登录

Password Filter DLL在渗透测试中的应用

wilsonlee1 / 2018-03-02 16:01:21 / 浏览数 12914 技术文章 技术文章 顶(0) 踩(0)

0x00 前言

在之前的文章《域渗透——Hook PasswordChangeNotify》介绍了通过dll注入Hook PasswordChangeNotify来记录新密码的方法，相当于是对API PasswordChangeNotify的利用。

我们知道，API PasswordChangeNotify是Password Filter DLL的一个功能函数，那么，对于Password Filter DLL本身，能否直接开发一个可供利用的DLL呢？

0x01 简介

本文将要介绍以下内容：

- Password Filter DLL简介
- 利用Password Filter DLL记录明文密码
- 利用Password Filter DLL实现的后门
- 非Windows Server系统下的应用

0x02 Password Filter DLL简介

现实中使用Windows系统时，为了提高系统安全性，防止用户密码被暴力破解，系统管理员往往会对用户密码的复杂度提出要求，可通过配置组策略开启

位置如下：

`gpedit.msc -> ■■■■■■■■ -> ■■■■■■ -> Windows■■ -> ■■■■■ -> ■■■■■ -> ■■■■■ -> ■■■■■■■■■■■■`

启用后，密码必须符合下列最低要求:

- 不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分
- 至少有六个字符长
- 包含以下四类字符中的三类字符:
- 英文大写字母(A 到 Z)
- 英文小写字母(a 到 z)
- 10 个基本数字(0 到 9)
- 非字母字符(例如 !、$、#、%)

默认值:

- 在域控制器上启用
- 在独立服务器上禁用

如果该策略仍无法满足对密码复杂度的要求，可以使用Password Filter DLL进一步提高密码的复杂度

实现思路：

1. 通过修改注册表的方式安装Password Filter DLL
2. 用户修改密码时，自动加载Password Filter DLL，导入明文密码
3. 在Password Filter DLL中开发者可以自定义密码复杂度，同明文密码的复杂度进行比较，如果明文密码不满足复杂度条件，弹框提醒用户，密码修改失败

具体使用方法可参考官方文档：

https://msdn.microsoft.com/en-us/library/windows/desktop/ms721766(v=vs.85).aspx

0x03 Password Filter DLL的开发

支持以下三个函数：

```
BOOLEAN InitializeChangeNotify(void);

NTSTATUS PasswordChangeNotify(In PUNICODE_STRING UserName,In ULONG RelativeId,In PUNICODE_STRING NewPassword);

BOOLEAN PasswordFilter(In PUNICODE_STRING AccountName,In PUNICODE_STRING FullName,In PUNICODE_STRING Password,In BOOLEAN SetOperation);
```

参考资料：

https://msdn.microsoft.com/en-us/library/windows/desktop/ms721849(v=vs.85).aspx#password_filter_functions

值得注意的地方：

- API PasswordChangeNotify和PasswordFilter的传入参数均包括用户的明文密码
- API PasswordFilter的返回值为TRUE表示密码符合要求，返回FALSE表示密码不符合复杂度要求，弹框提示用户修改
- 在编写Password Filter DLL时，需要声明导出函数

提供一个可供参考的POC，地址如下：

https://github.com/3gstudent/PasswordFilter

该工程声明了导出函数`InitializeChangeNotify`、`PasswordChangeNotify`和`PasswordFilter`

分别使用`PasswordChangeNotify`和`PasswordFilter`记录明文密码，保存在`c:\logFile1`和`c:\logFile2`

在编译时需要同目标系统的平台对应

%wZ表示输出PUNICODE_STRING，unicode的字符串指针类型

0x04 Password Filter DLL的安装

1、注册表`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`下的`Notification Packages`，添加Password Filter DLL的名称，不包括后缀名.dll

2、将Password Filter DLL保存在%windir%\system32\下

3、组策略开启组策略密码必须符合复杂性要求

4、重启系统(注销当前用户不会生效)

5、修改任一用户密码，加载Password Filter DLL

实际测试：

测试系统： Windows Server 2008 R2 x64

将Password Filter DLL工程编译生成64位的Win32Project3.dll

1、将Win32Project3.dll保存在%windir%\system32\下

2、修改注册表键值`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`下的`Notification Packages`，添加`Win32Project3`

如下图

通过命令行实现的方式如下：

读取键值：

```
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages"
```

获得键值内容：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
   Notification Packages    REG_MULTI_SZ    scecli\0rassfm
```

添加Win32Project3：

```
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v "Notification Packages" /t REG_MULTI_SZ /d "scecli\0rassfm\0Win32Projec
```

注：

`\0`表示换行

3、Windows Server系统的组策略默认开启密码必须符合复杂性要求

4、重启系统

5、修改用户密码

6、记录明文密码

如下图

注：

能够记录所有用户，包括未登录用户

0x05 域环境下的应用

1、记录明文密码

针对域控服务器,需要获得域控服务器权限，在%windir%\system32\下放置Password Filter DLL，修改注册表键值

优势：

域控服务器默认开启组策略密码必须符合复杂性要求

不足：

必须重启系统才能生效，对于域控服务器来说，很少重启

扩展：

将payload改为将明文密码发送至Web服务器，可供参考的代码地址：

https://malicious.link/post/2013/2013-09-11-stealing-passwords-every-time-they-change/

2、后门

将Password Filter DLL改为启动后门，例如弹回Meterpreter的shell

域内任一用户在修改密码时均会加载Password Filter DLL，弹回高权限的shell

0x06 非Windows Server系统的应用

目前大部分资料均认为Password Filter DLL仅适用Windows Server系统

对于非Windows Server系统来说，同样可以使用，只是组策略默认禁用■■■■■■■■■■■■■■■

因此需要注意以下问题：

1、命令行查看当前系统的组策略配置

组策略配置存储在数据库中，位于`%windir%\security\database\secedit.sdb`

读取命令如下(管理员权限)：

```
secedit /export /cfg gp.inf /quiet
```

参数说明：

没有设置/db参数，表示数据库采用默认`%windir%\security\database\secedit.sdb`

/quiet表示不生成日志，否则生成的日志默认保存在`%windir%\security\logs\scesrv.log`

命令执行后生成文件gp.inf，查看gp.inf中的PasswordComplexity项，1代表开启，0代表关闭

注：

gp.inf中的内容不完整，想要获得完整的组策略配置还需要读取注册表

2、修改组策略配置，开启组策略密码必须符合复杂性要求

首先导出配置文件gp.inf，将PasswordComplexity项设为1，保存

导入数据库：

```
secedit /configure /db gp.sdb /cfg gp.inf /quiet
```

刷新组策略，立即生效(否则，重启后生效)：

```
gpupdate/force
```

0x07 防御检测

根据利用思路，攻击者首先需要获得当前系统的管理员权限

检测思路如下：

1、查看`%windir%\system32\`下有无可疑dll

2、查看注册表键值`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`下的`Notification Packages`

3、查看进程lsass.exe加载的dll

如下图

0x08 小结

Password Filter DLL本是系统提供的正常功能，但如果获得了系统的管理员权限，利用这项功能不仅能够记录明文密码，还能用作后门。

本文结合具体的利用思路，介绍了检测方法。

点击收藏 | 0 关注 | 1
上一篇：我的面经，渗透测试 下一篇：漏洞分析与实践之基于SAML实现的...
1. 0 条回复
- 动动手指，沙发就是你的了！

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