Browser Pivot for Chrome

mss**** / 2019-03-14 08:01:00 / 浏览数 1863 技术文章 翻译文章 顶(0) 踩(1)

原文地址：https://ijustwannared.team/2019/03/11/browser-pivot-for-chrome/

大家好，在本文中，我们将为读者详细介绍适用于Chrome的Browser Pivoting技术。所谓的Browser Pivoting，就是一种劫持目标机器中已经通过身份验证的浏览器会话的技术。当然，这并非一种新型技术，事实上，早在2013年，Raphael Mudge就在一篇文章中介绍过这种技术。遗憾的是，那篇文章中介绍的Cobalt Strike的Browser Pivot模块好像只能用于IE浏览器，而无法用于Chrome浏览器。在这篇文章中，我们将为读者介绍一种异曲同工的方法，也能对Chrome浏览器实现类似的效果——实时截获

读者可能会想"为什么要费这个劲呢"？如果已经拿下了目标系统，则可以借助mimikatz或keylog工具来获取相应的凭据，进而访问相应的资源即可。好吧，这里考虑的是应

你也可能会想——"本文明明是要介绍如何劫持MFA会话的，你却在这里吹嘘MFA的功效"。再次强调，这种技术自2013年就已经出现了，并且，为该PoC开发的特定代码是

如何进行防御

首先，如果您已经迫使攻击者求助于超越传统的凭据盗窃技术来访问关键的网络资源的话，那么恭喜您！同时，对于这种攻击来说，防御方可以通过多种指标来检测相关的恶

攻击过程

概括来说，该PoC尝试执行以下操作：

1. 修改系统，以允许多个远程桌面连接，并删除RemoteApp限制。
2. 使用VSS，将目标系统中正在使用的Chrome配置文件复制到另一个文件夹中。
3. 使用RemoteApp和 proxychains，远程打开指向这个复制的配置文件路径的Chrome实例。
4. 如果您愿意，也可以将配置文件复制到攻击虚拟机，然后通过 proxychains和Chrome完成劫持过程。不过，这样做比较耗时。

POC代码

需要提醒的是，这里提供的只是POC代码，使用时请自行承担风险。并且，Thunderrapp不仅会修改System32文件，还会修改ThunderVSS接口。这里给大家一个建议，不

- ThunderChrome

  ThunderRApp (x64 DLL) – 修改系统，使其允许接受多个RDP和RemoteApp会话

  ThunderVSS (x64 DLL) –使用VSS复制目标Chrome配置文件，以解决文件锁定问题。

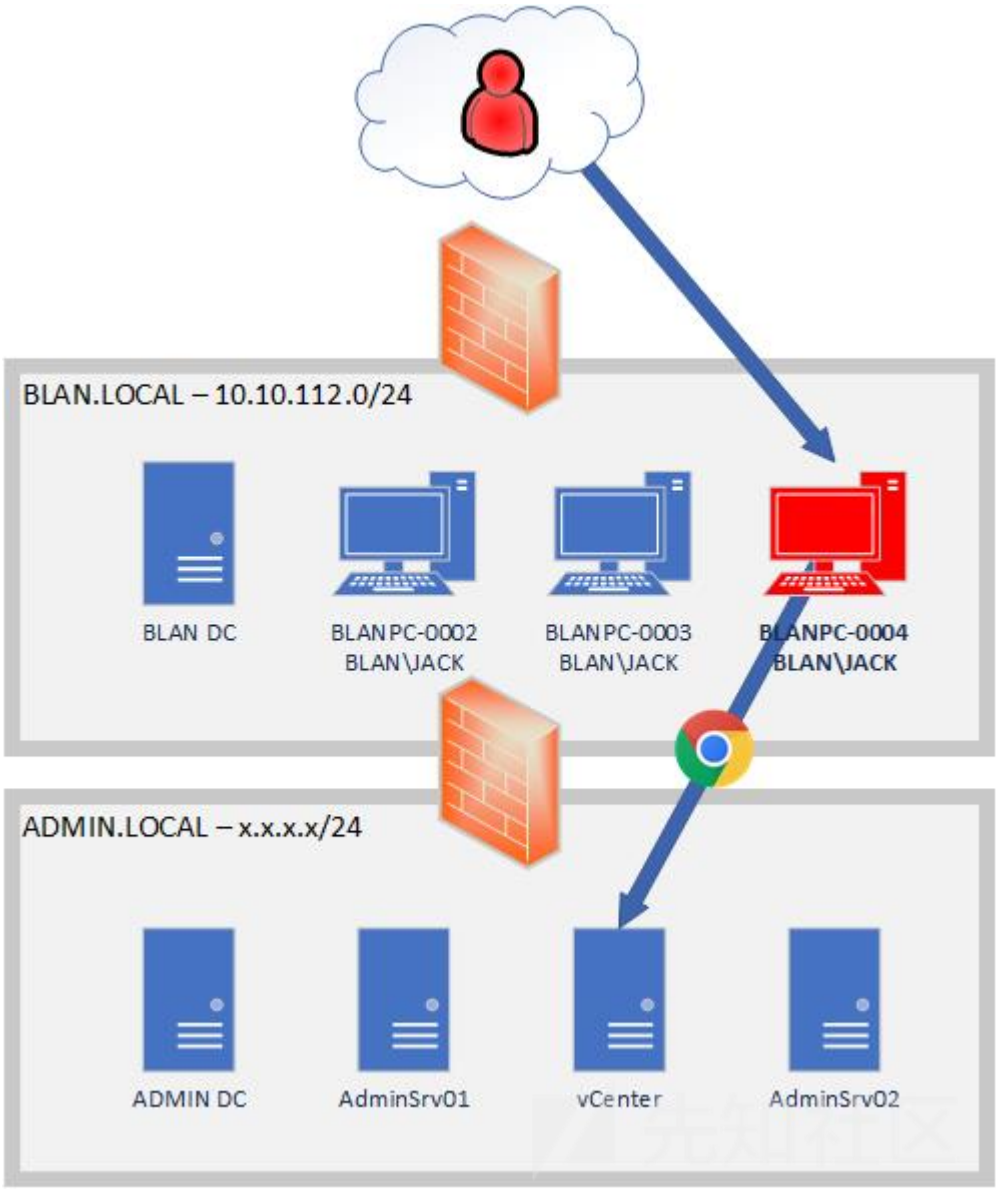
  ThunderChrome.cna – 允许DLL的攻击脚本

- 枚举Chrome的标签页（未包含）

攻击场景

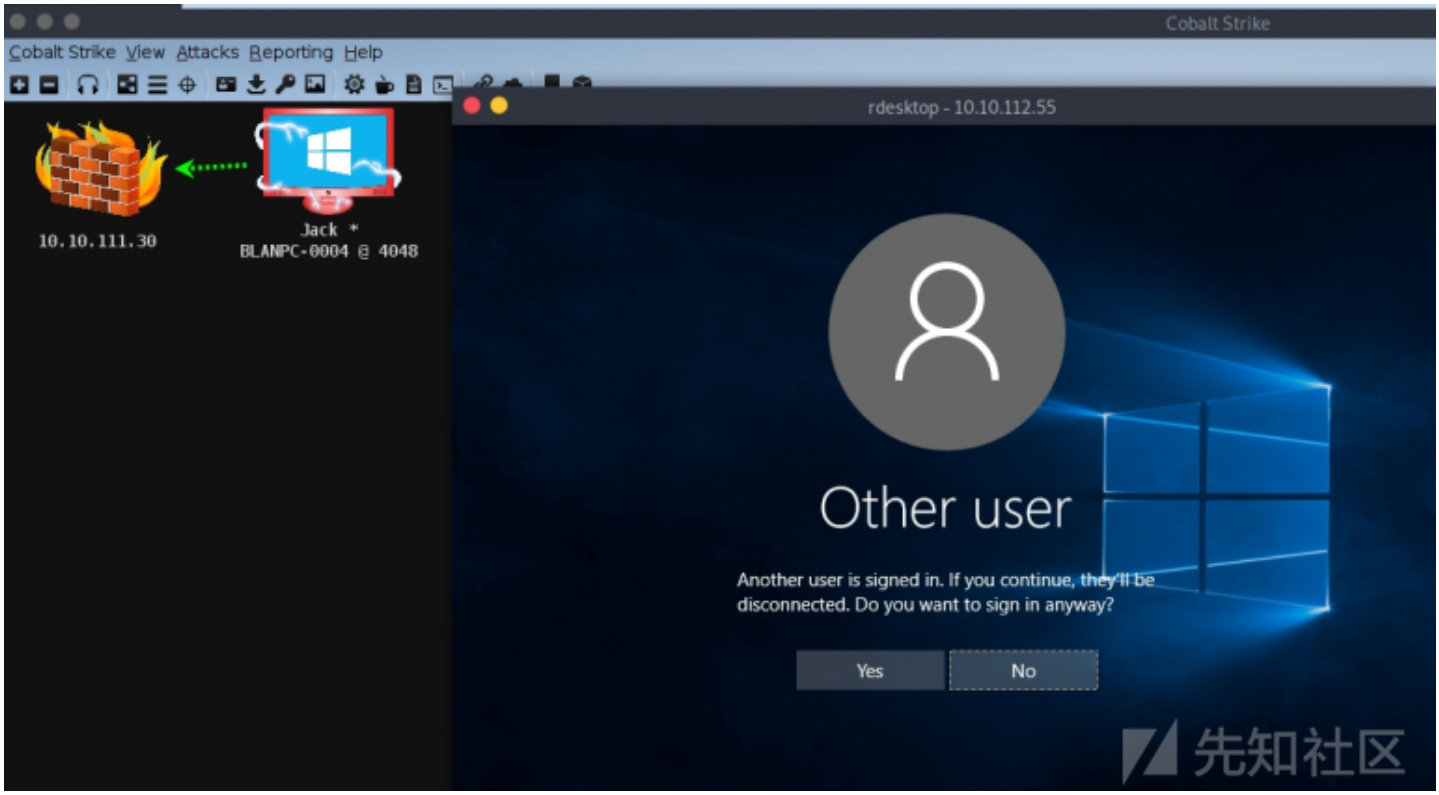
攻击者能够以BLAN\Jack身份访问BlanPC-0004。Jack使用浏览器访问管理域中的vCenter服务器。在vCenter服务器上进行身份验证时，ADMIN\Jack使用的凭据不同于BL

- 没有使用MFA时：派上mimikatz或keylog就能搞定！
- 使用MFA时：派上mimikatz或keylog，修改System32文件，启动和停止服务，通过VSS复制正在使用的文件，并建立RDP会话——折腾半天，真能搞定吗？

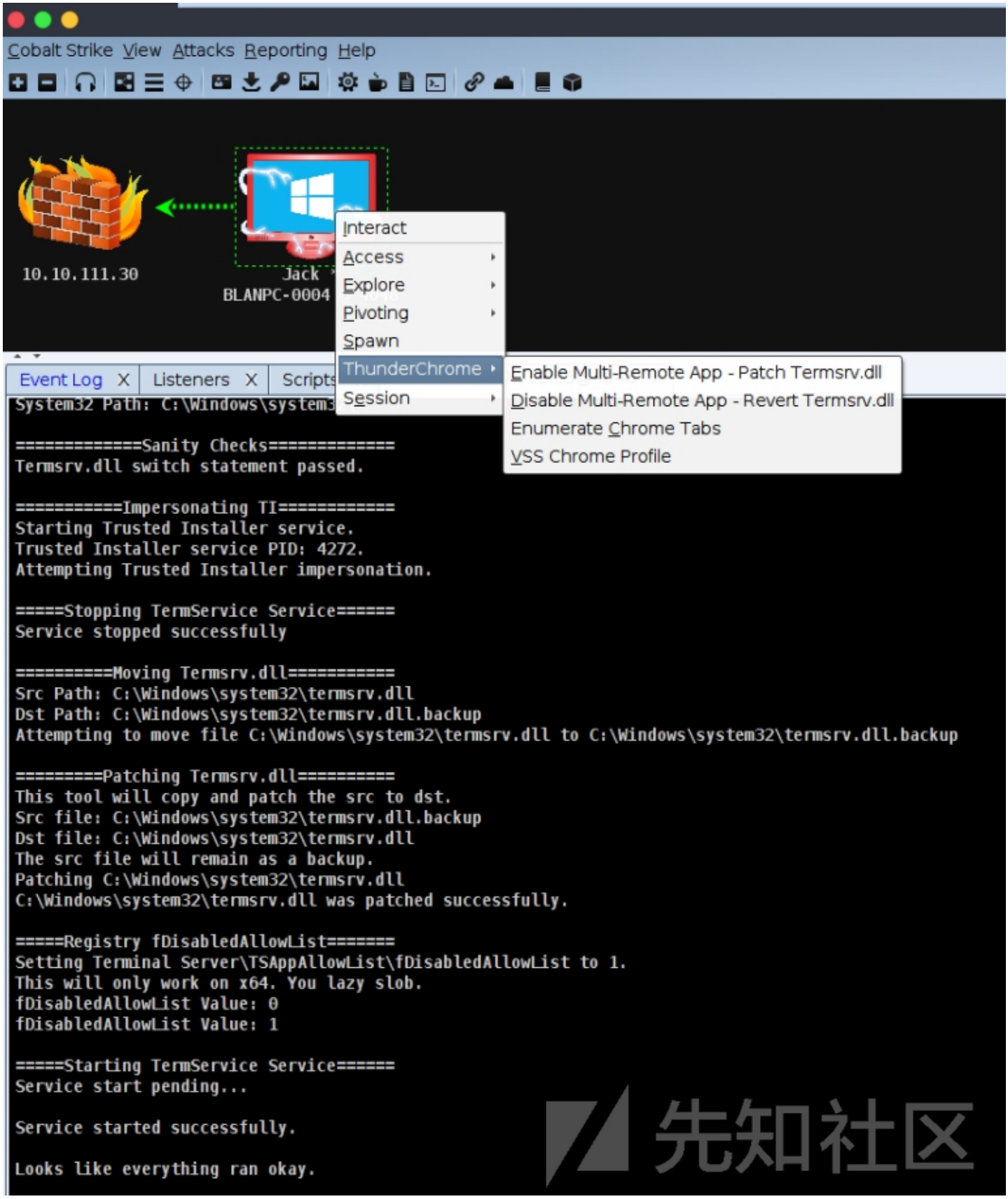


Multi-RemoteApp会话

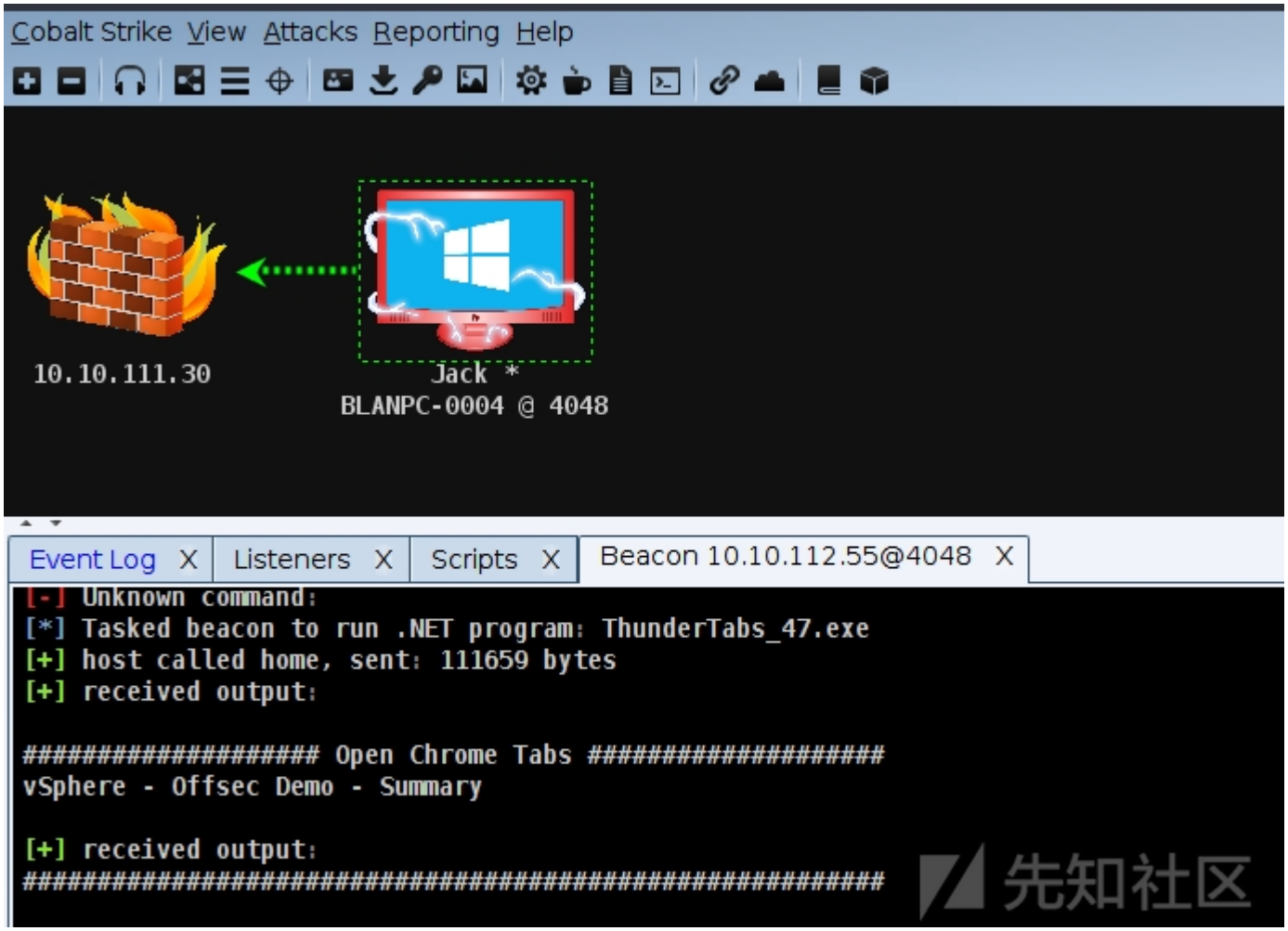
在本例中，我们尝试通过RemoteApp来访问Chrome会话。但是，在未经修改的Windows Workstation OS上，我们无法在具有活动会话的目标系统上使用RemoteApp。下面展示的是如何使用RDP连接具有活动会话的系统。



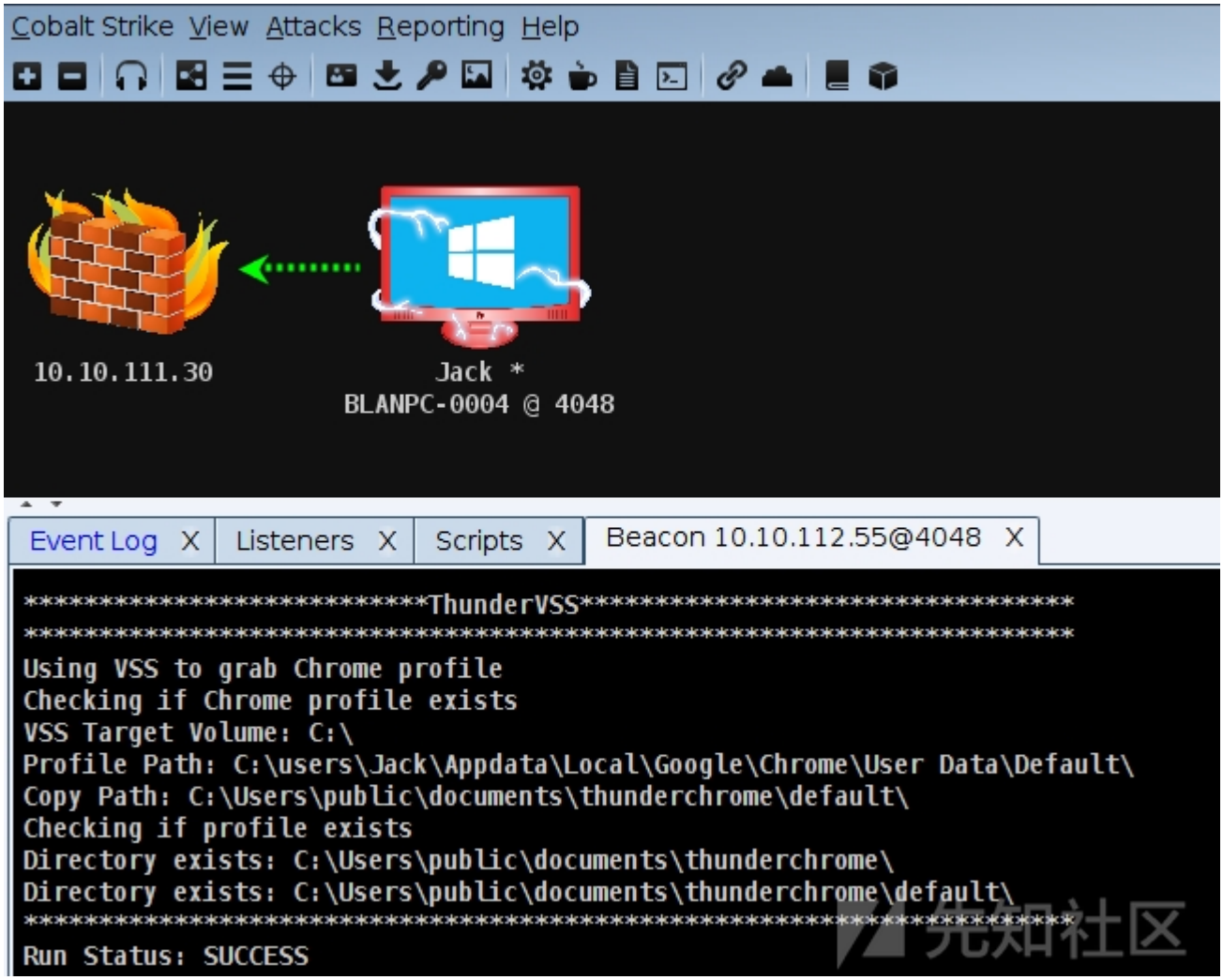
在这篇文章中，详细介绍了如何通过修改termsrv.dll，允许系统使用多个远程桌面会话，以便可以通过RemoteApp连接已经存在活动会话的系统。注意，该过程需要修补w



修改termsrv.dll后，即使用户在目标系统上还处于活动状态，我们也能够继续建立多个RemoteApp会话。在本例中，我们正在等待ADMIN\Jack在ADMIN vCenter服务器上进行身份验证。因此，本质上来说，我们要持续监视Chrome标签页中与vSphere相关的内容。为了枚举标签页，我使用了这里的PoC代码。



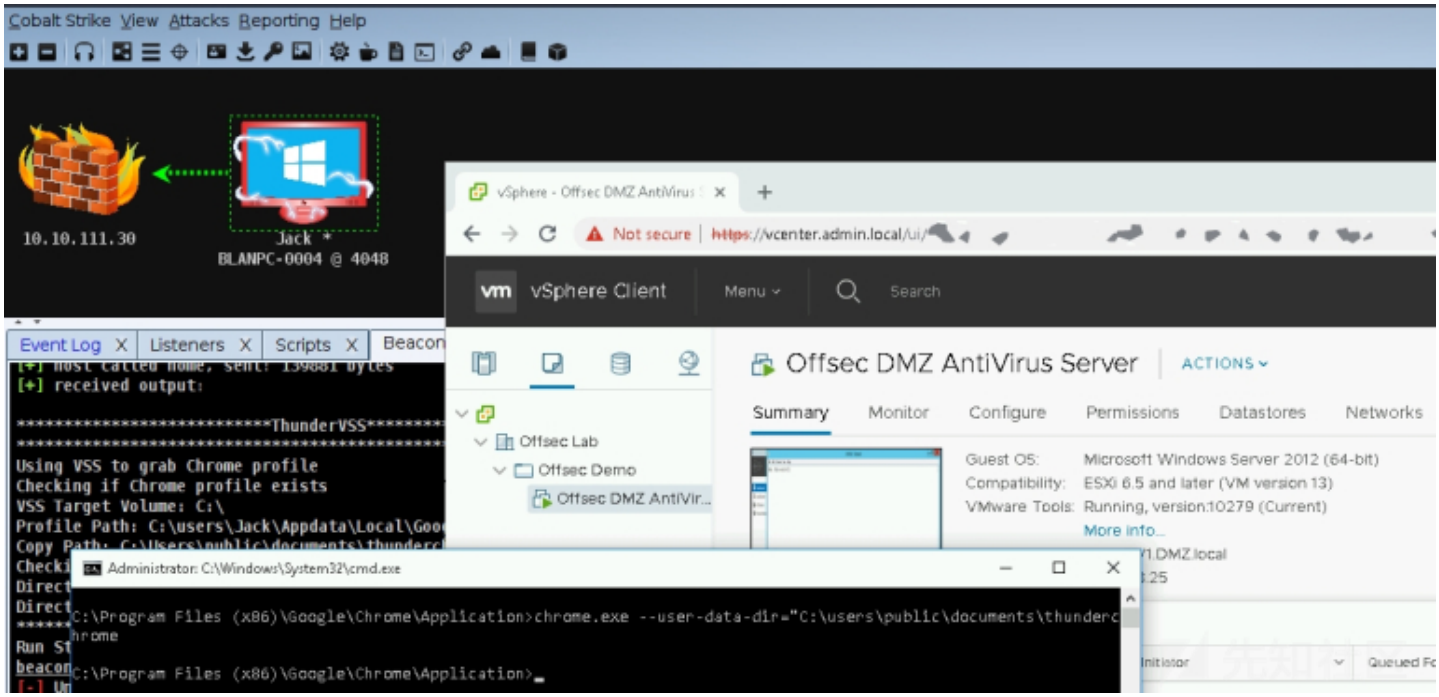
从图5可以看到，Jack在Chrome中建立一个vSphere标签页，我们假设vCenter的会话cookie保存在Jack的Chrome配置文件中。然而，这里面临的主要问题是，当Chrome




```
┌──[✗]─[root@thundergun]─[~]
└──╼ #proxychains xfreerdp /u:jack /app:"C:\windows\explorer.exe" /v:10.10.112.55
ProxyChains-3.1 (http://proxychains.sf.net)
[15:10:42:562] [101547:101548] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[15:10:42:562] [101547:101548] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rail
|S-chain|-<>-127.0.0.1:9000-<><>-10.10.112.55:3389-<><>-OK
Password:
[15:10:50:985] [101547:101548] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[15:10:50:985] [101547:101548] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_RGB16
[15:10:50:987] [101547:101548] [INFO][com.winpr.clipboard] - initialized POSIX local file subsystem
```

将Chrome配置文件复制到C:\users\public\documents\thunderchrome\default\目录中之后，我们可以使用-user-data-dir参数启动一个Chrome实例，该参数指向复制

最后，通过proxychains和RemoteApp，我们就可以劫持vCenter会话了。



点击收藏 | 1 关注 | 1

上一篇：RCE——从一个错别字到获取域管理... 下一篇：Bug Bounty：从SSRF到RCE

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