UNIVERSIDAD DE LA INTEGRACIÓN DE LAS AMÉRICAS

Facultad de Ingeniería

Carreras de Ingeniería en Informática e Ingeniería en Sistemas

SISTEMAS OPERATIVOS

Informe de Laboratorio 4

Seguridad Del Sistema

Nombre: Gonzalo Aquino Alvarenga
Materia: Sistemas Operativos
Fecha: 21/06/25

Introducción

Este laboratorio tuvo como objetivo explorar mecanismos básicos de seguridad en sistemas operativos tipo Unix, como la auditoría de eventos del sistema, el análisis de vulnerabilidades, y la simulación de un respaldo y restauración. A través de pruebas prácticas, se identificaron eventos relevantes en los logs, se revisaron servicios activos y se ejecutaron tareas de respaldo para comprobar la integridad y recuperación del sistema.

Auditoría de Seguridad

Se configuró el sistema para observar eventos relacionados a seguridad, utilizando registros del sistema ubicados en /var/log/auth.log y herramientas como journalctl. Para generar actividad, se simuló un intento de inicio de sesión fallido con un usuario real, ingresando una contraseña incorrecta. Luego, se creó un directorio con permisos restringidos, y se intentó acceder sin los privilegios necesarios.

Estas acciones generaron eventos visibles tanto en la terminal como en los registros del sistema. Posteriormente, se utilizaron filtros para localizar dichas entradas.

```
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo mkdir /seguridad
[sudo] contraseña para sole-cardozo:
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo chmod 000 /seguridad
sole-cardozo@sole-cardozo-VirtualBox:~$ cd /seguridad
bash: cd: /seguridad: Permiso denegado
```

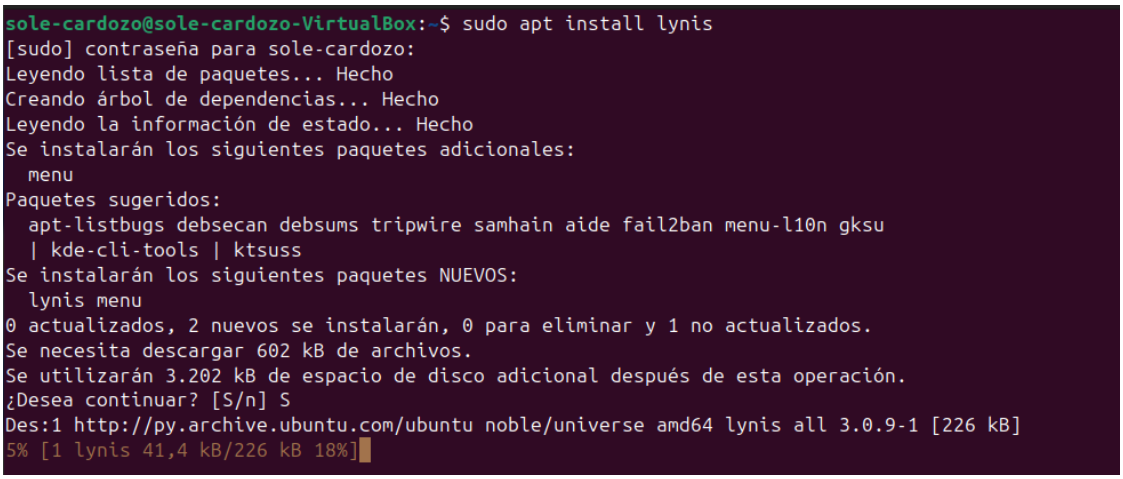
```
sole-cardozo@sole-cardozo-VirtualBox:~$ su sole-cardozo
Contraseña:
su: Fallo de autenticación
```

Análisis de Vulnerabilidades

Se utilizó la herramienta **Lynis** para realizar una auditoría básica del sistema. El análisis arrojó advertencias relacionadas a paquetes vulnerables, servicios innecesarios activos y configuraciones que podían mejorarse, como la instalación de fail2ban, configuración de firewall y protección de GRUB.

Además, se listaron los servicios en ejecución usando systemctl. Entre ellos se encontraron procesos como cups.service o avahi-daemon, que no eran necesarios en este entorno. Finalmente, se revisaron las actualizaciones pendientes del sistema.

Lynis:



```
-[ Lynis 3.0.9 Results ]-

Warnings (2):
----------------------------
! Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/lynis/controls/PKGS-7392/

! iptables module(s) loaded, but no rules active [FIRE-4512]
    https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (43):
----------------------------
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
    https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
    https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
    https://cisofy.com/lynis/controls/DEB-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
    https://cisofy.com/lynis/controls/DEB-0811/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restart
ing. [DEB-0831]
    https://cisofy.com/lynis/controls/DEB-0831/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
    https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
    https://cisofy.com/lynis/controls/BOOT-5122/
```

```
Lynis security scan details:

Hardening index : 58 [###########          ]
Tests performed : 254
Plugins enabled : 1

Components:
- Firewall               [V]
- Malware scanner        [X]

Scan mode:
Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

Lynis modules:
- Compliance status      [?]
- Security audit         [V]
- Vulnerability scan     [V]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                     : /var/log/lynis-report.dat
```

Servicios Activos:

```
sole-cardozo@sole-cardozo-VirtualBox:~$ systemctl list-units --type=service --state=running
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service             loaded active running Accounts Service
  apache2.service                     loaded active running The Apache HTTP Server
  avahi-daemon.service                loaded active running Avahi mDNS/DNS-SD Stack
  colord.service                      loaded active running Manage, Install and Generate Color Profiles
  cron.service                        loaded active running Regular background program processing daemon
  cups-browsed.service                loaded active running Make remote CUPS printers available locally
  cups.service                        loaded active running CUPS Scheduler
  dbus.service                        loaded active running D-Bus System Message Bus
  gdm.service                         loaded active running GNOME Display Manager
  gnome-remote-desktop.service        loaded active running GNOME Remote Desktop
  kerneloops.service                  loaded active running Tool to automatically collect and submit kernel crash signatures
  ModemManager.service                loaded active running Modem Manager
  NetworkManager.service              loaded active running Network Manager
  polkit.service                      loaded active running Authorization Manager
  power-profiles-daemon.service       loaded active running Power Profiles daemon
  rsyslog.service                     loaded active running System Logging Service
  rtkit-daemon.service                loaded active running RealtimeKit Scheduling Policy Service
  snapd.service                       loaded active running Snap Daemon
  switcheroo-control.service          loaded active running Switcheroo Control Proxy service
  systemd-journald.service            loaded active running Journal Service
  systemd-logind.service              loaded active running User Login Management
  systemd-oomd.service                loaded active running Userspace Out-Of-Memory (OOM) Killer
  systemd-resolved.service            loaded active running Network Name Resolution
  systemd-udevd.service               loaded active running Rule-based Manager for Device Events and Files
  udisks2.service                     loaded active running Disk Manager
  unattended-upgrades.service         loaded active running Unattended Upgrades Shutdown
  upower.service                      loaded active running Daemon for power management
  user@1000.service                   loaded active running User Manager for UID 1000
  virtualbox-guest-utils.service loaded active running Virtualbox guest utils
  wpa_supplicant.service              loaded active running WPA supplicant

Legend: LOAD   → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB    → The low-level unit activation state, values depend on unit type.

30 loaded units listed.
```

Lista de actualizaciones pendientes con “apt”:

```
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo apt list --upgradable
[sudo] contraseña para sole-cardozo:
Listando... Hecho
linux-firmware/noble-updates,noble-security 20240318.git3b128b60-0ubuntu2.13 amd64 [actualizable desde: 20240318.git3b128b60-0ubuntu2.12]
N: Hay 2 versiones adicionales. Utilice la opción «-a» para verlas
```

Respaldo y Recuperación

Para esta sección se realizó un respaldo comprimido de la carpeta /etc utilizando “tar”, ya que contiene configuraciones críticas del sistema. A modo de prueba, se eliminó el archivo /etc/issue, que muestra información al iniciar sesión en consola. Luego, se extrajo ese archivo desde el respaldo y se restauró a su ubicación original.

El proceso sirvió para comprobar que es posible recuperar archivos del sistema mediante herramientas básicas, y que la restauración se puede realizar de manera rápida si el respaldo fue bien hecho.

```
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo tar -czvf respaldo_etc.tar.gz /etc
tar: Eliminando la `/' inicial de los nombres
/etc/
/etc/protocols
/etc/dbus-1/
/etc/dbus-1/session.d/
/etc/dbus-1/system.d/
/etc/dbus-1/system.d/com.hp.hplip.conf
/etc/dbus-1/system.d/com.ubuntu.WhoopsiePreferences.conf
/etc/dbus-1/system.d/com.ubuntu.SoftwareProperties.conf
/etc/dbus-1/system.d/com.ubuntu.LanguageSelector.conf
/etc/dbus-1/system.d/com.ubuntu.USBCreator.conf
/etc/dbus-1/system.d/org.opensuse.CupsPkHelper.Mechanism.conf
/etc/dbus-1/system.d/com.redhat.PrinterDriversInstaller.conf
/etc/dbus-1/system.d/com.redhat.NewPrinterNotification.conf
/etc/dbus-1/system.d/org.debian.apt.conf
/etc/dbus-1/system.d/kerneloops.conf
/etc/login.defs
/etc/pm/
/etc/pm/sleep.d/
/etc/pm/sleep.d/10_grub-common
/etc/pm/sleep.d/10_unattended-upgrades-hibernate
/etc/ghostscript/
/etc/ghostscript/cidfmap.d/
/etc/ghostscript/cidfmap.d/90gs-cjk-resource-japan1.conf
/etc/ghostscript/cidfmap.d/90gs-cjk-resource-gb1.conf
/etc/ghostscript/cidfmap.d/90gs-cjk-resource-korea1.conf
/etc/ghostscript/cidfmap.d/90gs-cjk-resource-cns1.conf
/etc/ghostscript/cidfmap.d/90gs-cjk-resource-japan2.conf
/etc/ghostscript/fontmap.d/
/etc/ghostscript/fontmap.d/10fonts-urw-base35.conf
/etc/shells
/etc/subgid-
/etc/menu/
/etc/menu/README
/etc/gprofng.rc
/etc/dhcp/
```

```
/etc/kerneloops.conf
/etc/rc5.d/
/etc/rc5.d/S01saned
/etc/rc5.d/S01sssd
/etc/rc5.d/S01grub-common
/etc/rc5.d/S01whoopsie
/etc/rc5.d/S01open-vm-tools
/etc/rc5.d/S01apport
/etc/rc5.d/S01gdm3
/etc/rc5.d/S01sysstat
/etc/rc5.d/S01virtualbox-guest-utils
/etc/rc5.d/S01plymouth
/etc/rc5.d/S01console-setup.sh
/etc/rc5.d/S01bluetooth
/etc/rc5.d/K01apache-htcacheclean
/etc/rc5.d/S01cups
/etc/rc5.d/S01unattended-upgrades
/etc/rc5.d/S01dbus
/etc/rc5.d/S01uuidd
/etc/rc5.d/S01anacron
/etc/rc5.d/K01speech-dispatcher
/etc/rc5.d/S01cron
/etc/rc5.d/S01rsync
/etc/rc5.d/S01openvpn
/etc/rc5.d/S01spice-vdagent
/etc/rc5.d/S01kerneloops
/etc/rc5.d/S01apache2
```

Borrado del archivo, restauración del archivo desde el backup, comprobación final mostrando el contenido restaurado:

```
sole-cardozo@sole-cardozo-VirtualBox:~$ cat /etc/issue
Ubuntu 24.04.2 LTS \n \l

sole-cardozo@sole-cardozo-VirtualBox:~$ sudo rm /etc/issue
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo tar -xzvf respaldo_etc.tar.gz etc/issue
etc/issue
sole-cardozo@sole-cardozo-VirtualBox:~$ sudo cp etc/issue /etc/issue
sole-cardozo@sole-cardozo-VirtualBox:~$ cat /etc/issue
Ubuntu 24.04.2 LTS \n \l
```

Conclusión

Este laboratorio permitió aplicar conceptos esenciales de seguridad en sistemas Linux. Se evidenció cómo el sistema registra eventos críticos, cómo herramientas como lynis pueden servir como guía para mejorar la configuración del sistema, y cómo realizar un respaldo efectivo que permita restaurar archivos importantes. Estas prácticas son fundamentales para mantener la estabilidad y seguridad del sistema en entornos reales.