Gráfico de embudo

Descripción generada automáticamente con confianza media

Imagen que contiene Tabla

Descripción generada automáticamente

Buenas tardes, para poder avanzar necesitaría , los siguientes archivos para tener de referencia

\*sshd\_config

\*/etc/sudoers

\*/etc/cron.d/cron.allow

\*/etc/cron.d/cron.deny

\*/etc/passwd

Definiciones

IPTABLES

\*Puertos necesarios para la operatoria. (se denegara no que no este en esta lista)

\*Definición de usuarios de SUDOERS / usuario con permiso de CRON / Criterio para baja de SHELL  NO USADOS

\*Archivos a pasar por SIEM

EJEMPLO

"audit.log"  
"auth.log"  
"cron"  
"dpkg.log"  
"faillog"  
"mail.err"  
"maillog"  
"mail.log"  
"messages"  
"samba"  
"secure"  
"sudo"  
"syslog"  
"wtmp"  
"utmp"  
"yum.log"

Desde ya muchas gracias

Quedo a su disposición.

Sebastian

Día 20/12/2021- mayoría de las acciones de remediación.

echo 'export HISTTIMEFORMAT="%F %T "' >> ~/.bashrc

source ~/.bashrc

echo 'export HISTTIMEFORMAT="%F %T "' >> /etc/profile

source /etc/profile

syslog

find / -name "audit.log"

find / -name "auth.log"

find / -name "cron"

find / -name "dpkg.log"

find / -name "faillog"

find / -name "mail.err"

find / -name "maillog"

find / -name "mail.log"

find / -name "messages"

find / -name "samba"

find / -name "secure"

find / -name "sudo"

find / -name "syslog"

find / -name "wtmp"

find / -name "utmp"

find / -name "yum.log"

cron

allow - usuarios a definir

/etc/cron.d/cron.allow

/etc/cron.d/cron.deny

configuracion iptables definicion cliente

/etc/sysconfig/iptables

iptables yml

cat /etc/passwd | awk -F: '($3 == 0) { print $1 }'

grep ‘<groupname>’ /etc/group

grep '^root' /etc/passwd

yum install rsyslog -y

configuracion

mask

echo 'umask 0027' >> ~/.bash\_profile

kernel.randomize\_va\_space = 2

echo 2 > /proc/sys/kernel/randomize\_va\_space

sysctl -w kernel.randomize\_va\_space=2

ver que se hace con twripe