

ELOY CELDRAN MADRID
SAD TAREA 2
AUDITORÍA DEL SISTEMA

Contenido

Lynis (Linux)	2
Descripción de la herramienta.....	2
Proceso de Instalación	2
Ejecución de los análisis	3
Propuestas de solución	3
Clara (Windows).....	4
Descripción de la herramienta.....	4
Proceso de Instalación	4
Ejecución del análisis.....	5
Nessus (Windows).....	7
Descripcion de la herramienta.....	7
Proceso de Instalación	7
Ejecución de los análisis	9
Nessus (Linux)	10
Proceso de Instalación	10
Ejecución de los análisis	12

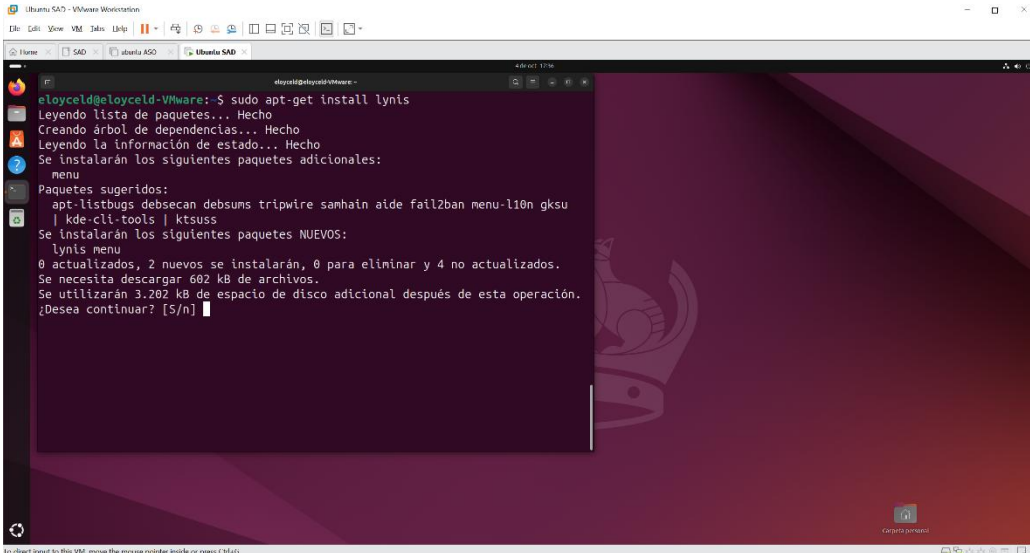
Lynis (Linux)

Descripción de la herramienta

Se trata de una herramienta de auditoría escrita en bash, utilizada principalmente en Linux, para realizar un análisis en profundidad del sistema operativo en busca de errores de configuración, paquetes obsoletos, servicios en ejecución innecesarios y otros puntos débiles relacionados con la seguridad.

Proceso de Instalación

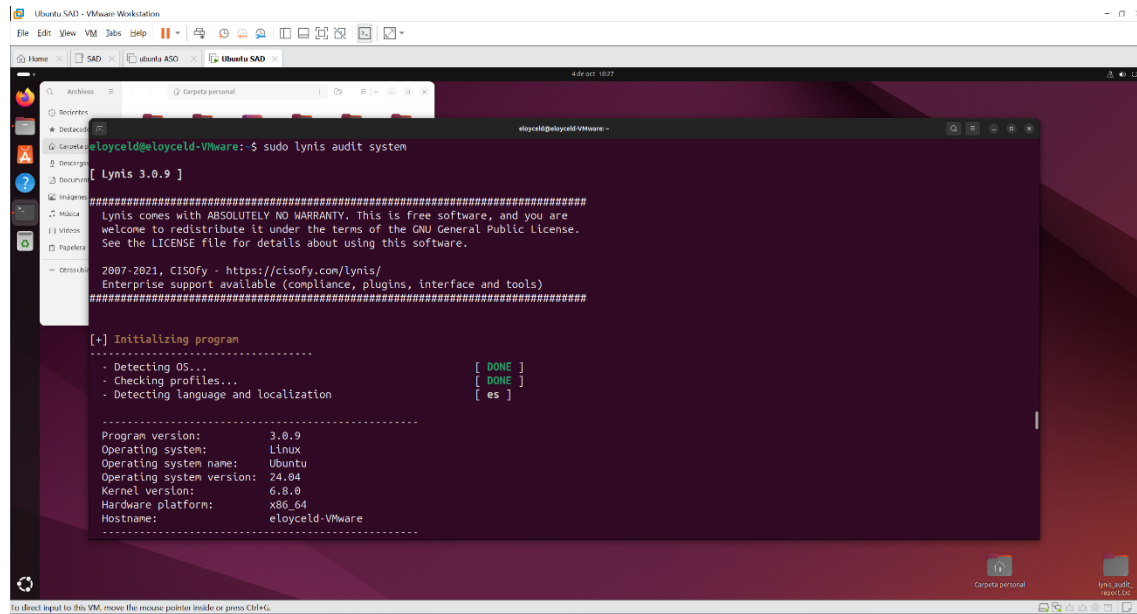
El proceso de instalación de Lynis es bastante sencillo, lo único que tienes que hacer es descargar el paquete con el comando “sudo apt-get install lynis” y una vez hecho ya tendrás instalado Lynis.



```
eloycel@eloycel-VirtualBox:~$ sudo apt-get install lynis
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
menu
Paquetes sugeridos:
apt-listbugs debsecan debsums tripwire sanhain aide fail2ban menu-l10n gksu
| kde-cli-tools | ktsuss
Se instalarán los siguientes paquetes NUEVOS:
lynis menu
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 602 kB de archivos.
Se utilizarán 3.202 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Ejecución de los análisis

Para realizar un análisis en lynis deberemos escribir en el terminal “sudo lynis audit system” y empezará a realizar un análisis de nuestro equipo



```
elyceld@elyceld-Vmware:~$ sudo lynis audit system
[ Lynis 3.0.9 ]

=====
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 License.
See the LICENSE file for details about using this software.
=====

2007-2021, CISOFy - https://cisoify.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
=====

[+] Initializing program
-----
- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
- Detecting language and localization [ es ]
-----

Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: elyceld-Vmware
```

El archivo total que muestra al realizar el análisis esta adjunto en la entrega de esta tarea ya que es bastante grande como para añadirlo a esta documentación.

Propuestas de solución

Problemas en seguridad de permisos y contraseñas

- El directorio “/etc/sudoers.d” se marcó como “DANGER” marca que tiene permisos inseguros, es un directorio que contiene archivos de configuración que otorgan privilegios elevados, debería realizar un “chmod 440 /etc/sudoers.d” para así restringir el acceso.
- El valor por defecto de umask no está establecido explícitamente en /etc/profile o /etc/login.defs. Debería establecer una umask más restrictiva como “027” así limitaría los accesos no deseados.

Dispositivos

- Los puertos USB no deberían estar activos a no ser que sea estrictamente necesario, debería implantar medidas mas estrictas o bien deshabilitarlos completamente

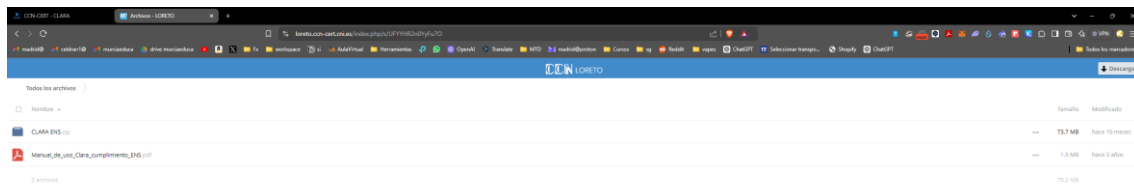
Clara (Windows)

Descripción de la herramienta

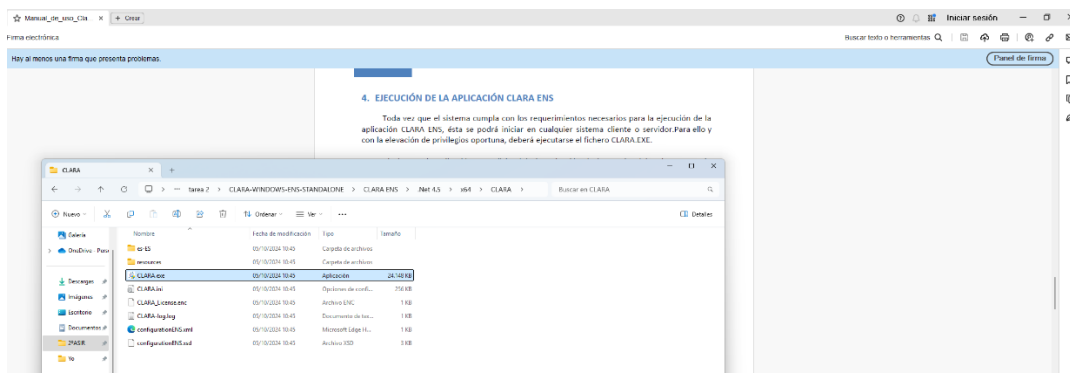
Clara es una herramienta de análisis de seguridad dirigida a aplicaciones desarrolladas sobre .NET Framework y .NET Core. Señala la ubicación de las vulnerabilidades en el código fuente y el lugar donde están habilitadas en la configuración de la aplicación.

Proceso de Instalación

Ingresamos a la URL: <https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html> para desde ahí realizar su instalación

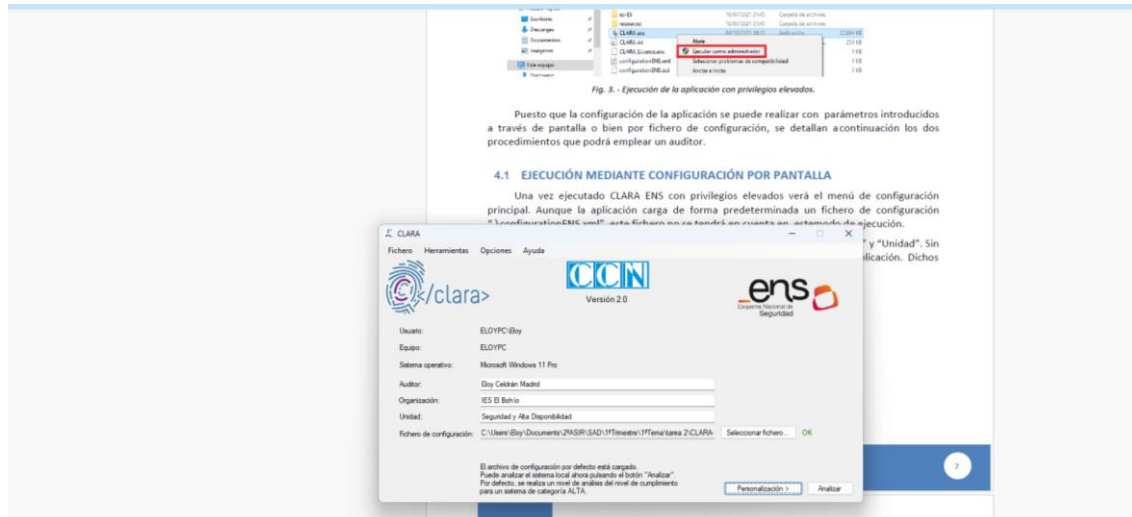


Una vez descargado el zip ingresaremos a “.Net 4.5” después a “x64” y “CLARA” y lanzaremos el instalador

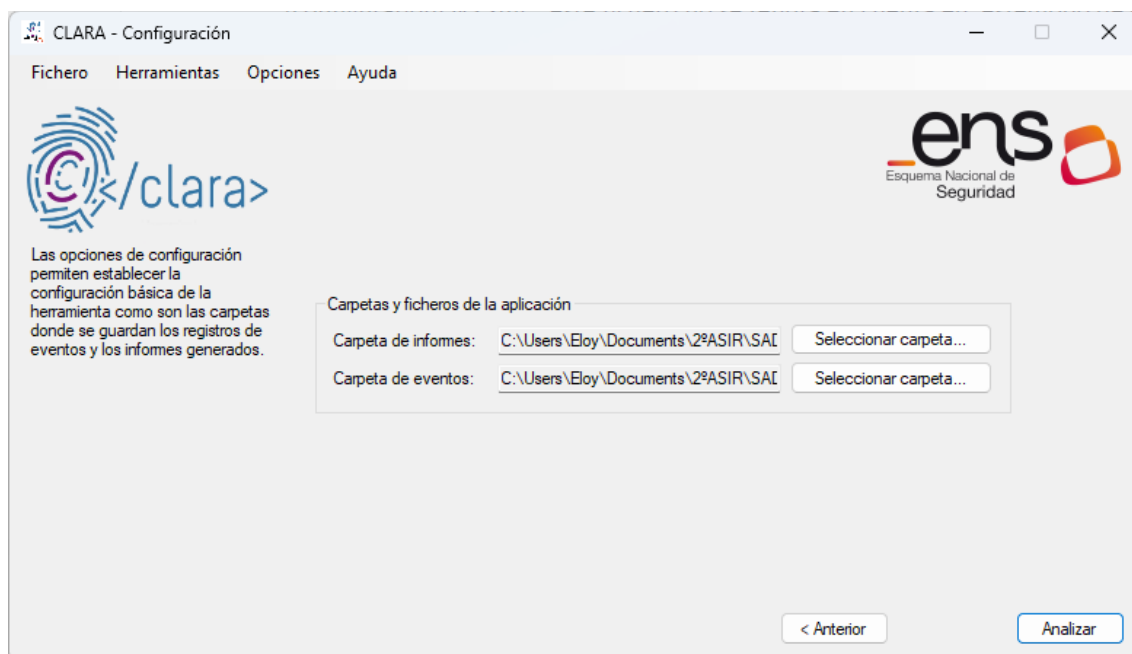


Ejecución del análisis

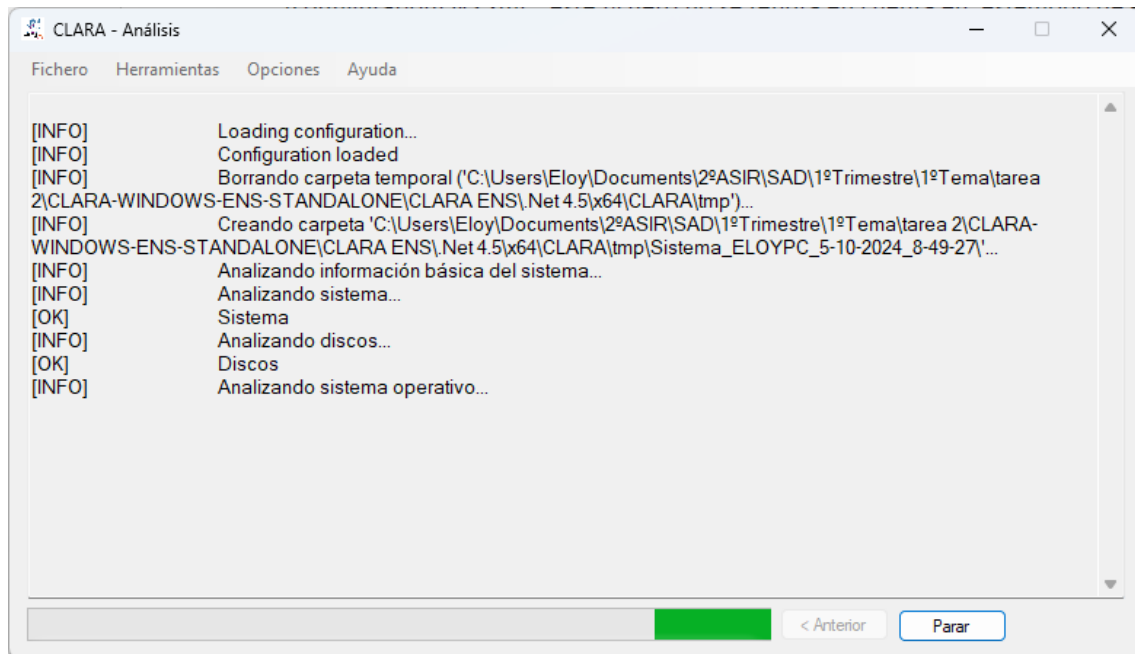
Una vez iniciado nos pedirá datos como quien va a ser el autor de análisis, que organización y la unidad, todos estos serán para posteriormente mostrarlos en el informe



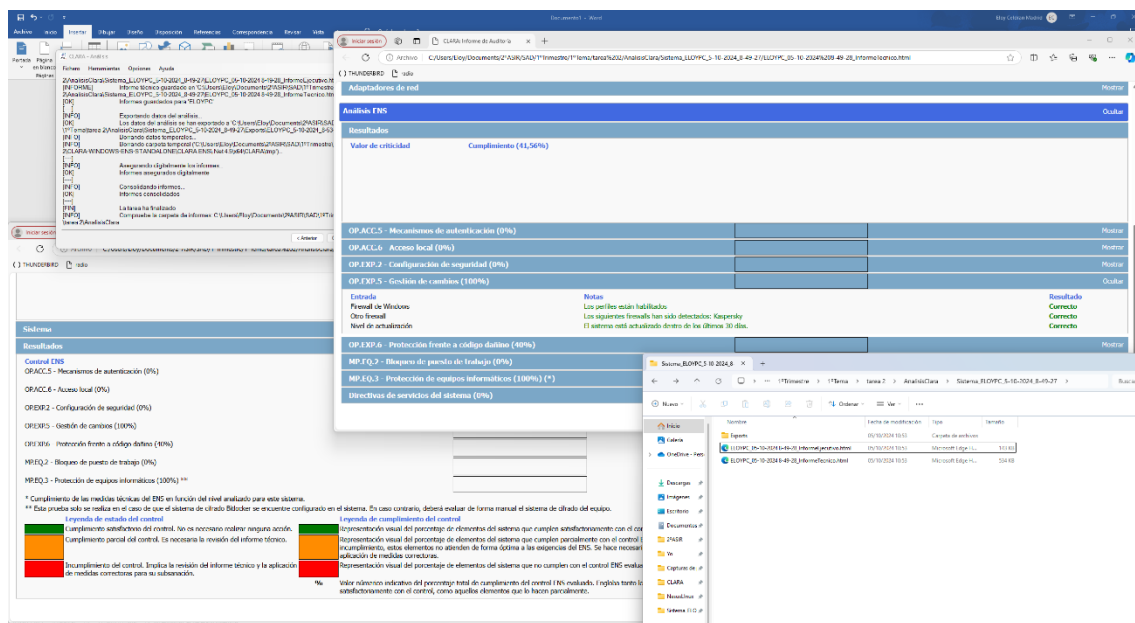
Le decimos en que ruta queremos que guarde los informes como los eventos del analisis.



Le damos a analizar y comenzará el análisis.



Cuando finalice encontraremos en la carpeta que le indicamos anteriormente tres nuevos archivos, dos de ellos html, uno de ellos es el informe técnico y el otro el informe ejecutivo, además de una carpeta que son los eventos.



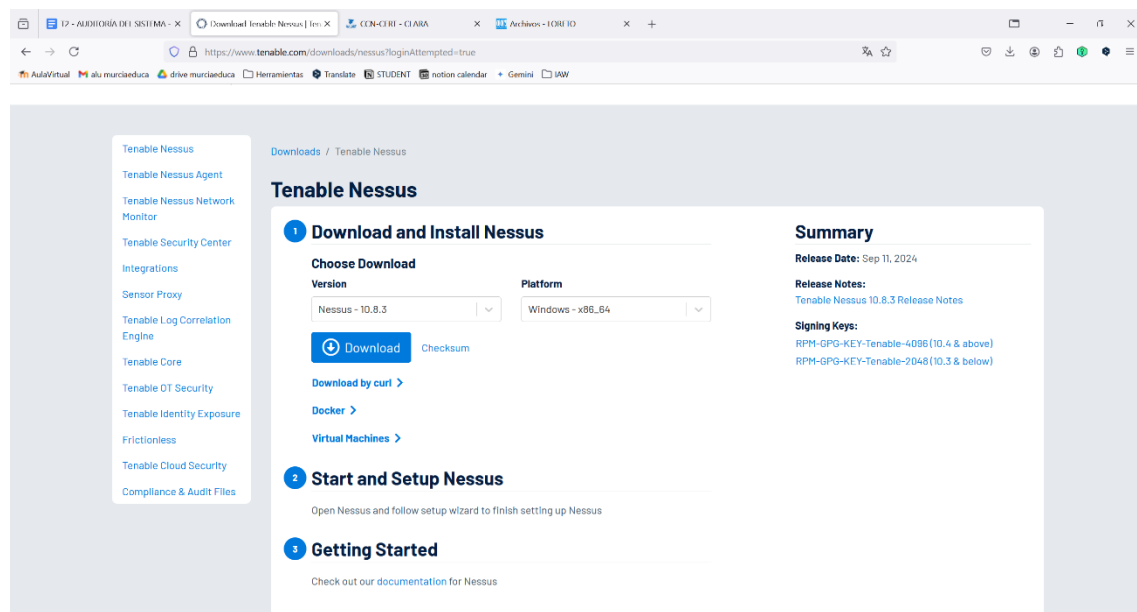
Nessus (Windows)

Descripción de la herramienta

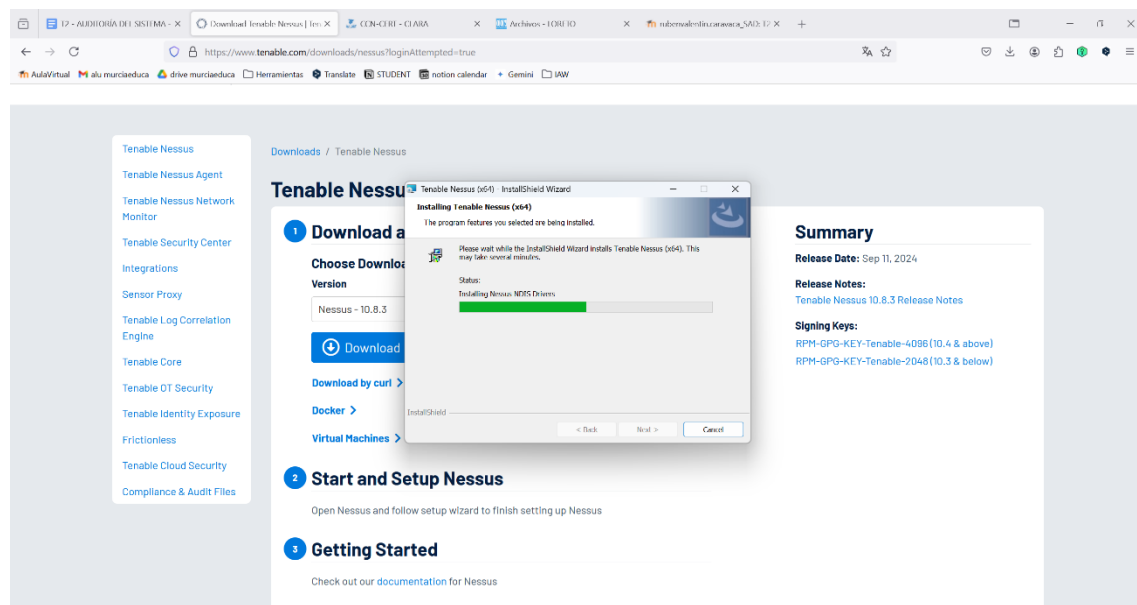
Entre las herramientas más conocidas y utilizadas actualmente en el mercado para el escaneo de vulnerabilidades, Nessus es capaz de descubrir una gran variedad de vulnerabilidades en sistemas operativos, dispositivos de red y aplicaciones dentro de entornos Windows y Linux.

Proceso de Instalación

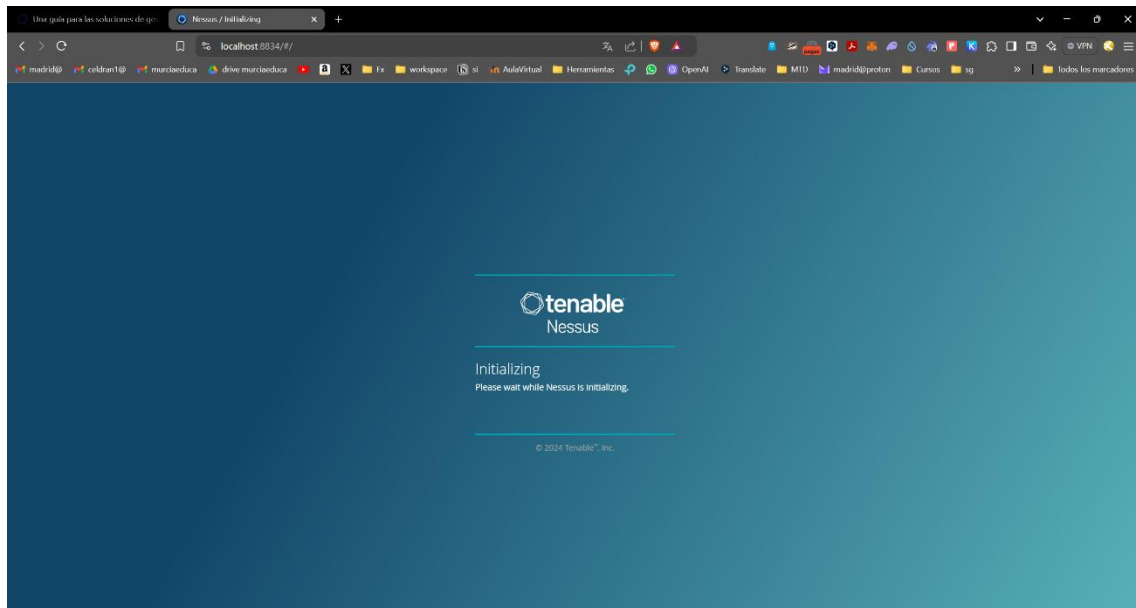
Accedemos a su página de descargas (previamente debemos tener cuenta) y de descargamos la versión más reciente.



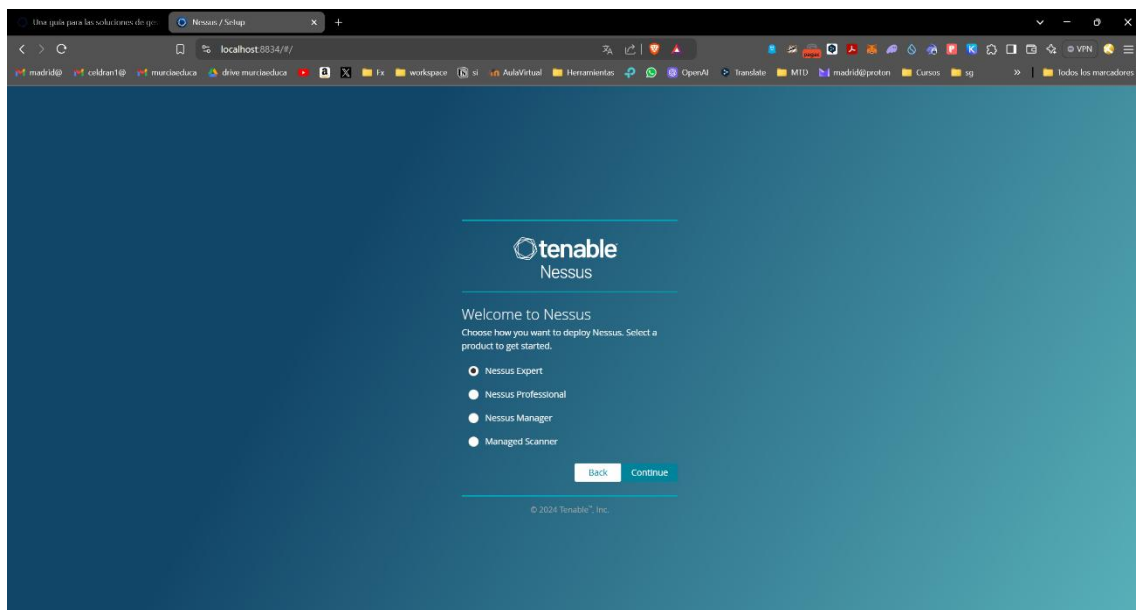
Accedemos e instalamos



Una vez instalado ponemos “localhost:8834” para acceder, y veremos un mensaje de que esta inicializando.

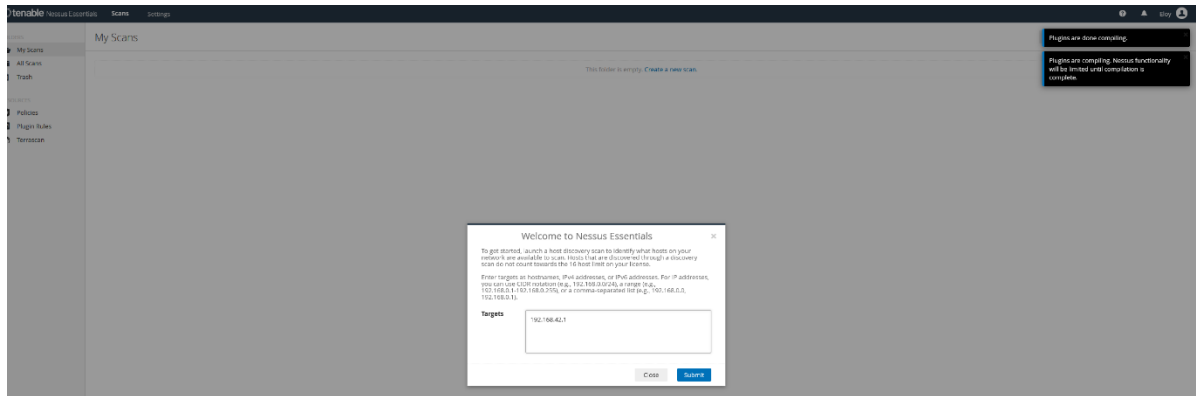


Deberemos seleccionar la versión de Nessus que vamos a trabajar, en nuestro caso será la de “Nessus Manager”

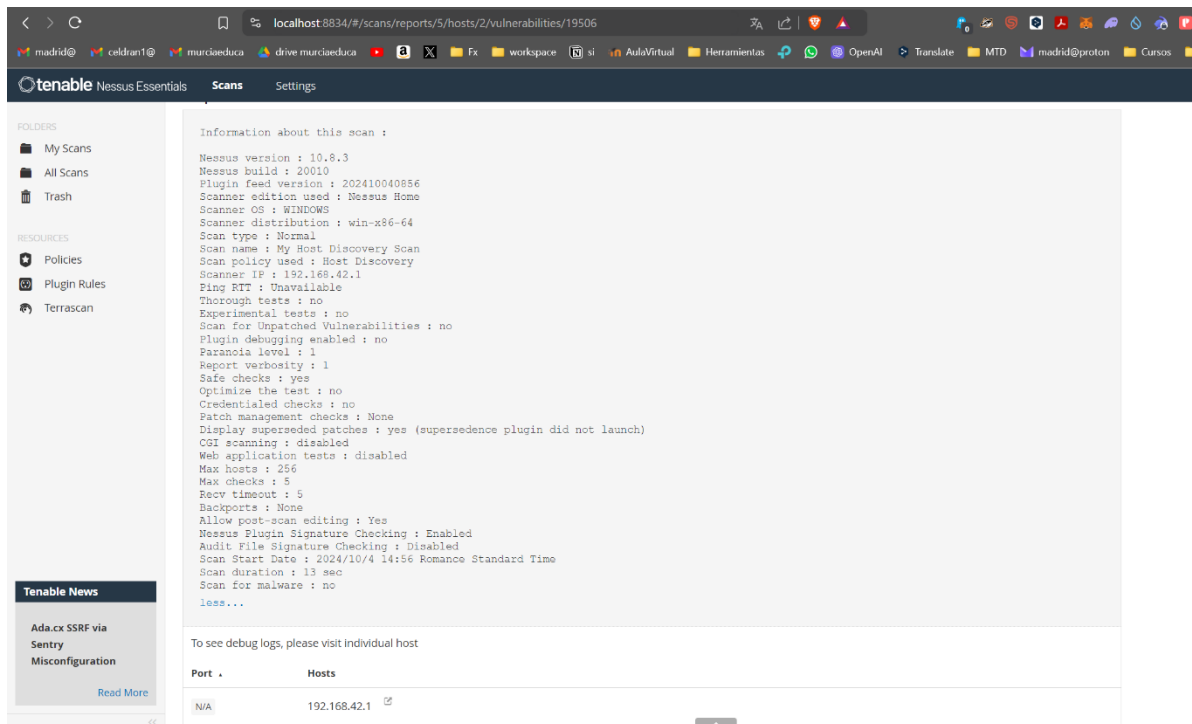


Ejecución de los análisis

Una vez que iniciamos y tenemos los plugins instalados, le daremos a la opción de “New Scan” y deberemos escribir la IP que queremos escanear, una vez escrita le daremos a “Submit”



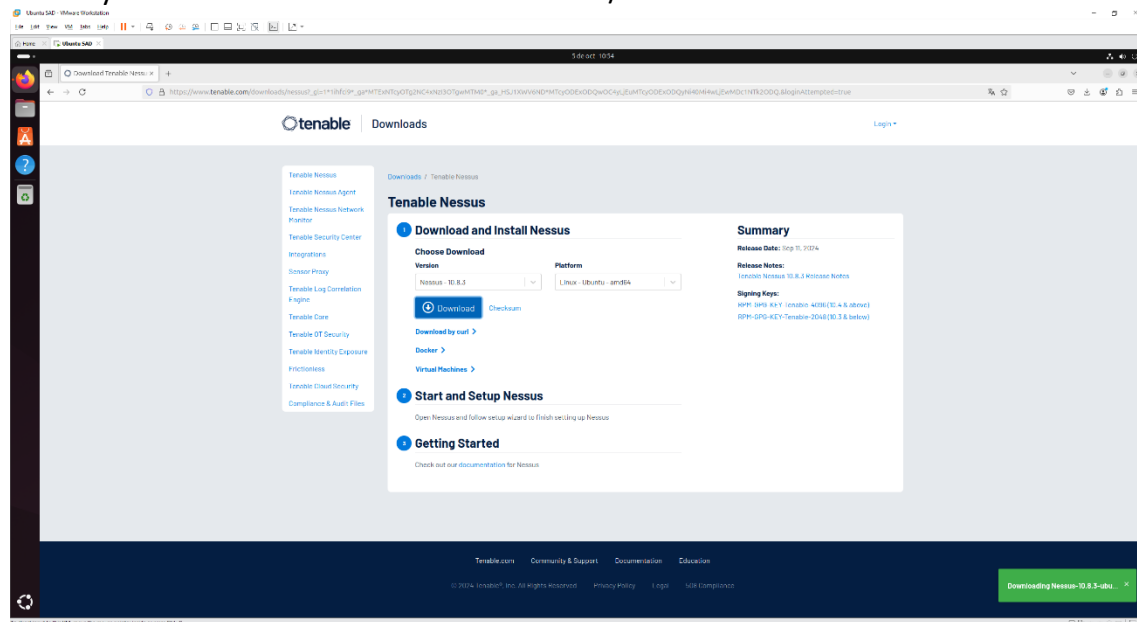
Pasado un rato en el apartado de “My Scans” encontraremos el análisis que acaba de realizar con el informe correspondiente.



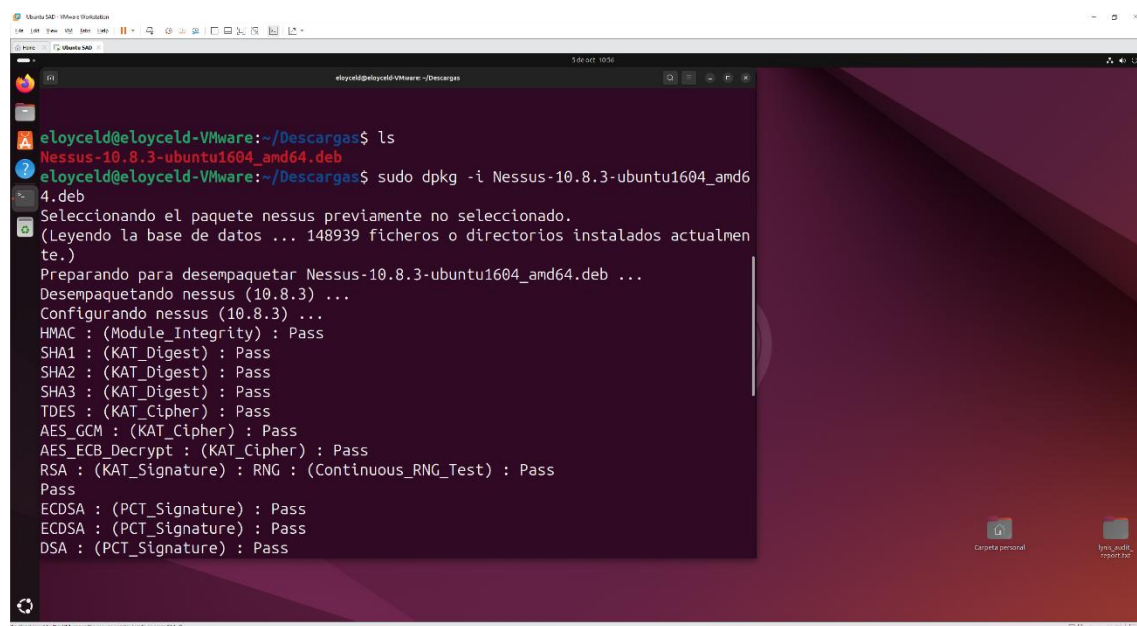
Nessus (Linux)

Proceso de Instalación

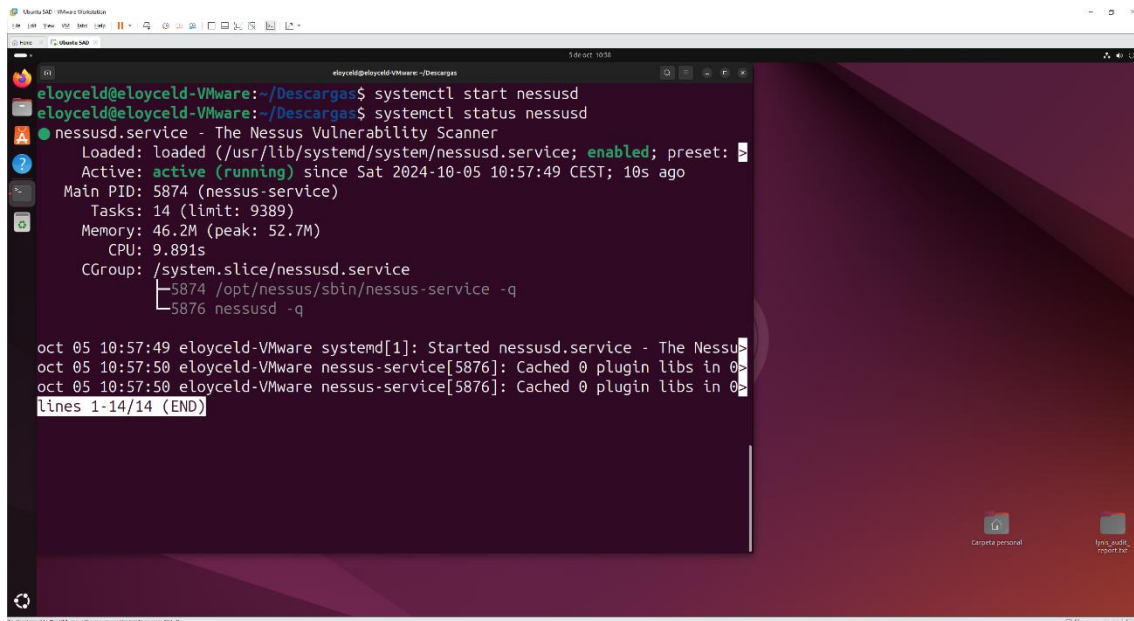
El proceso de instalación es relativamente parecido a instalarlo en Windows. Iniciamos sesión y seleccionamos el instalador de “Linux/Ubuntu – amd64”



Escribimos el comando “sudo dpkg -i <nombre_archivo>” para así descomprimirlo



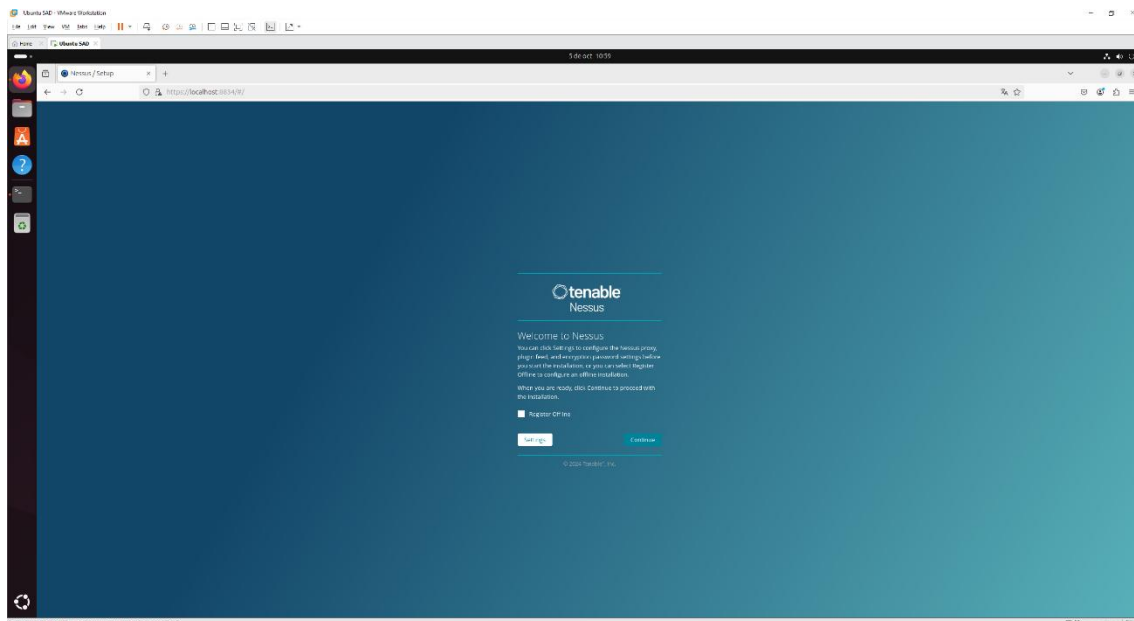
Con el comando “systemctl start nessusd” lo iniciaremos, además con el comando “systemctl status nessusd” podremos comprobar el estado del mismo.



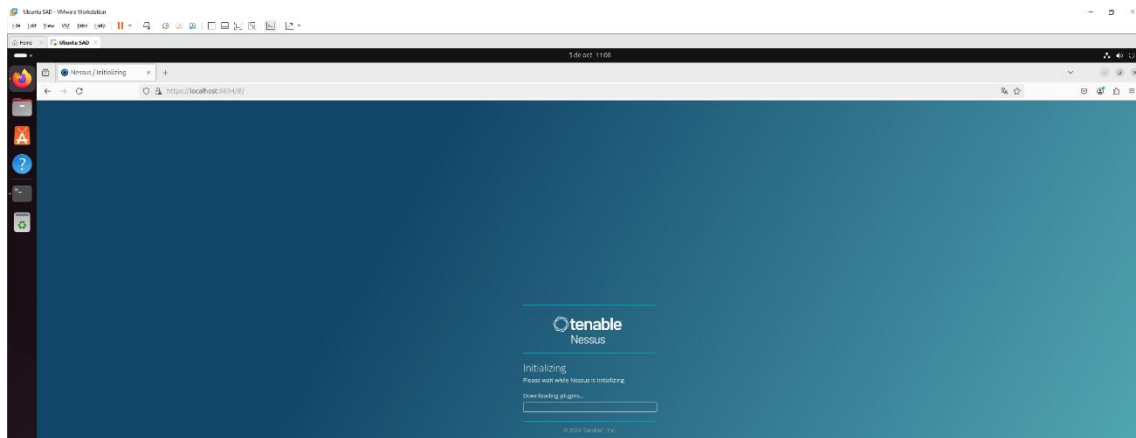
```
eloyceld@eloyceld-VMware: ~/Descargas$ systemctl start nessusd
eloyceld@eloyceld-VMware: ~/Descargas$ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset:
   Active: active (running) since Sat 2024-10-05 10:57:49 CEST; 10s ago
     Main PID: 5874 (nessus-service)
        Tasks: 14 (limit: 9389)
       Memory: 46.2M (peak: 52.7M)
          CPU: 9.891s
      CGroup: /system.slice/nessusd.service
              └─5874 /opt/nessus/sbin/nessus-service -q
                └─5876 nessusd -q

oct 05 10:57:49 eloyceld-VMware systemd[1]: Started nessusd.service - The Nessu
oct 05 10:57:50 eloyceld-VMware nessus-service[5876]: Cached 0 plugin libs in 0
oct 05 10:57:50 eloyceld-VMware nessus-service[5876]: Cached 0 plugin libs in 0
lines 1-14/14 (END)
```

Una vez iniciado comprobaremos en localhost si se nos ha instalado correctamente y haremos lo mismo que en Windows.

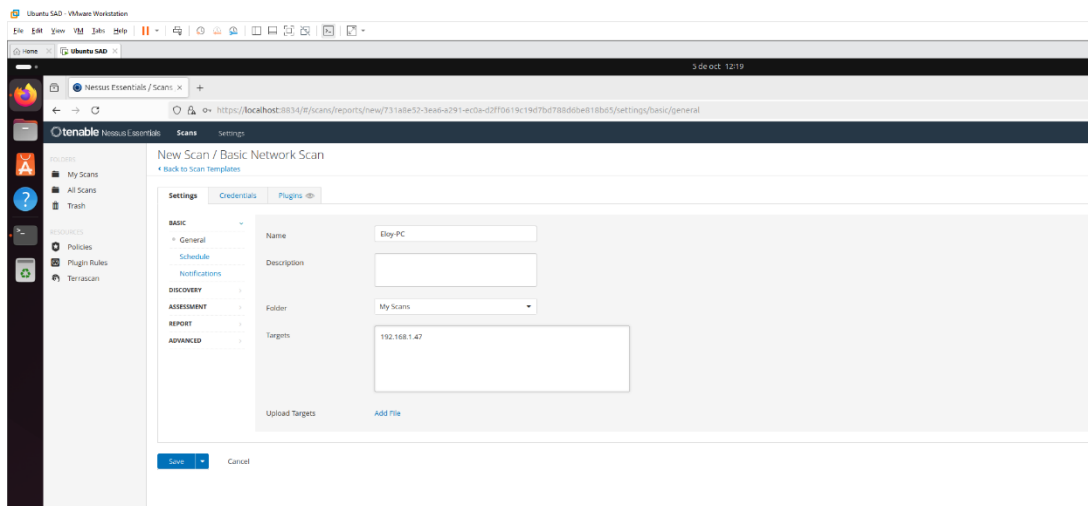


Una vez que entremos empezará a inicializar



Ejecución de los análisis

Le daremos a “New Scan” y seleccionaremos el análisis de “Basic Network Scan” este análisis es algo diferente que el que hemos realizado pero ya que lo vamos a hacer dos veces probaremos algo diferente, añadimos el nombre del análisis, además deberemos añadir en “Targets” la IP que queremos analizar.



Una vez realizado nos mostrará las vulnerabilidades que ha encontrado en el análisis.

The screenshot displays the OpenVAS (Greenbone) web interface. The main content area shows a vulnerability scan report for a host named "Bloy-PC / 192.168.1.47". The report lists 44 vulnerabilities, with the first few being "104 (Multiple Issues)", "SSH (Multiple Issues)", "HTTP (Multiple Issues)", and "153 (Multiple Issues)". The interface includes a sidebar with navigation options like "My Scans", "All Scans", "Tools", "Policies", "Plugins/Plugins", and "Templates". The top right corner shows the user's name "Hernan Perez" and the date "14 de oct 1925".

Severity	CVE	Vulnerability	Family	Count	Host Details
Low	104	104 (Multiple Issues)	General	4	IP: 192.168.1.47 MAC: 08:00:27:AA:BB:7A OS: Linux Kernel 3.8-40 generic on Ubuntu 12.04
Low	SSH	SSH (Multiple Issues)	General	6	Start: Today at 12:19 PM End: Today at 12:19 PM Elapsed: 2 minutes KB: Download
Low	HTTP	HTTP (Multiple Issues)	Web Services	2	
Low	153	153 (Multiple Issues)	Service Detection	2	
Low	Port	Port Scanner (SSH)	Port Scanner	4	
Low	Service	Service Detection	Service Detection	2	
Low	Common	Common Platform Enumeration (CPE)	General	1	
Low	Device	Device Hostname	General	1	
Low	Device	Device Type	General	1	
Low	Enumerate	Enumerate the PATH Variables	General	1	
Low	Enumerate	Enumerate Card Manufacturer Detection	MITC	1	
Low	Enumerate	Enumerate MAC addresses	General	1	
Low	Enumerate	Enumerate contain Dangerous characters (Linux)	MITC	1	
Low	Enumerate	Enumerate shell installed (Linux / UNIX)	MITC	1	
Low	Enumerate	Enumerate Fully Qualified Domain Name (FQDN) resolution	General	1	
Low	Enumerate	Enumerate Hostname and IP Address	Settings	1	
Low	Enumerate	IP Assignment Method Detection	General	1	
Low	Enumerate	Enumerate Installed (Linux / UNIX)	MITC	1	
Low	Enumerate	Enumerate Installed (Linux / UNIX)	MITC	1	
Low	Enumerate	Enumerate Mounted Devices	General	1	

•[1;37m[Lynis 3.0.9]•[0m

#####

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 License. See the LICENSE file for details about using this software.

2007-2021, CISOfy - <https://cisofy.com/lynis/>

Enterprise support available (compliance, plugins, interface and tools)

#####

[+] •[1;33mInitializing program•[0m

•[2C- Detecting OS... •[41C [•[1;32mDONE•[0m]

•[2C- Checking profiles...•[37C [•[1;32mDONE•[0m]

•[2C- Detecting language and localization•[22C [•[1;37mes•[0m]

Program version: 3.0.9
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: eloyceld-VMware

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

•[2C- Program update status... •[32C [•[1;32mSIN ACTUALIZACIÓN•[0m]

[+] •[1;33mHerramientas del sistema•[0m

•[2C- Scanning available tools...•[30C

•[2C- Checking system binaries...•[30C

[+] •[1;35mPlugins (fase 1)•[0m

•[0CNota: los plugins contienen pruebas más extensivas y toman más tiempo•[0C

•[0C •[0C

•[2C- •[0;36mPlugin•[0m: •[1;37mdebian•[0m•[21C

[

[+] •[1;33mDebian Tests•[0m

```
•[2C- Checking for system binaries that are required by Debian Tests...•[0C
•[4C- Checking /bin... •[38C [ •[1;32mFOUND•[0m ]
•[4C- Checking /sbin... •[37C [ •[1;32mFOUND•[0m ]
•[4C- Checking /usr/bin... •[34C [ •[1;32mFOUND•[0m ]
•[4C- Checking /usr/sbin... •[33C [ •[1;32mFOUND•[0m ]
•[4C- Checking /usr/local/bin... •[28C [ •[1;32mFOUND•[0m ]
•[4C- Checking /usr/local/sbin... •[27C [ •[1;32mFOUND•[0m ]
•[2C- Authentication:•[42C
•[4C- PAM (Pluggable Authentication Modules):•[16C
```

```
•[30;43m[WARNING]•[0m: Test DEB-0001 had a long execution: 11.444613
seconds•[0m
```

```
•[6C- libpam-tmpdir•[40C [ •[1;31mNot Installed•[0m ]
•[2C- File System Checks:•[38C
•[4C- DM-Crypt, Cryptsetup & Cryptmount:•[21C
•[2C- Software:•[48C
•[4C- apt-listbugs•[43C [ •[1;31mNot Installed•[0m ]
•[4C- apt-listchanges•[40C [ •[1;31mNot Installed•[0m ]
•[4C- needrestart•[44C [ •[1;31mNot Installed•[0m ]
•[4C- fail2ban•[47C [ •[1;31mNot Installed•[0m ]
]
```

```
[+] •[1;33mArranque y servicios•[0m
```

```
-----
•[2C- Service Manager•[42C [ •[1;32msystemd•[0m ]
•[2C- Checking UEFI boot•[39C [ •[1;37mDESHABILITADO•[0m ]
•[2C- Checking presence GRUB2•[34C [ •[1;32mENCONTRADO•[0m ]
•[4C- Checking for password protection•[23C [ •[1;31mNINGUNO•[0m ]
•[2C- Check running services (systemctl)•[23C [ •[1;32mHECHO•[0m ]
•[8CResult: found 33 running services•[20C
•[2C- Check enabled services at boot (systemctl)•[15C [ •[1;32mHECHO•[0m ]
•[8CResult: found 57 enabled services•[20C
•[2C- Check startup files (permissions)•[24C [ •[1;32mOK•[0m ]
•[2C- Running 'systemd-analyze security'•[23C
•[8C- ModemManager.service:•[30C [ •[1;37mMEDIO•[0m ]
•[8C- NetworkManager.service:•[28C [ •[1;33mEXPUESTO•[0m ]
•[8C- accounts-daemon.service:•[27C [ •[1;37mMEDIO•[0m ]
•[8C- alsa-state.service:•[32C [ •[1;31mINSEGURO•[0m ]
•[8C- anacron.service:•[35C [ •[1;31mINSEGURO•[0m ]
•[8C- avahi-daemon.service:•[30C [ •[1;31mINSEGURO•[0m ]
•[8C- bluetooth.service:•[33C [ •[1;37mMEDIO•[0m ]
•[8C- colord.service:•[36C [ •[1;32mPROTEGIDO•[0m ]
•[8C- cron.service:•[38C [ •[1;31mINSEGURO•[0m ]
•[8C- cups-browsed.service:•[30C [ •[1;31mINSEGURO•[0m ]
•[8C- cups.service:•[38C [ •[1;31mINSEGURO•[0m ]
•[8C- dbus.service:•[38C [ •[1;31mINSEGURO•[0m ]
•[8C- dmesg.service:•[37C [ •[1;31mINSEGURO•[0m ]
•[8C- emergency.service:•[33C [ •[1;31mINSEGURO•[0m ]
•[8C- gdm.service:•[39C [ •[1;31mINSEGURO•[0m ]
•[8C- getty@tty1.service:•[32C [ •[1;31mINSEGURO•[0m ]
•[8C- gnome-remote-desktop.service:•[22C [ •[1;31mINSEGURO•[0m ]
•[8C- kerneloops.service:•[32C [ •[1;31mINSEGURO•[0m ]
•[8C- lynis.service:•[37C [ •[1;31mINSEGURO•[0m ]
```



```

•[8C- networkd-dispatcher.service:•[23C [ •[1;31mINSEGURO•[0m ]
•[8C- open-vm-tools.service:•[29C [ •[1;31mINSEGURO•[0m ]
•[8C- packagekit.service:•[32C [ •[1;31mINSEGURO•[0m ]
•[8C- plymouth-start.service:•[28C [ •[1;31mINSEGURO•[0m ]
•[8C- polkit.service:•[36C [ •[1;32mPROTEGIDO•[0m ]
•[8C- power-profiles-daemon.service:•[21C [ •[1;37mMEDIO•[0m ]
•[8C- rc-local.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- rescue.service:•[36C [ •[1;31mINSEGURO•[0m ]
•[8C- rsyslog.service:•[35C [ •[1;37mMEDIO•[0m ]
•[8C- rtkit-daemon.service:•[30C [ •[1;37mMEDIO•[0m ]
•[8C- snapd.service:•[37C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-autofs.service:•[31C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-nss.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-pac.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-pam.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-ssh.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd-sudo.service:•[33C [ •[1;31mINSEGURO•[0m ]
•[8C- sssd.service:•[38C [ •[1;33mEXPUESTO•[0m ]
•[8C- switcheroo-control.service:•[24C [ •[1;33mEXPUESTO•[0m ]
•[8C- systemd-ask-password-console.service:•[14C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-ask-password-plymouth.service:•[13C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-ask-password-wall.service:•[17C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-bsod.service:•[30C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-fsckd.service:•[29C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-initctl.service:•[27C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-journald.service:•[26C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-logind.service:•[28C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-networkd.service:•[26C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-oomd.service:•[30C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-resolved.service:•[26C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-rfkill.service:•[28C [ •[1;31mINSEGURO•[0m ]
•[8C- systemd-timesyncd.service:•[25C [ •[1;32mPROTEGIDO•[0m ]
•[8C- systemd-udev.service:•[29C [ •[1;37mMEDIO•[0m ]
•[8C- thermal.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- tpm-udev.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- ubuntu-advantage.service:•[26C [ •[1;31mINSEGURO•[0m ]
•[8C- udisks2.service:•[35C [ •[1;31mINSEGURO•[0m ]
•[8C- unattended-upgrades.service:•[23C [ •[1;31mINSEGURO•[0m ]
•[8C- upower.service:•[36C [ •[1;32mPROTEGIDO•[0m ]
•[8C- user@1000.service:•[33C [ •[1;31mINSEGURO•[0m ]
•[8C- uidd.service:•[37C [ •[1;37mMEDIO•[0m ]
•[8C- vgauth.service:•[36C [ •[1;31mINSEGURO•[0m ]
•[8C- whoopsie.service:•[34C [ •[1;31mINSEGURO•[0m ]
•[8C- wpa_supplicant.service:•[28C [ •[1;31mINSEGURO•[0m ]

```

```

[+] •[1;33mKernel•[0m
-----

```

```

•[2C- Checking default run level•[31C [ •[1;32mRUNLEVEL 5•[0m ]
•[2C- Checking CPU support (NX/PAE)•[28C
•[4CCPU support: PAE and/or NoeXecute supported•[14C [ •[1;32mENCONTRADO•[0m ]
•[2C- Checking kernel version and release•[22C [ •[1;32mHECHO•[0m ]
•[2C- Checking kernel type•[37C [ •[1;32mHECHO•[0m ]
•[2C- Checking loaded kernel modules•[27C [ •[1;32mHECHO•[0m ]
•[6CFound 82 active modules•[32C

```

•[2C- Checking Linux kernel configuration file•[17C [•[1;32mENCONTRADO•[0m]
•[2C- Checking default I/O kernel scheduler•[20C [•[1;37mNO ENCONTRADO•[0m]
•[2C- Checking for available kernel update•[21C [•[1;32mOK•[0m]
•[2C- Checking core dumps configuration•[24C
•[4C- configuration in systemd conf files•[20C [•[1;37mPOR DEFECTO•[0m]
•[4C- configuration in /etc/profile•[26C [•[1;37mPOR DEFECTO•[0m]
•[4C- 'hard' configuration in /etc/security/limits.conf•[6C [•[1;37mPOR DEFECTO•[0m]
•[4C- 'soft' configuration in /etc/security/limits.conf•[6C [•[1;37mPOR DEFECTO•[0m]
•[4C- Checking setuid core dumps configuration•[15C [•[1;37mPROTEGIDO•[0m]
•[2C- Check if reboot is needed•[32C [•[1;32mNO•[0m]

[+] •[1;33mMemoria y procesos•[0m

•[2C- Checking /proc/meminfo•[35C [•[1;32mENCONTRADO•[0m]
•[2C- Searching for dead/zombie processes•[22C [•[1;32mNO ENCONTRADO•[0m]
•[2C- Searching for IO waiting processes•[23C [•[1;32mNO ENCONTRADO•[0m]
•[2C- Search prelink tooling•[35C [•[1;32mNO ENCONTRADO•[0m]

[+] •[1;33mUsuarios, grupos y autenticación•[0m

•[2C- Administrator accounts•[35C [•[1;32mOK•[0m]
•[2C- Unique UIDs•[46C [•[1;32mOK•[0m]
•[2C- Consistency of group files (grpck)•[23C [•[1;32mOK•[0m]
•[2C- Unique group IDs•[41C [•[1;32mOK•[0m]
•[2C- Unique group names•[39C [•[1;32mOK•[0m]
•[2C- Password file consistency•[32C [•[1;32mOK•[0m]
•[2C- Password hashing methods•[33C [•[1;33mSUGERENCIA•[0m]
•[2C- Checking password hashing rounds•[25C [•[1;33mDESHABILITADO•[0m]
•[2C- Query system users (non daemons)•[25C [•[1;32mHECHO•[0m]
•[2C- NIS+ authentication support•[30C [•[1;37mNO HABILITADO•[0m]
•[2C- NIS authentication support•[31C [•[1;37mNO HABILITADO•[0m]
•[2C- Sudoers file(s)•[42C [•[1;32mENCONTRADO•[0m]
•[4C- Permissions for directory: /etc/sudoers.d•[14C [•[1;31mPELIGRO•[0m]
•[4C- Permissions for: /etc/sudoers•[26C [•[1;32mOK•[0m]
•[4C- Permissions for: /etc/sudoers.d/README•[17C [•[1;32mOK•[0m]
•[2C- PAM password strength tools•[30C [•[1;32mOK•[0m]
•[2C- PAM configuration files (pam.conf)•[23C [•[1;32mENCONTRADO•[0m]
•[2C- PAM configuration files (pam.d)•[26C [•[1;32mENCONTRADO•[0m]
•[2C- PAM modules•[46C [•[1;32mENCONTRADO•[0m]
•[2C- LDAP module in PAM•[39C [•[1;37mNO ENCONTRADO•[0m]
•[2C- Accounts without expire date•[29C [•[1;33mSUGERENCIA•[0m]
•[2C- Accounts without password•[32C [•[1;32mOK•[0m]
•[2C- Locked accounts•[42C [•[1;32mOK•[0m]
•[2C- Checking user password aging (minimum)•[19C [•[1;33mDESHABILITADO•[0m]
•[2C- User password aging (maximum)•[28C [•[1;33mDESHABILITADO•[0m]
•[2C- Checking expired passwords•[31C [•[1;32mOK•[0m]
•[2C- Checking Linux single user mode authentication•[11C [•[1;32mOK•[0m]
•[2C- Determining default umask•[32C
•[4C- umask (/etc/profile)•[35C [•[1;33mNO ENCONTRADO•[0m]
•[4C- umask (/etc/login.defs)•[32C [•[1;33mSUGERENCIA•[0m]
•[2C- LDAP authentication support•[30C [•[1;37mNO HABILITADO•[0m]
•[2C- Logging failed login attempts•[28C [•[1;32mHABILITADO•[0m]

[+] •[1;33mShells•[0m

•[2C- Checking shells from /etc/shells•[25C
•[4CResult: found 7 shells (valid shells: 7).•[16C
•[4C- Session timeout settings/tools•[25C [•[1;33mNINGUNO•[0m]
•[2C- Checking default umask values•[28C
•[4C- Checking default umask in /etc/bash.bashrc•[13C [•[1;33mNINGUNO•[0m]
•[4C- Checking default umask in /etc/profile•[17C [•[1;33mNINGUNO•[0m]

[+] •[1;33mSistemas de ficheros•[0m

•[2C- Checking mount points•[36C
•[4C- Checking /home mount point•[29C [•[1;33mSUGERENCIA•[0m]
•[4C- Checking /tmp mount point•[30C [•[1;33mSUGERENCIA•[0m]
•[4C- Checking /var mount point•[30C [•[1;33mSUGERENCIA•[0m]
•[2C- Query swap partitions (fstab)•[28C [•[1;33mNINGUNO•[0m]
•[2C- Testing swap partitions•[34C [•[1;32mOK•[0m]
•[2C- Testing /proc mount (hidepid)•[28C [•[1;33mSUGERENCIA•[0m]
•[2C- Checking for old files in /tmp•[27C [•[1;32mOK•[0m]
•[2C- Checking /tmp sticky bit•[33C [•[1;32mOK•[0m]
•[2C- Checking /var/tmp sticky bit•[29C [•[1;32mOK•[0m]
•[2C- ACL support root file system•[29C [•[1;32mHABILITADO•[0m]
•[2C- Mount options of /•[39C [•[1;32mOK•[0m]
•[2C- Mount options of /dev•[36C [•[1;33mPARCIALMENTE BASTIONADO•[0m]
•[2C- Mount options of /dev/shm•[32C [•[1;33mPARCIALMENTE BASTIONADO•[0m]
•[2C- Mount options of /run•[36C [•[1;32mBASTIONADO•[0m]
•[2C- Total without nodev:6 noexec:22 nosuid:16 ro or noexec (W^X): 10 of total 38•[0C
•[2C- Disable kernel support of some filesystems•[15C

[+] •[1;33mDispositivos USB•[0m

•[2C- Checking usb-storage driver (modprobe config)•[12C [•[1;37mNO DESHABILITADO•[0m]
•[2C- Checking USB devices authorization•[23C [•[1;33mHABILITADO•[0m]
•[2C- Checking USBGuard•[40C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mAlmacenamiento•[0m

•[2C- Checking firewire ohci driver (modprobe config)•[10C [•[1;32mDESHABILITADO•[0m]

[+] •[1;33mNFS•[0m

•[2C- Check running NFS daemon•[33C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mServicios de nombres•[0m

•[2C- Checking search domains•[34C [•[1;32mENCONTRADO•[0m]
•[2C- Checking /etc/resolv.conf options•[24C [•[1;32mENCONTRADO•[0m]
•[2C- Searching DNS domain name•[32C [•[1;33mDESCONOCIDO•[0m]
•[2C- Checking /etc/hosts•[38C
•[4C- Duplicate entries in hosts file•[24C [•[1;32mNINGUNO•[0m]

```
•[4C- Presence of configured hostname in /etc/hosts•[10C [ •[1;32mENCONTRADO•[0m ]
•[4C- Hostname mapped to localhost•[27C [ •[1;32mNO ENCONTRADO•[0m ]
•[4C- Localhost mapping to IP address•[24C [ •[1;32mOK•[0m ]
```

```
[+] •[1;33mPuertos y paquetes•[0m
```

```
-----
•[2C- Searching package managers•[31C
•[4C- Searching dpkg package manager•[25C [ •[1;32mENCONTRADO•[0m ]
•[6C- Querying package manager•[29C
•[4C- Query unpurged packages•[32C [ •[1;32mNINGUNO•[0m ]
•[2C- Checking security repository in sources.list.d directory•[1C [ •[1;32mOK•[0m ]
•[2C- Checking APT package database•[28C [ •[1;32mOK•[0m ]
•[2C- Checking vulnerable packages•[29C [ •[1;32mOK•[0m ]
•[2C- Checking upgradeable packages•[28C [ •[1;37mOMITIDO•[0m ]
•[2C- Checking package audit tool•[30C [ •[1;32mINSTALADO•[0m ]
•[4CFound: apt-check•[41C
•[2C- Toolkit for automatic upgrades (unattended-upgrade)•[6C [ •
[1;32mENCONTRADO•[0m ]
```

```
[+] •[1;33mConectividad•[0m
```

```
-----
•[2C- Checking IPv6 configuration•[30C [ •[1;37mHABILITADO•[0m ]
•[6CConfiguration method•[35C [ •[1;37mAUTO•[0m ]
•[6CIPv6 only•[46C [ •[1;37mNO•[0m ]
•[2C- Checking configured nameservers•[26C
•[4C- Testing nameservers•[36C
•[8CNameserver: 127.0.0.53•[31C [ •[1;32mOK•[0m ]
•[4C- DNSSEC supported (systemd-resolved)•[20C [ •[1;31mDESCONOCIDO•[0m ]
•[2C- Getting listening ports (TCP/UDP)•[24C [ •[1;32mHECHO•[0m ]
•[2C- Checking promiscuous interfaces•[26C [ •[1;32mOK•[0m ]
•[2C- Checking status DHCP client•[30C
•[2C- Checking for ARP monitoring software•[21C [ •[1;33mNO ENCONTRADO•[0m ]
•[2C- Uncommon network protocols•[31C [ •[1;33m0•[0m ]
```

```
[+] •[1;33mImpresoras y spools•[0m
```

```
-----
•[2C- Checking cups daemon•[37C [ •[1;32mCORRIENDO•[0m ]
•[2C- Checking CUPS configuration file•[25C [ •[1;32mOK•[0m ]
•[4C- File permissions•[39C [ •[1;31mPELIGRO•[0m ]
•[2C- Checking CUPS addresses/sockets•[26C [ •[1;32mENCONTRADO•[0m ]
•[2C- Checking lp daemon•[39C [ •[1;37mNO ESTÁ CORRIENDO•[0m ]
```

```
[+] •[1;33mSoftware: correo electrónico y mensajería•[0m
```

```
[+] •[1;33mSoftware: firewalls•[0m
```

```
-----
•[2C- Checking iptables kernel module•[26C [ •[1;32mENCONTRADO•[0m ]
•[4C- Checking iptables policies of chains•[19C [ •[1;32mENCONTRADO•[0m ]
•[4C- Checking for empty ruleset•[29C [ •[1;31mPELIGRO•[0m ]
•[4C- Checking for unused rules•[30C [ •[1;32mOK•[0m ]
•[2C- Checking host based firewall•[29C [ •[1;32mACTIVO•[0m ]
```

[+] •[1;33mSoftware: servidor web•[0m

•[2C- Checking Apache•[42C [•[1;37mNO ENCONTRADO•[0m]
•[2C- Checking nginx•[43C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mSoporte SSH•[0m

•[2C- Checking running SSH daemon•[30C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mSoporte SNMP•[0m

•[2C- Checking running SNMP daemon•[29C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mBases de datos•[0m

•[4CNo database engines found•[32C

[+] •[1;33mServicios LDAP•[0m

•[2C- Checking OpenLDAP instance•[31C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mPHP•[0m

•[2C- Checking PHP•[45C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mSoporte Squid•[0m

•[2C- Checking running Squid daemon•[28C [•[1;37mNO ENCONTRADO•[0m]

[+] •[1;33mLogging y ficheros•[0m

•[2C- Checking for a running log daemon•[24C [•[1;32mOK•[0m]
•[4C- Checking Syslog-NG status•[30C [•[1;37mNO ENCONTRADO•[0m]
•[4C- Checking systemd journal status•[24C [•[1;32mENCONTRADO•[0m]
•[4C- Checking Metalog status•[32C [•[1;37mNO ENCONTRADO•[0m]
•[4C- Checking RSyslog status•[32C [•[1;32mENCONTRADO•[0m]
•[4C- Checking RFC 3195 daemon status•[24C [•[1;37mNO ENCONTRADO•[0m]
•[4C- Checking minilogd instances•[28C [•[1;37mNO ENCONTRADO•[0m]
•[2C- Checking logrotate presence•[30C [•[1;32mOK•[0m]
•[2C- Checking remote logging•[34C [•[1;33mNO HABILITADO•[0m]
•[2C- Checking log directories (static list)•[19C [•[1;32mHECHO•[0m]
•[2C- Checking open log files•[34C [•[1;32mHECHO•[0m]
•[2C- Checking deleted files in use•[28C [•[1;33mARCHIVOS ENCONTRADOS•[0m]

[+] •[1;33mServicios inseguros•[0m

•[2C- Installed inetd package•[34C [•[1;32mNO ENCONTRADO•[0m]
•[2C- Installed xinetd package•[33C [•[1;32mOK•[0m]
•[4C- xinetd status•[42C
•[2C- Installed rsh client package•[29C [•[1;32mOK•[0m]
•[2C- Installed rsh server package•[29C [•[1;32mOK•[0m]
•[2C- Installed telnet client package•[26C [•[1;32mOK•[0m]
•[2C- Installed telnet server package•[26C [•[1;32mNO ENCONTRADO•[0m]
•[2C- Checking NIS client installation•[25C [•[1;32mOK•[0m]

```
•[2C- Checking NIS server installation•[25C [ •[1;32mOK•[0m ]
•[2C- Checking TFTP client installation•[24C [ •[1;32mOK•[0m ]
•[2C- Checking TFTP server installation•[24C [ •[1;32mOK•[0m ]
```

```
[+] •[1;33mBanners e identificación•[0m
```

```
-----
•[2C- /etc/issue•[47C [ •[1;32mENCONTRADO•[0m ]
•[4C- /etc/issue contents•[36C [ •[1;33mDÉBIL•[0m ]
•[2C- /etc/issue.net•[43C [ •[1;32mENCONTRADO•[0m ]
•[4C- /etc/issue.net contents•[32C [ •[1;33mDÉBIL•[0m ]
```

```
[+] •[1;33mTareas programadas•[0m
```

```
-----
•[2C- Checking crontab and cronjob files•[23C [ •[1;32mHECHO•[0m ]
```

```
[+] •[1;33mContabilidad•[0m
```

```
-----
•[2C- Checking accounting information•[26C [ •[1;33mNO ENCONTRADO•[0m ]
•[2C- Checking sysstat accounting data•[25C [ •[1;37mDESHABILITADO•[0m ]
•[2C- Checking auditd•[42C [ •[1;37mNO ENCONTRADO•[0m ]
```

```
[+] •[1;33mTiempo y sincronización•[0m
```

```
-----
•[2C- NTP daemon found: systemd (timesyncd)•[20C [ •[1;32mENCONTRADO•[0m ]
•[2C- Checking for a running NTP daemon or client•[14C [ •[1;32mOK•[0m ]
•[2C- Last time synchronization•[32C [ •[1;32m331s•[0m ]
```

```
[+] •[1;33mCriptografía•[0m
```

```
-----
•[2C- Checking for expired SSL certificates [0/151]•[12C [ •[1;32mNINGUNO•[0m ]
```

```
•[30;43m[WARNING]•[0m: Test CRYPT-7902 had a long execution: 13.601958
seconds•[0m
```

```
•[2C- Kernel entropy is sufficient•[29C [ •[1;32mSÍ•[0m ]
•[2C- HW RNG & rngd•[44C [ •[1;33mNO•[0m ]
•[2C- SW prng•[50C [ •[1;33mNO•[0m ]
•[2C- MOR variable not found•[35C [ •[1;37mDÉBIL•[0m ]
```

```
[+] •[1;33mVirtualización•[0m
```

```
-----
[+] •[1;33mContenedores•[0m
```

```
-----
[+] •[1;33mFrameworks de seguridad•[0m
```

```
-----
•[2C- Checking presence AppArmor•[31C [ •[1;32mENCONTRADO•[0m ]
•[4C- Checking AppArmor status•[31C [ •[1;32mHABILITADO•[0m ]
•[8CFound 115 unconfined processes•[23C
•[2C- Checking presence SELinux•[32C [ •[1;37mNO ENCONTRADO•[0m ]
•[2C- Checking presence TOMOYO Linux•[27C [ •[1;37mNO ENCONTRADO•[0m ]
•[2C- Checking presence grsecurity•[29C [ •[1;37mNO ENCONTRADO•[0m ]
•[2C- Checking for implemented MAC framework•[19C [ •[1;32mOK•[0m ]
```

[+] •[1;33mSoftware: integridad de ficheros•[0m

•[2C- Checking file integrity tools•[28C

•[2C- Checking presence integrity tool•[25C [•[1;33mNO ENCONTRADO•[0m]

[+] •[1;33mSoftware: Herramientas del sistema•[0m

•[2C- Checking automation tooling•[30C

•[2C- Automation tooling•[39C [•[1;33mNO ENCONTRADO•[0m]

•[2C- Checking for IDS/IPS tooling•[29C [•[1;33mNINGUNO•[0m]

[+] •[1;33mSoftware: Malware•[0m

•[2C- Malware software components•[30C [•[1;33mNO ENCONTRADO•[0m]

[+] •[1;33mPermisos de ficheros•[0m

•[2C- Starting file permissions check•[26C

•[4CFile: /boot/grub/grub.cfg•[32C [•[1;32mOK•[0m]

•[4CFile: /etc/crontab•[39C [•[1;33mSUGERENCIA•[0m]

•[4CFile: /etc/group•[41C [•[1;32mOK•[0m]

•[4CFile: /etc/group-•[40C [•[1;32mOK•[0m]

•[4CFile: /etc/hosts.allow•[35C [•[1;32mOK•[0m]

•[4CFile: /etc/hosts.deny•[36C [•[1;32mOK•[0m]

•[4CFile: /etc/issue•[41C [•[1;32mOK•[0m]

•[4CFile: /etc/issue.net•[37C [•[1;32mOK•[0m]

•[4CFile: /etc/passwd•[40C [•[1;32mOK•[0m]

•[4CFile: /etc/passwd-•[39C [•[1;32mOK•[0m]

•[4CDirectory: /root/.ssh•[36C [•[1;32mOK•[0m]

•[4CDirectory: /etc/cron.d•[35C [•[1;33mSUGERENCIA•[0m]

•[4CDirectory: /etc/cron.daily•[31C [•[1;33mSUGERENCIA•[0m]

•[4CDirectory: /etc/cron.hourly•[30C [•[1;33mSUGERENCIA•[0m]

•[4CDirectory: /etc/cron.weekly•[30C [•[1;33mSUGERENCIA•[0m]

•[4CDirectory: /etc/cron.monthly•[29C [•[1;33mSUGERENCIA•[0m]

[+] •[1;33mDirectorios de inicio•[0m

•[2C- Permissions of home directories•[26C [•[1;32mOK•[0m]

•[2C- Ownership of home directories•[28C [•[1;32mOK•[0m]

•[2C- Checking shell history files•[29C [•[1;32mOK•[0m]

[+] •[1;33mBastionado del kernel•[0m

•[2C- Comparing sysctl key pairs with scan profile•[13C

•[4C- dev.tty.ldisc_autoload (exp: 0)•[24C [•[1;31mDIFERENTE•[0m]

•[4C- fs.protected_fifos (exp: 2)•[28C [•[1;31mDIFERENTE•[0m]

•[4C- fs.protected_hardlinks (exp: 1)•[24C [•[1;32mOK•[0m]

•[4C- fs.protected_regular (exp: 2)•[26C [•[1;32mOK•[0m]

•[4C- fs.protected_symlinks (exp: 1)•[25C [•[1;32mOK•[0m]

•[4C- fs.suid_dumpable (exp: 0)•[30C [•[1;31mDIFERENTE•[0m]

•[4C- kernel.core_uses_pid (exp: 1)•[26C [•[1;31mDIFERENTE•[0m]

•[4C- kernel.ctrl-alt-del (exp: 0)•[27C [•[1;32mOK•[0m]

•[4C- kernel.dmesg_restrict (exp: 1)•[25C [•[1;32mOK•[0m]

```

•[4C- kernel.kptr_restrict (exp: 2)•[26C [ •[1;31mDIFERENTE•[0m ]
•[4C- kernel.modules_disabled (exp: 1)•[23C [ •[1;31mDIFERENTE•[0m ]
•[4C- kernel.perf_event_paranoid (exp: 3)•[20C [ •[1;31mDIFERENTE•[0m ]
•[4C- kernel.randomize_va_space (exp: 2)•[21C [ •[1;32mOK•[0m ]
•[4C- kernel.sysrq (exp: 0)•[34C [ •[1;31mDIFERENTE•[0m ]
•[4C- kernel.unprivileged_bpf_disabled (exp: 1)•[14C [ •[1;31mDIFERENTE•[0m ]
•[4C- kernel.yama.ptrace_scope (exp: 1 2 3)•[18C [ •[1;32mOK•[0m ]
•[4C- net.core.bpf_jit_harden (exp: 2)•[23C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.all.accept_redirects (exp: 0)•[12C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.all.accept_source_route (exp: 0)•[9C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.conf.all.bootp_relay (exp: 0)•[17C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.conf.all.forwarding (exp: 0)•[18C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.conf.all.log_martians (exp: 1)•[16C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.all.mc_forwarding (exp: 0)•[15C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.conf.all.proxy_arp (exp: 0)•[19C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.conf.all.rp_filter (exp: 1)•[19C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.all.send_redirects (exp: 0)•[14C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.default.accept_redirects (exp: 0)•[8C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.default.accept_source_route (exp: 0)•[5C [ •
[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.conf.default.log_martians (exp: 1)•[12C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)•[10C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)•[4C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.tcp_syncookies (exp: 1)•[23C [ •[1;32mOK•[0m ]
•[4C- net.ipv4.tcp_timestamps (exp: 0 1)•[21C [ •[1;32mOK•[0m ]
•[4C- net.ipv6.conf.all.accept_redirects (exp: 0)•[12C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv6.conf.all.accept_source_route (exp: 0)•[9C [ •[1;32mOK•[0m ]
•[4C- net.ipv6.conf.default.accept_redirects (exp: 0)•[8C [ •[1;31mDIFERENTE•[0m ]
•[4C- net.ipv6.conf.default.accept_source_route (exp: 0)•[5C [ •[1;32mOK•[0m ]

```

[+] •[1;33mBastionado•[0m

```

-----
•[4C- Installed compiler(s)•[34C [ •[1;32mNO ENCONTRADO•[0m ]
•[4C- Installed malware scanner•[30C [ •[1;31mNO ENCONTRADO•[0m ]
•[4C- Non-native binary formats•[30C [ •[1;31mENCONTRADO•[0m ]

```

[+] •[1;33mPruebas personalizadas•[0m

```

-----
•[2C- Running custom tests... •[33C [ •[1;37mNINGUNO•[0m ]

```

[+] •[1;35mPlugins (fase 2)•[0m

```

=====
-[ •[1;37mLynis 3.0.9 Results•[0m ]-

```

```

•[1;31mWarnings•[0m (1):
•[1;37m-----•[0m
•[1;31m!•[0m iptables module(s) loaded, but no rules active [FIRE-4512]
    https://cisofy.com/lynis/controls/FIRE-4512/

```

```

•[1;33mSuggestions•[0m (39):
•[1;37m-----•[0m

```


•[1;33m*•[0m This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
•[0;37mhttps://cisofy.com/lynis/controls/LYNIS/•[0m

•[1;33m*•[0m Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions [DEB-0280]
•[0;37mhttps://cisofy.com/lynis/controls/DEB-0280/•[0m

•[1;33m*•[0m Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
•[0;37mhttps://cisofy.com/lynis/controls/DEB-0810/•[0m

•[1;33m*•[0m Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
•[0;37mhttps://cisofy.com/lynis/controls/DEB-0811/•[0m

•[1;33m*•[0m 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 restarting. [DEB-0831]
•[0;37mhttps://cisofy.com/lynis/controls/DEB-0831/•[0m

•[1;33m*•[0m Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
•[0;37mhttps://cisofy.com/lynis/controls/DEB-0880/•[0m

•[1;33m*•[0m Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
•[0;37mhttps://cisofy.com/lynis/controls/BOOT-5122/•[0m

•[1;33m*•[0m Consider hardening system services [BOOT-5264]
- Details : •[0;36mRun '/usr/bin/systemd-analyze security SERVICE' for each service•[0m
•[0;37mhttps://cisofy.com/lynis/controls/BOOT-5264/•[0m

•[1;33m*•[0m If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
•[0;37mhttps://cisofy.com/lynis/controls/KRNL-5820/•[0m

•[1;33m*•[0m Check PAM configuration, add rounds if applicable and expire passwords to encrypt with new values [AUTH-9229]
•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9229/•[0m

•[1;33m*•[0m Configure password hashing rounds in /etc/login.defs [AUTH-9230]
•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9230/•[0m

•[1;33m*•[0m When possible set expire dates for all password protected accounts [AUTH-9282]
•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9282/•[0m

•[1;33m*•[0m Configure minimum password age in /etc/login.defs [AUTH-9286]
•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/•[0m

•[1;33m*•[0m Configure maximum password age in /etc/login.defs [AUTH-9286]
•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/•[0m

•[1;33m*•[0m Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

•[0;37mhttps://cisofy.com/lynis/controls/AUTH-9328/•[0m

•[1;33m*•[0m To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

•[0;37mhttps://cisofy.com/lynis/controls/FILE-6310/•[0m

•[1;33m*•[0m To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

•[0;37mhttps://cisofy.com/lynis/controls/FILE-6310/•[0m

•[1;33m*•[0m To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

•[0;37mhttps://cisofy.com/lynis/controls/FILE-6310/•[0m

•[1;33m*•[0m Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

•[0;37mhttps://cisofy.com/lynis/controls/USB-1000/•[0m

•[1;33m*•[0m Check DNS configuration for the dns domain name [NAME-4028]

•[0;37mhttps://cisofy.com/lynis/controls/NAME-4028/•[0m

•[1;33m*•[0m Install debsums utility for the verification of packages with known good database. [PKGS-7370]

•[0;37mhttps://cisofy.com/lynis/controls/PKGS-7370/•[0m

•[1;33m*•[0m Install package apt-show-versions for patch management purposes [PKGS-7394]

•[0;37mhttps://cisofy.com/lynis/controls/PKGS-7394/•[0m

•[1;33m*•[0m Determine if protocol 'dccp' is really needed on this system [NETW-3200]

•[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/•[0m

•[1;33m*•[0m Determine if protocol 'sctp' is really needed on this system [NETW-3200]

•[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/•[0m

•[1;33m*•[0m Determine if protocol 'rds' is really needed on this system [NETW-3200]

•[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/•[0m

•[1;33m*•[0m Determine if protocol 'tipc' is really needed on this system [NETW-3200]

•[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/•[0m

•[1;33m*•[0m Access to CUPS configuration could be more strict. [PRNT-2307]

•[0;37mhttps://cisofy.com/lynis/controls/PRNT-2307/•[0m

•[1;33m*•[0m Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

•[0;37mhttps://cisofy.com/lynis/controls/LOGG-2154/•[0m

•[1;33m*•[0m Check what deleted files are still in use and why. [LOGG-2190]
•[0;37mhttps://cisofy.com/lynis/controls/LOGG-2190/•[0m

•[1;33m*•[0m Add a legal banner to /etc/issue, to warn unauthorized users
[BANN-7126]
•[0;37mhttps://cisofy.com/lynis/controls/BANN-7126/•[0m

•[1;33m*•[0m Add legal banner to /etc/issue.net, to warn unauthorized users
[BANN-7130]
•[0;37mhttps://cisofy.com/lynis/controls/BANN-7130/•[0m

•[1;33m*•[0m Enable process accounting [ACCT-9622]
•[0;37mhttps://cisofy.com/lynis/controls/ACCT-9622/•[0m

•[1;33m*•[0m Enable sysstat to collect accounting (disabled) [ACCT-9626]
•[0;37mhttps://cisofy.com/lynis/controls/ACCT-9626/•[0m

•[1;33m*•[0m Enable auditd to collect audit information [ACCT-9628]
•[0;37mhttps://cisofy.com/lynis/controls/ACCT-9628/•[0m

•[1;33m*•[0m Install a file integrity tool to monitor changes to critical and
sensitive files [FINT-4350]
•[0;37mhttps://cisofy.com/lynis/controls/FINT-4350/•[0m

•[1;33m*•[0m Determine if automation tools are present for system management
[TOOL-5002]
•[0;37mhttps://cisofy.com/lynis/controls/TOOL-5002/•[0m

•[1;33m*•[0m Consider restricting file permissions [FILE-7524]
- Details : •[0;36mSee screen output or log file•[0m
- Solution : Use chmod to change file permissions
•[0;37mhttps://cisofy.com/lynis/controls/FILE-7524/•[0m

•[1;33m*•[0m One or more sysctl values differ from the scan profile and could
be tweaked [KRNL-6000]
- Solution : Change sysctl value or disable test
(skip-test=KRNL-6000:<sysctl-key>)
•[0;37mhttps://cisofy.com/lynis/controls/KRNL-6000/•[0m

•[1;33m*•[0m Harden the system by installing at least one malware scanner, to
perform periodic file system scans [HRDN-7230]
- Solution : Install a tool like rkhunter, chkrootkit, OSSEC
•[0;37mhttps://cisofy.com/lynis/controls/HRDN-7230/•[0m

•[0;36mFollow-up•[0m:
•[1;37m-----•[0m
•[1;37m-•[0m Show details of a test (lynis show details TEST-ID)
•[1;37m-•[0m Check the logfile for all details (less /var/log/lynis.log)
•[1;37m-•[0m Read security controls texts (https://cisofy.com)
•[1;37m-•[0m Use --upload to upload data to central system (Lynis Enterprise
users)

=====

•[1;37mLynis security scan details•[0m:

•[0;36mHardening index•[0m : •[1;37m64•[0m [•[1;33m#####•[0m]

•[0;36mTests performed•[0m : •[1;37m249•[0m

•[0;36mPlugins enabled•[0m : •[1;37m1•[0m

•[1;37mComponents•[0m:

- Firewall [•[1;32mV•[0m]

- Malware scanner [•[1;31mX•[0m]

•[1;33mScan mode•[0m:

Normal [V] Forensics [] Integration [] Pentest []

•[1;33mLynis modules•[0m:

- Compliance status [•[1;33m?•[0m]

- Security audit [•[1;32mV•[0m]

- Vulnerability scan [•[1;32mV•[0m]

•[1;33mFiles•[0m:

- Test and debug information : •[1;37m/var/log/lynis.log•[0m

- Report data : •[1;37m/var/log/lynis-report.dat•[0m

=====

•[1;37mLynis•[0m 3.0.9

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2021, CISOfy - <https://cisofy.com/lynis/>

•[1;37mEnterprise support available (compliance, plugins, interface and
tools)•[0m

=====

•[0;44m[TIP]•[0m: •[0;94mEnhance Lynis audits by adding your settings to
custom.prf (see /etc/lynis/default.prf for all settings)•[0m

Centro Criptológico Nacional



Nombre del sistema: ELOYPC
Organización: IES El Bohío
Unidad: Seguridad y Alta Disponibilidad
Categoría del sistema: ALTA

Auditado por Eloy Celdrán Madrid
Informes generados el día 05/10/2024 08:49:28 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74

Mostrar todo

Resumen		Ocultar
Cumplimiento del sistema - 41,56%		
Sistema		Ocultar
Nombre del sistema	ELOYPC	
Sistema operativo	Microsoft Windows 11 Pro (No hay Service Pack instalado / Internet Explorer: 11.1882.26100.0 / Windows Media Player: 12.0.26100.1)	
Rol del dominio	Cliente independiente	
Dominio / Grupo de trabajo	WORKGROUP	
Discos	C: (NTFS) / D: (exFAT)	
Direcciones IP	192.168.1.42	
	192.168.1.44	
	192.168.56.1	
	192.168.42.1	
	192.168.1.1	
	169.254.66.109	
	3.0.0.1	
	154.47.28.1	

Resultados		
Control ENS	Estado del control	Cumplimiento del control *
OP.ACC.5 - Mecanismos de autenticación (0%)		
OP.ACC.6 - Acceso local (0%)		
OP.EXP.2 - Configuración de seguridad (0%)		
OP.EXP.5 - Gestión de cambios (100%)		
OP.EXP.6 - Protección frente a código dañino (40%)		
MP.EQ.2 - Bloqueo de puesto de trabajo (0%)		
MP.EQ.3 - Protección de equipos informáticos (100%) **		
<p>* Cumplimiento de las medidas técnicas del ENS en función del nivel analizado para este sistema.</p> <p>** Esta prueba solo se realiza en el caso de que el sistema de cifrado Bitlocker se encuentre configurado en el sistema. En caso contrario, deberá evaluar de forma manual el sistema de cifrado del equipo.</p>		
Leyenda de estado del control		Leyenda de cumplimiento del control
<div></div>	Cumplimiento satisfactorio del control. No es necesario realizar ninguna acción.	<div></div> Representación visual del porcentaje de elementos del sistema que cumplen satisfactoriamente con el control ENS evaluado.
<div></div>	Cumplimiento parcial del control. Es necesaria la revisión del informe técnico.	<div></div> Representación visual del porcentaje de elementos del sistema que cumplen parcialmente con el control ENS evaluado. Aún no tratándose de un incumplimiento, estos elementos no atienden de forma óptima a las exigencias del ENS. Se hace necesaria la revisión del informe técnico para la posible aplicación de medidas correctoras.
<div></div>	Incumplimiento del control. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.	<div></div> Representación visual del porcentaje de elementos del sistema que no cumplen con el control ENS evaluado.
		% Valor numérico indicativo del porcentaje total de cumplimiento del control ENS evaluado. Engloba tanto los elementos del sistema que cumplen satisfactoriamente con el control, como aquellos elementos que lo hacen parcialmente.

0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74


Centro Criptológico Nacional




Nombre del sistema: ELOYPC
Organización: IES El Bohío
Unidad: Seguridad y Alta Disponibilidad
Categoría del sistema: ALTA


Auditado por Eloy Celdrán Madrid
Informes generados el día 05/10/2024 08:49:28 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74


Ocultar todo

Datos del sistema		Ocultar
Valor de criticidad		
Sistema		Ocultar
 Recoge la información de datos básicos del sistema		
Nombre del sistema	ELOYPC	
Modelo	GE66 Raider 11UH	
Fabricante	Micro-Star International Co., Ltd.	
Descripción	AT/AT COMPATIBLE	
Nombre del propietario	Usuario de Windows	
Tipo de sistema	x64-based PC	
Memoria física	31,71 GB's	
Rol del dominio	Cliente independiente	
Dominio / Grupo de trabajo	WORKGROUP	

Versión de PowerShell	5
------------------------------	---

Discos		Ocultar
 Recopila la información de los diferentes medios de almacenamiento del sistema, evaluando el tipo de formato de almacenamiento		
Letra de unidad	C:	
Nombre		
Tamaño	952,88 GB's	
Sistema de ficheros	NTFS	
Letra de unidad	D:	
Nombre	CORSAIR	
Tamaño	931,5 GB's	
Sistema de ficheros	exFAT	

Sistema operativo		Ocultar
 Recoge información del sistema operativo		
Nombre	Microsoft Windows 11 Pro	
Servidor	No	
Instalación core	No	
Directorio del sistema	C:\WINDOWS\system32	
Organización		
Versión	10.0.26100	
Versión de Service Pack	No hay Service Pack instalado	
Versión de Internet Explorer	11.1882.26100.0	
Versión de Windows Media Player	12.0.26100.1	
Número de compilación	26100	
Usuario registrado	Usuario de Windows	
Número de serie	00330-80000-00000-AA205	
Último arranque	05/10/2024 10:29:04	

 Recoge información sobre la configuración de región

Zona horaria (UTC+01:00) Bruselas, Copenhague, Madrid, París
Código de país 34
Localización 0c0a
Lenguaje del sistema operativo 3082
Teclado SP / SP / SP / SP / SP / SP

Adaptadores de red

Ocultar

 Recoge el conjunto de adaptadores de red presentes en el sistema

Descripción Killer E3100G 2.5 Gigabit Ethernet Controller
MAC D8:BB:C1:77:8A:D9
DHCP Sí
IP 192.168.1.42
Subred 255.255.255.0
Puerta de enlace predeterminada 192.168.1.1
Orden de búsqueda servidor DNS 80.58.61.250 - 80.58.61.254
Servidor primario WINS
Servidor secundario WINS

Descripción Killer(R) Wi-Fi 6E AX1675x 160MHz Wireless Network Adapter (210NGW)
MAC 04:56:E5:E4:3D:4C
DHCP Sí
IP 192.168.1.44
Subred 255.255.255.0
Puerta de enlace predeterminada 192.168.1.1
Orden de búsqueda servidor DNS 80.58.61.250 - 80.58.61.254
Servidor primario WINS
Servidor secundario

WINS	
Descripción	VirtualBox Host-Only Ethernet Adapter
MAC	0A:00:27:00:00:12
DHCP	No
IP	192.168.56.1 - fe80::2cbc:65a0:f310:a31e
Subred	255.255.255.0 / 64
Puerta de enlace predeterminada	
Orden de búsqueda servidor DNS	
Servidor primario WINS	
Servidor secundario WINS	
Descripción	VMware Virtual Ethernet Adapter for VMnet1
MAC	00:50:56:C0:00:01
DHCP	Sí
IP	192.168.42.1
Subred	255.255.255.0
Puerta de enlace predeterminada	
Orden de búsqueda servidor DNS	
Servidor primario WINS	
Servidor secundario WINS	
Descripción	VMware Virtual Ethernet Adapter for VMnet19
MAC	00:50:56:C0:00:13
DHCP	No
IP	192.168.1.1 - fe80::3e76:ef22:caf4:147e
Subred	255.255.255.0 / 64
Puerta de enlace predeterminada	
Orden de búsqueda servidor DNS	

<div>Servidor primario WINS</div> <div>Servidor secundario WINS</div>	
<div>Descripción</div> <div>MAC</div> <div>DHCP</div> <div>IP</div> <div>Subred</div> <div>Puerta de enlace predeterminada</div> <div>Orden de búsqueda servidor DNS</div> <div>Servidor primario WINS</div> <div>Servidor secundario WINS</div>	<div>VMware Virtual Ethernet Adapter for VMnet3</div> <div>00:50:56:C0:00:03</div> <div>No</div> <div>169.254.66.109</div> <div>255.255.0.0</div> <div></div> <div></div> <div></div> <div></div>
<div>Descripción</div> <div>MAC</div> <div>DHCP</div> <div>IP</div> <div>Subred</div> <div>Puerta de enlace predeterminada</div> <div>Orden de búsqueda servidor DNS</div> <div>Servidor primario WINS</div> <div>Servidor secundario WINS</div>	<div>VMware Virtual Ethernet Adapter for VMnet4</div> <div>00:50:56:C0:00:04</div> <div>No</div> <div>3.0.0.1 - fe80::2a4c:a375:60ad:b148</div> <div>255.0.0.0 / 64</div> <div></div> <div></div> <div></div> <div></div>
<div>Descripción</div> <div>MAC</div> <div>DHCP</div> <div>IP</div> <div>Subred</div> <div>Puerta de enlace</div>	<div>VMware Virtual Ethernet Adapter for VMnet5</div> <div>00:50:56:C0:00:05</div> <div>No</div> <div>154.47.28.1 - fe80::f329:afed:fc99:3752</div> <div>255.255.255.0 / 64</div> <div></div>

<div>predeterminada</div> <div>Orden de búsqueda servidor DNS</div> <div>Servidor primario WINS</div> <div>Servidor secundario WINS</div>

Análisis ENS

Ocultar

Resultados

Valor de criticidad Cumplimiento (41,56%)

OP.ACC.5 - Mecanismos de autenticación (0%)

Ocultar

Nombre	Valor actual	Valor esperado	Resultado
Configuración del equipo/Componentes de Windows/Biometría/Permitir el uso de biometría	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Biometría/Permitir que los usuarios de dominio inicien sesión mediante biometría	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Biometría/Permitir que los usuarios inicien sesión mediante biometría	No configurado	Habilitada	No configurado

OP.ACC.6 - Acceso local (0%)

Ocultar

Nombre	Valor actual	Valor esperado	Resultado
Configuración del equipo/Componentes de Windows/Opciones de inicio de sesión de Windows/Mostrar información acerca de inicios de sesión anteriores durante inicio de sesión de usuario	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Opciones de inicio de	No configurado	Habilitada	No configu

rado

sesión de Windows/Informar cuando el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario

OP.EXP.2 - Configuración de seguridad (0%)

Ocultar

Nombre	Valor actual	Valor esperado	Resultado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar uso compartido de datos de personalización de escritura a mano	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a la información de la cuenta	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan al historial de llamadas	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows tengan acceso a los contactos	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan al correo electrónico	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedana la ubicación	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a los mensajes	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan al movimiento	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan al calendario	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la	No configurado	Forzar denegación	No configurado

aplicación/Permitir que las aplicaciones de Windows accedan a la cámara			
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones accedan al micrófono	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a dispositivos de confianza	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows controlen las radios	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows se sincronicen con dispositivos	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a las notificaciones	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows realicen llamadas telefónicas	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a las tareas	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows accedan a la información de diagnóstico sobre otras aplicaciones	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de Windows se ejecuten en el fondo	No configurado	Forzar denegación	No configurado
Configuración del equipo/Componentes de Windows/Asistencia en línea/Desactivar la ayuda activa	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Buscar/No buscar en Internet o mostrar resultados de Internet en Search	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Contenido en la nube/Desactivar experiencias del consumidor de Microsoft	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Contenido en la nube/No	No configurado	Habilitada	No configurado

mostrar sugerencias de Windows			rado
Configuración del equipo/Componentes de Windows/Internet Explorer/Permitir a los servicios de Microsoft ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/One drive/Impedir el uso de OneDrive para almacenar archivos	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Recopilación de datos y versiones preliminares/No volver a mostrar notificaciones de comentarios	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Recopilación de datos y versiones preliminares/Permitir telemetría	No configurado	Básico	No configurado
Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar scripting de ubicación	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar sensores	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar ubicación	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Windows Media Center/No permitir que se ejecute Windows Media Center	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Perfiles de usuario/Administración del usuario del uso compartido de nombre de usuario, imagen de cuenta e información de dominio con aplicaciones (que no sean aplicaciones de escritorio)	No configurado	Siempre desactivado	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Permitir que se elimine el historial de exploración al salir	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen los datos de formularios	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen contraseñas	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar	No configurado	Deshabilitada	No configurado

el historial de navegación/Impedir que se eliminen cookies			rado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se elimine el historial de descarga	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen los sitios web que el usuario visitó	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen los datos de filtrado InPrivate	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen los archivos temporales de Internet	No configurado	No configurada/Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Evitar la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Impedir que se eliminen datos del sitio de favoritos	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Activar sitios sugeridos	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Almacén Digital/No permitir que se ejecute el Almacén digital	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Informe de errores de Windows/Deshabilitar el informe de errores de Windows	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Informe de errores de Windows/No enviar datos adicionales	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar informe de errores de reconocimiento de escritura a mano	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de	No configurado	Habilitada	No configurado

comunicaciones de Internet/Desactivar el Programa para la mejora de la experiencia del usuario de Windows			
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar los vínculos 'Events.asp' del Visor de eventos	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar el contenido '¿Sabía que...?' del Centro de ayuda y soporte técnico	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y soporte técnico	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar el informe de errores de Windows	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar la actualización de archivos de contenido del Asistente para búsqueda	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar el acceso a la tienda	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar la tarea de imágenes 'Pedir copias fotográficas'	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de comunicaciones de Internet/Desactivar	No configurado	Habilitada	No configurado

el Programa para la mejora de la experiencia del usuario de Windows Messenger

Configuración del equipo/Componentes de Windows/Administración de derechos digitales de Windows Media/Impedir el acceso a Internet de Windows Media DRM	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Directivas de Reproducción automática/Comportamiento predeterminado para la ejecución automática	No configurado	No ejecutar ningún comando de ejecución automática	No configurado
Configuración del equipo/Componentes de Windows/Directivas de Reproducción automática/Desactivar Reproducción automática	No configurado	Todas las unidades	No configurado
Configuración del equipo/Componentes de Windows/Shell remoto de Windows/Permitir acceso a shell remoto	No configurado	Deshabilitada	No configurado
Configuración del equipo/Sistema/Net Logon/Permitir algoritmos de criptografía compatibles con Windows NT 4.0	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Tienda/Desactivar la aplicación Tienda	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Tienda/Deshabilitar todas las aplicaciones de la Tienda Windows	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Buscar/Permitir el uso de Cortana	No configurado	Deshabilitada	No configurado
Configuración del equipo/Panel de control/Configuración regional y de idioma/Personalización de escritura a mano/Desactivar el aprendizaje automático (recopilación manuscrita)	No configurado	Habilitada	No configurado
Configuración del equipo/Panel de control/Configuración regional y de idioma/Personalización de escritura a mano/Desactivar el aprendizaje automático (recopilación escritura)	No configurado	Habilitada	No configurado
Configuración del equipo/Sistema/Perfiles de usuario/Desactivar el identificador de publicidad	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Internet Explorer/Configuración de Internet/Autocompletar/Desactivar las sugerencias de direcciones URL	No configurado	Habilitada	No configurado

Entrada	Notas	Resultado
Firewall de Windows	Los perfiles están habilitados	Correcto
Otro firewall	Los siguientes firewalls han sido detectados: Kaspersky	Correcto
Nivel de actualización	El sistema está actualizado dentro de los últimos 30 días.	Correcto

OP.EXP.6 - Protección frente a código dañino (40%)

Ocultar

Entrada	Notas	Resultado
Antivirus	Los siguientes antivirus han sido detectados: Windows Defender, Kaspersky	Correcto

Nombre	Valor actual	Valor esperado	Resultado
Configuración del equipo/Componentes de Windows/Internet Explorer/Impedir administración del filtro SmartScreen. Seleccionar modo de filtro SmartScreen:	No configurado	No configurada/Deshabilitada	Correcto
Configuración del equipo/Componentes de Windows/Endpoint Protection/Desactivar Endpoint Protection	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Microsoft Edge/Desactivar el filtro SmartScreen	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Explorador de archivos/Configurar Windows SmartScreen	No configurado	Requerir la aprobación de un administrador antes de ejecutar un software desconocido descargado	No configurado

MP.EQ.2 - Bloqueo de puesto de trabajo (0%)

Ocultar

Nombre	Valor actual	Valor esperado	Resultado
Configuración de usuario/Panel de control/Personalización/Habilitar protector de pantalla	No configurado	Habilitada	No configurado
Configuración de usuario/Panel de control/Personalización/Proteger el protector de pantalla mediante contraseña	No configurado	Habilitada	No configurado

MP.EQ.3 - Protección de equipos informáticos (100%) (*)

Ocultar

Nombre	Valor actual	Valor esperado	Resultado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e intensidad de cifrado de unidad (Windows 8, Windows server 2012,	No configurado	AES 256 bits	No configurado

Windows 8.1, Windows server 2012 R2,
Windows 10 [version 1507])

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades del sistema operativo:

No configurado

XTS-AES 256 bits

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades de datos fijas:

No configurado

XTS-AES 256 bits

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades de datos extraíbles:

No configurado

AES-CBC 256 bits

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Impedir la sobrescritura de memoria al reiniciar

No configurado

Deshabilitada

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades de datos extraíbles/Controlar el uso de BitLocker en unidades extraíbles

No configurado

Deshabilitada

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades de datos extraíbles/Controlar el uso de BitLocker en unidades extraíbles. Permitir que los usuarios apliquen la protección de BitLocker en unidades de datos extraíbles

No configurado

Deshabilitada

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades de datos extraíbles/Controlar el uso de BitLocker en unidades extraíbles. Permitir que los usuarios suspendan y descifren la protección de BitLocker en unidades de datos extraíbles

No configurado

Deshabilitada

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar longitud mínima de PIN para el inicio

No configurado

8

No configurado

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema

No configurado

Habilitada

No configurado

operativo/Permitir los PIN mejorados para el inicio			
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar. Permitir Bitlocker sin un TPM compatible (Requiere contraseña o clave de inicio en unidad flash USB):	No configurado	Desactivado/Deshabilitado	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar. Configurar clave de inicio del TPM:	No configurado	No permitir clave de inicio con TPM	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar. Configurar PIN de inicio con TPM:	No configurado	Requerir PIN de inicio con TPM	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar. Configurar la clave de inicio y el PIN del TPM:	No configurado	No permitir clave y PIN de inicio con TPM	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Requerir autenticación adicional al iniciar. Configurar inicio del TPM:	No configurado	No permitir TPM	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 0: CRTM (Core Root of Trust of Measurement), BIOS y extensiones de la plataforma	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 1:	No configurado	Deshabilitada	No configurado

Configuración y datos de placa base y plataforma

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 2: Código ROM de opción	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 3: Configuración y datos de ROM de opción	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 4: Código de registro de arranque maestro (MBR)	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 5: Tabla de participaciones de registro de arranque maestro (MBR)	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 6: Eventos de activación y transición de estado	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 7: Específico del fabricante del equipo	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 8: Sector de arranque de NTFS	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 9: Bloque de arranque de NTFS	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación	No configurado	Habilitada	No configurado

de plataforma del TPM. PCR 10:

Administrador de arranque

Configuración del equipo/Componentes **No configurado**

Habilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 11: Control

de acceso de BitLocker

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 12:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 13:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 14:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 15:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 16:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 17:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 18:

Reservado para uso futuro

Configuración del equipo/Componentes **No configurado**

Deshabilitada

**No
configu
rado**

de Windows/Cifrado de unidad

BitLocker/Unidades del sistema

operativo/Configurar perfil de validación

de plataforma del TPM. PCR 19:

Reservado para uso futuro

9/10/24, 15:18

CLARA: Informe de Auditoría

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 20: Reservado para uso futuro	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 21: Reservado para uso futuro	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 22: Reservado para uso futuro	No configurado	Deshabilitada	No configurado
Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM. PCR 23: Reservado para uso futuro	No configurado	Deshabilitada	No configurado

(*)Esta prueba solo se realiza en el caso de que el sistema de cifrado Bitlocker se encuentre configurado en el sistema. En caso contrario, deberá evaluar de forma manual el sistema de cifrado del equipo

Directivas de servicios del sistema (0%)		Ocultar
No hay datos relevantes que mostrar en esta sección.		

0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74