

南开大学

《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_____孙璐_____

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。

三、实验环境

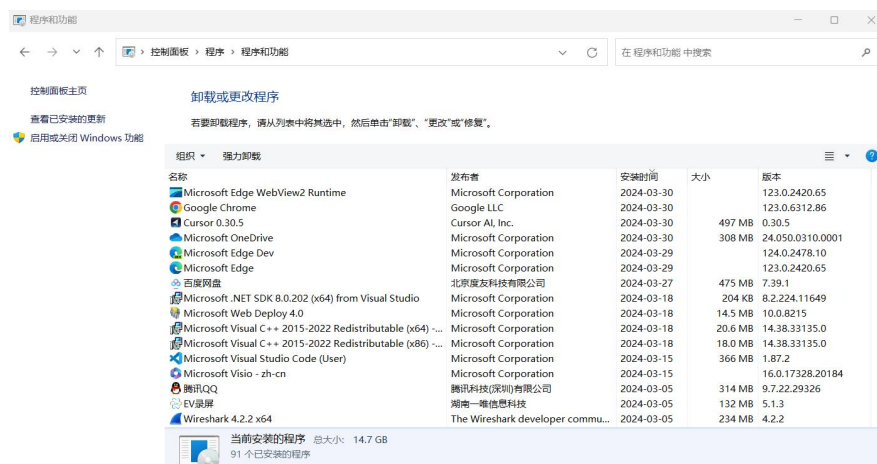
系统环境：Win10

使用软件：NMap

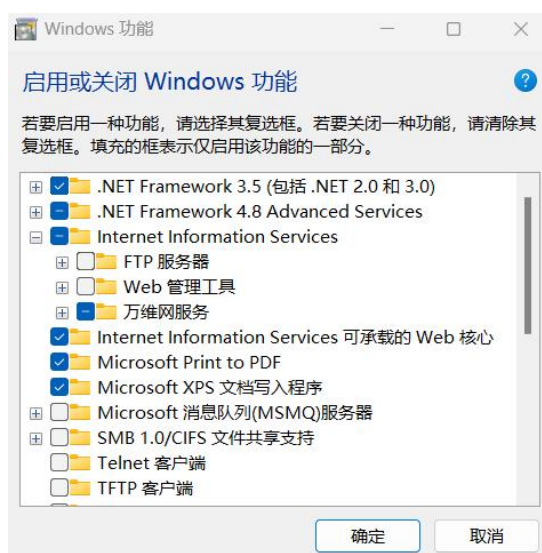
四、实验过程

(一) 配置计算机的相关功能

1. 控制面板->程序与功能

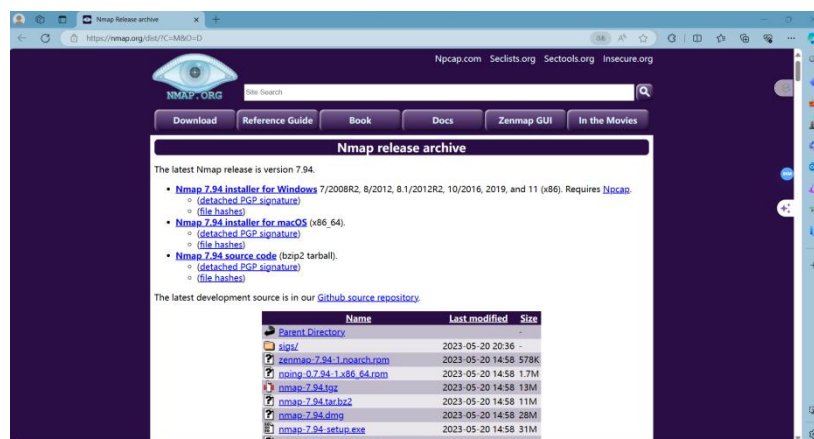


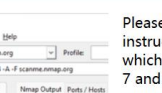
2. 选择启用或关闭 Windows 功能，勾选 Internet Information Services 的万维网服务



(二) Nmap 的获取安装

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





Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

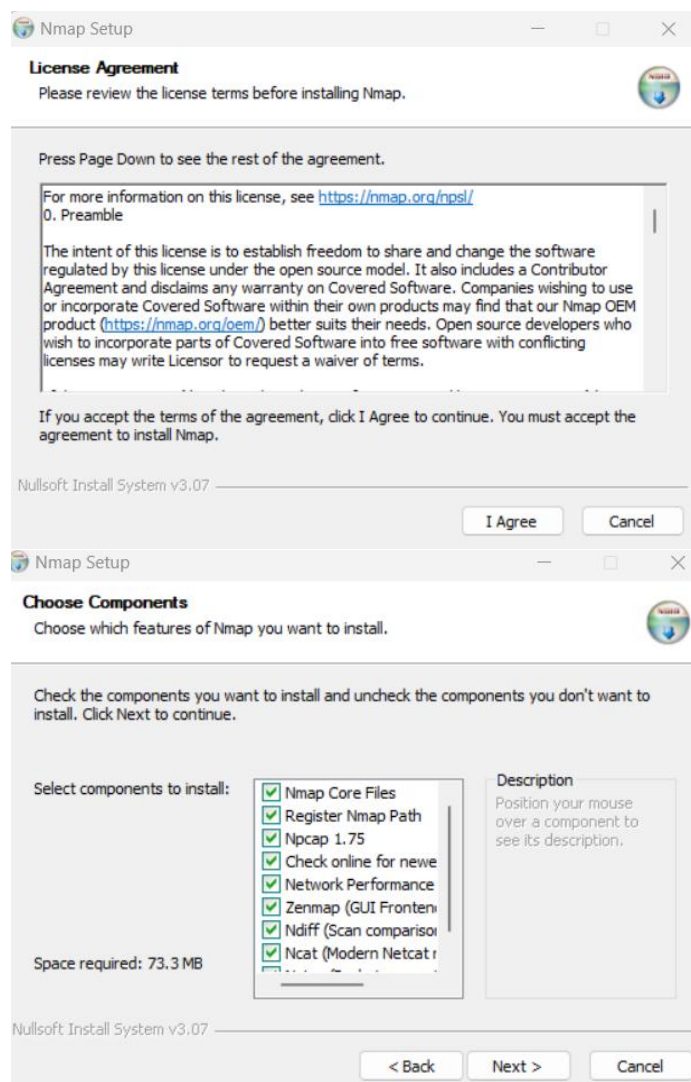
Latest Npcap release self-installer: [npcap-1.79.exe](#)

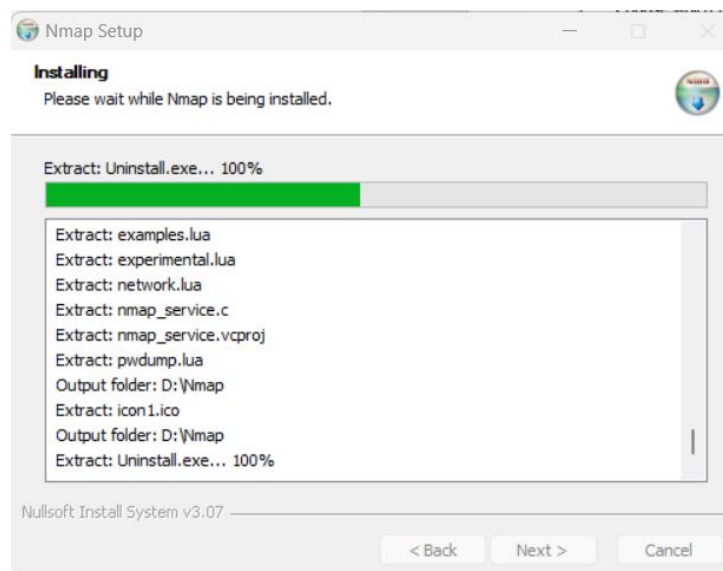
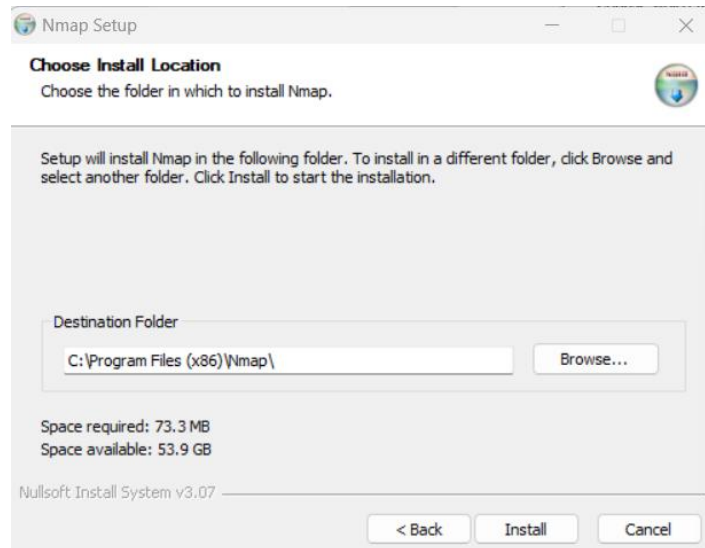
Latest [stable](#) release self-installer: [nmap-7.94-setup.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

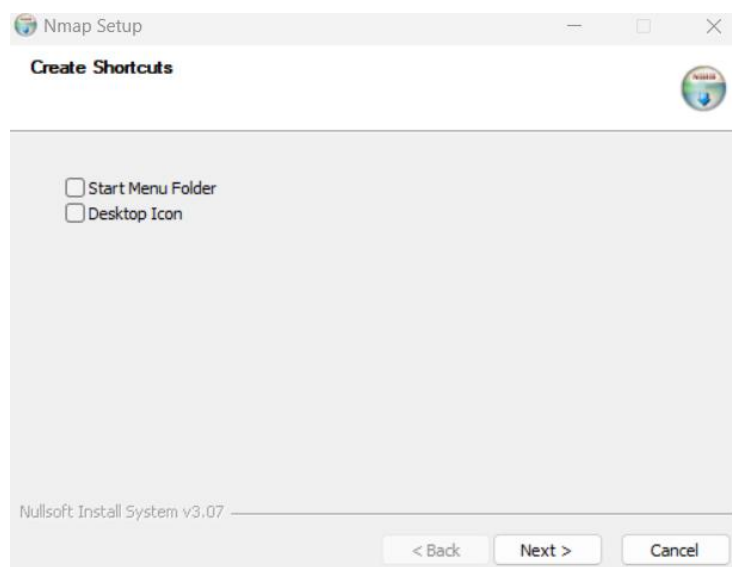
选择的是 7.94 的版本

2. 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。

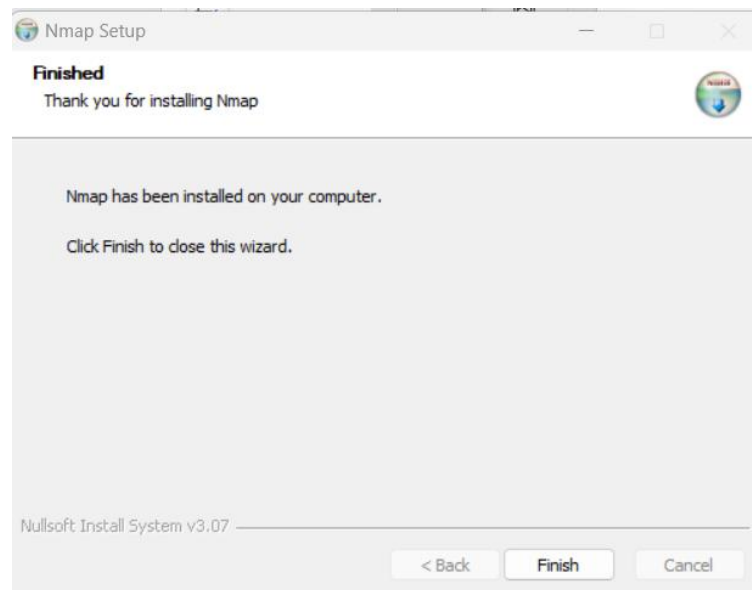




3. 根据自己的需要选择，然后点击 next

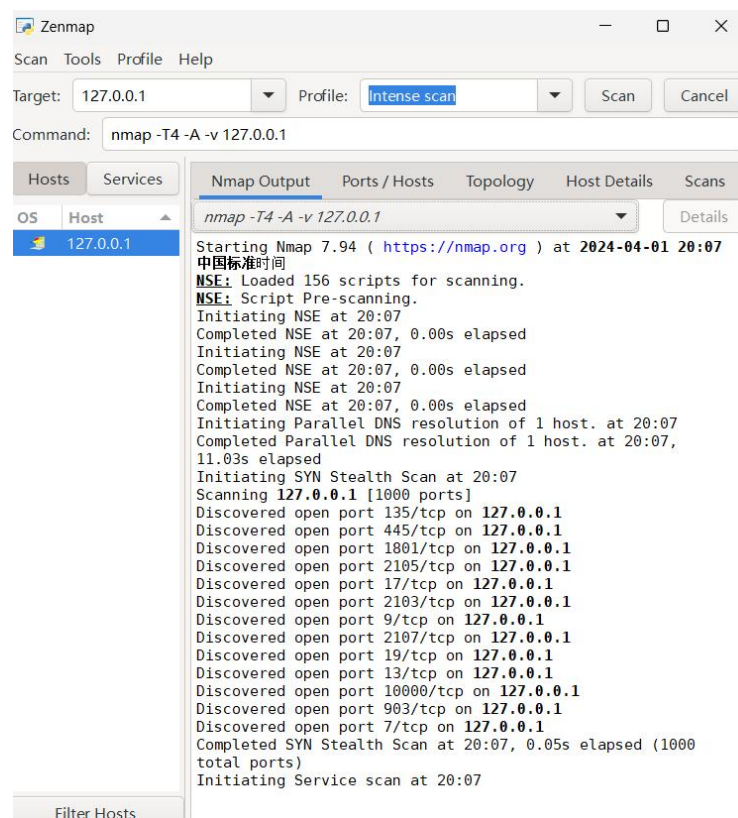


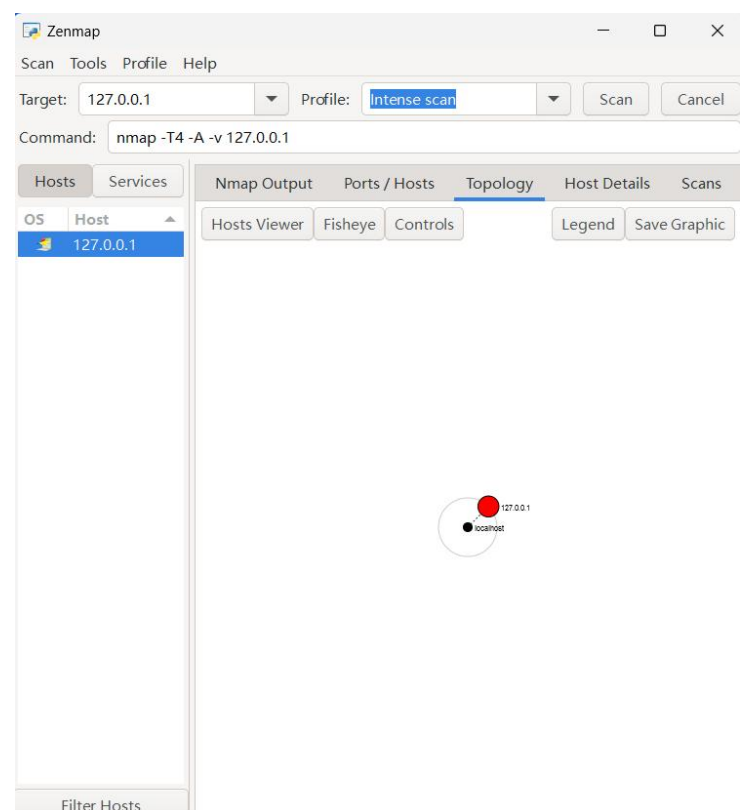
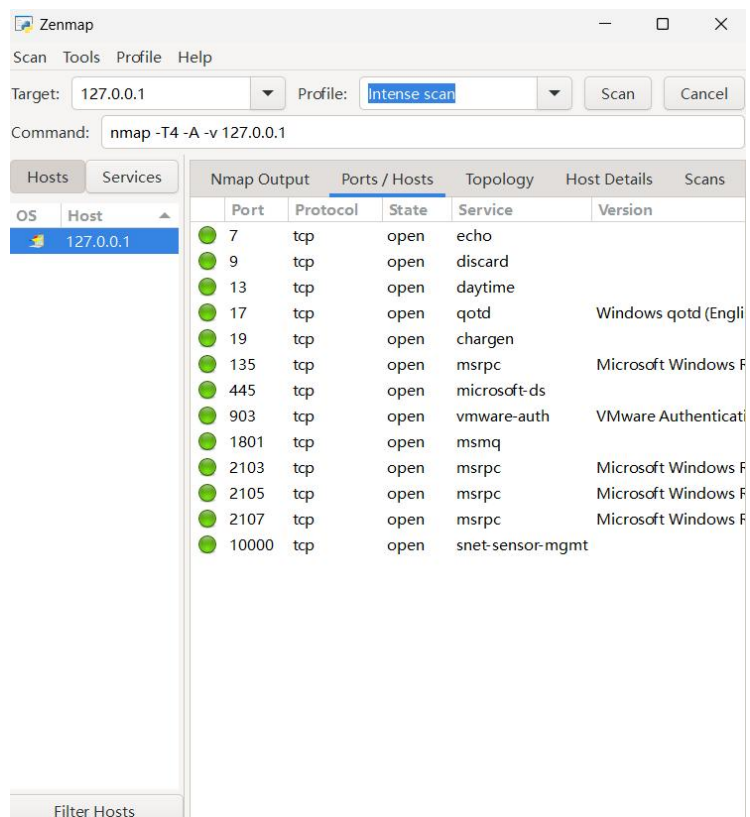
4. 点击 finish 完成安装



(三) 使用 Nmap 进行扫描

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，可以看到 tcp 的 80 端口和 443 端口打开了。

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS Host

www.baidu.com

127.0.0.1

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

Starting Nmap 7.94 (<https://nmap.org>) at 2024-04-01 20:11 中国标准时间

NSE: Loaded 156 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 20:11

Completed NSE at 20:11, 0.00s elapsed

Initiating NSE at 20:11

Completed NSE at 20:11, 0.00s elapsed

Initiating NSE at 20:11

Completed NSE at 20:11, 0.00s elapsed

Initiating Ping Scan at 20:11

Scanning www.baidu.com (39.156.66.14) [4 ports]

Completed Ping Scan at 20:11, 4.23s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 20:11

Completed Parallel DNS resolution of 1 host. at 20:12, 11.03s elapsed

Initiating SYN Stealth Scan at 20:12

Scanning www.baidu.com (39.156.66.14) [1000 ports]

Discovered open port 80/tcp on 39.156.66.14

Discovered open port 443/tcp on 39.156.66.14

Completed SYN Stealth Scan at 20:12, 5.13s elapsed (1000 total ports)

Initiating Service scan at 20:12

Scanning 2 services on www.baidu.com (39.156.66.14)

Completed Service scan at 20:12, 12.35s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against www.baidu.com (39.156.66.14)

Retrying OS detection (try #2) against www.baidu.com (39.156.66.14)

Initiating Traceroute at 20:12

Completed Traceroute at 20:12, 3.04s elapsed

Initiating Parallel DNS resolution of 6 hosts at 20:12

Zenmap

Scan Tools Profile Help

Target: Profile:

Command:

Hosts Services

OS Host

www.baidu.com

127.0.0.1

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
80	tcp	open	http	Apache httpd
443	tcp	open	http	Apache httpd

