**NFS服务安全加固**

**漏洞描述：**

NFS（Network File System）：是FreeBSD支持的文件系统中的一种，它允许网络中的计算机之间通过TCP/IP网络共享资源,不正确的配置使用NFS，会造成安全问题。

NFS的不安全性主要体现于以下4个方面:

缺少对NFS的访问控制机制;

NFS没有真正的用户验证机制,而只有对RPC/Mount请求的过程验证机制 ;

较早的NFS可以使未授权用户获得有效的文件句柄

在RPC远程调用中,一个SUID的程序就具有超级用户权限.

**加固方案：**

**1.合理的设定/etc/exports**

配置共享目录使用 anonuid,anongid以使MOUNT到NFS SERVER的CLIENT仅仅有最小的权限,不要使用root\_squash。

**2.网络访问控制**

使用[安全组策略](https://help.aliyun.com/document_detail/25475.html?spm=5176.doc25470.6.204.SlE11A)或IPTABLE防火墙限制能够连接到NFS SERVER的机器范围

iptables -A INPUT -i eth0 -p TCP -s 192.168.0.0/24 --dport 111 -j ACCEPT

iptables -A INPUT -i eth0 -p UDP -s 192.168.0.0/24 --dport 111 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP -s 140.0.0.0/8 --dport 111 -j ACCEPT

iptables -A INPUT -i eth0 -p UDP -s 140.0.0.0/8 --dport 111 -j ACCEPT

**2.账号认证**

使用Kerberos V5作为登陆验证系统，所有访问人员均需要使用账号登录，提高安全性。

**3.NFSD COPY数设置**

Linux中的NFSD的COPY数目是在/etc/rc.d/init.d/nfs这个启动文件中设置的，默认是8个NFSD,对于这个参数的设置一般是要根据可能的CLIENT数目来进行设定的，和WSIZE、RSIZE一样也是要通过测试来找到最近的数值。

可以手动进行设置，也可以自动进行选择。

mount -t nfs -o sync,tcp,noatime,rsize=1024,wsize=1024 EXPORT\_MACHINE:/EXPORTED\_DIR /DIR

UDP有着传输速度快，非连接传输的便捷特性，但是UDP在传输上没有TCP来的稳定，当网络不稳定或者黑客入侵的时候很容易使NFS的Performance 大幅降低甚至使网络瘫痪。

所以对于不同情况的网络要有针对的选择传输协议。nfs over tcp比较稳定，nfs over udp速度较快。在机器较少网络状况较好的情况下使用UDP协议能带来较好的性能，当机器较多，网络情况复杂时推荐使用TCP协议（V2只支持UDP协议）。在局域网中使用UDP协议较好，因为局域网有比较稳定的网络保证，使用UDP可以带来更好的性能，在广域网中推荐使用TCP协议，TCP协议能让NFS在复杂的网络环境中保持最好的传输稳定性。

**4.Client数量限制**

修改/etc/hosts.allow和/etc /hosts.deny达到限制Client的目的

/etc/hosts.allow

portmap: 192.168.0.0/255.255.255.0 : allow

portmap: 140.116.44.125 : allow

/etc/hosts.deny

portmap: ALL : deny

**5.改变默认的NFS 端口**

NFS默认使用的是111端口,但同时你也可以使用port参数来改变这个端口,这样就可以在一定程度上增强安全性.

**6.nosuid和noexec选项**

SUID(Set User ID)或SGID(Set Group ID)程序可以让普通用户以超过自己权限的形式执行。很多SUID/SGID可执行程序是必须的，比如上面提到的passwd。SUID/SGID程序会被一些恶意的本地用户利用，获取本不应有的权限。

尽量减少那些所有者是root或是在root组中却拥有SUID/SGID属性的文件，删除或对其属性进行更改。使用nosuid选项禁止set-UID程序在 NFS服务器上运行，可以修改文件/etc/exports加入一行：

/www www.abc.com(rw, root\_squash, nosuid)