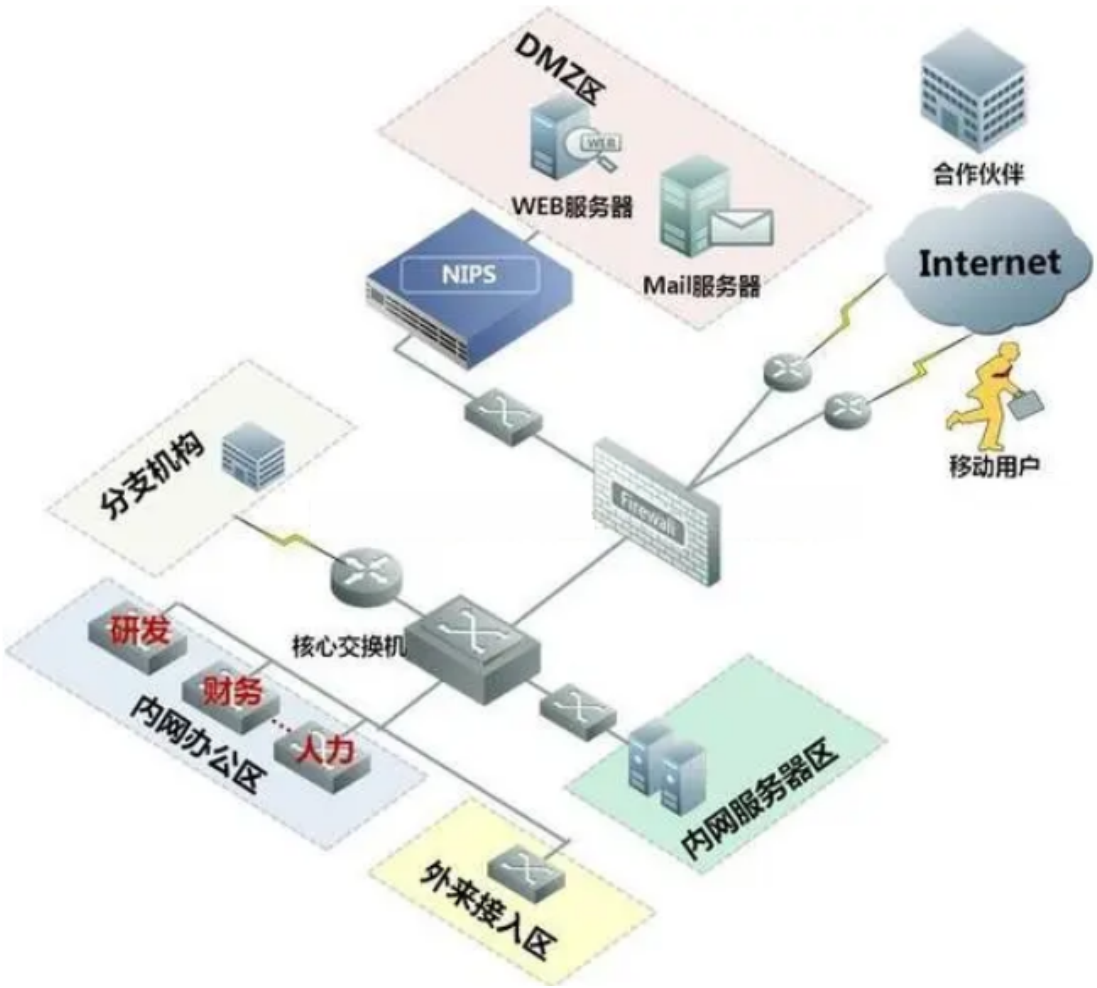
内网基础知识

内网也指局域网，是指在某一区域内由多台计算机互连而成的计算机组,组网范围通常在数千米以内。在局域网中,可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等。内网是封闭的,可以由办公室内的两台计算机组成,也可以由一个公司内的大量计算机组成

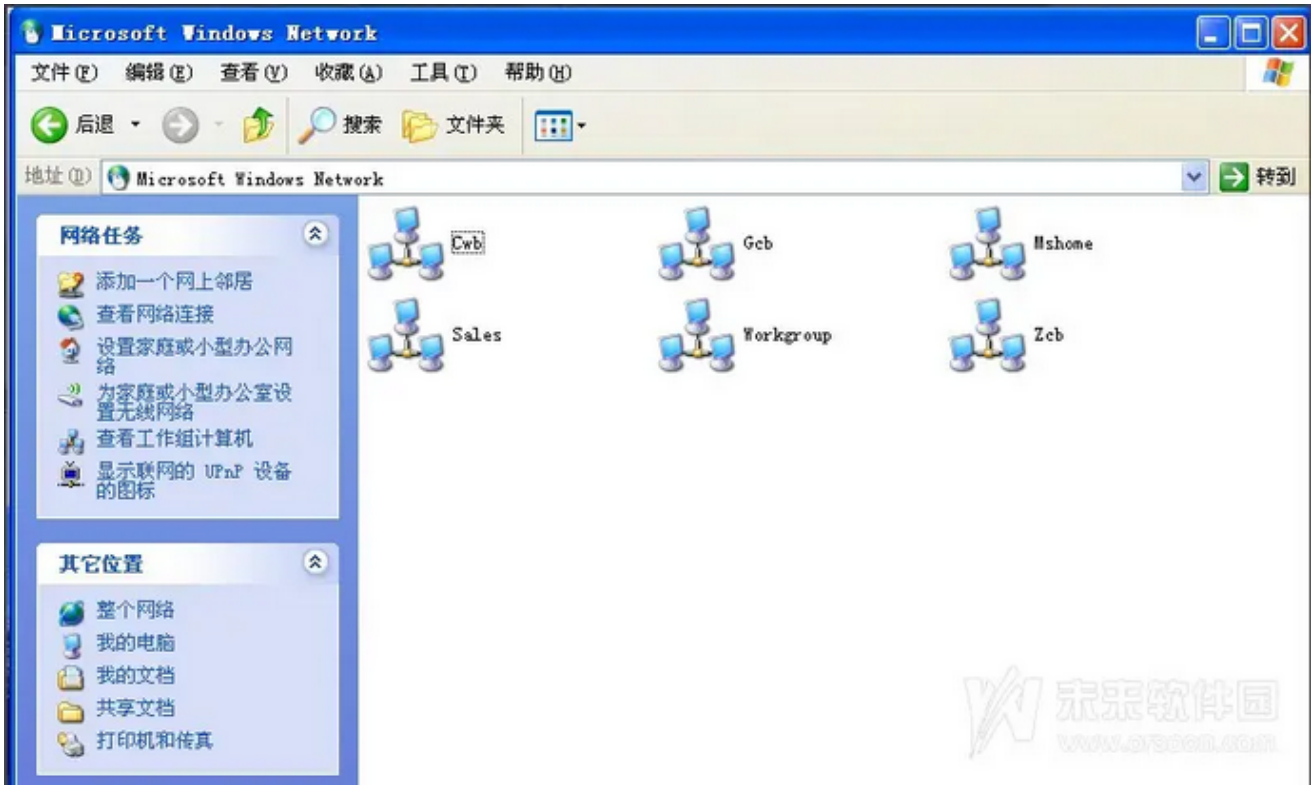


工作组介绍

1、工作组的介绍

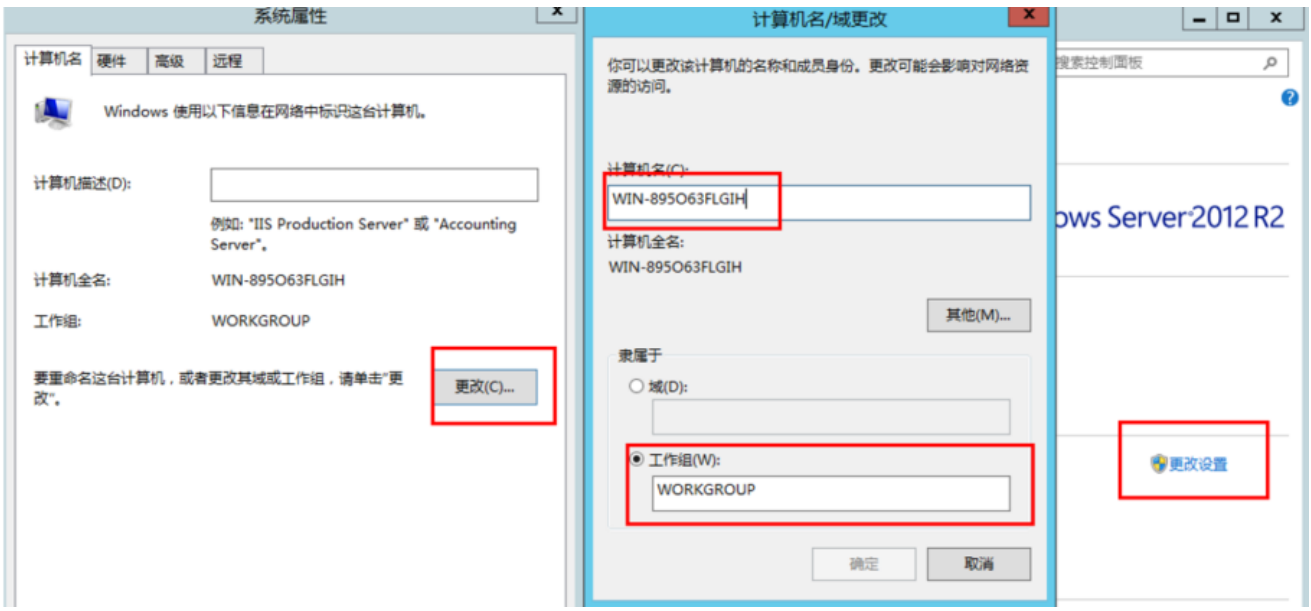
在一个大型单位里,可能有成百上千台计算机互相连接组成局域网,它们都会列在"网络"(网上邻居)内。如果不对这些计算机进行分组,网络的混乱程度是可想而知的 为了解决这一问题,产生了工作组(Work Group)这个概念。将不同的计算机按功能(或部 门)分别列入不同的工作组,例如技术部的计算机都列入"技术部"工作组、行政部的计算机都 列入"行政部"工作组。要想访问某个部门的资源,只要在"网络"里双击该部门的工作组名 就可以看到该部门的所有计算机了。相比不分组的情况,这样的情况有序得多(尤其对大型局域 网来说)。

工作组如图



2、如何加入工作组和创建工作组

加入工作组:加入工作组的方法很简单。右击桌面上的"计算机"图标,在弹出的快捷菜单中选择"属 性"选项,然后依次单击"更改设置"和"更改"按钮,在"计算机名"输入框中输入计算机的 名称,在"工作组"输入框中输入想要加入的工作组的名称



创建工作组:如果输入的工作组的名称在网络中不存在,就相当于新建了一个工作组(当然,暂时只有当 前这台计算机在该工作组内)。单击"确定"按钮, Windows会提示需要重新启动。在重新启动 之后进入"网络",就可以看到所加入的工作组的成员了。当然,也可以退出工作组(只要修改工 作组的名称即可)

这时在网络中,别人可以访问我们的共享资源,我们也可以加入同一网络中的任何工作组 工作组就像一个可以自由进入和退出的社团,方便同组的计算机互相访问。工作组没有集中管理 作用,工作组里的所有计算机都是对等的(没有服务器和客户机之分)

域介绍

Windows域是计算机网络的一种形式，其中所有用户帐户 ，计算机，打印机和其他安全主体都在位于称为域控制器的一个或多个中央计算机集群上的中央数据库中注册。 身份验证在域控制器上进行。 在域中使用计算机的每个人都会收到一个唯一的用户帐户，然后可以为该帐户分配对该域内资源的访问权限。

假如有一个以下的场景：

一个公司有200台计算机,我们希望某台计算机的账户Aan可以访每台计算机的资源或者在每台计算机上登录。那么,在工作组环境中,我们必须在这200台计算机各自的SAM数据库中创建Aan这个账户。一旦Alan想要更换密码,必须进行200次更改 密码的操作!这个场景中只有200台计算机,如果有5000计算机或者上万台计算机呢?这就是一个典型的域环境应用场景

域 (Domain)是一个有安全边界的计算机集合(安全边界的意思是,在两个域中,一个域中 的用户无法访问另一个域中的资源)可以简单地把域理解成升级版的工作组。与工作组相比,域 的安全管理控制机制更加严格。用户要想访问域内的资源,必须以合法的身份登录域,而用户对域内的资源拥有什么样的权限,还取决于用户在域内的身份。

域控制器(Domain Controller,DC)是域中的一台类似管理服务器的计算机,我们可以形象 可以 地将它理解为一个单位的门禁系统。域控制器负责所有连入的计算机和用户的验证工作。域内的计算机如果想互相访问,都要经过域控制器的审核。

域控制器中存在由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当计算 机连接到域时,域控制器首先要鉴别这台计算机是否属于这个域,以及用户使用的登录账号是否 存在、密码是否正确。如果以上信息有一项不正确,域控制器就会拒绝这个用户通过这台计算机登录。如果用户不能登录,就不能访问服务器中的资源。

域控制器是整个域的通信枢纽,所有的权限身份验证都在域控制器上进行,也就是说,域内 所有用来验证身份的账号和密码散列值都保存在域控制器中

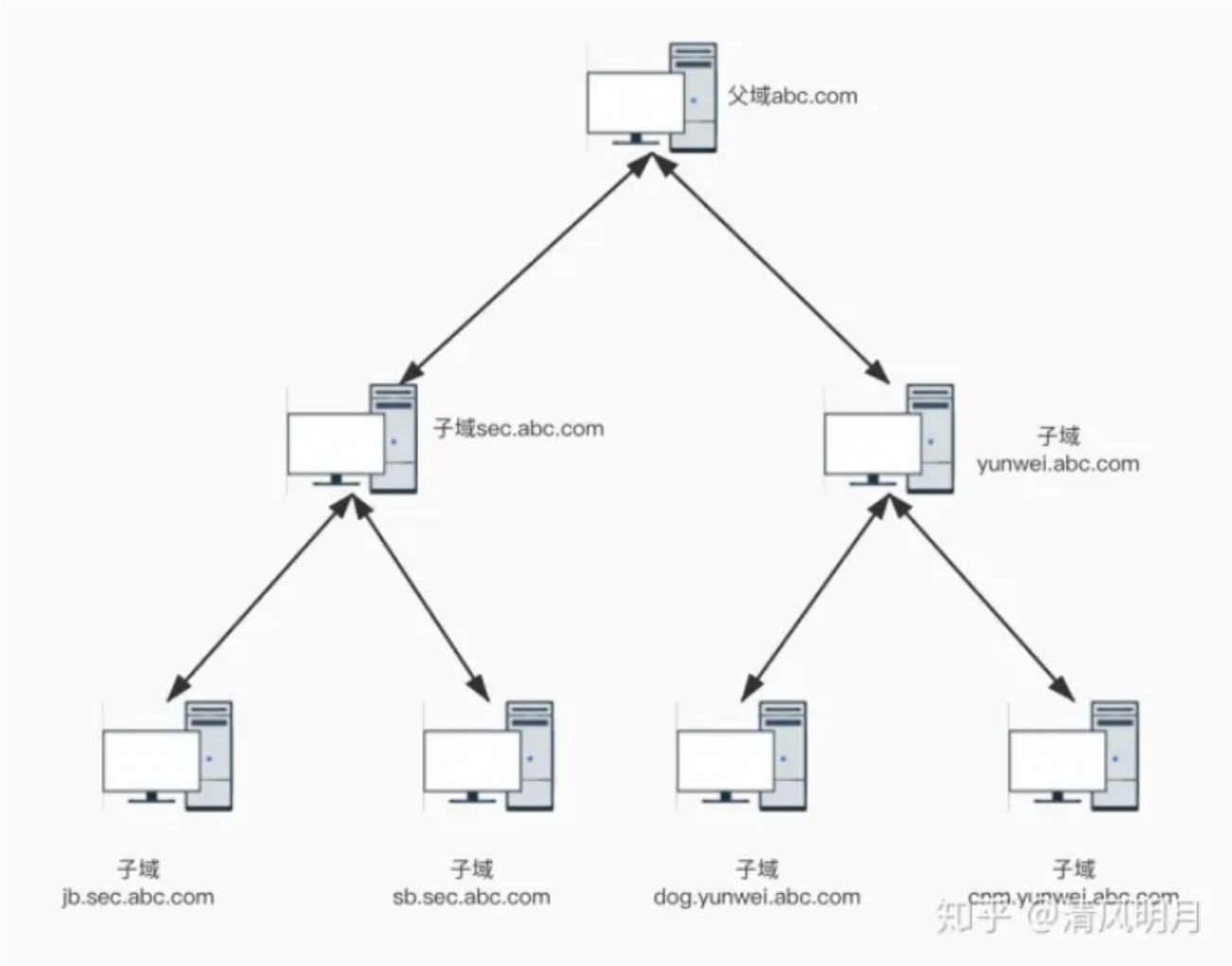
域中一般有如下几个环境：

1、单域

通常,在一个地理位置固定的小公司里,建立一个域就可以满足需求。在一个域内,一般要 有至少两台域服务器,一台作为DC,另一台作为备份DC。活动目录的数据库(包括用广的账号 信息)是存储在DC中的,如果没有备份DC,一旦DC瘫痪了,域内的其他用户就不能登录该域 了。如果有一台备份DC,至少该域还能正常使用(把瘫痪的DC恢复即可)

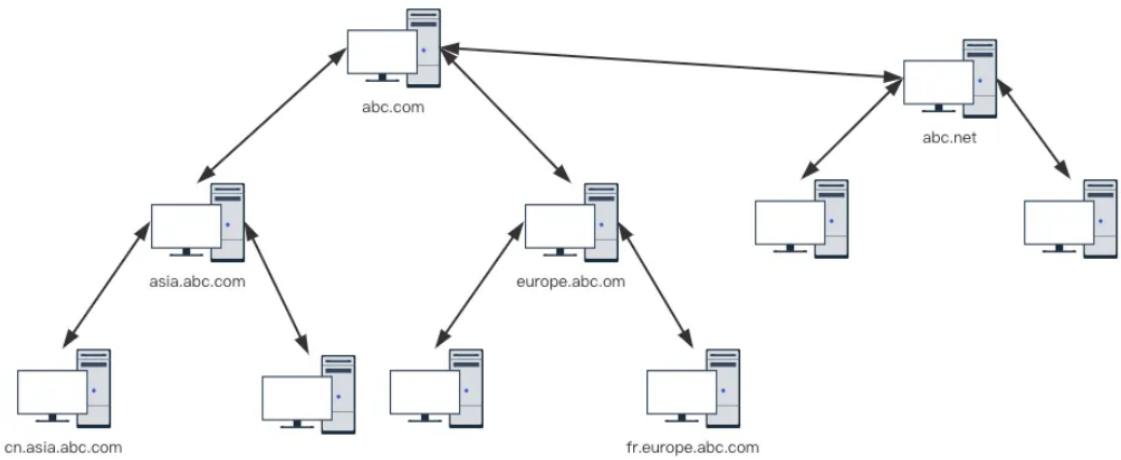
2、父域和子域

出于管理及其他需求,需要在网络中划分多个域。第一个域称为父域,各分部的域称为该域的子域。例如 大公司的各个分公司位于不同的地点,就需要使用父域及子域。如果把不同 地点的分公司放在同一个域内,那么它们之间在信息交互(包括同步、复制等)上花费的时间就 会比较长,占用的带宽也会比较大(在同一个域内,信息交互的条目是很多的,而且不会压缩; 在不同的域之间,信息交互的条日相对较少,而且可以压缩)。这样处理有一个好处,就是分公司 可以通过自己的域来管理自己的资源。还有一种情况是出于安全策略的考虑(每个域都有自己的 安全策略)例如,一个公司的财务部希望使用特定的安全策略(包括账号密码策略等)、那么可 以将财务部作为一个子域来单独管理 3、域树 域树(Tre)是多个域通过建立信任关系组成的集合。一个域管理员只能管理本域,不能访问 或者管理其他域。如果两个域之间需要互相访问,则需要建立信任关系(Trust Relation)信任关 系是连接不同域的桥梁。域树内的父域与子域,不但可以按照需要互相管理、还可以跨网络分配文 件和打印机等设备及资源,从而在不同的域之间实现网络资源的共享与管理、通信及数据传输。 在一个域树中,父域可以包含多个子域。子域是相对父域来说的,指的是域名中的每一个段。 各子域之间用点号隔开,一个"."代表一个层次。放在域名最后的子域称为最高级子域或一级 域,它前面的子域称为二级域。例如,域asia.abc.com的级别比域abc.com低(域asia.abc.com有 两个层次,而域abc.com只有一个层次)再如,域cn.asia.abc.com的级别比域asia.abc.com低 可以看出,子域只能使用父域的名字作为其域名的后缀,也就是说,在一个域树中,域的名字是连续的，如图



4、域森林

域森林(Forest)是指多个域树通过建立信任关系组成的集合。例如,在一个公司兼并场景中 某公司使用域树 abc. com,被兼并的公司本来有自己的域树 abc. net(或者在需要为被兼并公司建 立具有自己特色的域树时),域树abc.net无法挂在域树abc.com下。所以,域树abc.com与域树 abc. net之间需要通过建立信任关系来构成域森林。通过域树之间的信任关系,可以管理和使用整个域森林中的资源,并保留被兼并公司自身原有的特性,如图1-4所示。



5、域名服务器

域名服务器(Domain Name Server,DNs)是指用于实现域名(Domain Name)和与之相对的IP地址(IP Address)转换的服务器。从对域树的介绍中可以看出,域树中的域名和DNS域名非常相似。而实际上,因为域中的计算机是使用DNS来定位域控制器、服务器及其他计算机、网络服务的,所以域的名字就是DNS域的名字。在内网渗透测试中,大都是通过寻找DNS服务器 来确定域控制器的位置的(DNS服务器和域控制器通常配置在同一机器上)

活动目录介绍

活动目录(Active Directory,AD)是指域环境中提供目录服务的组件

目录用于存储有关网络对象(例如用户、组、计算机、共享资源、打印机和联系人等)的信息。目录服务是指帮助用户快速、准确地从目录中找到其所需要的信息的服务。活动目录实现了 目录服务,为企业提供了网络环境的集中式管理机制

如果将企业的内网看成一木字典,那么内网里的资源就是字典的内容,活动目录就相当于字典的索引。也就是说,活动目录存储的是网络中所有资源的快捷方式,用户可以通过寻找快捷方式来定位资源。

在活动目录中,管理员不需要考虑被管理对象的地理位置,只需要按照一定的方式将这些对象放置在不同的容器中。这种不考虑被管理对象的具体地理位置的组织框架称为逻辑结构

活动目录的逻辑结构包括前面讲过的组织单元(OU)、域、域树、域森林。域树内的所有域 共享一个活动目录,这个活动目录内的数据分散存储在各个域中,且每个域只存储该域内的数 据。例如,可以为甲公司的财务科、人事科、销售科各建一个域,因为这几个域同属甲公司,所 以可以将这几个域构成域树并交给甲公司管理;而甲公司、乙公司、丙公可都属于A集团,那 么,为了让A集团更好地管理这三家公司,可以将这三家公司的域树集中起米组成域森林(即A 集团)。因此,A集团可以按"A集团(域森林)→子公司(域树)→部门(域)→员工"的方式 对网络进行层次分明的管理。活动目录这种层次结构,可以使企业网络具有极强的可扩展性,便 于进行组织、管理及目录定位。

活动目录主要提供以下功能

> 账号集中管理:所有账号均存储在服务器中,以便执行命令和重置密码等。
> 软件集中管理:统一推送软件、安装网络打印机等。利用软件发布策略分发软件,可以让 用户自由选择需要安装的软件。
> 环境集中管理:统一客户端桌面、IE、TCPP协议等设置。 增强安全性:统一部署杀毒软件和病毒扫描任务、集中管理用户的计算机权限、统一制定用户密码策略等。可以监控网络,对资料进行统一管理。
> 更可靠,更短的宕机时间:例如,利用活动目录控制用户访问权限,利用群集、负载均衡等技术对文件服务器进行容灾设置。网络更可靠,宕机时间更短。
> 活动目录是微软提供的统一管理基础平台,ISA、 Exchange、SMS等都依赖这个平台

如果网络规模较大,就要把网络中的众多对象,例如计算机、用户、用户组、打印机、共享 文件等,分门别类、井然有序地放在一个大仓库中,并将检索信息整理好,以便查找、管理和使别 用这些对象(资源)这个拥有层次结构的数据库,就是活动目录数据库,简称AD库。

那么,我们应该把这个数据库放在哪台计算机上呢?要实现域环境,其实就是要安装AD。如 果内网中的一台计算机上安装了AD,它就变成了DC(用于存储活动目录数据库的计算机)回 顾之前的例子:在域环境中,只需要在活动目录中创建Aan账户一次,就可以在200台计 算机中的任意一台上使用该账户登录;如果要更改Aan账户的密码,只需要在活动目录中更改一次就可以了。

安全域的划分

划分安全域的目的是将一组安全等级相同的计算机划入同一个网段。这个网段内的计算机拥 有相同的网络边界,并在网络边界上通过部署防火墙来实现对其他安全域的网络访问控制策略 (NACL),从而对允许哪些P地址访问此域、允许此域访问哪些P地址和网段进行设置。这些 措施,将使得网络风险最小化,当攻击发生时,可以尽可能地将威胁隔离,从而降低对域内计算 机的影响。 一个典型的中小型内网的安全域划分,如图所示,一个虚线框表示一个安全域(也是网络的边界,一般分为DMZ和内网),通过硬件防火墙的不同端口实现隔离

在一个用路由器连接的内网中,可以将网络划分为三个区域:安全级别最高的内网;安全级 别中等的DMZ;安全级别最低的外网(Internet)。这三个区域负责完成不同的任务,因此需要设 置不同的访问策略。 DMZ称为隔离区,是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立 的一个非安全系统与安全系统之间的缓冲区。DMZ位于企业内部网络和外部网络之间。可以在 DMZ中放置一些必须公开的服务器设施,例如企业Web服务器、FTP服务器和论坛服务器等 DMZ是对外提供服务的区域,因此可以从外部访问

在网络边界上一般会部署防火墙及入侵检测、入侵防御产品等。如果有Web应用,还会设置 WAF,从而更加有效地保护内网。攻击者如果要进入内网,首先要突破的就是这重重防御

在配置一个拥有DMZ的网络时,通常需要定义如下访问控制策略,以实现其屏障功能。

> 内网可以访问外网:内网用户需要自由地访问外网。在这一策略中,防火墙需要执行NAT。
> 内网可以访问DMZ:此策略使内网用户可以使用或者管理DMZ中的服务器
> 外网不能访问内网:这是防火墙的基本策略。内网中存储的是公司内部数据,显然,这些数据一般是不允许外网用户访问的(如果要访问,就要通过PN的方式来进行)
> 外网可以访问DMZ:因为DMZ中的服务器需要为外界提供服务,所以外网必须可以访问DMZ。同时,需要由防火墙来完成从对外地址到服务器实际地址的转换。
> DMZ不能访问内网:如果不执行此策略,当攻击者攻陷DMZ时,内网将无法受到保护
> DMZ不能访问外网:此策略也有例外。例如,在DMZ中放置了邮件服务器,就要允许访问外网,否则邮件服务器无法正常工作。 内网又可以分为办公区和核心区。

办公区:公司员工日常的工作区,一般会安装防病毒软件、主机入侵检测产品等。办公区一般能够访问DMZ。如果运维人员也在办公区,那么部分主机也能访问核心数据区(很多企业还会使用堡垒机来统一管理用户的登录行为)攻击者如果想进入内网,一艘会使用鱼叉攻击、水坑攻击,当然还有社会工程学手段。办公区人员多而杂,变动也很频繁,在安全管理上可能存在诸多漏洞,是攻击者进人内网的重要途径之 核心区:存储企业最重要的数据、文档等信息资产,通过日志记录、安全审计等安全措施进行严密的保护,往往只有很少的主机能够访问。从外部是绝难直接访问核心区的。一般来说,能够直接访问核心区的只有运维人员或者I部门的主管,所以,攻击者会重点关注这些用户的信息(攻击者在内网中进行横向移动攻击时,会优先查找这些主机)

域中计算机的分类

域中计算机的分类在域结构的网络中,计算机的身份是不平等的,有域控制器、成员服务器、客户机、独立服务 器四种类型。

1、域控制器

域控制器用于管理所有的网络访问,包括登录服务器、访问共享目录和资源。域控制器中存 储了域内所有的账户和策略信息,包括安全策略、用户身份验证信息和账户信息。

在网络中,可以有多台计算机被配置为域控制器,以分拒用广的登录、访问等操作。多个域控制器可以一起工作,自动备份用户账尸和活动目录数据。这样,即使部分域控制器痪,网络访问也不会受到影响,提高了网络的安全性和稳定性

2、成员服务器

成员服务器是指安装了服务器操作系统并加入了域、但没有安装活动目录的计算机,其主要任务是提供网络资源。成员服务器的类型通常有文件服务器、应用服务器、数据库服务器、web服务器、邮件服务器、防火墙、远程访问服务器、打印服务器等

3、客户机

域中的计算机可以是安装了其他操作系统的计算机,用户利用这些计算机和域中的账户就可以登录域。这些计算机被称为域中的客户机。域用户账号通过域的安全验证后,即可访间网络中的各种资源。

4、独立服务器

独立服务器和域没有关系。如果服务器既不加入域,也不安装活动目录,就称其为独立服务器。独立服务器可以创建工作组、与网络屮的其他计算机共享资源,但不能使用活动目录提供的任何服务

域控制器用于冇放活动目录数据库,是域屮必须要有的,而其他三种计算机则不是必须要有的，也就是说,最简单的域可以只包含一台计算机,这台计算机就是该域的域控制器。当然,域中各服务器的角色是可以改变的。例如,独立服务器既可以成为域控制器,也可以加入某个域成为成员服务器