呼伦贝尔学院 计算机学院

题 目： 服务器配置与管理

学生姓名： 薛彬

学 号： 201512108051

专业班级： 2015级本7（云计算）班

指导教师： 王继钢

完成时间： 2017年11月20日

摘要

本文以配置网络服务器为主,基于Windows Server 2008系统的介绍了DNS服务器;DHCP服务器;FTP服务器;网络存储,的原理及工作过程,以及在Windows Server 2008下常用的服务器配置,还对常用的服务器软件进行了对比和优缺点的说明.

DNS服务器的是计算机域名系统.域名服务器是保存网络在所有主机和域名对应的IP地址,并有域名转换功能.在域名必须符合IP地址,IP地址不必须域名.域名系统类似目录树层次结构.DNS服务器的客户端服务器模型在服务器端,它主要有两种主服务器和重定向服务器.域名是IP地址映射到的过程被称为“域名解析”.

生活与互联网越来越密切.不同网络建设.网络管理是大型计算机网络成功的关键.DHCP服务,成为非常受欢迎的配置协议.动态主机主机（DHCP）适用也越来越重要.在实际操作中,DHCP服务器建设越来越常见.使用DHCP动态主机配置参数,可以解决有效地处IP地址资源不足和用户移动性,可以大大减少管理人员的工作量,在大型网络,减少错误手动配置网络.

文件传输协议（FTP）作为网络共享文件的传输协议,在网络应用软件中具有广泛的应用.FTP的目标是提高文件的共享性和可靠高效地传送数据. 开始出现在Unix系统FTP文件传输协议文件传输,现在广泛使用的不同类型的,服务网络.在服务器/客户端,主要功能包括文件下载和文件上传.FTP服务器的默认设置,两个端口21和20,21为监测端口,监测FTP客户端连接请求.港20文件传输只在文件传输过程中打开,转换完成后关闭.FTP使用客户1024~65535动态端口由客户端FTP软件自动分配.

网络存储(Network Storage)是基于数据存储的一种,网络存储结构大致分为三种:直连式存储(DAS:Direct Attached Storage)、网络存储设备(NAS:Network Attached Storage)和存储网络(SAN:Storage Area Network),由于NAS对于普通消费者而言较为熟悉,所以一般网络存储都指NAS.

关键词 DNS服务器;DHCP服务器;FTP服务器;网络存储

目录

[第1章 绪论 5](#_Toc499411788)

[第2章 DNS服务器 6](#_Toc499411789)

[2.1 DNS原理及工作过程 6](#_Toc499411790)

[2.1.1 概述 6](#_Toc499411791)

[2.1.2 工作原理 6](#_Toc499411792)

[2.1.3 工作过程 6](#_Toc499411793)

[2.2 几种DNS服务器使用的软件及它们的比较、特点 7](#_Toc499411794)

[2.2.1 Bind 7](#_Toc499411795)

[2.2.2 dnspod-sr 7](#_Toc499411796)

[2.2.3 DNSmasq 7](#_Toc499411797)

[2.3 选取一种软件进行DNS服务器配置,说明过程 7](#_Toc499411798)

[2.4 DNS服务器的安全问题及解决方法 12](#_Toc499411799)

[第3章 第三章 DHCP服务器 15](#_Toc499411800)

[3.1 DHCP的原理及工作过程 15](#_Toc499411801)

[3.1.1 DHCP 基本原理简介 15](#_Toc499411802)

[3.1.2 DHCP的工作过程 15](#_Toc499411803)

[3.2 比较几种架构DHCP服务器的软件,及它们的优缺点 16](#_Toc499411804)

[3.2.1 Open DHCP Server 16](#_Toc499411805)

[3.2.2 DHCP Server 7.0 17](#_Toc499411806)

[3.2.3 DHCP Server for Windows 17](#_Toc499411807)

[3.3 选取一种软件进行DHCP服务器的配置,说明过程 17](#_Toc499411808)

[3.4 针对DHCP服务器的安全问题提出解决方法 18](#_Toc499411809)

[3.4.1 DHCP服务欺骗攻击 18](#_Toc499411810)

[3.4.2 ARP“中间人”攻击 19](#_Toc499411811)

[3.4.3 IP/MAC欺骗攻击 19](#_Toc499411812)

[3.4.4 DHCP报文泛洪攻击 19](#_Toc499411813)

[3.4.5 应用限制 19](#_Toc499411814)

[第4章 FTP服务器 20](#_Toc499411815)

[4.1 介绍FTP的原理及工作过程 20](#_Toc499411816)

[4.1.1 FTP的原理 20](#_Toc499411817)

[4.2 FTP的及工作过程 20](#_Toc499411818)

[4.3 比较几种架构FTP服务器的软件、说明它们的优缺点 22](#_Toc499411819)

[4.3.1 net2ftp 22](#_Toc499411820)

[4.3.2 Wing FTP Server 22](#_Toc499411821)

[4.3.3 Apache FtpServer 22](#_Toc499411822)

[4.3.4 SwiFTP 22](#_Toc499411823)

[4.4 选取一种软件进行FTP服务器的配置,说明过程 23](#_Toc499411824)

[4.5 针对FTP服务器的安全问题提出解决方法 24](#_Toc499411825)

[4.5.1 ftp服务器存在的安全问题 24](#_Toc499411826)

[4.5.2 增强ftp服务器安全性 25](#_Toc499411827)

[第5章 网络存储 28](#_Toc499411828)

[5.1 介绍网络存储原理 28](#_Toc499411829)

[5.2 比较几种网络存储方案、说明它们的优缺点 28](#_Toc499411830)

[5.2.1 FC-SAN 28](#_Toc499411831)

[5.2.2 IP-SAN 29](#_Toc499411832)

[5.3 网络存储的安全问题 29](#_Toc499411833)

[总结 32](#_Toc499411834)

[参考文献 33](#_Toc499411835)

1. 绪论

Windows Server 2008是迄今最稳固的 Windows Server 操作系统,其内置的强化 Web 和虚拟化功能,是专为增加服务器基础架构的可靠性和弹性而设计,亦可节省时间及降低成本.其系利用功能强大的工具,拥有更好的服务器控制能力,并简化设定和管理工作；而增强的安全性功能则可强化操作系统,以协助保护数据和网路,并可为的企业提供扎实且可高度信赖的基础.

DNS就是进行域名解析的服务器. DNS 命名用于 Internet 等 TCP/IP 网络中,通过用户友好的名称查找计算机和服务.当用户在应用程序中输入 DNS 名称时,DNS 服务可以将此名称解析为与之相关的其他信息,如 IP 地址.因为,你在上网时输入的网址,是通过域名解析系统解析找到了相对应的IP地址,这样才能上网.其实,域名的最终指向是IP.

DHCP（Dynamic Host Configuration Protocol,动态主机配置协议）通常被应用在大型的局域网络环境中,主要作用是集中的管理、分配IP地址,使网络环境中的主机动态的获得IP地址、Gateway地址、DNS服务器地址等信息,并能够提升地址的使用率.

FTP 是 TCP/IP 协议组中的协议之一,是英文File Transfer Protocol的缩写.该协议是Internet文件传送的基础,它由一系列规格说明文档组成,目标是提高文件的共享性,提供非直接使用远程计算机,使存储介质对用户透明和可靠高效地传送数据.

网络存储被定义为一种特殊的专用数据存储服务器,包括存储器件（例如磁盘阵列、CD/DVD驱动器、磁带驱动器或可移动的存储介质）和内嵌系统软件,可提供跨平台文件共享功能.

# DNS服务器

## DNS原理及工作过程

### 概述

DNS( Domain Name System)是“域名系统”的英文缩写,是一种组织成域层次结构的计算机和网络服务命名系统,它用于TCP/IP网络,它所提供的服务是用来将主机名和域名转换为IP地址的工作.

### 工作原理

任何计算机如果需要连接internet网,那么,首先需要设置一些关于DNS的信息.您的电脑需要借助于Internet上的某台域名服务器帮助进行域名查询.所以您首先需要设置您的电脑,在需要进行域名查询时,向哪个服务器发出询问.Internet上有许许多多域名服务器,您可以选任何一台作为您首选的域名服务器.也就是说,您要告诉您的电脑,当需要进行域名查询时,首先去问哪一台域名服务器.域名服务器接收到您的电脑的查询请求,它会帮助您进行查询,然后将结果返回您的电脑.为了获得最快的响应,一般选择与您的电脑有最好的连接的服务器.一般的电脑上,其实已经不用在设置了,在>本地连接>属性>internet协议（TCP/IP）>自动获得DNS服务器后者手动添加首选DNS与备选DNS.

### 工作过程

主机向本地域名服务器的查询一般都是采用递归查询.所谓递归查询就是：如果主机所询问的本地域名服务器不知道被查询的域名的IP地址,那么本地域名服务器就以DNS客户的身份,向其它根域名服务器继续发出查询请求报文(即替主机继续查询),而不是让主机自己进行下一步查询.因此,递归查询返回的查询结果或者是所要查询的IP地址,或者是报错,表示无法查询到所需的IP地址.

本地域名服务器向根域名服务器的查询的迭代查询.迭代查询的特点：当根域名服务器收到本地域名服务器发出的迭代查询请求报文时,要么给出所要查询的IP地址,要么告诉本地服务器：“你下一步应当向哪一个域名服务器进行查询”.然后让本地服务器进行后续的查询.根域名服务器通常是把自己知道的顶级域名服务器的IP地址告诉本地域名服务器,让本地域名服务器再向顶级域名服务器查询.顶级域名服务器在收到本地域名服务器的查询请求后,要么给出所要查询的IP地址,要么告诉本地服务器下一步应当向哪一个权限域名服务器进行查询.最后,知道了所要解析的IP地址或报错,然后把这个结果返回给发起查询的主机.如图 2‑1 dns服务器的工作过程所示.

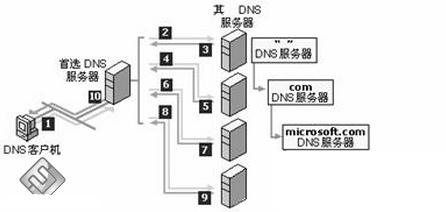


图 2‑1 dns服务器的工作过程

## 几种DNS服务器使用的软件及它们的比较、特点

### Bind

目前互联网上最为广泛的DNS服务器为bind,而企业内部,由于很多企业使用windows AD域,因此Windows DNS在企业内部应用较多.Bind是一款开放源码的DNS服务器软件,Bind由美国加州大学Berkeley分校开发和维护的,全名为Berkeley Internet Name Domain它是目前世界上使用最为广泛的DNS服务器软件,支持各种unix平台和windows平台.

### dnspod-sr

dnspod-sr 是一个运行在 Linux 平台上的高性能的递归 DNS 服务器软件,具备高性能、高负载、易扩展的优势,非 BIND 等软件可以比拟.高性能,比所有流行的开源 DNS 软件性能高出2倍以上,安全,能抵御一般攻击,稳定性,有效降低解析失败率,主动刷新缓存,响应速度更快,易于扩展,非常容易部署,防污染,能够正确解析被污染域名.dnspod-sr 依托于 DNSPod 多年运营和优化 DNS 服务的经验,针对国内复杂的网络情况,对递归 DNS 进行了一系列的优化,比较其他开源软件,性能得到大幅提升.

### DNSmasq

DNSmasq是一个轻巧的,容易使用的DNS服务工具,它可以应用在内部网和Internet连接的时候的IP地址NAT转换,也可以用做小型网络的DNS服务.轻量级DHCP和DNS缓存服务器,同时能提供轻量TFTP,PXE,路由广播服务,本地无法解析的dns请求,会向真正的dns服务器转发.自动加载/etc/hosts中内容,作为解析项之一,同时支持DHCPv4和DHCPv6.

## 选取一种软件进行DNS服务器配置,说明过程

下面给出win sever 2008上dns的服务器配置过程.

#### 1.安装dns服务器.如图 2‑2 安装dns服务器所示.

图 2‑2 安装dns服务器

#### 2.选择服务器角色.如图 2‑3 选择服务器角色所示.

图 2‑3 选择服务器角色

#### 73.完成安装.如图 2‑4 完成安装所示.

图 2‑4 完成安装

#### 4. 架设主DNS服务器.如图 2‑5 架设主dns服务器所示.

图 2‑5 架设主dns服务器

#### 5. 对DNS创建正向查找区域.如图 2‑6 对DNS创建正向查找区域所示.

图 2‑6 对DNS创建正向查找区域

#### 6.输入区域名称.如图 2‑7 输入区域名称所示.

图 2‑7 输入区域名称

#### 7.创建区域文件.如图 2‑8 创建区域文件所示.

图 2‑8 创建区域文件

#### 8. 正向查找区域创建成功.如图 2‑9 正向查找区域创建成功所示.

图 2‑9 正向查找区域创建成功

#### 9. 创建反向查找区域.如图 2‑10 创建反向查找区域所示.

图 2‑10 创建反向查找区域

#### 10．输入区域文件名.如图 2‑11 输入区域文件名所示.

图 2‑11 输入区域文件名

#### 11.完成创建.如图 2‑12 完成创建所示.

图 2‑12 完成创建

#### 12.新建指针.如图 2‑13 新建指针所示.

图 2‑13 新建指针

#### 13.新建完成.如图 2‑14 新建完成所示.

图 2‑14 新建完成

## DNS服务器的安全问题及解决方法

#### 1.DNS服务面临的攻击

DNS由于早期设计上的缺陷为日后的应用埋下了安全隐患.因为过于强调对网络的适应性,采用了面向非连接的UDP协议,但UDP协议本身是不安全的.而且从体系结构上来看,DNS采用树形结构,虽然便于查询操作,但是单点故障非常明显,也使得安全威胁加剧.另外,绝大多数DNS服务器都是基于BIND这个软件,但是BIND在提供

高效服务的同时也存在着众多的安全性漏洞.这里构成严重威胁的主要有两种漏洞：

一种是缓冲区溢出漏洞,如BIND4和BIND8中存在一个远程缓冲溢出缺陷,该缺陷使得攻击者可以在DNS上运行任意指令.另一种是拒绝服务漏洞,受攻击后DNS服务器不能提供正常服务,使得其所辖的子网无法正常工作

#### 2.拒绝服务攻击

DNS服务器的关键地位使它成为网络攻击的显著目标,加上其对拒绝服务攻击没有防御能力,所以在现有的树状结构下,一旦DNS服务器不能提供服务,其所辖的子域都无法解析域名,仅能通过难以记忆的IP地址访问网络,对多数网络用户而言,无法接入网络,甚至还会被利用来对其他主机进行反弹式DDoS攻击.

#### 3.缓冲区中毒

DNS为了提高查询的效率,采用缓存机制,在DNS缓存数据还没有过期之前,在DNS的缓存区中已存在的记录一旦被库户查询,DNS服务器将把缓存区中的记录直接返回客户.DNS缓存区中毒就是利用了DNS的缓存机制,在缓存区中存入错误的数据使其被其他查询客户所获得.在缓存数据的生存期内,缓存区中毒的机器又可能将错误的数据传播出去,导致更多的服务器缓存中毒.如果减少缓存数据的生存期,可以减少缓存中毒的影响范围,但过于频繁的缓存数据更新将大大增加服务器的负担.

#### 4.区域信息泄露

DNS服务器作为公开开放的数据库,对域名请求查询通常不加以验证,网络拓扑、子网结构等信息容易泄漏,也为各类攻击提供了机会.

#### 5.域名劫持

域名劫持通常是指通过采用非法手段获得某一个域名管理员的账户名称和密码,或者域名管理邮箱,然后将该域名的IP地址指向其他主机.域名被劫持后,不仅有关该域名的记录会该百年,甚至该域名的所有权可能会落到其他人手里.另外,域名服务器没有准入制度,域名服务提供商缺乏相应的监管制度,也是给各种攻击提供可乘之机.

#### 6.DNS安全增强方案

通过DNS服务器本身的配臵以及与防火墙等的合作来加强DNS的安全性.限制访问DNS服务器的网络数据包的类型,实施包过滤的依据主要是端口、IP、流量.端口过滤指仅允许对53端口的访问；IP地址限制指只允许具有合法II)地址的用户访问该DNS服务器；流量限制指对每个IP地址的DNS请求加以流量限制,正常用户数据包的长度应不大于512 byte. 1.2 防火墙保护(split DNS或split-split DNS)

#### 7.网络拓扑限制

为了减少单点故障的威胁,从网络拓扑结构角度应避免将DNS服务器臵于无旁路的环境下,不应将所有的DNS服务器臵于同一子网、同一租用链路、同一路由器、同一自治域甚至同一物理位臵.

#### 8.D D o S 攻击的防范

解决D D o S 攻击的最有效方法有以下几种：

一是部署I D S ,从单一技术和设备来看,I D S 是目前防范D D o S 攻击最有效的方法；

二是对于重要的D N S 服务器,可分别在不同的I D C 中部署,通过冗余方式来提高D N S 的安全；

三是在防火墙上通过设臵策略,对于超过某一限定值的D N S 请求报文进行过滤；

四是通过管理软件,对排名靠前的D N S 解析请求报文进行分析,重点分析哪些流量在短时间内急剧增大的报文,对可疑报文进行过滤处理.

#### 9.D N S 服务器的冗余备份

冗余备份是D N S 服务器安全管理中采用的一种较为普遍的方法.即使是在局域网中,为了保障D N S 服务的可靠性,会采用多机备份方案.与局域网相比,互联网的结构和应用要复杂的多,对D N S 的安全性要求也非常高.为此,对于互联网中的D N S服务器,建议能够创建位于不同I D C中的分布式系统.

# 第三章 DHCP服务器

## DHCP的原理及工作过程

### DHCP 基本原理简介

Dynamic Host Configuration Protocol----动态主机配置协议,DHCP的前身是BOOTP协议.当一台主机接入网络的时候,在没有IP地址的时候,向网络上发送DHCP请求（广播）获取IP地址时,正是因为自己没有IP地址,所以在发送数据包的时候,源IP是0.0.0.0,源MAC正常,而自己也不可能知道DHCPServer在什么地方,所以数据包是目的IP为255.255.255.255、目标MAC为FFFFFF的广播包.如果本地网络中存在DHCPServer时,那么DHCP从某个网卡收到请求后,便想客户端发送一个DHCP offer消息,其中包含了Client所需要的IP地址,子网掩码,默认网关,DNS,租期等信息.

### DHCP的工作过程

DHCP服务器提供三 种IP分配方式：自动分配（Automatic Allocation）、动态分配（Dynamic Allocation）和手动分配.自动分配是当DHCP客户端第一次成功地从DHCP服务器端分配到一个IP地址之后,就永远使用这个地址.动态分配是 当DHCP客户端第一次从DHCP服务器分配到IP地址后,并非永久地使用该地址,每次使用完后,DHCP客户端就得释放这个IP地址,以给其他客户端使 用,而手动分配是由DHCP服务器管理员专门指定IP地址.

DHCP客户机在启动时,会搜寻网络中是否存在DHCP服务器.如果找到,则给 DHCP服务器发送一个请求.DHCP服务器接到请求后,为DHCP客户机选择TCP/IP配置的参数,并把这些参数发送给客户端. 如果已配置冲突检测设置,则 DHCP 服务器在将租约中的地址提供给客户机之前会试用Ping测试作用域中每个可用地址的连通性.这可确保提供给客户的每个IP地址都没有被使用手动 TCP/IP配置的另一台非 DHCP 计算机使用.

根据客户端是否第一次登录网络,DHCP的工作形式会有所不同.客户端从DHCP服务器上获得IP地址的整个过程分为以下六个步骤：

#### 1．寻找DHCP服务器

当 DHCP客户端第一次登录网络的时候,计算机发现本机上没有任何IP地址设定,将以广播方式发送DHCP discover发现信息来寻找DHCP服务器,即向255.255.255.255发送特定的广播信息.网络上每一台安装了TCP/IP协议的主机都会 介绍这个广播信息,但只有DHCP服务器才会做出响应.

#### 2．分配IP地址

在网络中接收到DHCP discover发现信息的DHCP服务器都会做出相应,它从尚未分配的IP地址中挑选一个分配给DHCP客户机,向DHCP客户机发送一个包含分配的IP地址和其他设置的DHCP offer提供信息.

#### 3．接受 IP地址

DHCP客户端接受到DHCP offer提供信息之后,选择第一个接收到的提供信息,然后以广播的方式回答一个DHCP request请求信息,该信息包含向它所选定的DHCP服务器请求IP地址的内容.

#### 4．IP地址分配确认

当 DHCP服务器收到DHCP客户端回答的DHCP request请求信息之后,便向DHCP客户端发送一个包含它所提供的IP地址和其他设置的DHCP ack确认信息,告诉DHCP客户端可以使用它提供的IP地址.然后,DHCP客户机便将其TCP/IP协议与网卡绑定,另外,除了DHCP客户机选中的 服务器外,其他的DHCP服务器将收回曾经提供的IP地址.

#### 5．重新登录

以 后DHCP客户端每次重新登录网络时,就不需要再发送DHCP discover发现信息了,而是直接发送包含前一次所分配的IP地址的DHCP request请求信息.当DHCP服务器收到这一信息后,它会尝试让DHCP客户机继续使用原来的IP地址,并回答一个DHCP ack确认信息.如果此IP地址已无法再分配给原来的DHCP客户机使用时,则DHCP服务器给DHCP客户机回答一个DHCP nack否认信息.当原来的DHCP客户机收到此DHCP nack否认信息后,它就必须重新发送DHCPdiscover发现信息来请求新的IP地址.

#### 6．更新租约

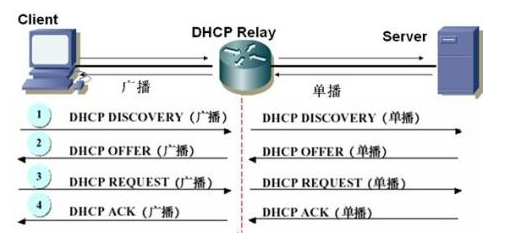
DHCP 服务器向DHCP客户机出租的IP地址一般都有一个租借期限,期满后DHCP服务器便会收回出租的IP地址.如果DHCP客户机要延长其IP租约,则必须 更新其IP租约.DHCP客户机启动时和IP租约期限过一半时,DHCP客户机都会自动向DHCP服务器发送更新其IP租约的信息.如图 3‑1 dhcp服务器工作过程所示.

图 3‑1 dhcp服务器工作过程

## 比较几种架构DHCP服务器的软件,及它们的优缺点

### Open DHCP Server

Open DHCP Server是多个子网DHCP服务器.它支持动态和静态租约.它支持多个域.它支持中继代理.它支持BOOTP和pxeboot.它有用户定义选项.选项可以是全局的、特定于范围的和特定于客户的.可以通过MAC地址范围过滤DHCP范围.

### DHCP Server 7.0

DHCP Server是指在一个特定的网络中管理DHCP标准的一台计算机.一个DHCP服务器能够够指定IP给其它局域网中的电脑,让每一台电脑都能够连在TCP/IP的通讯协议下,而且有其独立的IP,自成一个网段.而透过DHCP Server的管理方式,你能够设定IP分配的范围,清楚地了解到目前各台电脑被分配的IP与网卡编号信息等.

### DHCP Server for Windows

DHCP服务器为客户端计算机分配IP地址,通常应用在企业网络中以减小配置成本,所有客户端的IP地址都保存在服务器端.

这是一款非常简单且易用使用的基于Windows系统的DHCP服务器软件,支持从Windows 98至Windows 7的所有Windows系统.除客户端数据库之外的配置数据均保存在一个INI文件中,并且无需安装即可运行.这款DHCP服务器软件是免费的：可以以研究和商业目的使用和重新分发它而绝对没有任何费用,没有版税或类似GNU的“CopyLeft”的限制,无需包含版权信息或Logo,无需提供任何形式的担保.

## 选取一种软件进行DHCP服务器的配置,说明过程

下面给出win sever 2008上dhcp的服务器配置过程.

#### 添加角色.如图 3‑2 添加角色所示.

图 3‑2 添加角色

#### 网络连接绑定.如图 3‑3 网络连接绑定所示.

图 3‑3 网络连接绑定

#### 用激活作用域.如图 3‑4 用激活作用域所示.

图 3‑4 用激活作用域

#### 修改IP地址池和租约期限.如图 3‑5 修改IP地址池和租约期限所示.

图 3‑5 修改IP地址池和租约期限

#### 5.安装完成.如图 3‑6 安装完成所示.

图 3‑6 安装完成

## 针对DHCP服务器的安全问题提出解决方法

### DHCP服务欺骗攻击

在DHCP工作过程中,通常服务器和客户端没有认证机制,如果网络上存在多台DHCP服务器,不仅会给网络造成混乱,也对网络安全造成很大威胁.这种网络中出现非法的DHCP服务器,通常分为两种情况：1、用户不小心配置的DHCP服务器,由此引起的网络混乱非常常见. 2、黑客将正常的DHCP服务器的IP地址耗尽,然后冒充合法的DHCP服务器,为客户端分配IP地址等配置参数.例如黑客利用冒充的DHCP服务器,为用户分配一个经过修改的DNS服务器地址,在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站,骗取用户的账户和密码,这种攻击的危害是很大.

为了防止DHCP服务欺骗攻击,交换机提供了\ Snooping信任端口\特性,对DHCP服务器信息来源进行控制.只允许处理信任端口接收的DHCP响应报文,而非信任端口接收到的DHCP响应报文被交换机丢弃,防止DHCP客户端从网络中不可信任的DHCP服务器获取IP地址.

### ARP“中间人”攻击

按照ARP协议的设计,一个主机即使收到的ARP应答并非自身请求得到的,也会将其IP地址和MAC地址的对应关系添加到自身的ARP映射表中.这样可以减少网络上过多的ARP数据通信,但也为“ARP欺骗”创造了条件.

为了防止ARP中间人攻击,交换机提供了\入侵检测\特性,根据动态获取的DHCP Snooping表项或静态配置的IP与MAC绑定表项,对非法ARP报文进行过滤,保证接入交换机只传递合法的ARP请求和应答信息.

### IP/MAC欺骗攻击

常见的欺骗种类有MAC欺骗、IP欺骗、IP/MAC欺骗,黑客可以伪造报文的源地址进行攻击,其目的一般为伪造身份或者获取针对IP/MAC的特权,另外此方法也被应用与DOS（Deny of Service,拒绝服务）攻击,严重的危害了网络安全.

为了防止IP/MAC欺骗攻击,交换机提供了IP过滤特性,开启该功能后,减缓级可以强制经过某一端口流量的源地址符合动态获取的DHCP Snooping表项或静态配置的IP与MAC绑定表项的纪录,防止攻击者通过伪造源地址来实施攻击.此外,该功能也可以防止用户随便指定IP地址,造成的网络地址冲突等现象.

### DHCP报文泛洪攻击

DHCP报文泛洪攻击是指：恶意用户利用工具伪造大量DHCP请求报文发送到服务器,一方面恶意耗尽了IP资源,使得合法用户无法获得IP资源；另一方面,如果交换机上开启了DHCP Snooping功能,会将接受到的DHCP报文上传到CPU.因此大量的DHCP报文攻击设备会使DHCP服务器高负荷运行,甚至会导致设备瘫痪.

为了防止上述DHCP报文泛洪攻击,交换机提供了“DHCP报文限速”特性,使受到攻击的端口暂时关闭,来避免此类攻击对网络和服务器的冲击.

### 应用限制

DHCP中继和DHCP Snooping 的安全特性运行于不同的网络环境中,因此两者只需选择其一应用.在同一交换机上,DHCP Snooping的启动需以关闭DHCP中继为前提.为了使DHCP客户端通过DHCP Snooping 设备从合法的DHCP服务器获取IP地址,必须将DHCP Snooping 设备上与合法DHCP服务器相连的端口设置为信任端口,设置的信任端口和与DHCP客户端相连的端口必须在同一个VLAN内.

建议用户不要在交换机上同时配置DHCP Snooping 功能和灵活QinQ功能.否侧可能导致DHCP Snooping功能无法正常使用.配置IP过滤功能之前,需要先开启交换机的DHCP Snooping功能,并配置信任端口.建议用户不要在汇聚组中的端口上配置IP过滤功能.如果交换机支持IRF功能,建议用户不要在Fabric端口上配置IP过滤功能.

# FTP服务器

## 介绍FTP的原理及工作过程

### FTP的原理

FTP是文件传输控制协议.它可以使文件通过网络从一台主机传送到另一台主机上,而不受计算机类型和操作系统类型的限制.无论是PC机、服务器、大型机,还是DOS操作系统、Windows操作系统、Linux操作系统,只要双方都支持FTP协议,就可以方便地传送文件

FTP服务的具体工作过程如下图（主动模式）

1.当FTP客户端发出请求时,系统将动态分配一个端口（如1032）.

2.若FTP服务器在端口21侦听到该请求,则在FTP客户端的端口1032和FTP服务器的端口21之间建立起一个FTP会话连接.

3.当需要传输数据时,FTP客户端再动态打开一个连接到FTP服务器的端口20的第2个端口（如1033）,这样就可在这两个端口之间进行数据的传输.当数据传输完毕后,这两个端口会自动关闭.

4.当FTP客户端断开与FTP服务器的连接时,客户端上动态分配的端口将自动释放掉.

## FTP的及工作过程

根据数据连接的建立方式,FTP服务的数据传输可以分为Port（主动）模式和Passive（被动）模式 1）主动模式是FTP服务器向FTP客户端传输数据的默认模式.当FTP客户端请求以主动模式传输数据时,由客户端向服务端发送准备接收数据的IP地址和端口Y,该端口是大于1024的非特权端口.服务端主动发起并建立连接到指定的IP地址和端口20,所以称为主动模式 .

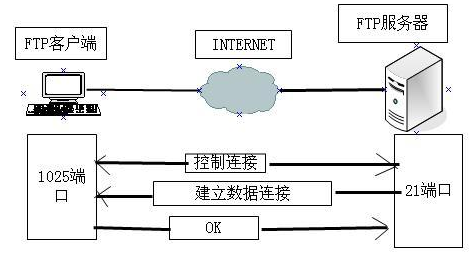
在主动模式中,FTP客户端随机开启一个大于1024的端口X向服务器的21号端口发起控制连接请求,然后开放X+1 号端口进行监听；FTP服务器接受请求并建立控制连接会话.如果客户端在控制会话中发送数据连接请求,那么服务器在接收到命令后,会用其本地的FTP数据 端口（通常是20）来连接客户端指定的端口X+1进行数据传输.如图 4‑1 ftp主动模式工作过程所示.

图 4‑1 ftp主动模式工作过程

在被动模式下,客户端通过PASV命令获得服务端IP地址和数据端口,然后向服务端发起连接请求,从而建立数据连接.因此,服务器端只是被动地监听在指定端口上的请求,所以称之为被动模式. 被动模式的控制连接和数据连接都是由FTP客户端发起的

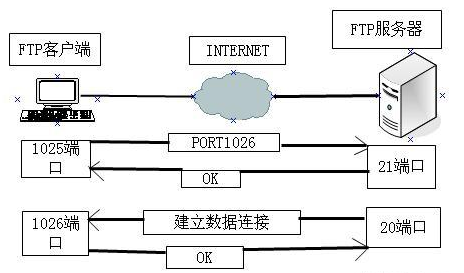
首先FTP客户端随机开启一个大于1024的端口X向服务器的21端口发起连 接,同时会开启X+1端口.然后向服务器发送PASV命令,通知服务器自己处于被动模式.服务器收到命令后,会开放一个端口Y(20)进行监听,然后用 PORT Y命令通知客户端,自己的数据端口是Y.客户端收到命令后,会通过X+1号端口连接服务器的端口Y,然后在两个端口之间进行数据传输.这样就能使防火墙知 道用于数据连接的端口号,而使数据连接得以建立.如图 4‑2 ftp被动模式工作过程所示.

图 4‑2 ftp被动模式工作过程

## 比较几种架构FTP服务器的软件、说明它们的优缺点

### net2ftp

net2ftp是一个开源,基于Web的FTP客户端.它可以连到任意服务器,浏览文件,上传/下载/复制/移动/删除/重命名文件,查看文件内容带语法高亮显示.net2ftp还可以将文件复制/移动到其它FTP服务器上或对文件进行Zip/Unzip.

特色：

1.带ZIP 打包解压缩,WIN主机下很正常,打包的文件可以用EMAIL发出.

2.编辑、删除、上传、下载

3.unix下修改文件权限

### Wing FTP Server

Wing FTP Server 是一个专业的跨平台FTP服务器端,它拥有不错的速度、可靠性和一个友好的配置界面.它 除了能提供FTP的基本服务功能以外,还能提供管理员终端、任务计划、基于Web的管理端,基于Web的客户端和Lua脚本扩展等,它还支持虚拟文件夹、 上传下载比率分配、磁盘容量分配,ODBC/Mysql存储账户等特性,支持 Windows, Linux, Mac OS和Solaris.

### Apache FtpServer

FTP 是FileTransfer Protocol（文件传输协议）的英文简称,而中文简称为“文传协议”.用于Internet上的控制文件的双向传输.同时,它也是一个应用程序 （Application）.基于不同的操作系统有不同的FTP应用程序,而所有这些应用程序都遵守同一种协议以传输文件.在FTP的使用当中,用户经常 遇到两个概念："下载"（Download）和"上传"（Upload）."下载"文件就是从远程主机拷贝文件至自己的计算机上；"上传"文件就是将文件 从自己的计算机中拷贝至远程主机上.用Internet语言来说,用户可通过客户机程序向（从）远程主机上传（下载）文件.

Apache Ftp Server 是 100% 纯 Java 的 FTP 服务器软件,它采用 MINA 网络框架开发,具有非常好的性能.Apache FtpServer 既可以嵌到 Java 应用中使用,也可以做为 Windows 服务或 Unix/Linux Daemon 单独运行.此外还提供与 Spring 相集成的模块.

### SwiFTP

SwiFTP 是一个Android手机平台上的FTP服务器软件,重点在简单易用、体积小.SwiFTP 默认运行在 2121 端口,也可以配置到其他端口上.SwiFTP 屏幕上将显示 wifi 的 IP 地址.支持任何一个 FTP 客户端软件.swiftp是一个开源的ftp server .

1. 源码default.java中

public static final boolean release = true;//可以改成false打开log的开关,方便调试.

2. 遇到“550 Invalid name or chroot violation”（可以从源码中找到打这个log的代码行）的错误,那一定是配置页面中sd卡的路径不正确.

## 选取一种软件进行FTP服务器的配置,说明过程

下面给出win sever 2008上ftp的服务器配置过程.

#### 1.安装ftp服务器.如图 4‑3 安装ftp服务器所示.

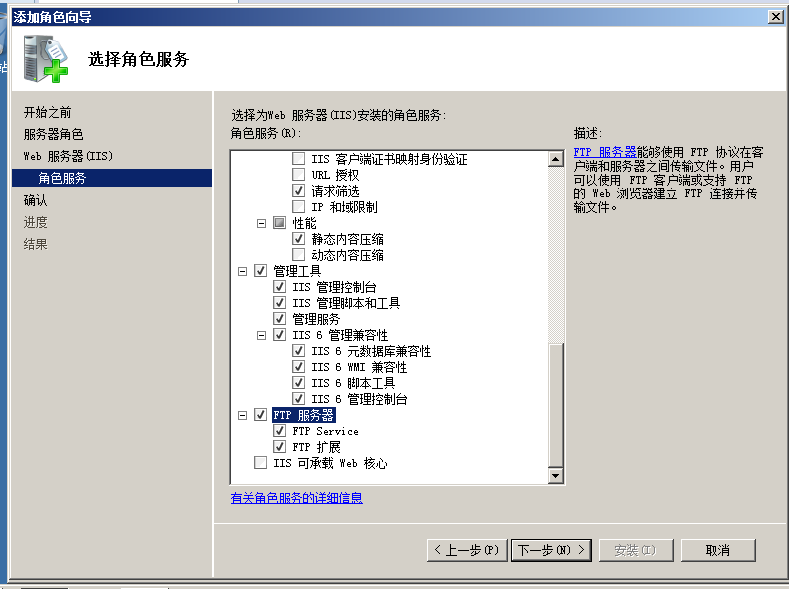


图 4‑3 安装ftp服务器

#### 2.设置共享文件夹.如图 4‑4 设置共享文件夹所示.

图 4‑4 设置共享文件夹

#### 3.添加ftp站点.如图 4‑5 添加ftp站点所示.

图 4‑5 添加ftp站点

#### 4.绑定和SSL设置.如图 4‑6 绑定和SSL设置所示.

图 4‑6 绑定和SSL设置

## 针对FTP服务器的安全问题提出解决方法

### ftp服务器存在的安全问题

虽然FTP是目前应用最广的Internet功能之一,但也是安全最弱的服务.FTP最大的安全漏洞在于其默认传输密码的过程是明文传送,很容易被人嗅探到.而ⅡS又是基于Windows用户账户进行管理的,因而很容易泄漏系统账户名及密码,如果该账户拥有一定管理权限,则更会影响到整个系统的安全.

FTP的全称是File Transfer Protocol（文件传输协议）.协议的任务是从一台计算机将文件传送到另一台计算机,它与这两台计算机所处的位置、联系的方式、以及使用的操作系统无关.在用户的本地计算机（FTP客户）与网络上的一台远程计算机（FTP服务器）建立了FTP连接后,就可以进行文件传输了.高效和安全的传输文件和信息是网络中心需要解决的一个实际问题.公开和毫无防范地使用FTP被视为安全政策范围内的信息透露,那是因为FTP原模式中不包含安全维护.使用FTP与服务器建立连接时,客户必须提供ID和密码.但是这种安全信息被直接用明码电文传输.因此,FTP存在很多安全问题与漏洞.为了防止恶意的,如 THEBOUNCE攻击、口令强迫破解攻击、端口偷窃等对FTP服务器进行破坏以至关键性数据被窃听.

FTP被广泛应用,自建立后其主框架相当稳定,二十多年没有什么变化,但是在Internet迅猛发展的形势下,其安全问题还是日益突出出来.现行研究的很多安全功能扩展和对协议中安全问题的防范也正是近年来人们不懈努力的结果,而且在一定程度上缓解了FTP的安全漏洞问题.FTP服务同数字授权、数字验证、数字签名结合访问控制机制结合和动态口令技术的建立以及完善了用户口令机制,使FTP服务的安全大大提高,可以解决大部分已知FTP漏洞攻击和基于TCP方法的攻击威胁.

### 增强ftp服务器安全性

#### 1．窗体身份验证

窗体身份验证即是当用户请求一个安全页面时,系统要对其进行判断,如果该用户已经登录系统并尚未超时,系统将返回此页面给请求用户; 反之如该用户尚未登录,系统就要将此用户重定向到登录页面.

#### 2．输入有效性验证

输入有效性验证即是对所有用户输入的字符范围进行限制,以防可用于向Web站点发送恶意脚本的字符被禁止使用.

#### 3．使用参数化存储过程

使用参数化存储过程是指在Web应用中,尽可能将对数据库的操作使用存储过程来完成,而不是动态构造SQL语句.

#### 4．输出数据HTML编码

输出数据HTML编码是指在将任何数据返回给用户前均应采用HTML编码,以防止跨站点的脚本攻击.因为攻击者一旦破坏了数据库,便可向记录中输入脚本,此脚本随后被返回给用户并在浏览器中执行.通过HTML编码,可将大多数脚本命令自动转换为无害文本.

#### 5.信息加密存储

信息加密存储是指对如数据库连接字符串、用户秘密等敏感信息进行加密存储,以妥善保护数据.

#### 6. 取消匿名访问功能

有些,ftp服务器默认允许匿名访问的,虽然匿名访问为用户上传和下载文件提供方便,但却存在极大的安全隐患,因此需要取消匿名访问功能方法是在Windows中,单击“开始——程序——管理工具——Internet服务管理器”打开管理控制台窗口,右键单击F作站点,并且在弹出菜单中选择“属性”命令,接着在FTP站点性窗口中进入“安全账号”选项卡,取消选中“允许匿名连接”复选框即可.

#### 7.正确设置用户访问权限

每个Ftp用户账号都具有一定的访问权限,但对用户权限的不合理设.置,能导致FTP服务器出现安全隐患.系统默认设置是允许其他用户对test文件夹有修改和读取的权限,因此必须重新设置该文件夹的用户访问

权限. 在资源管理器中右键单击test文件夹,在弹出菜单中选择“属性”命令,接着进入“安全”选项卡,首先删除Everyone用户账号,接着单击“添加”,按钮,将tester账号加到名称列表框中,然后在“权限”列表框中选中修改、读取及运行、列出文件夹目录、读

取和写入选项,最后单击“确定”按钮确保该文件夹只有tester用户才能访问.

#### 8.启用磁盘配额

无限制地让用户使用FTP服务器磁盘空间势必造成巨大的浪费,因此要对每位FTP用户使用的磁盘空间进行限制. 在资源管理器窗口中,右键单击test文件夹所在的硬盘盘符,在弹出的菜单中选择“属性”命令. 接着切换到“配额”选项卡,选中“启用配额管理”复选框,激活“配额”选项卡中的所有配额设置选项,为了不让某些FTP用户占用过多的服务器磁盘空间,一定要选中“拒绝将磁盘空间给超过配额限制的用户”复选框. 在“为该卷上的新用户选择默认配额限制”选项组中选择“将磁盘空间限制为”单选按钮,接着在后面的文本框中输入120,磁盘容量单位选择为“MB”.然后进行警告等级设置,在“将警告等级设为”文本框中输入“l00”,容量单位也选择为“MB.’,这样就完成了默认配额设置. 单击“配额项”按钮,打开磁盘配额项目对话框,接着单击“配额——新建

“配额项”弹出选择用户对话框,选中tester用户后单击“确定”按钮.接着在“添加新配额项”对话框中为tester用户设置配额参数,选择“将磁盘空间

限制为”一项,在后面的文本框中输入“120”,接着在“将警告等级设置为”文本框中输入“l00”,它们的磁盘容量单

位为“MB”,最后单击“确定”按钮,完成磁盘配额设置,这样tester用户就只能使用120mb磁盘空间.超过100MB就会发出警告.

#### 9.账号登录限制

有些非法用户使用黑客工具,反复登录FTP服务器猜测账号密码,这对于FTP服务器的性能有很大影响,因此需要对账号登录次数进行限制. 依次展开“安全设置——账尸策略——账户锁定策略”,在右侧框体中找到“账户锁定阙值”项,双击打开后,设置账号登录的最大次数,如果超过此数值,账号会被自动锁定.接着打开“账户锁定时间”项,设置FTP账号被锁定的时间,账号一旦被锁定,超过这个时间值才能重新使用.这样F开服务器就会更加安全

# 网络存储

## 介绍网络存储原理

SAN（Storage Area Network）存储区域网络,是一种高速的、专门用于存储操作的网络,通常独立于计算机局域网（LAN）.SAN将主机和存储设备连接在一起,能够为其上的任意一台主机和任意一台存储设备提供专用的通信通道.SAN将存储设备从服务器中独立出来,实现了服务器层次上的存储资源共享.SAN将通道技术和网络技术引入存储环境中,提供了一种新型的网络存储解决方案,能够同时满足吞吐率、可用性、可靠性、可扩展性和可管理性等方面的要求.

## 比较几种网络存储方案、说明它们的优缺点

### FC-SAN

#### 1. FC-SAN的组成

在FC-SAN中,有一些专用的硬件和软件.硬件包括FC卡、FC HUB、FC交换机、存储系统等,软件主要是FC控制卡针对各种操作系统的驱动程序和存储管理软件. FC卡：主要用于主机与FC设备之间的连接. FC HUB：内部运行仲裁环拓扑,连接到HUB的节点共享100MB/S带宽（或

更高）. FC交换机：内部运行Fabric拓扑,每端口独占100MB/S带宽（或更高）.FC存储设备：采用FC连接方式,光纤接口可以有一到多个.FC存储设备通常采用光纤的硬盘,也有Fibre to SCSI（Fibre to ATA）的解决方案,使用SCSI（或ATA）的硬盘,在整个配置上较便宜. 存储网络管理软件：存储管理软件主要的功能是自动发现网络拓扑及映射,当在存储网络中增加或减少时自动发现及组态.高性能的光纤通道交换机和光纤通道网络协议是FC-SAN的关键.把以光纤通道交换机为骨干的网络拓扑结构称为“SAN Fabric”.而光纤通道协议是FC-SAN的另一个本质特征.FC-SAN正是利用光纤通道协议上加载SCSI协议来达到可靠的块级数据传输.

#### 2. FC-SAN的应用场合

由于FC-SAN是为在服务器和存储设备之间传输大块数据而进行优化的,因此对于以下应用来说是理想的选择： 关键任务数据库应用,其中可预计的响应时间、可用性和可扩展性是基本要素. 集中的存储备份,其中性能、数据一致性和可靠性可以确保企业关键数据的安全.高可用性和故障切换环境可以确保更低的成本、更高的应用水平.可扩展的存储虚拟化,可使存储与直接主机连接相分离,并确保动态存储分区. 改进的灾难容错特性,在主机服务器及其连接设备之间提供光纤通道高性能和扩展的距离.

#### 3. FC-SAN的主要好处：

面对迅速增长的数据存储需求,企业和服务提供商渐渐开始选择FC-SAN作为网络基础设施,因为SAN具有出色的可扩展性.事实上,SAN比传统的存储架构具有更多显著的优势.例如,传统的服务器连接存储通常难于更新或集中管理.每台服务器必须关闭才能增加和配置新的存储.相比较而言,FC-SAN不

必宕机和中断与服务器的连接即可增加存储.FC-SAN还可以集中管理数据,从而降低了总体拥有成本.

利用光纤通道技术,FC-SAN可以有效地传输数据块.通过支持在存储和服务器之间传输海量数据块,SAN提供了数据备份的有效方式.因此,传统上用于数据备份的网络带宽可以节约下来用于其他应用.

开放的、业界标准的光纤通道技术还使得FC-SAN非常灵活.FC-SAN克服了传统上与SCSI相连的线缆限制,极大地拓展了服务器和存储之间的距离,从而增加了更多连接的可能性.改进的扩展性还简化了服务器的部署和升级,保护了原有硬件设备的投资.

此外,FC-SAN可以更好地控制存储网络环境,适合那些基于交易的系统在性能和可用性方面的需求.SAN利用高可靠和高性能的光纤通道协议来满足这种需要.

FC-SAN的另一个长处是传送数据块到企业级数据密集型应用的能力.在数据传送过程中,FC-SAN在通信结点（尤其是服务器）上的处理费用开销更少,因为数据在传送时被分成更小的数据块.因此,光纤通道FC-SAN在传送大数据块时非常有效,这使得光纤通道协议非常适用于存储密集型环境.

### IP-SAN

IP-SAN（IP存储）的通信通道是使用IP通道,而不是光纤通道,把服务器与存储设备连接起来的技术,除了标准已获通过的iSCSI,还有FCIP、iFCP等正在制定的标准.而iSCSI发展最快,已经成了IP存储一个有力的代表.

像光纤通道一样,IP存储是可交换的,但是与光纤通道不一样的是,IP网络是成熟的,不存在互操作性问题,而光纤通道SAN最令人头痛的就是这个问题.IP已经被IT业界广泛认可,有非常多的网络管理软件和服务产品可供使用.

IP存储的标准： IP存储除了标准已获通过的iSCSI,还有iFCP、FCIP等正在制定的标准.

IP存储的优势： 利用无所不在的IP网络,一定程度上保护了现有投资. IP存储超越了地理距离的限制.IP能延伸到多远,存储就能延伸到多远,这几乎是一个划时代的革命,十分适合于对现存关键数据的远程备份. IP网络技术成熟.IP存储减少了配置、维护、管理的复杂度.

## 网络存储的安全问题

Internet的迅速发展在提高了工作效率的同时,也带来了一个日益严峻的问题——网络数据存储安全,网络数据存储安全成为当今研究热点和社会关注焦点.面对一个越来越开放的网络环境,高效安全的信息存储与传输已经成为网络经济发展必不可少的特性.由于黑客入侵、内部人员泄密、管理员权限的滥用等原因,很容易发生文件或资料丢失泄漏,由此造成的重大后果将是无法弥补的,传统的研究方法和解决方案通常是对单一的安全技术进行改进优化或对多个安全措施的简单组合；只有综合运用各种安全措施,使之相互协调工作,从而构建一个全方位的纵深安全防御系统,才能有效提高网络数据存储安全.网络数据存储安全作为一个无法回避的问题呈现在我们面前,通过安全存储技术的应用,在相当程度上能够有效地防止此类事件的发生,避免由于资料泄漏所造成的严重损失.开放式环境下的安全存储技术研究旨在面向开放式的网络环境,利用加密技术、身份鉴别与认证技术、访问控制技术提供安全的存储与传输能力,获取强大的信息安全保证.

存储安全是指保证存储资源只被授权用户或可信网络所访问的一组安全措施、安全配置和安全控制.电子商务正在改变传统的业务模型,因为它以网络为中心,面向全球而且数据强化.数据强化一词说明了所有的电子事物都可以存储以供处理和分析这一个事物.目前,我们正面临着由电子商务应用所生成的数据爆炸,这些数据必须得到适当的存储和管理,而且有时还需要使用数据挖掘应用程序从原始数据中提取信息；企业资源计划（ERP）,数据挖掘和决策支持应用也推动了对网络存储安全的需求,因为其中涉及的数据必须从异构环境中存取和拷贝.

网络存储的安全可以采取如下措施：

#### 1. 加密与数字签名

任何良好的安全系统必须包括加密！这已成为既定的事实.网络上的加密可以分为三层：第一层为数据链路层加密,即将数据在线路传输前后分别对其进行加密和解密,这样可以减少在传输线路上被窃取的危险；第二层是传输层的加密,使数据在网络传输期间保持加密状态；第三层是应用层上的加密,让网络应用程序对数据进行加密和解密.当然可以对这三层进行综合加密,以增强信息的安全性和可靠性.

数字签名是数据的接收者用来证实数据的发送者确实无误的一种方法,它主要通过加密算法和证实协议而实现.

#### 2. 防火墙

防火墙（Firewall）是Internet上广泛应用的一种安全措施,它可以设置在不同网络或网络安全域之间的一系列部件的组合.它能通过监测、限制、更改跨越防火墙的数据流,尽可能地检测网络内外信息、结构和运行状况,以此来实现网络的安全保护.

#### 3. User Name/Password认证

该种认证方式是最常用的一种认证方式,用于操作系统登录、telnet（远程登录）、rlogin（远程登录）等,但此种认证方式过程不加密,即password容易被监听和解密.

#### 4. 使用摘要算法的认证

Radius（远程拨号认证协议）、OSPF（开放路由协议）、SNMP Security Protocol等均使用共享的Security Key（密钥）,加上摘要算法（MD5）进行认证,但摘要算法是一个不可逆的过程,因此,在认证过程中,由摘要信息不能计算出共享的security key,所以敏感信息不能在网络上传输.市场上主要采用的摘要算法主要有MD5和SHA-1.

#### 5. 基于PKI的认证

使用PKI（公开密钥体系）进行认证和加密.该种方法安全程度较高,综合采用了摘要算法、不对称加密、对称加密、数字签名等技术,很好地将安全性和高效性结合起来.这种认证方法目前应用在电子邮件、应用服务器访问、客户认证、防火墙认证等领域.该种认证方法安全程度很高,但是涉及到比较繁重的证书管理任务.

# 总结

经过一段时间的努力,完成了本次论文. 这次的论文中涉及到了很多的内容, 在论文的写作过程中遇到了许多的困难和障碍.但是都一一克服了,其中有老师与同学的帮助,也有自己查询资料慢慢解决的.我觉得自己的知识还是有欠缺.希望能在以后的学习中加强.随着时代的发展,网络服务器显得越来重要,本文以配置网络服务器为主,系统的介绍了DNS服务器;DHCP服务器;FTP服务器;网络存储,的原理及工作过程,以及在Windows Server 2008下常用的服务器配置,还对常用的服务器软件进行了对比和优缺点的说明.

域名系统（DNS）服务在Internet服务中占据着重要的地位.本文介绍了DNS服务面临的安全问题,讨论了dns安全加固策略.服务器的安全问题及解决方法. 本文档针对dhcp安全加固策略,从网络安全风险、安全架构和安全加固策略等方面指导加强网络安全和设备安全.

由于DHCP 协议在设计时未考虑安全的因素,在使用DHCP 服务器为网络地址和参数的网络中面临着很多DHCP 威胁,所以对DHCP 安全性的研究具有重大意义.本人即围绕DHCP 网络协议的安全性问题展开集中讨论研究,包括归纳DHCP 网络安全的主要威胁、提出了消除威胁的策略建议、用对比的方式挖掘减少威胁的方法以及安全实现.

在ftp上传与下载的过程中许多地方都存在着安全隐患,随着互联网和普及了深入,网络安全也越来越被人们重视,在这里我把一些常见的关于FTP的安全隐患提出来,希望引起人们对FTP安全的重视,使FTP服务器和数据传输过程更加安全.

近年来,信息技术发展迅速,网络已逐渐成为人们存储各种信息的重要空间,现代化军队建设中更加离不开网络.但是,在网络技术高速发展的同时,网络数据存储的安全和传输过程中出现的问题也越来越多,并且越来越严重.本文通过对网络数据存储的安全和传输问题进行剖析,提出了相应的解决策略.

基于之前的实践,我能够很好地将这次的论文完成.在老师的指导下,我对实验和论文有了一定地准备.在老师和同学的热心帮助下,实验顺利地进行,并成功地完成了论文内容.通过本次论文,我很好地利用了所学的理论知识,从而在实践和理论学习两方面都增长了见识和知识.

# 参考文献

1. 潘凯华, 邹天思.明日科技. Windows Server 2008大全[M]. 北京:人民邮电出版社,2014. 255-256.
2. 兰旭辉 熊家军 邓刚.设计动态网站的最佳方案:Apache+PHP+MySQL[M]. 计算机工程与设计2017 28(4):36-45.
3. 陈湘扬, 陈国益.Windows Server 2008. [M] 计算机工程与设计2016. 25(3):128-236.
4. 邹天思, 孙鹏. 网络储存系统开发设计[M]. 北京:电子工业出版社,2017.99-155.
5. (美)戴尔.Windows Server 2008权威指南[M]. 北京:人民邮电出版社,2016.49-68.
6. 王坤.ftp核心技术手册[M]. 机械工业,2014-09-01.北京智恒联盟科技有限公司. 2015:208-256.
7. 张翼.WEB网站系统安全全面解决方案[M]. 2016中国计算机信息防护年会论文集, 2006:147-189.
8. 李峰, 晁阳.Web环境下数据库系统安全访问控制机制研究[M]. 2014:168-180.
9. 屠立,俞剑琳,宋伟文. dhcp开发技术详解[M]. 北京:清华大学出版社,2016:196-239.
10. 玉利 赵丽艳.基于Web的企业管理信息系统安全方案的设计. 轻工机械2015:283-286.