

0X00 前言

我一直想做一个大一点的内网环境的，配置如下：

```
■■■■■■■
■■■■■■■■
■■■■■
■■■web■■■
■■■AV
■■■■
*nix
■■■■■
.....
```

过年回家没网，win2012我没下，只能先用08当DC。

我本人没有服务器，一般来说应该用exsi部署,主要是想让不熟悉AD的人去关注和理解它，后续就可以执行一些基本的操作，枚举和攻击。

PS：我最后会把环境发出来

以不同角度看AD

可能在一些企业内网里面，管理员选择性的偷懒，并没有添加安全策略去强化AD环境，造成安全问题。

与此同时，攻击者也会想方设法的去绕过这些安全策略，攻防永不停歇。

0x01 基本概念

AD（Active Directory）

AD是英文词汇Active Directory活动目录的缩写活动目录

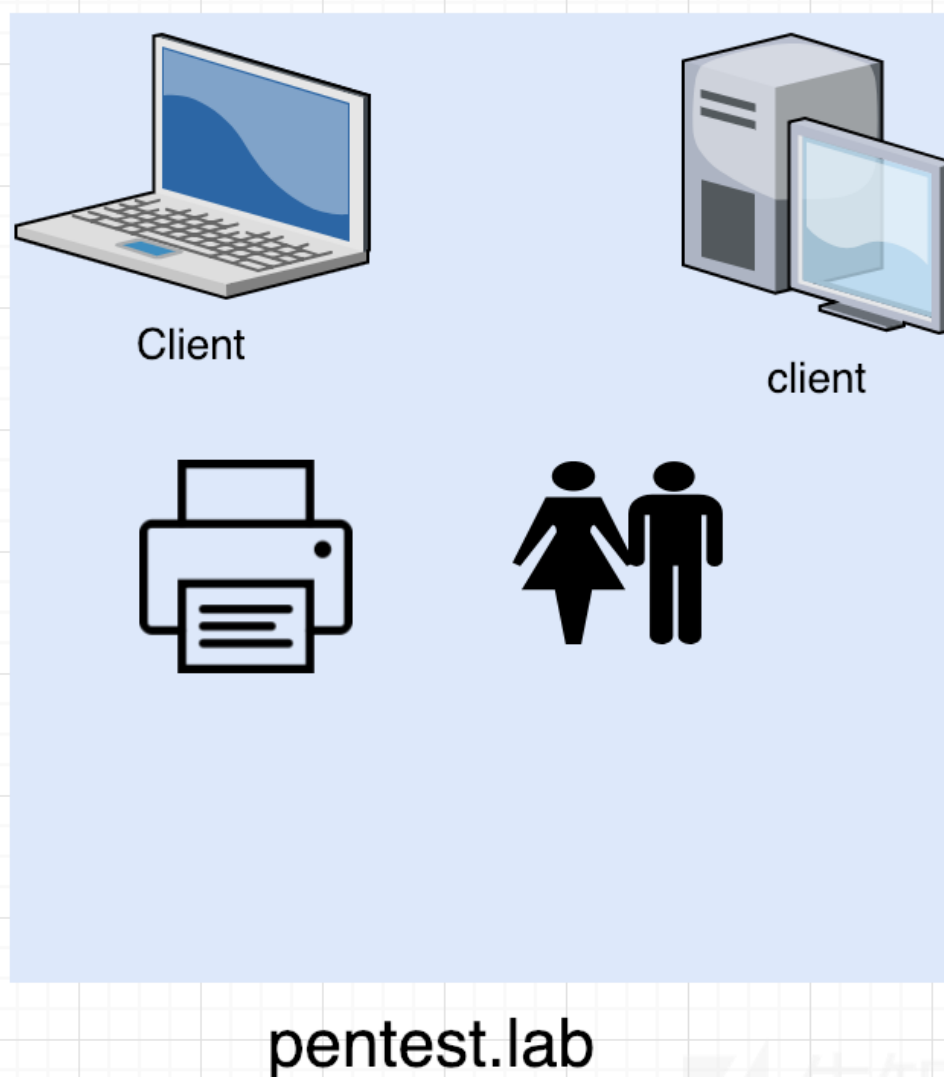
- 1) 活动目录（Active Directory）是面向Windows Standard Server、Windows Enterprise Server以及 Windows Datacenter Server的目录服务。
 - 2) Active Directory存储了有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息。
 - 3) Active Directory使用了一种结构化的数据存储方式，并以此作为基础对目录信息进行合乎逻辑的分层组织。
 - 4) Microsoft Active Directory 服务是Windows 平台的核心组件，它为用户管理网络环境各个组成要素的标识和关系提供了一种有力的手段。
- 来自百度百科

它就相当于一个存储库，可存储与组织的用户，计算机，服务器，资源等相关的所有数据，并使系统管理员可以轻松管理。



所有的对象都是在一个域里面，名称是唯一的。

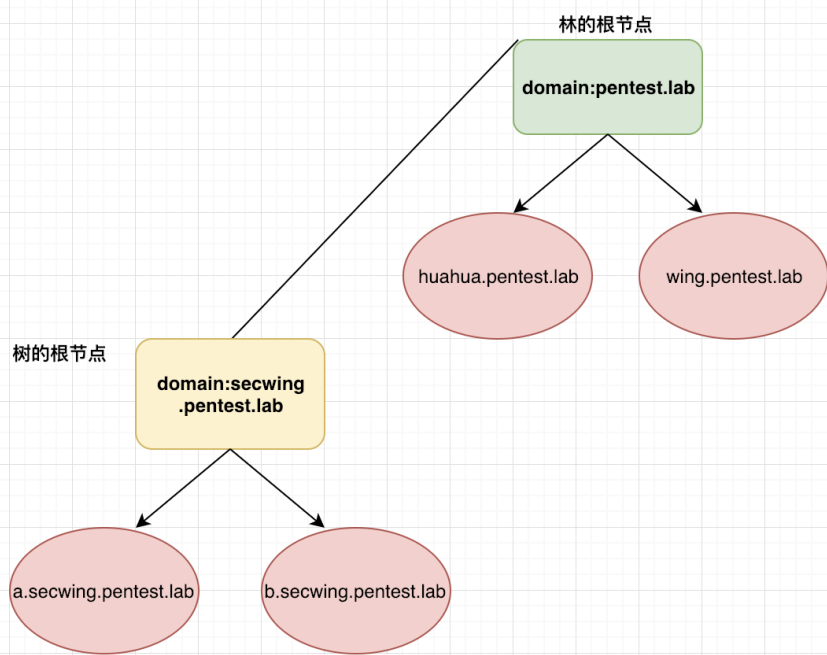
emmm，我画的一个图。



域名也可以作为一个DNS服务器。

共享同一个的域名的连续AD domain叫做AD Tree,树中的对象是有层次结构的，比如有一台计算机secwing在pentest.lab的子域huahua中。他的FQDN(FQDN : Fully Qualified Domain Name 全限定域名)就是:secwing.huahua.pentest.lab

这些的集合我们称之为林，即使只有一个域，域也始终是林的一部分。林由多棵树组成，与树不同，林可以有几个不连续的命名空间，



Active Directory域控制器

PS■AD DS■Active Directory■■■

用户登陆到域时，AD 域控制器会进行认证，认证需要的就是AD DS，

AD 数据库

用户的身份认证信息以及计算机，组，服务等等的信息都存储在Active Directory数据库中，该数据库由名为ntds.dit的单个文件组成。默认情况下，它存储在%SYSTEMROOT%\NTDS文件夹中。

LDAP

LDAP代表轻量级目录访问协议。该服务负责跟踪网络上的内容。

AD DNS

DNS对于Active Directory的工作非常重要。AD需要多个DNS记录来确定域上可用的服务以及提供哪些服务。在AD中配置DNS时，将自动管理这些记录。

Kerberos

Kerberos是允许您使用一个用户名和密码登录整个域中的多台计算机的服务。它基本上处理整个域中的单点登录。

GPP-组策略

组策略用于在机器级别定义用户，安全和网络策略。管理员可以将组策略从集中位置应用到整个域或少数计算机/用户。

0x02 Active Directory域控制器实验室

由于资源限制，我就设置了两台，电脑空间少，但也足够模拟AD攻击。

- 域控制器
windows 2012
在生产环境中，有多个域控制器，如ADC(附加域控制器)，RODC(只读域控制器)，CDC(子域控制器)。
- 客户端机器
win7和win10
- 成员服务器
- 如SQL服务器，文件服务器，FTP服务器，IIS服务器，代理服务器,防病毒服务器等。

建立虚拟机的时候，DC的网络模式用仅主机模式，然后只有DC和代理服务器能访问互联网，其他客户端将通过代理服务器访问互联网，因此我们也可以收集日志。

- 分配ip：
win+r■ncpa.cpl

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):

10 . 10 . 0 . 2

子网掩码(U):

255 . 0 . 0 . 0

默认网关(D):

. . .

☐ 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):

127 . 0 . 0 . 1

备用 DNS 服务器(A):

. . .

☐ 退出时验证设置(L)

高级(V)...

确定

取消

更改名称

win+r■sysdm.cpl

安装ADDS

点击添加角色和功能

服务器管理器

服务器管理器 仪表板

管理(M) 工具(T) 视图(V) 帮助(H)

仪表板

本地服务器

所有服务器

AD DS

文件和存储服务

欢迎使用服务器管理器

快速启动(Q)

新增功能(W)

了解详细信息(L)

1 配置此本地服务器

2 添加角色和功能

3 添加要管理的其他服务器

4 创建服务器组

隐藏

角色和服务组

角色: 2 | 服务器组: 1 | 服务器总数: 1

AD DS

1

可管理性

事件

服务

性能

BPA 结果

文件和存储服务

1

可管理性

事件

性能

BPA 结果

点击基于角色或功能的安装。

添加角色和功能向导

选择服务器角色

目标服务器
WIN-1M6565QQM4K

开始之前

安装类型

服务器选择

服务器角色

功能

DNS 服务器

确认

结果

选择要安装在所选服务器上的一个或多个角色。

角色

☐ Active Directory Federation Services

☐ Active Directory Rights Management Services

☐ Active Directory 轻型目录服务

☒ Active Directory 域服务 (已安装)

☐ Active Directory 证书服务

☐ DHCP 服务器

☒ DNS 服务器

☐ Hyper-V

☐ Web 服务器(IIS)

☐ Windows Server Essentials 体验

☐ Windows Server 更新服务

☐ Windows 部署服务

☐ 传真服务器

☐ 打印和文件服务

☐ 批量激活服务

☐ 网络策略和访问服务

描述

域名系统(DNS)服务器为 TCP/IP 网络提供名称解析。如果与 Active Directory 域服务安装在同一服务器上，DNS 服务器将更易于管理。如果选择 Active Directory 域服务角色，你可以安装并配置 DNS 服务器和 Active Directory 域服务一起工作。

< 上一步(P)

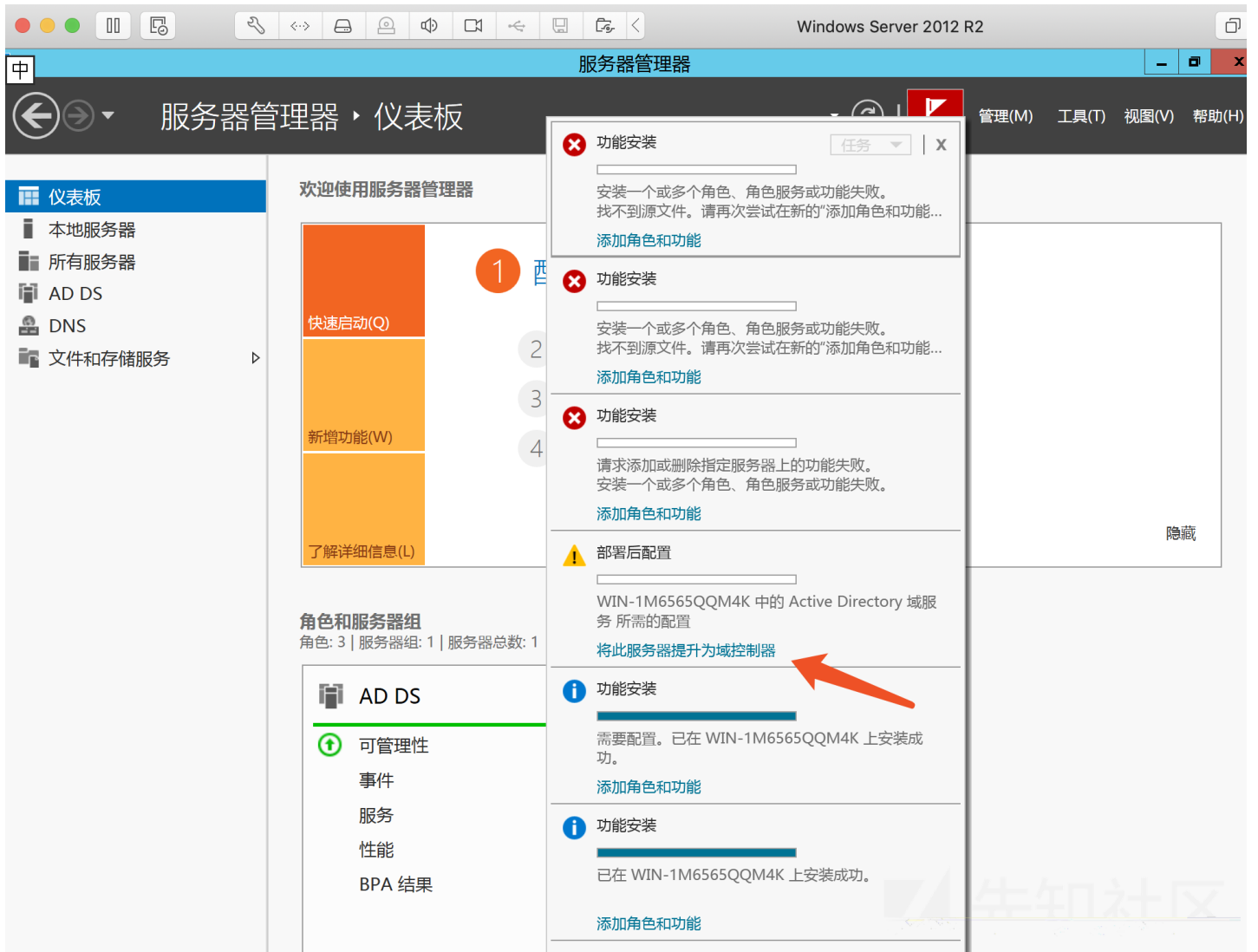
下一步(N) >

安装(I)

取消

继续下一步

- 提升为DC



看图吧

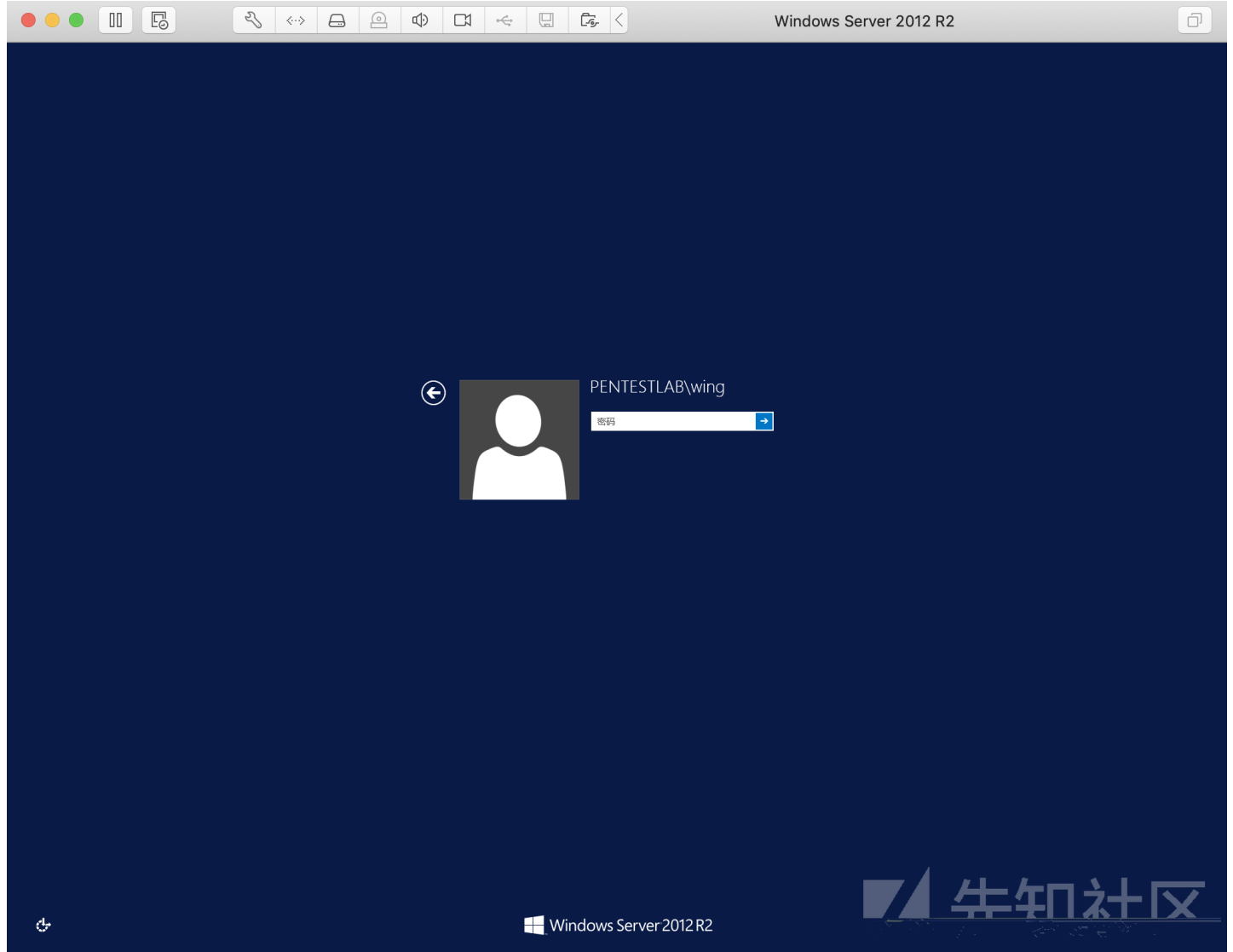


设置DSRM密码，域服务出现问题的时候通过这个密码还原。



一直下一步，前面更改完计算机名称后再安装一遍，会检查一些先决条件。

安装完成之后会自动重启，



0x03 Powershell设置域控制器

我们也可以通过命令的方式设置域控制器
以管理员身份运行PowerShell并输入以下命令：

安装AD DS Role

```
Install-windowsFeature AD-Domain-Services
```

Microsoft Windows [版本 6.3.9600]

(c) 2013 Microsoft Corporation。保留所有权利。

C:\Windows\system32>powershell

Windows PowerShell

版权所有 (C) 2013 Microsoft Corporation。保留所有权利。

PS C:\Windows\system32> Install-windowsFeature AD-Domain-Services

Success	Restart Needed	Exit Code	Feature Result
True	No	NoChangeNeeded	{}

PS C:\Windows\system32>



安装ADDS RSAT功能：

Add-windowsfeature RSAT-ADDS

将服务器提升为域控制器

Import-Module ADDSDeployment

这个命令没回显。

添加一个新的林：

Install-ADDSForest

0x04 添加计算机进入域

ip:10.10.0.3

DNS:10.10.0.2

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):

10 . 10 . 0 . 3

子网掩码(U):

255 . 0 . 0 . 0

默认网关(D):

. . .

☐ 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):

10 . 10 . 0 . 2

备用 DNS 服务器(A):

. . .

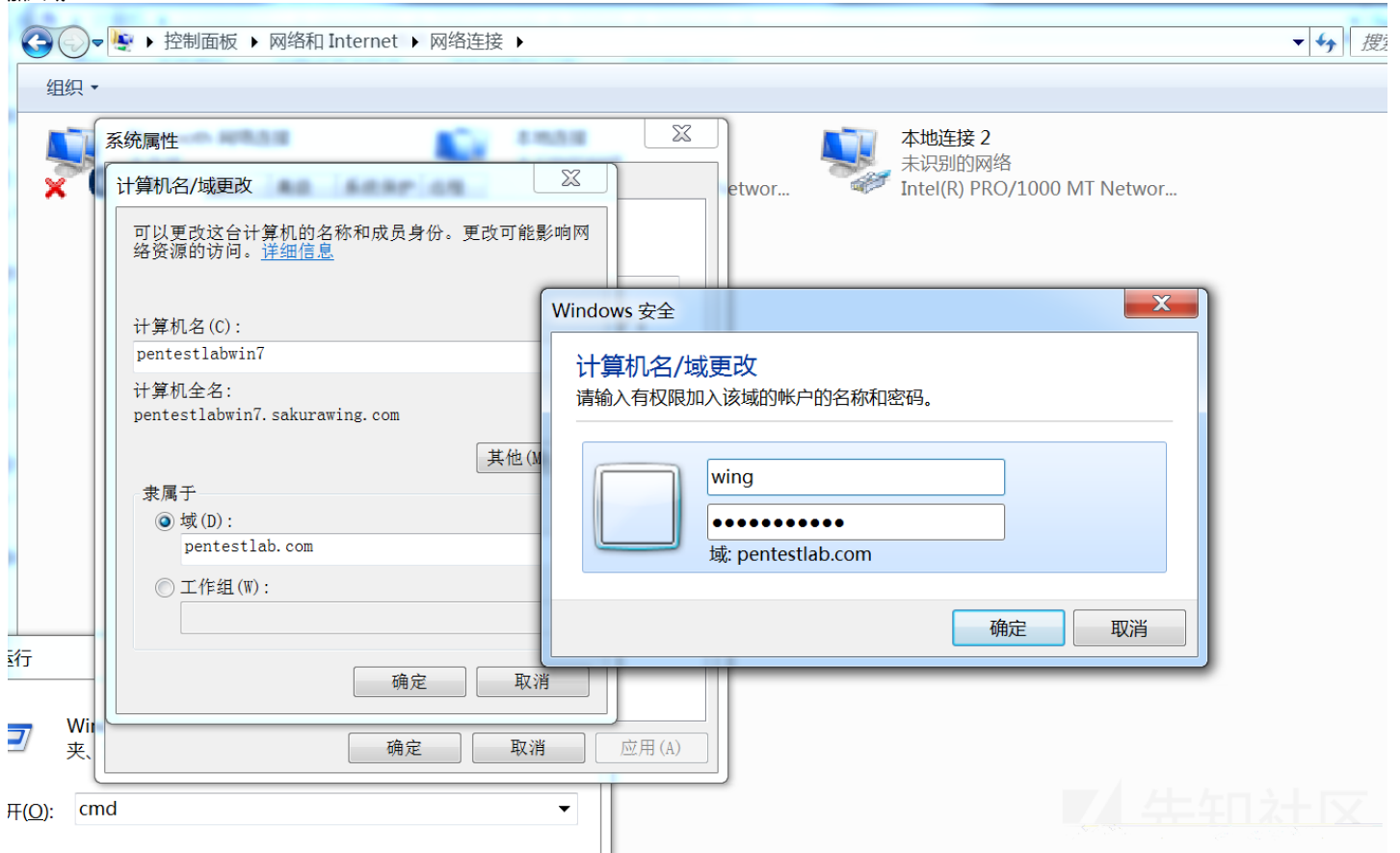
☐ 退出时验证设置(L)

高级(V)...

确定

取消

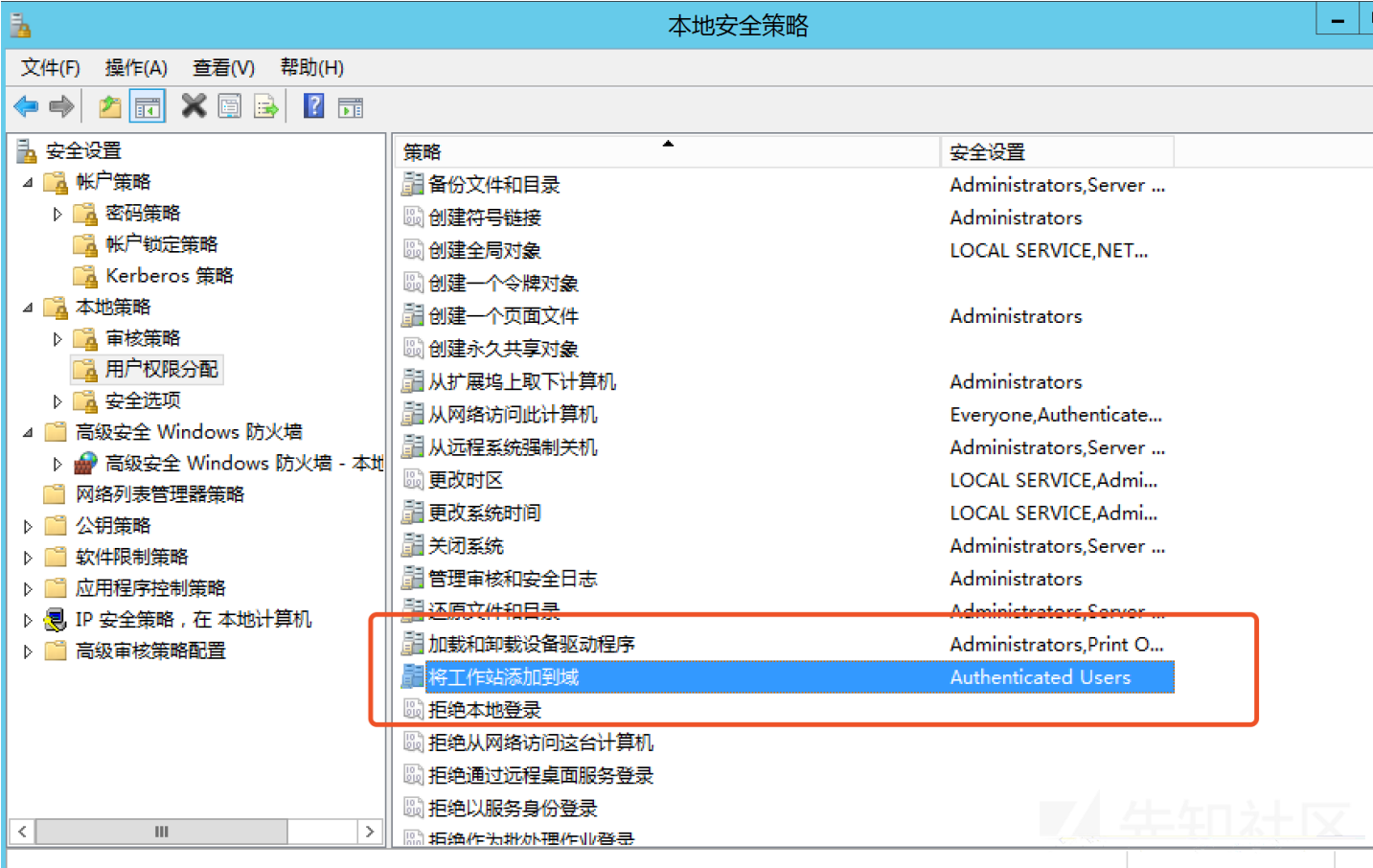
加入域



OK



可以将几个客户端添加到域中。

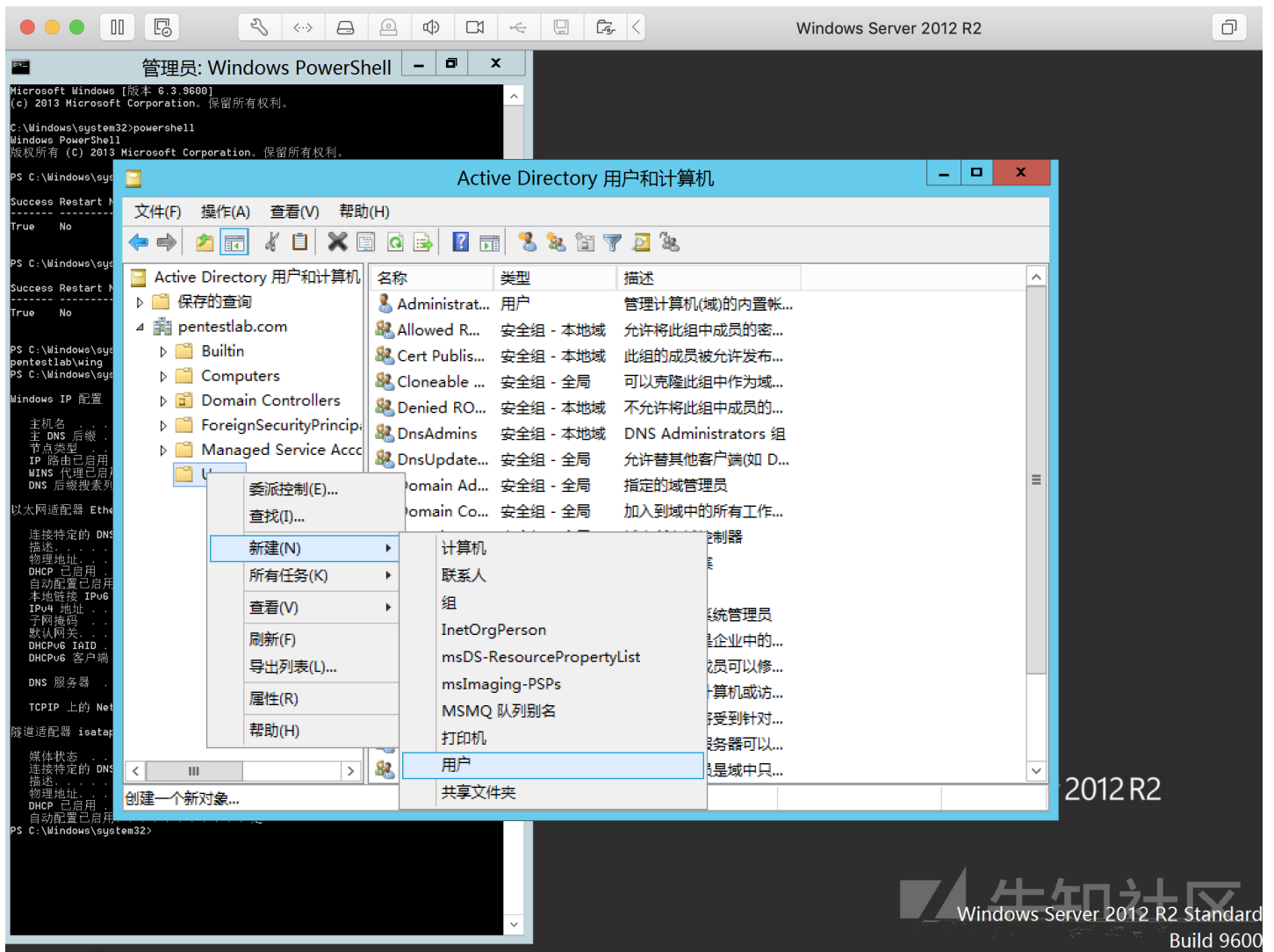


认证的用户可以将workstation添加到域
域用户可以在域中添加最多10个系统。

这是因为ms-DS-MachineAccountQuota属性。默认情况下，它设置为10.如果我们将其更改为0，则将禁用此限制。

0x05 将用户添加到Active Directory Domain

打开ADUC:
win+r:dsa.msc



2012 R2

Windows Server 2012 R2 Standard
Build 9600

设置好密码即可

cmd的方式

```
net user username password /add /domain
```

Powershell的方式

```
New-ADUser -Name "Winsaaf Man" -DisplayName "Winsaaf Man" -SamAccountName "winsaaf.man" -UserPrincipalName "winsaaf.man@script
```

批量添加用户

使用powershell脚本从CSV文件导入用户的详细信息。运行此脚本时，它会在域中创建多个用户帐户。

通过访问[此链接](#)从Microsoft的repo下载脚本和csv文件。


DHCP服务器

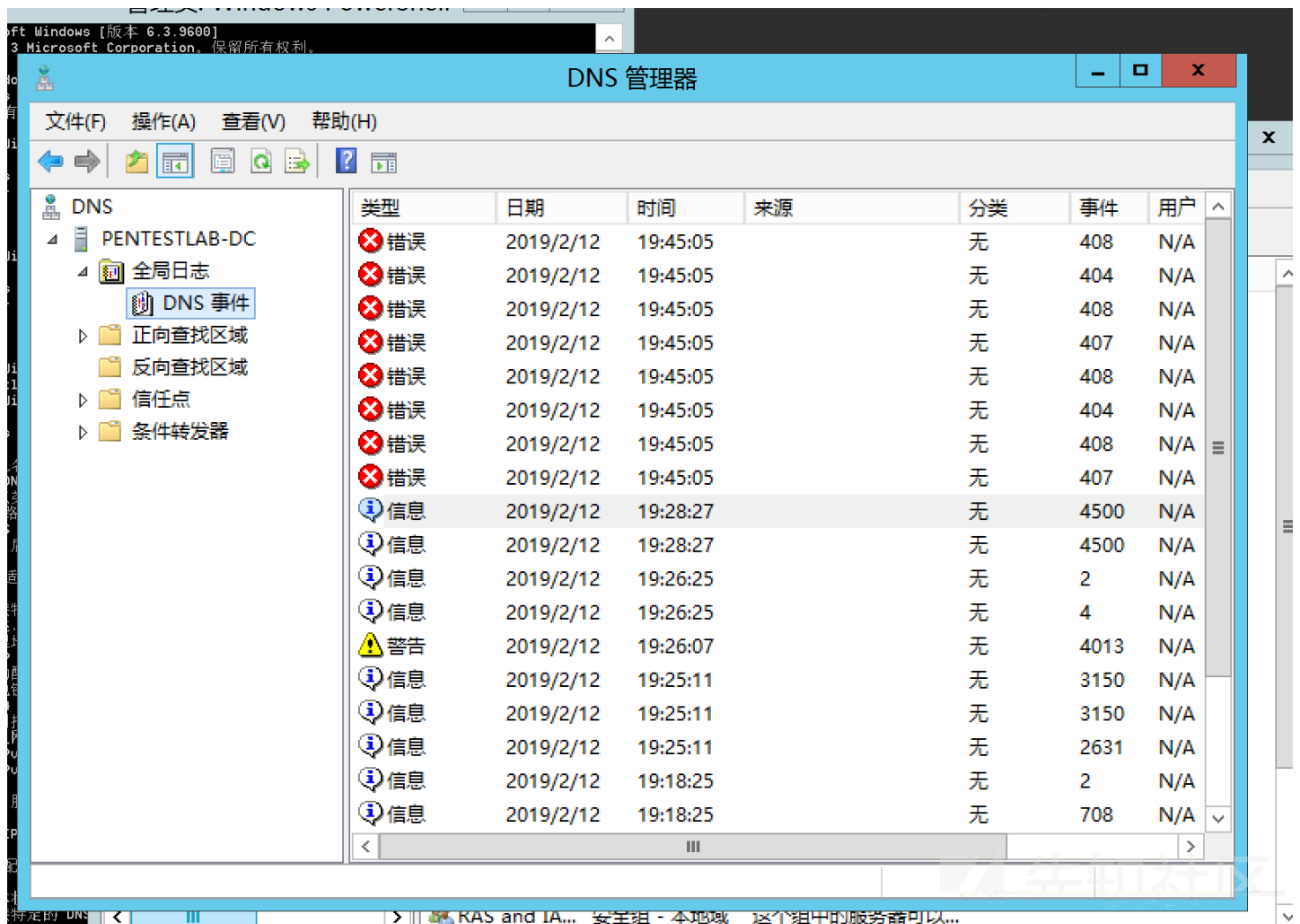
AD环境中需要动态配置协议服务器，以减少通过输入静态IP并加入域来配置每台计算机的手动操作。如果域中有DHCP服务器，则所有客户端计算机都会自动获取IP地址和子网掩码。

由于我们的目的是设置一个小的AD环境来执行测试，并且客户端机器不多，我们也可以跳过DHCP设置并手动分配IP地址。

AD集成DNS服务器设置

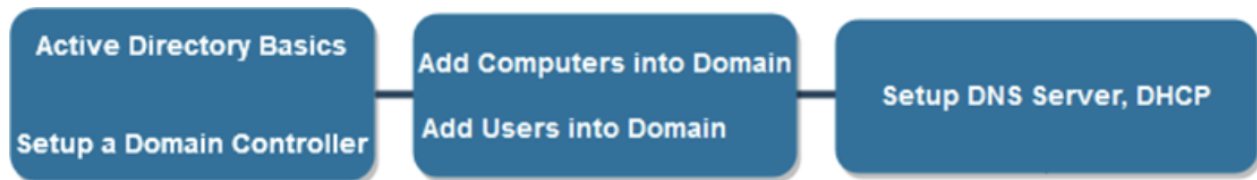
DNS是Active

Directory的主要名称解析服务。可以通过访问服务器管理器并单击部分来安装此角色。选择DNS。这将在您域控制器上安装DNS服务器角色，它将成为域环境的DNS服务器。



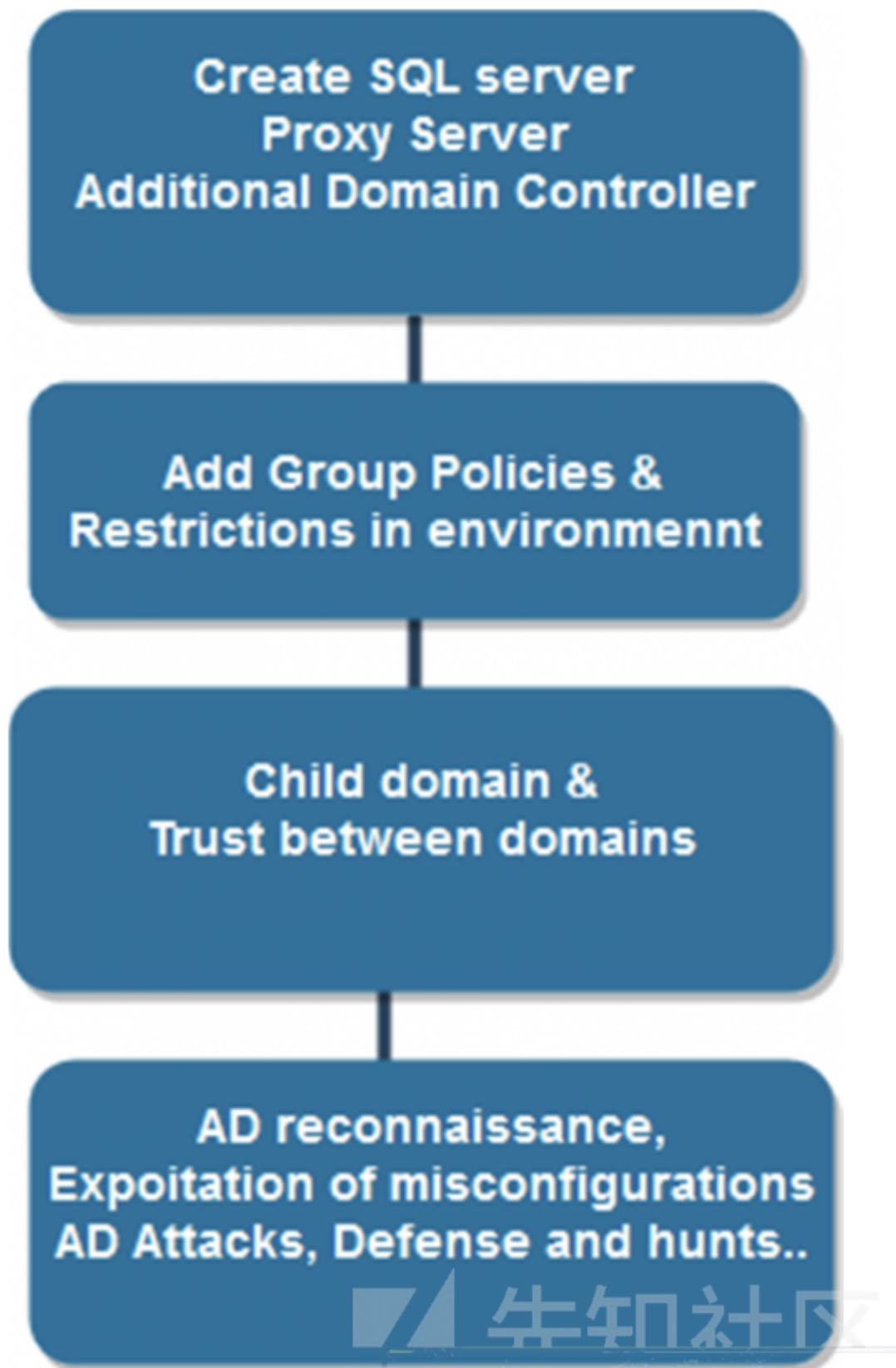
0x06 模块流程

环境流程



网络安全社区

在下一部分中，我将添加更多的服务器，如SQL服务器，代理服务器和身份验证。创建子域并在域之间建立信任并实施组策略然后限制环境。



接下来就是AD侦察，利用错误配置和基于DC的攻击和使用Powershell，WMIC进行枚举，执行Kerberos攻击，滥用SQL服务器信任等。

我也是通过这个作者的文章跟着走一遍，后面我会自己复现一些漏洞，结合cs和msf。

[原文链接](#)

点击收藏 | 0 关注 | 1

[上一篇：Nexus Repository ...](#) [下一篇：用ARM编写shellcode](#)

1. 1 条回复



[fs冷逸](#) 2019-09-22 20:43:48

师傅，您说的下载地址在哪？

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)