NMAP 实验

一、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。

二、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。

三、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。

四、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。

五、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。

```
C:\Users\Franpin>nmap
Nmap 7.92 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -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
  --traceroute: Trace hop path to each host
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
```

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

```
C:\Users\Franpin>Nmap -sP 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:20 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.0050s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```

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

```
C:\Users\Franpin>Nmap -sT 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:24 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.0060s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
443/tcp open  https
902/tcp open  iss-realsecure
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 52.35 seconds
```

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

```
C:\Users\Franpin>Nmap -sS 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:20 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.0086s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
902/tcp open     iss-realsecure
912/tcp open     apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

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

```
C:\Users\Franpin>Nmap -sU 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:21 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.0070s latency).
Not shown: 986 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open|filtered ntp
135/udp  open|filtered msrpc
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
139/udp  open|filtered netbios-ssn
162/udp  open|filtered snmptrap
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
520/udp  open|filtered route
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 9.56 seconds
```

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

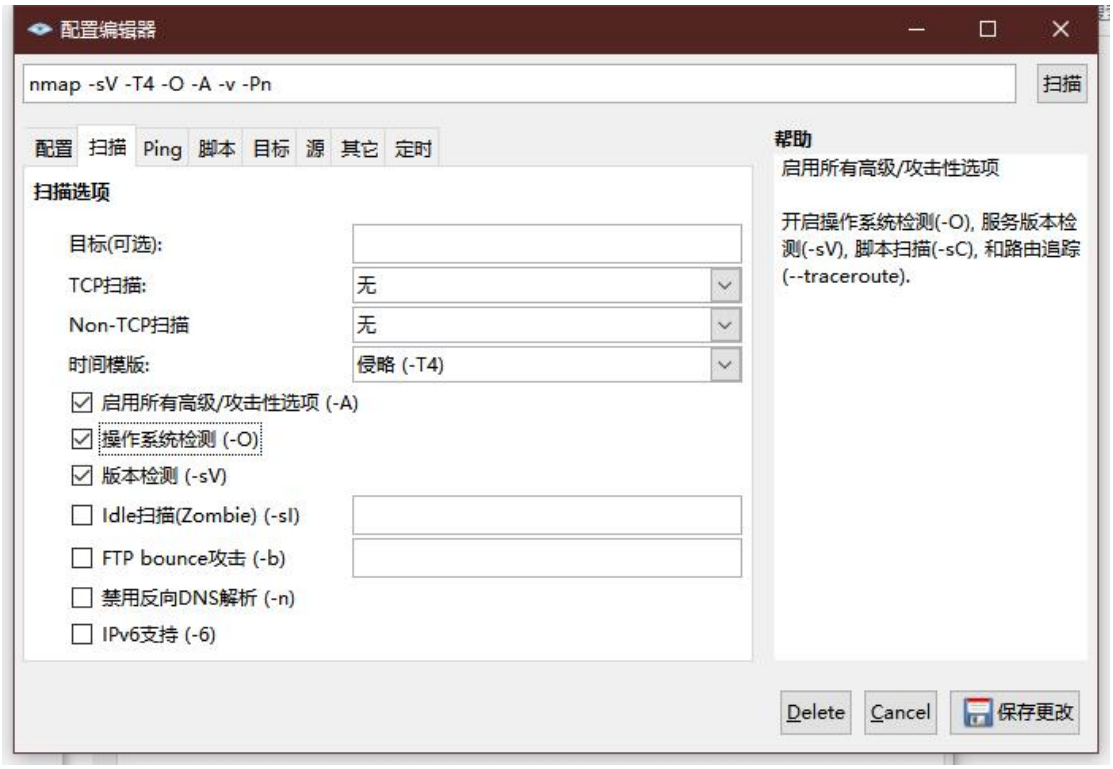
```
C:\Users\Franpin>Nmap -sV 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:30 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.011s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE    SERVICE         VERSION
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     ssl/https       VMware Workstation SOAP API 14.1.1
445/tcp filtered microsoft-ds
902/tcp open     ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open     vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Service Info: CPE: cpe:/o:vmware:Workstation:14.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 146.34 seconds
```

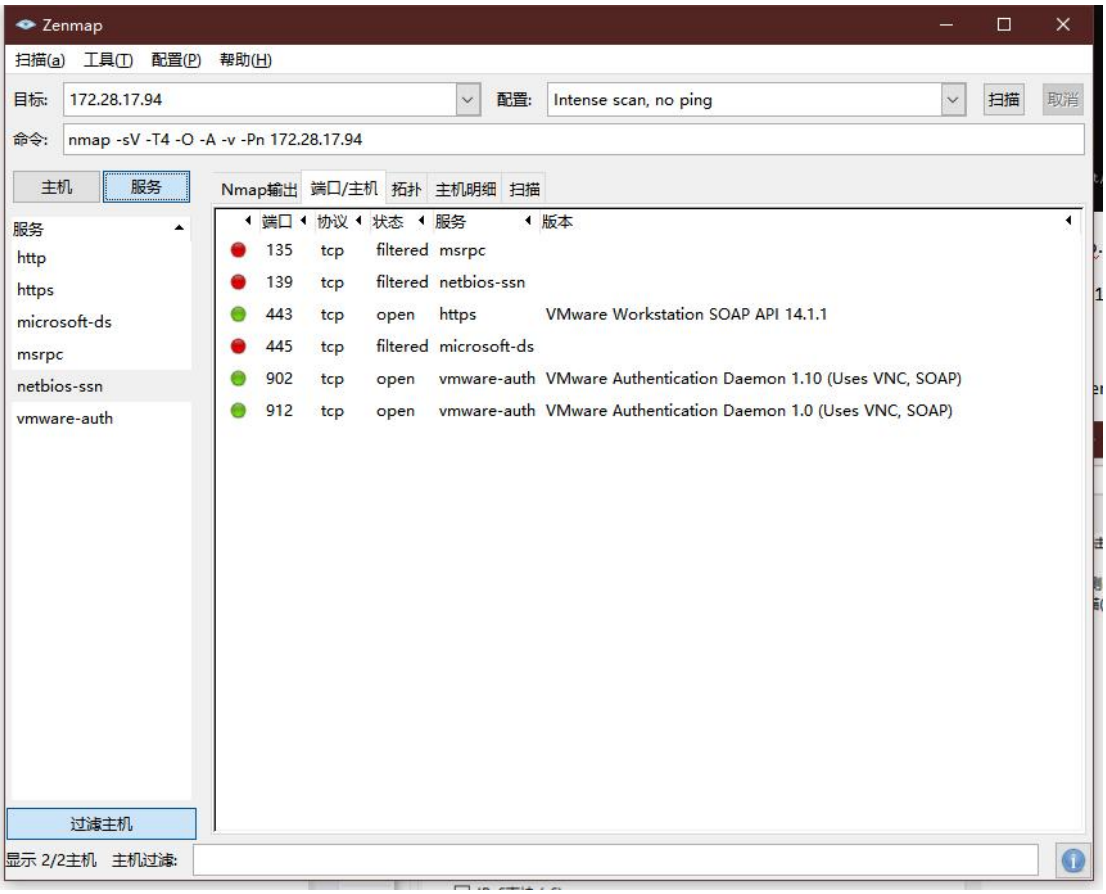
5.7 探测目标主机的操作系统类型，运行如下命令:

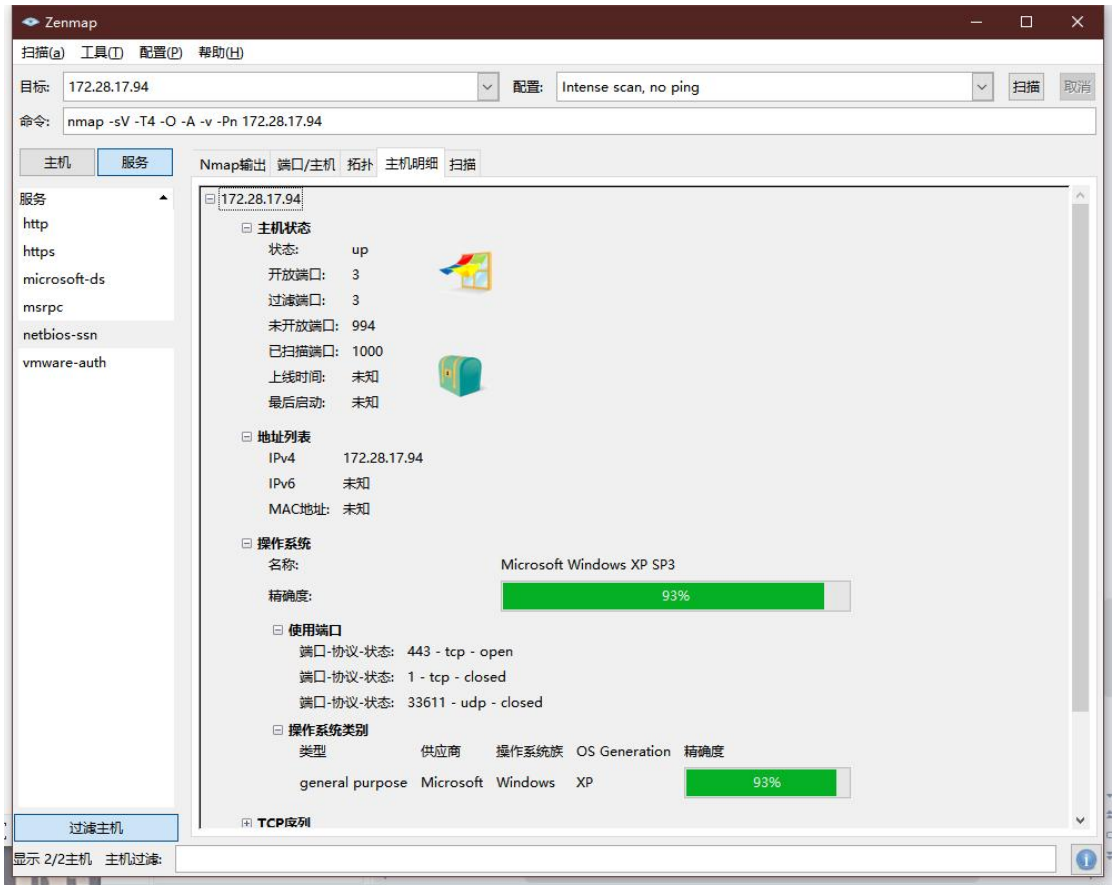
Nmap -O -P0 172.18.17.94

```
C:\Users\Franpin>Nmap -O -P0 172.28.17.94
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-04 21:28 中国标准时间
Nmap scan report for 172.28.17.94
Host is up (0.0070s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE    SERVICE
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
902/tcp open     iss-realsecure
912/tcp open     apex-mesh
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=5/4%OT=443%CT=1%CU=30768%PV=Y%DS=5%DC=I%G=Y%TM=62727F8
OS:B%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=10B%TI=I%TS=U)OPS(O1=M5
OS:72NW8NNS%O2=M572NW8NNS%O3=M572NW8%O4=M572NW8NNS%O5=M572NW8NNS%O6=M572NNS
OS:)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W
OS:=FFFF%O=M572NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R
OS:=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:N)

Network Distance: 5 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.13 seconds
```

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”




Zenmap
扫描(a) 工具(T) 配置(P) 帮助(H)
目标: 172.28.17.94
配置: Intense scan, no ping
扫描
取消
命令: nmap -sV -T4 -O -A -v -Pn 172.28.17.94
主机
服务
Nmap输出 端口/主机 拓扑 主机明细 扫描
服务
http
https
microsoft-ds
msrpc
netbios-ssn
vmware-auth
端口 协议 状态 服务 版本
135 tcp filtered msrpc
139 tcp filtered netbios-ssn
443 tcp open https VMware Workstation SOAP API 14.1.1
445 tcp filtered microsoft-ds
902 tcp open vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912 tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
过滤主机
显示 2/2主机 主机过滤:


Zenmap
扫描(a) 工具(T) 配置(P) 帮助(H)
目标: 172.28.17.94
配置: Intense scan, no ping
扫描
取消
命令: nmap -sV -T4 -O -A -v -Pn 172.28.17.94
主机
服务
Nmap输出 端口/主机 拓扑 主机明细 扫描
服务
http
https
microsoft-ds
msrpc
netbios-ssn
vmware-auth
172.28.17.94
主机状态
状态: up
开放端口: 3
过滤端口: 3
未开放端口: 994
已扫描端口: 1000
上线时间: 未知
最后启动: 未知
地址列表
IPv4 172.28.17.94
IPv6 未知
MAC地址: 未知
操作系统
名称: Microsoft Windows XP SP3
精确度: 93%
使用端口
端口-协议-状态: 443 - tcp - open
端口-协议-状态: 1 - tcp - closed
端口-协议-状态: 33611 - udp - closed
操作系统类别
类型 供应商 操作系统族 OS Generation 精确度
general purpose Microsoft Windows XP 93%
TCP序列
过滤主机
显示 2/2主机 主机过滤: