ssh

Secure SHell 用来取代telnet V1 V2版本

默认TCP/22

rpm -qa \*ssh\*

有四个配置文件

rpm -ql 详细介绍

家目录：~/.ssh

认证方式：

基于口令认证

password:

基于密钥认证

~/.ssh/authorized\_keys 公钥信息

ssh-keygen -t 生成密钥 -t指定加密算法

ssh -X -Y

登陆远程主机

默认配置文件 and SSH Port

/etc/ssh/sshd\_config - OpenSSH server configuration file.

/etc/ssh/ssh\_config - OpenSSH client configuration file.

~/.ssh/ - Users ssh configuration directory.

~/.ssh/authorized\_keys or ~/.ssh/authorized\_keys2 - Lists the public keys (RSA or DSA) that can be used to log into the user’s account（生成密钥使用）

**/etc/nologin** -（与PAM有关） If this file exists, sshd refuses to let anyone except root log in.拒绝除root外登陆 touch一个即可拒绝其他使用ssh

**/etc/hosts.allow and /etc/hosts.deny** : Access controls lists that should be enforced by tcp-wrappers are defined here. 定义允许和不允许的主机

/etc/ssh下的xx\_key文件都是基于主机的认证文件

/etc/sshd\_config中

StrictModes yes 用户家目录不为700即不允许登陆

RhostRSAAuthentication no 远程主机登陆 禁止

IgnoreRhost yes 忽略远程主机

ssh第一次主机连接的密钥

PrintMotd /etc/下 登陆会有提示

7个默认ssh安全 设置：

7 Default OpenSSH Security Options You Should Change in /etc/ssh/sshd\_config

1. Disable Root Login (PermitRootLogin)

2. Allow Only Specific Users or Groups (AllowUsers AllowGroups)

3. Deny Specific Users or Groups (DenyUsers DenyGroups)

4. Change SSHD Port Number (Port) 改端口

5. Change Login Grace Time (LoginGraceTime)

6. Restrict the Interface (IP Address) to Login (ListenAddress)

7. Disconnect SSH when no activity (ClientAliveInterval)

ClientAliveCountMax – This indicates the total number of checkalive message sent by the ssh server without getting any response from the ssh client. Default is 3.

ClientAliveInterval – This indicates the timeout in seconds. After x number of seconds, ssh server will send a message to the client asking for response. Deafult is 0 (server will not send message to client to check.).

20个SSH的安全性实践：

#1: Disable OpenSSH Server 不使用不打开

#2: Only Use SSH Protocol 2 使用第二版协议

#3: Limit Users' SSH Access 限制使用用户、

AllowUsers root redhat 白名单

AllowGroups

DenyUsers named apache mysql 黑名单

DenyGroups

#4: Configure Idle Log Out Timeout Interval 配置空闲登出的时间间隔

ClientAliveInterval 300s

ClientAliveCountMax 0

#5: Disable .rhosts Files 禁用Rhost文件 在配置文件中

#6: Disable Host-Based Authentication

#7: Disable root Login via SSH

#8: Enable a Warning Banner

Banner /etc/issue

#9: Firewall SSH Port # 22

(1)limit，限制， --limit 3/minute --limit-burst 3

(2)IN: NEW, ESTABLISHED; OUT: ESTABLISHED

#10: Change SSH Port and Limit IP Binding

#11: Use Strong SSH Passwords and Passphrase

genpasswd() {

local l=$1

[ "$l" == "" ] && l=20

tr -dc A-Za-z0-9\_ < /dev/urandom | head -c ${l} | xargs

}

#12: Use Public Key Based Authentication

#13: Use Keychain Based Authentication

#14: Chroot SSHD (Lock Down Users To Their Home Directories)

#15: Use TCP Wrappers

#16: Disable Empty Passwords

PermitEmptyPasswords no

#17: Thwart SSH Crackers (Brute Force Attack)

DenyHosts is a Python based security tool for SSH servers. It is intended to prevent brute force attacks on SSH servers by monitoring invalid login attempts in the authentication log and blocking the originating IP addresses.

Fail2ban is a similar program that prevents brute force attacks against SSH.

security/sshguard-pf protect hosts from brute force attacks against ssh and other services using pf.

security/sshguard-ipfw protect hosts from brute force attacks against ssh and other services using ipfw.

security/sshguard-ipfilter protect hosts from brute force attacks against ssh and other services using ipfilter.

security/sshblock block abusive SSH login attempts.

security/sshit checks for SSH/FTP bruteforce and blocks given IPs.

BlockHosts Automatic blocking of abusive IP hosts.

Blacklist Get rid of those bruteforce attempts.

Brute Force Detection A modular shell script for parsing application logs and checking for authentication failures. It does this using a rules system where application specific options are stored including regular expressions for each unique auth format.

IPQ BDB filter May be considered as a fail2ban lite.

#18: Rate-limit Incoming Port # 22 Connections 连接速率限制

iptables -I INPUT -p tcp --dport ${ssh\_port} -i ${inet\_if} -m state --state NEW -m recent --set

iptables -I INPUT -p tcp --dport ${ssh\_port} -i ${inet\_if} -m state --state NEW -m recent --update --seconds 60 --hitcount 5 -j DROP