Auditando LINUX

Auditoria Informatica

Camila Lóndero

- Ubuntu Linux 20.04.1 LTS
- CIS Ubuntu LInux 20.04.1 LTS Benchmark

RECOMENDACIONES

01 Configuración Inicial

02 Servicios

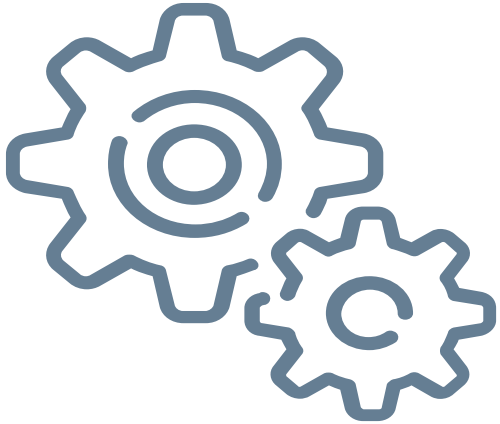
03 Configuración de red

04 Registro y auditoría

05 Acceso, autenticación y autorización

06 Mantenimiento del Sistema

01 CONFIGURACIÓN INICIAL



1.1.23 Deshabilitar el montaje automático.
1.9 Asegúrese de que las actualizaciones, los parches y el software de seguridad adicional estén instalados

1.1.23 Deshabilitar el montaje automático

Audit

```
camila@camila:~$ dpkg -s autofs
dpkg-query: el paquete `autofs' no está instalado y no hay ninguna información disponible.
Use dpkg --info (= dpkg-deb --info) to examine archive files.
```

```
camila@camila:~$ systemctl is-enabled autofs
Failed to get unit file state for autofs.service: No such file or directory
```

Remediation

```
camila@camila:~$ systemctl --now disable autofs
```

```
camila@camila:~$ apt purge autofs
```

1.9 Asegúrese de que las actualizaciones, los parches y el software de seguridad adicional estén instalados

Audit

```
camila@camila:~$ sudo apt -s upgrade
[sudo] contraseña para camila:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-headers-5.8.0-50-generic linux-hwe-5.8-headers-5.8.0-50
  linux-image-5.8.0-50-generic linux-modules-5.8.0-50-generic
  linux-modules-extra-5.8.0-50-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  distro-info docker-ce-rootless-extras docker-scan-plugin libllvm11
  slirp4netns
Se actualizarán los siguientes paquetes:
  alsa-ucm-conf alsa-utils apt apt-transport-https apt-utils base-files bluez
  bluez-cups bluez-obexd bolt bsdutils busybox-initramfs busybox-static cheese
  cheese-common command-not-found containerd.io dirmngr docker-ce
  docker-ce-cli enchant-2 evince evince-common evolution-data-server
  evolution-data-server-common fdisk fonts-noto-color-emoji fonts-noto-mono
  fonts-opensymbol friendly-recovery gdb gdbserver gdm3 gir1.2-gdm-1.0
  gir1.2-gnomebluetooth-1.0 gir1.2-gnomedesktop-3.0 gir1.2-goa-1.0
  gir1.2-gweather-3.0 gir1.2-mutter-6 gir1.2-nm-1.0 gir1.2-nma-1.0
```

1.9 Asegúrese de que las actualizaciones, los parches y el software de seguridad adicional

Remediation

```
camila@camila:~$ sudo apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-headers-5.8.0-50-generic linux-hwe-5.8-headers-5.8.0-50
  linux-image-5.8.0-50-generic linux-modules-5.8.0-50-generic
  linux-modules-extra-5.8.0-50-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  distro-info docker-ce-rootless-extras docker-scan-plugin libllvm11
  slirp4netns
Se actualizarán los siguientes paquetes:
  alsa-ucm-conf alsa-utils apt apt-transport-https apt-utils base-files bluez
  bluez-cups bluez-obexd bolt bsdutils busybox-initramfs busybox-static cheese
  cheese-common command-not-found containerd.io dirmngr docker-ce
  docker-ce-cli enchant-2 evince evince-common evolution-data-server
  evolution-data-server-common fdisk fonts-noto-color-emoji fonts-noto-mono
  fonts-opensymbol friendly-recovery gdb gdbserver gdm3 gir1.2-gdm-1.0
```

02
SERVICIOS

2.1.8 Asegúrese de que el servidor DNS no esté instalado
2.1.10 Asegúrese de que el servidor HTTP no esté instalado

2.1.8 Asegúrese de que el servidor DNS no esté instalado

Audit

```
camila@camila:~$  dpkg -s bind9 | grep -E '(Status:|not installed)'
dpkg-query: el paquete `bind9' no está instalado y no hay ninguna información disponible.
```

Remediation

```
camila@camila:~$  apt purge bind9
```

2.1.10 Asegúrese de que el servidor HTTP no esté instalado

Audit

```
camila@camila:~$ dpkg -s apache2 | grep -E '(Status:|not installed)'
dpkg-query: el paquete `apache2' no está instalado y no hay ninguna información disponible.
```

Remediation

```
camila@camila:~$  apt purge apache2
```

04
Registro y auditoría

4.1.1.1 Asegúrese de que auditd esté instalado
4.1.1.2 Asegúrese de que el servicio auditado esté habilitado

4.1.1.1 Asegúrese de que auditd esté instalado

Audit

```
camila@camila:~$ dpkg -s auditd audispd-plugins
dpkg-query: el paquete `auditd' no está instalado y no hay ninguna información disponible.
```

Remediation

```
camila@camila:~$ sudo apt install auditd audispd-plugins
```

4.1.1.2 Asegúrese de que el servicio auditado esté habilitado

Audit

```
camila@camila:~$ systemctl is-enabled auditd
enabled
```

Remediation

```
camila@camila:~$  systemctl --now enable auditd
```

05
Acceso, autenticación y autorización

5.1.9 Asegúrese de que esté restringido a usuarios autorizados
5.2.1 Asegúrese de que sudo esté instalado

5.1.9 Asegúrese de que esté restringido a usuarios autorizados

Audit

```
camila@camila:~$ stat /etc/at.deny
stat: no se puede efectuar `stat' sobre '/etc/at.deny': No existe el archivo o el directorio
camila@camila:~$ stat /etc/at.allow
stat: no se puede efectuar `stat' sobre '/etc/at.allow': No existe el archivo o el directorio
```

Remediation

```
camila@camila:~$ rm /etc/at.deny
```

```
camila@camila:~$ sudo touch /etc/at.allow
```

```
camila@camila:~$ sudo chmod g-wx,o-rwx /etc/at.allow
camila@camila:~$ sudo chown root:root /etc/at.allow
camila@camila:~$ stat /etc/at.allow
  Fichero: /etc/at.allow
  Tamaño: 0             Bloques: 0          Bloque E/S: 4096   fichero regular vacío
Dispositivo: 806h/2054d Nodo-i: 265006      Enlaces: 1
Acceso: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (    0/    root)
Acceso: 2021-06-08 23:09:59.669477197 -0300
Modificación: 2021-06-08 23:09:59.669477197 -0300
      Cambio: 2021-06-08 23:10:27.045540078 -0300
    Creación: -
```

5.2.1 Asegúrese de que sudo esté instalado

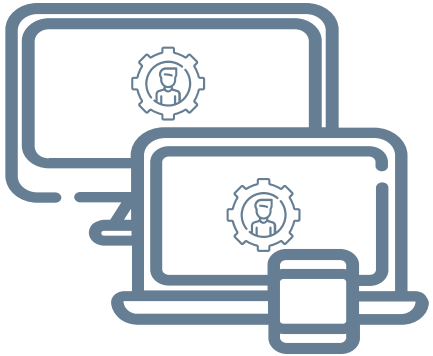
Audit

```
camila@camila:~$ dpkg -s sudo
Package: sudo
Status: install ok installed
Priority: important
Section: admin
Installed-Size: 2204
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Version: 1.8.31-1ubuntu1.2
```

Remediation

```
camila@camila:~$ apt install sudo
```

06 Mantenimiento del Sistema



6.1.2 Asegúrese de que los permisos en / etc / passwd estén configurados
6.1.6 Asegúrese de que los permisos en / etc / shadow estén configurados

6.1.2 Asegúrese de que los permisos en / etc / passwd estén configurados

Audit

```
camila@camila:~$  stat /etc/passwd
  Fichero: /etc/passwd
  Tamaño: 3156          Bloques: 8          Bloque E/S: 4096   fichero regular
Dispositivo: 806h/2054d Nodo-i: 264977      Enlaces: 1
Acceso: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Acceso: 2021-06-08 19:35:01.841615994 -0300
Modificación: 2020-11-05 15:33:35.023353069 -0300
      Cambio: 2020-11-05 15:33:35.059353678 -0300
    Creación: -
```

Remediation

```
camila@camila:~$ sudo chown root:root /etc/passwd
camila@camila:~$ sudo chmod u-x,go-wx /etc/passwd
```

6.1.6 Asegúrese de que los permisos en / etc / shadow estén configurados

Audit

```
camila@camila:~$ stat /etc/shadow
  Fichero: /etc/shadow
  Tamaño: 1643          Bloques: 8          Bloque E/S: 4096   fichero regular
Dispositivo: 806h/2054d Nodo-i: 264930      Enlaces: 1
Acceso: (0640/-rw-r-----)  Uid: (    0/    root)   Gid: (   42/  shadow)
Acceso: 2021-06-08 19:35:32.613310086 -0300
Modificación: 2020-11-05 15:33:35.115354624 -0300
      Cambio: 2020-11-05 15:33:35.147355165 -0300
    Creación: -
```

Remediation

```
camila@camila:~$ sudo chown root:root /etc/shadow
camila@camila:~$ sudo chown root:shadow /etc/shadow
camila@camila:~$ sudo chmod u-x,g-wx,o-rwx /etc/shadow
```

¡GRACIAS!

¿PREGUNTAS?