SE ha escogido Linys como una herramientadentro de Linux para **auditar diferentes aspectos** y asegurar la integridad **del sistema, detectando configuraciones inadecuadas y proponiendo medidas correctivas**. Sobre el entorno de Kali -Linux

Aunque existen diversas formas para instalar Lynis, para este caso realizaremos la instalación desde el repositorio más reciente.

 Paso 1

Es importante recalcar que este repositorio usa el protocolo HTTPS para su acceso por lo cual debemos confirmar que nuestro servidor cuente con el soporte HTTPS, para validar esto ejecutaremos la siguiente línea:

1. dpkg -s apt-transport-https | grep -i status



Paso 2

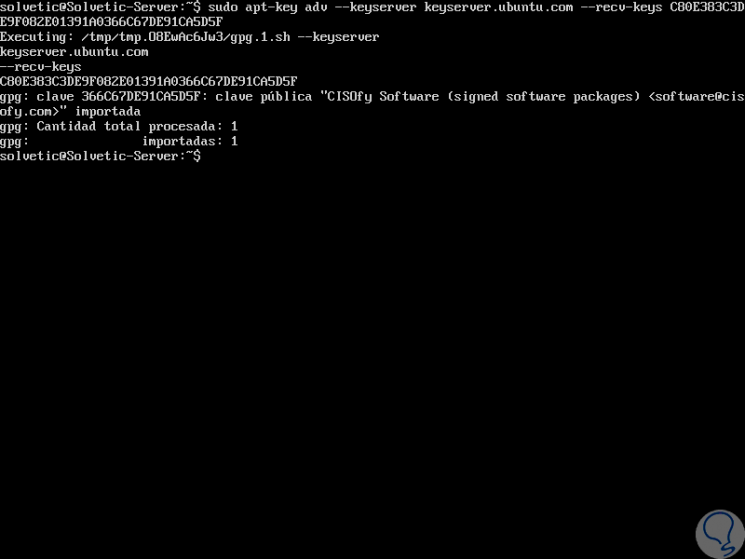
En caso de no contar con este soporte ejecutaremos la siguiente línea para su instalación:

1. apt-get install apt-transport-https

Paso 3

Una vez estemos seguros que contamos con el soporte HTTPS procedemos a instalar la clave del repositorio oficial ejecutando lo siguiente:

1. apt-key adv --keyserver keyserver.ubuntu.com --recv-keys C80E383C3DE9F082E01391A0366C67DE91CA5D5F



Paso 4

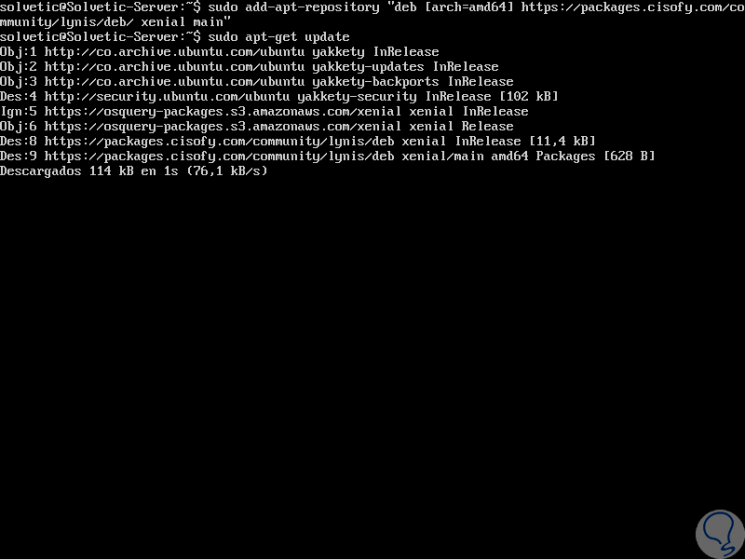
Ahora agregaremos el repositorio oficial de Lynis para que esté disponible en el administrador de paquetes, para ello ejecutamos lo siguiente:

1. add-apt-repository "deb [arch=amd64] https://packages.cisofy.com/community/lynis/deb/ xenial main"



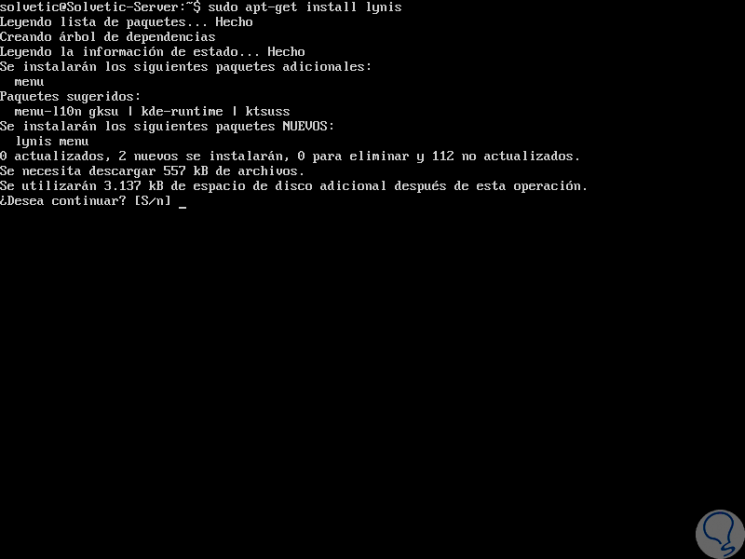
Actualizamos los paquetes del sistema operativo:

1. apt-get update



Una vez actualizados los paquetes procedemos con la instalación de Lynis en Ubuntu Server ejecutando el siguiente comando:

1. apt-get install lynis

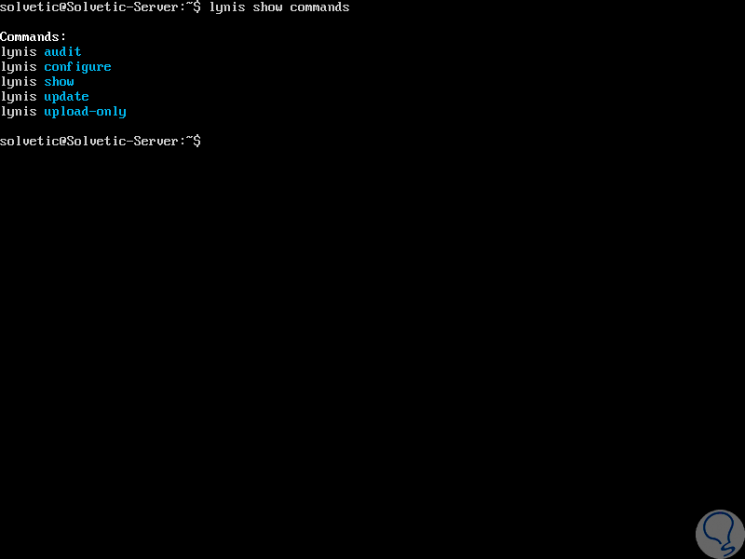


Aceptamos la descarga y respectiva instalación de los paquetes de Lynis en Ubuntu Server 16.10.

**Auditoría de seguridad con Lynis en Kali**

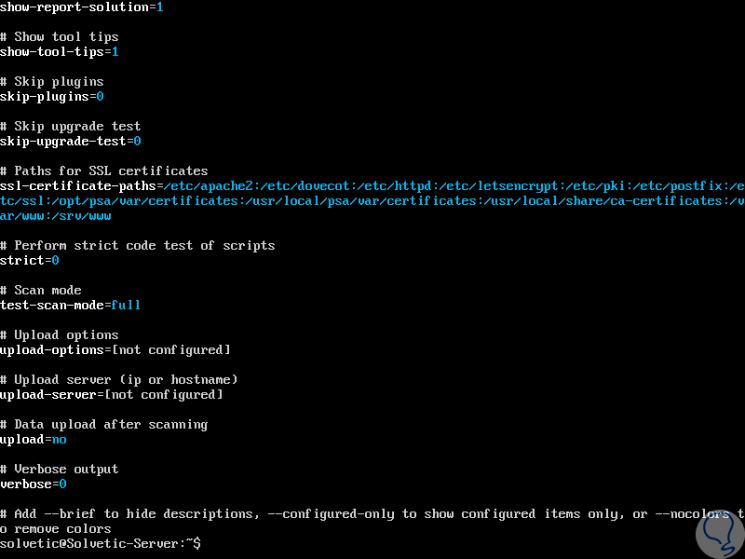
Una vez instalada la aplicación podremos ver los comandos disponibles de Lynis ejecutando la siguiente línea:

lynis show commands



Cada auditoría de seguridad en Lynis se realiza mediante perfiles que no son más que archivos de configuración con diversos parámetros para controlar la forma como se lleva a cabo la auditoría . Para ver el perfil predeterminado de Lynis usaremos la siguiente línea:

1. **lynis show settings**



Podemos comprobar, antes de realizar la auditoría , si existe alguna versión más reciente Lynis que pueda incluir mejoras para comprobar esto usaremos la siguiente línea:

1. **lynis update info**



Esto indica que contamos con la versión más actual de Lynis. También podemos comprobar este resultado ejecutando la línea:

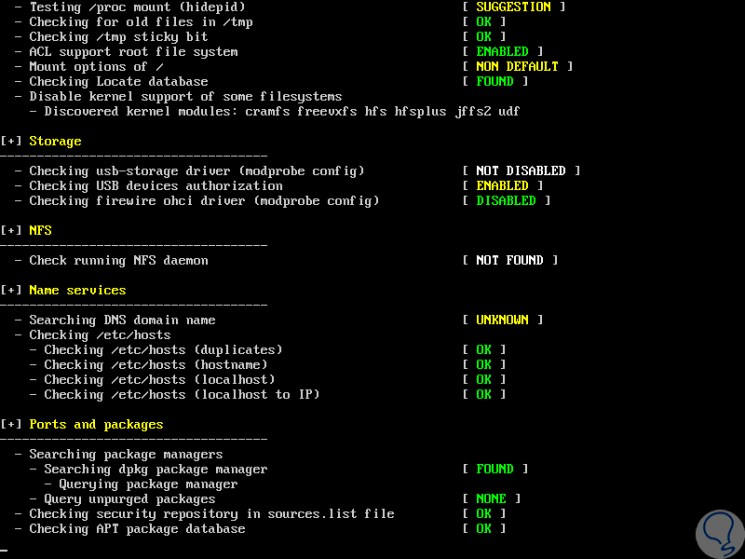
1. **lynis update check**

Paso 5

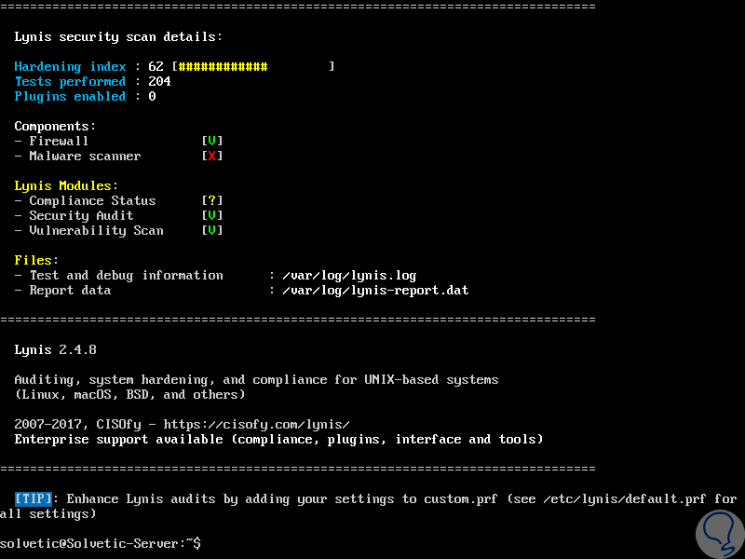
Para realizar nuestra primer auditoría del sistema procedemos a ejecutar el siguiente comando como usuarios root par que se haga plenamente y no omita algunos aspectos:

1. **lynis audit system**

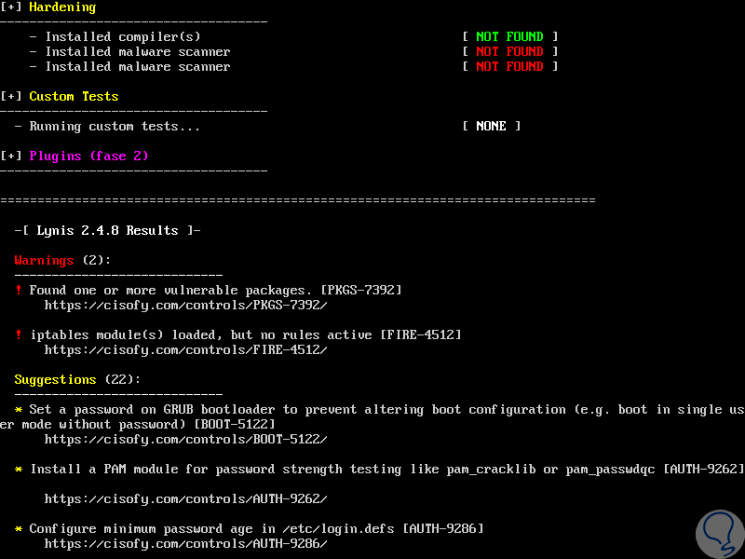
Podremos ver que inicia el proceso de auditoría en Ubuntu Server:



Este proceso tarda entre uno a dos minutos máximo. Al finalizar la auditoría veremos lo siguiente:



La información detalla de este resultado se almacena en la ruta **/var/log/lynis.log** y los datos del informe, donde tenemos toda la información asociada al servidor, será almacenada en la ruta **/var/log/lynis-report.dat**.  
Lo interesante de Lynis es que en informe anterior nos muestra advertencias y las respectivas sugerencias de seguridad a tener en cuenta para contar con un sistema estable y fiable:



**Corregir las advertencias generadas por Lynis**

Una advertencia (Warning) nos permite estar atentos ante vulnerabilidades que pueden presentarse en el sistema operativo. Por lo general la advertencia incluye la solución a la misma.

Una de las formas que tenemos en Lynis para analizar más en detalle una advertencia es usar la siguiente sintaxis:

1. **lynis show details** (Código)

Por ejemplo, si deseamos saber en detalle la advertencia del código FIRE-4512 ejecutaremos lo siguiente:

1. **lynis show details FIRE-4512**



**implementar las sugerencias de Lynis Server**

Podemos ver que dentro del respectivo análisis de auditoría tenemos diversas sugerencias (suggestions) ofrecidas por la herramienta con el fin de mejorar los niveles de seguridad del servidor.

La sugerencia está compuesta de la siguiente forma:

* Información de la sugerencia.
* ID de la sugerencia.
* Finalmente, una solución.

Al igual que con las advertencias podemos usar la línea **sudo lynis show details** para obtener mayor información:



En este caso vemos que la solución propuesta es instalar un antimalware en el servidor. De este modo cada sugerencia incluye una solución.

**Perzonalizar las auditorías de Lynis en KALI Server**

Como mencionamos al inicio Lynis se basa en perfiles para llevar a cabo las auditorías s y esta cuenta con un perfil predefinido.

Estos perfiles cuentan con la extensión .prf y se encuentran alojados en la ruta:

1. **/etc/lynis**

Para crear un nuevo perfil e indicarle a Lynis que solo audite lo que necesitamos y no todo el sistema crearemos un nuevo archivo llamada solvetic ejecutando lo siguiente:

1. **nano /etc/lynis/solvetic.prf**

En este archivo añadiremos las pruebas que deseamos omitir las cuales son:

* **FILE-6310:** Es usada para comprobar el estado de las particiones.
* **HTTP-6622:** Es usado para validar Nginx en una instalación de un servidor web.
* **HTTP-6702:** Se usa para comprobar Apache.
* **PRNT-2307 y PRNT-2308:** Se usa para comprobar servidores de impresión.
* **TOOL-5002:** Se usa para comprobar herramientas automáticas como Puppet ySalt.
* **SSH-7408:tcpkeepalive:** Es usado para realizar comprobaciones básicas de pruebas.

En dicho archivo se agregó s lo siguiente:

# Lines starting with "#" are comments

# Skip a test (one per line)

# This will ignore separation of partitions test

skip-test=FILE-6310

# Is Nginx installed?

skip-test=HTTP-6622

# Is Apache installed?

skip-test=HTTP-6702

# Skip checking print-related services

skip-test=PRNT-2307

skip-test=PRNT-2308

# If a test id includes more than one test use this form to ignore a particular test

skip-test=SSH-7408:tcpkeepalive



**Se guardan los** los cambios usando la combinación de teclas:

 Ctrl + O

 y **salimos** del editor usando:

 Ctrl + X

De esta forma la próxima vez que llevemos a cabo una auditoría estos parámetros serán omitidos.

Hemos comprendido como **Lynis** se convierte en una gran aliada para todos los administradores y personal que desea llevar un control sobre los niveles de seguridad de las diversas distros de Linux. Existe también la posibilidad de usarla en otras distribuciones.

## A través de los resultados, se especifican como mejoras para el sistema ante las posibles vunerabilidades:

### **Habilitar el Firewall del Kernel**

No solo habilitarlo, también configurarlo para denegar todas las conexiones entrantes por defecto. Al final de lo que se trata es de comunicarte con Iptables, ya sea directamente, a través de herramientas intermedias como UFW o Arno Iptables, como te indico a continuación.

* **Habilitar UFW**. Es La más senciila de instalar l, sobretodo si se estás en Kali u Ubuntu, , que automáticamente creará una serie de reglas en Iptables para denegar todas las conexiones entrantes por defecto. Solo habilitando UFW.
* **Instalar y habilitar Arno-Iptables-Firewall**. Otra opción es utilizar el script Arno Iptables Firewall, que en lo que se refiere a denegar las conexiones entrantes, vendría a hacer la misma función que UFW, aunque de seguro tendrá diferencias en el conjunto de reglas utilizadas.

### **Proteger el Grub de Kali con Contraseña**

Uno de los aspectosque tiene en cuenta Lynis, es si el gestor de arranque Grub está protegido con contraseña o no. Esto ayudará a evitar que otros usuarios puedan acceder a la línea de comandos de Grub, o que arranquen en modo de recuperación.

### **Utiliza el Cifrado**

Esto es algo que, aunque puedes realizar a posteriori, lo mejor es realizarlo en el momento de la instalación.

* **Cifrado completo de disco. LUKS**.  La mayoría de distribuciones te dan la opción de utilizar LVM, junto con el cifrado completo de tu disco duro, conocido como dm-crypt+ LUKS.
* **Cifrado del directorio Home. eCryptfs**. Otra opción alternativa es optar por cifrar el directorio Home mediante eCryptfs.

### **Antivirus o Antimalware**

Una de las comprobaciones que realiza Lynis es verificar si se dispone de un Antivirus como ClamAV. Esto es algo que se podría ser más o menos discutido, pero lo cierto es que de cara a Lynis, el hecho de contar con este u otro antivirus sobre la plataforma Unix, se tendrá más protección ante otras amenazas .

* **ClamAV**. Hay otros antivirus, pero este es el que tiene en cuenta Lynis Instala un Analizador de Rootkits

Otra cosa que tiene en cuenta Lynis a lo largo del escaneo; es si se dispone de una herramienta de escaneo de rootkits.

* **Chkrootkit y Rkhunter**. Son probablemente las dos herramientas Anti-Rootkit más conocidas y utilizadas en entornos GNU/Linux.

### **Utilizar un IDS ó IPS**

Otro de los parámetros analizados es el hecho de **disponer de un sistema de detección de intrusos** (IDS o Intrusion Detection System). Este es uno de los puntos que probablemente se debe valorar o aplicar.

Mientras que en el caso de un administrador de sistemas responsable de toda una red de ordenadores es algo frecuente, sobre todo de cara a la protección de toda la red), se necesitara del **Snort**. Es uno de los IPS más conocidos y utilizados en GNU/Linux.

### **Instalacion de Herramientas de Chequeo de Paquetes**

A continuación, un listado de los que recomienda Lynis, por sí se quieres informar sobre ellos y valorar si interesan o no:

* **Apt-listbugs**. Instalando esta utilidad podrás conocer los bugs críticos relativos a uno o varios paquetes antes de ser instalados mediante APT.
* **Apt-listchanges**. Esta herramienta te indicará los cambios más significativos antes de un upgrade mediante APT.

### **Comprobacion de la Mejora**

Una vez aplicadas todas estas mejoras, o como mínimo aquellas que se consideren aplicables de acuerdo a las necesidades, conocimientos, etc., es mejor comprobar la mejora.

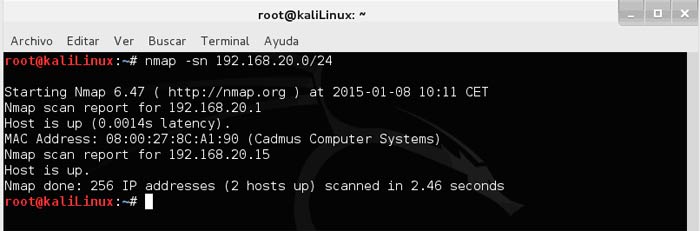
Ejecutando:

./lynis audit system

Por supuesto que hay muchas otras mejoras que puedes aplicar, pero se trata de valorar realmente cuales se pueden aplicar, de acuerdo también a la mejora real .

Por otra parte se utilizó en la línea de comando de una nueva terminal, la aplicación nmap para saber que equipos hay en una red de ordenadores. Por ejemplo si sabemos que un equipo tiene la IP 192.168.20.15 o la que sea, ponemos esa misma IP acabada en cero y ponemos /24 como se muestra en la imagen. Esto lo que hace es que busca en una red que va desde la IP 192.168.20.0 hasta la 192.168.20.254.

  Se ejecuta el comando **nmap –sn 192.168.20.0/24** o la IP acabada en cero que sea.



Con la opción **–v** añadida nos dirá los puertos de la red.

Ahora lo hacemos sobre un servidor interno o externo en este caso con la opción **–v y –sS -O** - **–p 1-65535** el cual nos da como respuesta: la IP del servidor su tipo de sistema operativo y escanea todos los puertos abiertos con los servicios asociados. Para la escogencia del cierre de puertos solo nos valdrá instalar un firewall.