

# 渗透测试思路篇——常见端口及利用方式

原创 c00lman 小老弟安全 昨天

## 渗透测试思路篇——常见端口及利用方式

大家好，我是c00lman，渗透测试第一步往往是信息搜集，而端口扫描是信息搜集不可或缺的一部分，今天给大家分享的是常见端口及利用方式。



放弃该放弃的是无奈；  
放弃不该放弃的是无能；  
不放弃该放弃的是无知；  
不放弃不该放弃的是执着。

——唐宁

### FTP服务：

- ①使用系统软件来配置，比如IIS中的FTP文件共享或Linux中的默认服务软件；
- ②是通过第三方软件来配置，比如Serv-U还有一些网上写的简易ftp服务器等；

### 默认端口号：

- 20（数据端口）
- 21（控制端口）
- 22（Sftp安全文件传送协议）
- 69（Tftp小型文件传输协议）

### 攻击方式：

- ①爆破：Metasploit下的ftp\_login模块；
- ②匿名访问：
  - 用户名：空                      密码：空
  - 用户名：anonymous   密码：为空或任意邮箱
  - 用户名：FTP                    密码：FTP或为空
  - 用户名：USET                密码：pass
- ③嗅探：ftp使用明文传输技术所以可以嗅探密码
- ④后门技术：在linux的vsftpv2.3.4中，存在一个后门程序，只要在用户名后面加上“: )”（笑脸符号），就会在6200上打开一个监听Shell，我们可以使用telnet直接连接；
- ⑤远程溢出漏洞：IIS FTP远程溢出漏洞，在IIS FTP服务器中NLST命令存在一个缓冲区溢出漏洞，这个漏洞可能是攻击者在服务器运行一条非法命令。（还有其他版本远程溢出漏洞）
- ⑥跳转攻击：攻击者发送一个FTP“PORT”命令给目标FTP服务器，其中包含该主机的网络地址和被攻击的服务的端口号。这样，客户端就能命令FTP服务器发一个文件给被攻击的服务。这个文件可能包括根被攻击的服务有关的命令（如SMTP,NNTP等）。由于是命令第三方去连接到一种服务，而不是直接连接，就使得跟踪攻击者变得困难，并且还避开了基于网络地址的访问限制。

---

## Nfs服务

### Nfs服务：

Nfs（Network File System）即网络文件系统，是FreeBSD支持的文件系统中的一种，它允许网络中的计算机之间通过TCP/IP网络共享资源。在Nfs的应用中，本地NFS的客户端应用可以透明地读写位于远端NFS服务器上的文件，就像访问本地文件一样。

**默认端口号：**2049

### 攻击方式：

未授权访问：未限制IP以及用户权限设置错误。

---

## Samba服务

### Samba服务:

Samba是linux和unix系统上实现smb协议的一个免费软件，由客户机和服务器构成。SMB是一种在局域网上实现共享文件和打印机的协议。存在一个服务器，客户机通过该协议可以服务器上的共享文件系统和打印机以及其他的资源。Samba登录分为两种方式，一种是需要用户名口令；另一种是不需要用户名口令。

### 默认端口号:

137 (主要用户NetBIOS Name Service; NetBIOS名称服务)

139 (NetBIOS Session Service, 主要提供samba服务)

### 攻击方式:

- ①爆破：爆破工具采用hydra `hydra -l username -P sanPassFile IP smb`
- ②未授权访问：给予public用户高权限
- ③远程代码执行漏洞：CVE-2015-0240等等

---

## LDAP协议

### LDAP协议:

LDAP(Lightweight Directory Access Protocol):轻量级目录访问协议，是一种在线目录访问协议。LDAP主要用于目录中资源的搜索和查询，是X.500的一种简便的实现。

**默认端口号:** 389

### 攻击方式:

- ①爆破：弱口令
- ②未授权访问
- ③注入攻击：盲注

02

## 远程连接服务端口

---

## SSH服务

### SSH服务:

SSH 为建立在应用层基础上的安全协议，SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。

**默认端口号:** 22

### 攻击方式:

- ①爆破：`hydra -l root -P password.txt -t 6 ssh://ip`
- ②漏洞：28退格漏洞、OpenSSL漏洞等等

---

## Telnet服务

### Telnet服务:

Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议和主要方式。Telnet是常用的远程控制Web服务器的方法。

**默认端口号：**23

**攻击方式：**

- ①爆破：hydra -L u.txt -P p.txt ip telnet
- ②嗅探

---

### Rdp服务

**远程桌面连接：**

远程桌面协议（RDP, Remote Desktop Protocol）是一个多通道（multi-channel）的协议，让用户（客户端或称“本地电脑”）连上提供微软终端机服务的电脑（服务器端或称“远程电脑”）。

**默认端口号：**3389

**攻击方式：**

- ①爆破：hydra ip rdp -L users.txt -P pass.txt -V
- ②Shift粘滞键后门：5次shift后门
- ③3389漏洞攻击：ms12-020

---

### VNC

**VNC：**

VNC 是在基于 UNIX 和 Linux 操作系统的免费的开源软件，远程控制能力强大，高效实用，其性能可以和 Windows 和 MAC 中的任何远程控制软件媲美。

**默认端口号：**5900+桌面ID（5901；5902）

**攻击方式：**

- ①爆破：hydra -P pass.txt -f -v -t 20 vnc://ip
- ②认证口令绕过
- ③拒绝服务攻击：CVE-2015-5239
- ④权限提升：CVE-2013-6886

---

### Pcanywhere服务

**PyAnywhere服务：**

PcAnywhere是一款远程控制软件，你可以将你的电脑当成主控端去控制远方另一台同样安装有pcANYWHERE的电脑（被控端），你可以使用被控端电脑上的程序或在主控端与被控端之间互传文件。你也可以使用其闸道功能让多台电脑共享一台MODEM或是向网路使用者提供打进或打出的功能。

**默认端口号：**5632

**攻击方式：**

- ①提权控制服务

②拒绝服务攻击

③代码执行

03

## Web应用服务端口

### HTTP服务

#### HTTP:

超文本传输协议 (HTTP, HyperText Transfer Protocol)是互联网上应用最为广泛的一种网络协议。所有的WWW文件都必须遵守这个标准。

**默认端口号:** 80

#### 攻击方式:

①web攻击

②相关漏洞

### IIS服务

#### IIS:

iis是Internet Information Services的缩写，意为互联网信息服务，是由微软公司提供的基于运行Microsoft Windows的互联网基本服务。IIS是一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络（包括互联网和局域网）上发布信息成了一件很容易的事。

**默认端口号:** 80/81/443

#### 攻击方式:

①IIS PUT写文件：利用IIS漏洞，put方法直接将文件放置到服务器上

②短文件名泄漏

③解析漏洞

### Apache/Tomcat/Nginx

**默认端口号:** 80/8080

#### 攻击方式:

①爆破

②HTTP慢速攻击

### WebLogic

#### WebLogic:

WebLogic是一个基于JAVAEE架构的中间件，WebLogic是用于开发、集成、部署和管理大型分布式Web应用、网络应用和数据库应用的Java应用服务器。将Java的动态功能和Java Enterprise标准的安全性引入大型网络应用的开发、集成、部署和管理之中。

**默认端口号:** 7001、7002

### 攻击方式:

- ①爆破
- ②Congsole后台部署webshell
- ③Java反序列化:
- ④泄漏源代码/列目录
- ⑤SSRF窥探内网

---

Jboss\Resin\Jetty\Jenkins

**默认端口号:** 8080、8089

### 攻击方式:

- ①爆破
- ②远程代码执行
- ③Java反序列化

---

Websphere

### WebSphere:

WebSphere 包含了编写、运行和监视全天候的工业强度的随需应变 Web 应用程序和跨平台、跨产品解决方案所需要的整个中间件基础设施，如服务器、服务和工具。WebSphere 提供了可靠、灵活和健壮的软件。

**默认端口号:** 9080、9081、9090

### 攻击方式:

爆破  
任意文件泄漏: CVE-2014-0823  
Java反序列化

---

GlassFish

### GlassFish:

GlassFish是一款强健的商业兼容应用服务器，达到产品级质量，可免费用于开发、部署和重新分发。

**默认端口号:** 8080、3700、4848

### 攻击方式:

- ①爆破
- ②任意文件读取
- ③认证绕过

---

Lotus

### Lotus:

IBM Lotus Notes是一个协作客户端-服务器平台的客户端。IBM Lotus Domino是此应用程序的服务器端。

**默认端口号：**1352

**攻击方式：**

- ①爆破：弱口令（admin password）控制台
- ②信息泄露
- ③跨站脚本攻击

04

## 数据库服务端口

### MySQL数据库

**默认端口号：**3306

**攻击方式：**

- ①爆破
- ②身份认证漏洞：CVE-2012-2122
- ③拒绝服务攻击
- ④Phpmyadmin万能密码绕过：  
用户名：'localhost'@'@" 密码任意

### MSSQL数据库

**默认端口号：**

- 1433（Server 数据库服务）
- 1434（Monitor 数据库监控）

**攻击方式：**

爆破：弱口令/使用系统用户

### Oracle数据库

**默认端口号：**

- 1521（数据库端口）
- 1158（Oracle EMCTL端口）
- 8080（Oracle XDB数据库）
- 210（Oracle XDB FTP服务）

**攻击方式：**

- ①爆破：弱口令
- ②注入攻击
- ③漏洞攻击

### PostgreSQL数据库

**默认端口号：**5432

### 攻击方式:

- ①爆破: 弱口令: postgres postgres
- ②缓冲区溢出: CVE-2014-2669

### MongoDB数据库

默认端口号: 27017

### 攻击方式:

- ①爆破: 弱口令
- ②未授权访问

### Redis数据库

默认端口号: 6379

### 攻击方式:

- ①爆破: 弱口令
- ②未授权访问+配合ssh key提权

### SysBase数据库

### 默认端口号:

服务端口5000  
监听端口4100  
备份端口4200

### 攻击方式:

- ①爆破: 弱口令
- ②命令注入

### DB2数据库

默认端口号: 5000

### 攻击方式:

安全限制绕过: CVE-2015-1922

05

## 邮件服务端口

### SMTP协议

### SMTP:

SMTP (Simple Mail Transfer Protocol) 即简单邮件传输协议,它是一组用于由源地址到目的地址传送邮件的规则,由它来控制信件的中转方式。

### 默认端口号:

25 (smtp)  
465 (smtps)



### 攻击方式:

- ①爆破: 弱口令
- ②未授权访问

---

## POP3协议

### POP3协议:

POP3全名为“Post Office Protocol - Version 3”，即“邮局协议版本3”。是TCP/IP协议族中的一员，由RFC1939 定义。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。提供了SSL加密的POP3协议被称为POP3S。

### 默认端口号:

- 109 (POP2)
- 110 (POP3)
- 995 (POP3S)

### 攻击方式:

- ①爆破; 弱口令
- ②未授权访问;

---

## IMAP协议

### IMAP:

IMAP协议运行在TCP/IP协议之上，使用的端口是143。它与POP3协议的主要区别是用户不用把所有的邮件全部下载，可以通过客户端直接对服务器上的邮件进行操作。

### 默认端口号:

- 143 (imap)
- 993 (imaps)

### 攻击方式:

- ①爆破: 弱口令
- ②配置不当

06

## 网络常见协议端口

---

## DNS服务

默认端口号: 53

### 攻击方式:

- ①区域传输漏洞
- ②DNS劫持
- ③缓存投毒

---

## DHCP服务

默认端口号:

67、68、546

**攻击方式：**

①DHCP劫持

②DHCP欺骗

---

SNMP协议

**默认端口号：** 161

**攻击方式：**

爆破：弱口令

不努力  
你背井离乡干嘛  
当卧底啊

