登录

Linux版"永恒之蓝”（CVE-2017-7494）复现过程分析

嘶吼roartalk / 2017-06-01 07:22:02 / 浏览数 2578 安全技术 技术讨论 顶(0) 踩(0)

0x01.开始

睡觉睡的正香，在梦里正在做一些不可描述的事情，就被一边的手机吵醒了，真的很想把手机砸掉，但是又舍不得，好几个月的工资呢。拿起来看了看。群里的大牛们开始讨

0x02 各种失败

当我拿到这个漏洞的时候，做了大量的测试，攻击环境用的是Kali，靶机为ubuntu16.04、centos6.5等等。但是测试了一天，没有一次攻击成功，之前写了一篇关于这个漏

可以说成功么?当然不能，环境都是别人配置的，用别人配置的环境去复现显得多么的low啊。总之，各种环境失败，没有成功。看到了freebuf上的复现方法，讲真，真的不

0x03 辛酸过程

可以说进入正文了，先附上github的msf利用地址：点我

把它复制回来，或者用wget命令下载回来，移动到msf的目录中去

```
mv is_known_pipename.rb /opt/metasploit-framework/embedded/framework/modules/exploits/linux/samba/is_known_pipename.rb
```

之后查看本地ip，并打开metasploit

再看一眼靶机ip

执行reload_all，重新加载全部文件。

```
use exploit/linux/samba/is_known_pipename

Set rhost 192.168.12.104

Set target 3
```

按照别人说的方法，直接执行exploit就可以完成本次攻击，但是事实往往不是跟想象中的一样,

没有会话返回，我想了很久，换了各种环境来测试，但是很幸运，我一个都没有成功，无意之间想到了一个，本机测试。

直接攻击地址换成了kali的ip地址

```
set rhost 192.168.12.103

Set target 3

Exploit
```

很是神奇，但是还是没有想明白原因是什么

0x04老外相助

翻着国外的各大论坛，想着这个原因到底是什么，无意间翻到了推特上一个老外发的推文，说他成功了。

于是我就问他：“你的samba配置是怎么写的？”

老外：“一张图片”

但是我设置了这个配置仍然没有成功，我又问他：“我设置了跟你相同的配置，但是仍然没有成功”

老外：“exploit is working against 2:4.2.14+dfsg-0+deb8u5, does not work on 2:4.5.8+dfsg-1”

兄弟们，原谅我，我实在不知道这么怎么翻译了，我跟他交流都是靠着google翻译的。

虽然不是很明白老外的意思，但是连蒙带猜知道老外是想告诉我，我的版本是有问题的，但是不是samba的版本有问题。

我发现老外的攻击成功的系统是debian8.8，于是正准备安装debain的虚拟机，脑海里一个灵光，对调攻击机与靶机的攻防位置。简单说，就是用ubuntu去入侵kali。

攻击成功!

0x06 闲扯篇—-环境搭建

很多人纠结环境搭建这个东西，所以就在这里说一下。因为我也纠结了许久- -!攻击不成功，总是在怀疑是不是我samba环境搭建的有问题。

Ubuntu为靶机的环境:

```
sudo apt-get install samba
```

安装完成之后修改配置文件就行

```
sudo gedit /etc/samba/smb.conf
```

在文件末尾增加

```
[test]
path = /tmp
writeable = yes
browseable =yes
guest ok =yes
read only = no
create mask = 777
```

配置完成之后重启就好

```
sudo service smbd restart
```

Kali为靶机的环境：

Kali
默认是什么都有的，并不需要安装，直接添加配置文件，之后重启服务就行，不详细说明，参照ubuntu配置，其它类型的linux机器，参照ubuntu配置环境搭建

0x07 总结

光是单单复现这样一个简单的漏洞，就用了一天，可以说是很要命的东西，可能我复现的这一天，全球ip就不知道被扫了多少遍了。还是慢了老外一步。关于这个漏洞的复现

Qq群:617086434，这个漏洞的复现还有问题的可以在群里问，当然，没问题做别的技术交流也是没问题的，啊哈哈。只要你愿意来！

0x08 偷懒到极致

Docker复现方法：你真的要偷懒么

如若转载，请注明原文地址： http://www.4hou.com/technology/4983.html

上一篇：先学会利用工具，然后再编程？ 下一篇：PR的盛宴之下，不能缺席的是技术的...
1. 0 条回复
   - 动动手指，沙发就是你的了！