NMAP实验指导书

[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。

[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。

[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。

[实验原理]

端口及服务的基本概念

“端口”是专门为计算机通信而设计的，在 TCP/IP 协议中规定，用 IP 地址和端口作为套接字（socket），代表 TCP 或 UDP 通信的一端。端口分为知名（known）端口号和一般端口号，其中知名端口号的数值一般为 0~1023，分配给常用应用服务程序固定使用。

下面是常用的 TCP 知名端口号列表。

服务名臣	端口号	说明
FTP	21	文件传输服务
SSH	22	加密远程登录服务
Telnet	23	远程登录服务
SMTP	25	简单邮件传输服务
HTTP	80	WWW（Web）服务
POP3	110	邮件接受服务

Nmap 的功能介绍和技术原理

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。

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。

除了所感兴趣的端口表，Nmap 还能提供关于目标机的进一步信息，包括反向域名，操作系统猜测，设备类型，和 MAC 地址。

Nmap 的基本命令格式如下所示：

nmap [***扫描类型*** ...] [***选项***] { ***扫描目标说明*** }

```
Usage: nmap [Scan Type(s)] [Options] <target specification>
```

- 主机发现

任何网络探测任务的最初几个步骤之一就是把一组 IP 范围缩小为一列活动的或者您感兴趣的主机。扫描每个 IP 的每个端口很慢，通常也没必要。当然，什么样的主机令您感兴趣主要依赖于扫描的目的。由于主机发现的需求五花八门，Nmap 提供了很多的选项来定制您的需求。运行 Nmap 命令就可以发现主机发现的一些基本参数，如下图：

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -P0: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
```

参数	释义
-sL	列表扫描，仅仅列出指定网络上的每台主机，不发送任何报文到目标主机。
-sP	Ping 扫描，可以很方便地得出网络上有多少机器正在运行或者监视服务器是否正常运行。
-P0	无 Ping 扫描，对每一个指定的目标 IP 地址进行所要求的扫描，不管主机是否正在运行，跳过主机发现。
-PS/PA/PU	PS-TCP SYN Ping，PA-TCP ACK Ping，PU-UDP Ping
-n/-R	从不对永远对发现的活动 IP 地址进行反向域名解析
--dns-servers	指定系统域名解析器
--system-dns	使用操作系统域名解释器

- 端口扫描

Nmap 把端口分成六个状态: open(开放的)，closed(关闭的)，filtered(被过滤的)，unfiltered(未被过滤的)，open|filtered(开放或者被过滤的)，或者 closed|filtered(关闭或者未被过滤的)。

Nmap 支持大约十几种扫描技术。一般一次只用一种方法，除了 UDP 扫描(-sU)可能和任何一种 TCP 扫描类型结合使用。

```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idlescan
  -sO: IP protocol scan
  -b <ftp relay host>: FTP bounce scan
```

参数	释义
-sS/-sT/sA/sW/sM	TCP SYN 扫描/ TCP connect()扫描/ TCP ACK 扫描/ TCP 窗口扫描/ TCP Maimon 扫描
-sU	UDP 扫描。DNS，SNMP，和 DHCP (注册的端口是 53，161/162，和 67/68)是最常见的三个。
-sN/-sF/-sX	TCP Null/FIN/and Xmas 扫描。它们能躲过一些无状态防火墙和报文过滤路由器，甚至比 SYN 扫描还要隐秘一些。
-scanflags	定制的 TCP 扫描。可以通过指定任意 TCP 标志位来设计自己的扫描。
-sI	Idlescan。这种高级的扫描方法允许对目标进行真正的 TCP 端口盲扫描。
-sO	IP 协议扫描。可以确定目标机支持哪些 IP 协议 (TCP，ICMP，IGMP 等)。
-b	FTP 弹跳扫描。

除了所有前面讨论的扫描方法，Nmap 提供选项说明那些端口被扫描以及扫描是随机还是顺序进行。默认情况下，Nmap 用指定的协议对端口 1 到 1024 以及 nmap-services 文件中列出的更高的端口在扫描。

```
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast - Scan only the ports listed in the nmap-services file)
  -r: Scan ports consecutively - don't randonize
```

参数	释义
-p	只扫描指定的端口
-F	快速 (有限的端口) 扫描
-r	不要按随机顺序扫描端口

- 服务和版本探测

把 Nmap 指向一个远程机器，它可能告诉您端口 25/tcp，80/tcp，和 53/udp 是开放的。使用包含大约 2,200 个著名的服务的 nmap-services 数据库，Nmap 可以报告那些端口可能分别对应于一个邮件服务器 (SMTP)，web 服务器(HTTP)，和域名服务器(DNS)。

在用某种其它类型的扫描方法发现 TCP 和/或者 UDP 端口后，版本探测会询问这些端口，确定到底什么服务正在运行。nmap-service-probes 数据库包含查询不同服务的探测报文和解析识别响应的匹配表达式。Nmap 试图确定服务协议(如 ftp，ssh，telnet，http)，应用程序名(如 ISC Bind，Apache httpd，Solaris telnetd)，版本号，主机名，设备类型(如打印机，路由器)，操作系统家族 (如 Windows，Linux)以及其它的细节，如是否可以连 X server，SSH 协议版本，或者 KaZaA 用户名)。当然，并非所有服务都提供所有这些信息。如果 Nmap 被编译成支持 OpenSSL，它将连接到 SSL 服务器，推测什么服务在加密层后面监听。当发现 RPC 服务时，Nmap RPC grinder (-sR)会自动被用于确定 RPC 程序和它的版本号。
Nmap 用下列的选项打开和控制版本探测。

```
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

参数	释义
-sV	打开版本探测。也可以同时打开操作系统探测和版本探测。
--version-intensity<intensity>	快速（有限的端口）扫描。每个报文都被赋予一个 1 到 9 之间的值。被赋予较低值的探测报文对大范围的常见服务有效，而被赋予较高值的报文一般没什么用。数值越高，服务越有可能被正确识别。然而，高强度扫描花更多时间。强度值必须在 0 和 9 之间。默认是 7。
--version-light	打开轻量级模式。即--version-intensity 2。
--version-all	尝试每个探测。即--version-intensity 9。
--version-trace	跟踪版本扫描活动。

- 操作系统类型鉴别

Nmap 最著名的功能之一是用 TCP/IP 协议栈指纹技术（Fingerprinting）进行远程操作系统探测。每个 Fingerprint 包括一个自由格式的关于 OS 的描述文本，和一个分类信息，它提供供应商名称(如 Sun)，下面的操作系统（如 Solaris），OS 版本（如 10），和设备类型（通用设备，路由器，switch，游戏控制台，等）。

操作系统检测可以进行其它一些测试，这些测试可以利用处理过程中收集到的信息。例如运行时间检测，使用 TCP 时间戳选项(RFC 1323)来估计主机上次重启的时间，这仅适用于提供这类信息的主机。另一种是 TCP 序列号预测分类，用于测试针对远程主机建立一个伪造的 TCP 连接的可能难度。
采用下列选项启用和控制操作系统检测:

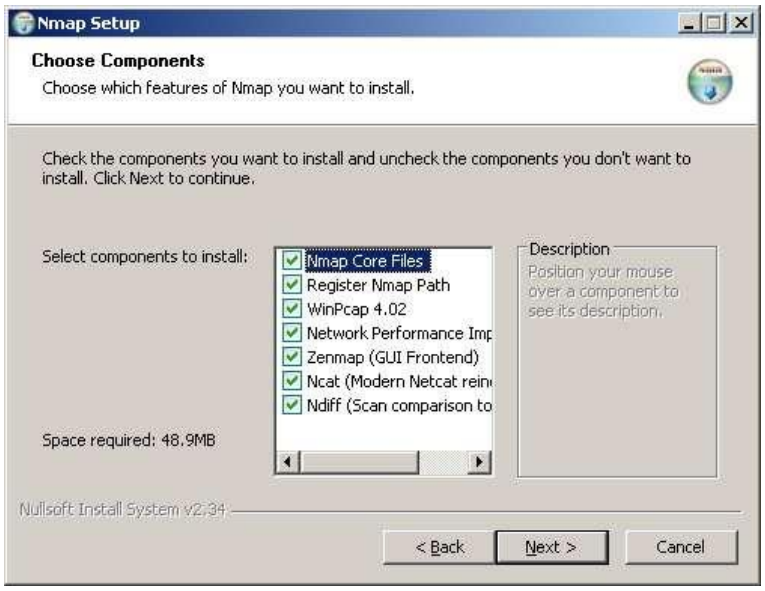
```
OS DETECTION:
  -O: Enable OS detection (try 2nd generation w/fallback to 1st)
  -O2: Only use the new OS detection system (no fallback)
  -O1: Only use the old (1st generation) OS detection system
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
```

参数	释义
-O	启用操作系统检测。也可以同时打开操作系统探测和版本探测。
-O2	仅使用新的操作系统检测。
-O1	仅使用第一代操作系统检测。
--osscan-limit	如果发现一个打开和关闭的 TCP 端口时，操作系统检测会更有效。采用这个选项，Nmap 只对满足这个条件的主机进行操作系统检测。
--osscan-guess	推测操作系统检测结果。

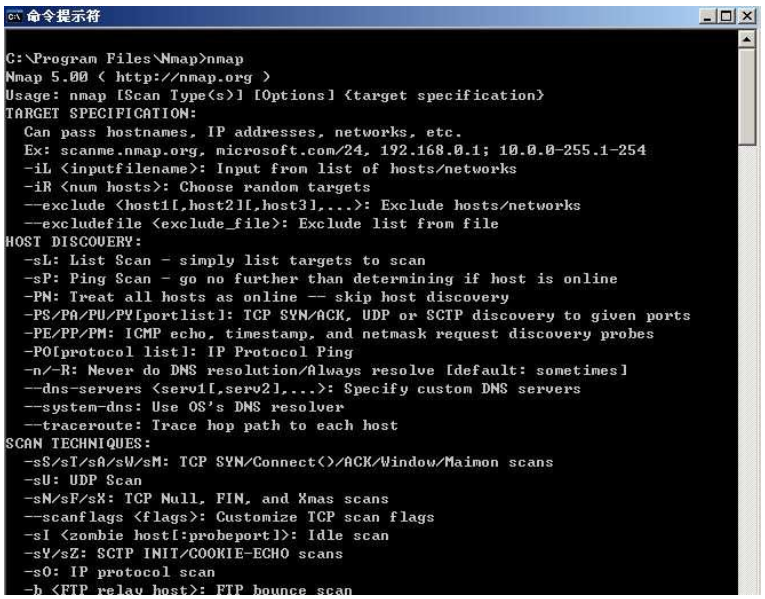
[实验过程]

1. 运行实验工具目录下的 Nmap 安装程序（nmap-5.00-setup.exe），安装 Nmap 到系统中的默认路径（C:\Program Files\Nmap）。

   注意：安装过程中保留默认包含的 Winpcap 和 Zenmap 组件，如下图所示。

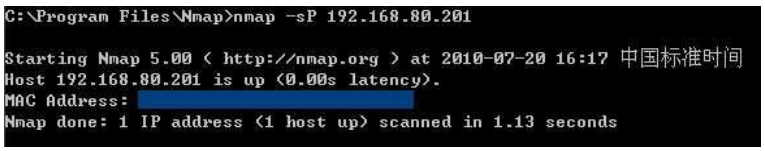


2. 打开系统中的“命令提示符”，进入到 Nmap 安装路径（默认为“C:\Program Files\Nmap”），运行 nmap.exe，查看可用参数。



3. 主机发现：进行连通性监测，来判断目标主机 Windows Server A（IP 地址为 192.168.80.201）是否可连通，运行如下命令：

Nmap –sP 192.168.80.201



请将扫描检测结果写入实验报告，包括目标主机是否存活，如果存活的话，请记录该主机的 MAC 地址及其网卡的厂商品牌等信息。

4. 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 192.168.80.201

```
C:\Program Files\Nmap>nmap -sT 192.168.80.201

Starting Nmap 5.00 ( http://nmap.org ) at 2010-07-20 16:28 中国标准时间
Interesting ports on 192.168.80.201:
Not shown: 986 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
25/tcp   open   smtp
80/tcp   open   http
```

   请将扫描检测结果写入实验报告，包括所有的端口及开放情况。

5. 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 192.168.80.201

   请将扫描检测结果写入实验报告，包括所有的端口及开放情况。

   比较上述两次扫描所花费的时间。请在实验报告中对此进行描述，并尝试对此进行解释。

6. 对目标主机进行 UDP 端口扫描，运行如下命令：

   Nmap –sU 192.168.80.201

   请将扫描检测结果写入实验报告，包括所有的端口及开放情况。

7. 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 192.168.80.201

```
C:\Program Files\Nmap>nmap -sV 192.168.80.201

Starting Nmap 5.00 ( http://nmap.org ) at 2010-07-20 16:35 中国标准时间
Interesting ports on 192.168.80.201:
Not shown: 987 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         Microsoft ESMTP 6.0.3790.3959
80/tcp   open  http         Microsoft IIS httpd 6.0
```

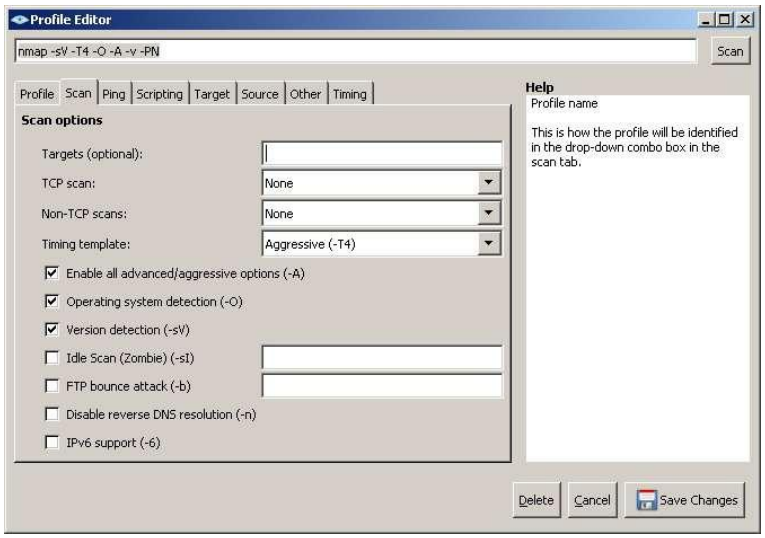
   请将扫描检测结果写入实验报告，包括所有的端口及其服务版本信息。

8. 探测目标主机的操作系统类型，运行如下命令：

   Nmap –O –P0 192.168.80.201

   请将扫描检测结果写入实验报告，包括探测出来的目标主机操作系统类型信息。

9. 进入到 Nmap 安装路径（默认为“C:\Program Files\Nmap”），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（192.168.80.201），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 detection”和“Version detection”后点击“Save Changes”按钮保存扫描配置，最后点击“Scan”按钮开始扫描。



请将扫描检测结果写入实验报告，包括目标主机的开放端口、服务版本、操作系统类型信息等。