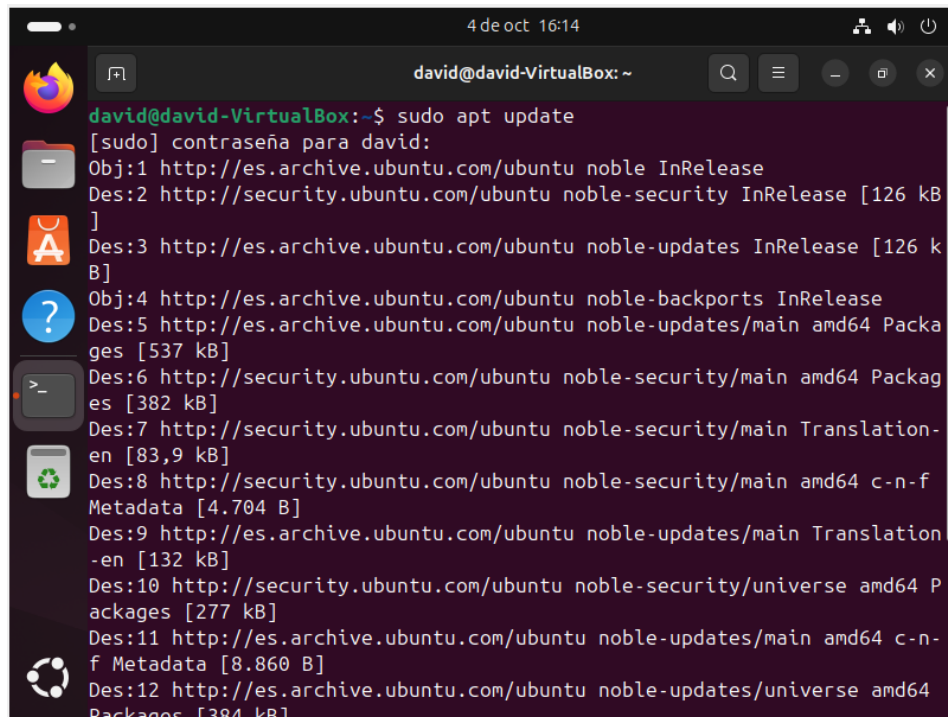


David Martinez 2ASIR

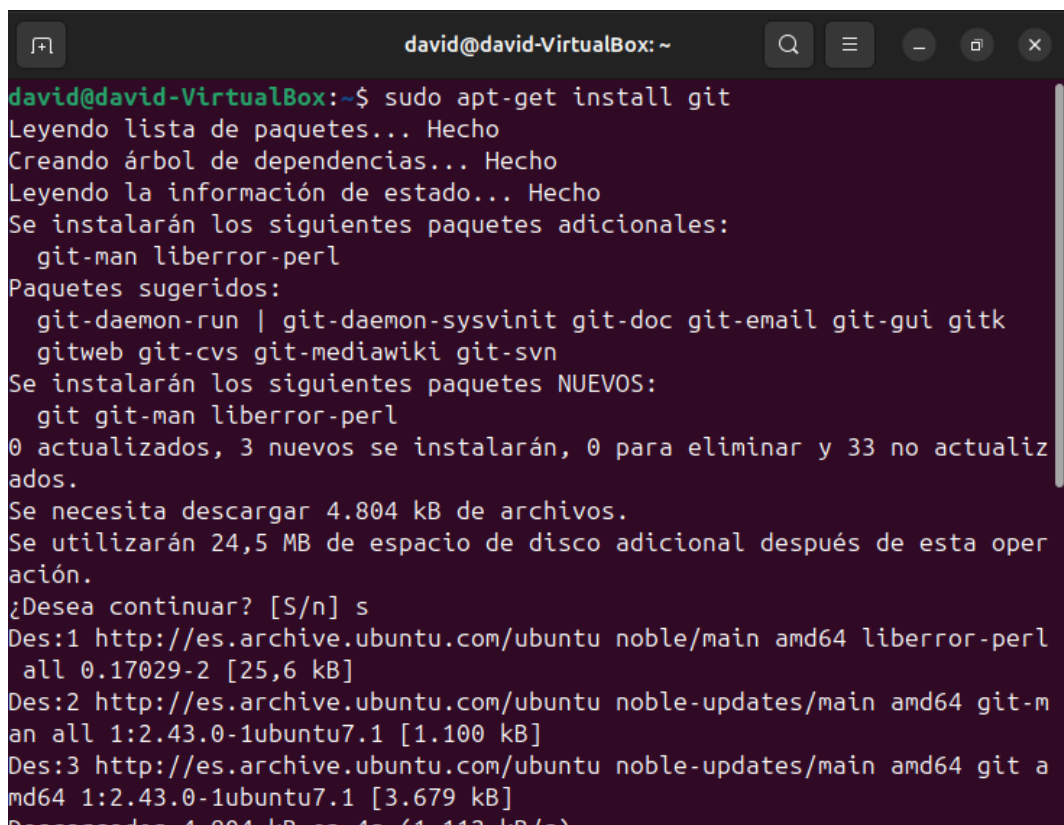
Linys (linux)

Primero actualizo los repositorios



```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ sudo apt update  
[sudo] contraseña para david:  
Obj:1 http://es.archive.ubuntu.com/ubuntu noble InRelease  
Des:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]  
Obj:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]  
Des:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease  
Des:5 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [537 kB]  
Des:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [382 kB]  
Des:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83,9 kB]  
Des:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4.704 B]  
Des:9 http://es.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [132 kB]  
Des:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [277 kB]  
Des:11 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8.860 B]  
Des:12 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [384 kB]
```

Instalo git para poder descargar el repositorio de linys



```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ sudo apt-get install git  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se instalarán los siguientes paquetes adicionales:  
  git-man liberror-perl  
Paquetes sugeridos:  
  git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk  
  gitweb git-cvs git-mediawiki git-svn  
Se instalarán los siguientes paquetes NUEVOS:  
  git git-man liberror-perl  
0 actualizados, 3 nuevos se instalarán, 0 para eliminar y 33 no actualizados.  
Se necesita descargar 4.804 kB de archivos.  
Se utilizarán 24,5 MB de espacio de disco adicional después de esta operación.  
¿Desea continuar? [S/n] s  
Des:1 http://es.archive.ubuntu.com/ubuntu noble/main amd64 liberror-perl all 0.17029-2 [25,6 kB]  
Des:2 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man all 1:2.43.0-1ubuntu7.1 [1.100 kB]  
Des:3 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 git amd64 1:2.43.0-1ubuntu7.1 [3.679 kB]  
Des:4 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 git-man amd64 1:2.43.0-1ubuntu7.1 [1.100 kB]
```

David Martinez 2ASIR

Instalo lynis

```
david@david-VirtualBox: ~  
david@david-VirtualBox:~$ git clone https://github.com/CISOfy/lynis  
Clonando en 'lynis'...  
remote: Enumerating objects: 15688, done.  
remote: Counting objects: 100% (1076/1076), done.  
remote: Compressing objects: 100% (457/457), done.  
Recibiendo objetos: 8% (1256/15688), 796.01 KiB | 83.00 KiB/s
```

Ejecuto el comando para iniciar el escaner de lynis

```
david@david-VirtualBox: ~/lynis  
david@david-VirtualBox:~/lynis$ ./lynis audit system -Q  
[ Lynis 3.1.3 ]  
#####  
#####  
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and yo  
u are  
welcome to redistribute it under the terms of the GNU General Public L  
icense.
```

David Martinez 2ASIR

Nessus (Windows)

descargo nessus de la pagina oficial

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version

Nessus - 10.8.3



Platform

Windows - x86_64



Download

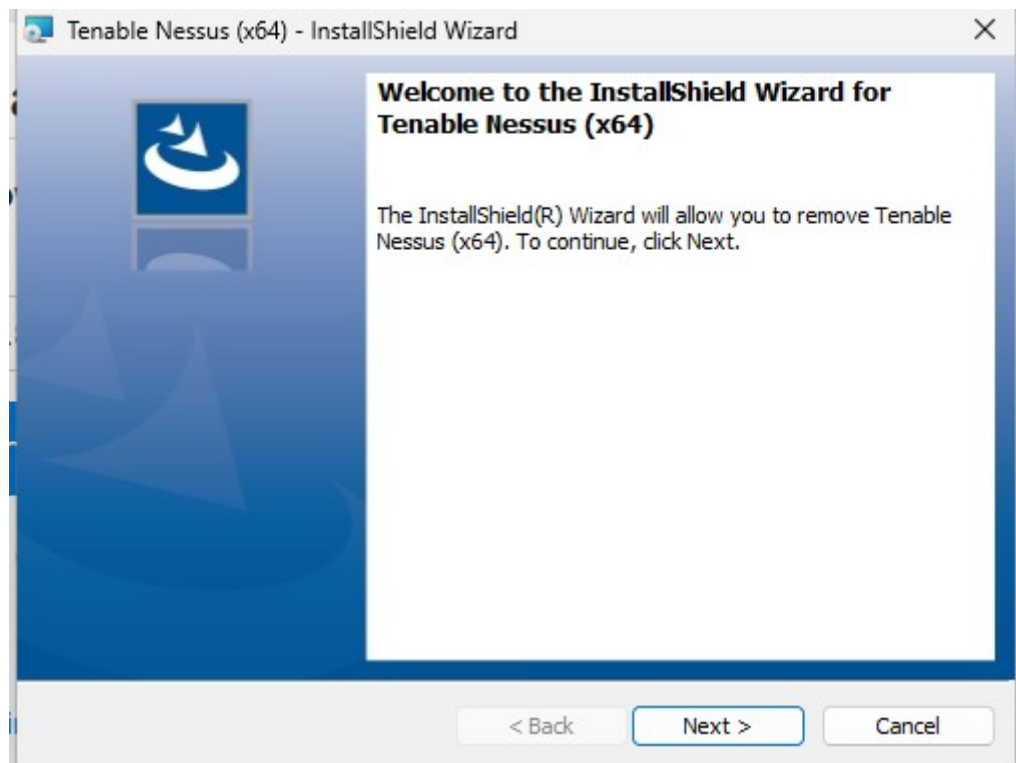
Checksum

[Download by curl >](#)

[Docker >](#)

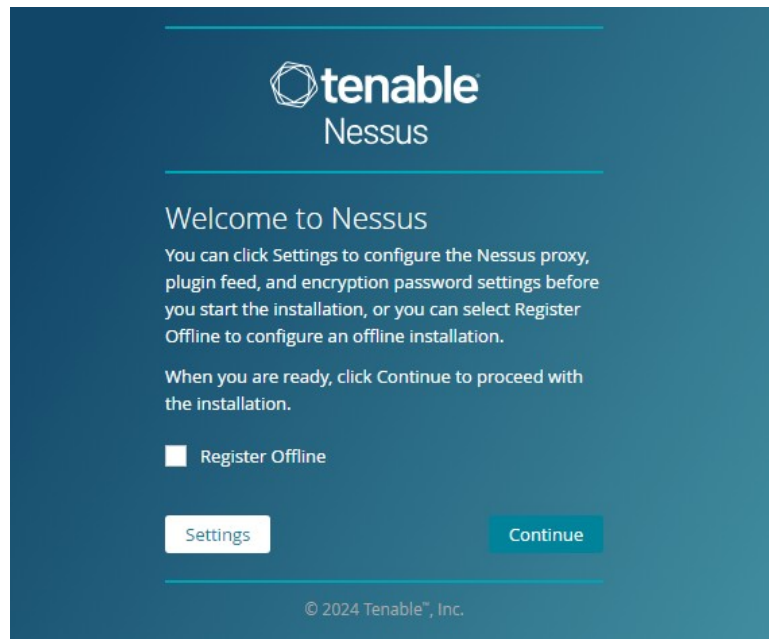
[Virtual Machines >](#)

Instalo nessus

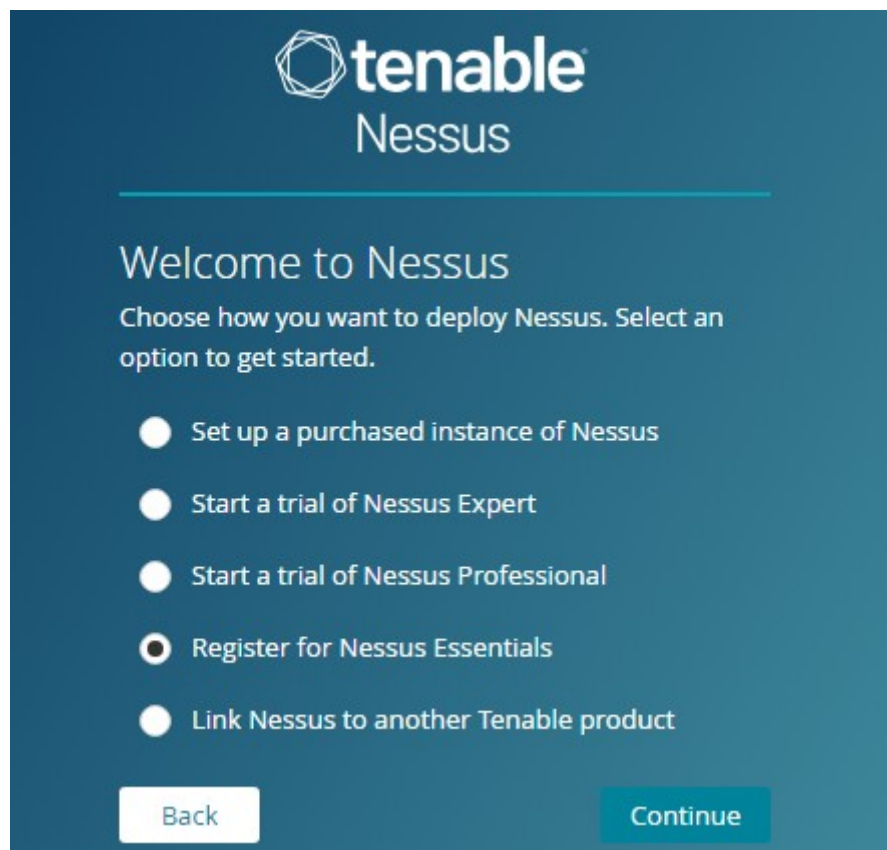


David Martinez 2ASIR

Configuro el nessus, pulso en continuar

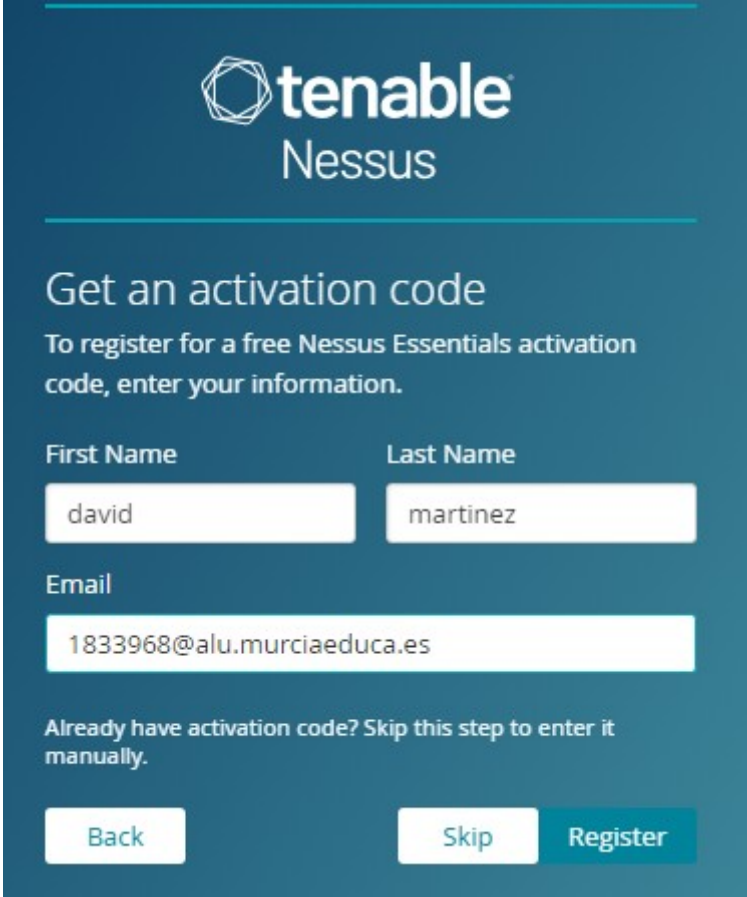


Selecciono register for nessus essentials



David Martinez 2ASIR

Me registro en nessus para que me envíe un código de activación



The image shows a registration form for Tenable Nessus. At the top is the Tenable Nessus logo. Below it, the heading "Get an activation code" is followed by the instruction "To register for a free Nessus Essentials activation code, enter your information." The form contains three input fields: "First Name" with the value "david", "Last Name" with the value "martinez", and "Email" with the value "1833968@alu.murciaeduca.es". Below these fields is a link that says "Already have activation code? Skip this step to enter it manually." At the bottom are three buttons: "Back", "Skip", and "Register".

tenable
Nessus

Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

First Name Last Name

david martinez

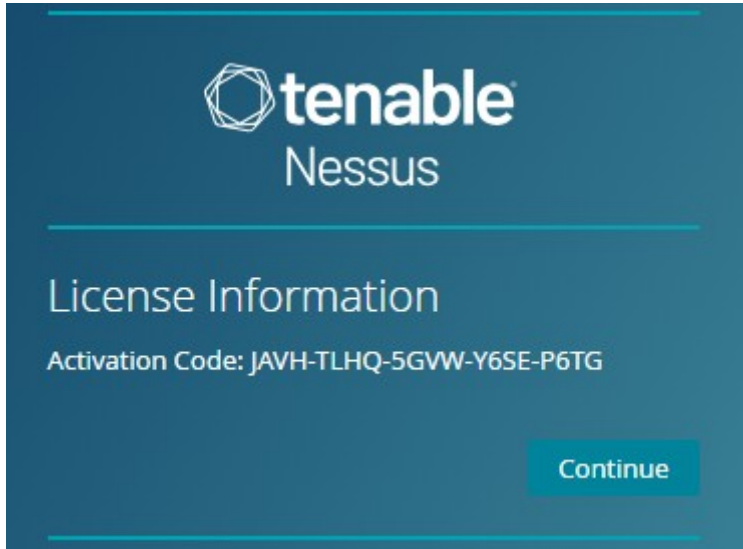
Email

1833968@alu.murciaeduca.es

Already have activation code? Skip this step to enter it manually.

Back Skip Register

Me da un código de activación



The image shows the "License Information" screen in Tenable Nessus. It features the Tenable Nessus logo at the top. Below the logo, the heading "License Information" is followed by the text "Activation Code: JAVH-TLHQ-5GVW-Y6SE-P6TG". At the bottom right is a "Continue" button.

tenable
Nessus

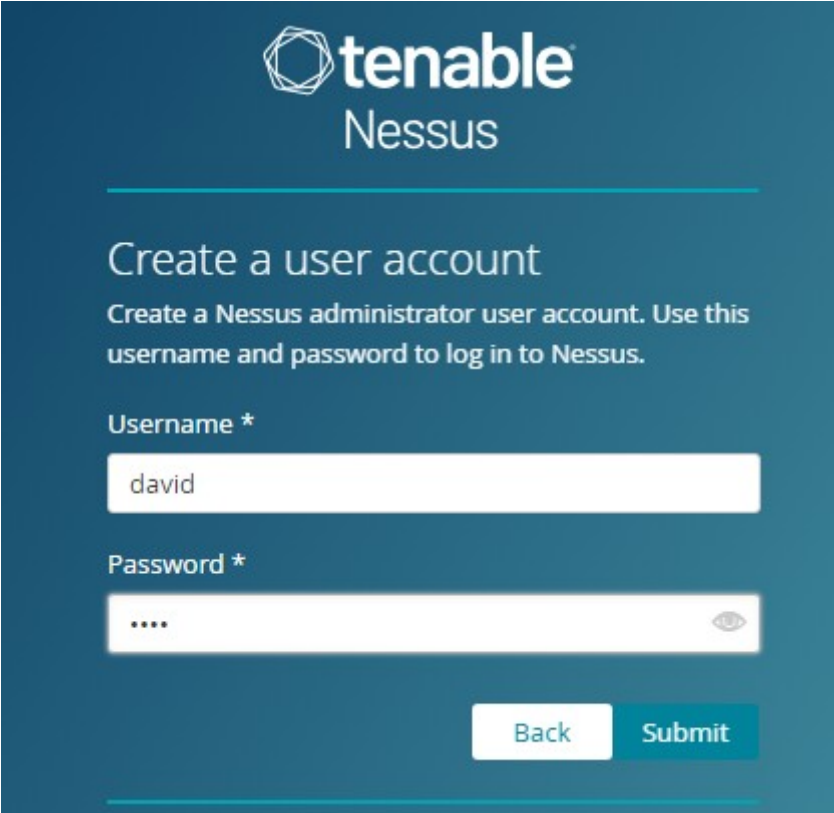
License Information

Activation Code: JAVH-TLHQ-5GVW-Y6SE-P6TG

Continue

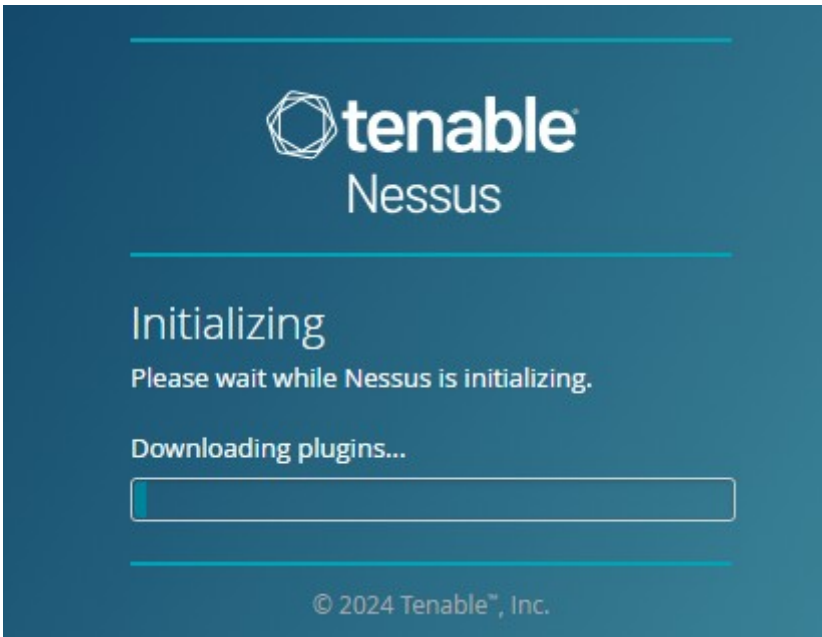
David Martinez 2ASIR

Creo la cuenta



The screenshot shows the 'Create a user account' page in the Tenable Nessus interface. At the top, the Tenable Nessus logo is displayed. Below the logo, the heading 'Create a user account' is followed by a sub-instruction: 'Create a Nessus administrator user account. Use this username and password to log in to Nessus.' There are two input fields: 'Username *' with the value 'david' and 'Password *' with masked characters '....'. A 'Back' button and a 'Submit' button are located at the bottom right of the form area.

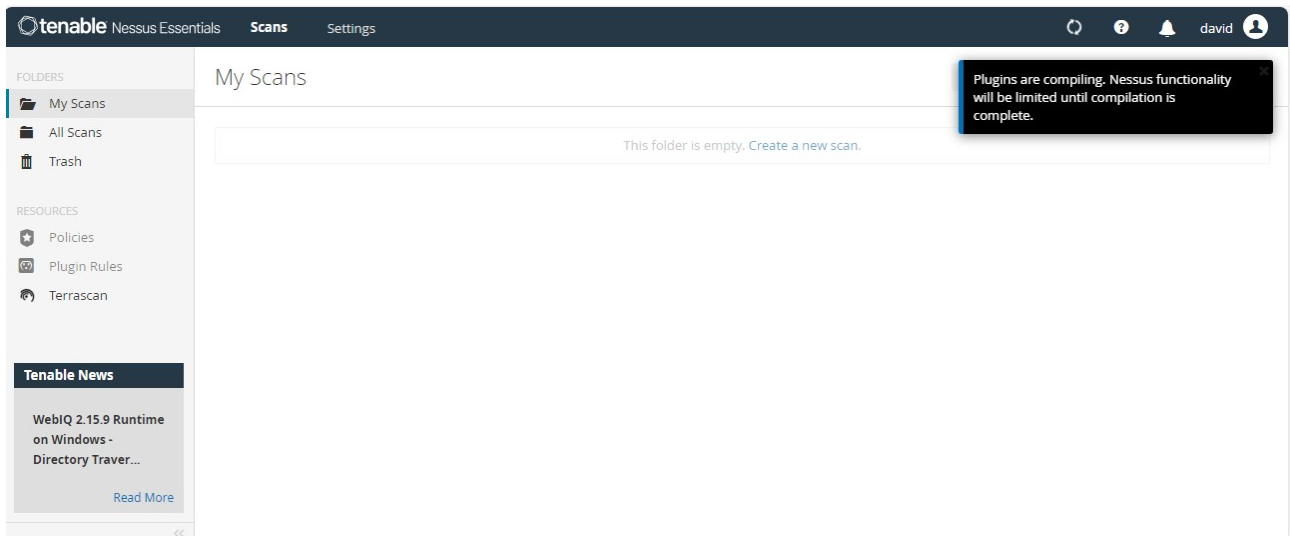
Y se empiezan a descargar los plugins



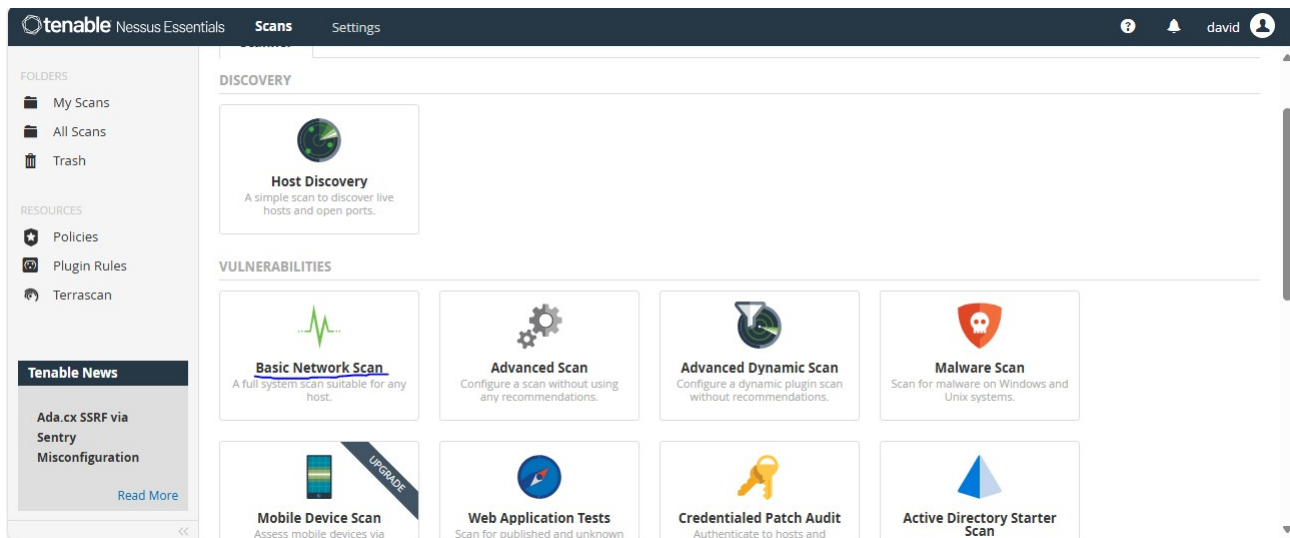
The screenshot shows the 'Initializing' screen in the Tenable Nessus interface. At the top, the Tenable Nessus logo is displayed. Below the logo, the heading 'Initializing' is followed by the text 'Please wait while Nessus is initializing.' and 'Downloading plugins...'. A progress bar is shown below the text, indicating the status of the plugin download. At the bottom, the copyright notice '© 2024 Tenable™, Inc.' is visible.

David Martinez 2ASIR

Ya he entrado al menu principal ahora espero a que los plugins se compilen



Cuando los plugins se compilen voy a nuevo escaneo y selecciono el escaneo basico



David Martinez 2ASIR

Le pongo de nombre prueba y pongo la ip de la maquina virtual que es la que voy a analizar y lo guardo

The screenshot shows the 'Settings' page of a security tool. The 'BASIC' tab is selected, and the 'General' sub-tab is active. The configuration fields are as follows:

- Name:** prueba
- Description:** (empty text box)
- Folder:** My Scans
- Targets:** 10.0.2.15

At the bottom, there is an 'Upload Targets' section with an 'Add File' button.

Ejecuto el escaneo

The screenshot shows the scan results page for the scan named 'prueba'. The page includes a 'Configure' button and a 'Back to My Scans' link. The 'History' tab is selected, showing a table of scan history.

Start Time	Last Scanned	Status
Today at 6:5...	N/A	Running

Below the table, there is a 'Scan Details' section with the following information:

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 6:55 PM

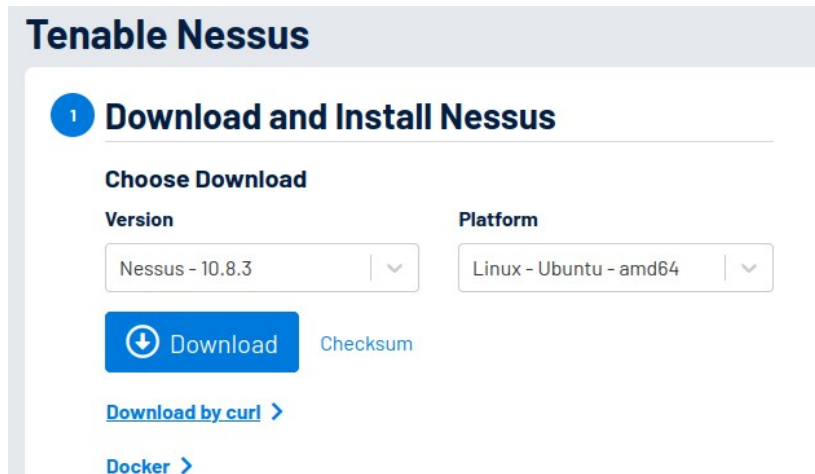
At the bottom, there is a 'Vulnerabilities' section with a donut chart showing the distribution of vulnerabilities by severity. The legend indicates the following categories:

- Critical
- High
- Medium
- Low

David Martinez 2ASIR

NESSUS (Linux)

Primero descargo nessus de la pagina oficial y lo instalo



```
david@david-VirtualBox: ~/Descargas
david@david-VirtualBox:~/Descargas$ ls
Nessus-10.8.3-ubuntu1604_amd64.deb  xampp-linux-x64-8.2.4-0-installer.run
david@david-VirtualBox:~/Descargas$ sudo dpkg -i Nessus-10.8.3-ubuntu1604_amd64.deb
Seleccionando el paquete nessus previamente no seleccionado.
(Leyendo la base de datos ... 149466 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar Nessus-10.8.3-ubuntu1604_amd64.deb ...
Desempaquetando nessus (10.8.3) ...
Configurando nessus (10.8.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
```

David Martinez 2ASIR

Activo el servicio de nessus

```
david@david-VirtualBox: ~/Descargas
david@david-VirtualBox:~/Descargas$ sudo systemctl start nessusd
david@david-VirtualBox:~/Descargas$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-10-13 22:04:11 CEST; 5s ago
     Main PID: 6363 (nessus-service)
        Tasks: 14 (limit: 4615)
       Memory: 50.9M (peak: 52.5M)
          CPU: 5.458s
       CGroup: /system.slice/nessusd.service
              └─6363 /opt/nessus/sbin/nessus-service -q
                 6364 nessusd -q

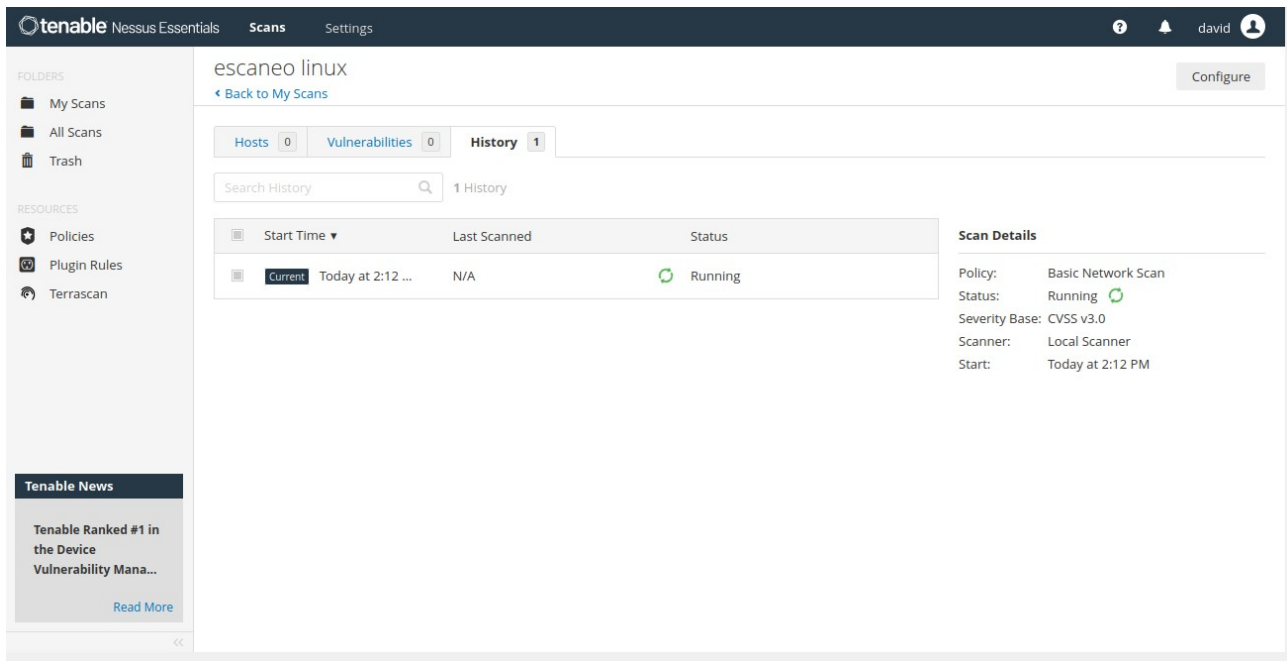
oct 13 22:04:11 david-VirtualBox systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
oct 13 22:04:13 david-VirtualBox nessus-service[6364]: Cached 0 plugin libs in 0msec
oct 13 22:04:13 david-VirtualBox nessus-service[6364]: Cached 0 plugin libs in 0msec
david@david-VirtualBox:~/Descargas$
```

Ahora entro en nessus me registro y espero a que se cargen los plugins. (Es igual que en windows por eso no hice capturas). Creo el escaneo basico.

The screenshot shows the Tenable Nessus Essentials web interface. The main heading is "New Scan / Basic Network Scan". Below it is a link "Back to Scan Templates". The interface has a sidebar on the left with "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). A "Tenable News" banner is at the bottom left. The main content area has tabs for "Settings", "Credentials", and "Plugins". The "Settings" tab is active, and the "Basic" section is expanded. The "Basic" section has a "General" sub-section with the following fields: "Name" (escaneo linux), "Description" (empty), "Folder" (My Scans), and "Targets" (10.0.2.15). There is an "Add File" link for uploading targets. At the bottom, there are "Save" and "Cancel" buttons.

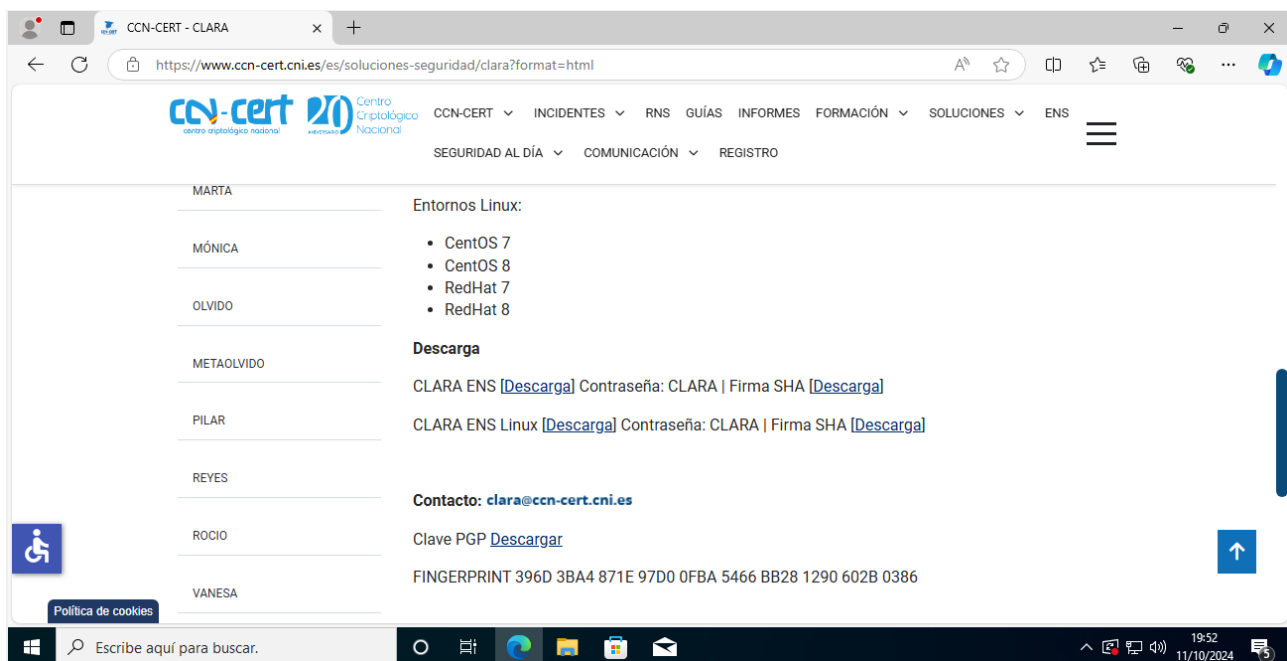
David Martinez 2ASIR

Ejecuto el escaneo

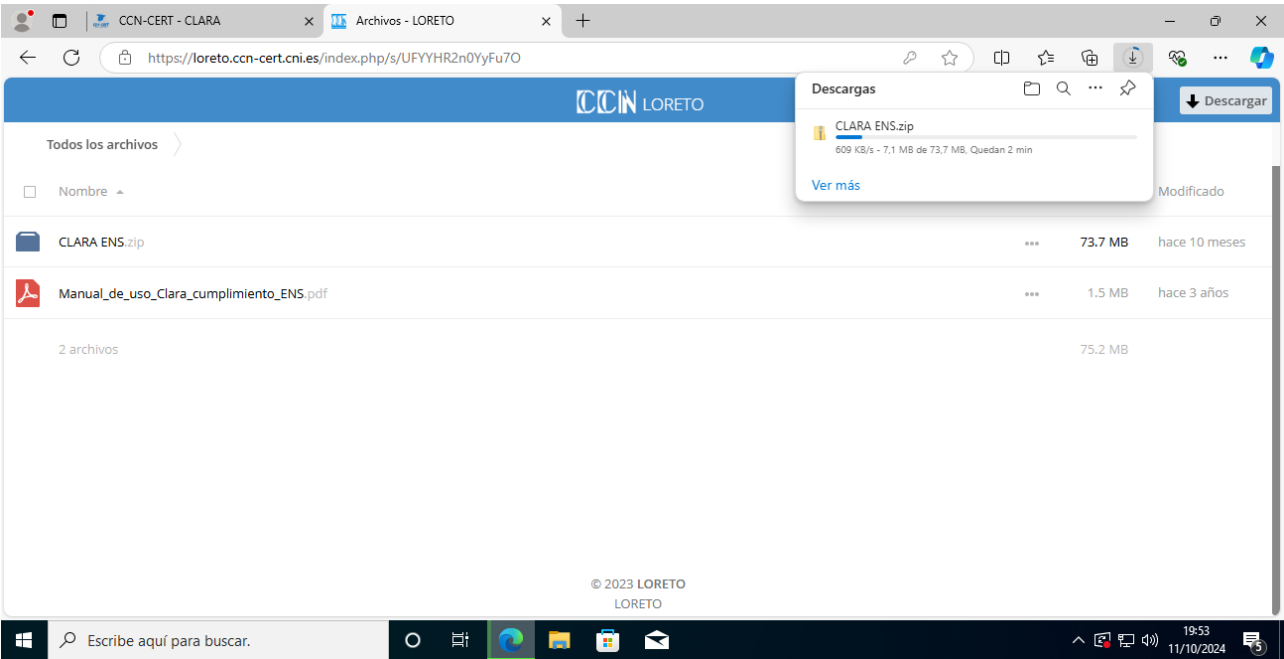


CLARA (WINDOWS)

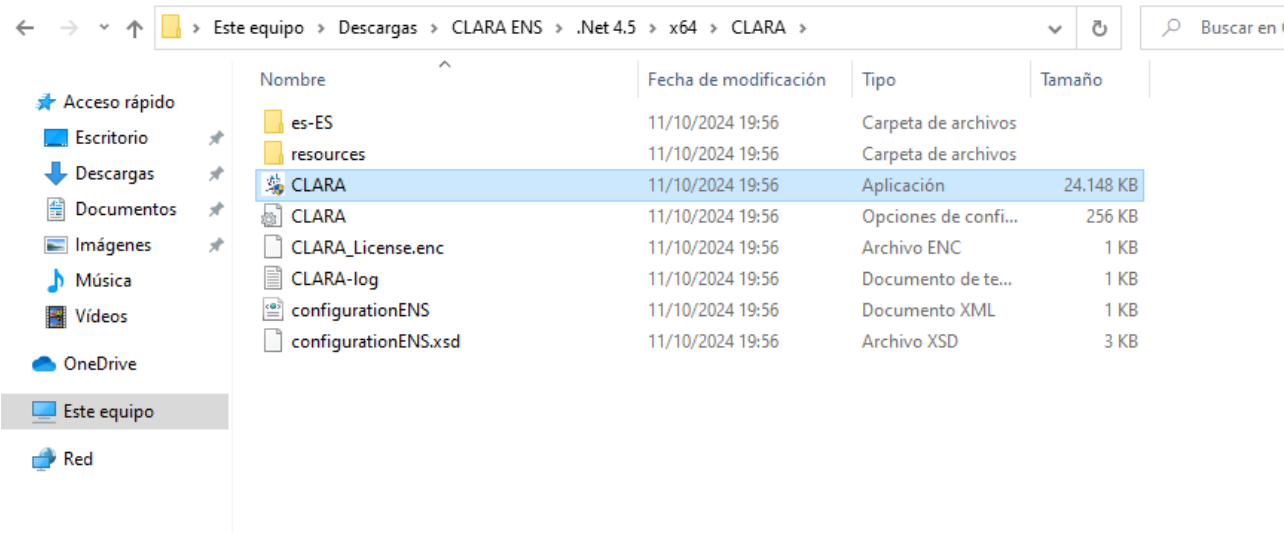
Descargo clara de la pagina oficial



David Martinez 2ASIR



Extraigo el zip y entro en clara ens, net 4.5, x64, y ejecuto el clara






David Martinez 2ASIR

Relleno los datos que pide le doy a analizar

CLARA

Fichero Herramientas Opciones Ayuda

  Versión 2.0 

Usuario: DESKTOP-L06B0TD\david

Equipo: DESKTOP-L06B0TD

Sistema operativo: Microsoft Windows 10 Pro

Auditor:

Organización:

Unidad:

Fichero de configuración:

El archivo de configuración por defecto está cargado.
Puede analizar el sistema local ahora pulsando el botón "Analizar".
Por defecto, se realiza un nivel de análisis del nivel de cumplimiento
para un sistema de categoría ALTA.

CLARA - Análisis

Fichero Herramientas Opciones Ayuda

[INFO] Loading configuration...
[INFO] Configuration loaded
[INFO] Borrando carpeta temporal ('C:\Users\david\Downloads\CLARA ENS\Net 4.5\x64\CLARA\tmp')...
[INFO] Creando carpeta 'C:\Users\david\Downloads\CLARA ENS\Net 4.5\x64\CLARA\tmp'
[INFO] \Sistema_DESKTOP-L06B0TD_11-10-2024_18-3-27'...
[INFO] Analizando información básica del sistema...
[INFO] Analizando sistema...
[OK] Sistema
[INFO] Analizando discos...
[OK] Discos
[INFO] Analizando sistema operativo...
[OK] Sistema operativo
[INFO] Analizando adaptadores de red...
[OK] Adaptadores de red
[OK] Información básica
[----]
[INFO] Analizar centro de seguridad...

David Martinez 2ASIR

Informe Lynis

#[1;37m[Lynis 3.1.3]#[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.

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

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

#####

[+] #[1;33mInitializing program#[0m

#[1;37m

#####

```
#                                     #
# #[0;35mNON-PRIVILEGED SCAN MODE#[1;37m          #
#                                     #
#####
```

#[0m

#[1;33mNOTES:#[0m

#[1;37m*#[0m Some tests will be skipped (as they require root permissions)

#[1;37m*#[0m Some tests might fail silently or give different results

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

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

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

#[4CTranslation file (db/languages/es) needs an update#[7C [#[1;31mOUTDATED#[0m]

#[4C=====

====#[0C

#[4CHelp other users and translate the missing lines:#[8C

#[4C1) Go to: <https://github.com/CISOfy/lynis/edit/master/db/languages/es>#[0C

#[4C2) Translate (some of) the lines starting with a hash (#) and remove the leading hash#[0C

#[4C3) Commit the changes#[36C

#[4CThank you!#[47C

#[4CNote: no lines with a hash? Look if the file recently has been changed by another translator.#[0C

#[4C=====

====#[0C

Program version: 3.1.3
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 24.04
Kernel version: 6.8.0

David Martinez 2ASIR

Hardware platform: x86_64
Hostname: david-VirtualBox

Profiles: /home/david/lynis/default.prf
Log file: /home/david/lynis.log
Report file: /home/david/lynis-report.dat
Report version: 1.0
Plugin directory: ./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;37mpam#[0m#[24C
[..
#[2C- #[0;36mPlugin#[0m: #[1;37msystemd#[0m#[20C
[.....]

[+] #[1;33mArranque y servicios#[0m

#[2C- Service Manager#[42C [#[1;32msystemd#[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 30 running services#[20C
#[2C- Check enabled services at boot (systemctl)#[15C [#[1;32mHECHO#[0m]
#[8CResult: found 55 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- colord.service:#[36C [#[1;32mPROTEGIDO#[0m]
#[8C- cron.service:#[38C [#[1;31mINSEGURO#[0m]
#[8C- cups-browsed.service:#[30C [#[1;31mINSEGURO#[0m]

David Martinez 2ASIR

```
#[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- fwupd.service:#[37C [ #[1;33mEXPUESTO#[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- networkd-dispatcher.service:#[23C [ #[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- whoopsie.service:#[34C [ #[1;31mINSEGURO#[0m ]
#[8C- wpa_supplicant.service:#[28C [ #[1;31mINSEGURO#[0m ]
```


[+] #1;33mKernel#[0m

#2C- Checking default runlevel#[32C [#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 61 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- Unique group IDs#[41C [#1;32mOK#[0m]
#2C- Unique group names#[39C [#1;32mOK#[0m]
#2C- Password file consistency#[32C [#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]
#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;32mOK#[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]

David Martinez 2ASIR

#[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;33mKerberos#[0m

#[2C- Check for Kerberos KDC and principals#[20C [#[1;37mNO ENCONTRADO#[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;32mOK#[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- 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:5 noexec:19 nosuid:13 ro or noexec (W^X): 9 of total 35#[0C

#[2C- JBD driver is not loaded#[33C [#[1;33mNECESITA VERIFICACIÓN#[0m]

#[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]

David Martinez 2ASIR

[+] #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 upgradeable packages#[28C [#1;37mOMITIDO#[0m]
#[2C- Checking package audit tool#[30C [#1;31mNINGUNO#[0m]
#[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 [#1;37mNOT ACTIVE#[0m]
#[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]

David Martinez 2ASIR

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

[+] #1;33mSoftware: firewalls#[0m

#2C- Checking iptables kernel module#[26C [#1;32mENCONTRADO#[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]

#4C- Checking wazuh-agent daemon status#[21C [#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]

David Martinez 2ASIR

#[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 [#[1;32mNOT ACTIVE#[0m]
#[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;32m335s#[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: 19.757921 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]

David Martinez 2ASIR

[+] #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;33mDESCONOCIDO#[0m]
#[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;33mNINGUNO#[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: /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]

David Martinez 2ASIR

[+] #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: 2 3 4)#[16C [#1;32mOK#[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.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]

David Martinez 2ASIR

#[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

#[2C- Plugins (phase 2)#[40C [#[1;32mHECHO#[0m]

=====

-[#[1;37mLynis 3.1.3 Results#[0m]-

#[1;32mGreat, no warnings#[0m

#[1;33mSuggestions#[0m (35):

#[1;37m-----#[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;37m<https://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;37m<https://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;37m<https://cisofy.com/lynis/controls/KRNL-5820/>#[0m

#[1;33m*#[0m Run pwck manually and correct any errors in the password file [AUTH-9228]

#[0;37m<https://cisofy.com/lynis/controls/AUTH-9228/>#[0m

#[1;33m*#[0m Configure password hashing rounds in /etc/login.defs [AUTH-9230]

#[0;37m<https://cisofy.com/lynis/controls/AUTH-9230/>#[0m

#[1;33m*#[0m Configure minimum password age in /etc/login.defs [AUTH-9286]

#[0;37m<https://cisofy.com/lynis/controls/AUTH-9286/>#[0m

#[1;33m*#[0m Configure maximum password age in /etc/login.defs [AUTH-9286]

#[0;37m<https://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;37m<https://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;37m<https://cisofy.com/lynis/controls/FILE-6310/>#[0m

David Martinez 2ASIR

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

- Details : #[0;36mSince boot-time, you have not been using any filesystems with journaling. Alternatively, reason could be driver is blacklisted.#[0m

#[0;37mhttps://cisofy.com/lynis/controls/FILE-6398/#[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 Install a package audit tool to determine vulnerable packages [PKGS-7398]

#[0;37mhttps://cisofy.com/lynis/controls/PKGS-7398/#[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]

David Martinez 2ASIR

```
#[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 Check output of aa-status [MACF-6208]
- Details : #[0;36m/sys/kernel/security/apparmor/profiles#[0m
- Solution : Run aa-status
#[0;37mhttps://cisofy.com/lynis/controls/MACF-6208/#[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, Wazuh
#[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 /home/david/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;37m250#[0m

#[0;36mPlugins enabled#[0m : #[1;37m2#[0m

#[1;37mComponents#[0m:

- Firewall [#[1;32mV#[0m]
- Malware scanner [#[1;31mX#[0m]

#[1;33mScan mode#[0m:

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

#[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/home/david/lynis.log#[0m
- Report data : #[1;37m/home/david/lynis-report.dat#[0m

=====

#[0;35mPruebas omitidas, debido a que el modo no privilegiado está activo#[0m

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

=====

David Martinez 2ASIR

#[1;37mLynis#[0m 3.1.3

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

2007-2024, 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
/home/david/lynis/default.prf for all settings)#[0m

Centro Criptológico Nacional



Nombre del sistema:
DESKTOP-L06B0TD
Organización: IES El Bohio
Unidad: ASIR
Categoría del sistema: ALTA

Auditado por David Martínez
Informes generados el día 11/10/2024 18:03:29 UTC
Versión de CLARA: 2.0
0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74

Ocultar todo

Resumen			Ocultar
Cumplimiento del sistema - 40,23%			
Sistema			Ocultar
Nombre del sistema	DESKTOP-L06B0TD		
Sistema operativo	Microsoft Windows 10 Pro (No hay Service Pack instalado / Internet Explorer: 11.630.19041.0 / Windows Media Player: 12.0.19041.4522)		
Rol del dominio	Cliente independiente		
Dominio / Grupo de trabajo	WORKGROUP		
Discos	C: (NTFS) / D: (Desconocido)		
Direcciones IP	10.0.2.15		
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 (33,33%)

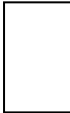
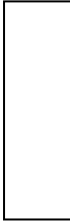
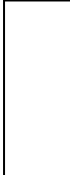
MP.EQ.2 - Bloqueo de puesto de trabajo (0%)

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




* Cumplimiento de las medidas técnicas del ENS en función del nivel analizado para este sistema.

** 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.

Leyenda de estado del control

	Cumplimiento satisfactorio del control. No es necesario realizar ninguna acción.
	Cumplimiento parcial del control. Es necesaria la revisión del informe técnico.
	Incumplimiento del control. Implica la revisión del informe técnico y la aplicación de medidas correctoras para su subsanación.

Leyenda de cumplimiento del control

	Representación visual del porcentaje de elementos del sistema que cumplen satisfactoriamente con el control ENS evaluado.
	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.
	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:
DESKTOP-L06B0TD
Organización: IES El Bohio
Unidad: ASIR
Categoría del sistema: ALTA

Auditado por David Martínez
Informes generados el día 11/10/2024 18:03:29 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	DESKTOP-L06B0TD	
Modelo	VirtualBox	
Fabricante	innotek GmbH	
Descripción	AT/AT COMPATIBLE	
Nombre del propietario	david	
Tipo de sistema	x64-based PC	
Memoria física	4,99 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 49,45 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 10 Pro
Servidor No
Instalación core No
Directorio del sistema C:\Windows\system32
Organización
Versión 10.0.19042
Versión de Service Pack No hay Service Pack instalado
Versión de Internet Explorer 11.630.19041.0
Versión de Windows Media Player 12.0.19041.4522
Número de compilación 19042
Usuario registrado david
Número de serie 00330-80000-00000-AA842
Último arranque 11/10/2024 19:32:39

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	08:00:27:3F:96:42	
DHCP	Sí	
IP	10.0.2.15 - fe80::180:b323:64e8:c7e1 - fd00::fd6b:a594:8a51:90b6 - fd00::180:b323:64e8:c7e1	
Subred	255.255.255.0 / 64 / 128 / 64	
Puerta de enlace predeterminada	10.0.2.2 - fe80::2	
Orden de búsqueda servidor DNS	10.0.2.3	
Servidor primario WINS		
Servidor secundario WINS		

Análisis ENS		Ocultar
Resultados		
Valor de criticidad	Cumplimiento (40,23%)	

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	No configurado	Forzar denegación	No configurado

aplicación/Permitir que las aplicaciones de Windows tengan acceso a los contactos			rado
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 los 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 (33,33%)	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/SmartScreen de Windows Defender/Explorador/Configurar SmartScreen de Windows Defender	No configurado	Habilitada	No configurado
Configuración del equipo/Componentes de Windows/SmartScreen de Windows Defender/Explorador/Configurar SmartScreen de Windows Defender/Opciones si está habilitado	No configurado	Advertir e impedir la omisión	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	No configurado	AES-CBC 256 bits	No configurado

posteriores). Método de cifrado de las unidades de datos extraíbles:

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 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 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: 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 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 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	No configurado	Deshabilitada	No configurado

BitLocker/Unidades del sistema operativo/Configurar perfil de validación de plataforma del TPM.PCR 23: Reservado para uso futuro

(*)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



prueba

Sun, 06 Oct 2024 19:01:29 Romance Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.15

Vulnerabilities by Host

Collapse All | Expand All

10.0.2.15



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	57608	SMB Signing not required
INFO	N/A	-	-	46180	Additional DNS Hostnames
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	-	-	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	-	-	46215	Inconsistent Hostname and IP Address
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	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
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



escaneo linux

Tue, 15 Oct 2024 14:14:55 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

- 10.0.2.15

Vulnerabilities by Host

Collapse All | Expand All

10.0.2.15



Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
HIGH	7.8	6.7	-	208701	Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : libgsf vulnerabilities (USN-7062-1)
HIGH	5.3	4.7	-	208471	Ubuntu 24.04 LTS : cups-browsed vulnerability (USN-7042-2)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.9	4.4	-	208758	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Ubuntu Advantage Desktop Daemon vulnerability (USN-7063-1)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	-	55472	Device Hostname
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	-	170170	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	-	179200	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	-	168980	Enumerate the PATH Variables
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses

INFO	N/A	-	-	168982	Filepaths contain Dangerous characters (Linux)
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	-	-	171410	IP Assignment Method Detection
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	200214	Libndp Installed (Linux / Unix)
INFO	N/A	-	-	157358	Linux Mounted Devices
INFO	N/A	-	-	193143	Linux Time Zone Information
INFO	N/A	-	-	95928	Linux User List Enumeration
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	-	-	117887	OS Security Patch Assessment Available
INFO	N/A	-	-	168007	OpenSSL Installed (Linux)
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	22869	Software Enumeration (SSH)
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110095	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
INFO	N/A	-	-	163326	Tenable Nessus Installed (Linux)
INFO	N/A	-	-	56468	Time of Last System Startup
INFO	N/A	-	-	192709	Tukaani XZ Utils Installed (Linux / Unix)
INFO	N/A	-	-	198218	Ubuntu Pro Subscription Detection
INFO	N/A	-	-	83303	Unix / Linux - Local Users Information : Passwords Never Expire

INFO	N/A	-	-	110483	Unix / Linux Running Processes Information
INFO	N/A	-	-	152743	Unix Software Discovery Commands Not Available
INFO	N/A	-	-	189731	Vim Installed (Linux)
INFO	N/A	-	-	198234	gnome-shell Installed (Linux / UNIX)
INFO	N/A	-	-	204828	libexiv2 Installed (Linux / Unix)
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

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

Hide