

AUDITORÍAS

LYNIS (LINUX/UBUNTU)

-Empezamos actualizando los repositorios de nuestro sistema.

```
aaron@aaron-VirtualBox:~$ sudo apt update
Obj:1 http://archive.ubuntu.com/ubuntu noble InRelease
Obj:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 81 paquetes. Ejecute «apt list --upgradable» para verlos.
aaron@aaron-VirtualBox:~$
```

-Descargamos el paquete git con el comando “sudo apt-get install git” para poder descargar el programa.

```
aaron@aaron-VirtualBox:~$ sudo apt-get install git
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
git ya está en su versión más reciente (1:2.43.0-1ubuntu7.1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 81 no actualizados.
aaron@aaron-VirtualBox:~$
```

-Descargamos la aplicación desde github.

```
aaron@aaron-VirtualBox:~$ git clone https://github.com/CISOfy/lynis
Clonando en 'lynis'...
remote: Enumerating objects: 15662, done.
remote: Counting objects: 100% (1050/1050), done.
remote: Compressing objects: 100% (444/444), done.
remote: Total 15662 (delta 729), reused 861 (delta 604), pack-reused 14612 (from 1)
Recibiendo objetos: 100% (15662/15662), 8.26 MiB | 1.76 MiB/s, listo.
Resolviendo deltas: 100% (11508/11508), listo.
aaron@aaron-VirtualBox:~$
```

-Con el comando “./lynis audit system -Q”, se realiza una auditoría a nuestro sistema.

```
aaron@aaron-VirtualBox: ~/lynis
aaron@aaron-VirtualBox:~/lynis$ ./lynis audit system -Q

[ Lynis 3.1.3 ]

#####
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.

2007-2024, CISofy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
#####

[+] Initializing program
-----

#####
#                                     #
#   NON-PRIVILEGED SCAN MODE         #
#                                     #
#####

NOTES:
-----
* Some tests will be skipped (as they require root permissions)
* Some tests might fail silently or give different results

- Detecting OS... [ DONE ]
- Checking profiles... [ DONE ]
```

- Pasamos la auditoría resultante a un fichero “.txt”.

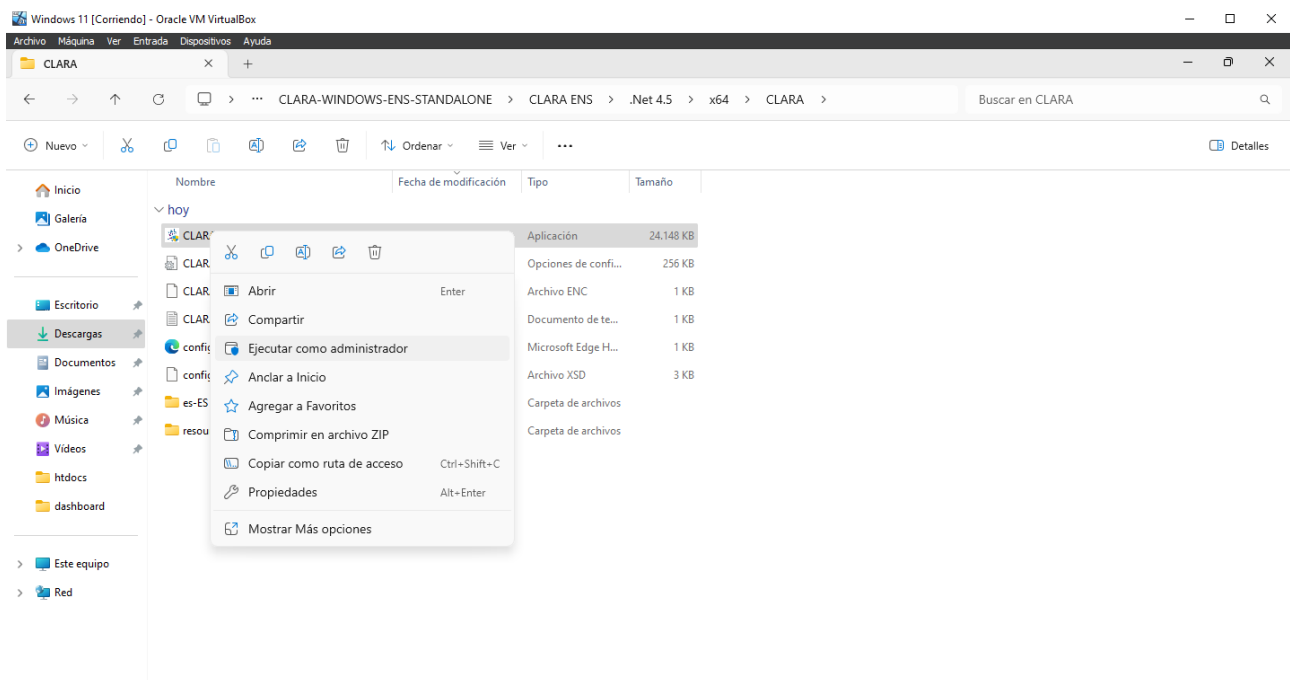
```
aaron@aaron-VirtualBox:~/lynis$ ./lynis audit system -Q >> auditoria.txt
aaron@aaron-VirtualBox:~/lynis$ ls
auditoria.txt      CONTRIBUTING.md  default.prf      FAQ              INSTALL          lynis.8          README.md
CHANGELOG.md      CONTRIBUTORS.md  developer.prf    HAPPY_USERS.md  LICENSE          plugins          SECURITY.md
CODE_OF_CONDUCT.md db              extras           include          lynis            README          TODO.md
aaron@aaron-VirtualBox:~/lynis$ cat auditoria.txt
```

CLARA (WINDOWS)

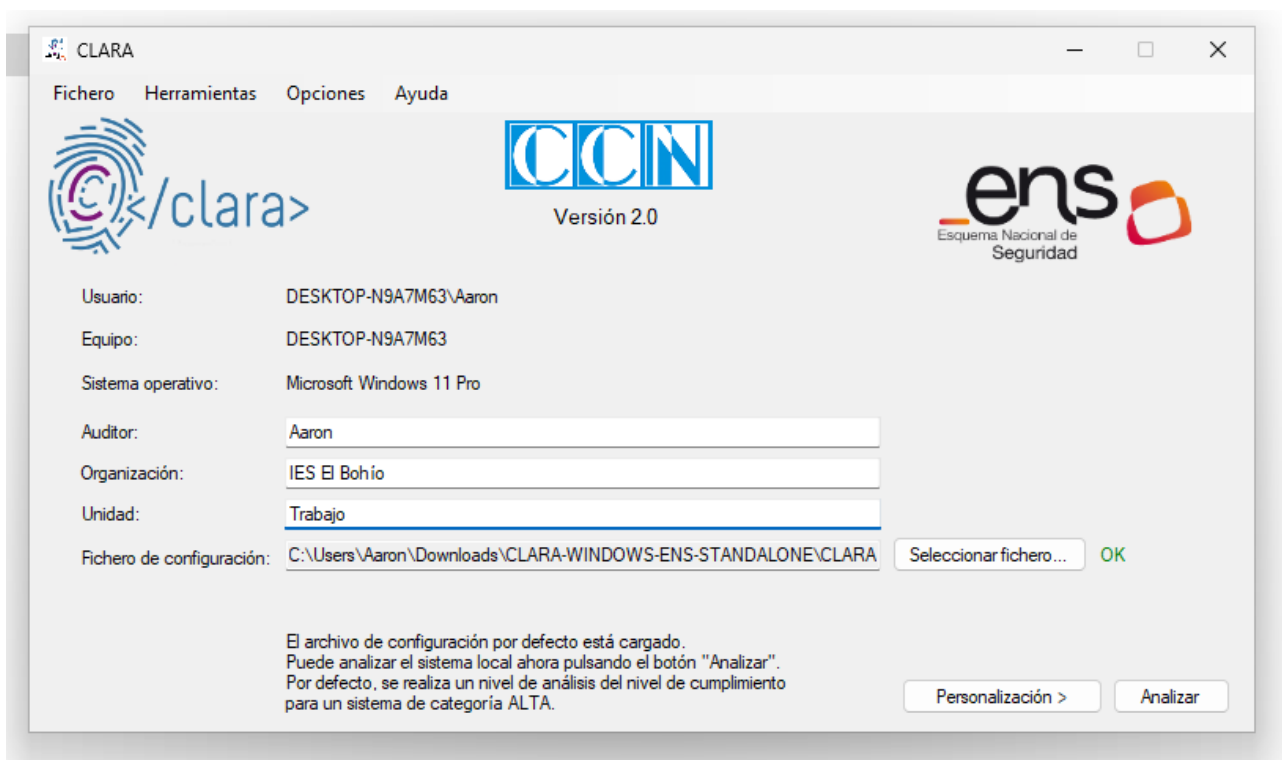
-Descargamos la aplicación de clara desde su página oficial.



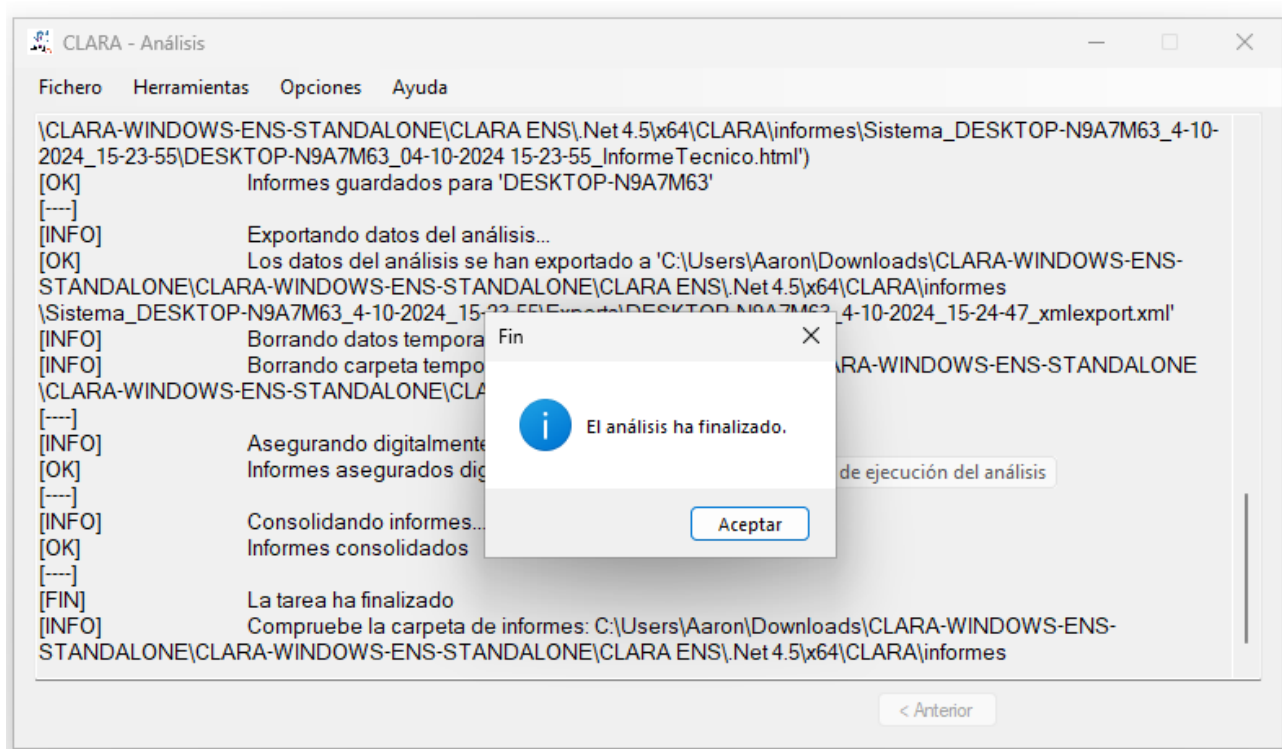
- Cuando se termine la descarga iniciamos el programa en modo administrador.



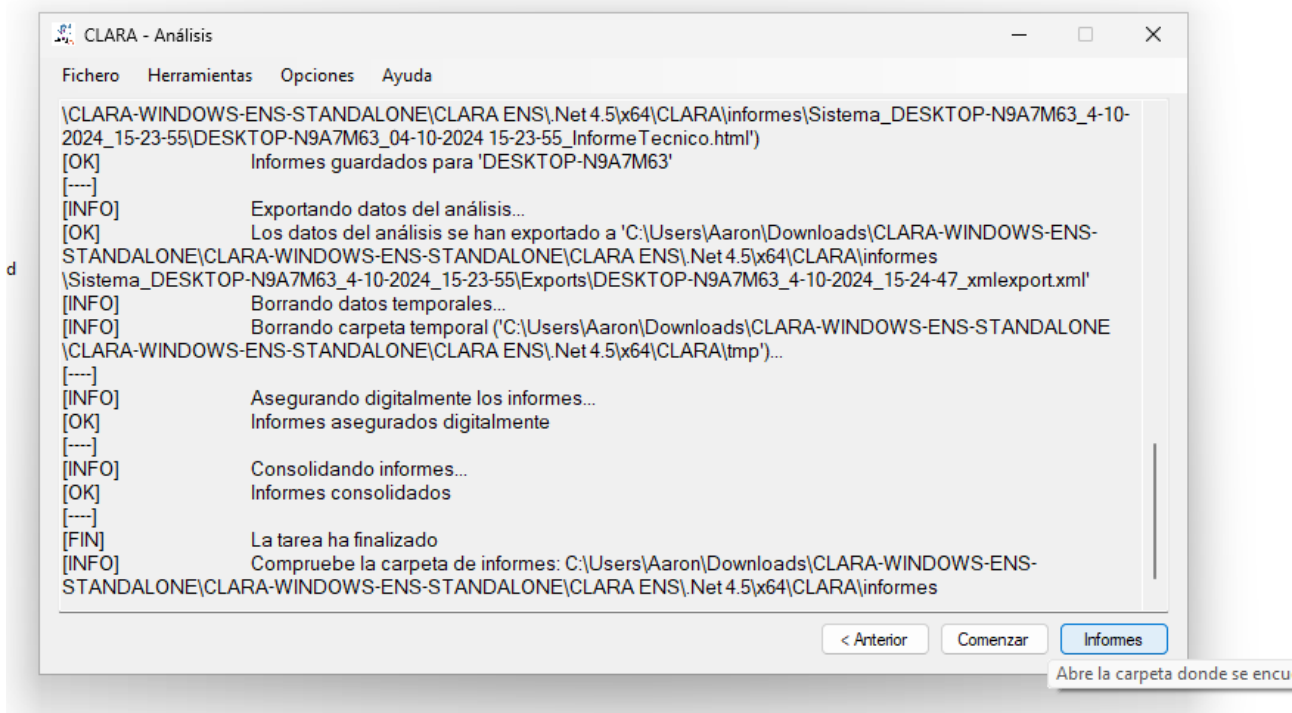
-Al abrir la aplicación se mostrará la siguiente interfaz gráfica, aquí tenemos que indicar el auditor, organización y unidad para poder realizar la auditoría. Teniendo esos datos puestos damos click en “Analizar” e iniciará la auditoría inmediatamente.



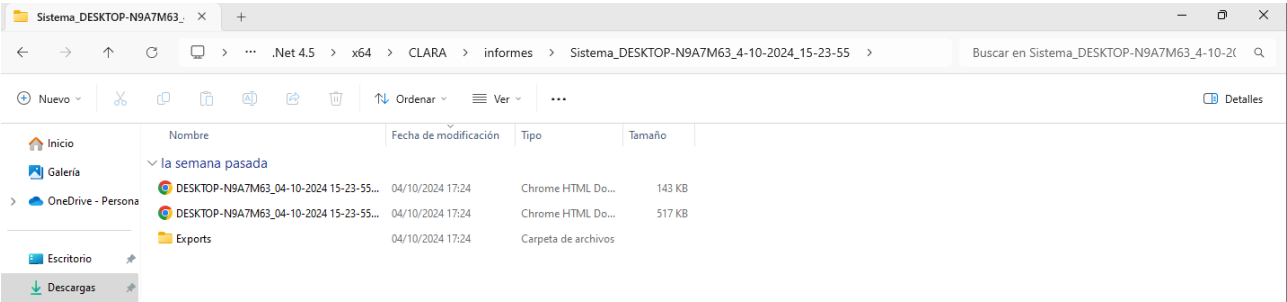
-Esperamos hasta que salga el mensaje de “El análisis ha finalizado” y aceptamos.



-Seleccionamos la opción de Informes y se abrirá una carpeta donde se encontrarán las auditorías realizadas.



- En este caso la auditoría se guarda en “C:\Users\Nombre_Usuario\Downloads\CLARA-WINDOWS-ENS-STANDALONE\CLARA-WINDOWS-ENS-STANDALONE\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-N9A7M63_4-10-2024_15-23-”.




- Abrimos la que mas tamaño ocupa, para que la auditoria esté completa.

Centro Criptológico Nacional

Nombre del sistema: DESKTOP-N9A7M63
Organización: IES El Bohío
Unidad: Trabajo
Categoría del sistema: ALTA

Auditado por Aaron
Informes generados el día 04/10/2024 15:23:55 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99a5-1647218f2953-09504d03-81c9-4dd8-a235-3b5bdc3239e1-2f74



centro criptológico nacional


Mostrar todo

Datos del sistema Ocultar

Valor de criticidad

NESSUS(WINDOWS/LINUX)

-Descargamos la aplicación de Nessus desde la página de tenable.



Downloads

Login

Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version
Nessus - 10.8.3

Platform
Windows - x86_64

[Download](#) Checksum

[Download by curl](#)

[Docker](#)

[Virtual Machines](#)

Summary

Release Date: Sep 11, 2024

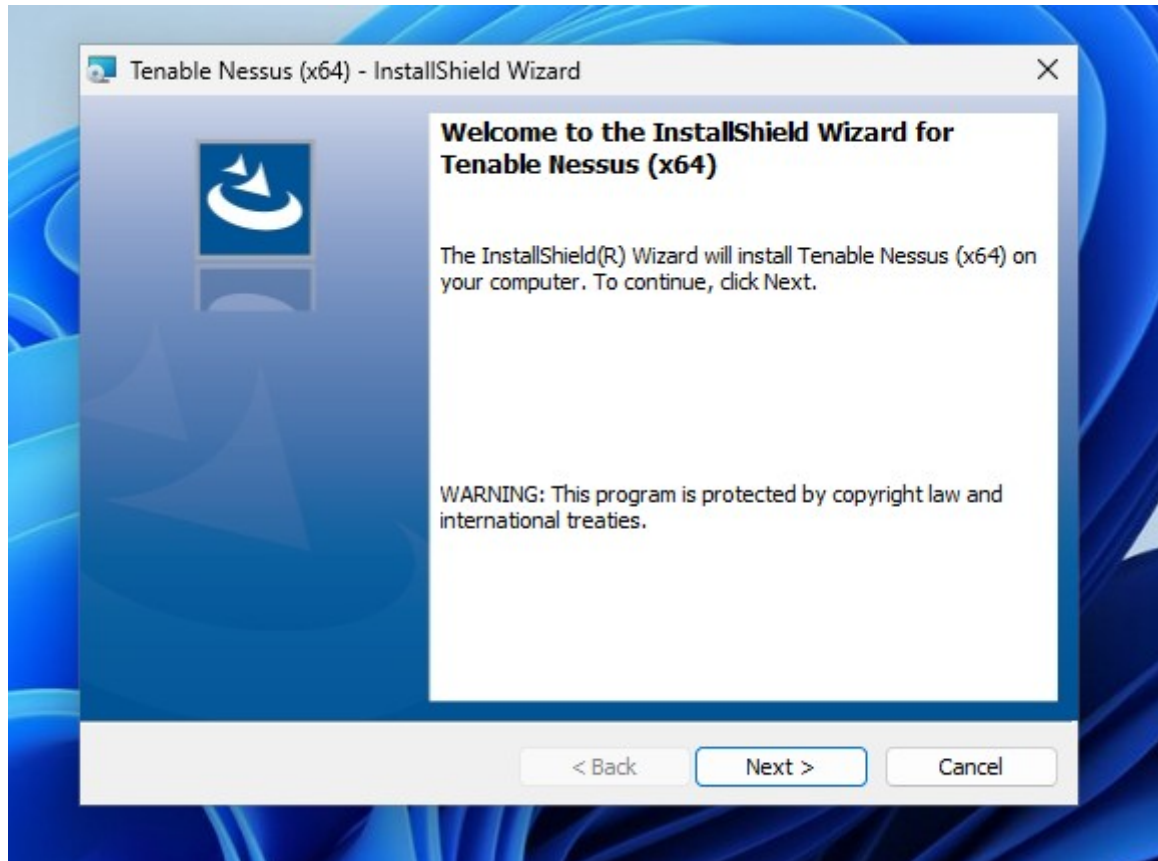
Release Notes:
[Tenable Nessus 10.8.3 Release Notes](#)

Signing Keys:
[RPM-GPG-KEY-Tenable-4096 \(10.4 & above\)](#)
[RPM-GPG-KEY-Tenable-2048 \(10.3 & below\)](#)

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

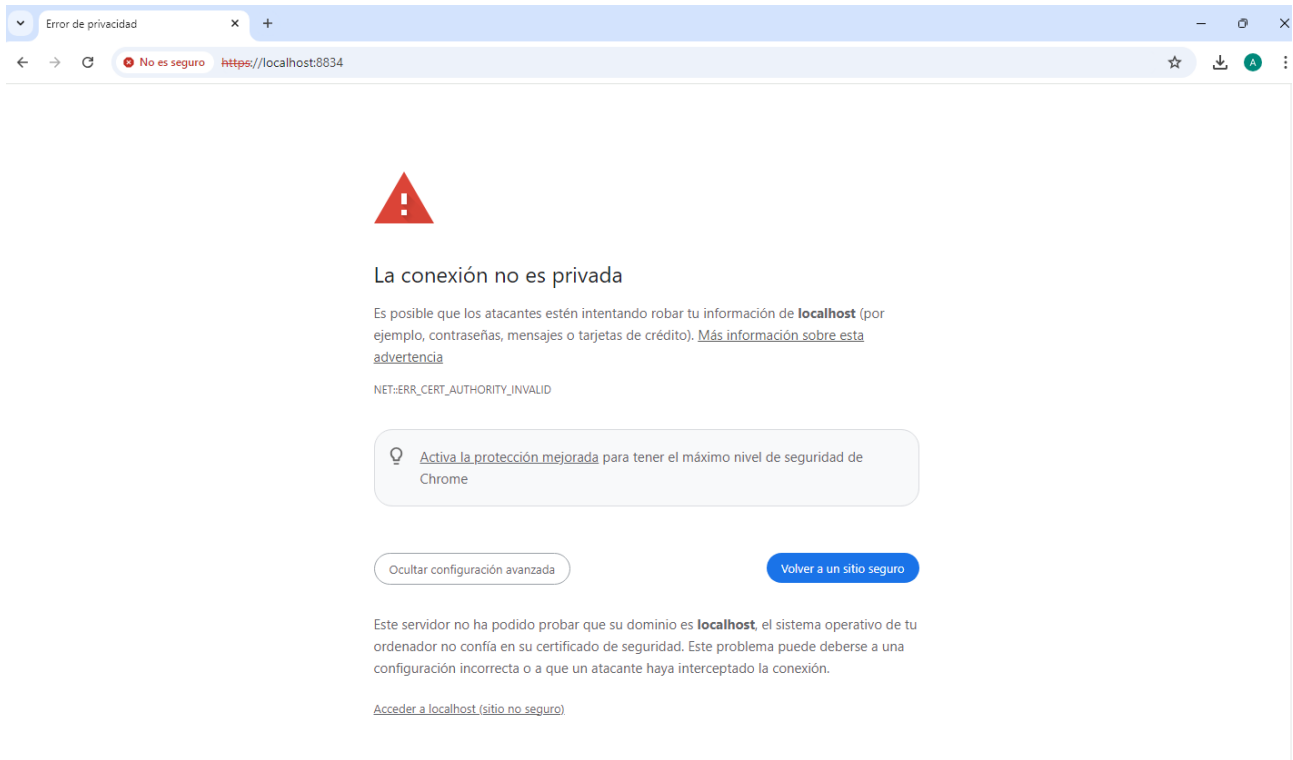
-Después de descargar la aplicación, iniciamos la instalación.



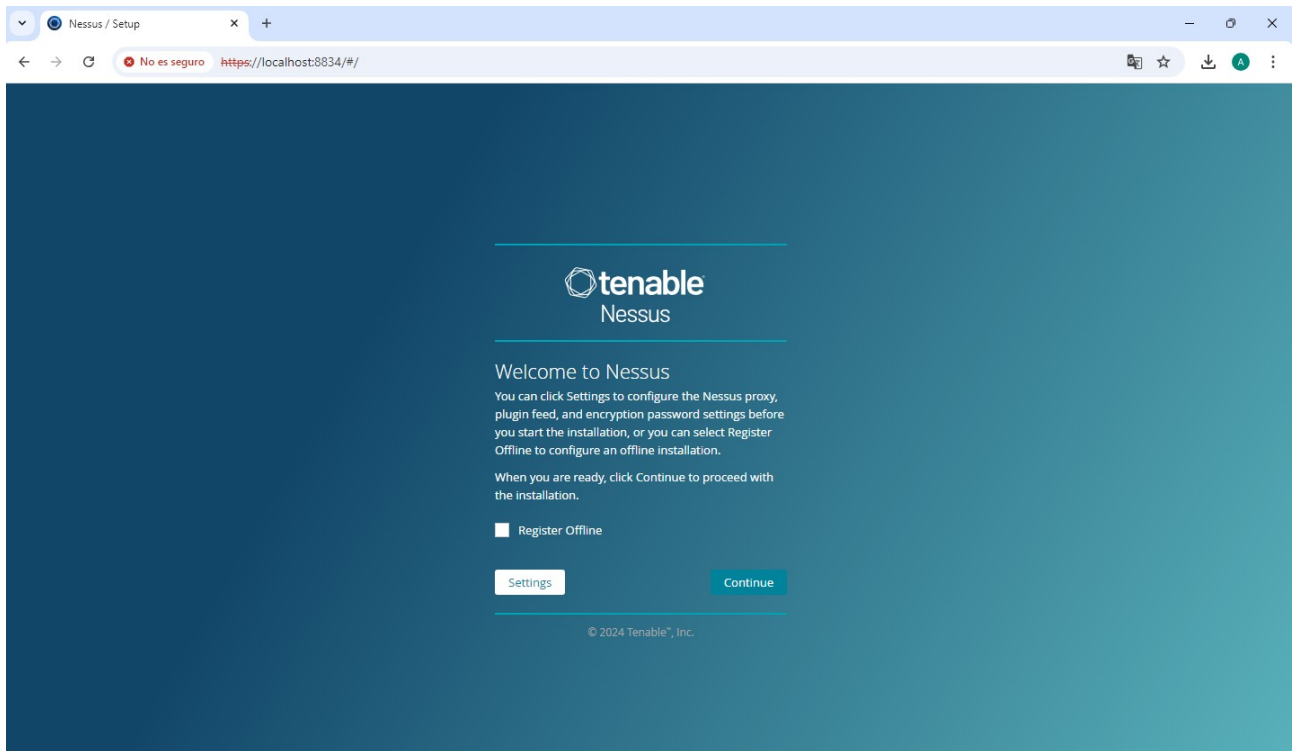
-Esperamos hasta que termine, nos abrirá el navegador web y hacemos click en “Connect via SSL”.



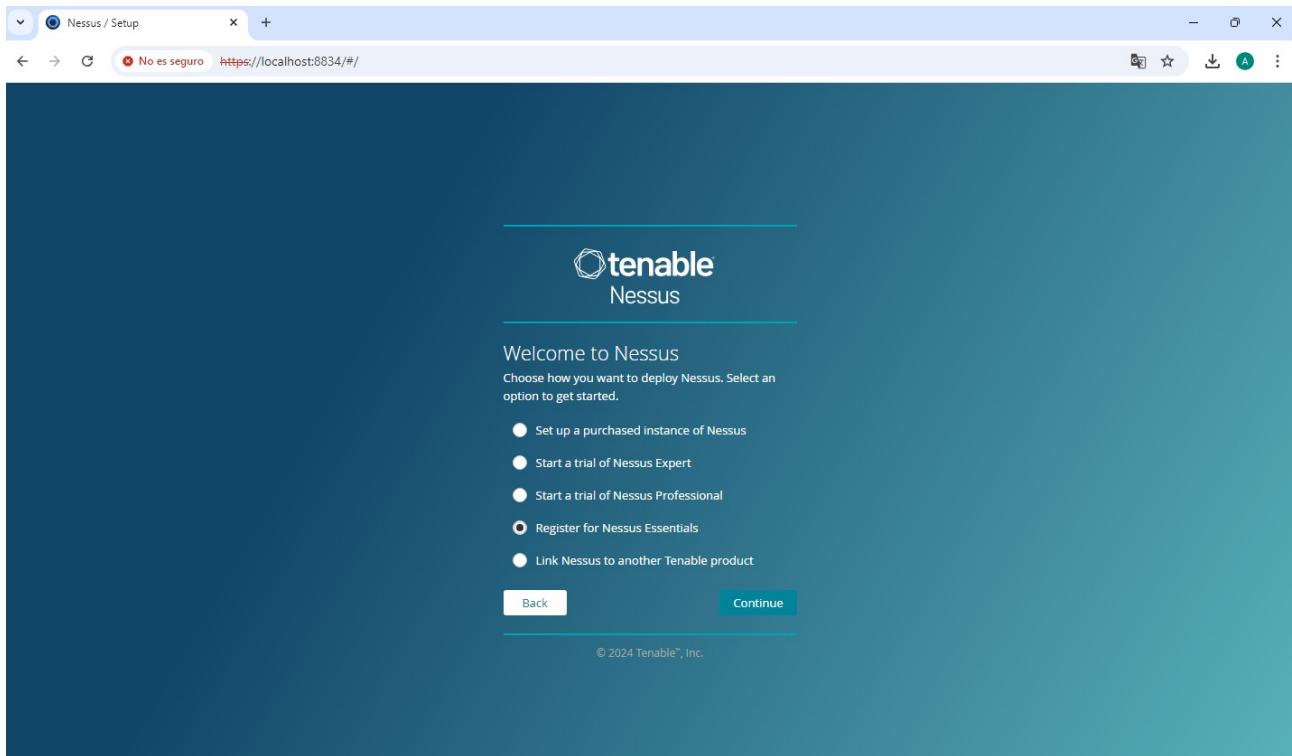
-Nos indicará que la conexión no es privada, igualmente aceptamos acceder al localhost.



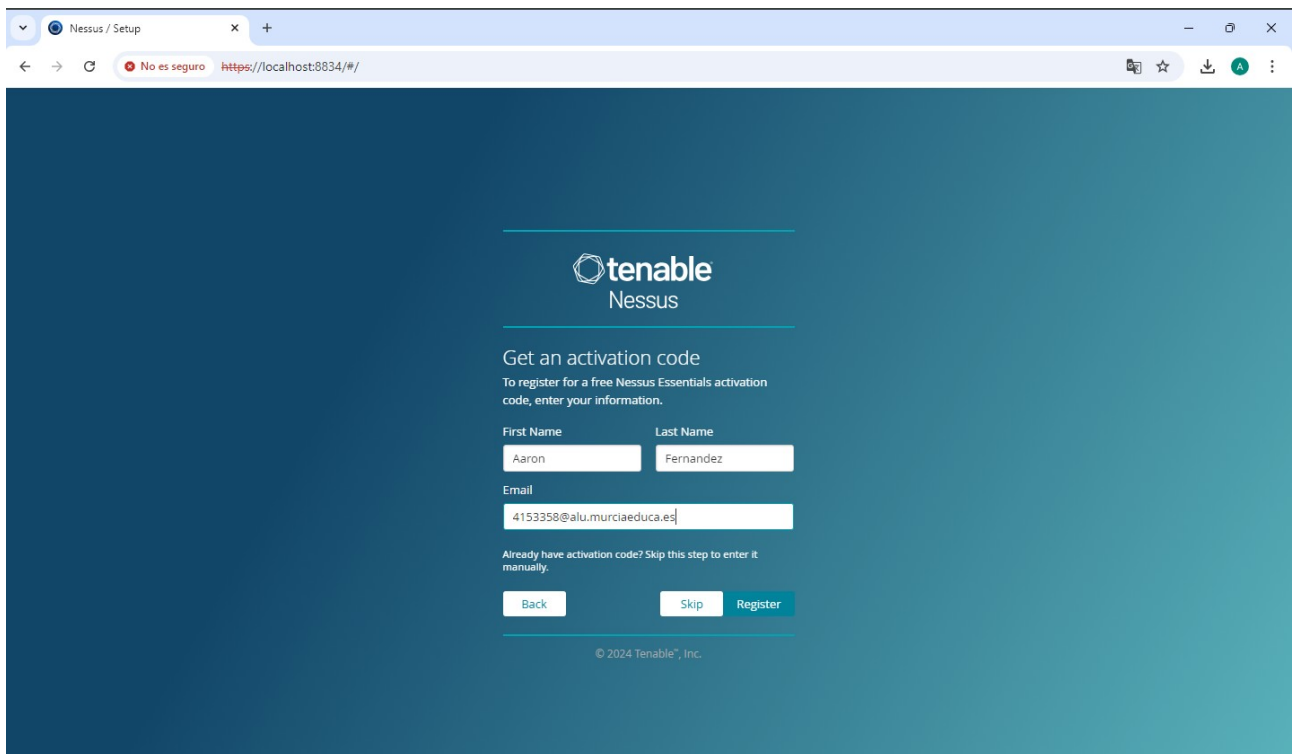
-Hacemos click en “Continue” para acceder a Nessus.



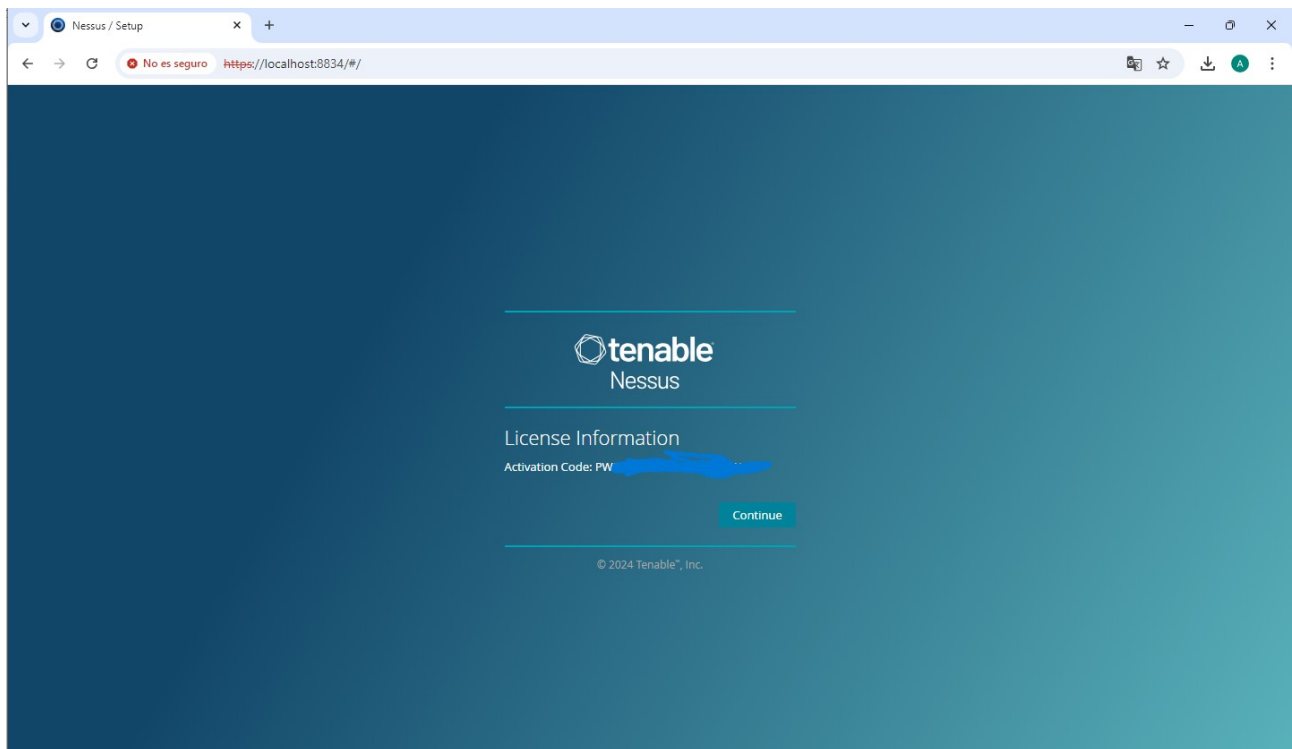
- Cambiamos la opción por defecto y seleccionamos la de “Register for Nessus Essentials”.



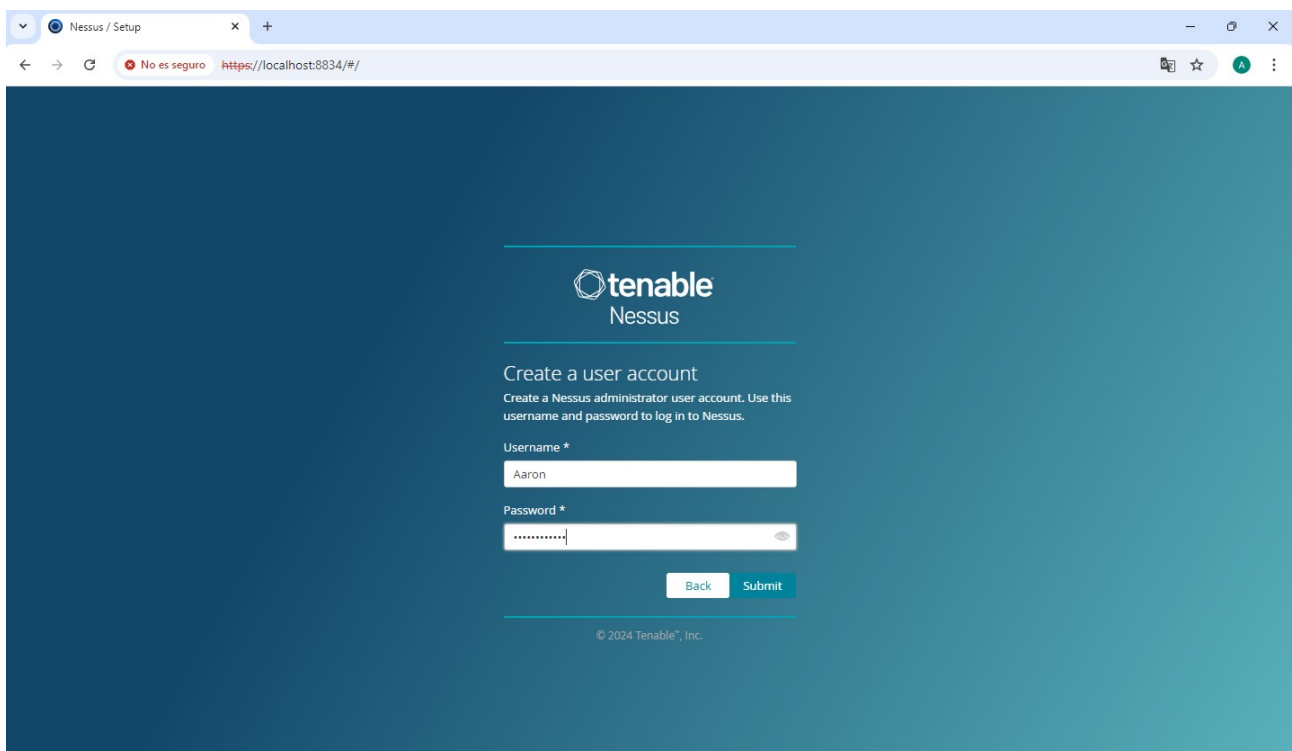
-Ahora debemos crear una cuenta para poder acceder.



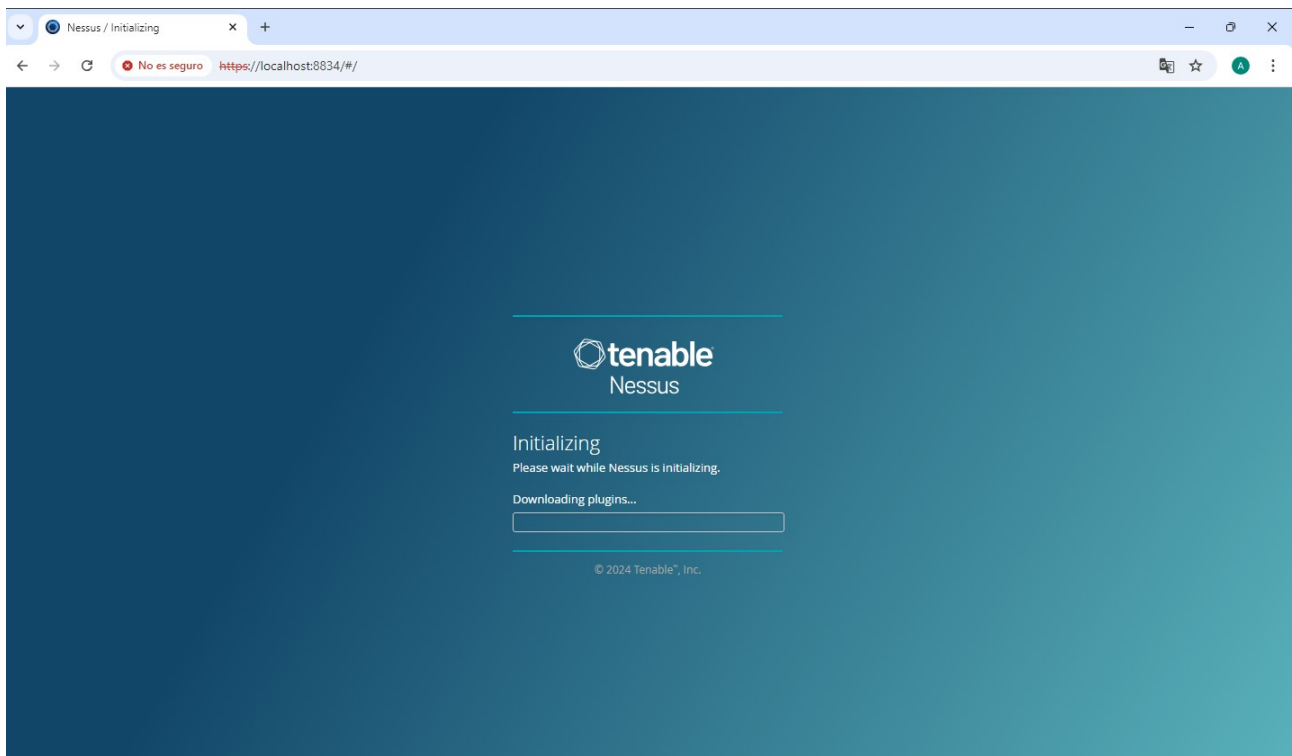
- Al crear el usuario nos dirá una clave de activación para poder confirmar la cuenta recién creada.



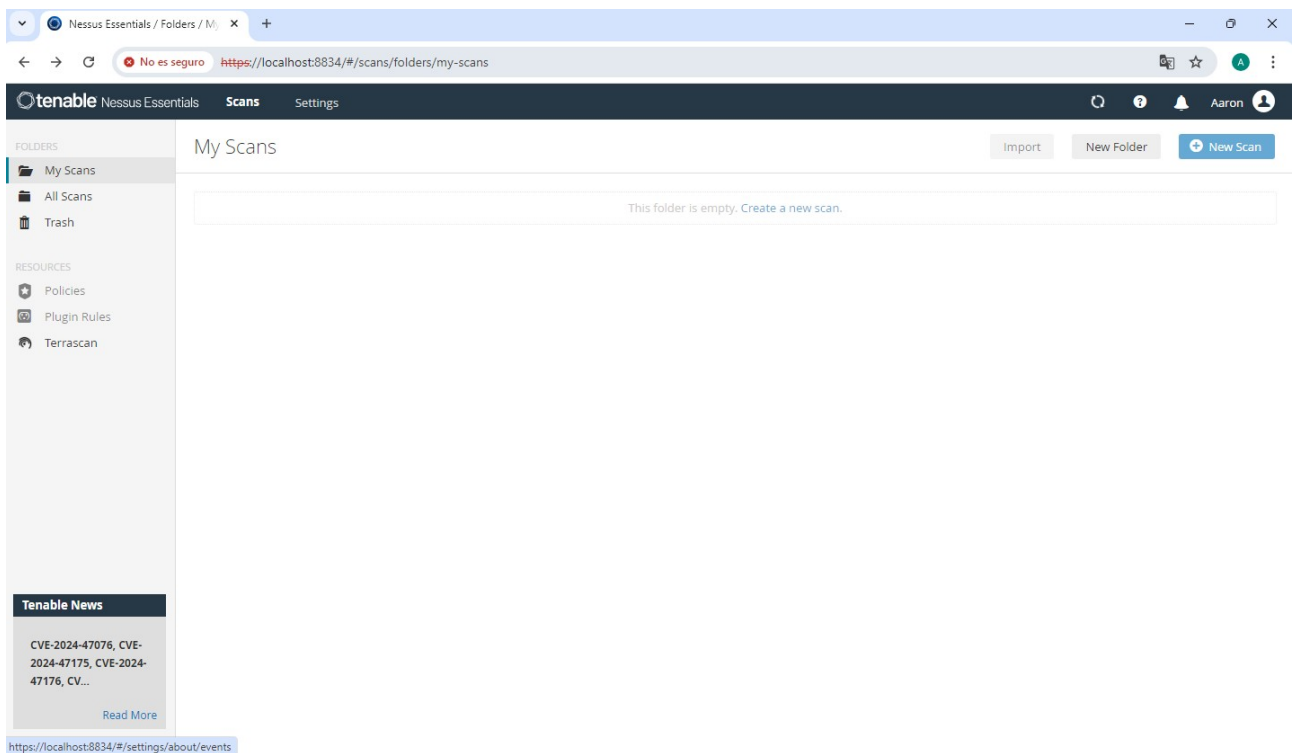
-Después iniciamos sesión con el usuario que hemos creado.



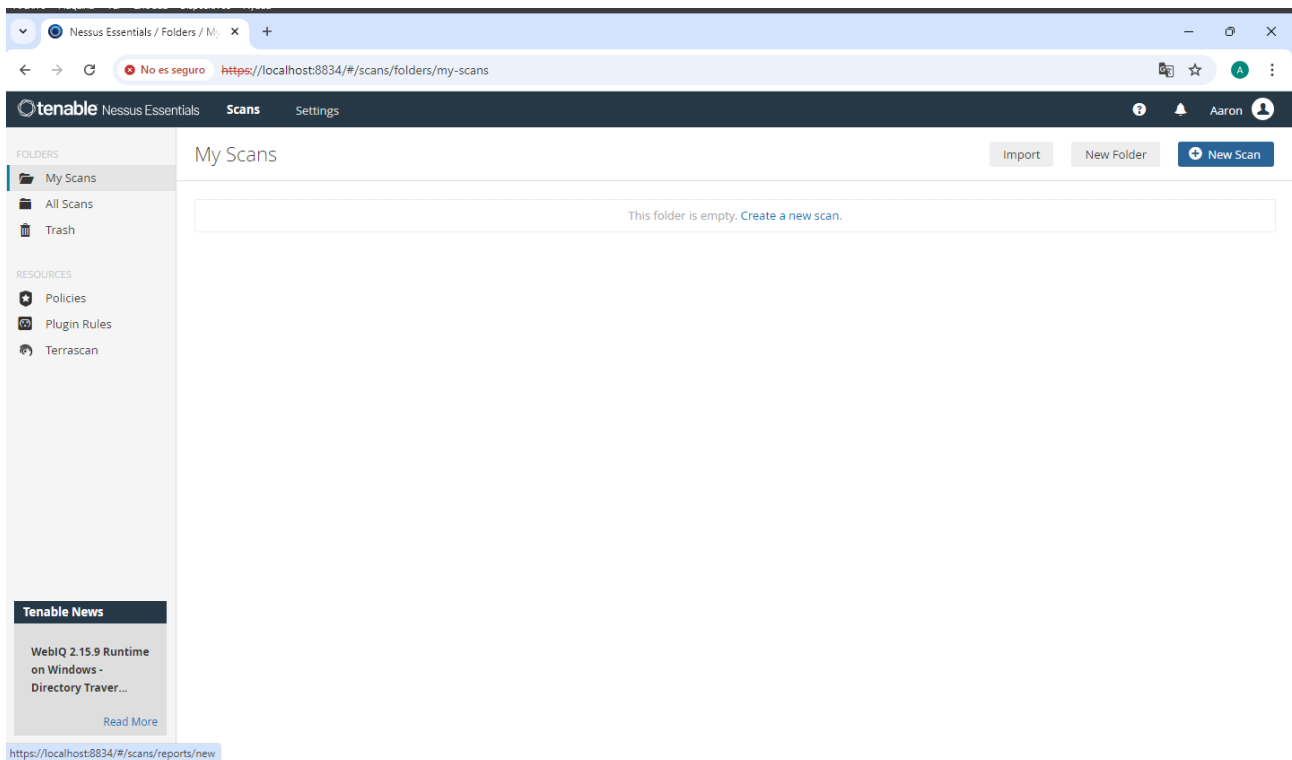
-Al iniciar sesión se empezará a descargar paquetes y plugins necesarios para poder usar Nessus.



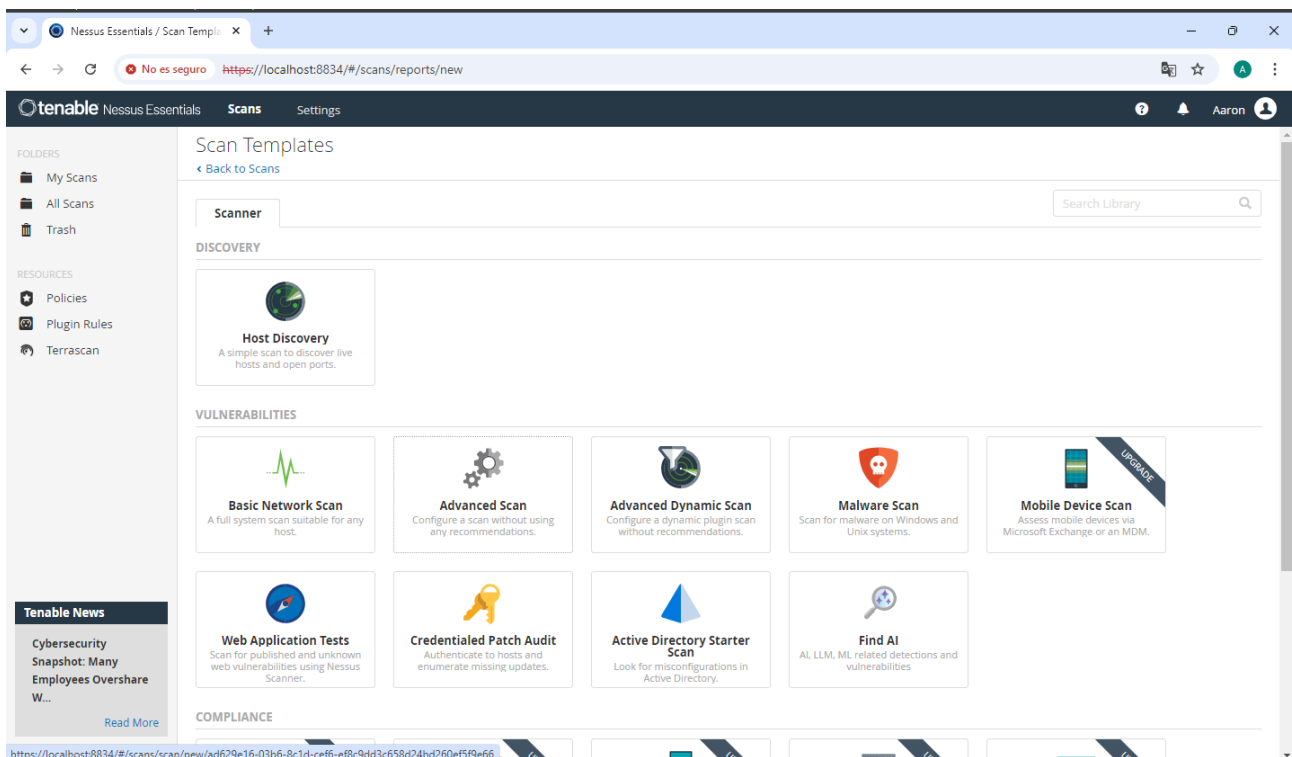
-Después de descargar los anteriores plugins seguirá descargando plugins adicionales.



-Al terminar de descargar todos los plugins creamos un perfil para poder hacer el escaneo, para ello hacemos click en "New Scan".



- Nos mostrarán los escaneos disponibles que tiene Nessus, en mi caso he realizado un “Advanced Scan”.



-Ahora debemos indicar:

- Nombre, nombre que queremos poner al escaneo.
- Descripción, una descripción para indicar el funcionamiento del escaneo.
- Folder, la carpeta donde se guarda el perfil de escaneo que creemos.
- Targets, aquí se puede poner un rango de IP's o nuestra propia IP, en mi caso lo he realizado con mi propia IP.

The screenshot shows the 'New Scan / Advanced Scan' configuration page in Tenable Nessus Essentials. The 'Settings' tab is selected, and the 'General' sub-tab is active. The configuration fields are as follows:

Field	Value
Name	ESCANER
Description	Escaner avanzado
Folder	My Scans
Targets	10.0.2.15

At the bottom, there is a 'Save' button and a 'Cancel' button. The left sidebar shows the 'My Scans' folder selected under 'FOLDERS'.

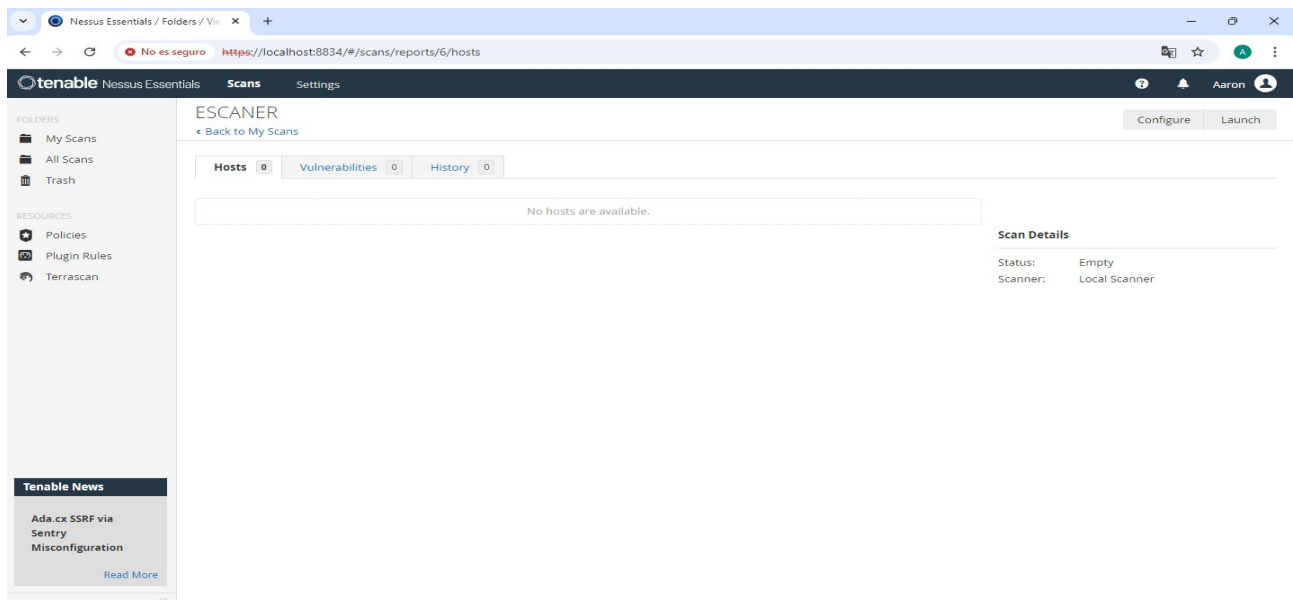
-Vemos que se ha creado nuestro perfil de escaneo correctamente, para acceder a él haremos click.

The screenshot shows the 'My Scans' page in Tenable Nessus Essentials. The table below lists the scans:

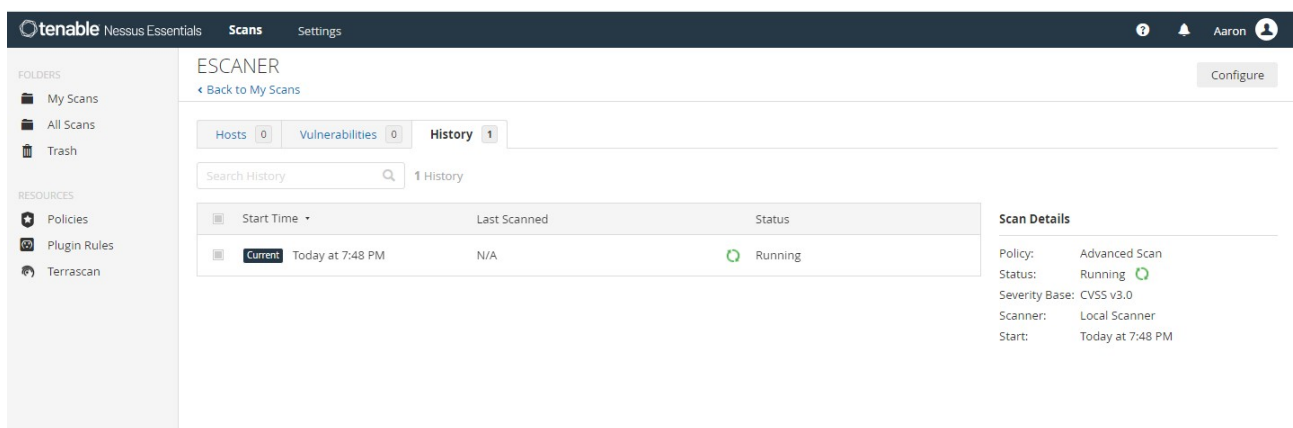
Name	Scan Type	Schedule	Last Scanned
ESCANER	Vulnerability	On Demand	N/A

The table has a search bar at the top with the text 'Search Scans' and a '1 Scan' indicator. The left sidebar shows the 'My Scans' folder selected under 'FOLDERS'.

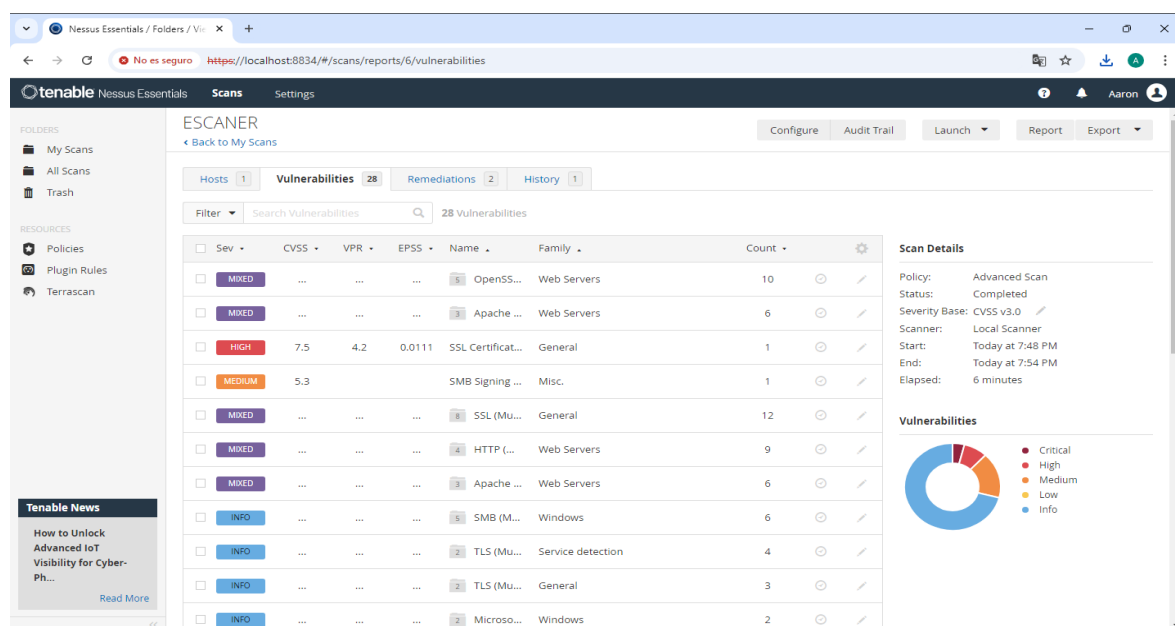
-Para iniciar dicho escaneo hacemos click en la opción de “Launch”.



-Podemos ver que el escaneo ha empezado correctamente.



-Cuando el escaneo haya terminado se mostrará el resultado de la siguiente manera.



INFORME LYNIS

[Lynis 3.1.3]

[Lynis 3.1.3]

#####

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.

2007-2024, CISOfy - <https://cisofy.com/lynis/>

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

#####

[+] Initializing program

#####

#

NON-PRIVILEGED SCAN MODE

#

#####

NOTES:

* Some tests will be skipped (as they require root permissions)

* Some tests might fail silently or give different results

- Detecting OS... [DONE]

- Checking profiles... [DONE]

- Detecting language and localization [es]

Translation file (db/languages/es) needs an update [OUTDATED]

=====

Help other users and translate the missing lines:

1) Go to: <https://github.com/CISOfy/lynis/edit/master/db/languages/es>

2) Translate (some of) the lines starting with a hash (#) and remove the leading hash

3) Commit the changes

Thank you!

Note: no lines with a hash? Look if the file recently has been changed by another translator.

=====

Program version: 3.1.3

Operating system: Linux

Operating system name: Ubuntu

Operating system version: 24.04

Kernel version: 6.8.0

Hardware platform: x86_64

Hostname: aaron-VirtualBox

Profiles: /home/aaron/lynis/default.prf

Log file: /home/aaron/lynis.log

Report file: /home/aaron/lynis-report.dat

Report version: 1.0

Plugin directory: ./plugins

Auditor: [Not Specified]

Language: es

Test category: all

Test group: all

- Program update status... [SIN ACTUALIZACIÓN]

[+] Herramientas del sistema

- Scanning available tools...

- Checking system binaries...

[+] Plugins (fase 1)

Nota: los plugins contienen pruebas más extensivas y toman más tiempo

- Plugin: pam

[..]

- Plugin: systemd

[.....]

[+] Arranque y servicios

- Service Manager [systemd]

- Checking presence GRUB2 [ENCONTRADO]

- Checking for password protection [NINGUNO]

- Check running services (systemctl) [HECHO]

Result: found 29 running services

- Check enabled services at boot (systemctl) [HECHO]

Result: found 55 enabled services

- Check startup files (permissions) [OK]

- Running 'systemd-analyze security'

- ModemManager.service: [MEDIO]

- NetworkManager.service: [EXPUESTO]

- accounts-daemon.service: [MEDIO]

- alsa-state.service: [INSEGURO]

- anacron.service: [INSEGURO]

- avahi-daemon.service: [INSEGURO]

- colord.service: [PROTEGIDO]

- cron.service: [INSEGURO]

- cups-browsed.service: [INSEGURO]

- cups.service: [INSEGURO]

- dbus.service: [INSEGURO]

- dmesg.service: [INSEGURO]

- emergency.service: [INSEGURO]

- gdm.service: [INSEGURO]

- getty@tty1.service: [INSEGURO]

- gnome-remote-desktop.service: [INSEGURO]

- kerneloops.service: [INSEGURO]

- networkd-dispatcher.service: [INSEGURO]

- plymouth-start.service: [INSEGURO]

- polkit.service: [PROTEGIDO]

- power-profiles-daemon.service: [MEDIO]

- rc-local.service: [INSEGURO]

- rescue.service: [INSEGURO]

- rsyslog.service: [MEDIO]

- rtkit-daemon.service: [MEDIO]
- snapd.service: [INSEGURO]
- sssd-autofs.service: [INSEGURO]
- sssd-nss.service: [INSEGURO]
- sssd-pac.service: [INSEGURO]
- sssd-pam.service: [INSEGURO]
- sssd-ssh.service: [INSEGURO]
- sssd-sudo.service: [INSEGURO]
- sssd.service: [EXPUESTO]
- switcheroo-control.service: [EXPUESTO]
- systemd-ask-password-console.service: [INSEGURO]
- systemd-ask-password-plymouth.service: [INSEGURO]
- systemd-ask-password-wall.service: [INSEGURO]
- systemd-bsod.service: [INSEGURO]
- systemd-fsckd.service: [INSEGURO]
- systemd-initctl.service: [INSEGURO]
- systemd-journald.service: [PROTEGIDO]
- systemd-logind.service: [PROTEGIDO]
- systemd-networkd.service: [PROTEGIDO]
- systemd-oomd.service: [PROTEGIDO]
- systemd-resolved.service: [PROTEGIDO]
- systemd-rfkill.service: [INSEGURO]
- systemd-timesyncd.service: [PROTEGIDO]
- systemd-udev.service: [MEDIO]
- thermal.service: [INSEGURO]
- tpm-udev.service: [INSEGURO]
- ubuntu-advantage.service: [INSEGURO]
- udisks2.service: [INSEGURO]
- unattended-upgrades.service: [INSEGURO]
- upower.service: [PROTEGIDO]
- user@1000.service: [INSEGURO]
- uidd.service: [MEDIO]
- whoopsie.service: [INSEGURO]
- wpa_supplicant.service: [INSEGURO]

[+] Kernel

- Checking default runlevel [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 68 active modules

- Checking Linux kernel configuration file [ENCONTRADO]
- Checking default I/O kernel scheduler [NO ENCONTRADO]
- Checking for available kernel update [OK]
- Checking core dumps configuration
- configuration in systemd conf files [POR DEFECTO]
- configuration in /etc/profile [POR DEFECTO]
- 'hard' configuration in /etc/security/limits.conf [POR DEFECTO]
- 'soft' configuration in /etc/security/limits.conf [POR DEFECTO]
- Checking setuid core dumps configuration [PROTEGIDO]

- Check if reboot is needed [NO]

[+] Memoria y procesos

- Checking /proc/meminfo [ENCONTRADO]
- Searching for dead/zombie processes [NO ENCONTRADO]
- Searching for IO waiting processes [NO ENCONTRADO]
- Search prelink tooling [NO ENCONTRADO]

[+] Usuarios, grupos y autenticación

- Administrator accounts [OK]
- Unique UIDs [OK]
- Unique group IDs [OK]
- Unique group names [OK]
- Password file consistency [SUGERENCIA]
- Checking password hashing rounds [DESHABILITADO]
- Query system users (non daemons) [HECHO]
- NIS+ authentication support [NO HABILITADO]
- NIS authentication support [NO HABILITADO]
- Sudoers file(s) [ENCONTRADO]
- PAM password strength tools [OK]
- 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]
- Locked accounts [OK]
- Checking user password aging (minimum) [DESHABILITADO]
- User password aging (maximum) [DESHABILITADO]
- Checking Linux single user mode authentication [OK]
- Determining default umask
- umask (/etc/profile) [NO ENCONTRADO]
- umask (/etc/login.defs) [SUGERENCIA]
- LDAP authentication support [NO HABILITADO]
- Logging failed login attempts [HABILITADO]

[+] Kerberos

- Check for Kerberos KDC and principals [NO ENCONTRADO]

[+] Shells

- Checking shells from /etc/shells
- Result: found 7 shells (valid shells: 7).
- Session timeout settings/tools [NINGUNO]
 - Checking default umask values
 - Checking default umask in /etc/bash.bashrc [NINGUNO]
 - Checking default umask in /etc/profile [NINGUNO]

[+] Sistemas de ficheros

- 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]
- Mount options of / [OK]
- Mount options of /dev [PARCIALMENTE BASTIONADO]
- Mount options of /dev/shm [PARCIALMENTE BASTIONADO]
- Mount options of /run [BASTIONADO]
- Total without nodev:6 noexec:21 nosuid:15 ro or noexec (W^X): 10 of total 37
- JBD driver is not loaded [NECESITA VERIFICACIÓN]
- Disable kernel support of some filesystems

[+] Dispositivos USB

-
- Checking usb-storage driver (modprobe config) [NO DESHABILITADO]
 - Checking USB devices authorization [HABILITADO]
 - Checking USBGuard [NO ENCONTRADO]

[+] Almacenamiento

-
- Checking firewire ohci driver (modprobe config) [DESHABILITADO]

[+] NFS

-
- Check running NFS daemon [NO ENCONTRADO]

[+] Servicios de nombres

-
- Checking search domains [ENCONTRADO]
 - Checking /etc/resolv.conf options [ENCONTRADO]
 - Searching DNS domain name [DESCONOCIDO]
 - Checking /etc/hosts
 - Duplicate entries in hosts file [NINGUNO]
 - Presence of configured hostname in /etc/hosts [ENCONTRADO]
 - Hostname mapped to localhost [NO ENCONTRADO]
 - Localhost mapping to IP address [OK]

[+] Puertos y paquetes

-
- Searching package managers
 - Searching dpkg package manager [ENCONTRADO]
 - Querying package manager
 - Query unpurged packages [NINGUNO]
 - Checking security repository in sources.list.d directory [OK]
 - Checking upgradeable packages [OMITIDO]
 - Checking package audit tool [NINGUNO]
 - Toolkit for automatic upgrades (unattended-upgrade) [ENCONTRADO]

[+] Conectividad

-
- Checking IPv6 configuration [HABILITADO]
- Configuration method [AUTO]
- IPv6 only [NO]
- Checking configured nameservers
 - Testing nameservers
- Nameserver: 127.0.0.53 [OK]

- DNSSEC supported (systemd-resolved) [DESCONOCIDO]
- Getting listening ports (TCP/UDP) [HECHO]
- Checking promiscuous interfaces [OK]
- Checking status DHCP client [NOT ACTIVE]
- Checking for ARP monitoring software [NO ENCONTRADO]
- Uncommon network protocols [0]

[+] Impresoras y spools

- Checking cups daemon [CORRIENDO]
- Checking CUPS configuration file [OK]
- File permissions [PELIGRO]
- Checking CUPS addresses/sockets [ENCONTRADO]
- Checking lp daemon [NO ESTÁ CORRIENDO]

[+] Software: correo electrónico y mensajería

[+] Software: firewalls

- Checking iptables kernel module [ENCONTRADO]
- Checking host based firewall [ACTIVO]

[+] Software: servidor web

- Checking Apache [NO ENCONTRADO]
- Checking nginx [NO ENCONTRADO]

[+] Soporte SSH

- Checking running SSH daemon [NO ENCONTRADO]

[+] Soporte SNMP

- Checking running SNMP daemon [NO ENCONTRADO]

[+] Bases de datos

No database engines found

[+] Servicios LDAP

- Checking OpenLDAP instance [NO ENCONTRADO]

[+] PHP

- Checking PHP [NO ENCONTRADO]

[+] Soporte Squid

- Checking running Squid daemon [NO ENCONTRADO]

[+] Logging y ficheros

- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NO ENCONTRADO]
- Checking systemd journal status [ENCONTRADO]
- Checking Metalog status [NO ENCONTRADO]
- Checking RSyslog status [ENCONTRADO]
- Checking RFC 3195 daemon status [NO ENCONTRADO]
- Checking minilogd instances [NO ENCONTRADO]
- Checking wazuh-agent daemon status [NO ENCONTRADO]
- Checking logrotate presence [OK]

- Checking remote logging [NO HABILITADO]
- Checking log directories (static list) [HECHO]
- Checking open log files [HECHO]
- Checking deleted files in use [ARCHIVOS ENCONTRADOS]

[+] Servicios inseguros

-
- Installed inetd package [NO ENCONTRADO]
 - Installed xinetd package [OK]
 - xinetd status [NOT ACTIVE]
 - Installed rsh client package [OK]
 - Installed rsh server package [OK]
 - Installed telnet client package [OK]
 - Installed telnet server package [NO ENCONTRADO]
 - Checking NIS client installation [OK]
 - Checking NIS server installation [OK]
 - Checking TFTP client installation [OK]
 - Checking TFTP server installation [OK]

[+] Banners e identificación

-
- /etc/issue [ENCONTRADO]
 - /etc/issue contents [DÉBIL]
 - /etc/issue.net [ENCONTRADO]
 - /etc/issue.net contents [DÉBIL]

[+] Tareas programadas

-
- Checking crontab and cronjob files [HECHO]

[+] Contabilidad

-
- Checking accounting information [NO ENCONTRADO]
 - Checking sysstat accounting data [DESHABILITADO]
 - Checking auditd [NO ENCONTRADO]

[+] Tiempo y sincronización

-
- NTP daemon found: systemd (timesyncd) [ENCONTRADO]
 - Checking for a running NTP daemon or client [OK]
 - Last time synchronization [426s]

[+] Criptografía

-
- Checking for expired SSL certificates [0/151] [NINGUNO]
 - Kernel entropy is sufficient [SÍ]
 - HW RNG & rngd [NO]
 - SW prng [NO]
 - MOR variable not found [DÉBIL]

[+] Virtualización

[+] Contenedores

[+] Frameworks de seguridad

-
- Checking presence AppArmor [ENCONTRADO]
 - Checking AppArmor status [DESCONOCIDO]
 - Checking presence SELinux [NO ENCONTRADO]

- Checking presence TOMOYO Linux [NO ENCONTRADO]
- Checking presence grsecurity [NO ENCONTRADO]
- Checking for implemented MAC framework [NINGUNO]

[+] Software: integridad de ficheros

-
- Checking file integrity tools
 - Checking presence integrity tool [NO ENCONTRADO]

[+] Software: Herramientas del sistema

-
- Checking automation tooling
 - Automation tooling [NO ENCONTRADO]
 - Checking for IDS/IPS tooling [NINGUNO]

[+] Software: Malware

-
- Malware software components [NO ENCONTRADO]

[+] Permisos de ficheros

-
- Starting file permissions check
- File: /boot/grub/grub.cfg [OK]
- File: /etc/crontab [SUGERENCIA]
- File: /etc/group [OK]
- File: /etc/group- [OK]
- File: /etc/hosts.allow [OK]
- File: /etc/hosts.deny [OK]
- File: /etc/issue [OK]
- File: /etc/issue.net [OK]
- File: /etc/passwd [OK]
- File: /etc/passwd- [OK]
- Directory: /etc/cron.d [SUGERENCIA]
- Directory: /etc/cron.daily [SUGERENCIA]
- Directory: /etc/cron.hourly [SUGERENCIA]
- Directory: /etc/cron.weekly [SUGERENCIA]
- Directory: /etc/cron.monthly [SUGERENCIA]

[+] Directorios de inicio

-
- Permissions of home directories [OK]
 - Ownership of home directories [OK]
 - Checking shell history files [OK]

[+] Bastionado del kernel

-
- Comparing sysctl key pairs with scan profile
 - dev.tty.ldisc_autoload (exp: 0) [DIFERENTE]
 - fs.protected_fifos (exp: 2) [DIFERENTE]
 - fs.protected_hardlinks (exp: 1) [OK]
 - fs.protected_regular (exp: 2) [OK]
 - fs.protected_symlinks (exp: 1) [OK]
 - fs.suid_dumpable (exp: 0) [DIFERENTE]
 - kernel.core_uses_pid (exp: 1) [DIFERENTE]
 - kernel.ctrl-alt-del (exp: 0) [OK]
 - kernel.dmesg_restrict (exp: 1) [OK]
 - kernel.kptr_restrict (exp: 2) [DIFERENTE]
 - kernel.modules_disabled (exp: 1) [DIFERENTE]

- kernel.perf_event_paranoid (exp: 2 3 4) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFERENTE]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFERENTE]
- kernel.yama.ptrace_scope (exp: 1 2 3) [OK]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFERENTE]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFERENTE]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFERENTE]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]

[+] Bastionado

- Installed compiler(s) [NO ENCONTRADO]
- Installed malware scanner [NO ENCONTRADO]
- Non-native binary formats [ENCONTRADO]

[+] Pruebas personalizadas

- Running custom tests... [NINGUNO]

[+] Plugins (fase 2)

- Plugins (phase 2) [HECHO]

=====

-[Lynis 3.1.3 Results]-

Great, no warnings

Suggestions (35):

- * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

<https://cisofy.com/lynis/controls/BOOT-5122/>

- * Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service

<https://cisofy.com/lynis/controls/BOOT-5264/>

- * If not required, consider explicit disabling of core dump in /etc/security/limits.conf file

[KRNL#5820]

<https://cisofy.com/lynis/controls/KRNL-5820/>

- * Run pwck manually and correct any errors in the password file [AUTH-9228]

<https://cisofy.com/lynis/controls/AUTH-9228/>

- * Configure password hashing rounds in /etc/login.defs [AUTH-9230]

<https://cisofy.com/lynis/controls/AUTH-9230/>

- * Configure minimum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

- * Configure maximum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

- * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

<https://cisofy.com/lynis/controls/AUTH-9328/>

- * To decrease the impact of a full /home file system, place /home on a separate partition

[FILE#6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

- * To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

- * To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

- * The JBD (Journal Block Device) driver is not loaded. [FILE-6398]

- Details : Since boot-time, you have not been using any filesystems with journaling.

Alternatively, reason could be driver is blacklisted.

<https://cisofy.com/lynis/controls/FILE-6398/>

- * Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft

[USB-1000]

<https://cisofy.com/lynis/controls/USB-1000/>

- * Check DNS configuration for the dns domain name [NAME-4028]

<https://cisofy.com/lynis/controls/NAME-4028/>

- * Install debsums utility for the verification of packages with known good database. [PKGS-7370]

<https://cisofy.com/lynis/controls/PKGS-7370/>

- * Install package apt-show-versions for patch management purposes [PKGS-7394]

<https://cisofy.com/lynis/controls/PKGS-7394/>

- * Install a package audit tool to determine vulnerable packages [PKGS-7398]

<https://cisofy.com/lynis/controls/PKGS-7398/>

- * Determine if protocol 'dccp' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- * Determine if protocol 'sctp' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- * Determine if protocol 'rds' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- * Determine if protocol 'tipc' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- * Access to CUPS configuration could be more strict. [PRNT-2307]

<https://cisofy.com/lynis/controls/PRNT-2307/>

- * Enable logging to an external logging host for archiving purposes and additional protection

[LOGG-2154]

<https://cisofy.com/lynis/controls/LOGG-2154/>

- * Check what deleted files are still in use and why. [LOGG-2190]

<https://cisofy.com/lynis/controls/LOGG-2190/>

- * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

<https://cisofy.com/lynis/controls/BANN-7126/>

- * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

<https://cisofy.com/lynis/controls/BANN-7130/>

- * Enable process accounting [ACCT-9622]

<https://cisofy.com/lynis/controls/ACCT-9622/>

- * Enable sysstat to collect accounting (disabled) [ACCT-9626]
<https://cisofy.com/lynis/controls/ACCT-9626/>
- * Enable auditd to collect audit information [ACCT-9628]
<https://cisofy.com/lynis/controls/ACCT-9628/>
- * Check output of aa-status [MACF-6208]
- Details : /sys/kernel/security/apparmor/profiles
- Solution : Run aa-status
<https://cisofy.com/lynis/controls/MACF-6208/>
- * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
<https://cisofy.com/lynis/controls/FINT-4350/>
- * Determine if automation tools are present for system management [TOOL-5002]
<https://cisofy.com/lynis/controls/TOOL-5002/>
- * Consider restricting file permissions [FILE-7524]
- Details : See screen output or log file
- Solution : Use chmod to change file permissions
<https://cisofy.com/lynis/controls/FILE-7524/>
- * 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>)
<https://cisofy.com/lynis/controls/KRNL-6000/>
- * 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, Wazuh
<https://cisofy.com/lynis/controls/HRDN-7230/>

Follow-up:

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /home/aaron/lynis.log)
- Read security controls texts (<https://cisofy.com>)
- Use --upload to upload data to central system (Lynis Enterprise users)

Lynis security scan details:

Hardening index : 64 [#####]

Tests performed : 250

Plugins enabled : 2

Components:

- Firewall [V]
- Malware scanner [X]

Scan mode:

Normal [] Forensics [] Integration [] Pentest [V] (running non-privileged)

Lynis modules:

- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:

- Test and debug information : /home/aaron/lynis.log
- Report data : /home/aaron/lynis-report.dat

Pruebas omitidas, debido a que el modo no privilegiado está activo

BOOT-5108 - Check Syslinux as bootloader

BOOT-5109 - Check rEFInd as bootloader

BOOT-5116 - Check if system is booted in UEFI mode
BOOT-5140 - Check for ELILO boot loader presence
AUTH-9216 - Check group and shadow group files
AUTH-9229 - Check password hashing methods
AUTH-9252 - Check ownership and permissions for sudo configuration files
AUTH-9288 - Checking for expired passwords
FILE-6368 - Checking ACL support on root file system
PKGS-7390 - Check Ubuntu database consistency
PKGS-7392 - Check for Debian/Ubuntu security updates
FIRE-4508 - Check used policies of iptables chains
FIRE-4512 - Check iptables for empty ruleset
FIRE-4513 - Check iptables for unused rules
FIRE-4540 - Check for empty nftables configuration
FIRE-4586 - Check firewall logging
CRYP-7930 - Determine if system uses LUKS block device encryption

=====
=====

Lynis 3.1.3

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

2007-2024, CISOfy - <https://cisofy.com/lynis/>

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

=====
=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/home/aaron/lynis/default.prf for all settings)

#####

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.

2007-2024, CISOfy - <https://cisofy.com/lynis/>

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

#####

[+] Initializing program

#####

#

NON-PRIVILEGED SCAN MODE

#

#####

NOTES:

* Some tests will be skipped (as they require root permissions)

* Some tests might fail silently or give different results

- Detecting OS... [DONE]

- Checking profiles... [DONE]

- Detecting language and localization [es]

Translation file (db/languages/es) needs an update [OUTDATED]

=====
=====

Help other users and translate the missing lines:

1) Go to: <https://github.com/CISOfy/lynis/edit/master/db/languages/es>

2) Translate (some of) the lines starting with a hash (#) and remove the leading hash

3) Commit the changes

Thank you!

Note: no lines with a hash? Look if the file recently has been changed by another translator.

=====

Program version: 3.1.3
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0
Hardware platform: x86_64
Hostname: aaron-VirtualBox

Profiles: /home/aaron/lynis/default.prf
Log file: /home/aaron/lynis.log
Report file: /home/aaron/lynis-report.dat
Report version: 1.0
Plugin directory: ./plugins

Auditor: [Not Specified]
Language: es
Test category: all
Test group: all

- Program update status... [SIN ACTUALIZACIÓN]
[+] Herramientas del sistema

- Scanning available tools...
- Checking system binaries...
[+] Plugins (fase 1)

Nota: los plugins contienen pruebas más extensivas y toman más tiempo
- Plugin: pam
[..]
- Plugin: systemd
[.....]
[+] Arranque y servicios

- Service Manager [systemd]
- Checking presence GRUB2 [ENCONTRADO]
- Checking for password protection [NINGUNO]
- Check running services (systemctl) [HECHO]
Result: found 29 running services
- Check enabled services at boot (systemctl) [HECHO]
Result: found 55 enabled services
- Check startup files (permissions) [OK]
- Running 'systemd-analyze security'
- ModemManager.service: [MEDIO]
- NetworkManager.service: [EXPUESTO]
- accounts-daemon.service: [MEDIO]
- alsa-state.service: [INSEGURO]
- anacron.service: [INSEGURO]

- avahi-daemon.service: [INSEGURO]
- colord.service: [PROTEGIDO]
- cron.service: [INSEGURO]
- cups-browsed.service: [INSEGURO]
- cups.service: [INSEGURO]
- dbus.service: [INSEGURO]
- dmesg.service: [INSEGURO]
- emergency.service: [INSEGURO]
- gdm.service: [INSEGURO]
- getty@tty1.service: [INSEGURO]
- gnome-remote-desktop.service: [INSEGURO]
- kerneloops.service: [INSEGURO]
- networkd-dispatcher.service: [INSEGURO]
- plymouth-start.service: [INSEGURO]
- polkit.service: [PROTEGIDO]
- power-profiles-daemon.service: [MEDIO]
- rc-local.service: [INSEGURO]
- rescue.service: [INSEGURO]
- rsyslog.service: [MEDIO]
- rtkit-daemon.service: [MEDIO]
- snapd.service: [INSEGURO]
- sssd-autofs.service: [INSEGURO]
- sssd-nss.service: [INSEGURO]
- sssd-pac.service: [INSEGURO]
- sssd-pam.service: [INSEGURO]
- sssd-ssh.service: [INSEGURO]
- sssd-sudo.service: [INSEGURO]
- sssd.service: [EXPUESTO]
- switcheroo-control.service: [EXPUESTO]
- systemd-ask-password-console.service: [INSEGURO]
- systemd-ask-password-plymouth.service: [INSEGURO]
- systemd-ask-password-wall.service: [INSEGURO]
- systemd-bsod.service: [INSEGURO]
- systemd-fsckd.service: [INSEGURO]
- systemd-initctl.service: [INSEGURO]
- systemd-journald.service: [PROTEGIDO]
- systemd-logind.service: [PROTEGIDO]
- systemd-networkd.service: [PROTEGIDO]
- systemd-oomd.service: [PROTEGIDO]
- systemd-resolved.service: [PROTEGIDO]
- systemd-rfkill.service: [INSEGURO]
- systemd-timesyncd.service: [PROTEGIDO]
- systemd-udev.service: [MEDIO]
- thermald.service: [INSEGURO]
- tpm-udev.service: [INSEGURO]
- ubuntu-advantage.service: [INSEGURO]
- udisks2.service: [INSEGURO]
- unattended-upgrades.service: [INSEGURO]
- upower.service: [PROTEGIDO]
- user@1000.service: [INSEGURO]
- uuidd.service: [MEDIO]
- whoopsie.service: [INSEGURO]

- wpa_supplicant.service: [INSEGURO]

[+] Kernel

- Checking default runlevel [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 68 active modules

- Checking Linux kernel configuration file [ENCONTRADO]

- Checking default I/O kernel scheduler [NO ENCONTRADO]

- Checking for available kernel update [OK]

- Checking core dumps configuration

- configuration in systemd conf files [POR DEFECTO]

- configuration in /etc/profile [POR DEFECTO]

- 'hard' configuration in /etc/security/limits.conf [POR DEFECTO]

- 'soft' configuration in /etc/security/limits.conf [POR DEFECTO]

- Checking setuid core dumps configuration [PROTEGIDO]

- Check if reboot is needed [NO]

[+] Memoria y procesos

- Checking /proc/meminfo [ENCONTRADO]

- Searching for dead/zombie processes [NO ENCONTRADO]

- Searching for IO waiting processes [NO ENCONTRADO]

- Search prelink tooling [NO ENCONTRADO]

[+] Usuarios, grupos y autenticación

- Administrator accounts [OK]

- Unique UIDs [OK]

- Unique group IDs [OK]

- Unique group names [OK]

- Password file consistency [SUGERENCIA]

- Checking password hashing rounds [DESHABILITADO]

- Query system users (non daemons) [HECHO]

- NIS+ authentication support [NO HABILITADO]

- NIS authentication support [NO HABILITADO]

- Sudoers file(s) [ENCONTRADO]

- PAM password strength tools [OK]

- 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]

- Locked accounts [OK]

- Checking user password aging (minimum) [DESHABILITADO]

- User password aging (maximum) [DESHABILITADO]

- Checking Linux single user mode authentication [OK]

- Determining default umask

- umask (/etc/profile) [NO ENCONTRADO]

- umask (/etc/login.defs) [SUGERENCIA]

- LDAP authentication support [NO HABILITADO]
- Logging failed login attempts [HABILITADO]

[+] Kerberos

- Check for Kerberos KDC and principals [NO ENCONTRADO]

[+] Shells

- Checking shells from /etc/shells

Result: found 7 shells (valid shells: 7).

- Session timeout settings/tools [NINGUNO]
- Checking default umask values
- Checking default umask in /etc/bash.bashrc [NINGUNO]
- Checking default umask in /etc/profile [NINGUNO]

[+] Sistemas de ficheros

- 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]
- Mount options of / [OK]
- Mount options of /dev [PARCIALMENTE BASTIONADO]
- Mount options of /dev/shm [PARCIALMENTE BASTIONADO]
- Mount options of /run [BASTIONADO]
- Total without nodev:6 noexec:21 nosuid:15 ro or noexec (W^X): 10 of total 37
- JBD driver is not loaded [NECESITA VERIFICACIÓN]
- Disable kernel support of some filesystems

[+] Dispositivos USB

- Checking usb-storage driver (modprobe config) [NO DESHABILITADO]
- Checking USB devices authorization [HABILITADO]
- Checking USBGuard [NO ENCONTRADO]

[+] Almacenamiento

- Checking firewire ohci driver (modprobe config) [DESHABILITADO]

[+] NFS

- Check running NFS daemon [NO ENCONTRADO]

[+] Servicios de nombres

- Checking search domains [ENCONTRADO]
- Checking /etc/resolv.conf options [ENCONTRADO]
- Searching DNS domain name [DESCONOCIDO]
- Checking /etc/hosts
- Duplicate entries in hosts file [NINGUNO]
- Presence of configured hostname in /etc/hosts [ENCONTRADO]
- Hostname mapped to localhost [NO ENCONTRADO]

- Localhost mapping to IP address [OK]

[+] Puertos y paquetes

- Searching package managers

- Searching dpkg package manager [ENCONTRADO]

- Querying package manager

- Query unpurged packages [NINGUNO]

- Checking security repository in sources.list.d directory [OK]

- Checking upgradeable packages [OMITIDO]

- Checking package audit tool [NINGUNO]

- Toolkit for automatic upgrades (unattended-upgrade) [ENCONTRADO]

[+] Conectividad

- Checking IPv6 configuration [HABILITADO]

Configuration method [AUTO]

IPv6 only [NO]

- Checking configured nameservers

- Testing nameservers

Nameserver: 127.0.0.53 [OK]

- DNSSEC supported (systemd-resolved) [DESCONOCIDO]

- Getting listening ports (TCP/UDP) [HECHO]

- Checking promiscuous interfaces [OK]

- Checking status DHCP client [NOT ACTIVE]

- Checking for ARP monitoring software [NO ENCONTRADO]

- Uncommon network protocols [0]

[+] Impresoras y spools

- Checking cups daemon [CORRIENDO]

- Checking CUPS configuration file [OK]

- File permissions [PELIGRO]

- Checking CUPS addresses/sockets [ENCONTRADO]

- Checking lp daemon [NO ESTÁ CORRIENDO]

[+] Software: correo electrónico y mensajería

[+] Software: firewalls

- Checking iptables kernel module [ENCONTRADO]

- Checking host based firewall [ACTIVO]

[+] Software: servidor web

- Checking Apache [NO ENCONTRADO]

- Checking nginx [NO ENCONTRADO]

[+] Soporte SSH

- Checking running SSH daemon [NO ENCONTRADO]

[+] Soporte SNMP

- Checking running SNMP daemon [NO ENCONTRADO]

[+] Bases de datos

No database engines found

[+] Servicios LDAP

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

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

- Checking running Squid daemon [NO ENCONTRADO]
[+] Logging y ficheros

- Checking for a running log daemon [OK]
- Checking Syslog-NG status [NO ENCONTRADO]
- Checking systemd journal status [ENCONTRADO]
- Checking Metalog status [NO ENCONTRADO]
- Checking RSyslog status [ENCONTRADO]
- Checking RFC 3195 daemon status [NO ENCONTRADO]
- Checking minilogd instances [NO ENCONTRADO]
- Checking wazuh-agent daemon status [NO ENCONTRADO]
- Checking logrotate presence [OK]
- Checking remote logging [NO HABILITADO]
- Checking log directories (static list) [HECHO]
- Checking open log files [HECHO]
- Checking deleted files in use [ARCHIVOS ENCONTRADOS]
[+] Servicios inseguros

- Installed inetd package [NO ENCONTRADO]
- Installed xinetd package [OK]
- xinetd status [NOT ACTIVE]
- Installed rsh client package [OK]
- Installed rsh server package [OK]
- Installed telnet client package [OK]
- Installed telnet server package [NO ENCONTRADO]
- Checking NIS client installation [OK]
- Checking NIS server installation [OK]
- Checking TFTP client installation [OK]
- Checking TFTP server installation [OK]
[+] Banners e identificación

- /etc/issue [ENCONTRADO]
- /etc/issue contents [DÉBIL]
- /etc/issue.net [ENCONTRADO]
- /etc/issue.net contents [DÉBIL]
[+] Tareas programadas

- Checking crontab and cronjob files [HECHO]
[+] Contabilidad

- Checking accounting information [NO ENCONTRADO]
- Checking sysstat accounting data [DESHABILITADO]
- Checking auditd [NO ENCONTRADO]
[+] Tiempo y sincronización

- NTP daemon found: systemd (timesyncd) [ENCONTRADO]
- Checking for a running NTP daemon or client [OK]
- Last time synchronization [426s]

[+] Criptografía

- Checking for expired SSL certificates [0/151] [NINGUNO]
- Kernel entropy is sufficient [SÍ]
- HW RNG & rngd [NO]
- SW prng [NO]
- MOR variable not found [DÉBIL]

[+] Virtualización

[+] Contenedores

[+] Frameworks de seguridad

- Checking presence AppArmor [ENCONTRADO]
- Checking AppArmor status [DESCONOCIDO]
- Checking presence SELinux [NO ENCONTRADO]
- Checking presence TOMOYO Linux [NO ENCONTRADO]
- Checking presence grsecurity [NO ENCONTRADO]
- Checking for implemented MAC framework [NINGUNO]

[+] Software: integridad de ficheros

- Checking file integrity tools
- Checking presence integrity tool [NO ENCONTRADO]

[+] Software: Herramientas del sistema

- Checking automation tooling
- Automation tooling [NO ENCONTRADO]
- Checking for IDS/IPS tooling [NINGUNO]

[+] Software: Malware

- Malware software components [NO ENCONTRADO]

[+] Permisos de ficheros

- Starting file permissions check
- File: /boot/grub/grub.cfg [OK]
- File: /etc/crontab [SUGERENCIA]
- File: /etc/group [OK]
- File: /etc/group- [OK]
- File: /etc/hosts.allow [OK]
- File: /etc/hosts.deny [OK]
- File: /etc/issue [OK]
- File: /etc/issue.net [OK]
- File: /etc/passwd [OK]
- File: /etc/passwd- [OK]
- Directory: /etc/cron.d [SUGERENCIA]
- Directory: /etc/cron.daily [SUGERENCIA]
- Directory: /etc/cron.hourly [SUGERENCIA]
- Directory: /etc/cron.weekly [SUGERENCIA]
- Directory: /etc/cron.monthly [SUGERENCIA]

[+] Directorios de inicio

- Permissions of home directories [OK]
- Ownership of home directories [OK]
- Checking shell history files [OK]

[+] Bastionado del kernel

- Comparing sysctl key pairs with scan profile
- dev.tty.ldisc_autoload (exp: 0) [DIFERENTE]
- fs.protected_fifos (exp: 2) [DIFERENTE]
- fs.protected_hardlinks (exp: 1) [OK]
- fs.protected_regular (exp: 2) [OK]
- fs.protected_symlinks (exp: 1) [OK]
- fs.suid_dumpable (exp: 0) [DIFERENTE]
- kernel.core_uses_pid (exp: 1) [DIFERENTE]
- kernel.ctrl-alt-del (exp: 0) [OK]
- kernel.dmesg_restrict (exp: 1) [OK]
- kernel.kptr_restrict (exp: 2) [DIFERENTE]
- kernel.modules_disabled (exp: 1) [DIFERENTE]
- kernel.perf_event_paranoid (exp: 2 3 4) [OK]
- kernel.randomize_va_space (exp: 2) [OK]
- kernel.sysrq (exp: 0) [DIFERENTE]
- kernel.unprivileged_bpf_disabled (exp: 1) [DIFERENTE]
- kernel.yama.ptrace_scope (exp: 1 2 3) [OK]
- net.ipv4.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv4.conf.all.bootp_relay (exp: 0) [OK]
- net.ipv4.conf.all.forwarding (exp: 0) [OK]
- net.ipv4.conf.all.log_martians (exp: 1) [DIFERENTE]
- net.ipv4.conf.all.mc_forwarding (exp: 0) [OK]
- net.ipv4.conf.all.proxy_arp (exp: 0) [OK]
- net.ipv4.conf.all.rp_filter (exp: 1) [DIFERENTE]
- net.ipv4.conf.all.send_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.accept_source_route (exp: 0) [DIFERENTE]
- net.ipv4.conf.default.log_martians (exp: 1) [DIFERENTE]
- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1) [OK]
- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1) [OK]
- net.ipv4.tcp_syncookies (exp: 1) [OK]
- net.ipv4.tcp_timestamps (exp: 0 1) [OK]
- net.ipv6.conf.all.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.all.accept_source_route (exp: 0) [OK]
- net.ipv6.conf.default.accept_redirects (exp: 0) [DIFERENTE]
- net.ipv6.conf.default.accept_source_route (exp: 0) [OK]

[+] Bastionado

- Installed compiler(s) [NO ENCONTRADO]
- Installed malware scanner [NO ENCONTRADO]
- Non-native binary formats [ENCONTRADO]

[+] Pruebas personalizadas

- Running custom tests... [NINGUNO]

[+] Plugins (fase 2)

- Plugins (phase 2) [HECHO]

-[Lynis 3.1.3 Results]-

Great, no warnings

Suggestions (35):

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

<https://cisofy.com/lynis/controls/BOOT-5122/>

* Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service

<https://cisofy.com/lynis/controls/BOOT-5264/>

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file

[KRNL#5820]

<https://cisofy.com/lynis/controls/KRNL-5820/>

* Run pwck manually and correct any errors in the password file [AUTH-9228]

<https://cisofy.com/lynis/controls/AUTH-9228/>

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]

<https://cisofy.com/lynis/controls/AUTH-9230/>

* Configure minimum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

* Configure maximum password age in /etc/login.defs [AUTH-9286]

<https://cisofy.com/lynis/controls/AUTH-9286/>

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

<https://cisofy.com/lynis/controls/AUTH-9328/>

* To decrease the impact of a full /home file system, place /home on a separate partition

[FILE#6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

<https://cisofy.com/lynis/controls/FILE-6310/>

* The JBD (Journal Block Device) driver is not loaded. [FILE-6398]

- Details : Since boot-time, you have not been using any filesystems with journaling.

Alternatively, reason could be driver is blacklisted.

<https://cisofy.com/lynis/controls/FILE-6398/>

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft

[USB-1000]

<https://cisofy.com/lynis/controls/USB-1000/>

* Check DNS configuration for the dns domain name [NAME-4028]

<https://cisofy.com/lynis/controls/NAME-4028/>

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

<https://cisofy.com/lynis/controls/PKGS-7370/>

* Install package apt-show-versions for patch management purposes [PKGS-7394]

<https://cisofy.com/lynis/controls/PKGS-7394/>

* Install a package audit tool to determine vulnerable packages [PKGS-7398]

<https://cisofy.com/lynis/controls/PKGS-7398/>

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]

<https://cisofy.com/lynis/controls/NETW-3200/>

- * Determine if protocol 'sctp' is really needed on this system [NETW-3200]
<https://cisofy.com/lynis/controls/NETW-3200/>
- * Determine if protocol 'rds' is really needed on this system [NETW-3200]
<https://cisofy.com/lynis/controls/NETW-3200/>
- * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
<https://cisofy.com/lynis/controls/NETW-3200/>
- * Access to CUPS configuration could be more strict. [PRNT-2307]
<https://cisofy.com/lynis/controls/PRNT-2307/>
- * Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]
<https://cisofy.com/lynis/controls/LOGG-2154/>
- * Check what deleted files are still in use and why. [LOGG-2190]
<https://cisofy.com/lynis/controls/LOGG-2190/>
- * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
<https://cisofy.com/lynis/controls/BANN-7126/>
- * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
<https://cisofy.com/lynis/controls/BANN-7130/>
- * Enable process accounting [ACCT-9622]
<https://cisofy.com/lynis/controls/ACCT-9622/>
- * Enable sysstat to collect accounting (disabled) [ACCT-9626]
<https://cisofy.com/lynis/controls/ACCT-9626/>
- * Enable auditd to collect audit information [ACCT-9628]
<https://cisofy.com/lynis/controls/ACCT-9628/>
- * Check output of aa-status [MACF-6208]
 - Details : /sys/kernel/security/apparmor/profiles
 - Solution : Run aa-status
<https://cisofy.com/lynis/controls/MACF-6208/>
- * Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]
<https://cisofy.com/lynis/controls/FINT-4350/>
- * Determine if automation tools are present for system management [TOOL-5002]
<https://cisofy.com/lynis/controls/TOOL-5002/>
- * Consider restricting file permissions [FILE-7524]
 - Details : See screen output or log file
 - Solution : Use chmod to change file permissions
<https://cisofy.com/lynis/controls/FILE-7524/>
- * 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>)
<https://cisofy.com/lynis/controls/KRNL-6000/>
- * 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, Wazuh
<https://cisofy.com/lynis/controls/HRDN-7230/>

Follow-up:

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /home/aaron/lynis.log)
- Read security controls texts (<https://cisofy.com>)
- Use --upload to upload data to central system (Lynis Enterprise users)

Lynis security scan details:

Hardening index : 64 [#####]

Tests performed : 250

Plugins enabled : 2

Components:

- Firewall [V]
- Malware scanner [X]

Scan mode:

Normal [] Forensics [] Integration [] Pentest [V] (running non-privileged)

Lynis modules:

- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:

- Test and debug information : /home/aaron/lynis.log
- Report data : /home/aaron/lynis-report.dat

=====

Pruebas omitidas, debido a que el modo no privilegiado está activo

BOOT-5108 - Check Syslinux as bootloader

BOOT-5109 - Check rEFInd as bootloader

BOOT-5116 - Check if system is booted in UEFI mode

BOOT-5140 - Check for ELILO boot loader presence

AUTH-9216 - Check group and shadow group files

AUTH-9229 - Check password hashing methods

AUTH-9252 - Check ownership and permissions for sudo configuration files

AUTH-9288 - Checking for expired passwords

FILE-6368 - Checking ACL support on root file system

PKGS-7390 - Check Ubuntu database consistency

PKGS-7392 - Check for Debian/Ubuntu security updates

FIRE-4508 - Check used policies of iptables chains

FIRE-4512 - Check iptables for empty ruleset

FIRE-4513 - Check iptables for unused rules

FIRE-4540 - Check for empty nftables configuration

FIRE-4586 - Check firewall logging

CRYP-7930 - Determine if system uses LUKS block device encryption

=====

Lynis 3.1.3

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

2007-2024, CISOfy - <https://cisofy.com/lynis/>

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

=====

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see
/home/aaron/lynis/default.prf for all settings)

Centro Criptológico Nacional




Nombre del sistema:
DESKTOP-N9A7M63
Organización: IES El Bohío
Unidad: Trabajo
Categoría del sistema: ALTA


Auditado por Aaron
Informes generados el día 04/10/2024 15:23:55 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74

Mostrar todo

Datos del sistema		Ocultar
Valor de criticidad		
Sistema		Ocultar
 Recoge la información de datos básicos del sistema		
Nombre del sistema	DESKTOP-N9A7M63	
Modelo	VirtualBox	
Fabricante	innotek GmbH	
Descripción	AT/AT COMPATIBLE	
Nombre del propietario	Aaron	
Tipo de sistema	x64-based PC	
Memoria física	4,98 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	99,12 GB's	
Sistema de ficheros	NTFS	
Letra de unidad	D:	
Nombre		
Tamaño	0 GB's	
Sistema de ficheros	Desconocido	

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	10.0.22631	
Versión de Service Pack	No hay Service Pack instalado	
Versión de Internet Explorer	11.1.22621.0	
Versión de Windows Media Player	12.0.22621.2506	
Número de compilación	22631	
Usuario registrado	Aaron	
Número de serie	00330-80000-00000-AA002	
Último arranque	04/10/2024 17:19:14	

Ocultar	
! 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

Adaptadores de red		Ocultar
! Recoge el conjunto de adaptadores de red presentes en el sistema		
Descripción	Intel(R) PRO/1000 MT Desktop Adapter	
MAC	08:00:27:4F:B4:22	
DHCP	Sí	
IP	10.0.2.15 - fe80::5010:da03:f47:fc02	
Subred	255.255.255.0 / 64	
Puerta de enlace predeterminada	10.0.2.2	
Orden de búsqueda servidor DNS	1.1.1.1 - 8.8.8.8	
Servidor primario WINS		
Servidor secundario WINS		

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

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	No configurado	Forzar denegación	No configurado

de Windows tengan acceso a los contactos

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 aplicación/Permitir que las aplicaciones de Windows accedan a la cámara	No configurado	Forzar denegación	No configurado
--	----------------	-------------------	----------------

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 mostrar sugerencias de Windows	No configurado	Habilitada	No configurado
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 el historial de navegación/Impedir que se eliminen cookies	No configurado	Deshabilitada	No configurado
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	No configurado	Deshabilitada	No configurado

el historial de navegación/Impedir que se eliminen datos del sitio de favoritos			rado
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 comunicaciones de Internet/Desactivar el Programa para la mejora de la experiencia del usuario de Windows	No configurado	Habilitada	No configurado
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	No configurado	Habilitada	No configurado

comunicaciones de Internet/Desactivar el informe de errores de Windows			
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 el Programa para la mejora de la experiencia del usuario de Windows Messenger	No configurado	Habilitada	No configurado
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

OP.EXP.5 - Gestión de cambios (100%)	Ocultar
---	---------

Entrada	Notas	Resultado
Firewall de Windows	Los perfiles están habilitados	Correcto
Otro firewall	No hay ningún firewall. Los siguientes firewalls han sido analizados de forma automatizada: McAfee, Norton, Trend Micro, F-Secure, Microsoft.	Inconcluso
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	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, Windows 8.1, Windows server 2012 R2, Windows 10 [version 1507])	No configurado	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 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	No configurado	Deshabilitada	No configurado

BitLocker/Impedir la sobrescritura de memoria al reiniciar			rado
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 operativo/Permitir los PIN mejorados para el inicio	No configurado	Habilitada	No configurado
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	No configurado	Requerir PIN de inicio con TPM	No configurado

adicional al iniciar. Configurar PIN de inicio con TPM:

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: Configuración y datos de placa base y plataforma	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 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	No configurado	Habilitada	No configurado

participaciones de registro de arranque maestro (MBR)

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 de plataforma del TPM. PCR 10: Administrador de arranque	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 11: Control de acceso de BitLocker	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 12: 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 13: 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 14: 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 15: 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 16: 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 17: 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 18: 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 19: 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 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

9/10/24, 18:56CLARA: Informe de Auditoría

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

ESCANER

Fri, 04 Oct 2024 19:54:43 Romance Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.15

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

10.0.2.15

2	4	9	0	38
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	9.8	6.7	0.0359	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
CRITICAL	9.1	6.0	0.0004	201082	OpenSSL 3.1.0 < 3.1.7 Vulnerability
HIGH	7.5	5.2	0.0012	192923	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities
HIGH	7.5	5.1	0.0009	202577	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities
HIGH	7.5	4.4	0.0013	183890	OpenSSL 3.1.0 < 3.1.4 Vulnerability
HIGH	7.5	4.2	0.0111	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.5	5.0	0.0023	185161	OpenSSL 3.1.0 < 3.1.5 Multiple Vulnerabilities
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	5.9	3.6	0.0004	192974	OpenSSL 3.1.0 < 3.1.6 Multiple Vulnerabilities
MEDIUM	5.3	-	-	10678	Apache mod_info /server-info Information Disclosure
MEDIUM	5.3	-	-	10677	Apache mod_status /server-status Information Disclosure
MEDIUM	5.3	4.0	0.0073	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	12634	Authenticated Check : OS Name and Installed Package Enumeration

INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10147	Nessus Server Detection
INFO	N/A	-	-	64582	Netstat Connection Information
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	57323	OpenSSL Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided

INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available;
the v2.0 score is shown

Hide