丢掉PSEXEC来横向渗透

f4a201

Author : Sanr

Editor: qingxp9

0. 前言:

在渗透测试时,很多人还是在使用PSEXEC类工具。PSEXEC类的工具有各种语言的实现,如Metasploit的psexec psexec_psh, Impacket psexec, pth-winexe, Empire Invoke-Psexec, 最早Sysinternals公司pstools工具包当中的psexec。

这些工具都非常出色,但经过这么多年的发展,在各种防御软件环境下psexec类工具很多时候已经无法开展渗透测试工作。

在win下要想执行命令有几种方法:

- IPC上传at&schtasks远程执行
- PSEXEC 这也是用的最多,但是会留下痕迹
- WMI 最安全方法,没有任何知觉,所有window系统启用服务,但防火墙开启将会无法连接
- PsRemoting posershel远程执行命令

1. PSEXEC

PSEXEC执行原理

- 1. 通过ipc\$连接,然后释放psexesvc.exe到目标机器。
- 2. 通过服务管理SCManager远程创建psexecsvc服务,并启动服务。
- 3. 客户端连接执行命令,服务端启动相应的程序并执行回显数据。

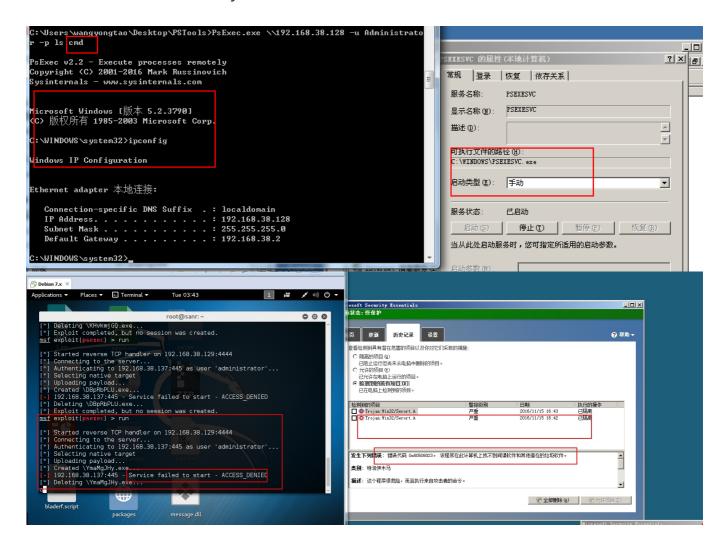
这里描述的是Sysinternals中的psexec,不过MSF、Impacket、pth 工具中的psexec用的都

是同种思路。

为什么丢弃PSEXEC

- psexec类工具会释放文件,特征明显,专业的杀毒软件都能检测到。
- 需要安装服务,会留下日志,并且退出时偶尔会出现服务不能删除的情况。
- 需要开启admin\$ 445端口共享。

在事后攻击溯源时,调查人员会通过日志信息来推测出你的攻击过程。但是它的优点在于,能直接给我们提供目标主机的system权限。



2. 使用WMI来执行命令

WMI 的全称是 Windows Management Instrumentation,它出现在所有的 Windows 操作系统中,由一组强大的工具集合组成,用于管理本地或远程的 Windows 系统。当攻击者使用

wmiexec来进行攻击时,Windows系统默认不会在日志中记录这些操作,这意味着可以做到攻击无日志,同时攻击脚本无需写入到磁盘,具有极高的隐蔽性。越来越多的APT事件中也出现了WMI攻击的影子,利用WMI可以进行信息收集、探测、反病毒、虚拟机检测、命令执行、权限持久化等操作。

最开始我不太喜欢WMI,因为通过WMI执行的命令是没有回显的,这会带来很大的不便。不过在HES2014上有研究者提出了回显的思路,加上psexec类的攻击已被很多的杀软查杀,研究下WMI攻击还是很有必要的。

《WMI SHELL》 - new way to get shells on remote Windows machines using only the WMI service

常见的WMI攻击工具有这些

- PTH-WMIS (最早wmi攻击的工具,单条命令执行,无回显,需要pth-smbget配合读取结果)
- impackets wmiexec(Linux跨window经常用)
- wmiexec.vbs (国人制造 为了回显会写文件)
- Invoke-WmiCommand&Invoke-PowerShellWmi



使用wmiexec.vbs执行命令测试。

```
Desktop\wmiexec-v1_1>cscript.exe wmiexec.vbs /cmd 192.168.3
C: Wsers 🚾
8.137 administrator Wcaonima123 "ipconfig"
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。
WMIEXEC : Target -> 192.168.38.137
WMIEXEC : Connecting...
WMIEXEC : Login -> OK
WMIEXEC : Result File -> C:\wmi.dll
WMIEXEC ERROR: Share could not be created.
WMIEXEC ERROR: Return value -> 22
WMIEXEC ERROR: Share Name Already In Used!
       192.168.38.137 >> ipconfig
Windows IP 配置
以太网适配器 本地连接:
   连接特定的 DNS 后缀
本地链接 IPv6 地址.
                      . . . . . . : localdomain
                                . . : fe80::98c6:4f57:864e:5877%10
  IPv4 地址
                                  .: 192.168.38.137
```

使用impackets wmiexec执行命令测试,执行命令可以回显。在Linux跨window渗透时候经常使用。

```
wmiexec.py administrator:pass@192.168.38.137
```

```
oot@sanr:~/Desktop/impacket-master/examples# wmiexec.py administrator:Wesser
23@192.168.38.137
Impacket v0.9.16-dev - Copyright 2002-2016 Core Security Technologies
INF0:root:SMBv2.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>ipconfig
Windows IP 🗘 🗘 🗘 🗘 🗘
6666666666 66666666:
   စိုင်ပိုင်ပို့ ပိုင်ပို့ DNS ဖိုင်း nearly . : localdomain
   ଡ଼ୖଡ଼ୖଡ଼ୖଡ଼ୖଡ଼ୖଡ଼ୖଡ଼ IPv6 ଡ଼ୖଡ଼. . . . . . . . : fe80::98c6:4f57:864e:5877%10
   IPv4 🚱 . . .
                      . . . . . . . : 192.168.38.137
   000000000
                      . . . . . . . . . . 255.255.255.0
   Ĭ000000. .
                           . . . . . : 192.168.38.2
```

3. 使用PsRemoting来执行命令

PowerShell远程命令执行基于WinRM。WinRM指的是Windows远程管理服务,它会监听http(5985)、https(5986),不过此服务除了Windows Server 2012及R2默认启用外,其他默认都是禁用的。管理员为了方便对服务器的远程管理,也许将此端口开启,这种事就像内网弱口令一样,做渗透嘛,什么奇迹都有可能发生。

利用PowerShell渗透可以绕过杀软、绕过白名单防护设备,并且还可以得到返回的数据,简直是杀人越货神器。但由于默认禁用的原因,在内网渗透测试时,我暂时还未使用过这种技术。

```
Enter-PSSession 192.168.38.137 -Credential administrator
```

4. 总结:

其实说了这么多,在内网渗透的时候更推荐使用WMI。WMI的好处有很多,但WMI也不是万能的,还是需要根据具体的网络环境来调整渗透手法,渗透测试过程中要牢记擦掉自己痕迹,不使用ARP等动静特别大攻击手法。

对于不知道psexec执行会留下什么痕迹的同学可以看看 http://bobao.360.cn/learning/detail/3186.html。昨天刚和同事讨论研究完psexec的执行 过程后便发现这篇文章,但是它没有讲清其执行原理。