Fortalecimiento Seguridad

BanCoppel

Acciones de remediación

Ruben Sebastian Velis

29/12/2021

Contenido

Objetivo……………………………………………………………………………………………………………………………………………………[2](https://docs.google.com/document/d/1moVLTJTAWvTa0SCyAYqIA_ZSE9KNE3yZ-of3VLjC5WM/edit#heading=h.1fob9te)

## Archivos necesarios para la ejecución …………………………………………………………………………………………………[3](https://docs.google.com/document/d/1moVLTJTAWvTa0SCyAYqIA_ZSE9KNE3yZ-of3VLjC5WM/edit#heading=h.3znysh7)

Archivos de Configuración …………………………………………………………………………………………………………………**4**

Configuración de Hosts e Inventario……………………………………………………………………………………5.

Ejecución……………………………………………………………………………………6

# Instrucciones para correr PLAYBOOKS de remediación

## Objetivo de remediación

• Intentos de autenticación exitosos y fallidos, con prioridad en los servicios de red.  
•/var/log/faillog Log deprecado.  
• /var/log/auth.log Para servidores Debian y derivados.  
• /var/log/secure Para servidores Redhat y derivados.  
• Uso de cualquier invocación de cuenta “root” o privilegiada, como el comando “su” (ej. Registro de “sudoers”).  
• /var/log/auth.log Para servidores Debian y derivados.  
• /var/log/secure Para servidores Redhat y derivados.  
• Conexiones entrantes denegadas (ej. aquellas bloqueadas por iptables).  
• /var/log/kern.log Para servidores Debian y derivados.  
• /var/log/messages Para servidores Redhat y derivados.  
• Historial de comandos (ej. bitácoras del historial de bash shell), incluidos los registros de fechas.  
•Install auditd, psacct, o acct.  
•Instalar y configurar psacct, o acct dependiendo el sistema operativo RHEL CentOS Debian, Ubuntu y derivados.  
• Iniciar servicios.  
•Configurar auditd, editar el archivo /etc/audit/auditd.conf.  
• Gestión de Reglas audit.rules.  
• Configurar en rsyslog.  
•/var/log/audit/audit.log.  
•/var/log/auth.log.  
•/var/log/cron.  
•/var/log/dpkg.log.  
•/var/log/messages.  
•/var/log/secure.  
•/var/log/sudo.  
•/var/log/syslog.  
•/var/log/wtmp.  
•/var/log/yum.log.  
•/var/log/httpd/access\_log.  
•/var/log/apache2/access.log.

## Archivos necesarios para la ejecución

* RedHat
* CentOs
* Ubuntu
* Debian

|  |  |  |
| --- | --- | --- |
| FILES | | |
| /Debian.yaml | /Debian/logrotatedebian.yml | /CentOS/rsyslog.conf |
| /RedHat.yaml | /Debian/rsyslogdebian.conf | /CentOS/rsyslogother.conf |
| /main.yaml | /Debian/copy.yml | /CentOS/rsyslogrhel.conf |
| /hosts | /inventario.tux | /CentOS/rules.yml |
| /README.md | /Ubuntu | /CentOS/uuid.yml |
| /Debian | /Ubuntu/50-default.conf | /RedHat |
| /Debian/50-default.conf | /Ubuntu/audit.yml | /RedHat/50-default.conf |
| /Debian/listen.conf | /Ubuntu/fecha.yml | /RedHat/listen.conf |
| /Debian/rsyslog.conf | /Ubuntu/rules.yml | /RedHat/logrotateother.yml |
| /Debian/kernel.yml | /Ubuntu/uuid.yml | /RedHat/rsyslog.conf |
| /Debian/fecha.yml | /Ubuntu/copy.yml | /RedHat/rsyslogother.conf |
| /Debian/uuid.yml | /Ubuntu/rsyslogdebian.conf | /RedHat/rsyslogrhel.conf |
| /Debian/pkgother.yml | /CentOS | /RedHat/logrotaterhel.yml |
| /Debian/pkgaudit.yml | /CentOS/50-default.conf | /RedHat/kernel.yml |
| /Debian/rules.yml | /CentOS/audit.yml | /RedHat/uuid.yml |
| /Debian/audit.yml | /CentOS/cfgedit.yml | /RedHat/audit.yml |
| /Ubuntu/kernel.yml | /CentOS/copy.yml | /RedHat/fecha.yml |
| /Ubuntu/listen.conf | /CentOS/fecha.yml | /RedHat/rhelyum.yml |
| /Ubuntu/logrotateother.yml | /CentOS/kernel.yml | /RedHat/rules.yml |
| /Ubuntu/pkgaudit.yml | /CentOS/listen.conf | /RedHat/logrotate.yml |
| /Ubuntu/pkgother.yml | /CentOS/logrotateother.yml | /RedHat/cfgedit.yml |
| /Ubuntu/rsyslog.conf | /CentOS/logrotaterhel.yml | /RedHat/copy.yml |
| /Ubuntu/rsyslogother.conf | /CentOS/logrotate.yml | /Ubuntu.yaml |
| /Ubuntu/rsyslogrhel.conf | /CentOS/rhelyum.yml | /CentOS.yaml |

## Archivos de Configuración

|  |
| --- |
| FILES |
| /Debian/50-default.conf |
| /Debian/listen.conf |
| /Debian/rsyslog.conf |
| /Debian/rsyslogdebian.conf |
| /Ubuntu/50-default.conf |
| /Ubuntu/listen.conf |
| /Ubuntu/rsyslog.conf |
| /Ubuntu/rsyslogother.conf |
| /Ubuntu/rsyslogrhel.conf |
| /CentOS/50-default.conf |
| /CentOS/listen.conf |
| /CentOS/rsyslog.conf |
| /CentOS/rsyslogother.conf |
| /CentOS/rsyslogrhel.conf |
| /RedHat/50-default.conf |
| /RedHat/listen.conf |
| /RedHat/rsyslog.conf |
| /RedHat/rsyslogother.conf |
| /RedHat/rsyslogrhel.conf |

## Configuración Archivo HOSTS / SSH-KEY

Se debe declarar en el archivo hosts las ip y los nombres de los server  
ejemplo:

[root@ss os\_detector]# cat /etc/hosts  
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4  
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

10.92.192.10 ubuntu.lab  
10.92.192.250 rhel.lab

[root@ss os\_detector]#

Se debe realizar la aceptación del cert. Ssh desde la vm que corre ansible hacia la vm a impactar.

## Configuración Archivo Inventario.tux

Se debe declarar usuario que va a ejecutar las tareas  
ejemplo  
[all:vars]  
ansible\_become=yes  
ansible\_become\_user=root  
ansible\_become\_password=07cf04cv  
ansible\_become\_method=su  
ansible\_python\_interpreter=auto\_silent

**Luego declarar por SO los servers  
ejemplo**

[DebianHosts]  
ubuntu.lab

[UbuntuHosts]  
ubuntu.lab

[CentOSHost]  
rhel.lab

[RedHatHost]  
rhel.lab

## EJECUCION

Este Playbook diferenciara el SO y ejecutara la tarea para cada una de las distribuciones.

ansible-playbook -i inventario.tux main.yaml -v

#VERSION 0.1

