

高级域渗透入侵及检测（下）

目录

- DSRM
- SIDHistory属性修改
- ESAE
- DNS
 - 普通用户权限获取DNS解析记录
 - Dns admin到Domain admin

DSRM

DSRM(目录还原模式)简单来讲就是AD出问题了，例如域管登陆DC都登录不了，那么可以通过DSRM,允许管理员用来修复或者重建活动目录数据库，DSRM账户密码在安装域控的时候确认，一般不会更改，DSRM账户不是域用户，属于DC的本地管理员

实际上在域控上这个DSRM账户就是administrator(这个说法并不完全正确，准确应该叫DSRM的administrator),DSRM并没有实际的账户名，但是修改DSRM密码后，域控本地管理员的administrator密码也会更改，但是反过来，改了administrator的密码，DSRM确不会受影响

更改DSRM密码的方式：

方式一：通过NTDSUTIL

```
^ 代码块

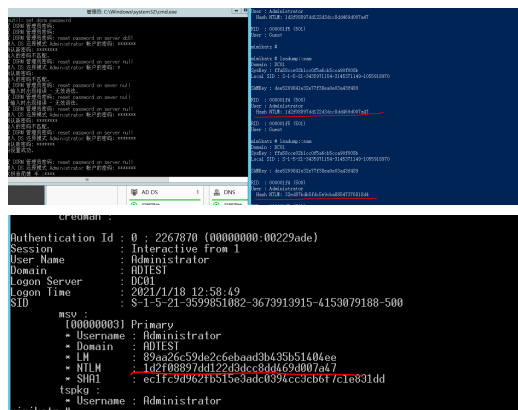
1 ntdsutil
2 set dsrm password           //进入设置DSRM密码选项
3 reset password on server null //在当前域控重设DSRM密码
4 q                           //推出
```

方式二：密码同步，可以指定同步一个域内用户的密码过来

```
^ 代码块

1 NTDSUTIL
2 set dsrm password
3 SYNC FROM DOMAIN ACCOUNT test //同步密码为test账户的密码
4 q
```

更改DSRM密码后，本地administrator账户也受到影响，但是通过域认证的administrator不会受影响



使用DSRM远程登录到DC的话需要做点配置，更改或加入以下注册表条目

```
^ 代码块

1 reg add "HKLM\System\CurrentControlSet\Control\Lsa" /f /v DsrmAdminLogonBehavior /t REG_DWORD /d 2
```

至于该注册表的数字所代表的其他含义可以看：<https://adsecurity.org/?p=1785>

更改后可以本地administrator远程登录



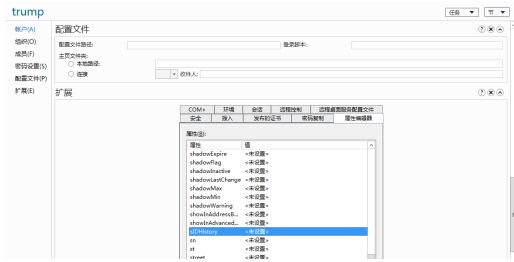
至于一些其他的利用方式如PTH等，后续都是可以用的在这里，无影响

检测方式：

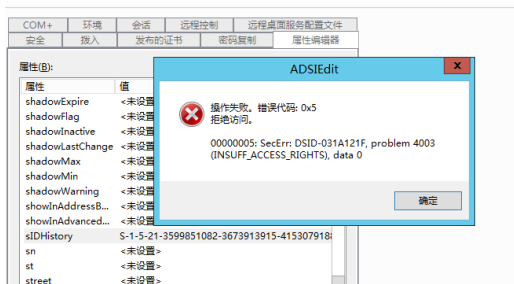
看注册表，没必要的话删了该注册表，同时注意id为4794的日志，该日志于DSRM密码有关

SIDHistory属性修改

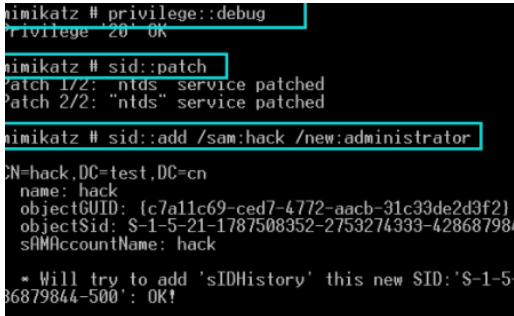
域用户当从一个域移动到另一个域的时候，会创建一个新的SID，这个SID为objectsid属性，而之前的SID则会被添加到SIDHistory属性中，这样确保用户仍能够访问原来域的资源



直接在这里更改是改不了的



一般通过如mimikatz等，将普通用户的SIDhistory/属性更改为administrator的SID，达到权限维持的一种效果，同样的子域中的普通用户sidhistory也可以改为Enterprise admin SID这样对整个集团都有权限



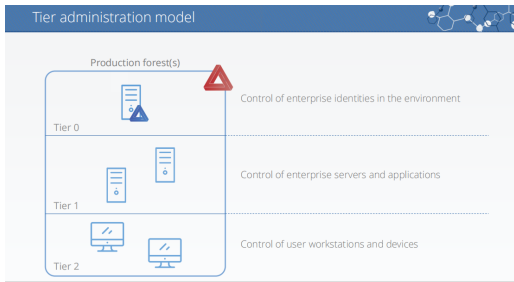
ps:慎用mimikatz更改，容易导致重启

ESAE

增强安全管理环境(Enhanced Security Admin Environment)体系结构，也被称为红森林，管理林，被用来对windows AD域环境提供增强的安全环境，旨在限制凭据的公开来阻止通过盗窃这些凭据来攻击关键要素

主要基于Active Directory分层模型设计，此分层模型的目的是通过在能完全控制环境的层级（第0层）和攻击者经常破坏的高风险工作站资产之间使用一组缓冲区来保护标识系统。分层层模型由三个级别组成，其中仅包括管理

帐户，不包括标准普通用户帐户



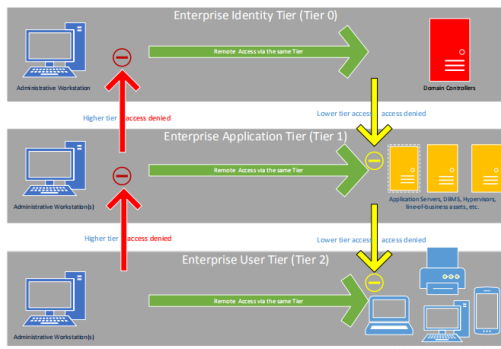
<https://www.blackhat.com/docs/us-17/wednesday/us-17-Coltel-WSUSpendu-Use-WSUS-To-Hang-Its-Clients.pdf>

层级0：直接控制整体环境，包括对Active Directory林，域或域控制器以及其中的所有资产具有直接或间接管理控制权的帐户或组，第0层的资产所以资产敏感性相同，并有相同的权限

层级1：控制企业的服务应用等，第1层资产包括服务器操作系统，云服务和企业应用程序，第1层的管理员对托管在这些资产上的业务具有管理权，毕竟常见的就是系统管理员，可以维护所有的服务器

层级2：控制用户工作站主机设备等，第2层管理员帐户对托管在用户工作站和设备上的业务具有管理控制权，例如it管理员以及技术支持等，因为他们可以影响所有用户的数据

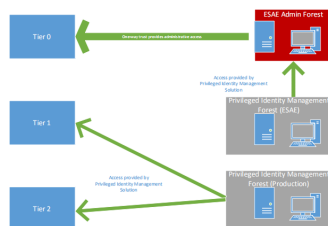
如图，不同层级之间的访问控制关系：



https://download.ernw-insight.de/troopers/tr18/slides/TR18_AD_Attack-and-Defend-Microsoft-Enhanced-Security.pdf

红森林与具有访问控制的生产网络隔离，红森林到生产网络的单向信任是强制的，是一个独立的域森林，通过加密通道管理生产林/域，生产网络的AD admin账号是无法访问红森林的，所有的ad admin账号以及组都是通过密码管理解决方案来统一管理的，在ESAE中应建立双因素认证、严格的日志记录和警报以及其他安全控制

RED FOREST OVERVIEW – ADMINISTRATIVE FOREST



在针对红森林攻击中需要注意的点：

1.重点查找shadow admin

何为shadow admin呢，就是不在管理员组里面却具有一些特权操作，比如目录复制，可以进行DCSync等

Accounts / Groups with DCSYNC rights

Accounts / Groups with special control to root domain objects

Microsoft Exchange servers

Accounts / Groups with special control to AdminSDHolder

域内Microsoft SharePoint User Profile Synchronization (UPS) service , Riverbed SteelHead AD service account, Azure AD Sync service account, 都默认具有

Replicate Directory Changes

Replicate Directory Changes All

这俩可以目录复制也就是可以用来DCSync操作的权限

域内exchange的两个组，具有更改域内账户full control的权限

Exchange Windows Permissions

Exchange Trusted Subsystem

如果搞到了exchange的机器，就可以通过类似powerview等方式，给用户添加对应的权限：

Add-DomainObjectAcl -TargetIdentity 'DC=DOMAIN,DC=COM' -PrincipalIdentity username -Rights DCSync

其他的还有查找针对敏感用户或者组有权限的，如针对AdminSDHolder容器等

2.针对红森林基础设施里的虚拟平台

如果目标环境里面使用了虚拟化环境，存在VMware vCenter或者ESXi等关键控制节点，那么就可以利用，前提是vCenter或者ESXi不在红森林的0层中，并且有对应的管理员权限

主要目的，就是从vCenter数据存储中搞到目标机器的vmdk镜像，以下是三种查找镜像的方式：

通过vSphere客户端查找特定机器的vmdk

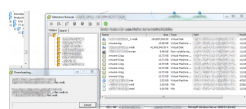
ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage vSphere Client to retrieve VMDK images from datastore:

- Authenticate to VMware vCenter / ESXi via vSphere client.
- Identify the target server (i.e. Domain Controller)
- Go to the Summary tab
- Under Resources, right click the datastore under "storage" (should be next to a gray icon)
- Go to the VM name and download the VMDK file(s)

Drawback: This approach does not work all the time in VMware vCenter environment, especially for hot clone



通过VMware PowerCLI查找对应的镜像

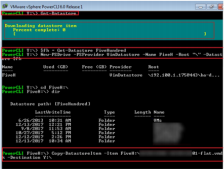
ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage PowerShell via VMware PowerCLI to retrieve VMDK images

- Connect to VMware vCenter / ESXi via VMware PowerCLI by initializing the connection/session using the Connect-VIServer command
- Obtain the names of the datastore and map them individually to a drive using New-PSDrive
- Download the VMDK files from the targeted datastore

Drawback: This approach does not consistently work in the VMware vCenter environment, especially for hot clone.



通过Veeam备份客户端获取vmdk镜像

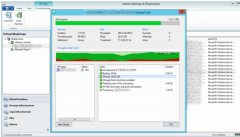
ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage Veeam backup client to retrieve VMDK images

- Authenticate to VMware vCenter / ESXi via Veeam backup client
- Identify the target server (i.e. Domain Controller)
- Backup / Replicate the VMDK files from the targeted sever

Advantage: This approach is reliable even for hot clone.



然后的话就是本地挂载了，之后就可以搞ntds.dit了

ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

- Mount VMDK file as a loop device on using the following command once the VMDK file is downloaded :

```
mount xxxxx-flat.vmdk <mount path> -o ro,loop=/dev/loopX,offset=<offset> -t ntfs
```


- Retrieve sensitive files such as NTDS.dit and dump password hashes:



3.针对红森林里的 endpoint 防护设备

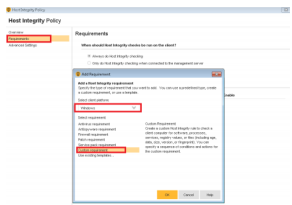
- 赛门铁克管理控制台：
- 前提：对应的管理员权限，赛门铁克管理主机不在0层，
- 利用方式：推送payload到端点主机上
- 1)创建主机策略，可以执行脚本

- Execute scripts by creating Host Integrity Policy:
- Go to Policies > Host Integrity > Add a new policy

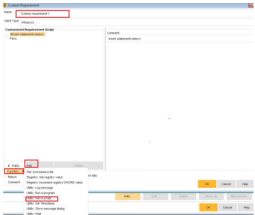


2)为主机策略增加自定义需求

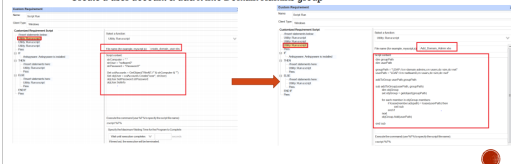
- Create a Custom Requirement for the new Host Integrity Policy



- Create payload by adding a Function



- Create payload by adding a Function
- Create a user account & add it into Domain Admins group



系统中心配置管理：



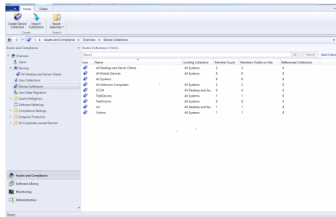
前提还是一样的，对应的管理员权限，以及不在0层当中

利用点：系统中心配置管理GUI界面以及PowerSCCM

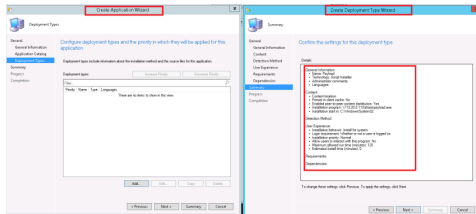
利用过程：

- 1.创建SCCM连接
- 2.创建SCCM应用(payload)
- 3.推送payload到目标机器

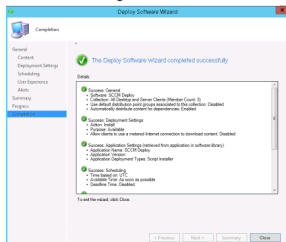
- Create a SCCM connection



- Create a SCCM application



- Deploy SCCM application to the targeted collection



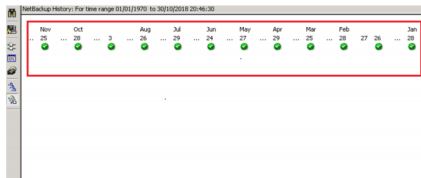
通过PowerSCCM实现同样的效果

- Accomplish the same attack procedures from PowerSCCM:
- \$Creds = Get-Credentials
 - Enter the credentials and they will be stored in the \$Creds variable
- \$S = New-ScmSession -ComputersName <SCCM Server> -SiteCode <SiteCode> -Credentials \$Creds -ConnectionType WMI
 - Store the session into a variable, this session is basically used for every PowerSCCM Command
- New-ScmApplication -ApplicationName <App Name> -Session \$S -PowershellScript .\script.ps1
 - Create the actual application to be deployed
- New-ScmApplicationDeployment -AssignmentName <Any String Value> -Session \$S -ApplicationName <App Name> -CollectionName <Collection Name>
 - Deploy the application assuming you already know the collectionname you want to target. If you do not know which collection name, this can be found using "Get-ScmCollection -filter *"

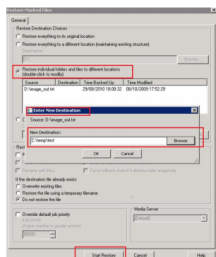
利用网络备份解决方案

主要利用方式就是为目标机器如域控做备份，然后还原复制特定文件

- Identify a valid file restoration point for a targeted server



- Restore the marked files from the backup file image





也就是通过dns admins组用户的权限，加载我们的dll后，可以获取到对应机器的system权限。

ps:后来微软好像对此做了配置修复,只有域管可以更改 `ServerLevelPluginDll` 的值了