《信息对抗技术》课程作业

学号：1911562 姓名：沙璇 专业：信息安全

实验 扫描工具的使用

1. **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：WinXP

2．使用软件：NMap

**三、实验原理**

1.NMap

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，显示的信息依赖于所使用的选项。

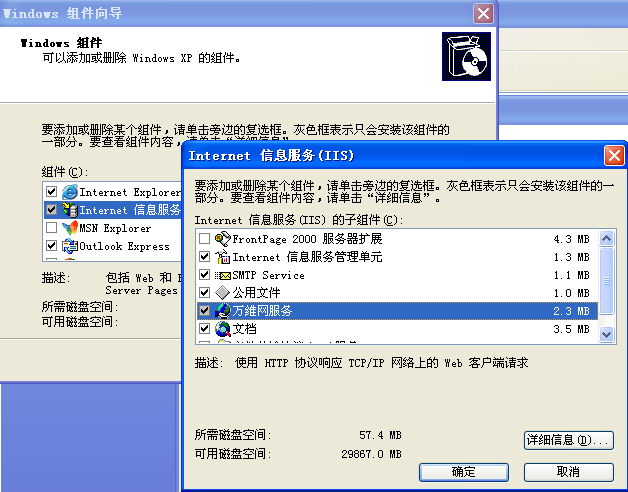
**四、实验步骤**

***（一）配置计算机的相关功能***

1、打开计算机控制面板，找到添加或删除程序，打开添加/删除windows组件

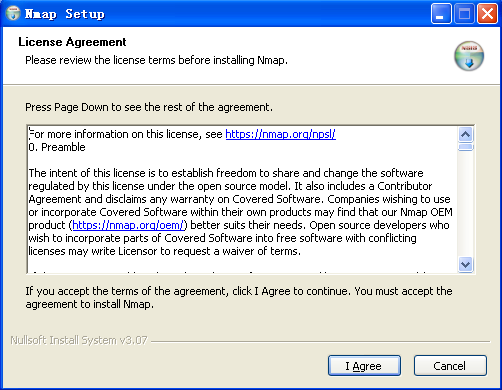


1. 勾选IIS下的万维网服务，点击确定

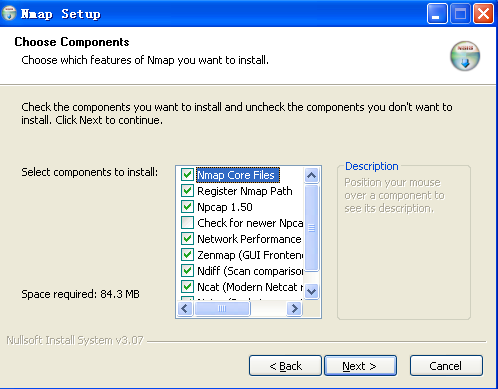


1. ***Nmap的安装***

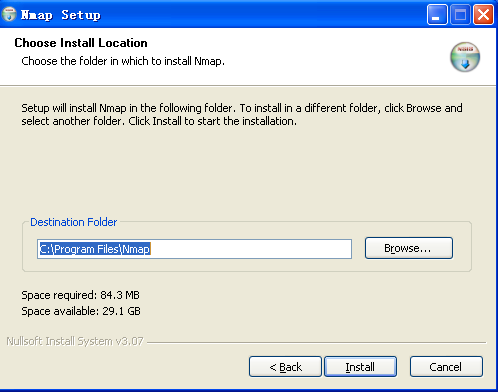
1、点击开始安装，选择 I agree



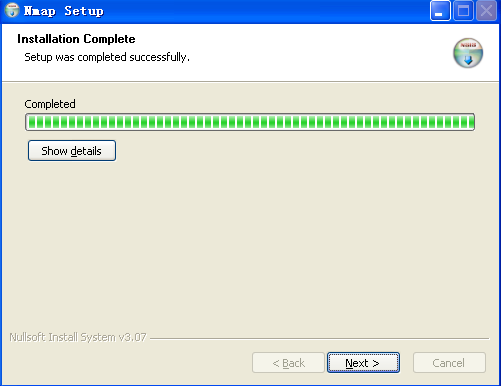
2、保持默认，点击next->

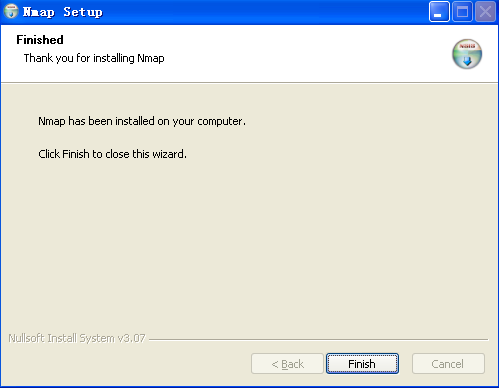


1. 选择安装位置

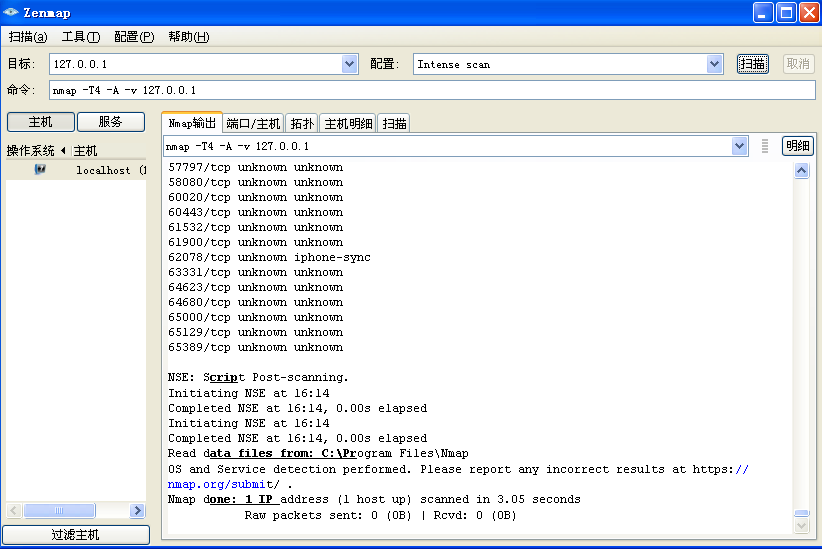


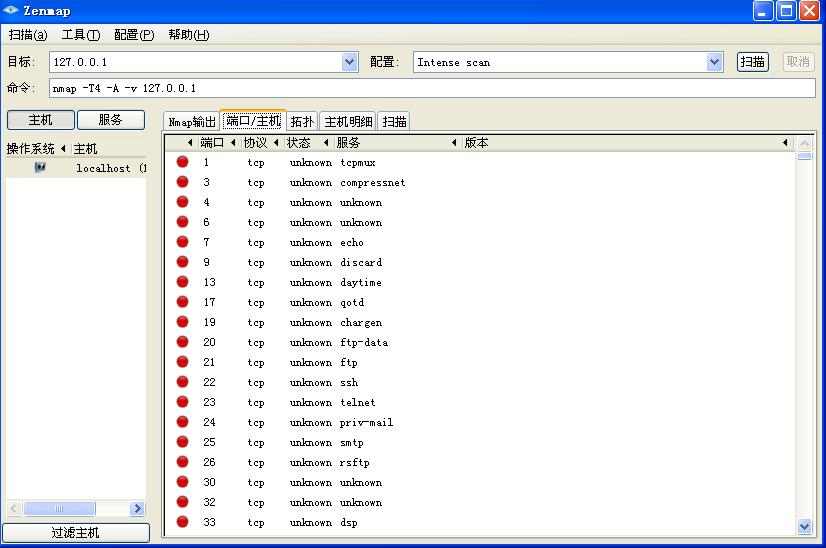
1. 点击install，点击next，最后点击finish安装成功

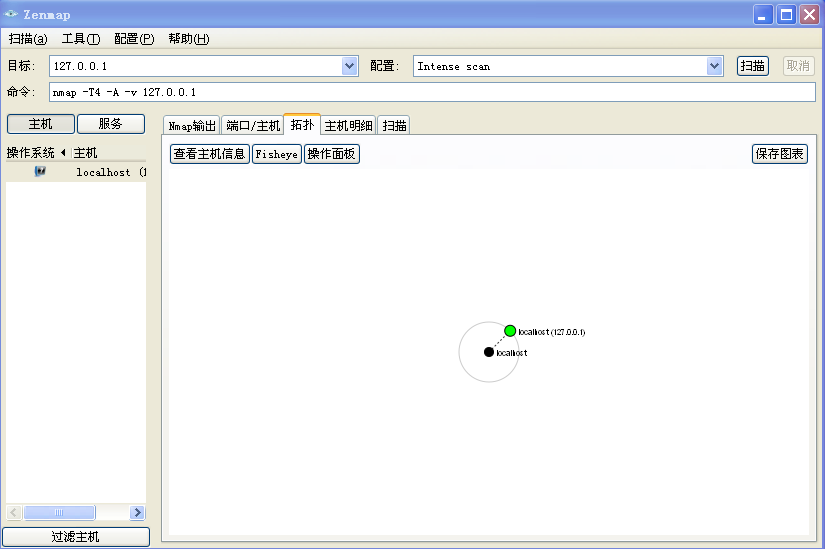




1. ***Nmap的扫描***
2. 打开 Nmap，在目标上输入： 127.0.0.1







1. 接下来把目标改为：www.baidu.com。可以看到 tcp 的 80 端口和 443 端口打开了。



