

# 搭建域环境

在学习内网渗透测试时,需要构建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,从而采取相应的防范措施。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。在本节中,将详细讲解如何在 Windows平台上搭建域环境

## 域环境介绍

通常所说的内网渗透测试,很大程度上就是域渗透测试。搭建域渗透测试环境,在 Windows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,对内网的安全维护有很大的帮助。常见的域环境是使用 Windows server2012R2、Windows7或者 Windows Server2003操作系统搭建的 Windows域环境。

在下面的实验中,将创建一个域环境。配置一台 WindowsServer2012R2服务器,将其升级为域控制器,然后将 Windows Server2008R2计算机和 Windows7、Windows Server2003计算机加入该域。四台机器

机器名称	机器IP
WindowsServer 2012 R2 ( 域控 )	192.168.41.10
WindowsServer 2008 R2 ( 域内主机 )	192.168.41.20
WindowsServer 2003 R2 ( 域内主机 )	192.168.41.30

## 搭建环境

### 1、设置服务器

在虚拟机中安装 Windowsserver2012R2操作系统,设置其P地址为192.168.41.10子网掩码为255252550,DNS指向本机IP地址。

## Internet 协议版本 4 (TCP/IPv4) 属性



### 常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址(O)

☒ 使用下面的 IP 地址(S):

IP 地址(I):

192 . 168 . 41 . 10

子网掩码(U):

255 . 255 . 255 . 0

默认网关(D):

192 . 168 . 41 . 2

☐ 自动获得 DNS 服务器地址(B)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P):

192 . 168 . 41 . 10

备用 DNS 服务器(A):

. . .

☐ 退出时验证设置(L)

高级(V)...

确定

取消

## 2、更改计算机名

使用本地管理员账户登录,将计算机名改为"DC"(可以随意取名),如图所示。在将本机升级为域控制器后,机器全名会自动变成"DC.xxx.com"。更改后,需要重启服务器

## 计算机名/域更改



你可以更改该计算机的名称和成员身份。更改可能会影响对网络资源的访问。

计算机名(C):

DC

计算机全名:

DC

其他(M)...

隶属于

☐ 域(D):

☒ 工作组(W):

WORKGROUP

确定

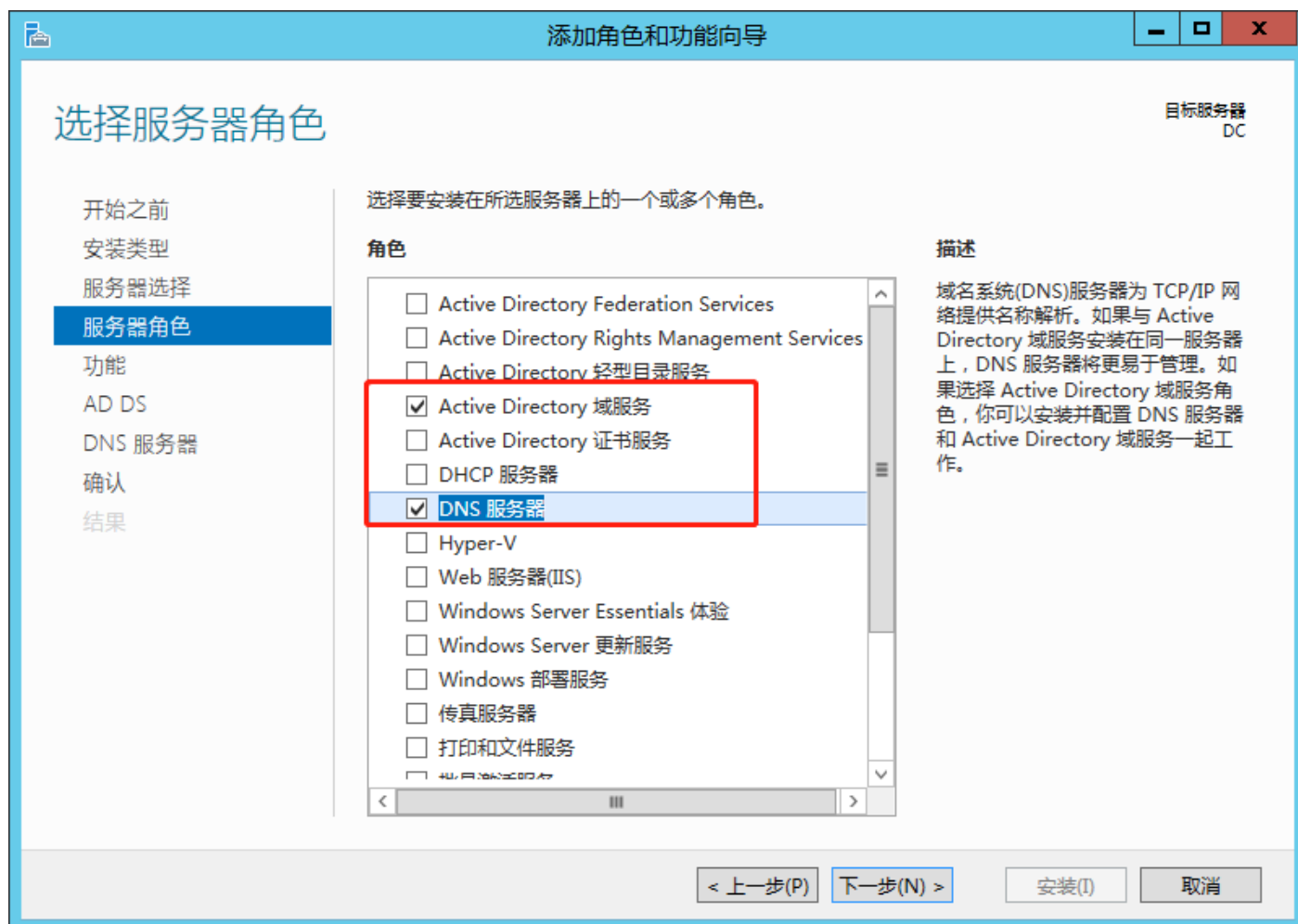
取消

### 3、安装域控制器和DNS服务

接下来,在 Windows server2012R2服务器上安装域控制器和DNS服务。登录 WindowsServer2012R2服务器,可以看到"服务器管理器"窗口,如图所示



单击【添加角色和功能】选项,进入添加角色和功能向导界面。在【开始之前】部分,本保持默认设置。单击下一步按钮,进入【安装类型】部分,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】部分。目前,在服务器池中只有当前这台机器,保持默认设置。单击下一步按钮,在【服务器角色】部分勾选【Active Directory域服务】和【DNS服务器】复选框



在"功能"界面保持默认设置,单击"下一步"按钮,进入"确认"部分。确认需要安装的组件,勾选"如果需要,自动重新启动目标服务器"复选框,然后单击"安装"按钮

## 4、升级服务器

安装 Active Directory域服务后,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,可以打开"服务器管理器"界面进行操作),在界面右上角可以看到一个中间有"!"的三角形按钮。单击该按钮,如图所示。



接着,进入 "ActiveDirectory域服务配置向导" 界面,在"部署配置"部分单击选中"添加新林(F)"单选按钮,然后输入根域名"hack.com"(必须使用合DNS命名约定的根域名)

Active Directory 域服务配置向导

部署配置

目标服务器  
DC

部署配置

域控制器选项

其他选项

路径

查看选项

先决条件检查

安装

结果

选择部署操作

☐ 将域控制器添加到现有域(D)

☐ 将新域添加到现有林(E)

☒ 添加新林(F)

指定此操作的域信息

根域名(R):

hack.com

[详细了解 部署配置](#)

< 上一步(P)

下一步(N) >

安装(I)

取消

在【域控制器选项】部分,将林功能级别、域功能级别都设置为" WindowsServer2012R2",创建域林时,在默认情况下应选择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)。然后,设置目录服务还原模式的密码(在开机 进入安全模式修复活动目录数据库时将使用此密码)



Active Directory 域服务配置向导

域控制器选项

部署配置  
域控制器选项  
DNS 选项  
其他选项  
路径  
查看选项  
先决条件检查  
安装  
结果

选择新林和根域的功能级别  
林功能级别:  
域功能级别:  
指定域控制器功能  
☒ 域名系统(DNS)服务器(O)  
☒ 全局编录(GC)(G)  
☐ 只读域控制器(RODC)(R)  
键入目录服务还原模式(DSRM)密码  
密码(D):  
确认密码(C):  
[详细了解 域控制器选项](#)

目标服务器  
DC

< 上一步(P)

下一步(N) >

安装(I)

取消

在【DNS选项】部分会出现关于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"部分。在"NetBIOS域名"(不支持DNS域名的旧版本操作系统,例如Windows98、NT,需要通过NetBIOS域名进行通信)部分保持默认设置。单击"下一步"按钮,进入"路径"部分,指定数据库、日志、SYSVOL文件夹的位置,其他选项保持默认设置。单击"下一步"按钮,保持默认设置。单击"下一步"按钮,最后单击"安装按钮。安装后,需要重新启动服务器,最后升级为域控

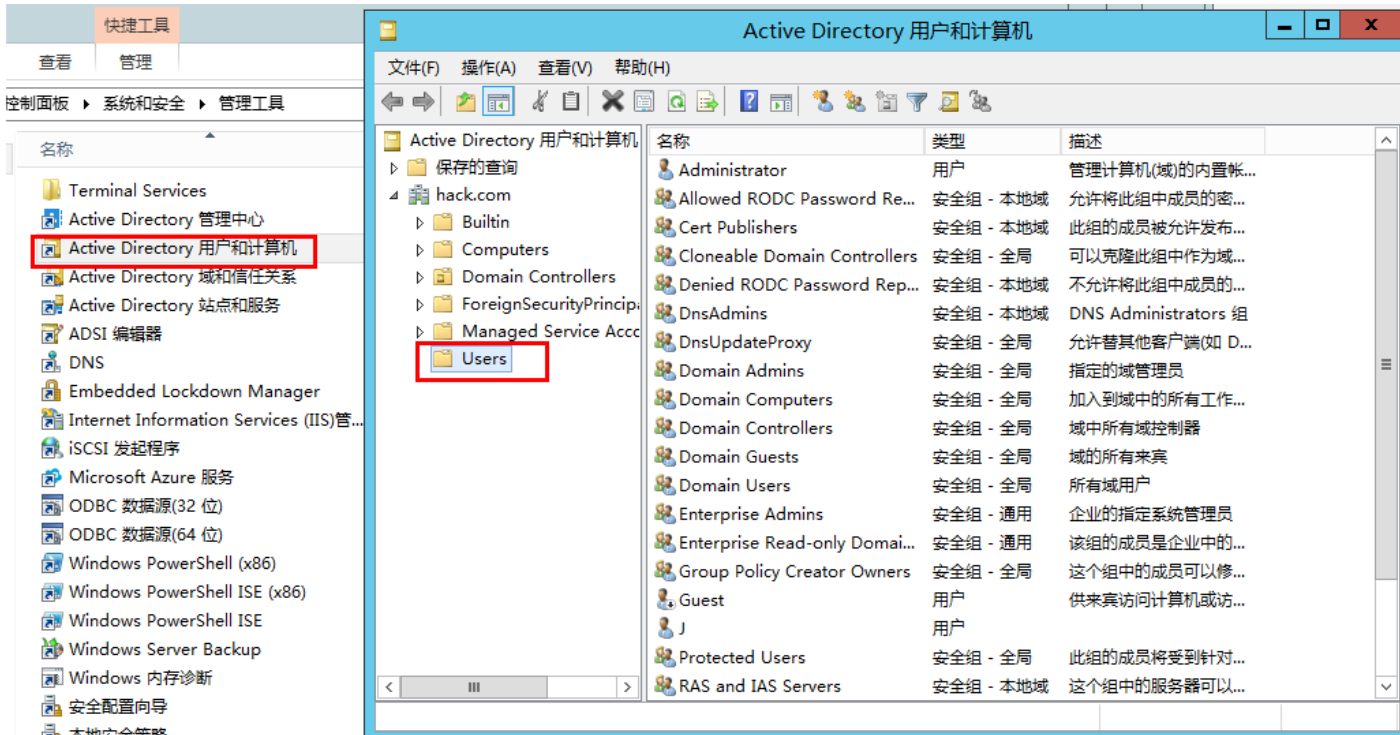


服务器重新启动后,需要使用域管理员账户( HACHE Administrator)登录。此时,在"服务器管理器"界面中就可以看到ADDS、DNS服务了



# 5、创建 Active Directory用户


为 Windows Server2008R2/2003和Windows7用户创建域控制器账户。如图1-26所示,在" Active Directory用户和计算机"界面中选择Users"目录并单击右键,使用弹出的快捷菜单添加用户。



创建用户

新建对象 - 用户

X



创建于:    hack.com/Users

---

姓(L):

名(F):

英文缩写(I):

姓名(A):

用户登录名(U):

@hack.com ▼

用户登录名(Windows 2000 以前版本)(W):

HACK\

---

< 上一步(B)

下一步(N) >

取消

## 将机器加入域

将Windows server 2008 计算机添加到该域中。如图所示,设置IP地址为192.168.41.20,设置DNS 地址为192.168.41.10,然后运行" ping hack.com"命令进行测试。

Internet 协议版本 4 (TCP/IPv4) 属性

?

×

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，您需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址 (O)

☒ 使用下面的 IP 地址 (S):

IP 地址 (I):

192 . 168 . 41 . 20

子网掩码 (U):

255 . 255 . 255 . 0

默认网关 (D):

192 . 168 . 41 . 10

☐ 自动获得 DNS 服务器地址 (B)

☒ 使用下面的 DNS 服务器地址 (E):

首选 DNS 服务器 (F):

192 . 168 . 41 . 10

备用 DNS 服务器 (A):

8 . 8 . 8 . 8

☐ 退出时验证设置 (L)

高级 (V)...

确定

取消

ping 域控

```
管理员: 命令提示符 - ping hack.com
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping hack.com

正在 Ping hack.com [192.168.41.10] 具有 32 字节的数据:
来自 192.168.41.10 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.41.10 的回复: 字节=32 时间=1ms TTL=128
来自 192.168.41.10 的回复: 字节=32 时间<1ms TTL=128
```

接下来,将主机添加到域中,将计算机名改为"PC-2008"域名改为"hack.com"。单击"确定"按钮,会弹出要求输入拥有权限的域账户名和密码的对话框。在本实验中,输入域管理员的账号和密码,如图所示。操作完成后,会出现需要重新启动计算机的提示。

