JBoss引起的内网渗透-2

rcoil / 2018-03-15 19:38:25 / 浏览数 17049

切入点

Jboss的反序列化漏洞，接下来看站点信息

正常来说这个admin-console及web-console/都是能正常访问的，就算不能正常访问也不会是404状态 ，所以为了搞清楚原因，去翻了其目录，进行对比,发现:

```
server\default\deploy  #■■■■war■■
server\web\deploy  # ■■war■■■■■■■■■■
```

两个目录中，在\web\deploy\中缺少了admin-console和web-console，所以原因是：管理员在安装了JBoss后，为了安全起见，就在server\web\deploy删除了ad
所以接下来就进行常规的war部署，发现war已经上传上去了，但是访问出现404，所以跑去server\web\deploy查看，发现是没有生成相对应的文件夹，原因暂时未知。

所以就直接将jsp脚本上传到了jmx-console.war当中，成功获取WebShell

```
server\default\deploy\jmx-console.war\  # ■■■■■■■
server\web\deploy\jmx-console.war\  # ■■■■■■■
```

信息收集

接下来又是常规的信息收集

发现在菜刀里面执行命令，多数都是超时状态，所以还是回到之前的工具进行执行或是上传个命令执行马或是用web访问马。

进程里面是存在avguard.exe，所以需要做免杀。

在查看环境变量的时候发现是存在powershell的,但是没起作用。

```
net user #■■■■■■■
-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
postgres                 saverio                  SUPPORT_388945a0

net group "domain admins" /domain  #■■■■■■■
-------------------------------------------------------------------------------
Administrator            bckagent                 dbagent
faxmaker                 idsmessina               lattuca
SpaceGuardSvcAccnt       trovato                  VMwareVDPBackupUser

net group "domain controllers" /domain  #■■■■■■■
-------------------------------------------------------------------------------
DOMAIN1$                 DOMAIN2$

■■■■■■■■■■■■■■■
```

信息收集到这里，就有些蹊跷，因为本机用户里面，除了Administrator存在于域用户中，其余的账户均不见，所以这里能直接判断Administrator就是域管理员。

综合以上信息：

```
DOMAIN2 - 192.168.20.10 # ■■■■■
PROTRIBUTCT -Administrator # ■■■■■
avguard.exe # ■■■■■■
powershell # ■■■
```

小小免杀

续上次的shellter免杀，是过不了小红伞的，所以，这种时候，该储备的东西就起作用了。

生成一个Metasploit的马，去Virustotal做测试免杀，是过了AVG的，所以尝试一波。但是，生成的exe在windows
7下面是能正常执行的，但是到了xp上面就不行了。

用Veil生成个吧，安装Veil也是个大坑，图就不放了。

横向内网

接下来思路就很明确了。将PROTRIBUTCT的密码dump下来，幸运的话整个域就能拿下来了。

至此，这个域已经拿下，比上篇难度相对来说要小一些。

还有一个点，就是在查看域控的时候发现是有两台的，也是一样的登陆方式进行登陆即可。但是在这两台域控执行`net view /domain:xxxxx`结果都是不一样的，这也许就是两台域控的缘故吧。但是DOMAIN1所在的段只能通过DOMAIN2出来，其他机器做跳板均没数据，或许这是玄学了吧。

至此，整个测试流程就结束了。整个过程有点顺利，不是我发blog的初衷。

首发于个人博客

上一篇：代码审计之DM建站系统 下一篇：翻译 MySQL UDF Expl...

1. 3 条回复

master 2018-03-15 19:47:57

666，有时候对于企业来说域是个很好的东西，但是对于安全研究人员来说，拿到域管理，基本上内网可以通行无阻了，我还是觉得工作组的机器相对来说安全一点。

0 回复Ta

master 2018-03-15 19:48:20

LZ是个内网渗透大神。

0 回复Ta

rcoil 2018-03-16 12:42:06

说明：
本文中有个错误的概念验证，在判断域用户的时候不能这么判断的，是不合理的。主要原因是在实操的时候，刚好能够使用Administrator用户密码登陆域，所以文章中就

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