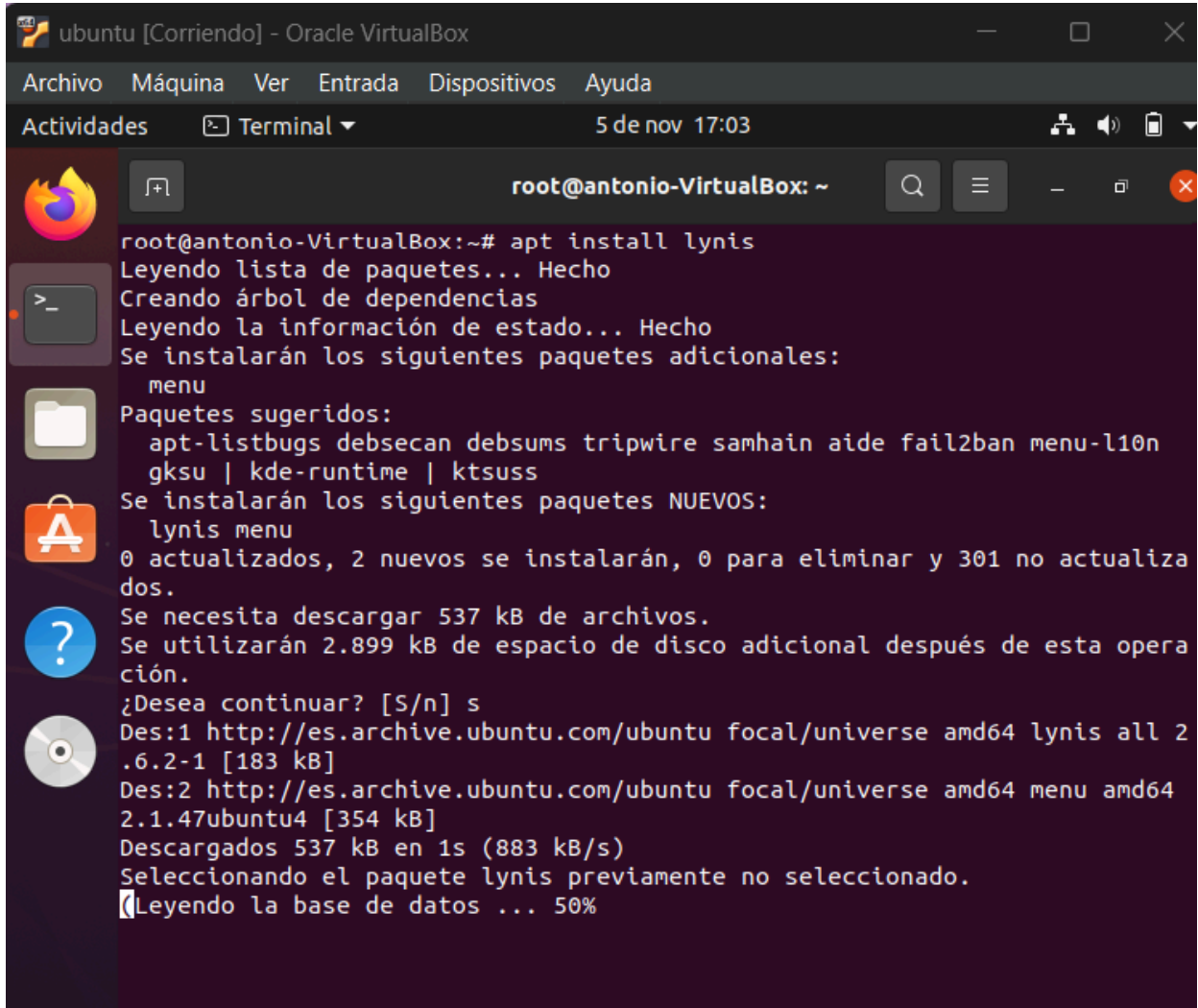


EJERCICIO 2

1.Instala Lynis:

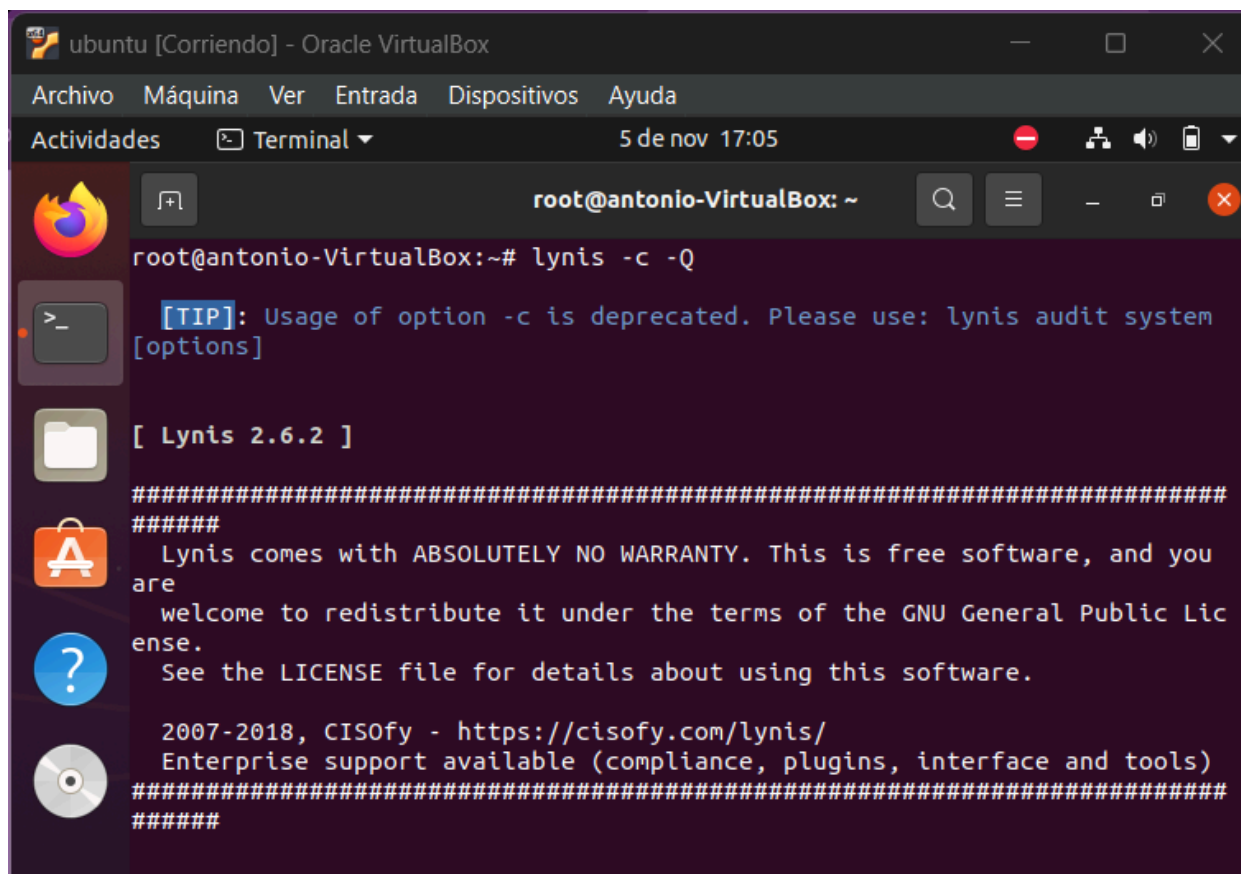
apt install lynis



```
ubuntu [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  5 de nov 17:03
root@antonio-VirtualBox: ~
root@antonio-VirtualBox:~# apt install lynis
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  menu
Paquetes sugeridos:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban menu-l10n
  gksu | kde-runtime | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
  lynis menu
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 301 no actualiza
dos.
Se necesita descargar 537 kB de archivos.
Se utilizarán 2.899 kB de espacio de disco adicional después de esta opera
ción.
¿Desea continuar? [S/n] s
Des:1 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 lynis all 2
.6.2-1 [183 kB]
Des:2 http://es.archive.ubuntu.com/ubuntu focal/universe amd64 menu amd64
2.1.47ubuntu4 [354 kB]
Descargados 537 kB en 1s (883 kB/s)
Seleccionando el paquete lynis previamente no seleccionado.
Leyendo la base de datos ... 50%
```

2.Ejecutar Lynis para un escaneo rápido

lynis -c -Q



```
ubuntu [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  5 de nov 17:05
root@antonio-VirtualBox: ~
root@antonio-VirtualBox:~# lynis -c -Q
[TIP]: Usage of option -c is deprecated. Please use: lynis audit system
[options]
[ Lynis 2.6.2 ]
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are
welcome to redistribute it under the terms of the GNU General Public Lic
ense.
See the LICENSE file for details about using this software.
2007-2018, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####
```

Este escaneo mostrará:

1. Resumen del sistema y estado de la aplicación

Estado de la instalación de Lynis.

Verificación de nuevas actualizaciones disponibles.

Información básica del sistema operativo, incluyendo la versión y el kernel.

```
root@antonio-VirtualBox: ~  
+ ] Initializing program  
-----  
- Detecting OS... [ DONE ]  
- Checking profiles... [ DONE ]  
- Detecting language and localization [ es ]  
  
-----  
Program version: 2.6.2  
Operating system: Linux  
Operating system name: Ubuntu Linux  
Operating system version: 20.04  
Kernel version: 5.15.0  
Hardware platform: x86_64  
Hostname: antonio-VirtualBox  
-----  
Profiles: /etc/lynis/default.prf  
Log file: /var/log/lynis.log  
Report file: /var/log/lynis-report.dat  
Report version: 1.0  
Plugin directory: /etc/lynis/plugins  
-----  
Auditor: [Not Specified]  
Language: es  
Test category: all  
Test group: all  
-----  
- Program update status... [ WARNING ]  
  
===== Lynis Actualización disponible =====  
  
Current version is more than 4 months old  
  
Current version : 262 Latest version : 312  
  
Please update to the latest version.  
New releases include additional features, bug fixes, tests, and baselines.  
  
Download the latest version:  
  
Packages (DEB/RPM) - https://packages.cisofy.com  
Website (TAR) - https://cisofy.com/downloads/  
GitHub (source) - https://github.com/CISOfy/lynis  
  
=====
```

2. Herramientas y plugins instalados:

Revisión de las herramientas instaladas en el sistema.

Sugerencias para actualizar o instalar herramientas faltantes.

```

[+] System Tools
-----
- Scanning available tools...
- Checking system binaries...

[+] Plugins (fase 1)
-----
Nota: los plugins contienen pruebas más extensivas y toman más tiempo

- Plugin: debian
[
[+] Debian Tests
-----
- Checking for system binaries that are required by Debian Tests...
- Checking /bin... [ FOUND ]
- Checking /sbin... [ FOUND ]
- Checking /usr/bin... [ FOUND ]
- Checking /usr/sbin... [ FOUND ]
- Checking /usr/local/bin... [ FOUND ]
- Checking /usr/local/sbin... [ FOUND ]
- Authentication:
- PAM (Pluggable Authentication Modules):
  - libpam-tmpdir [ Not Installed ]
  - libpam-usb [ Not Installed ]
- File System Checks:
- DM-Crypt, Cryptsetup & Cryptmount:
- Software:
- apt-listbugs [ Not Installed ]
- apt-listchanges [ Not Installed ]
- checkrestart [ Not Installed ]
- needrestart [ Not Installed ]
- debsecan [ Not Installed ]
- debsums [ Not Installed ]
- fail2ban [ Not Installed ]
]

```

3. Análisis del gestor de arranque:

Detecta el gestor de arranque en uso (por ejemplo, GRUB).

Servicios que se inician automáticamente al arrancar el sistema.

Revisión de otros aspectos críticos del núcleo del sistema operativo.

```
root@antonio-VirtualBox: ~  
[+] Boot and services  
-----  
- Service Manager [ SysV Init ]  
- Checking UEFI boot [ DESACTIVADO ]  
- Checking presence GRUB2 [ ENCONTRADO ]  
  - Checking for password protection [ PELIGRO ]  
- Check running services (systemctl) [ HECHO ]  
  Result: found 30 running services  
- Check enabled services at boot (systemctl) [ HECHO ]  
  Result: found 66 enabled services  
- Check startup files (permissions) [ OK ]  
- Checking sulogin in rescue.service [ NO ENCONTRADO ]  
  
[+] Kernel  
-----  
- Checking default run level [ RUNLEVEL 5 ]  
- Checking CPU support (NX/PAE)  
  CPU support: PAE and/or NoeXecute supported [ ENCONTRADO ]  
- Checking kernel version and release [ HECHO ]  
- Checking kernel type [ HECHO ]  
- Checking loaded kernel modules [ HECHO ]  
  Found 69 active modules  
- Checking Linux kernel configuration file [ ENCONTRADO ]  
- Checking default I/O kernel scheduler [ NO ENCONTRADO ]  
- Checking for available kernel update [ DESCONOCIDO ]  
- Checking core dumps configuration [ DESACTIVADO ]  
  - Checking setuid core dumps configuration [ PROTECTED ]  
- Check if reboot is needed [ NO ]
```

4. Memoria y procesos:

- Información sobre el uso de la memoria.
- Listado de procesos en ejecución.
- Identificación de posibles procesos zombies.

```
root@antonio-VirtualBox: ~  
[+] Memoria y Procesos  
-----  
- Checking /proc/meminfo [ ENCONTRADO ]  
- Searching for dead/zombie processes [ OK ]  
- Searching for IO waiting processes [ OK ]
```

5. Usuarios, grupos y autenticación:

- Información sobre los usuarios y grupos configurados en el sistema.
- Detalles sobre los sistemas de autenticación en uso.

[+] Users, Groups and Authentication

- Administrator accounts	[OK]
- Unique UIDs	[OK]
- Consistency of group files (grpck)	[OK]
- Unique group IDs	[OK]
- Unique group names	[OK]
- Password file consistency	[OK]
- Query system users (non daemons)	[HECHO]
- NIS+ authentication support	[NOT ENABLED]
- NIS authentication support	[NOT ENABLED]
- sudoers file	[ENCONTRADO]
- Check sudoers file permissions	[OK]
- PAM password strength tools	[SUGERENCIA]
- PAM configuration files (pam.conf)	[ENCONTRADO]
- PAM configuration files (pam.d)	[ENCONTRADO]
- PAM modules	[ENCONTRADO]
- LDAP module in PAM	[NO ENCONTRADO]
- Accounts without expire date	[OK]
- Accounts without password	[OK]
- Checking user password aging (minimum)	[DESACTIVADO]
- User password aging (maximum)	[DESACTIVADO]
- Checking expired passwords	[OK]
- Checking Linux single user mode authentication	[PELIGRO]
- Determining default umask	
- umask (/etc/profile)	[NO ENCONTRADO]
- umask (/etc/login.defs)	[SUGERENCIA]
- LDAP authentication support	[NOT ENABLED]
- Logging failed login attempts	[ENABLED]

Auditoría completa con Lynis

lynis audit system

1. Escudos del sistema:

Análisis de las configuraciones de seguridad.

Comprobación de políticas de seguridad aplicadas.

[+] Software: firewalls

- Checking iptables kernel module	[ENCONTRADO]
- Checking iptables policies of chains	[ENCONTRADO]
- Checking for empty ruleset	[PELIGRO]
- Checking for unused rules	[OK]
- Checking host based firewall	[ACTIVE]

2. Sistemas de ficheros y almacenamiento:

Información sobre los sistemas de archivos.

Estado de los dispositivos de almacenamiento masivo.

```
[+] File systems
-----
- Checking mount points
  - Checking /home mount point [ SUGERENCIA ]
  - Checking /tmp mount point [ SUGERENCIA ]
  - Checking /var mount point [ SUGERENCIA ]
- Query swap partitions (fstab) [ OK ]
- Testing swap partitions [ OK ]
- Testing /proc mount (hidepid) [ SUGERENCIA ]
- Checking for old files in /tmp [ OK ]
- Checking /tmp sticky bit [ OK ]
- Checking /var/tmp sticky bit [ OK ]
- ACL support root file system [ ENABLED ]
- Mount options of / [ NON DEFAULT ]
- Disable kernel support of some filesystems
  - Discovered kernel modules: cramfs freevxfs hfs hfsplus jffs2 udf
```

3. Servicios y gestor de paquetes:

Información sobre los servicios de nombre de dominio y el gestor de paquetes de la distribución.

Análisis de dispositivos de red y otros servicios como impresoras compartidas, servidores de correo y estado del cortafuegos.

```
[+] Name services
-----
- Checking /etc/resolv.conf options [ ENCONTRADO ]
- Searching DNS domain name [ DESCONOCIDO ]
- Checking /etc/hosts
  - Checking /etc/hosts (duplicates) [ OK ]
  - Checking /etc/hosts (hostname) [ OK ]
  - Checking /etc/hosts (localhost) [ OK ]
  - Checking /etc/hosts (localhost to IP) [ OK ]

[+] Ports and packages
-----
- Searching package managers
  - Searching dpkg package manager [ ENCONTRADO ]
  - Querying package manager [ NONE ]
  - Query unpurged packages [ OK ]
- Checking security repository in sources.list file [ OK ]
- Checking APT package database [ OK ]
- Checking vulnerable packages [ PELIGRO ]
- Checking upgradeable packages [ OMITIDO ]
- Checking package audit tool [ INSTALLED ]
Found: apt-get
```

4. Servidores y aplicaciones:

Información sobre servidores web instalados, servidores SSH, SNMP, bases de datos del sistema y otros servicios como controladores de dominio LDAP, programas PHP, servidores proxy y squid.

```
[+] Software: firewalls
-----
- Checking iptables kernel module           [ ENCONTRADO ]
- Checking iptables policies of chains      [ ENCONTRADO ]
- Checking for empty ruleset                 [ PELIGRO ]
- Checking for unused rules                  [ OK ]
- Checking host based firewall               [ ACTIVE ]

[+] Software: webserver
-----
- Checking Apache                           [ NO ENCONTRADO ]
- Checking nginx                             [ NO ENCONTRADO ]

[+] SSH Support
-----
- Checking running SSH daemon               [ NO ENCONTRADO ]

[+] SNMP Support
-----
- Checking running SNMP daemon              [ NO ENCONTRADO ]

[+] Databases
-----
No database engines found

[+] LDAP Services
-----
- Checking OpenLDAP instance                [ NO ENCONTRADO ]

[+] PHP
-----
- Checking PHP                              [ NO ENCONTRADO ]

[+] Squid Support
-----
- Checking running Squid daemon             [ NO ENCONTRADO ]
```