**Herramienta de análisis y auditoría de seguridad**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Ubuntu**](#_g59i8ewd3ed3) **2**

[**2.1 Lynis:**](#_5d38uxjyswtl) **2**

[**3. Windows**](#_b06vwfkulqiv) **7**

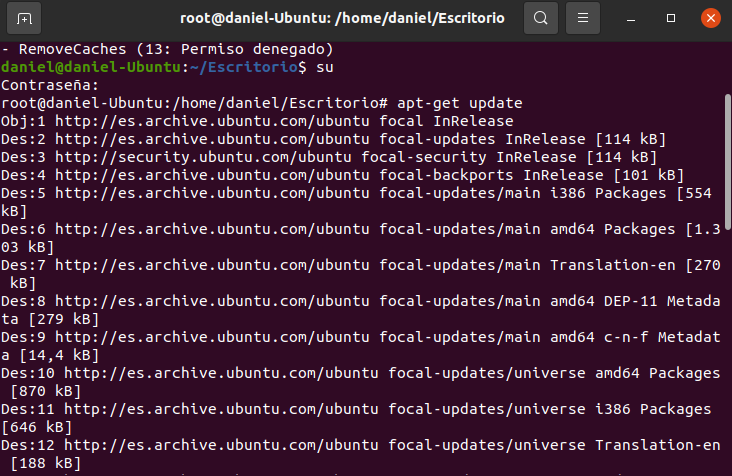
[**3.1 CLARA:**](#_79l19m8png1) **7**

# **2. Ubuntu**

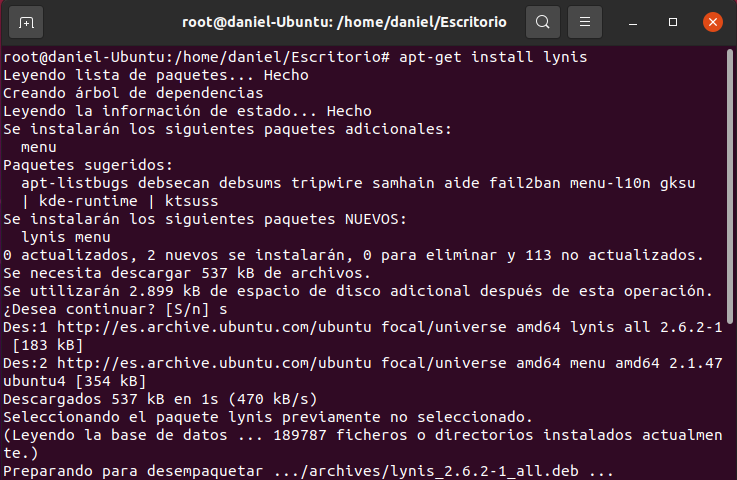
### **2.1 Lynis:**

1. Preparar una máquina Ubuntu con recomendaciones de optimización vistas en clase.

2. Actualizar listado de paquetes en la máquina

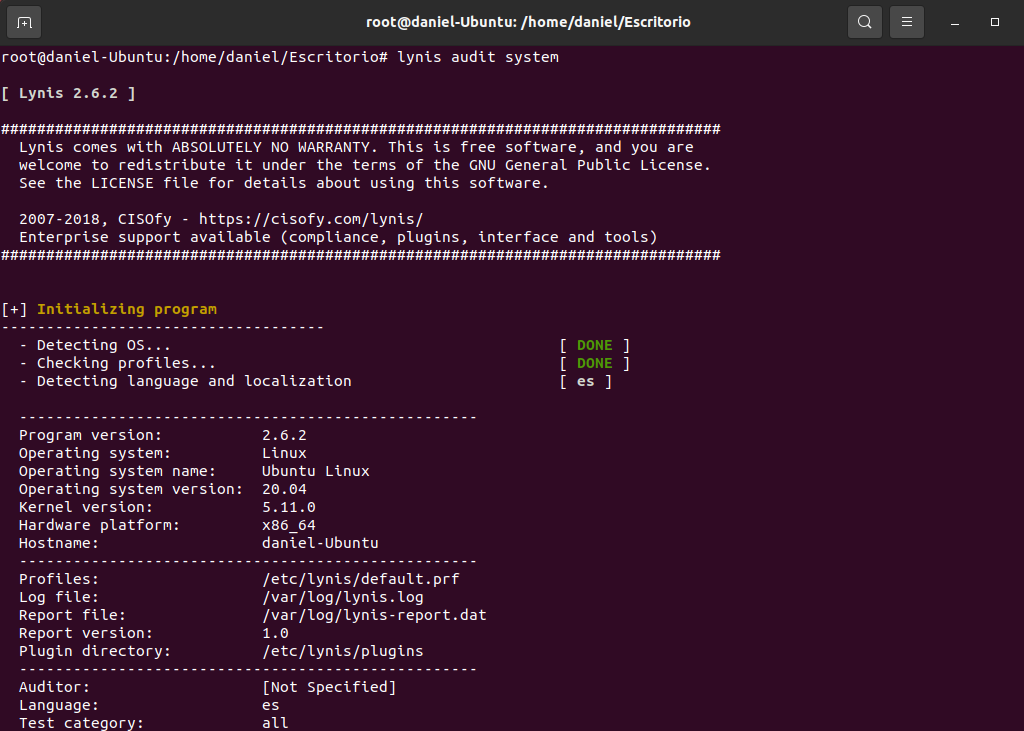


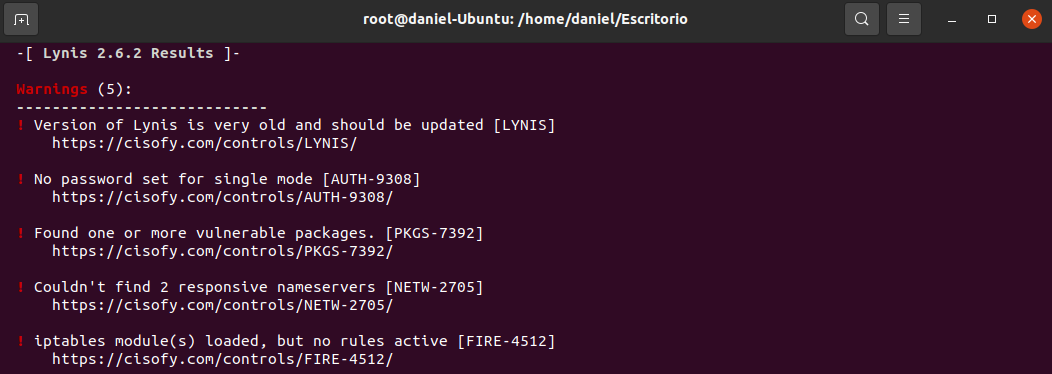
3. Instalar herramienta Lynis



4. Ejecutar para detectar las vulnerabilidades del sistema. Hacer un análisis del resultado

que nos ofrece, tanto de los avisos como de las soluciones propuestas.





**AUTH-9308:**

El acceso físico a la máquina se puede utilizar para cargar software alternativo o un sistema operativo diferente, durante la fase de arranque. Configure una contraseña en el cargador de arranque para evitar este riesgo.

El modo de usuario único en Linux está protegido de diferentes formas. Depende de qué administrador de servicios. Para distribuciones que usan systemd, eche un vistazo a los objetivos relacionados como rescate, shell de consola y emergencia.

Archivos relacionados

/usr/lib/systemd/system/emergency.target

/usr/lib/systemd/system/rescue.target

**PKGS-7392:**

Lynis prueba paquetes vulnerables, paquetes con fallas de seguridad conocidas y que ya tienen una actualización disponible.

Lynis prueba la presencia de paquetes vulnerables. Cuando encuentra alguno, este control se activa con una advertencia relacionada. Está marcado como de alto impacto, ya que cada paquete vulnerable tiene un potencial diferente para ser explotado por atacantes. Aún así, debe determinar el impacto para su entorno y ver cuándo desea aplicar la actualización de seguridad relacionada.

Comandos

apt-get update

apt-get upgrade

**NETW-2705:**

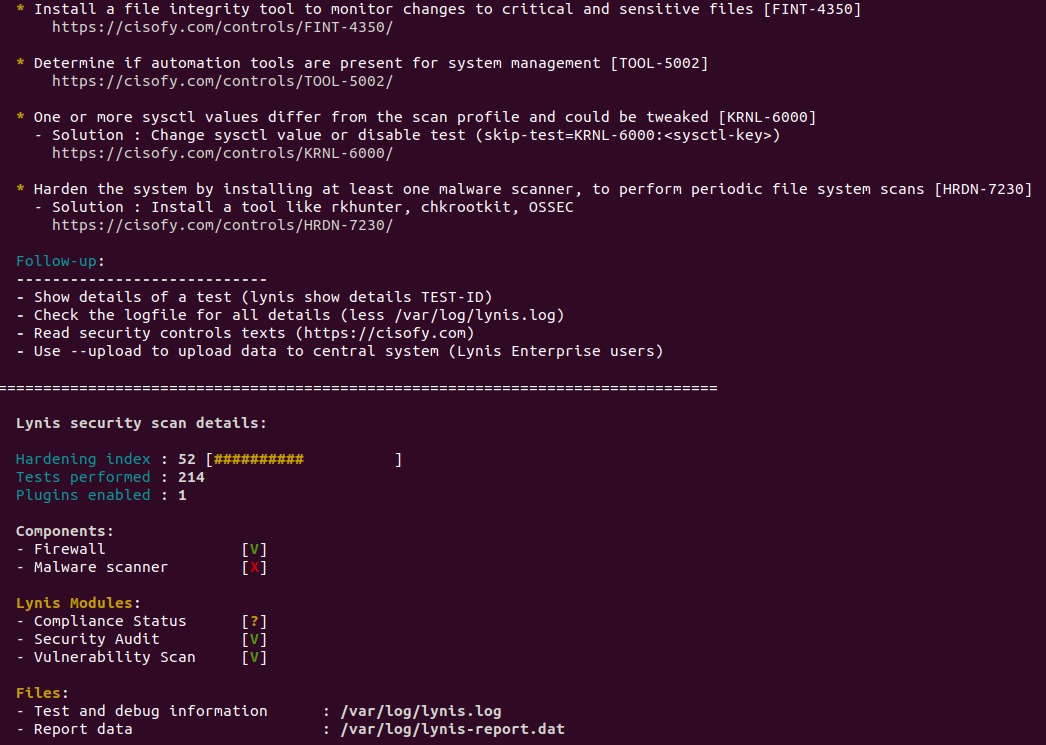
Para limitar la posibilidad de fallas o un mal rendimiento, se recomiendan al menos dos servidores de nombres en funcionamiento. Lynis prueba la disponibilidad de los servidores de nombres y si realmente responden a las consultas. Para determinar qué servidores DNS se utilizan, consulte el archivo /etc/resolv.conf.

Dependiendo de su sistema, es posible que deba realizar cambios en su archivo /etc/resolv.conf , o de otra manera. Los sistemas basados ​​en Debian pueden usar / etc / network / interfaces para definir servidores de nombres (dns-nameservers 1.2.3.4 5.6.7.8 9.10.11.12), o /etc/resolvconf/resolv.conf.d/tail.

**FIRE-4512:**

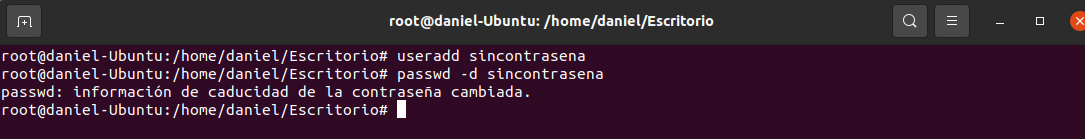
Lynis comprueba la disponibilidad de IPtables, pero también si el conjunto de reglas no está vacío. Esto puede indicar una mala configuración o que falta un conjunto de reglas en el sistema.

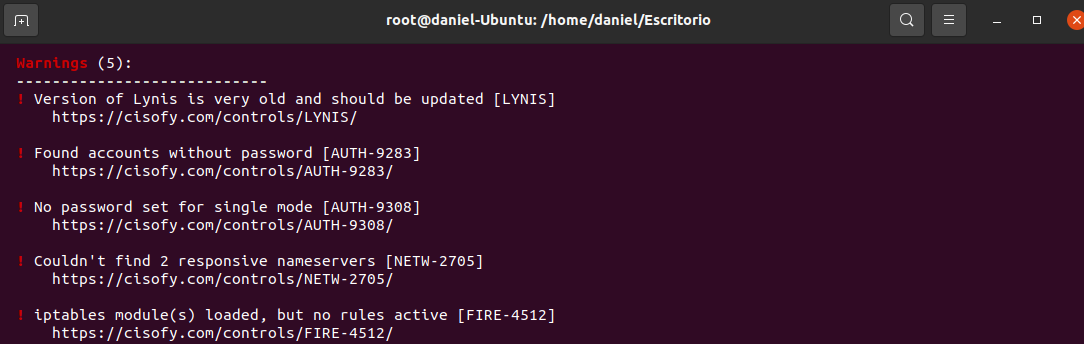
Por lo general, este control aparece cuando se carga el módulo iptables, mientras que no se cargan reglas de firewall. Considere apagar el software de firewall por completo o, preferiblemente, complétalo con una política de firewall adecuada.



5. Crea un nuevo usuario sin contraseña. Vuelve a ejecutar Lynis y comprueba si aparece

esto como un incidente.

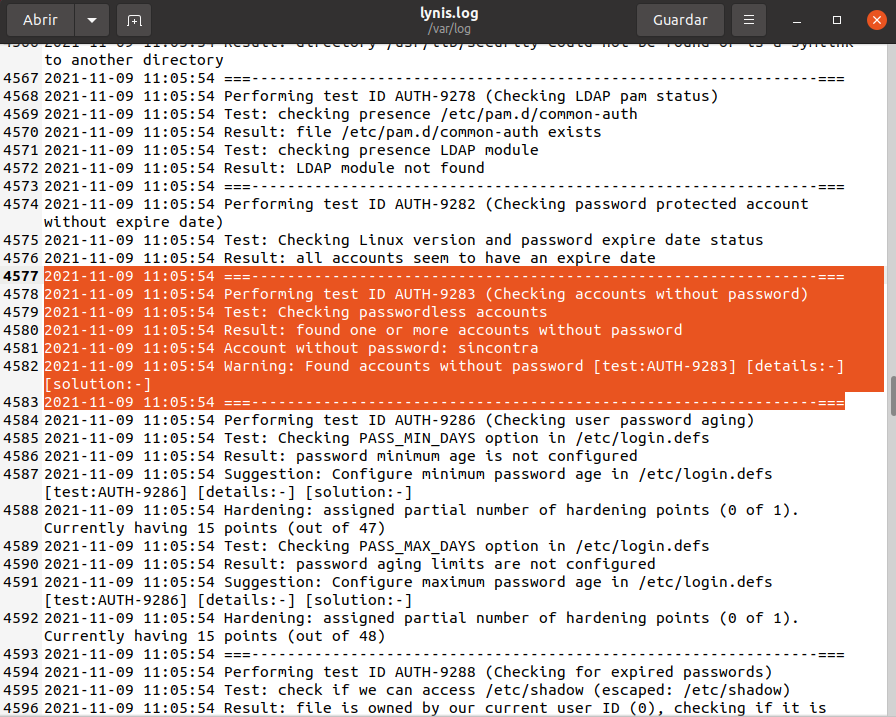




6. Comprueba que la información de cada auditoría ha sido guardada en los logs en la

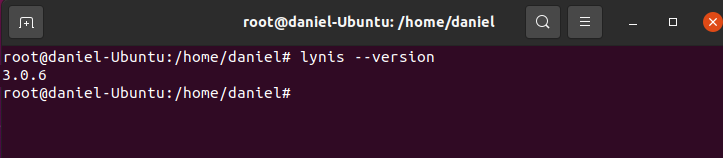
carpeta /var/log/lynis.log Buscar cómo aparece la información sobre el suceso que se ha

dado en el punto cinco de la práctica.



7. Si instalaste Lynis desde los repositorios oficiales de ubuntu, podrás comprobar que te

indica que no está en su última versión (lynis show version). Realiza los cambios necesarios para actualizar Lynis desde sus repositorios y obtener la versión más actualizada.



8. Busca las diferencias principales entre Lynis y otros software de análisis de vulnerabilidades como OpenVAS o Nessus.

|  | **Lynis** | **Open VAS** |
| --- | --- | --- |
| **Descripción** | Lynis es una herramienta de auditoría de seguridad para sistemas que ejecutan Linux, macOS o Unix. Se puede utilizar para evaluaciones de seguridad y auditorías de configuración. | OpenVAS es un framework de varios servicios y herramientas que ofrece una solución de escaneo y gestión de vulnerabilidades. |
| **Fortalezas** | * El código fuente es fácil de leer y comprender. * Más de 100 colaboradores * Más de 8000 estrellas de GitHub * La herramienta es fácil de usar * Disponible como paquete (instalación simplificada) * Soporte comercial disponible * El lenguaje utilizado es el script de shell * Número muy bajo de dependencias * El proyecto está maduro (más de 10 años) * El código fuente de este software está disponible | * El código fuente de este software está disponible * Herramienta conocida |
| **Lenguaje de programación** | Secuencia de comandos de shell | C |
| **Última actualización** | 2021-07-03 | 2021-06-24 |

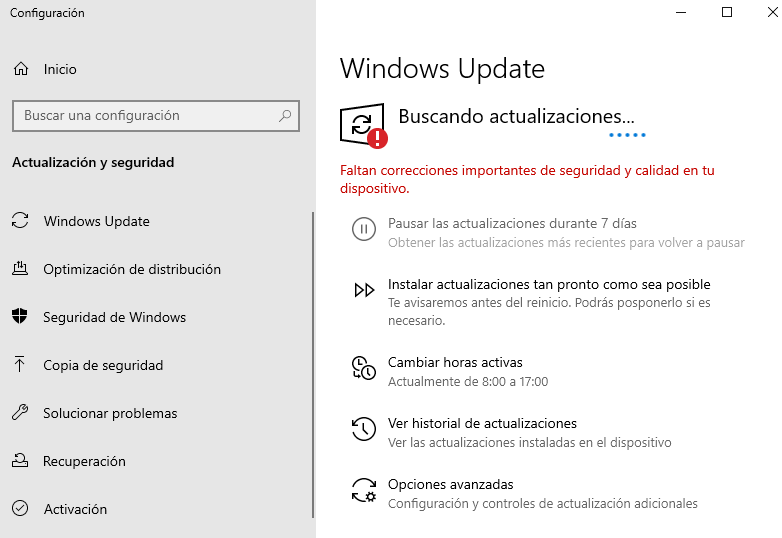
# **3. Windows**

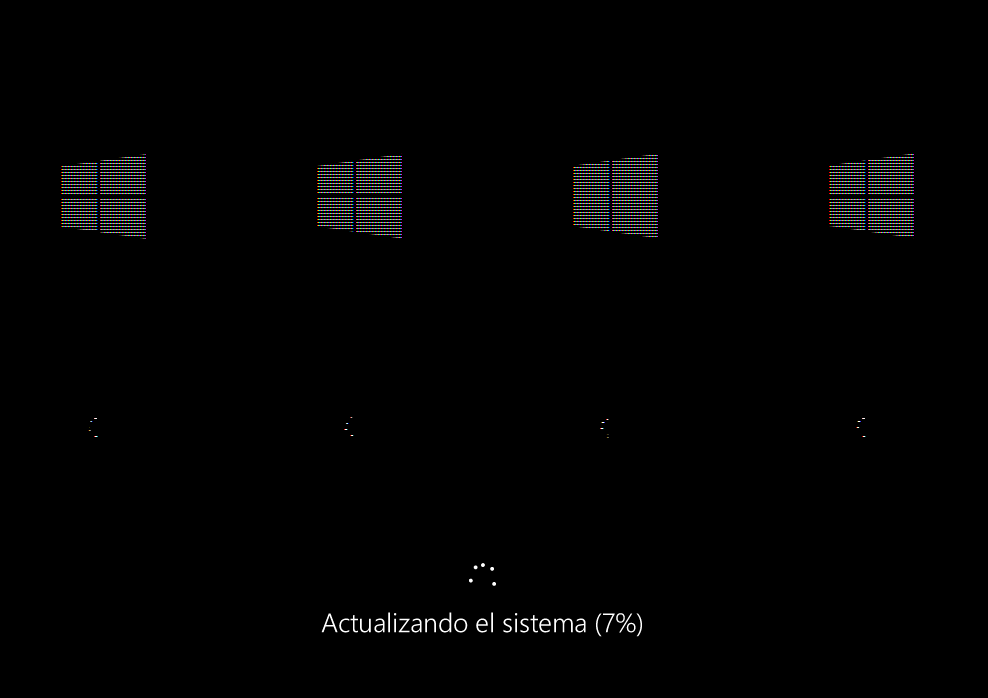
### **3.1 CLARA:**

1. Preparar una máquina con Windows 10 siguiendo las recomendaciones de optimización vistas en clase.

2. Actualizar el S.O. con los últimos parches y actualizaciones

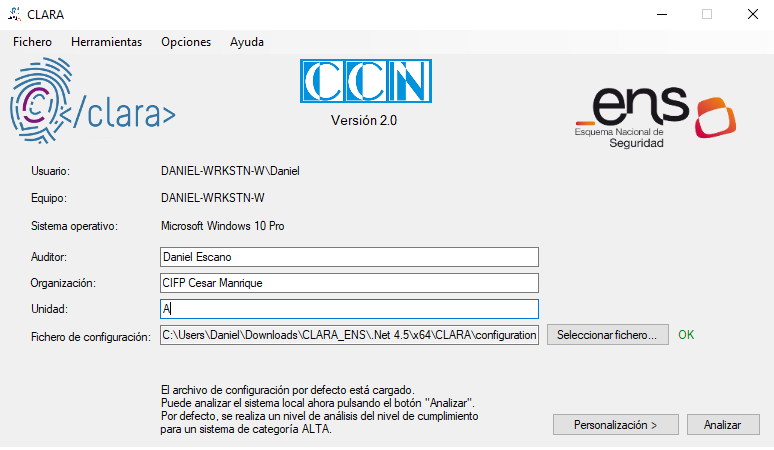
3. Iniciar sesión con el usuario que hemos creado en el punto 1



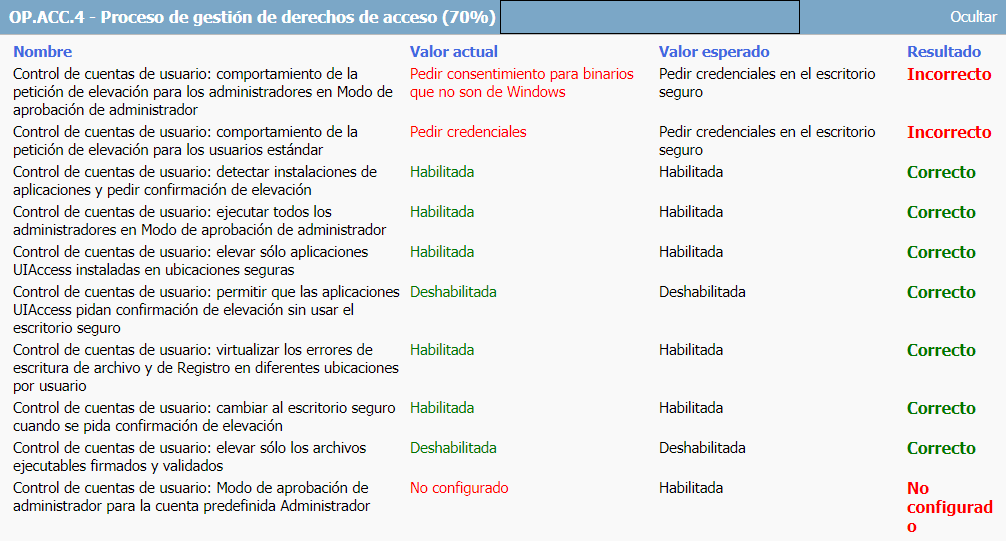


4. Instalar CLARA en la máquina virtual. En el mismo archivo comprimido de descarga se encuentra el manual de uso de la herramienta.

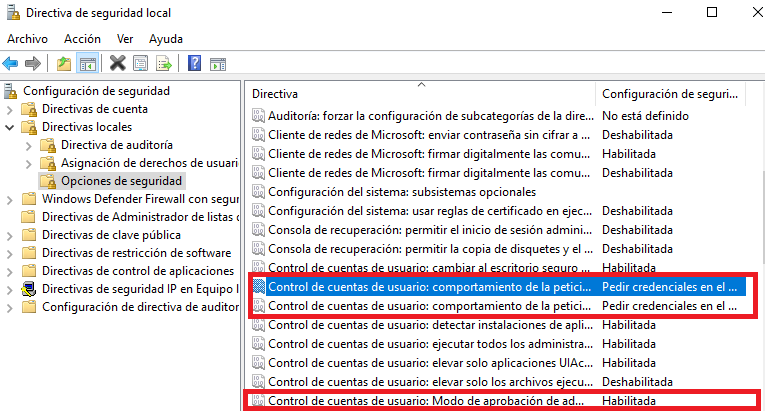
5. Iniciamos la herramienta y rellenamos los datos que nos pide. Analiza el sistema.



6. Realiza un análisis del informe con el fin de comprender los elementos que ha analizado y los resultados.



7. Trata de solucionar los elementos que te propone como Incorrectos o No configurados.



8. Vuelve a ejecutar el análisis con la herramienta y comprobar que han sido corregidos.

