Metasploit权限提升全剧终

shuteer / 2017-02-20 13:11:00 / 浏览数 6794 新手 入门资料 顶(0) 踩(0)

0×01 引言

通常，我们在渗透过程中很有可能只获得了一个系统的Guest或User权限。低的权限级别将会使我们受到很多的限制，所以必须将访问权限从Guset提升到User,再到Admini
渗透的最终目的是获取服务器的最高权限，即Windows操作系统中管理员账号的权限，或LINUX操作系统中root账户权限。
提升权限的方式分为两类。

纵向提权：低权限角色获得高权限角色的权限。比如，一个webshell权限通过提权之后拥有了管理员的权限，那么这种提权就是纵向提权。

横向提权：获取同级别角色的权限。比如，通过已经攻破的系统A获取了系统B的权限，那么这种提权就属于横向提权。

所以在成功获取目标机meterpreter shell后，我们要知道现在已经拥有了什么权限。

1. 在meterpreter shell下输入命令shell进入目标机CMD命令行
2. 输入whoami /groups 命令

可以看到这个表是Mandatory Label\Medium MandatoryLevel，说明我们是一个标准用户，需要将用户权限从标准用户提升到管理员权限，也就是Mandatory Label\High MandatoryLevel。
提权大体有以下几种方法：

使用getsystem提升权限
利用本地漏洞
假冒令牌
绕过Windows账户控制（UAC）
HASH

0×02 getsystem

利用meterpreter中的getsystem命令，该命令自动寻找各种可能的适应技术，以便将用户权限提升到更高级别。我们输入getsystem –h
来看下它使用的3种技术，如下图。

默认值0会尝试所有列出技术来尝试提权，直至成功。提权方式采用命令管道模拟提升的方法和令牌复制的方法。输入getsystem命令即完成操作。具体效果见下图。

该命令使用方便，并且简单高效，在渗透测试中会频繁使用到，建议所有提权过程中先行尝试此方法。

0×03利用本地漏洞

本地漏洞提权，即使用本地漏洞的利用程序（loca>exploit）提升权限。就是说通过运行一些现成的造成溢出漏洞的exploit,把用户从users组或其它系统用户中提升到admi
溢出漏洞就像杯子里装水,水多了杯子装不进去,就会把里面的水溢出来。而相对计算机来说计算机有个地方叫缓存区,程序的缓存区长度是被事先设定好的,如果用户输入的数据

1. 利用getuid命令查看已经获得的权限，可以看到现在的权限很低，是个user权限。尝试利用getsystem提权，失败。见下图：

2.输入命令shell进入目标机CMD命令行，再利用systeminfo命令或者通过查询 c:\windows\ 里留下的补丁号.log来看看目标机大概打了哪些补丁。

可以看到目标机基本上没有打任何补丁，我们可以尝试利用Windows下已有的漏洞提权，如ms13_053,ms14_058,ms16_016,ms16_032等等。

相关漏洞的具体信息分析和共享可以参考下面2个网站：

安全焦点，其BugTraq是一个出色的漏洞和exploit数据源，可以通过CVE编号，或者产品信息漏洞直接搜索。网址：http://www.securityfocus.com/bid。
Exploit-DB,取代了老牌安全网站milw0rm。不断更新大量的Exploit程序和报告，它的搜索功能可以搜索整个网站内容。网址：http://www.exploit-db.com。

*附上收集的部分系统对应补丁号 Win2003 Win2008
Win2012

KB2360937|MS10-084
KB2478960|MS11-014
KB2507938|MS11-056
KB2566454|MS11-062
KB2646524|MS12-003
KB2645640|MS12-009
KB2641653|MS12-018
KB944653|MS07-067
KB952004|MS09-012 PR
KB971657|MS09-041
KB2620712|MS11-097
KB2393802|MS11-011

KB942831|MS08-005
KB2503665|MS11-046
KB2592799|MS11-080
KB956572|MS09-012烤肉
KB2621440|MS12-020
KB977165|MS10-015Ms Viru
KB3139914|MS16-032
KB3124280|MS16-016
KB3134228|MS16-014
KB3079904|MS15-097
KB3077657|MS15-077
KB3045171|MS15-051
KB3000061|MS14-058
KB2829361|MS13-046
KB2850851|MS13-053EPATHOBJ 0day 限32位
KB2707511|MS12-042 sysret -pid
KB2124261|KB2271195 MS10-065 IIS7
KB970483|MS09-020IIS6
KB3139914|MS16-032
KB3124280|MS16-016
KB3134228|MS16-014
KB3079904|MS15-097
KB3077657|MS15-077
KB3045171|MS15-051
KB3000061|MS14-058
KB2829361|MS13-046
KB2850851|MS13-053EPATHOBJ 0day 限32位
KB2707511|MS12-042 sysret -pid
KB2124261|KB2271195 MS10-065 IIS7
KB970483|MS09-020IIS6
KB3139914|MS16-032
KB3124280|MS16-016
KB3134228|MS16-014
KB3079904|MS15-097
KB3077657|MS15-077
KB3045171|MS15-051
KB3000061|MS14-058
KB2829361|MS13-046
KB2850851|MS13-053EPATHOBJ 0day 限32位
KB2707511|MS12-042 sysret -pid
KB2124261|KB2271195 MS10-065 IIS7
KB970483|MS09-020IIS6

1. 接着我们输入命令background,就是把你当前的metasploit shell转为后台执行。

4.然后搜索Metasploit中是否有相应的exploit程序，下面以ms16_016（该模块在windows 32位和64位下都有效）为例。

5.通过这个exploit进行提权，具体命令如下图：

我们可以看到成功利用了notepad漏洞，启动了一个PID为708的进程。接着输入PS命令查看目标机进程，找到PID
708这个进程，并且利用migrate命令迁移到该进程中。最后执行getsystem，再次查看权限，看到没有，已经是系统权限了。

0×04假冒令牌

令牌是系统临时密钥，它允许你在不提供密码或其他凭证的前提下，访问网络和系统资源。这些令牌将持续存在于系统中，除非系统重新启动。我们输入use
incognito命令，然后输入list_tokens –u，列出可用token，见下图：

我们可以看到有二种类型的令牌，一种是Delegation
Tokens，也就是授权令牌，它支持交互式登录（比如可以通过远程桌面登陆访问）。还有一种是Impersonation
Tokens，也就是模拟令牌，它是非交互的会话。可看到令牌的数量，取决于我们meterpreter
shell的访问级别。我们可以看到已经获得一个系统管理员的授权令牌，现在我们就是要假冒这个令牌，成功后我们就可以拥有它的权限。接下来我们在incognito中调用imp

运行成功，我们在meterpreter shell下运行shell命令并输入whoami，可以看到我现在就是我们假冒的那个win-57tj4b561mt\administrator系统管理员了。

0×05 绕过Windows用户账户控制（UAC）

在Windows Vista
以及更高的版本中，微软引进了安全控制策略，分为高、中、低三个等级。高等级的进程具有管理员权限，中等级进程拥有一个基本用户的权限，低级别的进程的权限是受
UAC有4种设置要求：

始终通知：这是最严格的设置，任何时候，当有程序要使用高级别权限时，都会提示本地用户。
仅在程序试图更改我的计算机时通知我：这是UAC的默认设置。本地Windows程序要使用高级别权限时，不通知用户。但当第三方程序要求使用高级别权限时，它会提示
仅在程序试图更改我的计算机时通知我（不降低桌面的亮度）：与上一条设置要求相同，但提示用户时不降低桌面的亮度。
从不提示：当用户为系统管理员时，所有程序都会以最高权限运行。
一.使用Bypassuac提权
Bypassuac主要有以下4个模块

1. 我们先看下现在已经获得的权限？该权限能否直接通过getsystem来直接提权？

可以看到是shuteer用户权限，通过getsystem提权提示权限不够，拒绝访问。

2.下面利用bypassuac模块来提权，这里使用exploit/windows/local/bypassuac模块（该模块在windows
32位和64位下都有效），本模块执行成功后将会返回一个新的meterpreter shell，设置如下图：

已经攻击成功，返回了一个session 5的meterpreter shell，此时我们通过sessions 命令可以看到已经有了2个meterpreter shell。

3.执行getuid查看权限，如果发现还是普通权限，不要失望，继续执行getsystem，再次查看权限，已经成功绕过UAC，且已经是系统权限了。

其他几个模块用法和上面一样，原理有所不同，执行成功后都会返回一个新的meterpreter shell，且都需要执行getsystem才能获取系统权限。
使用bypassuac模块时一些注意事项：

使用bypassuac模块进行提权时，系统当前用户必须在管理员组，而且用户账户控制程序UAC设置为默认，即"仅在程序试图更改我的计算机时通知我"。
Bypassuac模块运行时会在目标机上创建多个文件，会被杀毒软件识别。exploit/windows/local/bypassuac_injection模块直接运行在内存中的反射DLL中，所以它不触
Metasploit框架攻击目前没有针对Windows 8的模块

二.使用RunAs提权
这种方法可以利用exploit/windows/local/ask模块（该模块在windows
32位和64位下都有效），创建一个可执行文件，目标机会运行一个发起提升权限请求的程序，提示用户是否要继续运行，如果用户选择"是"，就会触发返回一个高权限的me
shell。设置如下图：

输入run命令后会在目标机上会弹出UAC，提示用户是否运行

选择"是"就会成功返回一个新的meterpreter shell。

同样执行getuid查看权限，发现是普通权限时，继续执行getsystem，再次查看权限，已经是系统权限了。

使用RunAs模块时一些注意事项：

使用RunAs模块进行提权时，系统当前用户须在管理员组或者知道管理员的密码，用户账户控制程序UAC设置则没有要求。
使用RunAs模块进行提权时，会创建一个可执行文件，为了避免给杀毒软件查杀，该可执行文件（需进行免杀处理）的创建要使用EXE::Custom选项。
RunAs攻击的缺点是，程序企图修改计算机设置时，系统会对用户发出提醒。此警报可能会被管理人员认定为攻击。建议多次运行，系统多次对用户发出提醒后，对于缺

0×06 HASH攻击

1.使用hashdump命令
Hashdump
meterpreter脚本可以从目标机器中提取hash值，破解hash值即可获得登陆密码。计算机中的每个账号（如果是域服务器，则为域内的每个账号）的用户名和密码都存储在S
在meterpreter shell提示符下输入hashdump命令，将导出目标机SAM数据库中HASH，见下图：

抓取到的HASH可以使用暴力破解或者使用彩虹列表进行破解，个人建议可以直接到http://www.cmd5.com/或者http://www.xmd5.com/进行破解。
还有一个命令smart_hashdump,可以导出域所有用户的HASH。

2.WindowsCredentials Editor (WCE)或者MIMIKATZ
Windows Credentials Editor (WCE)是一款功能强大的windows平台内网渗透工具，它可以列举登陆会话，并且可以添加、改变和删除相关凭据（例如：LM/NT
hashes）。这些功能在内网渗透中能够被利用，例如，在windows平台上执行绕过hash或者从内存中获取NT/LM
hashes（也可以从交互式登陆、服务、远程桌面连接中获取）以用于进一步的攻击，而且体积也非常小，是内网渗透手必备工具。
先使用upload命令将wce.exe上传到目标主机C盘中，然后在目标机shell下输入 wce –w命令，便会成功提取到系统明文管理员密码。如下图。

MIMIKATZ的使用比较简单，就不演示了！
这2个工具必须要在管理员权限下使用，还要注意工具的免杀。

上一篇：安全盒子沙龙Web议题分享（中/英） 下一篇：Metasploit驰骋内网直取域管首级
1. 0 条回复
- 动动手指，沙发就是你的了！

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