



Fuente: Microsoft Copilot

LABORATORIO 5. SEGURIDAD DEL SO LINUX

DEPARTAMENTO DE INFORMÁTICA. UNIVERSIDAD DE OVIEDO

Seguridad de Sistemas Informáticos | 2024 – 2025 (v4.2 "S-81 Isaac Peral")





Contenido

	La infraestructura de este laboratorio	2
	Acerca de Wazuh.....	2
	Bloque 1: Gestionando de un servidor	4
🛠	Ejercicio L5B1_WEBMIN: Instalar y ejecutar WebMin	4
🛠	Ejercicio L5B1_WMRESOURCER: Comprobar el consumo de recursos del servidor	4
🛠	Ejercicio L5B1_WMADDUSER: Agregar un usuario de prueba al servidor	5
🛠	Ejercicio L5B1_WMPACKAGEHANDLE: Gestión de paquetes	6
🛠	Ejercicio L5B1_WMBOOTSERVICE: Deshabilitar algunos servicios que se ejecutan en el momento del arranque	6
	Bloque 2: Seguridad relacionada con el usuario	8
🛠	Ejercicio L5B2_SECSSH: Seguridad adicional para OpenSSH	8
🛠	Ejercicio L5B2_PAM: Configuración segura del módulo PAM	8
🛠	Ejercicio L5B2_PWDAGE: Antigüedad de la contraseña y cuentas inactivas	9
	Bloque 3: Seguridad relacionada con los procesos	11
🛠	Ejercicio L5B3_APPARMOR: Gestión de AppArmor	11
🛠	Ejercicio L5B3_SECAPT: Instalar software de seguridad de apt	11
	Bloque 4: Logs y monitorización.....	13
🛠	Ejercicio L5B4_AUDIT: Configurar reglas de auditoría	13
🛠	Ejercicio L5B4_WMLLOG: Inspeccionar los logs en busca de comportamientos sospechosos	13
🛠	Ejercicio L5B4_WAZUH: HIDS implementado con un XDR profesional: Wazuh como herramienta de monitorización de archivos, procesos y usuarios	14
	Insignias y autoevaluación	20

BACK

1

2

3

4



La infraestructura de este laboratorio

Este laboratorio solo trabaja con la máquina virtual *Ubuntu* del curso. No obstante, hay una serie de consideraciones previas que debes leer con atención.

- **Recomendamos encarecidamente crear primero una instantánea o un clon vinculado de la máquina virtual en caso de que rompas algo 😊.**
- Algunas actividades requieren ir a la sección indicada de un archivo **PDF de CIS Benchmark** (*Ubuntu 24.04*) y seguir sus instrucciones detalladas. **Junto con este documento se da el CIS Benchmark que debes usar**, así que descárgalo también..

 **ADVERTENCIA GENERAL:** *Este laboratorio requiere copiar algunos comandos del archivo PDF. Por favor, COMPRUEBA CUIDADOSAMENTE lo que copias, ya que caracteres Unicode copiados como ☐, ☑, etc. pueden considerarse sintácticamente incorrectos en línea de comandos aunque visualmente parezcan los mismos. Debes reemplazarlos por sus equivalentes a ASCII (tecléalos, vamos 😊). Esto es especialmente problemático con las comillas.*

Si la sintaxis de un comando no funciona, revisa cuidadosamente la línea de comandos en busca de caracteres no válidos copiados accidentalmente. Esto es aplicable a partir de ahora, incluso en futuros laboratorios.

BACK

1

2

3

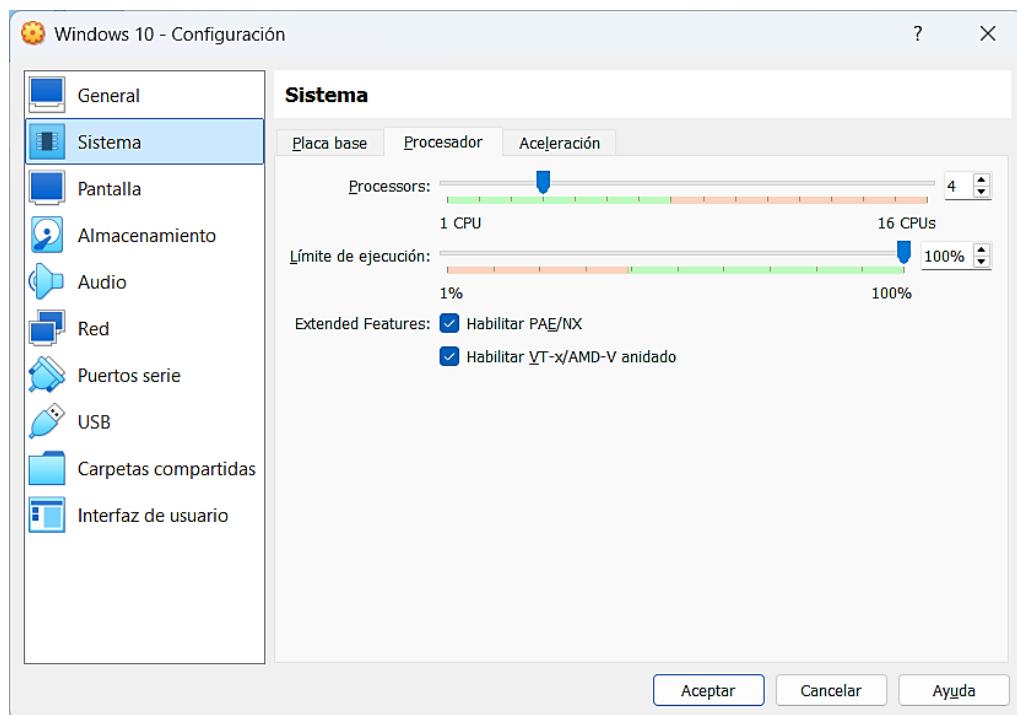
4

5

Acerca de Wazuh

Al final del laboratorio, tienes su actividad "estrella", la puesta en marcha de un XDR/SIEM llamado **Wazuh**. Esta es una herramienta gratuita muy poderosa **para uso profesional** con una gran cantidad de funciones. Es tan completo que **volveremos a él en futuros laboratorios**, y en este solo veremos una parte de sus funciones. Usarlo tiene un precio, sin embargo, y es que necesitas aumentar los recursos de la VM que te damos **a 6Gb de RAM y 4 núcleos para que funcione adecuadamente**. Para ello, te aconsejamos que hagas lo siguiente:

- Si no tienes una máquina en casa capaz de soportar la creación de una VM con estas características, te recomendamos que **priorices la actividad de Wazuh para hacerla en el laboratorio**, donde sí tienes *hardware* que soporte esa VM. **Incluso puedes empezar por él sin ningún problema.**
- Para esta actividad **se recomienda hacer un clon vinculado de la VM base** (mucho más ligero de crear y usar) y aumentar los recursos solo a ese clon. La creación de un clon vinculado se cubre en **el laboratorio 0A**.
- Si ves que tu SO va lento al aumentar la RAM, activa la opción PAE/NX con la máquina apagada y arráncala de nuevo.



BACK

1

2

3

4

5

Si también haces el ejercicio L5B4_AUDIT antes de clonar la máquina para crear la de Wazuh, este XDR probablemente será capaz de capturar más información de tu sistema, pero no es estrictamente necesario para este laboratorio

- De esta forma, te quedarás con dos MVs, pero solo tendrás que arrancar una a la vez: **La MV "normal"** (con sus snapshots o copias que quieras hacer y con las que trabajarás en los diferentes labs) y su clon vinculado, **la MV "Wazuh"** con Wazuh instalado, que no necesita ninguna otra para funcionar. **Tenga en cuenta que si eliminas la máquina virtual "normal" y has creado un clon vinculado, también perderás la máquina virtual "Wazuh".** Si crees que vas a eliminarla, es mejor crear un clon completo de la máquina virtual, aunque ocupe más recursos.
- **No borres la MV Wazuh cuando termines la actividad** porque lo vamos a usar en otros, por favor.
- En este laboratorio pondremos en marcha y solo veremos una parte de sus características. Volveremos a la misma interfaz más adelante para ver qué significan otras cosas. Pero **es importante que primero hagas esta actividad de Wazuh** para obtener una buena comprensión del resto.



Bloque 1: Gestionando de un servidor

🛠 Ejercicio L5B1_WEBMIN: Instalar y ejecutar WebMin

👷 Descripción de la actividad / Aplicación práctica

Puede instalar un GUI que **te ayude con la administración del servidor Linux**, llamado *WebMin*

⭐ Resultados esperados

Puede instalar *WebMin* y **entender cómo funciona** en general, por lo que puedes buscar en él distinta y hacer las acciones que te pidan. Puedes responder a estas preguntas:

- *¿Entiendes por qué es importante usar HTTPs con WebMin en un entorno de producción?*
- *¿Entiendes también por qué no podemos hacerlo en nuestro entorno de pruebas, por lo que nos vemos obligados a usar HTTP?*
- *¿Pondrías WebMin en un servidor de producción, o mejor en uno de desarrollo / pruebas? ¿Por qué?*

BACK

1

❓ **Pregunta que debes resolver:** *¿Sabes iniciar sesión y usar una instalación de WebMin para resolver diferentes tareas de administración/seguridad que se te pidan, sin que necesites usar la consola?*

2

📘 Información adicional requerida para hacerlo

3

🔍 **Se recomienda encarecidamente crear un clon / clon vinculado (mejor) / instantánea (mejor) de tu máquina virtual de Ubuntu antes de realizar cambios en el servidor, por si acaso 😊.** Recuerda que el Lab 0A tiene toda la información necesaria para hacerlo

4

💡

Para instalar *WebMin* usa este tutorial: <https://docs.vultr.com/how-to-install-webmin-on-ubuntu-24-04>. Omite la parte sobre la instalación de compatibilidad con HTTPs, pero entiende **por qué no puedes hacerlo en nuestro escenario**. Una vez instalado, inicia sesión en *WebMin* en el puerto indicado. El usuario y la contraseña son **los mismos que usas para iniciar sesión en Ubuntu**. Usa tu usuario *sudoer*, ya que se necesita acceso como **root** para muchas operaciones.

🛠 Ejercicio L5B1_WMRESOURCEC: Comprobar el consumo de recursos del servidor

👷 Descripción de la actividad / Aplicación práctica

Puede ver los **parámetros de uso de recursos** del servidor en *WebMin*

⭐ Resultados esperados

Puede **dar una interpretación a los datos de uso de recursos** que *WebMin* te muestra para saber si hay algo sospechoso o incorrecto. Puede responder a las siguientes preguntas:



- Un servidor recién instalado muestra continuamente un uso de recursos muy alto. ¿Crees que es un ataque o hay otras razones?
- Si, en lugar de esto, tu servidor de repente tiene un alto consumo continuo de CPU que no corresponde a una razón obvia, ¿qué podría indicar?

📘 Información adicional requerida para hacerlo

Localiza la GUI de estadísticas de uso en tiempo real de *WebMin* y analiza lo que ves para determinar si es normal. No se espera que encuentres problemas en tu entorno de pruebas, pero puede usar la información para responder a las preguntas anteriores, pensando si lo que ves es normal (o no).

🛠 Ejercicio L5B1_WMADDUSER: Agregar un usuario de prueba al servidor

👷 Descripción de la actividad / Aplicación práctica

Usar *WebMin* para crear un usuario nuevo y administrarlo junto con sus grupos.

⭐ Resultados esperados

Sabes cómo **crear nuevos usuarios, configurar** algunos de sus parámetros, **introducirlos** en un grupo o **eliminar usuarios y grupos** si se te pide. También puedes responder a estas preguntas:

- ¿*WebMin* te permite tener fácilmente un inventario de usuarios/grupos?
- ¿Puedes pensar en razones por las que usuarios desconocidos pueden estar registrados en un sistema?
- ¿Puedes pensar en razones por las que los usuarios de inicio de sesión normalmente no interactivo (su shell es `/usr/sbin/nologin`) pueden aparecer como interactivos (su shell es `/bin/bash`)?

❓ Pregunta que debes resolver: ¿Sabes usar *WebMin* para gestionar usuarios / grupos o para resolver tareas típicas que se te pueden encomendar como, por ejemplo, solucionar problemas de seguridad en su configuración?

📘 Información adicional requerida para hacerlo

El objetivo de este ejercicio es permitirte ver **los usuarios del sistema y su configuración**, para que puedas determinar si es correcta en cuanto a seguridad y cambiar cualquier cosa que no cumpla con ciertos parámetros.

🔍 En otras palabras, si tienes que cambiar algo con respecto a usuarios o grupos, debes saber a dónde tienes que ir

Para probar esto, puedes, por ejemplo, eliminar el grupo "**games**" que no se usa en nuestra instalación o eliminar el usuario que creaste una vez que termines de familiarizarte con *WebMin*. No olvides resolver las preguntas, pensando en lo que puede pasar por error o porque alguien olvidó algo y lo que solo se puede explicar si alguien ha tenido mala intención.



NOTA: Si se produce un error al eliminar un usuario mediante WebMin, simplemente crea un archivo `/etc/postfix/main.cf` vacío. Si no se encuentra este archivo, es posible que algunas versiones de WebMin falle al eliminar un usuario debido a que se intenta actualizar la configuración del correo al borrar el usuario.

🛠 Ejercicio L5B1_WMPACKAGEHANDLE: Gestión de paquetes

👷 Descripción de la actividad / Aplicación práctica

Sabes cómo **administrar correctamente los paquetes** usando WebMin

⭐ Resultados esperados

Puedes **actualizar, instalar, ver información y eliminar** paquetes del sistema mediante WebMin. También puedes ver dónde está el inventario de paquetes del sistema.

? **Pregunta que debes resolver:** ¿Sabes a dónde ir y qué hacer si se te pide desinstalar / deshabilitar un paquete rápidamente porque se encontró una vulnerabilidad dentro de él o cualquier otra operación relacionada con paquetes?

BACK

1
2
3
4

📘 Información adicional requerida para hacerlo

Para practicar operaciones de administración de paquetes con WebMin, puedes intentar lo siguiente:

- Ver y buscar dentro del inventario de **paquetes**
- Realizar un **procedimiento** completo de actualización y mejora del paquete
- Ver la **información y el manual** de cualquier paquete
- **Instalar un nuevo paquete** (por ejemplo: `exiftool`) y pruebe que funciona

🛠 Ejercicio L5B1_WMBOOTSERVICE: Deshabilitar algunos servicios que se ejecutan en el momento del arranque

👷 Descripción de la actividad / Aplicación práctica

Sabe dónde está el **inventario** de programas en ejecución en un sistema y cómo administrarlos

⭐ Resultados esperados

Sabes cómo **deshabilitar o desinstalar** servicios del sistema no deseados o potencialmente peligrosos que se inician en el momento del arranque

📘 Información adicional requerida para hacerlo

Puedes usar esta información para realizar este ejercicio, desinstalando estos servicios:

- Por **servicios peligrosos** nos referimos a los no utilizados que se sabe que tienen problemas de seguridad en el pasado, por lo que podríamos estar expuestos a ellos (o a otros futuros)



simplemente ejecutándolos. Los más famosos que cumplen con este criterio son *Avahi*, *Bluetooth* y *CUPS*.

- Otro **servicio que normalmente no se utiliza** es *motd* (*mensaje del día*).





Bloque 2: Seguridad relacionada con el usuario

🛠 Ejercicio L5B2_SECSSH: Seguridad adicional para OpenSSH

👷 Descripción de la actividad / Aplicación práctica

Es necesario **mejorar la seguridad de las conexiones remotas a través de SSH** tanto como sea posible

⭐ Resultados esperados

Esta actividad finalizará cuando **mejores la seguridad de la configuración del servicio SSH** de acuerdo con las especificaciones de los CIS Benchmarks y sepas cómo usar WebMin para ver la configuración SSH actual.

❓ **Pregunta que debes resolver:** ¿Puedes analizar la configuración por defecto de la cuenta de root en SSH y determinar si es segura o no y por qué?

📘 Información adicional requerida para hacerlo

En laboratorios anteriores instalamos *OpenSSH* y te enseñamos a crear contraseñas seguras. Esto mejora su seguridad, pero podemos ir mucho más allá siguiendo la tarea **5.1 Configurar servidor SSH** y la mayoría de sus subtareas.

No obstante, se recomienda **hacer una copia de seguridad de la configuración actual** en caso de que algo salga mal y **ssh** no esté disponible por ello.

🔍 **Siempre puedes iniciar sesión a través de la consola del software de virtualización para solucionar cualquier desastre 😊**

```
sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.factory-defaults
sudo chmod a-w /etc/ssh/sshd_config.factory-defaults
```

Una vez hecho esto, modifica **/etc/ssh/sshd_config** con los valores y directivas indicados por las tareas de la sección **5.1 Configure SSH Server** del Benchmark CIS.

🔍 **Puede utilizar WebMin para facilitar estos cambios al seguir la especificación de CIS Benchmark. Si una directiva no está en el fichero, añádela**

🛠 Ejercicio L5B2_PAM: Configuración segura del módulo PAM

👷 Descripción de la actividad / Aplicación práctica

Necesitas **mejorar tus políticas de contraseñas** tanto como sea posible



⭐ Resultados esperados

Esta actividad finalizará cuando **mejores la política de contraseñas del sistema** de acuerdo con las especificaciones del *Benchmark CIS*.

? *Pregunta que debes resolver:* Si te piden que gestiones las características y la configuración de la autenticación, ¿sabes qué sección del CIS Benchmark tienes que consultar?

▀ Información adicional requerida para hacerlo

PAM (*Pluggable Authentication Modules*) es un servicio que implementa módulos de sistemas de autenticación en sistemas UNIX. PAM se implementa como un conjunto de objetos compartidos que se cargan y ejecutan cuando un programa necesita autenticar a un usuario. Los archivos de PAM normalmente están en el directorio `/etc/pam.d`. **PAM debe configurarse con cuidado** para asegurar la autenticación del sistema, y podemos hacerlo siguiendo la tarea **5.3 Pluggable Authentication Modules** del *CIS Benchmark* y sus subtareas.

No obstante, como se trata más o menos del mismo tipo de operaciones, para ahorrar tiempo **sólo es necesario hacer las subtareas de estas entradas** del documento:

- **5.3.1 Configure PAM software packages**
- **5.3.2 Configure pam-auth-update profiles**

Además, en la tarea **5.3.3 Configure PAM Arguments**, solo se piden las subtareas de **5.3.3.1 Configure pam_faillock** en este ejercicio.

Esto no significa que no podamos pedirte cualquier otra tarea en el mismo bloque en el examen, pero limitamos lo que tienes que hacer ahora porque todas las tareas son muy similares 😊

🛠 Ejercicio L5B2_PWDAGE: Antigüedad de la contraseña y cuentas inactivas

👷 Descripción de la actividad / Aplicación práctica

Debes eliminar las **cuentas no usadas y las contraseñas antiguas**

⭐ Resultados esperados

Esta actividad finalizará cuando **mejores la política de inactividad y caducidad de la contraseña del sistema** de acuerdo con las especificaciones del *CIS Benchmark*.

? *Pregunta que debe resolver:* Si te piden que administres las funciones relacionadas con el tiempo de la administración de contraseñas, sabes la sección de CIS Benchmark que debes consultar?

▀ Información adicional requerida para hacerlo

La antigüedad de la contraseña (el número de días que una contraseña ha estado sin cambiar) y las cuentas inactivas pueden ser un vector de problemas de seguridad.



🔍 **No solo porque tienes más cuentas de usuario para administrar, sino también porque nadie las está usando (y por lo tanto nadie detectará si alguien más está usando su cuenta) y/o es más fácil filtrar una contraseña válida si nunca se cambia**

Podemos controlar este vector de ataque aplicando la tarea **5.4.1 Configure shadow password suite parameters** y sus subtareas:

- **5.4.1.1 Ensure password expiration is configured**
- **5.4.1.2 Ensure minimum password days is configured**
- **5.4.1.3 Ensure password expiration warning days is configured**
- **5.4.1.4 Ensure strong password hashing algorithm is configured**
- **5.4.1.5 Ensure inactive password lock is configured**
- **5.4.1.6 Ensure all users last password change date is in the past**

🔍 **De nuevo, esto no significa que no podamos pedirte cualquier otra tarea en el mismo bloque en el examen, pero limitamos lo que tienes que hacer ahora de nuevo porque todas las tareas son muy similares 😊**



BACK

1

2

3

4





Bloque 3: Seguridad relacionada con los procesos

🔨 Ejercicio L5B3_APPARMOR: Gestión de AppArmor

👷 Descripción de la actividad / Aplicación práctica

Debes asegurarte de que **el sistema MAC AppArmor esté habilitado correctamente**

⭐ Resultados esperados

Esta actividad finalizará cuando compruebes que el **estado de AppArmor sigue las especificaciones de los Benchmark CIS**.

BACK

1

2

3

4

Hand icon

📘 Información adicional requerida para hacerlo

AppArmor es un **sistema de control de acceso** obligatorio (MAC) que limita el conjunto de recursos que pueden usar o a los que puede acceder un programa.

💡 Esto significa que restringe los programas a un conjunto de archivos, atributos y capacidades, por lo que no pueden causar daños graves si se modifican para realizar operaciones no deseadas o son maliciosos

AppArmor funciona a nivel del *kernel* y se carga durante el arranque y administra los permisos a través de **profiles**. Son un conjunto de reglas que determinan lo que el programa puede y no puede hacer. Hay dos formas de aplicar los profiles:

- **Enforce**: Aplica la política definida en el perfil y notifica intentos de violación de esta.
- **Complain**: Solo informa de los intentos de violación de la política, pero no la aplica.

La mayoría de los profiles se cargan en el modo *Enforce*, aunque puede haber profiles de terceros que también se carguen en el modo *Complain*. Para comprobar que AppArmor está correctamente configurado en un sistema, implementa la tarea **1.3.1 Configure AppArmor** del CIS Benchmark, pero concretamente estos tres.

- **1.3.1.1 Ensure AppArmor is installed**
- **1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode**
- **1.3.1.4 Ensure all AppArmor Profiles are enforcing**

🔨 Ejercicio L5B3_SECAPT: Instalar software de seguridad de apt

👷 Descripción de la actividad / Aplicación práctica

Instalar el soporte para asegurarte de que **no se instalen paquetes dañados**



⭐ Resultados esperados

Esta actividad finalizará cuando se instale el *software* mencionado y puedas **verificar la integridad** de algunos paquetes

▀ Información adicional requerida para hacerlo

Puede tener más seguridad en las instalaciones de *software* gracias a la instalación con **apt** de los paquetes **debsums** y **apt-show-versions**. Para probar esto, sigue estas instrucciones <https://manpages.ubuntu.com/manpages/trusty/man1/debsums.1.html> para verificar la integridad de algunos paquetes que elijas.

 **Esta actividad no está en los puntos de referencia de CIS, pero sí en los controles de seguridad de Lynis**





Bloque 4: Logs y monitorización

🛠 Ejercicio L5B4_AUDIT: Configurar reglas de auditoría

👷 Descripción de la actividad / Aplicación práctica

Debes habilitar la auditoría en un SO Linux

⭐ Resultados esperados

Esta actividad finalizará cuando te asegures de que algunos controles de seguridad del CIS Benchmark que configuren una **política de auditoría sólida** estén activos, y que el servicio de auditoría funciona una vez reiniciado después de realizar los cambios.

📘 Información adicional requerida para hacerlo

Este ejercicio requiere la implementación de las siguientes tareas de la sección **6. Logging and Auditing** del archivo CIS Benchmark que te damos. No obstante, la configuración manual de estos archivos **puede llevar mucho tiempo**, por lo que solo tienes que asegurarte de que se implementen los siguientes para tener una **configuración de auditoría predeterminada**.

🔍 **La mayoría de estos controles técnicos de seguridad se pueden automatizar, por lo que perder tiempo cambiando todos estos valores no conviene**

- **6.2.1 Configure audit Service**
 - 6.2.1.1 Ensure auditd packages are installed
 - 6.2.1.2 Ensure auditd service is enabled and active
 - 6.2.1.3 Ensure auditing for processes that start prior to auditd is enabled
 - 6.2.1.4 Ensure audit_backlog_limit is sufficient
- **6.2.2 Configure Data Retention**
 - 6.2.2.1 Ensure audit log storage size is configured
 - 6.2.2.2 Ensure audit logs are not automatically deleted
 - 6.2.2.3 Ensure system is disabled when audit logs are full
 - 6.2.2.4 Ensure system warns when audit logs are low on space

🛠 Ejercicio L5B4_WMLOG: Inspeccionar los logs en busca de comportamientos sospechosos

👷 Descripción de la actividad / Aplicación práctica

Entender cómo se pueden usar los logs para **capturar eventos interesantes** que pueden ser indicios de un ataque.



⭐ Resultados esperados

Sabes que los logs **contienen toda la información en tiempo de ejecución** sobre lo que pasa al usar el sistema y cómo un análisis cuidadoso de su contenido puede revelar indicios de ataques, comportamientos extraños o errores que se pueden usar para varios propósitos relacionados con la seguridad

? Pregunta que debes resolver: ¿Sabes cómo usar WebMin para buscar cosas específicas en los archivos de log?

▀ Información adicional requerida para hacerlo

La mejor manera de ver los registros en acción es provocar eventos que puedan registrarse y representar información interesante. Por ejemplo, realice las siguientes operaciones para ver qué sucede

- Vaya a la sección de logs de *WebMin* y **filtre el contenido del log** buscando la palabra "**login**". ¿Qué ves?
- Ahora **intenta iniciar sesión como un usuario inexistente** (puedes abrir un terminal y escribir **sudo login**). ¿Qué pasa ahora en los archivos de log?
- Haz la misma operación pero **con un usuario existente y una contraseña incorrecta**. ¿Qué pasa ahora en los archivos de log?
- Ahora piensa en lo siguiente: ¿Qué pasa si encuentras varios intentos de inicio de sesión fallidos en el mismo día, hora y minuto? ¿Qué podría significar?

BACK

1

2

3

4

5

🛠 Ejercicio L5B4_WAZUH: HIDS implementado con un XDR profesional: Wazuh como herramienta de monitorización de archivos, procesos y usuarios

扈 Descripción de la actividad / Aplicación práctica

Consiste en **aprender a instalar un software XDR profesional** que pueda monitorizar tu VM, para que tengas una visión completa de lo que está sucediendo en ella y así entender parte de las funciones que puede realizar un XDR en una máquina y su importancia en un despliegue real.

⭐ Resultados esperados

Comprendes cómo el *XDR Wazuh*, entre sus muchas características, **puede funcionar como un HIDS** y ayudarte a vigilar las anomalías que ocurren en tu MV. Puedes responder a estas preguntas:

- *Enlazando con el ejercicio anterior, ¿crees que podrías investigar todas las posibles actividades sospechosas en tu log simplemente filtrando y analizando sus contenidos en un tiempo razonable? Por lo tanto, ¿entiendes la utilidad de un XDR en un entorno real?*
- *Ahora que sabes cómo desplegar un XDR/SIEM y sus agentes, ¿cómo crees que funcionan las empresas que alquilan uno a una empresa de seguridad (que supervisa sus máquinas en busca de anomalías)?*
- *¿Qué crees que significa que Wazuh informe de una ejecución con éxito de sudo?*
- *¿Y de uno que no ha tenido éxito?*



- ¿Qué crees que significa cuando Wazuh detecta una instalación de software que no iniciaste tú? ¿Se te ocurre alguna posibilidad legítima de que eso suceda? ¿E ilegítima? (Vale, esto último es muy fácil 😊)
- Si pones a Wazuh a monitorizar archivos importantes del SO en determinados directorios y detecta un cambio en el hash de alguno de ellos, ¿eso significa siempre que ha pasado algo malo?
- Por ejemplo, ¿qué razones legítimas y no legítimas pueden explicar cambios en el archivo /etc/shadow o en el archivo /etc/passwd?
- Aunque en este ejercicio vemos cómo Wazuh detecta comportamientos sospechosos, no estamos respondiendo a ellos de ninguna manera. Si te digo que en un SOC tienen preparado un procedimiento de respuesta para cualquiera de estas anomalías de manera que, cuando se detecta y confirma una, se pone en marcha ese procedimiento para dar respuesta a ella (manual, automático o mixto), ¿entiendes ahora más o menos cómo funciona un SOC en general?

? **Pregunta que debes resolver:** Si alguien te da acceso a una instancia de Wazuh en funcionamiento, ¿sabes cómo buscar eventos específicos que te pidan?

■ Información adicional requerida para hacerlo

Un sistema de detección de intrusos basado en host (HIDS) es un **sistema de detección de intrusos** capaz de monitorizar y analizar **los componentes internos** de un sistema. Este tipo de software puede monitorizar todo o parte del comportamiento en funcionamiento y el estado de un sistema dependiendo de cómo esté configurado.

🔍 **Por ejemplo, un HIDS podría detectar qué programa accede a qué recursos y descubrir que, por ejemplo, un procesador de textos ha comenzado repentina e inexplicablemente a modificar la base de datos de contraseñas del sistema, lo que es indicativo de una infección en curso**

Además, un HIDS podría examinar el estado de un sistema, su información almacenada, ya sea en la memoria RAM, en el sistema de archivos, archivos de log, etc., y verificar que el contenido de estos es el esperado, es decir, que no ha sido modificado por intrusos o de forma inesperada. Para ello, crea **firmas criptográficas** (como las del **Tema 2** de teoría) de los archivos que le indicamos monitorizar, de forma que se detecte cualquier cambio en ellos.

🔍 **En comparación con los sistemas de detección de intrusos basados en la red, los HIDS tiene la ventaja de poder identificar ataques internos. NIDS examina el tráfico de red, mientras que HIDS examina los datos que se originan en los sistemas operativos.**

Es importante mencionar que los HIDS suelen hacer todo lo posible para evitar que sus bases de datos de objetos / hashes y sus informes sean manipulados. Si los intrusos pudieron modificar cualquiera de los objetos que monitoriza el HIDS, también podrían modificar los datos que usa.

En los CIS Benchmarks hay una sección para instalar un HIDS, ya que tener uno eleva el nivel de seguridad de un sistema. El CIS ha optado por un HIDS que **no depende de ningún componente externo** y que funciona dentro del mismo host, llamado **AIDE**. En concreto, su instalación se trata en estos apartados:

- **6.3 Filesystem Integrity Checking**
 - **6.3.1 Ensure AIDE is installed (Automated)**
 - **6.3.2 Ensure filesystem integrity is regularly checked (Automated)**

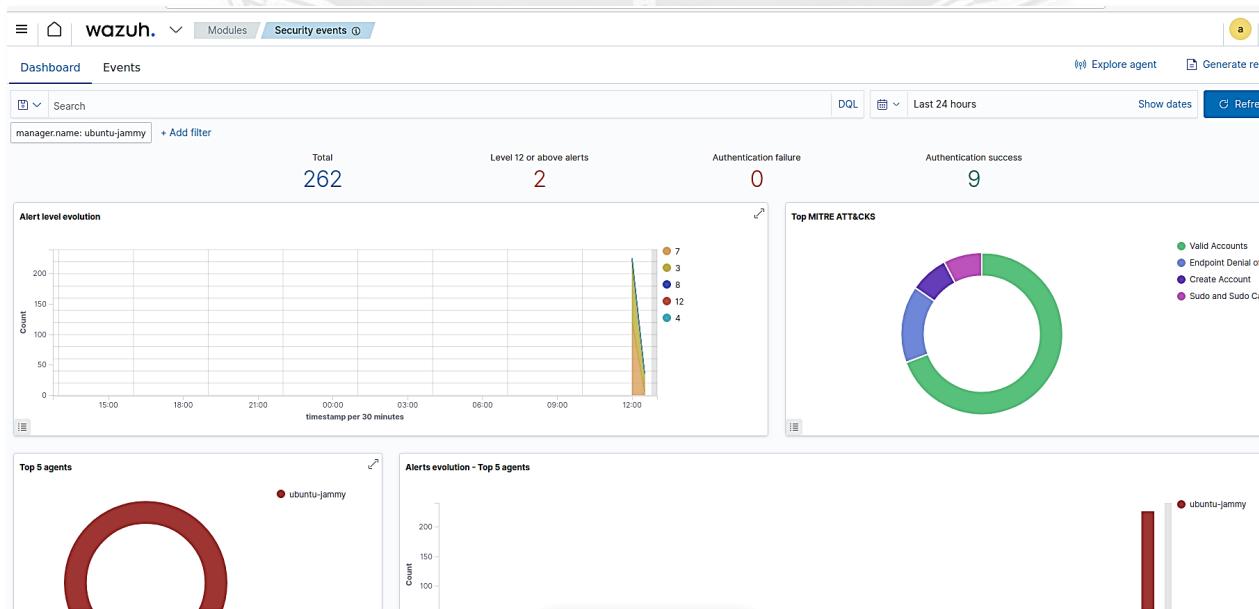
Un HIDS muy similar a este, que se puede usar como sustituto, es **Tripwire** (<https://linuxconfig.org/intrusion-detection-systems-using-tripwire-on-linux>). Sin embargo, estos HIDS, precisamente por no depender de nada externo, cuentan con una serie muy limitada de funcionalidades (básicamente la detección de cambios en ficheros importantes). *Wazuh* los supera con creces en funciones, como veremos, ya que se trata de un XDR que incluye funciones HIDS.

Wazuh no forma parte de los benchmarks del CIS, pero como es una herramienta que cubre las mismas necesidades y muchas más que utilizaremos en laboratorios posteriores, la usaremos para reemplazar AIDE

Instalación de un solo nodo de Wazuh en una máquina virtual mediante Docker

Para poner en marcha *Wazuh* fácilmente, recomendamos los siguientes pasos:

- **Hacer el clon enlazado** de la VM del curso como indicamos al principio del laboratorio, con **6Gb de RAM y 4 núcleos** (¡la potencia tiene un precio!).
- Hay varias formas de instalar *Wazuh*, pero la mejor en nuestro caso es ***Wazuh-Docker***, que lo instala utilizando el mismo sistema que utilizamos en el curso para desplegar algunos laboratorios (contenedores *Docker*). Las instrucciones están aquí: <https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html>, y debes asegurarte de lo siguiente:
 - El tipo de instalación que vamos a hacer es **el despliegue de un solo nodo**. Es igual de funcional que la otra, pero con todo en una sola máquina (no tenemos los recursos para hacer una instalación distribuida).
 - En el paso de generar certificados, nos da dos opciones: **generarlos o proporcionarlos nosotros mismos**. En este caso, es mejor **generarlos** con el software proporcionado (`generate-indexer-certs.yml`). Asegúrate de ejecutarlo una vez antes de iniciar *Wazuh* como indica el sitio web. No es necesario cambiar ninguno de los archivos que proporcionan.
- Inicia el XDR como se indica en el tutorial, yendo al directorio donde has descomprimido el contenido del *git* y escribiendo `docker-compose up -d`. Espera unos 30 segundos para que todo el sistema se active. Cuando todo esté listo, deberías poder acceder al XDR abriendo el navegador de la VM y yendo a <https://127.0.0.1>. La cuenta de usuario predeterminada es "**admin**" y la contraseña es "**SecretPassword**". Si todo va bien, deberíamos ver una pantalla como esta:





 Si vas a implementar esto en un entorno real, ¡no olvides cambiar la contraseña de administrador! 😊

Wazuh trabajando como HIDS

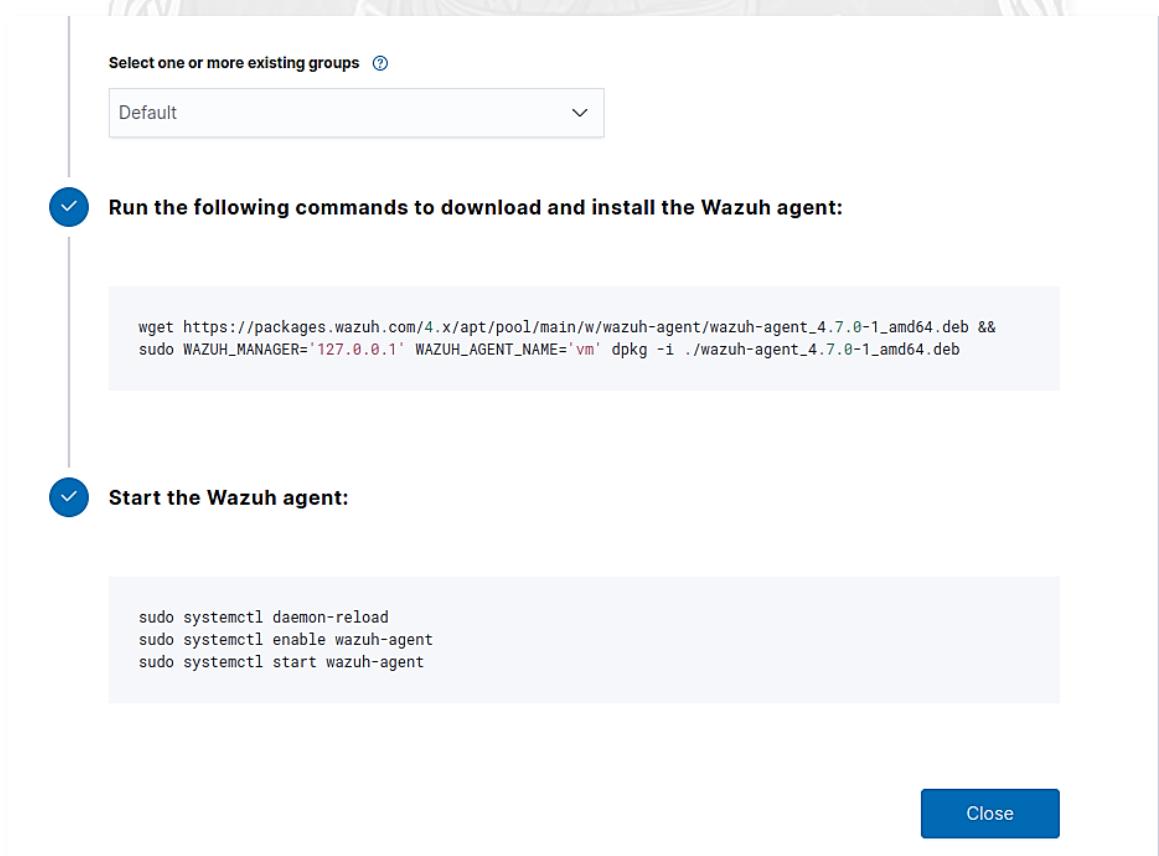
Wazuh es un sistema de vigilancia en este momento, pero **aún no tiene máquinas para vigilar**. De hecho, nos advierte que **no tiene agentes**. Un agente es el software que desplegamos en cada máquina monitorizada, y que se encarga de:

- **Recopilación de información** del sistema en el que está instalado
- Estar configurado para recopilar **diferentes tipos de información** (cosas como los diferentes *logs* de las acciones que se producen, firmas de archivos... todo lo que necesitas)
- **Enviárselo al XDR** mediante comunicaciones cifradas. De hecho, si juegas un poco con la GUI puedes ver el algoritmo que usa para enviar la información. *¿Sabes qué algoritmo utiliza? ¿Es un cifrado simétrico o asimétrico?*

A continuación, el XDR interpreta la información de todos los sistemas que monitoriza (es decir, en los que tiene desplegados sus agentes) para detectar anomalías. *¿Cómo se despliega un agente?* **Wazuh los genera por nosotros**. Hacemos clic en el mensaje que se queja de que no hay agentes y configuraremos uno nuevo para **monitorizar la propia MV**, seleccionando la creación de un agente de **.deb** de 64 bits:

BACK

1
2
3
4

Select one or more existing groups [?](#)

Default

Run the following commands to download and install the Wazuh agent:

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.0-1_amd64.deb &&
sudo WAZUH_MANAGER='127.0.0.1' WAZUH_AGENT_NAME='vm' dpkg -i ./wazuh-agent_4.7.0-1_amd64.deb
```

Start the Wazuh agent:

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

[Close](#)

 **NOTA:** Aprovechando la tarjeta de red bridge que tienes en tu máquina virtual, también puedes realizar pruebas en parejas. Uno de vosotros tendrá la máquina monitorizada (el agente) y el otro la interfaz de monitorización de Wazuh. Solo tienes que cambiar la IP al instalar OSSEC a la IP de la red bridge de la VM de tu compañero que ejecuta la instancia de Wazuh. Esto es opcional, y solo para mostrarte cómo puedes monitorizar fácilmente varias máquinas con un solo Wazuh



Ahora, desde un terminal de nuestra VM **copiamos los comandos que el propio Wazuh** nos da para instalar e iniciar el agente. Con esto, *Wazuh* debería mostrar que tiene **1 agente activo** y comenzará a recopilar información de la máquina que lo ejecuta. Ni que decir tiene que monitorizar más máquinas es lo mismo, y solo tendríamos que indicar la IP en la que se encuentra la VM en la que ejecutamos *Wazuh* al generar el agente, obviamente suponiendo que esta IP es accesible desde la máquina a monitorizar.

🔍 ¿Entiendes ahora lo fácil que es monitorizar toda una infraestructura de máquinas con un solo Wazuh? El principal problema es que cuantas más máquinas monitorizas más recursos necesitas, pero para una instalación pequeña es una muy buena solución. Por cierto, en caso de que te lo estés preguntando, sí, Wazuh también tiene agentes para Windows y MAC (tengo alumnos que ahora monitorizan los equipos de su casa así 😊)

Wazuh, para ahorrar recursos, **no viene con todas sus funcionalidades activas**. Uno de las inactivas es la monitorización de cambios en archivos importantes (**File Integrity Monitoring** o FIM) y su posterior notificación si se detecta alguno. Para ello, *Wazuh* utiliza un software que está integrado en sus agentes llamado **OSSEC**. Por defecto OSSEC viene con esta funcionalidad deshabilitada y debes activarla cambiando su archivo de configuración (**/var/ossec/etc/ossec.conf**) en la VM (o la máquina monitorizada) así:

```
GNU nano 6.2                               /var/ossec/etc/ossec.conf *           I
93      <interval>12h</interval>
94      <skip_nfs>yes</skip_nfs>
95  </sca>
96
97  <!-- File integrity monitoring -->
98  <syscheck>
99      <disabled>no</disabled>
100
101 <!-- Frequency that syscheck is executed default every 12 hours -->
102 <frequency>43200</frequency>
103
104 <scan_on_start>yes</scan_on_start>
105
106 <!-- Directories to check (perform all possible verifications) -->
107 <directories realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</di>
108 <directories>/bin,/sbin,/boot</directories>
109
110 <!-- Files/directories to ignore -->
111 <ignore>/etc/mtab</ignore>
112 <ignore>/etc/hosts.deny</ignore>
[ line 107/220 (48%), col 23/86 ( 26%), char 2926/6043 (48%) ]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line
```

Con esta configuración, le pedimos a OSSEC que monitorice todos los cambios en tiempo real en los directorios `/etc`, `/usr/bin/y` `/usr/bin`, que contienen programas ejecutables críticos del sistema operativo. Más información:

- <https://www.ossec.net/docs/manual/syscheck/index.html>
 - <https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/how-to-configure-fim.html>

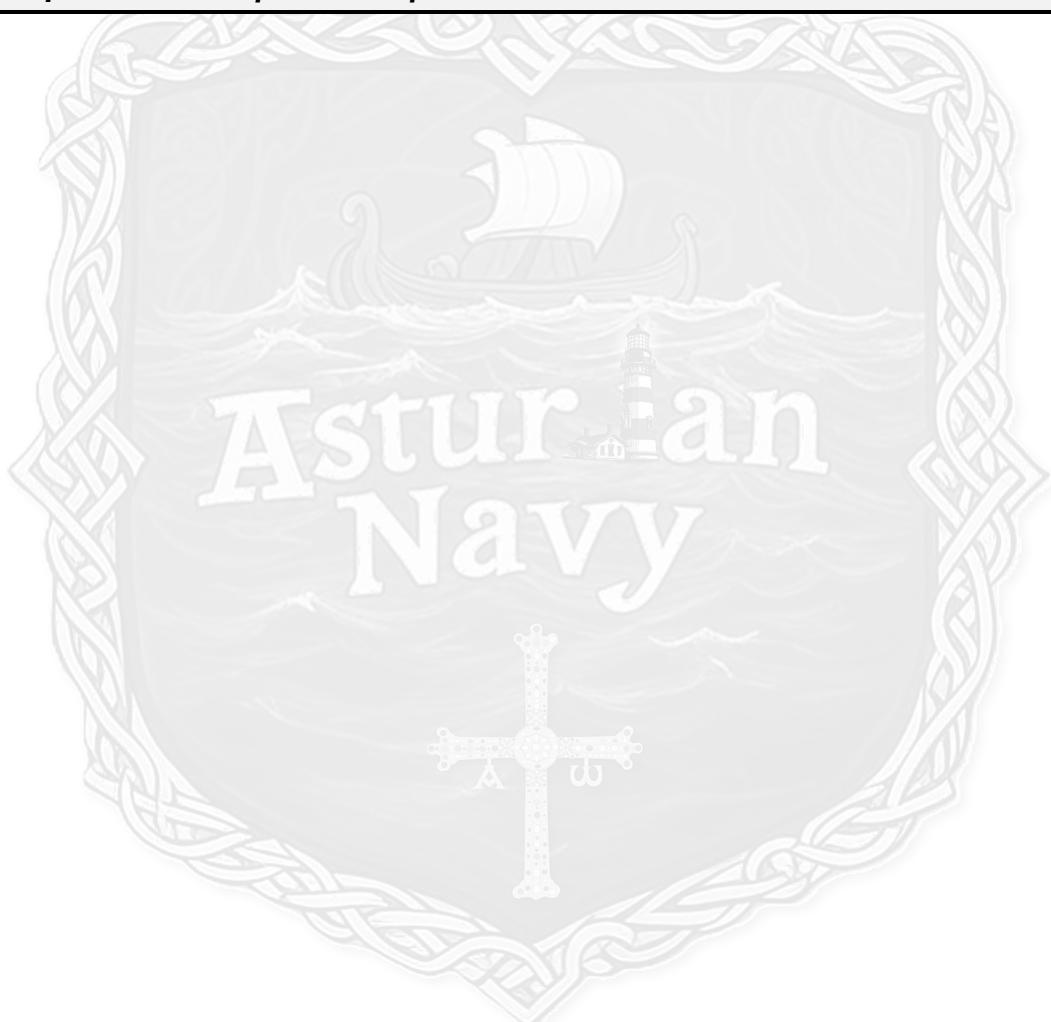
 **Podemos monitorizar más directorios, e incluso archivos individuales, agregando más entradas al archivo. Todo depende de lo que nos interese y de lo que haya en el sistema, por supuesto. ¡Es solo cuestión de probar y experimentar!**



Una vez hecho esto, tenemos que **reiniciar el agente en la VM** (`sudo systemctl wazuh-agent restart`), y podremos detectar cambios en los archivos de esos directorios. Ahora ya tenemos *Wazuh* listo para funcionar como HIDS, así que para finalizar el ejercicio haremos las siguientes pruebas en la VM, comprobando luego en la GUI de *Wazuh* (pulsamos en *Refresh*) si se detectan:

- **sudo** a un comando, pero **con la contraseña incorrecta** para que falle
- Vuelve a hacer el **sudo**, pero esta vez con la **contraseña correcta**
- Instala algo con **apt** o actualiza el sistema operativo
- Edita el archivo **/etc/passwd** y cambie el shell de usuario **root** de **nologin** a **/bin/bash**. ¿Qué crees que hace esto? ¿Para qué se podría usar si, en lugar de **root**, fuera otro usuario más "inocente"? ¿*Wazuh* lo detecta?

 **Recuerda:** ¡Guarda esta máquina virtual para futuros laboratorios!



 BACK

1

2

3

4





Insignias y autoevaluación

NOTA: Dispones de una versión de esta tabla de insignias en formato editable en el *Campus Virtual*. Puedes usar ese archivo para crear fácilmente un documento en el formato que quieras y tomar notas de tus actividades para crear un log de lo que has hecho. Recuerda que este material se puede llevar a los exámenes de laboratorio.

Nivel de insignia	Se desbloquea cuando	¿Desbloqueado?
	Puedes instalar un <i>WebMin</i> funcional y entender qué máquinas servidor deben (o no) tener uno	
	Conoces el significado de los diferentes parámetros que controlan la caducidad de las contraseñas y el hash según los <i>Benchmarks CIS</i>	
	Sabes cómo ver e interpretar la información de uso de recursos del servidor mediante <i>WebMin</i>	
	Sabes dónde configurar los parámetros del servicio SSH en <i>WebMin</i>	
	Sabes dónde está el archivo de configuración de SSH y entiendes la función de sus diferentes parámetros de seguridad	
	Puedes responder a la siguiente pregunta: <i>Si cambiamos el puerto ssh por defecto de 22 a otro, ¿qué ventaja de seguridad crees que podríamos tener?</i>	
	Comprendes por qué ser root puede suponer un problema de seguridad serio y por qué existen todas las medidas que evitan los inicios de sesión de root no autorizados	
	Entiendes por qué las cuentas de servicio no deben usarse para inicios de sesión interactivos. Puedes responder a la siguiente pregunta: <i>si suponemos que por defecto no hay ninguna cuenta de servicio configurada para que haga inicio de sesión interactivo, ¿cuál podría ser la causa de encontrar de repente una configurada de esa manera?</i>	
	Comprendes la utilidad del módulo PAM en cuanto al control de autenticación, y sus roles si tienes que cambiar alguno de sus parámetros	
	Entiendes que un uso continuo de recursos muy alto puede ser causado por malas decisiones al elegir los parámetros del servidor (CPU, RAM...) o por <i>malware</i> , y qué situaciones indican una u otra	
	Puedes verificar el estado de <i>AppArmor</i> y sabes cómo habilitar perfiles	
	Puedes usar <i>WebMin</i> para tener un control preciso sobre los usuarios registrados en un sistema, conociendo también las posibles razones que pueden explicar la presencia de usuarios desconocidos o usuarios con inicio de sesión no interactivos que ahora son interactivos	
	Sabes cómo comprobar el inventario de paquetes y realizar operaciones generales de administración de paquetes con <i>WebMin</i>	

BACK

1

2

3

4





	Puedes desinstalar servicios mediante <i>WebMin</i> porque no se utilizan o son peligrosos, y por qué son peligrosos	
	Puedes habilitar el <i>demonio de auditoría de Linux (auditd)</i>	
	Comprendes la importancia de comprobar los registros y de contar con herramientas capaces de detectar comportamientos inusuales a través de su contenido	
	Puedes instalar y usar <i>wazuh</i> en una máquina virtual y entender la utilidad de un XDR para monitorizar las actividades de los usuarios, los procesos y el uso de archivos de la máquina. Puedes responder a la siguiente pregunta: <i>¿Qué tipo específico de malware crees que puedes detectar más fácilmente con este tipo de herramientas?</i>	



BACK
1
2
3
4