

原

Linux安全基础——day1

2018年11月05日 22:38:21Lu-Yu 阅读数：1 标签：Linux安全设置ssh设定更多

个人分类：Linux安全与监控

0

- 进行安全配置的思路
- 1. 非技术手段：管理制度(核实设备安全、网络物理连接)（社会工程学）
 - 2. 技术手段：系统安全(权限限定) 服务安全(优化，高可用) 数据安全(备份) 网络安全(加密)

/etc/passwd	用户信息
/etc/shadow	用户密码数据(加密过)
/etc/group	组信息
/etc/gshadow	组密码
/etc/skel/*	添加用户初始环境配置文件，有不少隐藏文件
	这文件夹下的所有文件，再创建用户后，其加目录下就有什么
/etc/profile/	系统配置文件，定义环境变量等信息
/etc/login.defs	添加用户时候如果没有指定信息的时候，设定的默认参数
/etc/issue	决定用户登陆纯字符界面的时候，会出现什么样子的介绍页面

用户安全

相关信息的设定命令

useradd	添加用户
userdel	删除用户（如果使用量参数-r，那么就删除用户的同时删除家目录）
usermod	修改用户信息(-G修改所属组)
chage -l 用户	查看用户的设置信息(用chage设定的信息)
chage -d 天数 用户	设置用户自命令开始计算，多久时间内要修改好密码，不然不能进行任何操作
	如果天数为0，那么用户一旦登陆，必须立刻设置密码
chage -E yyyy-mm-dd 用户	设置用户失效日期，时间到了，用户就会被锁定
	如果年月日那里写成 -1 那么就是永久保留
chage -m 天数 用户	在密码更改之间的最小天数设置，默认天数为 0
	天数为 0 时，表示用户可以在任何时间更改其密码。
passwd 用户	设置密码(--stdin代表非交互设置密码)
passwd -l 用户	锁定用户，锁定后用户不能登陆，在/etc/shadow文件中的密码项前会多处两个叹号作为标识
	这会导致用户将无法通过密码进行登陆，相当于让密码暂时失效，不过密钥还是可以进行登陆等操作
passwd -u 用户	解锁用户
passwd -S 用户	查看用户密码相关信息，第二列是LK是用户被锁定了，如果是PS那就是非锁定
passwd -d 用户	删除用户密码(删除后，用户将无法被远程登陆)

登陆后被强制设定密码的注意点：

- 1. 密码必须符合复杂性要求
- 2. 密码不能包含用户名
- 3. 密码错误超过3次，会弹出
- 4. 密码设定成功后，也会弹出，再次登陆就是使用新密码了

特例：

如果root用户，被锁定了，这时候就没办法登陆root了，而只有root可以解锁，这就成了一个死循环，root被锁不能登陆，而想解锁必须先登陆root，解如下：

首先，我们在做锁操作前必须思考再三，而且锁后也要确认一下，因为锁用户不会强制下线，所以操作要谨慎
再之，如果已经出现问题了，那就看看能不能通过密钥登陆，如果可以，那就可以补救
或者，就看也没有某个用户之前赋予了以root身份使用passwd *的权限，通过其实现
最后，前面的办法都没用，就重启机器，然后进入抢救模式，和破解root密码差不多的操作，然后解锁root，问题解决

文件系统安全

锁定文件

对EXT3/EXT4文件属性控制

```
1 | chattr  +=属性          # 修改
2 | lsattr          # 查看文件属性
```

控制	
+	在原来的的文件属性上添加一个属性，原来属性不变
-	在原来的的文件属性上删除一个属性，如果没有，该操作无意义，不过不报错
=	清空原来文件中所有属性，把=后面的属性加入
	如果=后面为空，其作用就是清空文件属性
属性	
	空代表没有特殊控制
i	不可变，不能进行任意的写操作，不能mv、rm等
a	仅仅可以追加，只能用 >> 进行重定向追加操作
c	文件在磁盘上由内核自动进行压缩处理

注意： 当一个文件属性中有i和a两个属性的时候，将只有i的作用， a的权限将被忽略

```
1 | [root@client50 ~]# chattr =a /mnt/test.txt
2 | [root@client50 ~]# lsattr /mnt/test.txt
3 | -----a----- /mnt/test.txt
4 | [root@client50 ~]# echo 1> /mnt/test.txt
5 | -bash: /mnt/test.txt: 不允许的操作
6 | [root@client50 ~]# echo 1>> /mnt/test.txt
7 | [root@client50 ~]# chattr +i /mnt/test.txt
8 | [root@client50 ~]# lsattr /mnt/test.txt
9 | -----ia----- /mnt/test.txt
10| [root@client50 ~]# echo 1>> /mnt/test.txt
11| -bash: /mnt/test.txt: 权限不够
12| [root@client50 ~]# chattr = /mnt/test.txt
13| [root@client50 ~]# lsattr /mnt/test.txt
14| ----- /mnt/test.txt
```

控制服务

RHEL6	RHEL7	作用
service 服务 start	systemctl start 服务	开启服务
service 服务 stop	systemctl stop 服务	停止服务
chkconfig 服务 on	systemctl enable 服务	开机自动启动服务
chkconfig 服务 off	systemctl disable 服务	不开机自动启动服务

登陆安全

whoami	查看当前用户
su 用户	切换用户，当前所在目录不变，shell环境不变(\$PATH等)
su - 用户	切换用户，并且当前所在目录切换到用户的家目录，以及shell环境
su - 用户 -c "命令"	不切换用户，只是切换用户的shell环境，执行命令，然后返回命令返回值
tail -f /var/log/secure	动态监听用户相关的所有操作

很多时候，告知他人某个用户密码会使其拥有用户的所有权，尤其是root，但是有的时候我们又需要把root部分权限分享给某写用户，这时候，就涉及到了提权操作

提权操作，全程提升权限执行操作，也就是root根据需求对个别用户赋予提权操作的权限，之后用户就可以以指定用户的权限执行某些操作
举个例子，加入root赋予用户user2可以以用户user的身份执行 vim /home/user/*，那就意味着，user2可以在登陆自己的账户。然后修改原来自己不能的/home/user/目录下所有文件。

which 命令	查找到命令的绝对路径
visudo	管理员配置提权的命令
vim /etc/sudoers	
sudo -u 用户 命令	根据管理员设定的提权信息，以命令中-u后面用户的身份运行后面的命令
	不写 -u 用户 则 等效于 -u root，也就不指定用户，默认以root身份
	所有操作都一定要注意必须是管理员设置量提权的才可以
sudo -l	列出当前用户所有可以使用的提权操作

设置提权其实就是修改配置文件，而且修改后立刻生效

/etc/sudoers的详解

```
1 # 可以设置别名
2 Host_Alias 设置主机的别名 = 主机名1, 主机名2
3 User_Alias 设置用户、组的别名 = 用户1, 用户2 ,%组1 .....
4 Cmnd_Alias 设置命令的别名 = (用户1)命令1, (用户2)命令2
5
6 用户别名 主机别名=命令别名
7
8 # 在配置文件中有注释，写了一部分命令的别名，比如，下面就是软件包操作的命令集合的别名
9 ## Installation and management of software
10 # Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum
11
12 ## Allow root to run any commands anywhere
13 root    ALL=(ALL)        ALL
14 提权的用户名      localhost,主机名=(用户)命令的绝对路径 相关参数 , (用户)命令的绝对路径 相关参数
```

```
15 | 16 | # 每行行首 如果由%开头代表后面操作的是一个组，不过必须先注释wheel那行，因为赋予一个组root全部权限很不安全
17 | ## Allows people in group wheel to run all commands
18 | # %wheel ALL=(ALL)        ALL
19 | %提权用户组                localhost,主机名=(用户)命令的绝对路径 相关参数 ,(用户)命令的绝对路径 相关参数
20 |
21 | # 开启日志记录功能，所有用户用sudo进行提权操作都会记录下来
22 | Defaults logfile="/var/log/sudo"
```

- 注意：
- 1.使用的时候可以不用写绝对路径，但是配置的时候必须是命令的绝对路径
 - 2.配置文件中，相关参数可以用*，来做通配任意多个任意字符
 - 3.如果想用多个组，设置User别名，只需要在每个具体组名前加上一个%即可

ssh远程登录控制

控制其他机器远程访问本机器，提高安全性

修改配置文件/etc/ssh/sshd_config

配置信息	功能解释
Port 端口	设置ssh监听的端口，修改成非22端口，别的机器远程，就要 ssh -p 端口 IP 才可以登录量
	默认是注释了的，因为没有指定的时候是22端口
ListenAddress 其他服务器IP列表	设置允许远程访问来的的机器的IP列表
	默认也是注释的，没有定义的时候，默认允许所有的IP远成分访问
PermitRootLogin yes	是否允许root远程登陆，如果是no就是不允许
	默认被注释量，没有定义的时候，默认是yes，也就是允许root远程登陆
LoginGraceTime 2m	登陆限制时间，也就是用户输入密码等待时间太久，服务器会断开
	这样不管密码对不对输入密码超时都会拒绝连接
MaxAuthTries 6	设定最大密码验证次数
	不过当设定值超过3的时候，也值能输入错误3次，否则报错
AllowUsers 用户1@登陆使用的主机IP 用户1	设置白名单，只有通过指定的指定的主机登陆对应的用户才能登陆成功
	如果没有@，默认是允许所有的主机登陆该用户访问
AllowGroups 组名1 组名2	设置组内所有成员的一个白名单
DenyUsers 用户1@登陆使用的主机IP 用户1	设置黑名单，只要用户不以指定的主机登陆指定用户就可以正常登陆
	如果没有@，默认是不允许所有的主机登陆该用户访问
DenyGroups 组名1 组名2	设置组内所有成员的一个黑名单
PasswordAuthentication yes	指定能否用密码登陆，默认是yes，也就是允许的
	如果改为no，那么远程访问值能通过密钥进行连接

- 特例：
- 1. 当AllowUsers和DenyUsers同时存在，不管哪个在前哪个在后，都是只要Deny明确拒绝了某个用户，这个用户就不能登陆，而AllowUsers列表以外的是不能登陆的
 - 2. 当一个用户属于一个组，这个组设置允许登陆，用户设置不能登陆，结果这个用户是不能登陆，这个用户设置允许登陆，组设置不能登陆，结果这个不能登陆，总结下来对于一个用户，不管其对其所属组还是直接对用户，Deny会覆盖Allow的设置

举例：假设当前有3个用户：tes1、test2、test3； test1和test2属于组test，test3没有所属组

配置文件中的内容	test1能否登陆	test2能否登陆	test3能否登陆

AllowUsers test1	能	不能	不能
AllowGroups test	能	能	不能
AllowUsers test3	能	能	能
AllowGroups test			
DenyUsers test1	不能	能	能
DenyGroups test	不能	不能	能
DenyUsers test3	不能	不能	不能
DenyGroups test			
AllowUsers test1 test2	不能	能	不能
DenyUsers test1			
AllowGroups test	不能	能	不能
DenyUsers test1			
AllowUsers test1 test2	不能	不能	不能
DenyGroup test			
AllowUsers test1 test3	不能	不能	能
DenyGroup test			

密钥登陆

原理：

配置过程：客户端生成公私钥对，然后把公钥发给服务端，服务端接收合并到自己的authorized_keys文件中

验证过程：客户端登陆的时候发送请求，服务端查看自己的公钥进行加密把随机临时密码发给客户端，客户端用私钥解密，然后通过解密的密码进行验证

配置：

生成密钥对： ssh-keygen ，然后一直回车即可

将公钥发给服务端： ssh-copy-id 服务端IP地址

设置完密钥配置，就可以免密登录，然后如果ssh设置了，不能通过密码登录就只能用这个免密登录进行远程操作。

我和8个程序员聊了一下午，攒齐这些了观点...

如今，所有的互联网企业都在试图 AI 化，众所周知，技术的竞争归根结底表现为人才的竞争，所以说到底，还是人才供需不平衡



想对作者说点什么

大数据第一季--java基础（day1）

大数据第一季--java基础（day1）

linux基础学习-day1 - 天马流欣(时间花在哪，哪就要有成绩~)

绝对路径：cd /home/python 相对路径：cd Downloads . 表示：当前那路径 ..表示：...

来自： 天马流欣

linux的一些基本安全策略 - phpchandler(分享，学习，进步)

禁用ROOT远程 # vi /etc/ssh/sshd_config 把PermitRootLogin yes 改成 PermitRo...

来自： phpchandler

Python全栈学完需要多少钱？

零基础学爬虫，你要掌握学习那些技能？需要学多久？

Unix/Linux文件系统安全 - shaoqunliu的博客

601

文件系统安全：文件系统安全是Unix/Linux系统安全的核心，文件系统用来控制谁能... 来自： ShaoqunLiu的...

【安全牛学习笔记】Kali Linux基本工具 - edu_aqniu的博客

194

基本工具 netcat (nc: 网络工具中的瑞士军刀) 小身材' 大智慧 使用: nc -h 查看参... 来自： edu_aqniu的博客

下载

linux鸟哥私房菜2

06-27

linux基础 linux服务 linux安全

下载

雄鹰Linux教程

06-07

Linux 基础 Linux 技巧 Linux 安全 Linux 漏洞 Linux 相关

下载

linux学习资料

02-17

linux,linux基础, linux命令, linux文件系统, linux安全



免费云主机试用一年

百度广告

NOIP2013提高组Day1 解题报告 - sxybiglawisgood的博客

943

(同步个人博客 http://sxysxy.org/blogs/37 到csdn)总的来说NOIP2013Day1的这三道... 来自： sxybiglawisgoo...

文章热词 linux没有启用的源 linux系统1.0.0 linux select 源码 linux 查看磁盘io linux数据库删不掉

相关热词 linux . linux .. linux [[linux的at linux 与

【JZOJ5698】【GDOI2018 day1】密码锁（lock）（差分） - qq_365511...

218

Problem 给出一个长度为n序列a，其中的每个数在0到m-1之间。每次操作可以... 来自： qq_36551189的...



天马流欣

关注

24篇文章



phpchandler

关注

7篇文章



ShaoquLiu

关注

102篇文章

ZJOI2017Day1题解（真·抄标解） - wzf_2000的博客(博客已搬迁，请查看...

1212

ZJOI2017Day1题解 来自： wzf_2000的博客

LOJ 6100 「2017 山东二轮集训 Day1」第一题 - 无尽(the road ahead will...

770

可持续化线段树+二分注意到如果[l,r]不降，[l,r-1]就肯定也不降，因此如果能对于每... 来自： 无尽

牛客国庆集训派对Day1——题解 - scar_halo(比代码复杂的、是人心)

252

来自： Scar_Halo

新的赚钱内情曝光，网友：白玩这么多年手机了！
爱顺 · 猿猴

牛客国庆集训派对Day1（A、C、E、L） - hpu-辞树(既见君子，云胡不喜?)

53

A Tobaku Mokushiroku Kaiji #pragma GCC optimize(2) #include <bits/stdc++.h>... 来自： HPU-辞树

基础day1 - l_lichen的博客

55

基础day1 面向对象的实质就是合理的划分变量的作用域 编程就是问题的分解，把大... 来自： L_lichen的博客

loj 6030「雅礼集训 2017 Day1」矩阵 - rising_shit的博客(bzoj yyxzhj, ...

304

loj 6030「雅礼集训 2017 Day1」矩阵 来自： Rising_shit的博客

2018牛客国庆集训派对day1 J Princess Principal（思维or线段树，RMQ...

102

题意大致是给出一个括号序列，然后给出多组询问，每次判断一个区间里的括号是否... 来自： 自己选择的路，...

[下载](#) **鸟哥的Linux私房菜.part1.rar**

12-18

初学者Linux入门的经典文档，详细准确全面 包括 Linux基础文件 Linux架设安全 Linux安全 Solari

**零基础英语**

百度广告

[下载](#) **linux培训教材ppt文档**

05-19

某公司内部linux培训教材 linux 基础，安全，服务器架设等===

NOIp2017 提高组 Day1 T2 时间复杂度 - allen yuk-tak lee 's blog(半年oi一... 👁 291

裸模拟，代码量超大。。。 来自: [Allen Yuk-Tak L...](#)

bzoj #6029.「雅礼集训 2017 Day1」市场 线段树 - beginend(只要在路上... 👁 108

题意 给一个长度为n的序列，要求资瓷区间加，区间整除和求区间最小值，区间和。... 来自: [beginend](#)

网络安全—Web安全基础 - wchstrife的博客 👁 817

本博客题库来源于 实验吧使用Sqlmap进行SQL注入1. 搭建python2.7的环境2. 启动S... 来自: [WchStrife的博客](#)

linux安全策略! - 天涯路的专栏 👁 1092

1. 重要数据完整性.(Tripwire或者其它替代品AIDE) 2. 入侵检测系统(SNORT+... 来自: [天涯路的专栏](#)

广州24岁美女辞职在家赚钱，如今环游世界！

北京谷汉 · 熈熈

NOIP2016提高组Day1题解 - zigzagk的博客(never give up fighting!) 👁 961

NOIP2016提高组Day1题解。 来自: [ZigZagK的博客](#)

Linux安全加固——第一篇 - fly_鹏程万里(专注于it技术，只做it技术的分享... 👁 866

Redhat是目前企业中用的最多的一类Linux，而目前针对Redhat攻击的黑客也越来越... 来自: [Fly_鹏程万里](#)

[下载](#) **网络安全基础+网络攻防、协议与安全.pdf**

06-16

本书从网络攻防、协议与安全解决方案的角度阐述网络安全，把网络看成安全与不安全的源头。全书共分为四部分，第一部分讨论网络概念与威胁的入门知识，分别介绍了网络体系...

NOI2018 Day1 归程（Kruskal重构树） - czl_233的博客(一个蒟蒻~) 👁 218

题意： 题解： 题意： 本题的故事发生在魔力之都，在这里我们将为你介绍一些必要... 来自: [czl_233的博客](#)

Linux安全基础 - 建伟博客(记录工作) 👁 1055

一、帐户密码策略 a) 密码长度需要 8 位以上（强制） b) 密码应同时使用英文，数... 来自: [建伟博客](#)

**发现了一个免费的云服务器,号称是永久的**

百度广告

[下载](#) **LINUX帐号安全基础**

12-19

LINUX帐号安全基础,包括:选择安全的口令,口令机制,帐号管理.....

linux基础安全加固 - maxsun321的博客(白茶清欢无别事，我在等分也等你) 👁 116

这里介绍一下最基础的linux服务器安全加固 1禁止root用户远程登录 vi /etc/ssh/sshd... 来自: [Maxsun321的博客](#)

[下载](#) **鸟哥的Linux私房菜**

04-15

适合于Linux初学者.包括linux基础文件、linux架构文件、linux安全

【NOIP 2017 提高组 DAY1 T2】时间复杂度 - forever_dreams的博客(wher... 👁 53

算法标签：模拟+栈 来自: [forever_dreams...](#)

牛客day1 - 火锅——博客(在路上)153

1.关于不同类型数据计算：自动转换为最高的，如果int与float或double 型数据进行...来自：火锅——博客

戒烟的好方法，戒烟用这个方法坚持三个月轻松恢复！
喜雁居健康 · 戒烟

NOIP2012 提高组 复赛 day1 game 国王游戏 再见 - mrcrack的博客876

NOIP2012 提高组 复赛 day1 game 再见 2017-1-15 20:48 1.经过近半年的历练，重...来自：mrcrack的博客

【安全牛学习笔记】Kali Linux渗透测试介绍 - edu_aqniu的博客1055

Kali Linux渗透测试介绍 安全问题的根源 优点：分工明确，工作效率高。 ... 来自：edu_aqniu的博客

WEB安全基础-WEB通信 - it1995的博客(博主qq570176391，qq78442761)783

1.URL（Uniform Resource Locator）协议：就是站点连接;支持多种协议：HTTP、...来自：IT1995的博客

转转：解决Error"基础连接已经关闭: 未能为SSL/TLS 安全通道建立信任关...1260

随笔- 129 文章- 0 评论- 28 转转：解决Error"基础连接已经关闭: 未能为SSL/TLS ...来自：cxzhq2002的杂记

基础连接已经关闭: 未能为 SSL/TLS 安全通道建立信任关系。 - 学习笔记(...1.1万

1,先加入命名空间： using System.Net.Security; using System.Security.Authenticati...来自：学习笔记

新的赚钱内情曝光，网友：白玩这么多年手机了！
爱顺 · 戒烟

牛客国庆集训派对Day1 I Steins;Gate（原根 + FFT） - alpc_qleonardo(alp...91

上一次用到原根这个东西，应该是一年之前了吧..... 所谓原根，就是指对于某个...来自：alpc_qleonardo

A. 【NOIP2018 模拟赛day1】古代密码 - to the moon(如果我们都迷路或...554

这道题一开始读的时候以为是深搜，仔细一想可以发现-----尼玛这道题为什么需要去...来自：To the moon

【NOIP2014提高组】【Day1】【解题报告】 - sunshinezff的专栏2018


T1:生活大爆炸版石头剪刀布 题目链接：http://codevs.cn/problem/3716/ 题解:预处理...来自：sunshinezff的专栏

解决基础连接已经关闭: 未能为 SSL/TLS 安全通道建立信任关系 - gzeehg...8410

1,先加入命名空间： using System.Net.Security; using System.Security.Authenticati...来自：gzeehg007的博客

C#模拟HttpRequest时出现 基础连接已经关闭 未能为 SSLTLS 安全通道建立...1400

https://www.cnblogs.com/ianunspace/p/5508179.html //解决方法： //引入命名空间...来自：soarheaven的专栏



上班玩手机，不如学英语✓
不用死记硬背,试试极简英语学习法

下载 NOIP2015 Day1试题07-26

NOIP2015 Day1试题 全国信息学奥林匹克联赛 2015 noip day1

LibreOJ #6030.「雅礼集训 2017 Day1」矩阵 乱搞 - beginend(只要在路上...64

题意 现在有一个n*n的01矩阵，现在每次可以把某一列替换成某一行，问最少操作次...来自：beginend

牛客国庆集训派对Day1 L New Game!(SPFA) - 咸鱼有梦想47

题意： 有两条直线，n个圆，让你从一条直线走到另外一条直线，问你最少需要花...来自：咸鱼有梦想

下载 JavaScript基础复习大纲09-10

JavaScript基础复习大纲DAY1,很好，很强大，还有下半部分

下载

Java基础视频-深入浅出精华版视频

Java基础视频-深入浅出精华版视频.day1~~day27 很好很实用的...

07-21

Lu-Yu

原创77

粉丝18

喜欢4

评论1

等级：

博客

访问：1万+

积分：869

排名：6万+

勋章：

恒

1024



特斯拉suv



最新文章

Linux数据库管理——day15——MongoDB副本集、管理副本集

Linux数据库管理——day14——MongoDB数据库

Linux数据库管理——day13——Redis的主从同步、数据格式

Linux数据库管理——day12——Redis数据库集群、Ruby软件简析

Linux数据库管理——day11——NoSQL的Redis数据库、内存策略简析

博主专栏

Linux基础学习

阅读量：139724 篇

Linux——Shell脚本

阅读量：2657 篇

https://blog.csdn.net/Yu1543376365/article/details/83758074

第 9 页 (共 11 页)

个人分类

Linux

66篇

网络

6篇

shell

13篇

基本服务

8篇

集群存储

5篇

展开

归档

2018年11月

3篇

2018年10月

23篇

2018年9月

19篇

2018年8月

27篇

2018年3月

1篇

展开

热门文章

浅谈char字符类型和string字符串类型

阅读量： 5847

用ansible自动化搭建web、sql服务器、lvs调度器

阅读量： 1316

初学者浅谈C++入门

阅读量： 1178

浅谈变量和函数——函数基本问题解析

阅读量： 703

Linux数据库管理——day10——分库分表、数据库硬件优化

阅读量： 615

最新评论

Linux数据库管理——day10...

m0_37508531：分库分表、数据库硬件优化



指甲分层



联系我们




扫码联系客服



下载CSDN APP

 QQ客服

 客服论坛

 kefu@csdn.net

 400-660-0108

工作时间 8:00-22:00

关于我们

招聘

广告服务

网站地图

 百度提供站内搜索

京ICP证09002463号

©2018 CSDN版权所有

网络110报警服务

经营性网站备案信息

北京互联网违法和不良信息举报中心

中国互联网举报中心