



SecureFilter

在组策略之外，Windows 允许你自定义密码策略，滥用这个机制可以实现一些恶意行为。今天为大家科普下

当我们按下 CTRL + ALT + DEL，修改用户密码时，在 Windows 服务器端，会发生什么呢？

首先，Windows 服务器（域控）会检查注册表，找到 Password Filter，也就是 LSA Notification Package。然后挨个调用DLL，检查密码是否符合策略，

Name	Value type	Value
NoLmHash	REG_DWORD	0x00000001 (1)
Notification Packages	REG_MULTI_SZ	scecli rassfm
ProductType	REG_DWORD	0x0000000a (10)
restrictanonymouse	REG_DWORD	0x00000000 (0)
restrictanonymouse...	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest tspkg pku2







Edit Multi-String
Value name:
Notification Packages
Value data:
scecli
rassfm



如果不符合策略，就提示密码不够健壮，

```
C:\Windows\system32>net user ok 111 /ad
The password does not meet the password policy requirements. Check the minimum
password length, password complexity and password history requirements.
More help is available by typing NET HELPMSG 2245.
```

在默认情况下，域上的服务器包含两个DLL，其中 seccli 负责实现密码安全策略，也就我们常用的GPO了

Policy	Policy Setting
 Enforce password history	Not Defined
 Maximum password age	Not Defined
 Minimum password age	Not Defined
 Minimum password length	Not Defined
 Password must meet complexity requirements	Not Defined
 Store passwords using reversible encryption	Not Defined

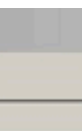
我们今天的主题，就是如何滥用这个机制，实现一个密码策略插件，以记录所有域用户的密码

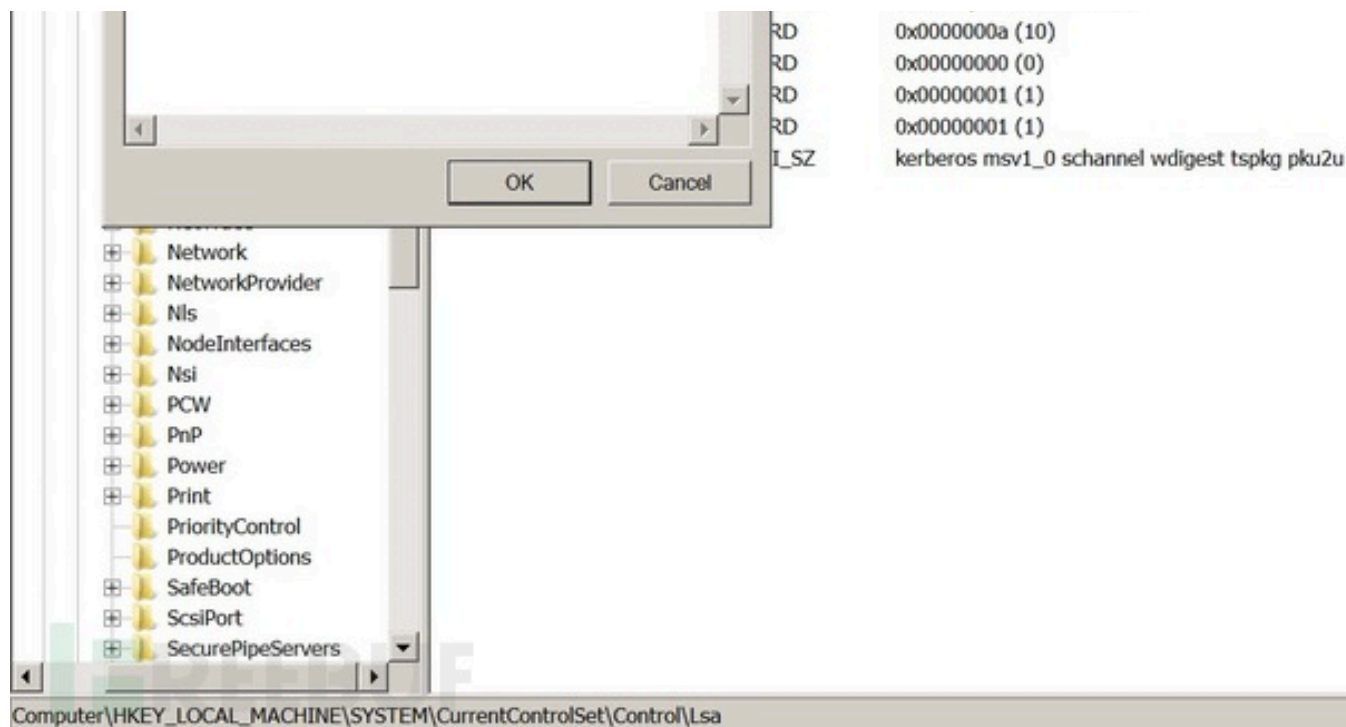
一家上市公司，为了符合SOX 404审计要求，密码每三个月就要强制修改一次，刚好可以触发这个机制

查了下[官方文档](#)，一个密码插件需要导出三个函数，

um p

Name,
e,
d,

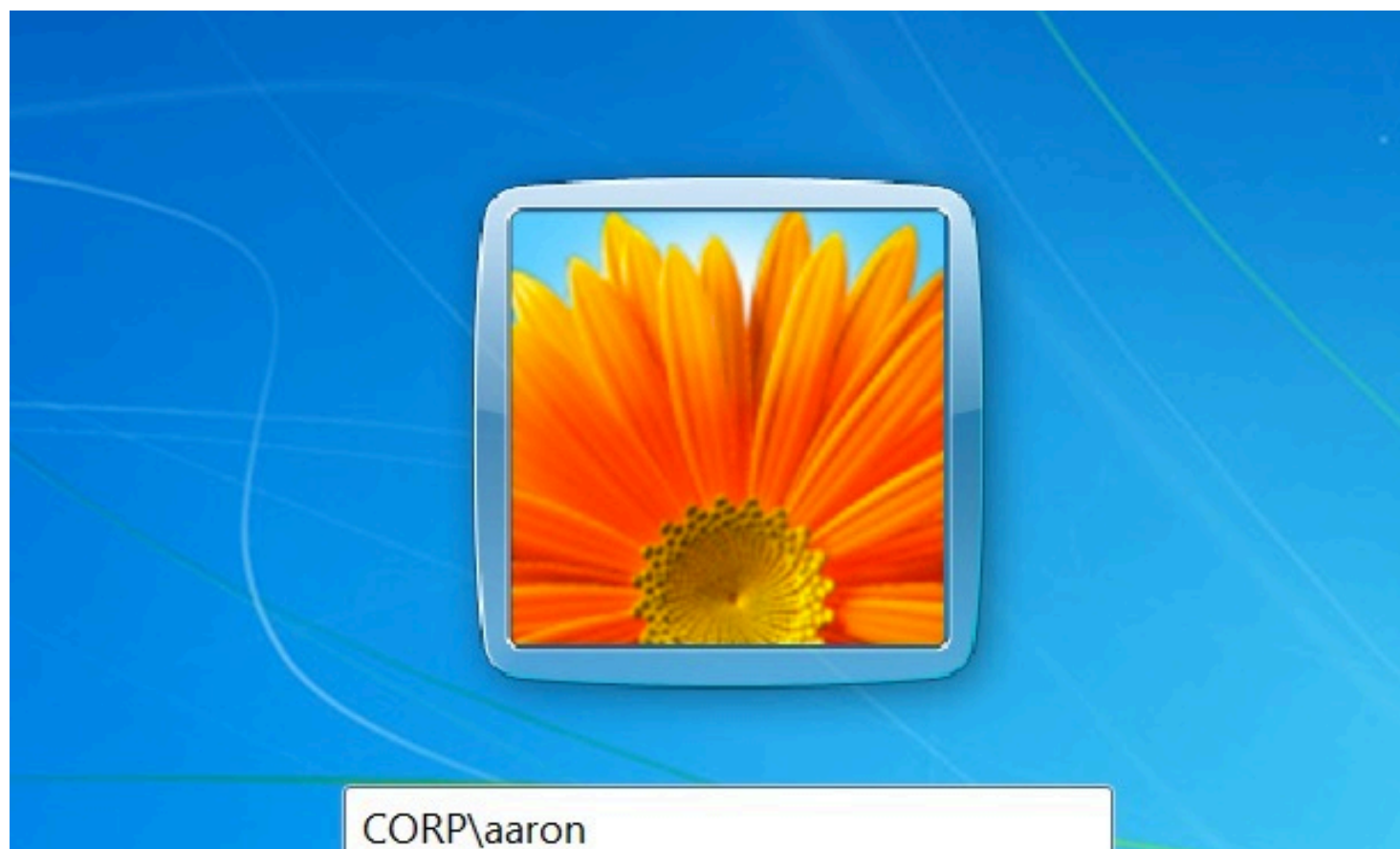


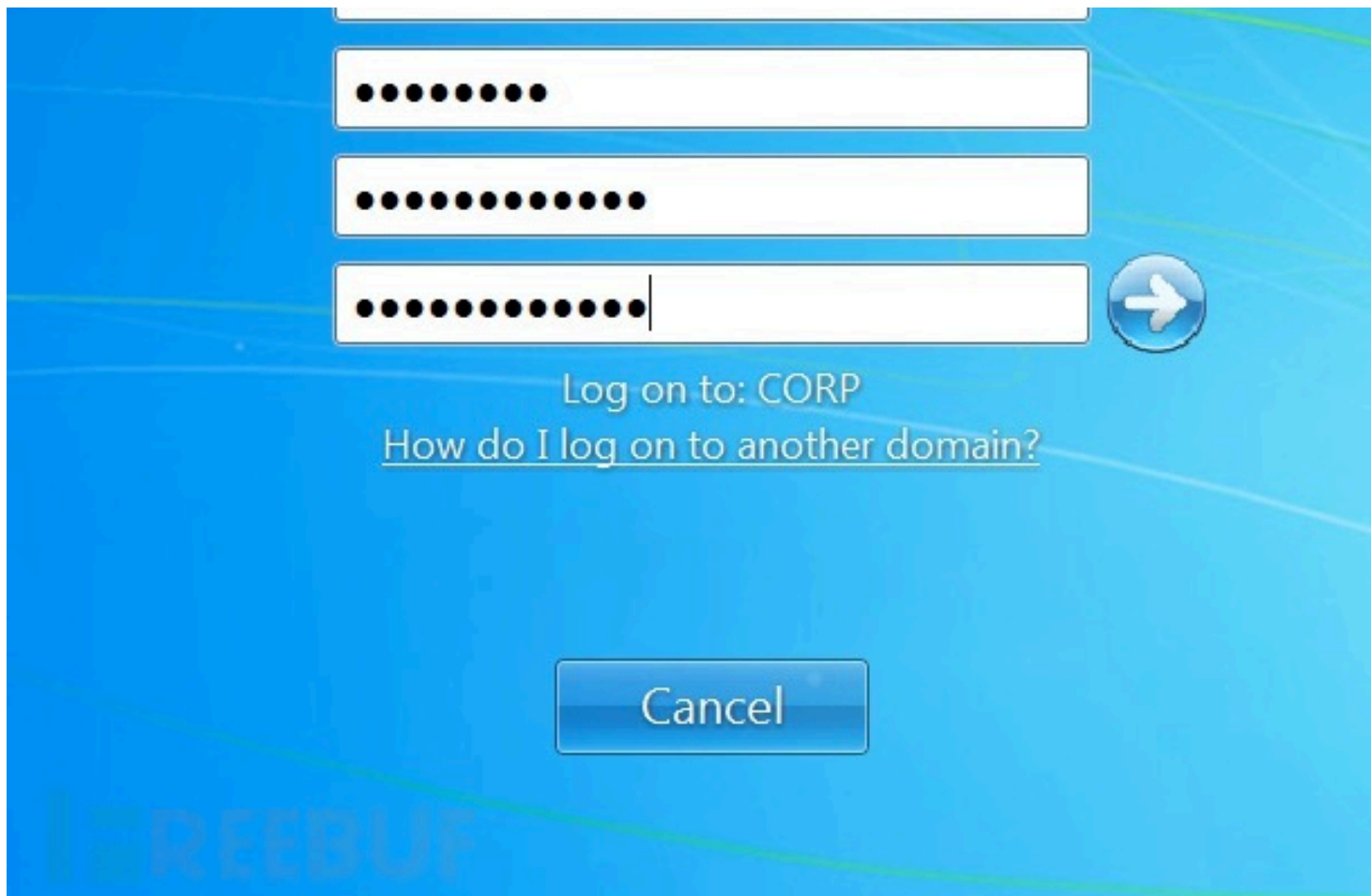


重启 DC 服务器后生效

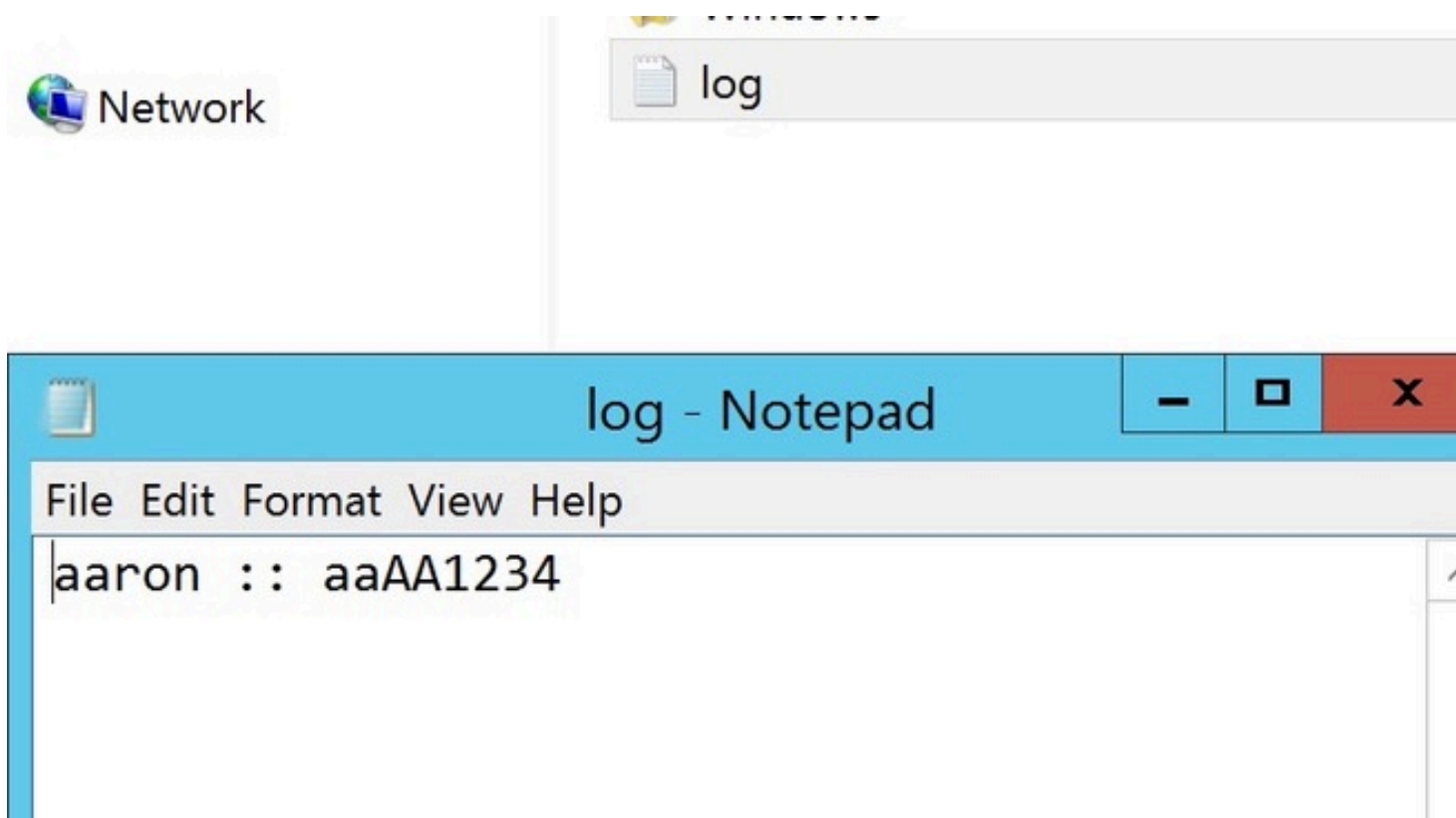
实战演示

我们登陆一台工作站，修改密码，





回到域控，发现日志已经写入了





写在最后

经过测试，无论你用何种方式修改密码，OWA 还是命令行，效果都是一样的；在未加域的服务器上效果也是一样

如果想要立即获取某个用户的密码，在域控上轻轻一勾即可“User must change password at next logon”，如图所示：



The screenshot shows the 'Account options' section of a Windows user account settings window. It contains four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Store password using reversible encryption' (unchecked). Below this is the 'Account expires' section, which has two radio buttons: 'Never' (selected) and 'End of:' (unselected). The 'End of:' option is followed by a date picker showing 'Friday, April 14, 2017'.

Account options:

- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Store password using reversible encryption

Account expires

☒ Never

☐ End of: Friday, April 14, 2017

