

**《信息对抗技术》课程实验报告**

**实验四：扫描工具的使用**

****

学 院 网络空间安全学院

专 业 信息安全

学 号 2112060

姓 名 孙蕗

1. **实验目的**
2. 熟悉Nmap使用方法，熟悉扫描工具的原理

2. 使用 Nmap 扫描网站。

1. **实验原理**

1.NMap

NMap（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。

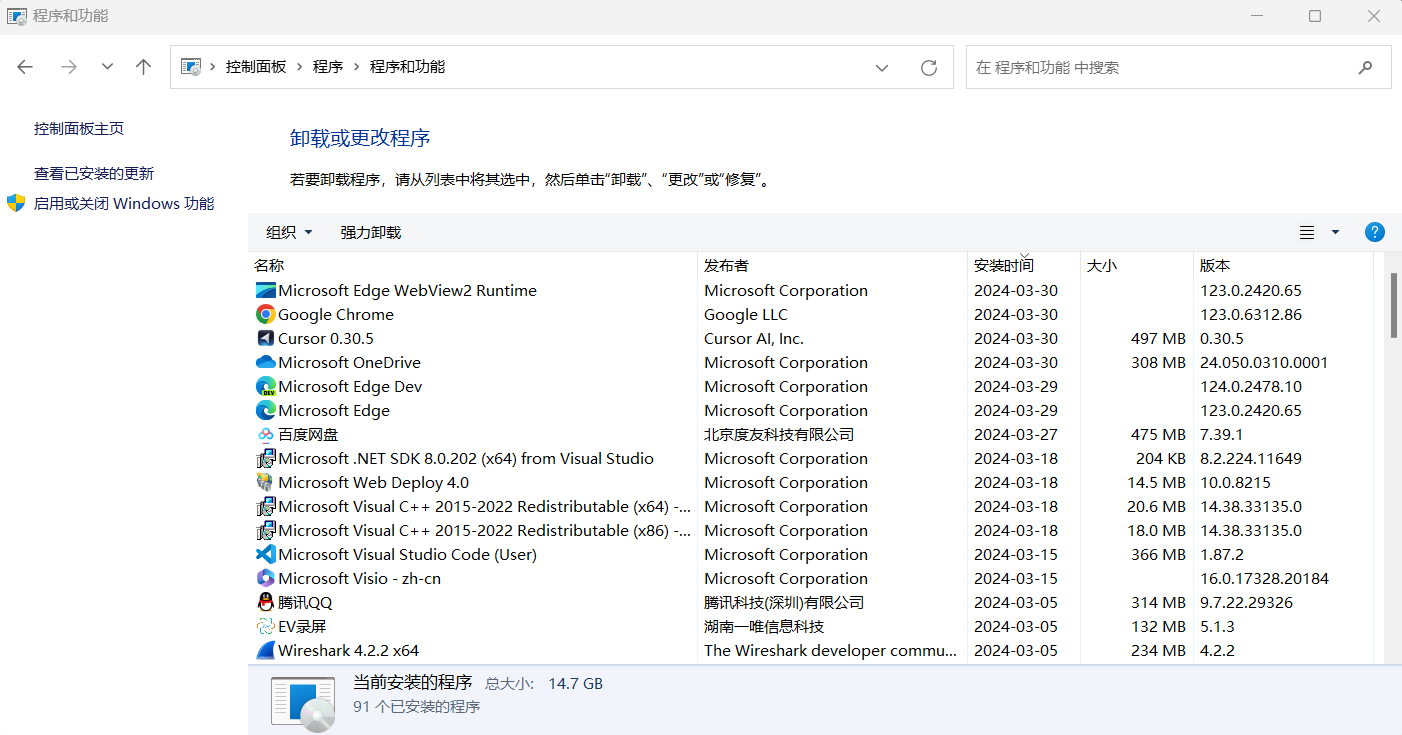
Nmap 输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。

1. **实验环境**

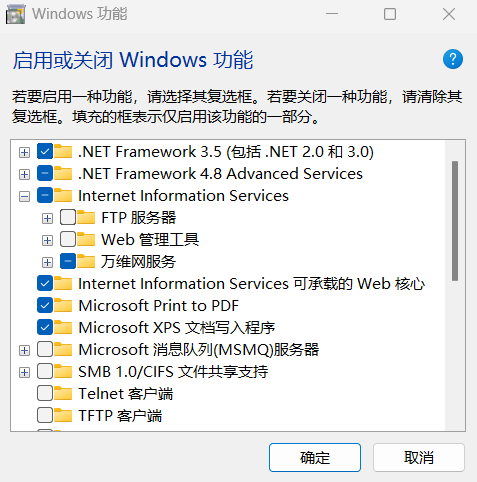
系统环境：Win10

使用软件：NMap

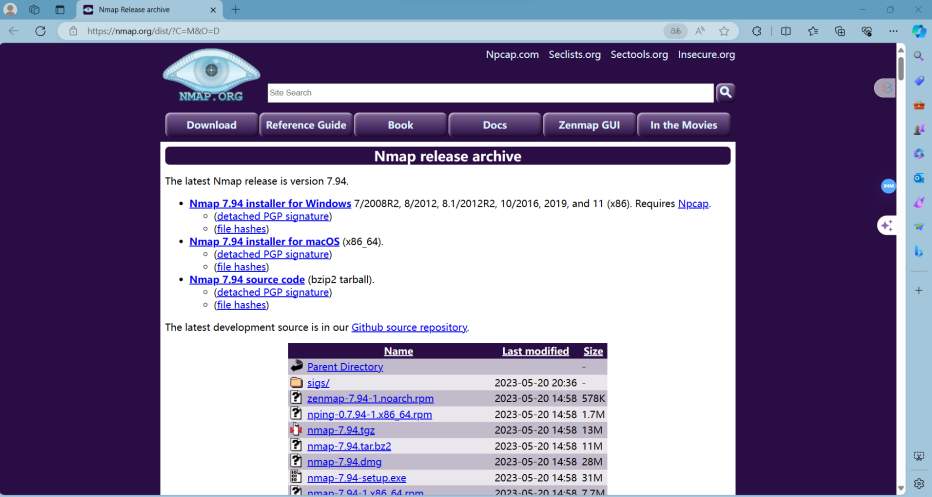
1. **实验过程**
2. 配置计算机的相关功能
3. 控制面板->程序与功能

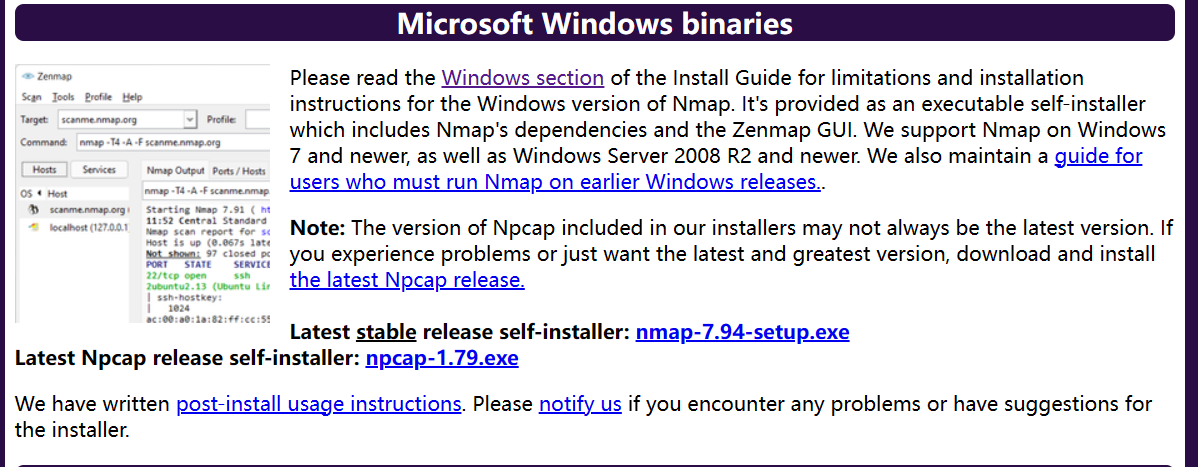


1. 选择启用或关闭Windows功能，勾选Internet Information Services的万维网服务



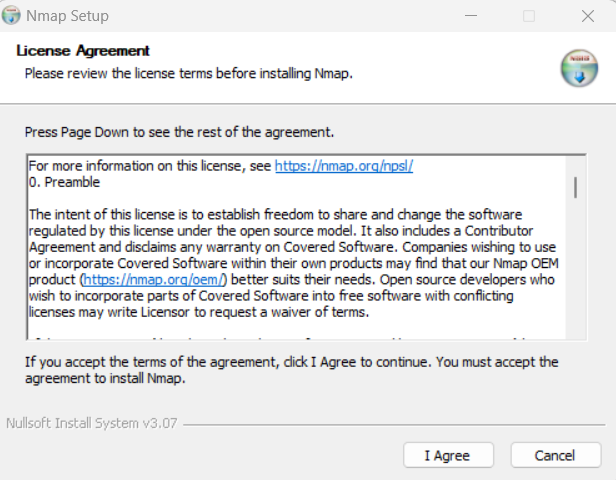
1. Nmap的获取安装
2. 进入网站 <https://nmap.org/dist/?C=M&O=D，选择自己需要的版本>

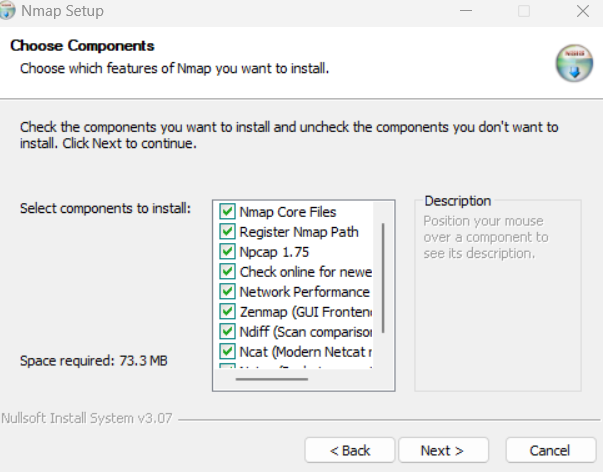


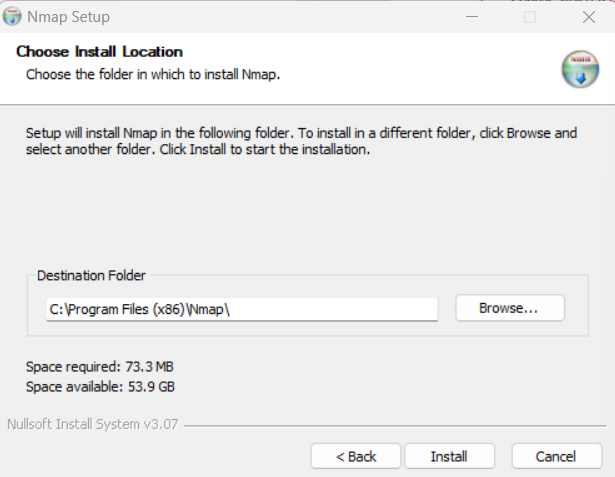


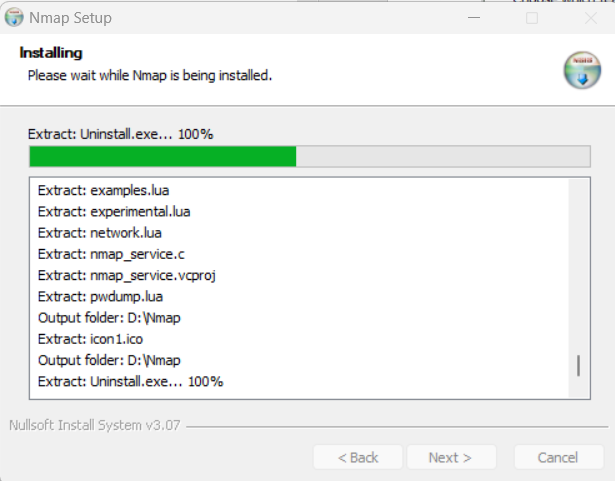
选择的是7.94的版本

1. 选择安装I agree，点击Next，选择好路径后install。等待一段时间完成安装。安装完成点击next。

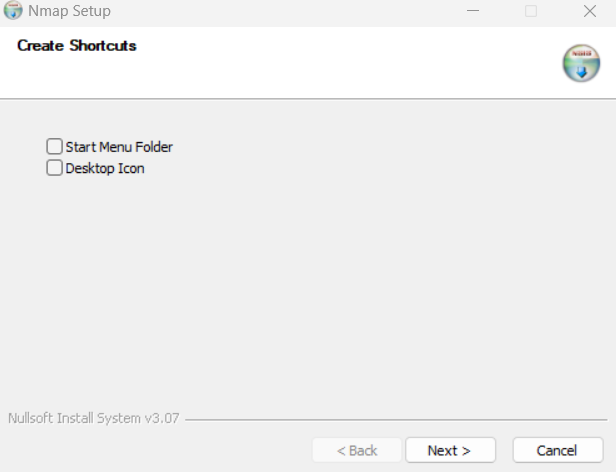




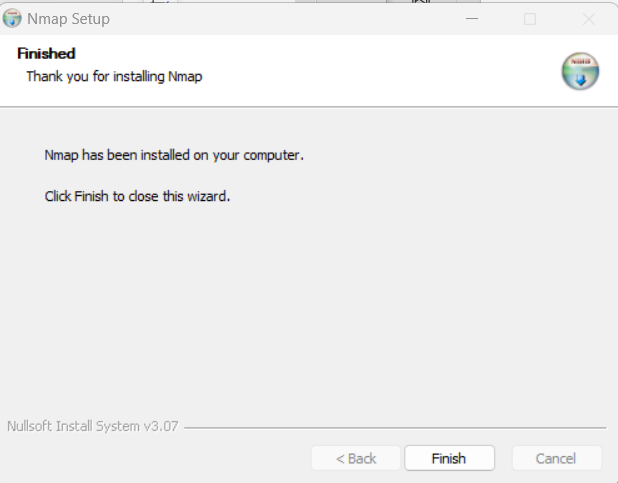




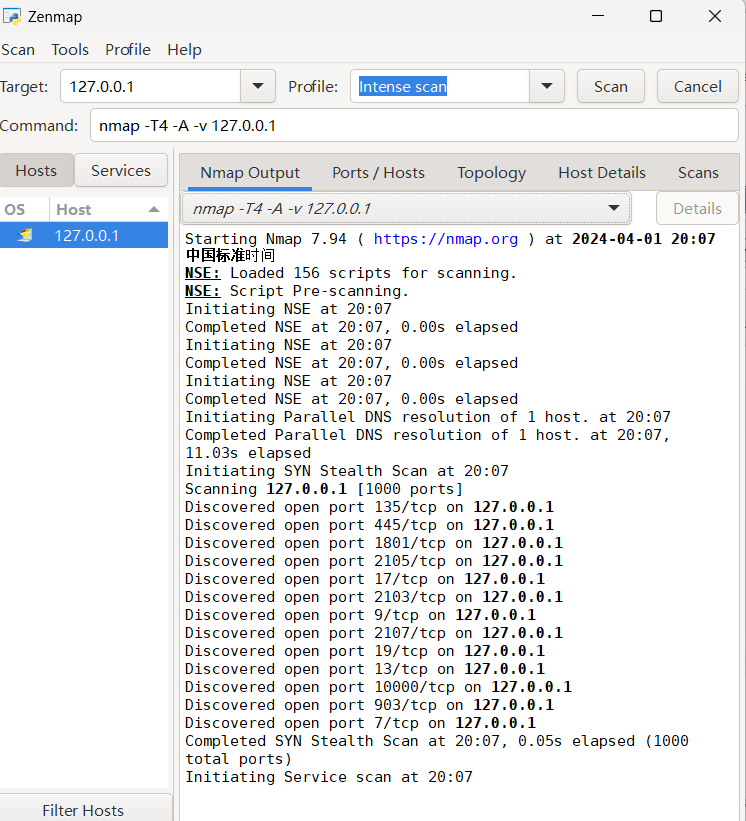
1. 根据自己的需要选择，然后点击next

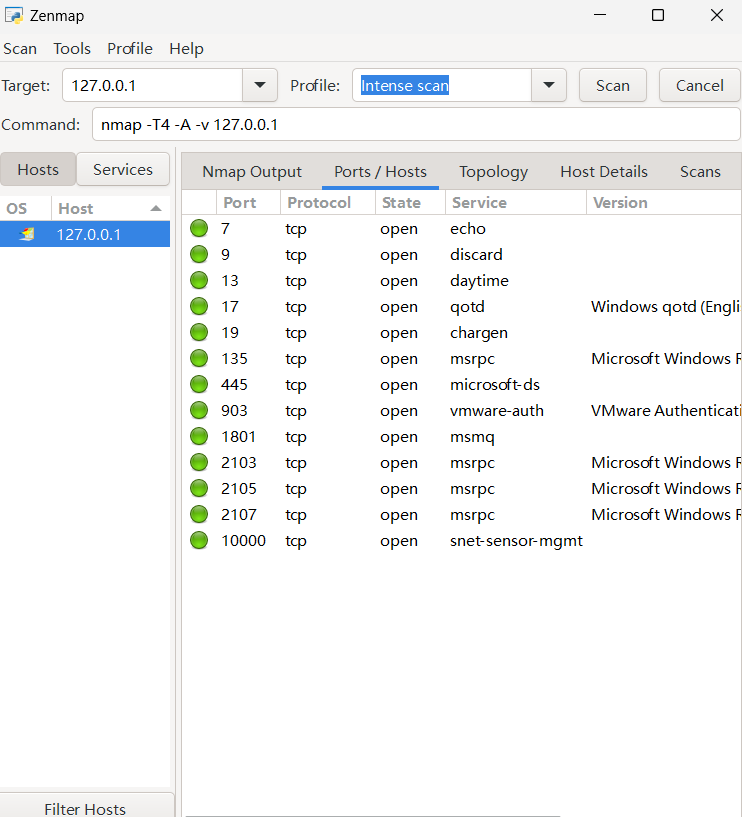


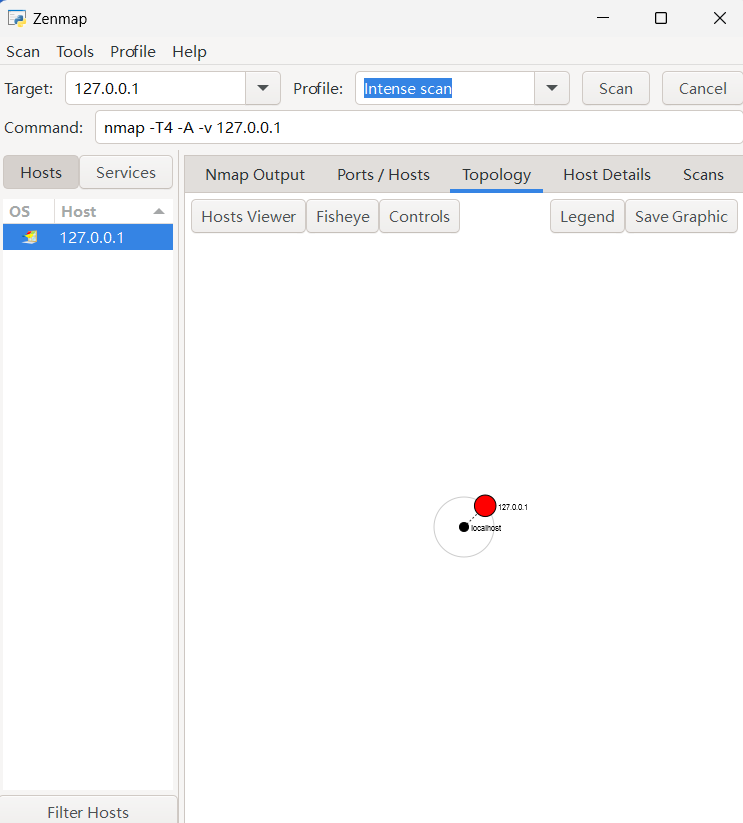
1. 点击finish完成安装



1. 使用Nmap进行扫描
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。

