

一、实验目的

- 掌握网络端口扫描器的使用方法，熟悉常见端口和其对应的服务程序，掌握发现系统漏洞的方法。
- 掌握综合扫描及安全评估工具的使用方法，了解进行简单系统漏洞入侵的方法，了解常见的网络和系统漏洞以及其安全防护方法。

二、实验原理

- 端口扫描原理
 - 端口扫描向目标主机的 **TCP/IP** 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。
 - 端口扫描主要有经典的扫描器（全连接）、**SYN**（半连接）扫描器、秘密扫描等。
 - 全连接扫描：扫描主机通过 **TCP/IP** 协议的三次握手与目标主机的指定端口建立一次完整的连接。建立连接成功则响应扫描主机的 **SYN/ACK** 连接请求，这一响应表明目标端口处于监听（打开）的状态。如果目标端口处于关闭状态，则目标主机会向扫描主机发送 **RST** 的响应。
 - 半连接（**SYN**）扫描：若端口扫描没有完成一个完整的 **TCP** 连接，在扫描主机和目标主机的一指定端口建立连接时候只完成了前两次握手，在第三步时，扫描主机中断了本次连接，使连接没有完全建立起来，这样的端口扫描称为半连接扫描，也称为间接扫描。
 - **TCP FIN**（秘密）扫描：扫描方法的思想是关闭的端口会用适当的 **RST** 来回复 **FIN** 数据包。另一方面，打开的端口会忽略对 **FIN** 数据包的回复。
- 综合扫描和安全评估技术工作原理
 - 获得主机系统在网络服务、版本信息、**Web** 应用等相关信息，然后采用模拟攻击的方法，对目标主机系统进行攻击性的安全漏洞扫描，如果模拟攻击成功，则视为漏洞存在。最后根据检测结果向系统管理员提供周密可靠的安全性分析报告。

- 常见的TCP端口如下：

服务名称	端口号	说明
FTP	21	文件传输服务
TELNET	23	远程登录服务
HTTP	80	网页浏览服务
POP3	110	邮件服务
SMTP	25	简单邮件传输服务
SOCKS	1080	代理服务

- 常见的UDP端口如下：

服务名称	端口号	说明
RPC	111	远程调用
SNMP	161	简单网络管理
TFTP	69	简单文件传输
DNS	53	域名解析服务

三、实验环境

- 实验室所有机器安装了 Windows 操作系统，并组成了一个局域网，并且都安装了 SuperScan 端口扫描工具和流光 Fluxay5 综合扫描工具。
- 每两个学生为一组：互相进行端口扫描和综合扫描实验。

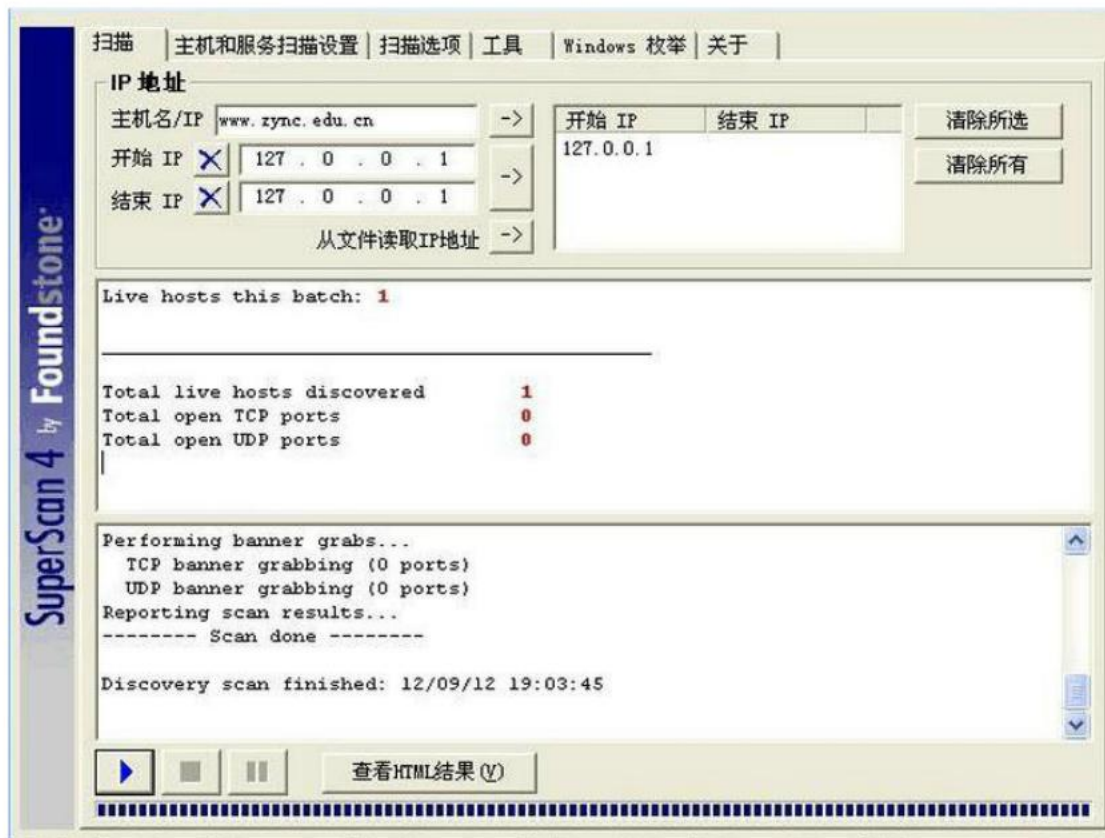
四、实验内容和步骤

任务一：使用 **Superscan** 端口扫描工具并分析结果

实验步骤：

- (1) 添加扫描远程主机，并执行端口扫描

在程序“扫描”标签页下面下的“IP 地址”栏中输入远程主机的主机名/IP 地址。然后点击开始按钮，程序在默认设置下开始对远程主机进行扫描。扫描结束后，出现如图所示的扫描结果。



从图中可以看出，对主机扫描和端口扫描结果都为 0，这是由于主机禁止了扫描器的 ICMP 扫描响应。因此需要修改对主机的扫描方式。

（2）修改主机和服务扫描设置

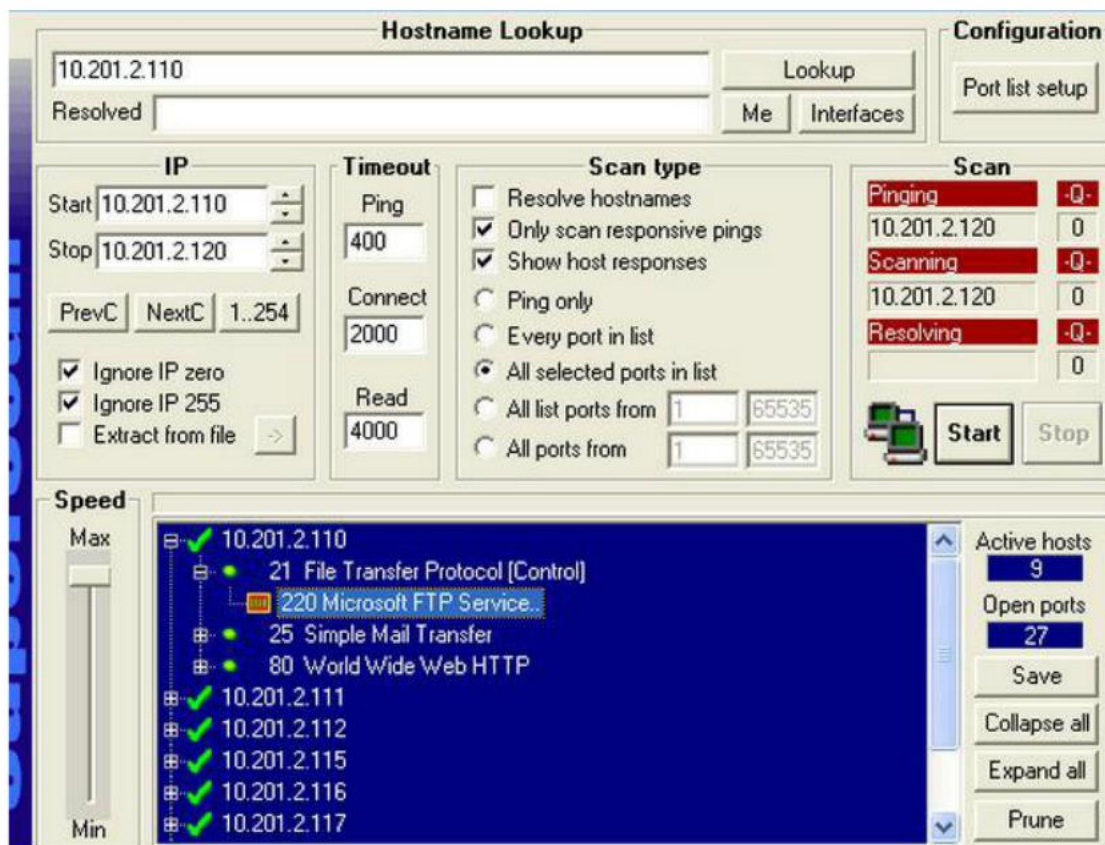
点击“主机和服务扫描设置”标签页，并在该标签页中去掉“查找主机”复选框。选中 UDP 端口扫描复选框，并将 UDP 扫描类型设置为“Data”。选中 TCP 端口扫描复选框，并将 TCP 扫描类型设置为“直接连接”，如图所示。



(3) 执行端口扫描

点击“扫描”回到扫描标签页，然后点击开始按钮重新扫描远程主机。

扫描结果如图所示。



关闭某些端口后





任务二：使用综合扫描工具 **Fluxay5** 并分析结果

(1) 打开“文件”菜单下的“高级扫描向导”选项，如图 14。填入要扫描主机的起始地址和结束地址，在此我们只扫描靶机服务器一台主机故填入的主机 IP 地址一样。如果想要同时扫描靶机服务器和该服务器上的虚拟机则可以在“起始地址”中填入靶机服务器 IP “192. 168. 20. 245”；在“结束地址”中填入靶机服务器上的虚拟机 IP 地址 “192. 168. 20. 247”。

“Ping 检查”一般要选上，这样会先 Ping 目标扫描主机，若成功再进行扫描，这样可节省扫描时间。在检测项目选项中选上 PORTS, FTP, TELNET, IPC, IIS, PLUGINS, 我们只对这些漏洞进行扫描。



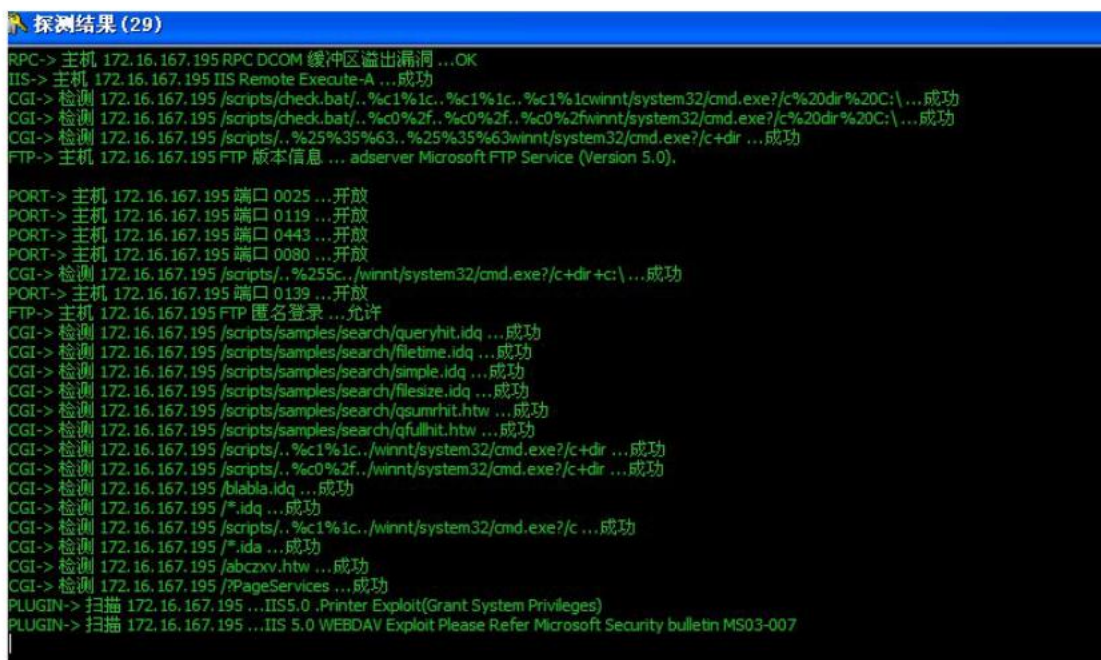
(2) 接着我们进入扫描对话框，如图 15。在“标准端口扫描”选项中，流光会扫描约几十个标准服务端口，而自定义扫描端口的范围可以在 1—65535 内任选。我们选择“标准端口扫描”。

(3) 接下来要配置的对话框是尝试获取 POP3 的版本信息，用户密码，以及获取 FTP 的 Banner，尝试匿名登录，尝试简单字典对 FTP 帐号进行暴力破解的对话框，我们选中这 3 项，再单击“下一步”。弹出询问获取 SMTP, IMAP 和操作系统版本信息以及用户信息的提示，并询问扫描 SunOS/bin/login 远程溢出弱点的对话框。

(4) 我们经过默认对 MSSQL2000 数据库漏洞，SA 密码和版本信息进行扫描的对话框后，将对主机系统的 IPC 漏洞进行扫描，查看是否有空连接，共享资源，获得用户列表并猜解用户密码。

(5) 这个对话框将设置 IIS 的漏洞扫描选项，包括扫描 Unicode 编码漏洞，是否安装了 FrontPage 扩展，尝试得到 SAM 文件，尝试得到 PCAnywhere 的密码等。

(6) 在扫描引擎对话框中选择默认的本地主机作为扫描引擎。



```
探测结果 (29)
RPC-> 主机 172.16.167.195 RPC DCOM 缓冲区溢出漏洞 ...OK
IIS-> 主机 172.16.167.195 IIS Remote Execute-A ...成功
CGI-> 检测 172.16.167.195 /scripts/check.bat/..%c1%1c..%c1%1c..%c1%1cwinnt/system32/cmd.exe?/c%20dir%20C:\...成功
CGI-> 检测 172.16.167.195 /scripts/check.bat/..%c0%2f..%c0%2f..%c0%2fwinnt/system32/cmd.exe?/c%20dir%20C:\...成功
CGI-> 检测 172.16.167.195 /scripts/..%25%35%63..%25%35%63winnt/system32/cmd.exe?/c+dir ...成功
FTP-> 主机 172.16.167.195 FTP 版本信息 ... adserver Microsoft FTP Service (Version 5.0).

PORT-> 主机 172.16.167.195 端口 0025 ...开放
PORT-> 主机 172.16.167.195 端口 0119 ...开放
PORT-> 主机 172.16.167.195 端口 0443 ...开放
PORT-> 主机 172.16.167.195 端口 0080 ...开放
CGI-> 检测 172.16.167.195 /scripts/..%255c../winnt/system32/cmd.exe?/c+dir +c:\...成功
PORT-> 主机 172.16.167.195 端口 0139 ...开放
FTP-> 主机 172.16.167.195 FTP 匿名登录 ...允许
CGI-> 检测 172.16.167.195 /scripts/samples/search/queryhit.idq ...成功
CGI-> 检测 172.16.167.195 /scripts/samples/search/filetime.idq ...成功
CGI-> 检测 172.16.167.195 /scripts/samples/search/simple.idq ...成功
CGI-> 检测 172.16.167.195 /scripts/samples/search/filesize.idq ...成功
CGI-> 检测 172.16.167.195 /scripts/samples/search/qsumhit.htw ...成功
CGI-> 检测 172.16.167.195 /scripts/samples/search/qfullhit.htw ...成功
CGI-> 检测 172.16.167.195 /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir ...成功
CGI-> 检测 172.16.167.195 /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir ...成功
CGI-> 检测 172.16.167.195 /blabla.idq ...成功
CGI-> 检测 172.16.167.195 /*.idq ...成功
CGI-> 检测 172.16.167.195 /scripts/..%c1%1c../winnt/system32/cmd.exe?/c ...成功
CGI-> 检测 172.16.167.195 /*.ida ...成功
CGI-> 检测 172.16.167.195 /abcxv.htw ...成功
CGI-> 检测 172.16.167.195 /?PageServices ...成功
PLUGIN-> 扫描 172.16.167.195 ...IIS5.0 .Printer Exploit(Grant System Privileges)
PLUGIN-> 扫描 172.16.167.195 ...IIS 5.0 WEBDAV Exploit Please Refer Microsoft Security bulletin MS03-007
```

分析主机漏洞

根据图 22 的探测结果，进行分析并模拟入侵

(1) 端口漏洞分析

主要是 21，23，25，53，80，139，443，3389 端口。

端口 21： FTP 端口，攻击者可能利用用户名和密码过于简单，甚至可以匿名登录到目标主机上，并上传木马或病毒进而控制目标主机。

端口 23： Telnet 端口，如果目标主机开放 23 端口，但用户名和密码过于简单，攻击破解后就可以登录主机并查看任何消息，设置控制目标主机。

端口 25: 25 端口, 为 SMTP 服务器所开放, 主要用于发送邮件。

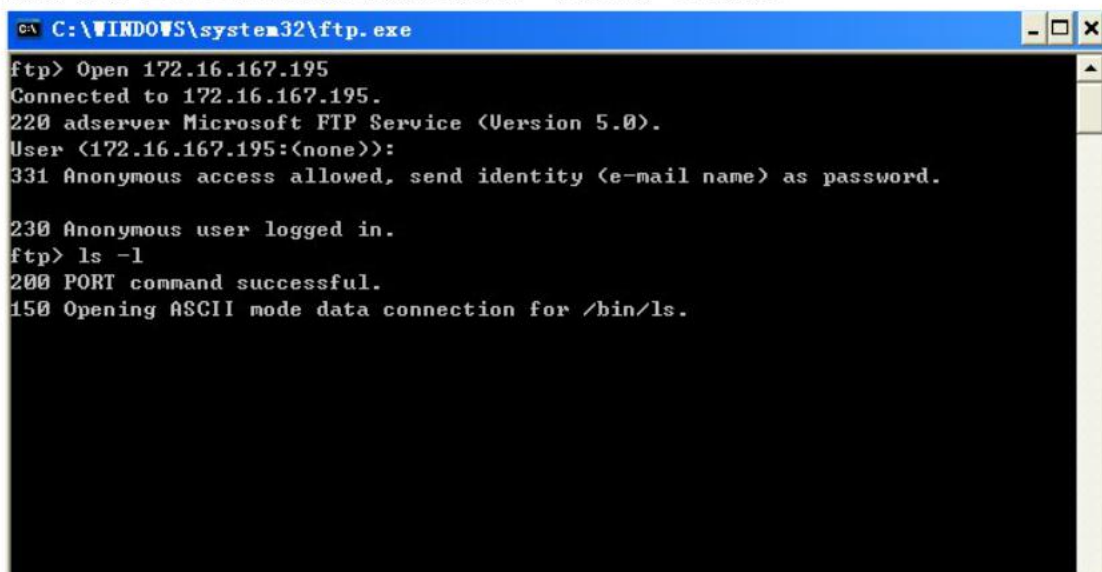
端口 53: 53 端口, 为 DNS 服务器所开放, 主要用于域名解析。

端口 80: HTTP 端口, 80 端口最易受到攻击。

端口 139: NETBIOS 会话服务端口, 主要用于提供 Windows 文件和打印机共享以及 Unix 中的 Samba 服务。139 端口可以被攻击者利用, 建立 IPC 连接入侵目标主机, 获得目标主机的 root 权限并放置病毒或木马。

端口 443: 网页浏览端口, 主要用于 HTTPS 服务, 是提供加密和通过安全端口传输的另一种 HTTP。

端口 3389: 这个端口的开放使安装终端服务和全拼输入法的 Windows2000 服务器存在着远程登录并获得超级用户权限的严重漏洞。



```
C:\WINDOWS\system32\ftp.exe
ftp> Open 172.16.167.195
Connected to 172.16.167.195.
220 adserver Microsoft FTP Service (Version 5.0).
User (172.16.167.195:(none)):
331 Anonymous access allowed, send identity (e-mail name) as password.
230 Anonymous user logged in.
ftp> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
```

五、实验总结

通过 superscan 端口扫描实验, 学习和了解到端口扫描的原理、操作及利用它进行网络安全分析。如: 通过扫描某一特定主机或某已知网段, 可以探测出它们的开放端口, 从而了解到主机的危险程度, 还可以利用它对指定的端口进行扫描, 方便对该类主机做好相关的维护工作, 从而有效避免病毒或黑客的攻击。

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷, 从而使攻击者能够在未授权的情况下访问或破坏系统。通过本次实验我大概懂得了如何利用软件检测出目标主机的漏洞。并认识到了如 FTP、IPC\$ 等漏洞的危害性。所以我们要加强网络安全建设, 未雨绸缪, 做到最小的损失。