CIELO servers - Task #729

Milestone # 728 (New): Server security

Modify sshd_config in /etc/ssh in Montecillo

07/14/2016 04:41 PM - Jose Gomero

Status:	New	**Start date:**	07/14/2016
Priority:	Inmediate	**Due date:**	07/14/2016
Assignee:	Jose Gomero	**% Done:**	100%
Category:		**Estimated time:**	1.00 hour
Target version:	V 1.0	**Spent time:**	1.00 hour

Description

Package generated configuration file

See the sshd_config(5) manpage for details

What ports, IPs and protocols we listen for

Port 22

Use these options to restrict which interfaces/protocols sshd will bind to

#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2

HostKeys for protocol version 2

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

Lifetime and size of ephemeral version 1 server key

KeyRegenerationInterval 3600
ServerKeyBits 768

Logging

SyslogFacility AUTH
LogLevel INFO

Authentication:

LoginGraceTime 120
PermitRootLogin yes
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile	%h/.ssh/authorized_keys

Don't read the user's ~/.rhosts and ~/.shosts files

IgnoreRhosts yes

For this to work you will also need host keys in /etc/ssh_known_hosts

RhostsRSAAuthentication no

similar for protocol version 2

HostbasedAuthentication no

Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication

#IgnoreUserKnownHosts yes

To enable empty passwords, change to yes (NOT RECOMMENDED)

PermitEmptyPasswords no

Change to yes to enable challenge-response passwords (beware issues with

some PAM modules and threads)

ChallengeResponseAuthentication no

Change to no to disable tunnelled clear text passwords

#PasswordAuthentication yes

Kerberos options

#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

GSSAPI options

#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

Allow client to pass locale environment variables

AcceptEnv LANG LC_*

#Subsystem sftp /usr/lib/openssh/sftp-server
Subsystem sftp internal-sftp

Set this to 'yes' to enable PAM authentication, account processing, and session processing. If this is enabled, PAM authentication will be allowed through the ChallengeResponseAuthentication and PasswordAuthentication. Depending on your PAM configuration, PAM authentication via ChallengeResponseAuthentication may bypass the setting of "PermitRootLogin without-password".
If you just want the PAM account and session checks to run without PAM authentication, then enable this but set PasswordAuthentication and ChallengeResponseAuthentication to 'no'.

UsePAM yes

UseDNS no

Match user cesar
ChrootDirectory %h
ForceCommand internal-sftp
AllowTCPForwarding no

Match user tuser
ChrootDirectory /chroot
AllowTCPForwarding no
X11Forwarding no

History

#1 - 07/14/2016 04:44 PM - Jose Gomero

Antes figuraba en la parte del usuario cesar, lo siguiente:

Match user cesar
ChrootDirectory /chroot
AllowTCPForwarding no
X11Forwarding no

En el Codigo anterior a este debio decir lo siguiente:

Match user cesar
ChrootDirectory %h
ForceCommand internal-sftp
AllowTCPForwarding no
X11Forwarding no

#2 - 07/14/2016 05:27 PM - Jose Gomero

Correcion Final :

UsePAM yes

UseDNS no

Match user cesar
ChrootDirectory /chroot
ForceCommand internal-sftp
AllowTCPForwarding no
X11Forwarding no

Match user tuser
ChrootDirectory /chroot
AllowTCPForwarding no
X11Forwarding no