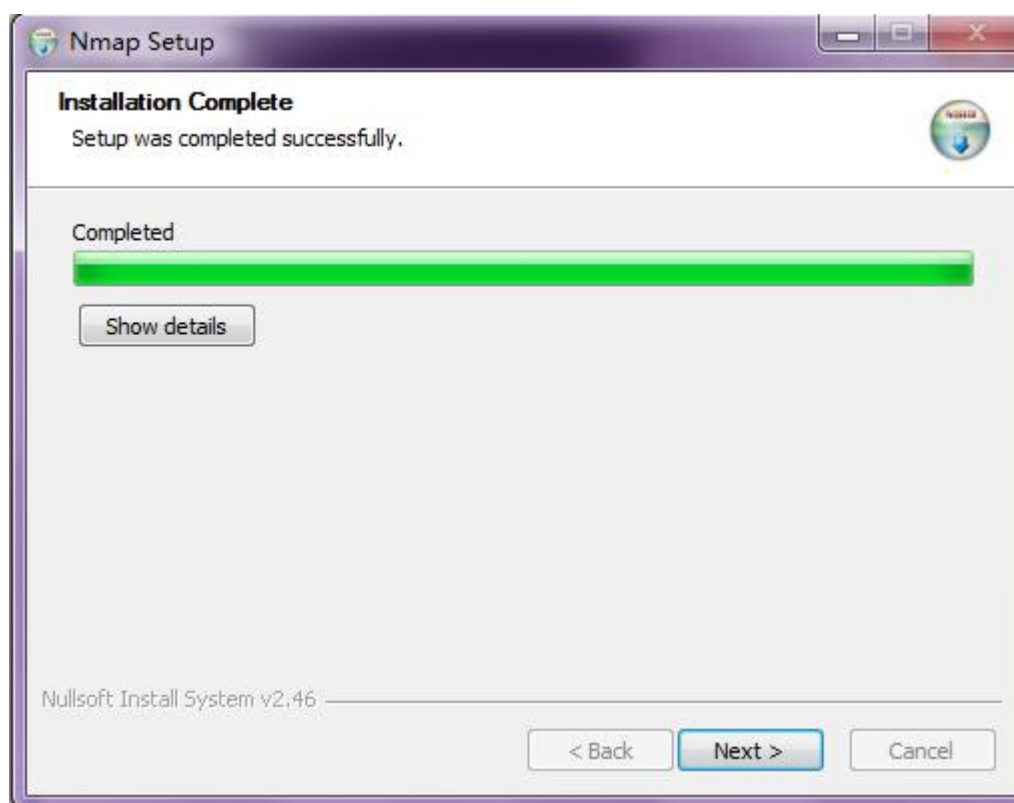
4、选择安装位置。



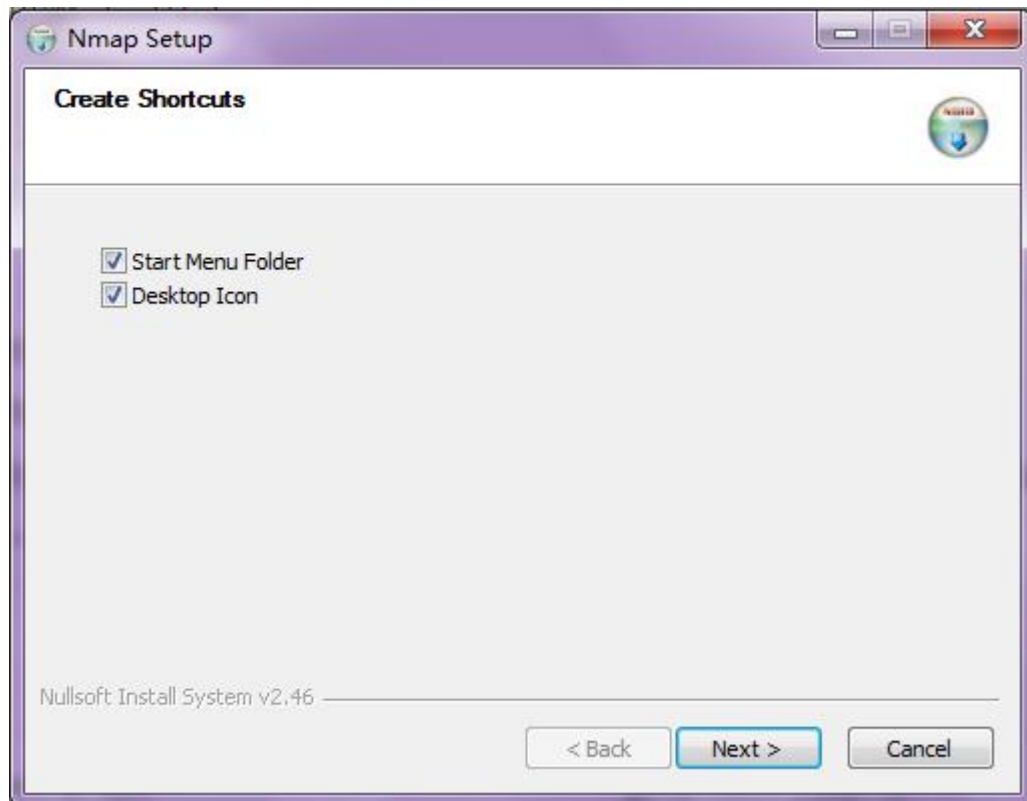
5、点击 Install



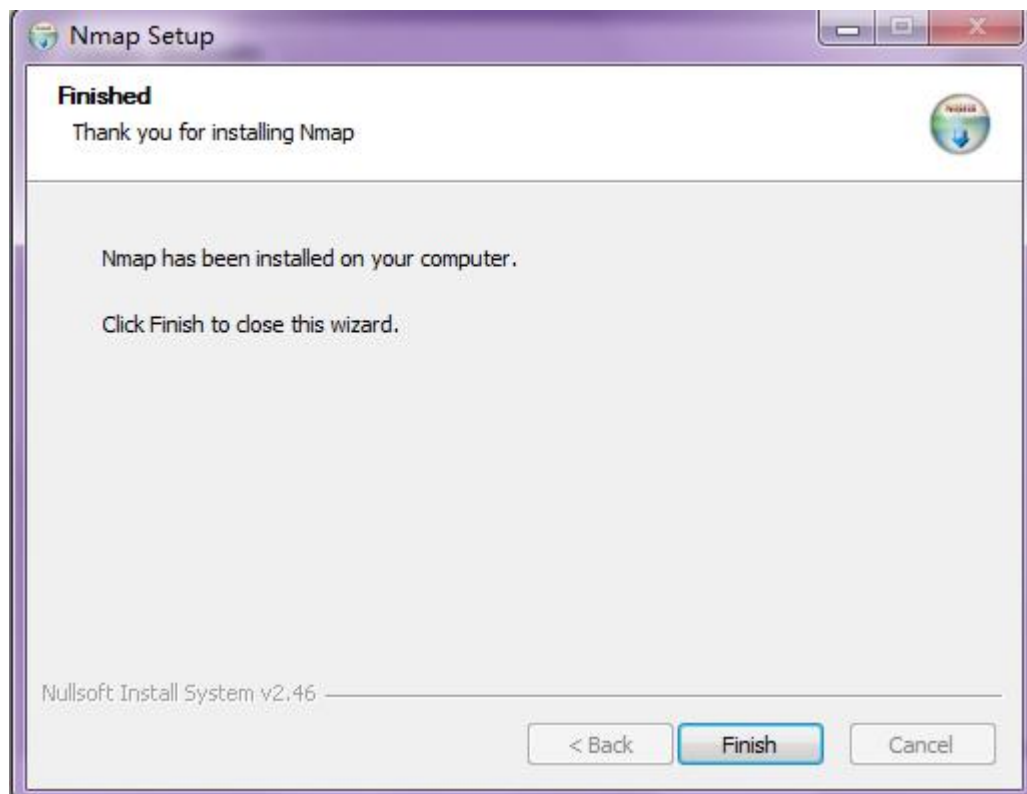
6、安装完成，点击 next



7、根据自己需要选择，并点击 next



8、点击 finish

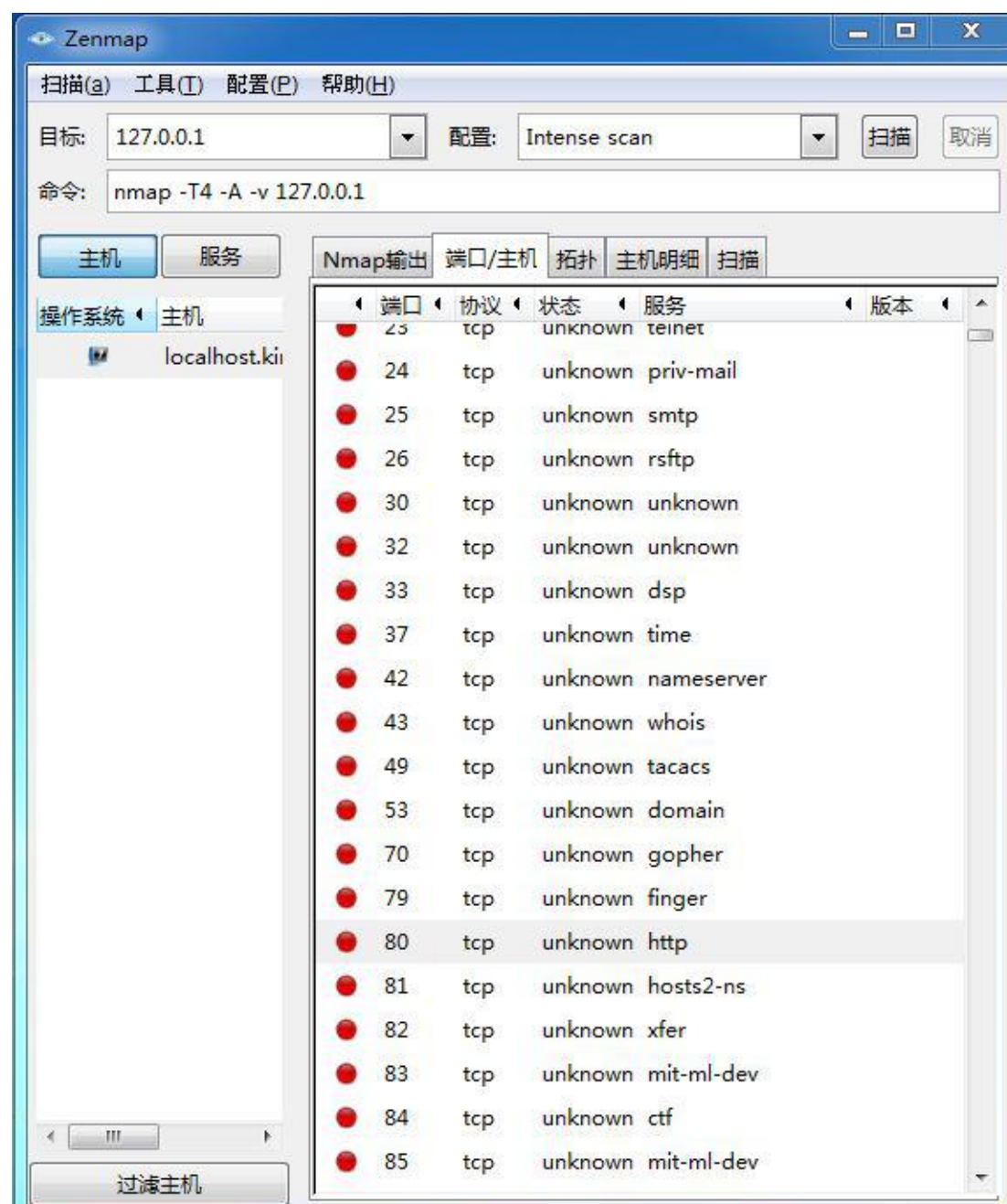


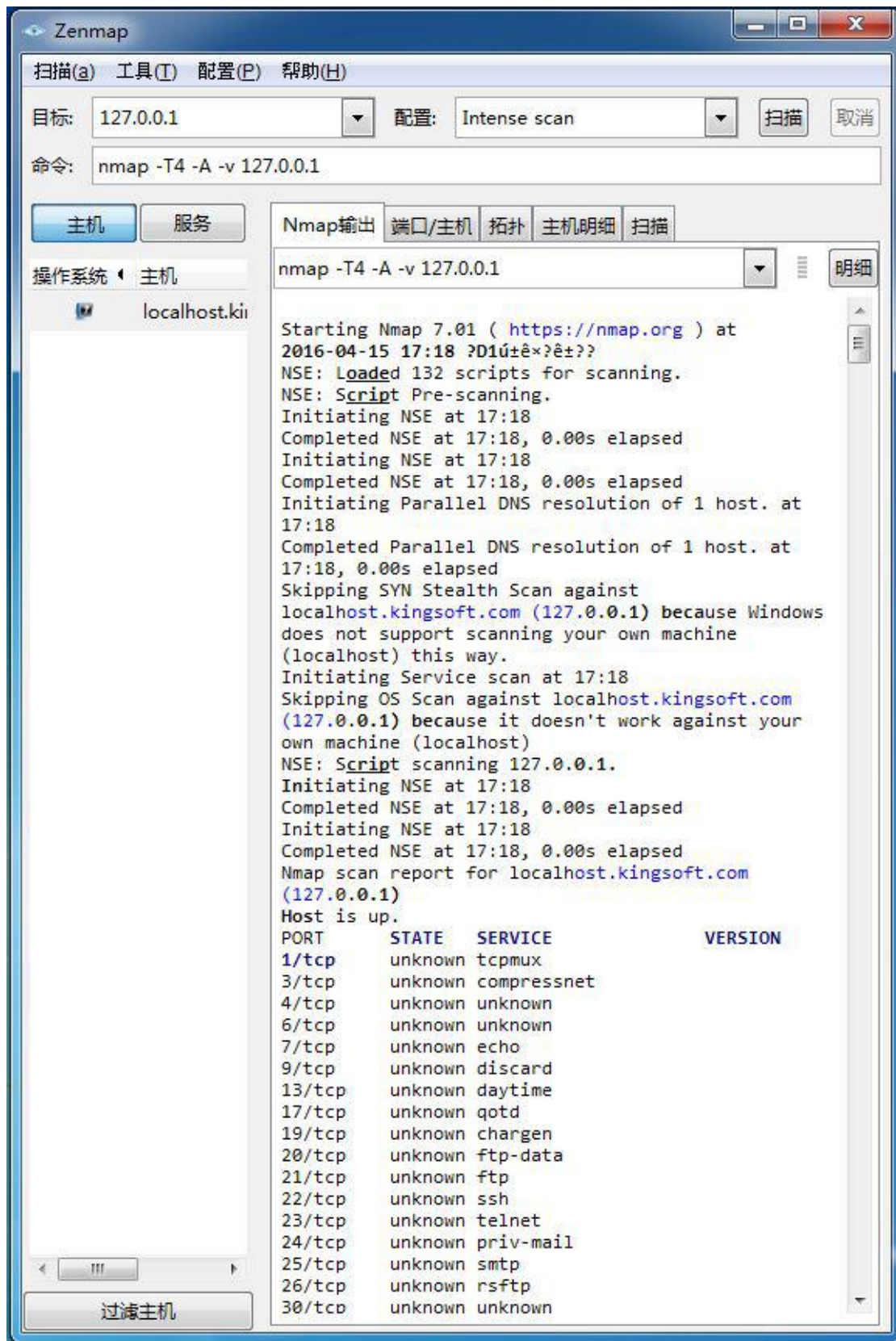


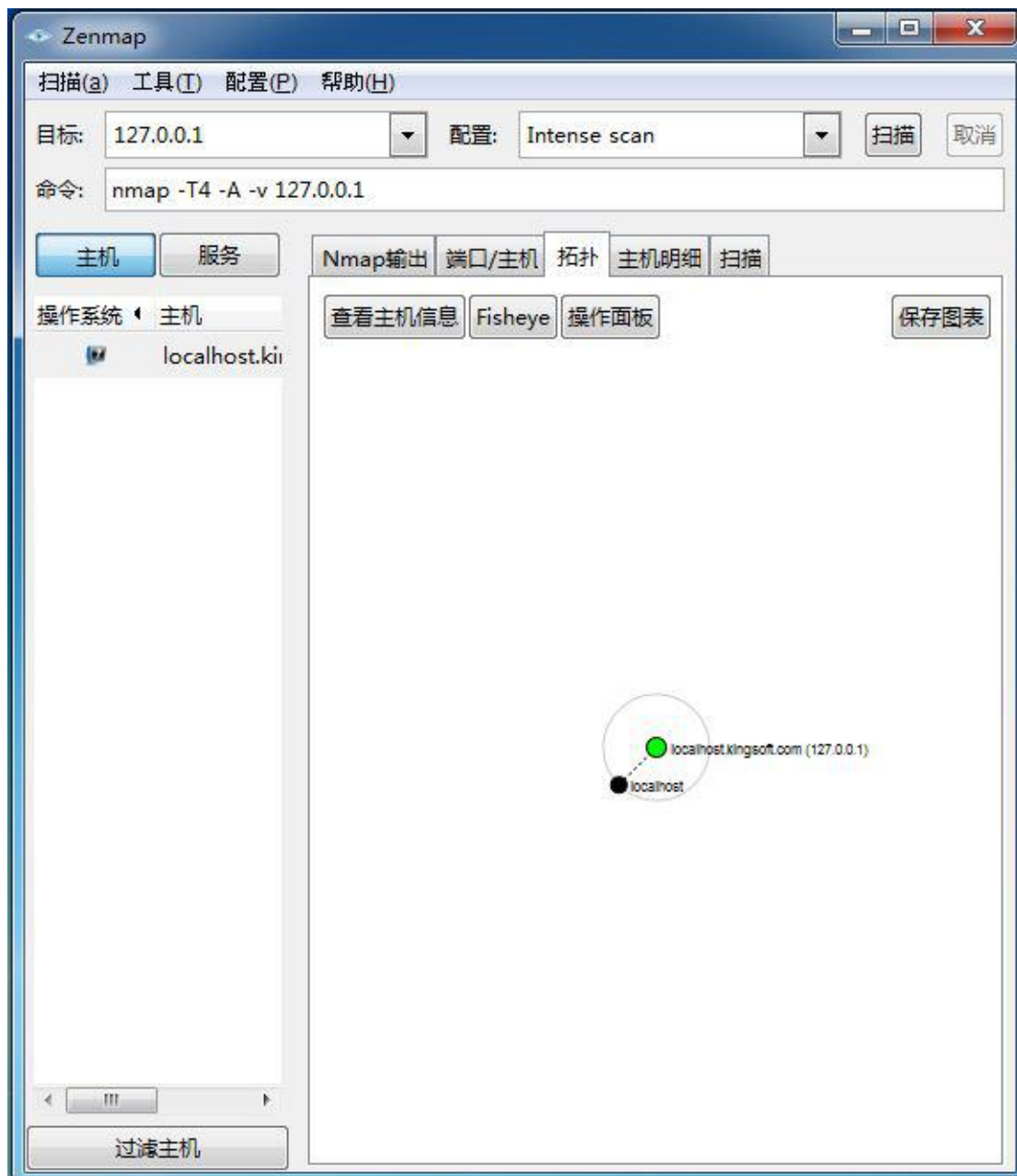
## (c) Nmap 的扫描实验

1、打开 Nmap，在目标上输入：

127.0.0.1







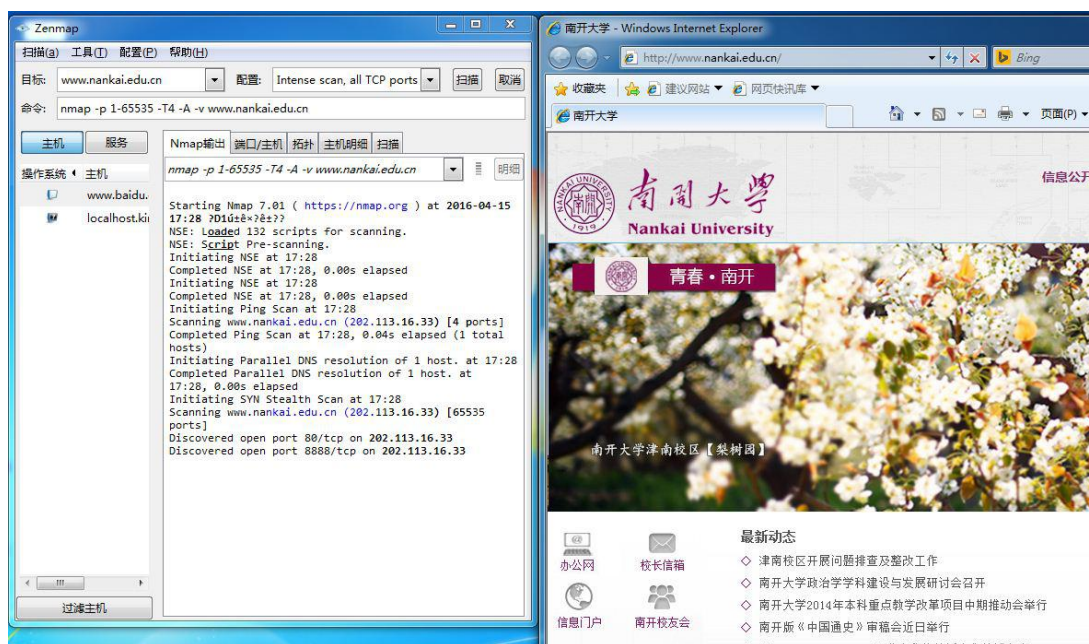
2、接下来把目标改为：[www.baidu.com](http://www.baidu.com)。可以看到 tcp 的 80 端口和 443 端口打开了。

**（注意：禁止扫描非实验用服务器！！！ 否则后果自负！！！）**

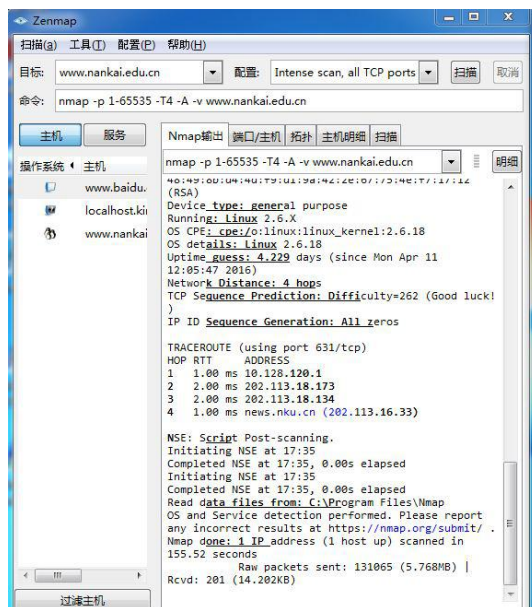
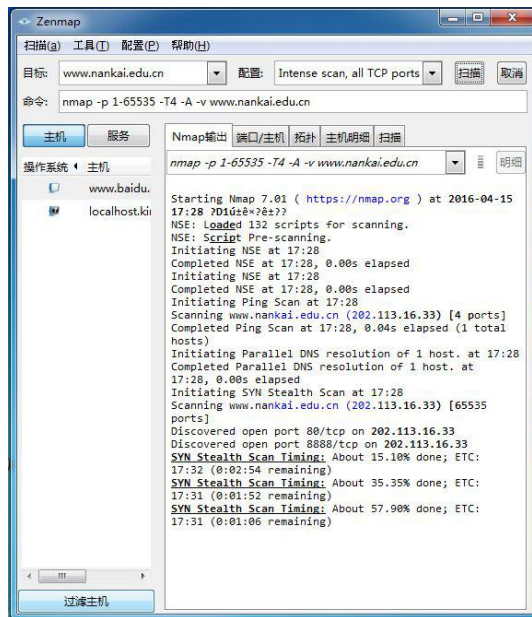


3、试一下学校的官网：[www.nankai.edu.cn](http://www.nankai.edu.cn).

(注意：禁止扫描非实验用服务器！！！否则后果自负！！！)









### 3. 检测端口

