记一些 CobaltStike 的一些基本操作与说明

作者：Gokourur1
原文链接：https://ld246.com/article/1571209462424
来源网站：链滴

说明

记录的是Cobaltstrike的一些基本操作， 相比较于一些教程，此文章并不会教如何使用，只是一些没去注意的问题。

横向移动

引用一下官方文档

使用 Beacon 的 psexec [target] [share] [listener]在远程主机上执行有效负 载。此命令将为您的侦器生成 Windows 服务可执行文件，将其复制到您指定 的共享，创建服务，启动服务以及自行清除。认共享包括 ADMIN `和 C`。 使用 psexec_psh [target] [listener]使用 PowerShell 在远程主机上执行有效 负载。此命令将创建一个服务来运行PowerShell 单行程序，启动它并自行除。 如果您不想接触磁盘，这种横向移动方法很有用。

一开始以为psh的横向是以被控目标用powershell进行横向，然后发现有的机器却不能上线。随后现攻击目标用powershell上线，对于没ps的机器用第一个横向，或者其他横向方法，而且听说Cs的winm和wmi的横向模块有点问题。

timestomp

引用一下ATT&CK

*Timestomping*是一种修改文件时间戳（修改，访问，创建和更改时间）的技术，通常用于模拟同

文件夹中的文件

引用一下官方文档

使用 timestomp 将一个文件的 Modified，Accessed 和 Created 时间与另一个文件的时间相匹配

简单点说就是修改文件的创建时间那些

使用方法:timestomp 要修改的文件(1.jpg) 匹配的文件(2.jpg)

端口扫描

Beacon有一个内置端口扫描器。

使用portscan [targets] [ports] [discovery method]来启动端口扫描器程序。

您可以指定以逗号分隔的目标范围列表。端口也是如此。

例如，端口扫描172.16.48.0/24 1-1024,8080将在端口1到1024和8080上扫描主机范围172.16.48.0 172.16.48.255。

三种扫描方式:arp icmp none

arp方法使用ARP请求来发现主机是否处于存活状态

icmp方法发送ICMP echo请求来检查目标是否处于存活状态

none选项告诉portscan工具假定所有主机都处于存活状态`

横向移动的一些错误代码

因为psexec横向是基于net use的所以大部分错误都是net use的问题

大部分的问题都是密码错误，或者权限不够和sid不为500（账号密码对却net use 不上），因为08 1以后sid不为500的问题，其他的问题由于目前知识盲区就不知道了

错误号5，拒绝访问： 很可能你使用的用户不是管理员权限的，先提升权限；

错误号51，Windows 无法找到网络路径 : 网络有问题；

错误号53，找不到网络路径： ip地址错误；目标未开机；目标lanmanserver服务未启动；目标有防墙（端口过滤）；

错误号67，找不到网络名： 你的lanmanworkstation服务未启动；目标删除了ipc$；

错误号1219，提供的凭据与已存在的凭据集冲突： 你已经和对方建立了一个ipc$，请删除再连。

错误号1326，未知的用户名或错误密码： 原因很明显了；

错误号1792，试图登录，但是网络登录服务没有启动： 目标NetLogon服务未启动。（连接域控会现此情况）

错误号2242，此用户的密码已经过期： 目标有帐号策略，强制定期要求更改密码。