NMAP实验

1. **实验目的**

掌握端口扫描这种信息探测技术的原理。

学会使用常见的端口扫描工具。

了解各种常用网络服务所对应的端口号。

1. **实验内容**

使用Nmap的命令行工具进行端口扫描。

使用Nmap的命令行工具进行网络服务及其版本探测。

使用Nmap的命令行工具进行操作系统类型鉴别。

使用Nmap 的图形化前端Zenmap工具同样进行上述任务。

1. **实验环境**

学生实验主机: Windows 2000/XP/Server 2003。

实验目标服务器: Windows Server A。

网络环境:局域网。

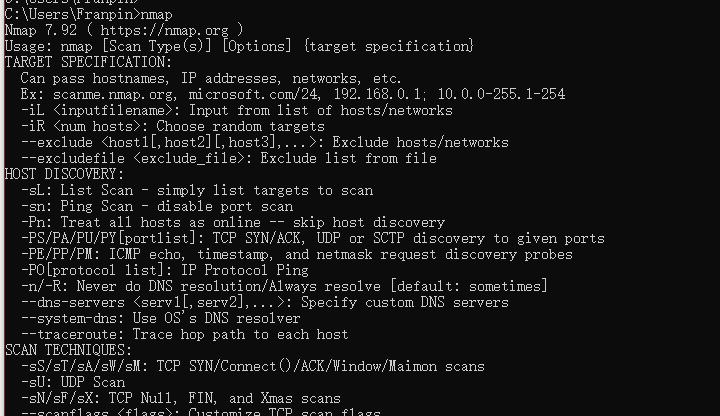
1. **实验原理**

Nmap(Network Mapper、网络映射器）是一款开放源代码的网络探测和安全审核的工具。它的设计目标是快速地扫描大型网络，当然用它扫描单个主机也没有问题。Nmap以新颖的方式使用原始IP报文来发现网络上有哪些主机，哪些主机提供什么服务，包括其应用程序名和版本，哪些服务运行在什么操作系统，包括版本信息，它们使用什么类型的报文过滤器/防火墙，以及一堆其它功能。虽然Nmap通常用于安全审核，许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

发现网络上有哪些主机，哪些主机提供什么服务，包括其应用程序名和版本，哪些服务运行在什么操作系统，包括版本信息，它们使用什么类型的报文过滤器/防火墙，以及一堆其它功能。虽然Nmap通常用于安全审核，许多系统管理员和网络管理员也用它来做一些日常的工作，比如查看整个网络的信息，管理服务升级计划，以及监视主机和服务的运行。

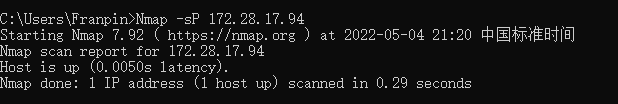
Nmap输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。“所感兴趣的端口表格"是其中的关键。状态可能是open(开放的)、filtered(被过滤的)、closed(关闭的)、或者unfiltered(未被过滤的)。“Open”意味着目标机器上的应用程序正在该端口监听连接/报文，“Filtered"意味着防火墙、过滤器或者其它网络障碍阻止了该端口被访问，“Closed”意味着没有应用程序在该端口上面监听，但是他们随时可能开放。当端口对Nmap 的探测做出响应，但是 Nmap无法确定它们是关闭还是开放时，这些端口就被认为是unfiltered。如果Nmap报告状态组合open|filtered和 closed filtered时，那说明Nmap无法确定该端口处于两个状态中的哪一个状态。当要求进行版本探测时，端口表也可以包含软件的版本信息。当要求进行IP协议扫描时(-sO)，Nmap提供关于所支持的IP协议而不是正在监听的端口的信息。

1. **实验过程**5.1 打开系统中的“"命令提示符”"，进入到Nmap安装路径（默认为“C:Program FilesNmap”)，运行nmap.exe，查看可用参数。



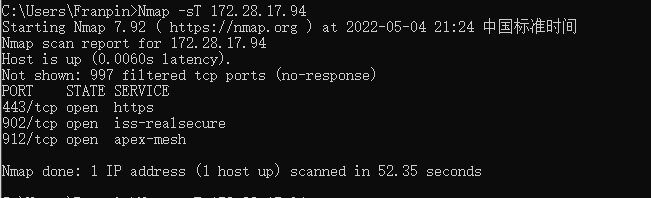
5.2 主机发现:进行连通性监测，来判断目标主机Windows ServerA(IP地址为172.18.1.207）是否可连通，运行如下命令:

Nmap -sP 172.18.17.94



5.3 使用常规扫描方式对目标主机进行TCP端口扫描，运行如下命令:

Nmap -sT 172.18.17.94



5.4使用SYN半扫描方式对目标主机进行TCP端口扫描，运行如下命令:

Nmap -sS 172.18.17.94



从上述结果中可以看出，使用SYN扫描花费的时间比使用TCP扫描花费的时间要短，因为在SYN扫描中。本地主机向目标主机发送一个SYN数据段，在TCP报文中SYN标志位用来建立连接，让连接的双方同步序列号.如果SYN=1而ACK=0，则表示该数据包为连接请求，如果SYN=1且ACK=1，则表示接受连接。如果目标主机的回应报文中SYN=1，ACK=1，则说明该端口是活动的，那么接着，我们再发一个RST给目标主机，拒绝建立连接。在这里，如果目标主机的回应为RST，则表示该端口为死端口，在这种情况下，我们不用再做任何回应。因此SYN扫描花费的时间比较短。

5.5对目标主机进行UDP端口扫描，运行如下命令:

Nmap -sU 172.18.17.94



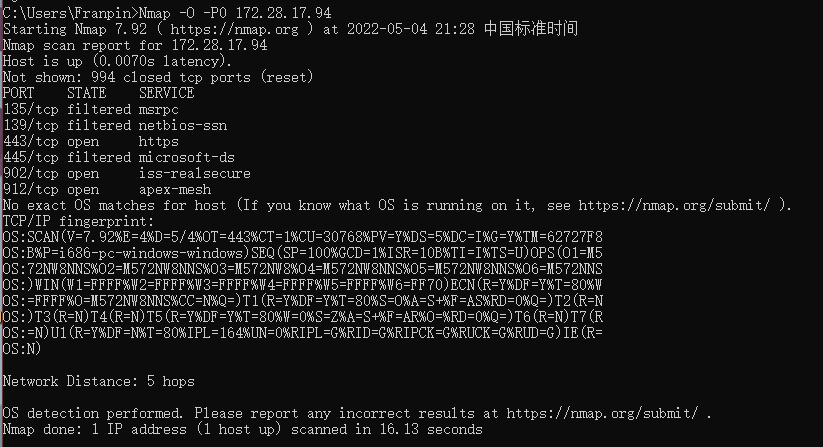
5.6 探测目标主机主机开放端口上所提供的服务及其类型和版本信息，运行如下命令:

Nmap -sV 172.18.17.94



5.7探测目标主机的操作系统类型，运行如下命令:

Nmap -O -P0 172.18.17.94



5.8 进入到Nmap安装路径（默认为“C:\Program FileslNmap”)，运行zenmap.exe，即 Nmap的图形化前端程序。在“Target”文本框中输入扫描目标IP地址/主机名称（172.28.17.94)），然后在“Profile”预定义配置下拉框中选择扫描配置“Intense Scan， no Ping”，然后点击菜单项“Profile”→"Edit Selected Profile”，切换到“Scan”选项卡，勾选上“Operating system”

