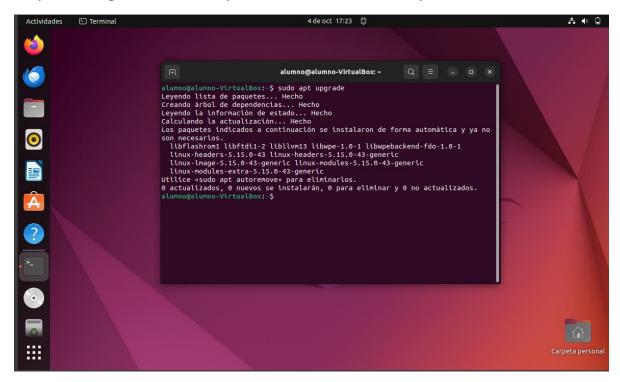
AUDITORÍA DEL SISTEMA

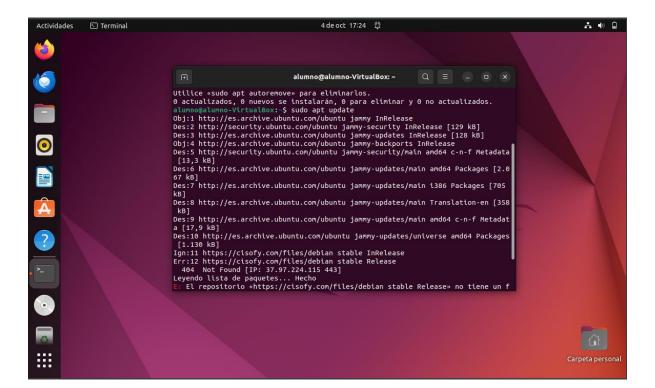
Indice

Instalación de Lynis	3
•	
Instalación de Clara	
Instalación Nessus (Ubuntu)	
,	
nstalación Nessus(Windows)	10

Instalación de Lynis

En primer lugar vamos a empezar actualizando la maquina.

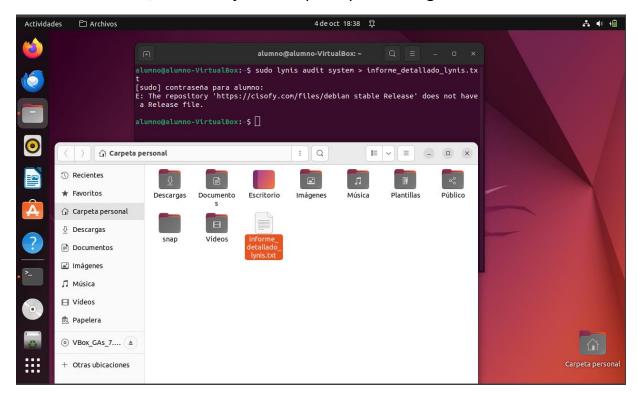




Ahora vamos a instalar el Lynis



Una vez instalado, vamos a ejecutarlo para que nos haga el informe

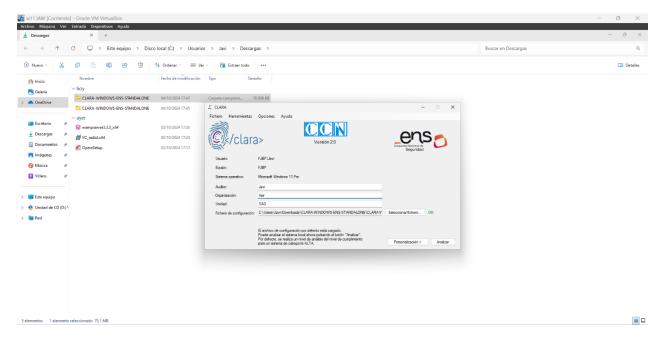


Instalación de Clara

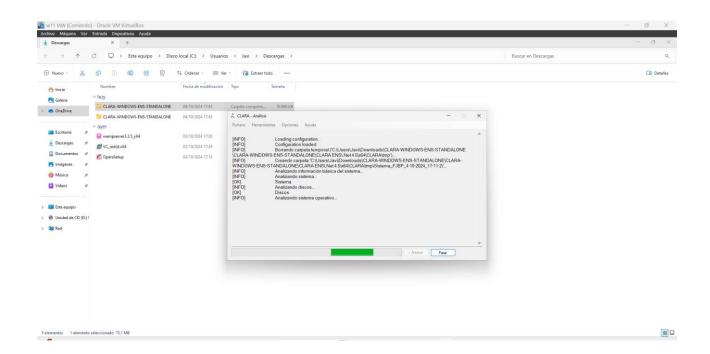
Vamos a descargar Clara desde el siguiente link:

https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html

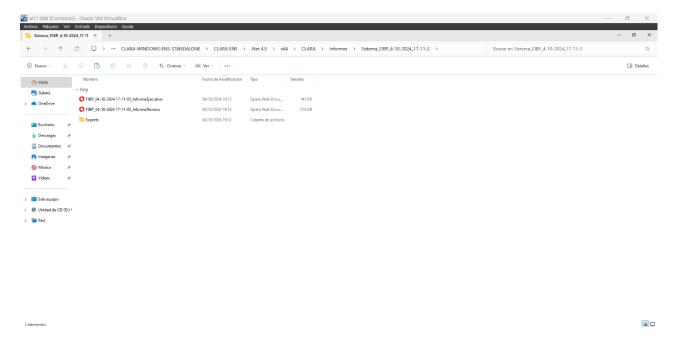
Una vez descargado, vamos a extraer el fichero y vamos a ejecutar el .exe, aparecerá la siguiente pantalla y ponemos los datos necesarios.



Una vez rellenado, le daremos a "Analizar".

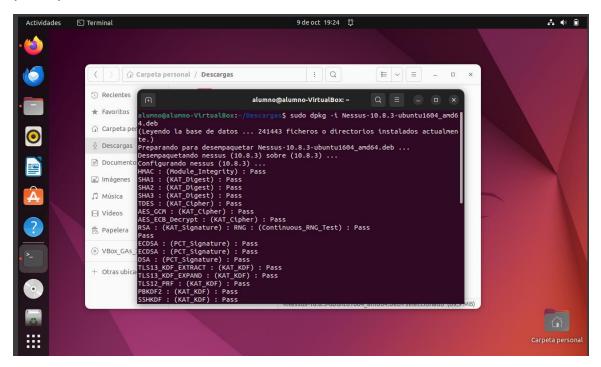


Y se guardaran los informes en una carpeta.



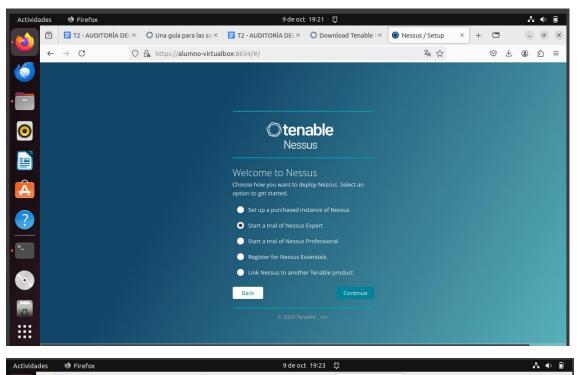
Instalación Nessus (Ubuntu)

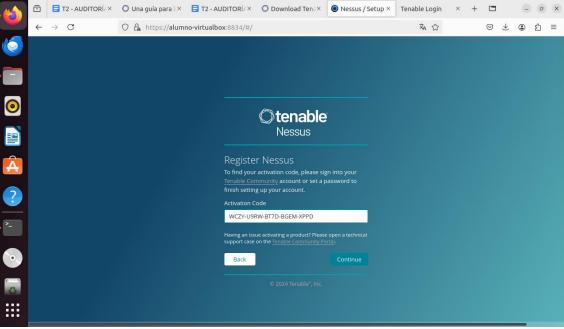
Primer lugar vamos a instalar Nessus y luego vamos a iniciar el servicio para que funcione.



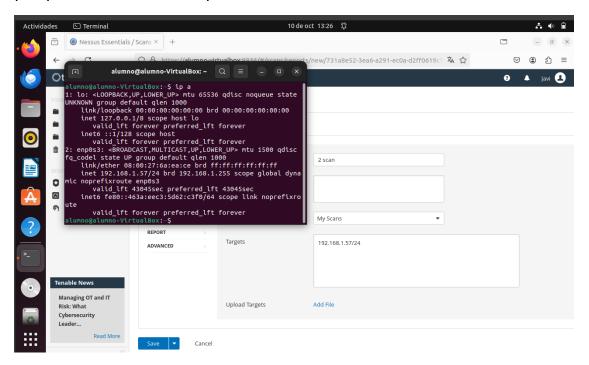
```
AKDF: (KAT_KDF): Pass
SSKDF: (KAT_KDF): Pass
K963KDF: (KAT_KDF): Pass
K963KDF: (KAT_KDF): Pass
K942KDF: (KAT_KDF): Pass
HASH: (DRBG): Pass
HASH: (DRBG): Pass
HASH: (DRBG): Pass
HAC: (DRBG): Pass
HMAC: (DRBG): Pass
HMAC: (DRBG): Pass
HMAC: (MAT_KA): Pass
RSA_Encrypt: (KAT_AsymmetricCipher): Pass
RSA_Decrypt: (KAT_Asymmetric
```

Ahora entramos en nuestro navegador y ponemos "localhost" y aparecerá lo siguiente:

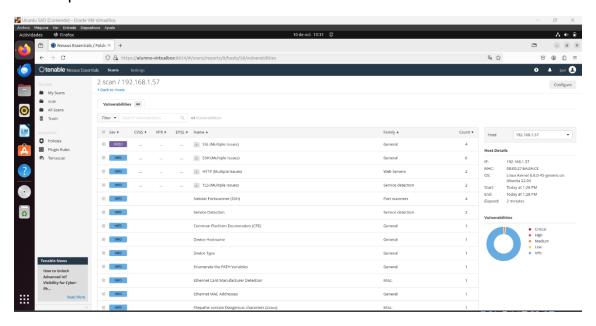




Una vez dentro esperaremos a que se instalen los plugins y una vez actualizados le daremos a "New Scan". Miramos la ip de nuestro equipo porque la necesitaremos para el informe.



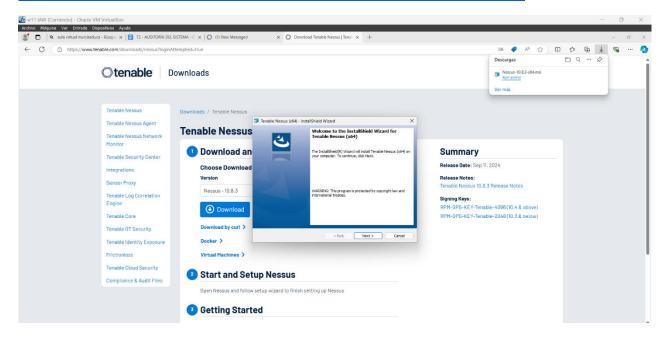
Así se quedaría el informe.

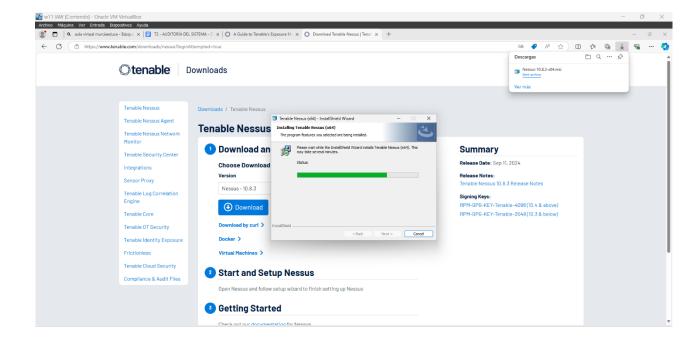


Instalación Nessus(Windows)

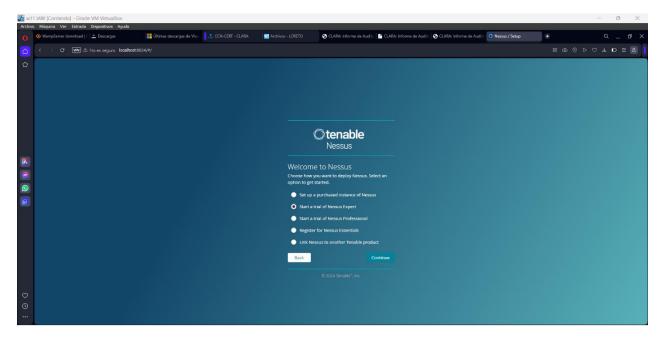
Vamos a descargarnos Nessus desde el siguiente enlace:

https://www.tenable.com/tenable-for-education/nessus-essentials

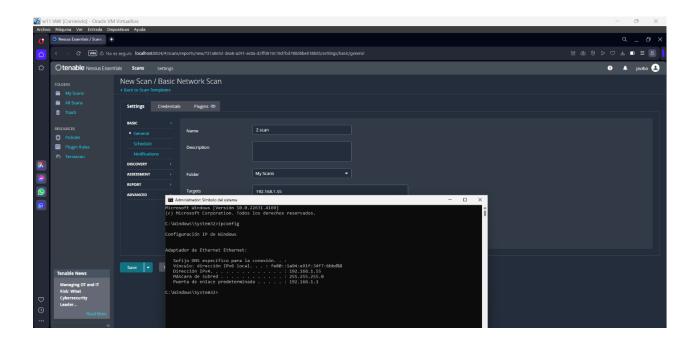




Una vez instalado es el mismo procedimiento que en Ubuntu



Una vez dentro esperaremos a que se instalen los plugins y una vez actualizados le daremos a "New Scan". Miramos la ip de nuestro equipo porque la necesitaremos para el informe.



Y con esto ya tendríamos todos los programas instalados y los informes hechos.

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

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

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

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

Program version: 3.0.7
Operating system: Linux
Operating system name: Ubuntu
Operating system version: 22.04
Kernel version: 6.8.0
Hardware platform: x86 64

Hostname: alumno-VirtualBox

Profiles: /etc/lynis/default.prf Log file: /var/log/lynis.log

Report file: /var/log/lynis-report.dat

Report version: 1.0

Plugin directory: /etc/lynis/plugins

Auditor: [Not Specified]

Language: es Test category: all Test group: all

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

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

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

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

[+] #[1;35mPlugins (fase 1)#[0m

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

#[0C #[0C

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

L

```
[+] #[1:33mDebian Tests#[0m
#[2C- Checking for system binaries that are required by Debian Tests...#[0C
#[4C- Checking /bin... #[38C [ #[1;32mFOUND#[0m ]
#[4C- Checking /sbin... #[37C [ #[1;32mFOUND#[0m ]
#[4C- Checking /usr/bin... #[34C [ #[1;32mFOUND#[0m ]
#[4C- Checking /usr/sbin... #[33C [ #[1;32mFOUND#[0m ]
#[4C- Checking /usr/local/bin... #[28C [ #[1;32mFOUND#[0m ]
#[4C- Checking /usr/local/sbin... #[27C [ #[1;32mFOUND#[0m ]
#[2C- Authentication:#[42C
#[4C- PAM (Pluggable Authentication Modules):#[16C
#[6C- libpam-tmpdir#[40C [ #[1;31mNot Installed#[0m ]
#[2C- File System Checks:#[38C
#[4C- DM-Crypt, Cryptsetup & Cryptmount:#[21C
#[2C- Software:#[48C
#[4C- apt-listbugs#[43C [ #[1;31mNot Installed#[0m ]
#[4C- apt-listchanges#[40C [ #[1;31mNot Installed#[0m ]
#[4C- needrestart#[44C [ #[1;31mNot Installed#[0m ]
#[4C- fail2ban#[47C [ #[1;31mNot Installed#[0m ]
[+] #[1;33mArranque y servicios#[0m
#[2C- Service Manager#[42C [ #[1;32msystemd#[0m ]
#[2C- Checking UEFI boot#[39C [ #[1;37mDESHABILITADO#[0m ]
#[2C- Checking presence GRUB2#[34C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking for password protection#[23C [ #[1;31mNINGUNO#[0m ]
#[2C- Check running services (systemctl)#[23C [ #[1;32mHECHO#[0m ]
#[8CResult: found 33 running services#[20C
#[2C- Check enabled services at boot (systemctl)#[15C [ #[1;32mHECHO#[0m ]
#[8CResult: found 51 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- acpid.service:#[37C [ #[1;31mINSEGURO#[0m ]
#[8C- alsa-state.service:#[32C [ #[1:31mINSEGURO#[0m ]
#[8C- anacron.service:#[35C [ #[1;31mINSEGURO#[0m ]
#[8C- apport.service:#[36C [ #[1;31mINSEGURO#[0m ]
#[8C- avahi-daemon.service:#[30C [ #[1;31mINSEGURO#[0m ]
#[8C- colord.service:#[36C [ #[1;33mEXPUESTO#[0m ]
#[8C- cron.service:#[38C [ #[1;31mINSEGURO#[0m ]
#[8C- cups-browsed.service:#[30C [ #[1;31mINSEGURO#[0m ]
#[8C- cups.service:#[38C [ #[1;31mINSEGURO#[0m ]
#[8C- dbus.service:#[38C [ #[1;31mINSEGURO#[0m ]
#[8C- dmesg.service:#[37C [ #[1;31mINSEGURO#[0m ]
#[8C- emergency.service:#[33C [ #[1;31mINSEGURO#[0m ]
#[8C- gdm.service:#[39C [ #[1;31mINSEGURO#[0m ]
#[8C- geoclue.service:#[35C [ #[1;33mEXPUESTO#[0m ]
#[8C- getty@tty1.service:#[32C [ #[1;31mINSEGURO#[0m ]
```

#[8C- irgbalance.service:#[32C [#[1;37mMEDIO#[0m]

```
#[8C- kerneloops.service:#[32C [ #[1:31mINSEGURO#[0m ]
#[8C-lynis.service:#[37C [ #[1;31mINSEGURO#[0m ]
#[8C- networkd-dispatcher.service:#[23C [ #[1;31mINSEGURO#[0m ]
#[8C- open-vm-tools.service:#[29C [ #[1;31mINSEGURO#[0m ]
#[8C- packagekit.service:#[32C [ #[1;31mINSEGURO#[0m ]
#[8C-plymouth-start.service:#[28C [ #[1;31mINSEGURO#[0m ]
#[8C- polkit.service:#[36C [ #[1;31mINSEGURO#[0m ]
#[8C- power-profiles-daemon.service:#[21C [ #[1;33mEXPUESTO#[0m ]
#[8C- rc-local.service:#[34C [ #[1;31mINSEGURO#[0m ]
#[8C- rescue.service:#[36C [ #[1;31mINSEGURO#[0m ]
#[8C-rsyslog.service:#[35C [ #[1;31mINSEGURO#[0m ]
#[8C- rtkit-daemon.service:#[30C [ #[1;37mMEDIO#[0m ]
#[8C- snapd.service:#[37C [ #[1;31mINSEGURO#[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-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-udevd.service:#[29C [ #[1;37mMEDIO#[0m ]
#[8C- thermald.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- uuidd.service:#[37C [ #[1;32mPROTEGIDO#[0m ]
#[8C-vboxadd-service.service:#[27C [ #[1;31mINSEGURO#[0m ]
#[8C- vgauth.service:#[36C [ #[1;31mINSEGURO#[0m ]
#[8C- whoopsie.service:#[34C [ #[1;31mINSEGURO#[0m ]
#[8C- wpa_supplicant.service:#[28C [ #[1;31mINSEGURO#[0m ]
[+] #[1;33mKernel#[0m
#[2C- Checking default run level#[31C [ #[1:32mRUNLEVEL 5#[0m ]
#[2C- Checking CPU support (NX/PAE)#[28C
#[4CCPU support: PAE and/or NoeXecute supported#[14C [ #[1;32mENCONTRADO#[0m ]
#[2C- Checking kernel version and release#[22C [ #[1;32mHECHO#[0m ]
#[2C- Checking kernel type#[37C [ #[1;32mHECHO#[0m ]
#[2C- Checking loaded kernel modules#[27C [ #[1;32mHECHO#[0m ]
#[6CFound 66 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#[27C [ #[1;37mPOR DEFECTO#[0m ]
#[4C- 'hard' configuration in security/limits.conf#[11C [ #[1;37mPOR DEFECTO#[0m ]
#[4C- 'soft' configuration in security/limits.conf#[11C [ #[1;37mPOR DEFECTO#[0m ]
#[4C- Checking setuid core dumps configuration#[15C [ #[1;37mPROTEGIDO#[0m ]
#[2C- Check if reboot is needed#[32C [ #[1;32mNO#[0m ]
[+] #[1;33mMemoria y procesos#[0m
#[2C- Checking /proc/meminfo#[35C [ #[1;32mENCONTRADO#[0m ]
#[2C- Searching for dead/zombie processes#[22C [ #[1;32mNO ENCONTRADO#[0m ]
#[2C- Searching for IO waiting processes#[23C [ #[1;32mNO ENCONTRADO#[0m ]
#[2C- Search prelink tooling#[35C [ #[1;32mNO ENCONTRADO#[0m ]
[+] #[1;33mUsuarios, grupos y autenticación#[0m
#[2C- Administrator accounts#[35C [ #[1;32mOK#[0m ]
#[2C- Unique UIDs#[46C [ #[1;32mOK#[0m ]
#[2C- Consistency of group files (grpck)#[23C [ #[1;32mOK#[0m ]
#[2C- Unique group IDs#[41C [ #[1;32mOK#[0m ]
#[2C- Unique group names#[39C [ #[1;32mOK#[0m ]
#[2C- Password file consistency#[32C [ #[1;32mOK#[0m ]
#[2C- Password hashing methods#[33C [ #[1;32mOK#[0m ]
#[2C- Checking password hashing rounds#[25C [ #[1;33mDESHABILITADO#[0m ]
#[2C- Query system users (non daemons)#[25C [ #[1;32mHECHO#[0m ]
#[2C- NIS+ authentication support#[30C [ #[1;37mNO HABILITADO#[0m ]
#[2C- NIS authentication support#[31C [ #[1;37mNO HABILITADO#[0m ]
#[2C- Sudoers file(s)#[42C [ #[1;32mENCONTRADO#[0m ]
#[4C- Permissions for directory: /etc/sudoers.d#[14C [ #[1;31mPELIGRO#[0m ]
#[4C- Permissions for: /etc/sudoers#[26C [ #[1;32mOK#[0m ]
#[4C- Permissions for: /etc/sudoers.d/README#[17C [ #[1;32mOK#[0m ]
#[2C- PAM password strength tools#[30C [ #[1;32mOK#[0m ]
#[2C- PAM configuration files (pam.conf)#[23C [ #[1;32mENCONTRADO#[0m ]
#[2C- PAM configuration files (pam.d)#[26C [ #[1;32mENCONTRADO#[0m ]
#[2C- PAM modules#[46C [ #[1;32mENCONTRADO#[0m ]
#[2C- LDAP module in PAM#[39C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Accounts without expire date#[29C [ #[1;33mSUGERENCIA#[0m ]
#[2C- Accounts without password#[32C [ #[1;32mOK#[0m ]
#[2C- Locked accounts#[42C [ #[1;32mOK#[0m ]
#[2C- Checking user password aging (minimum)#[19C [ #[1;33mDESHABILITADO#[0m ]
#[2C- User password aging (maximum)#[28C [ #[1;33mDESHABILITADO#[0m ]
#[2C- Checking expired passwords#[31C [ #[1;32mOK#[0m ]
#[2C- Checking Linux single user mode authentication#[11C [ #[1;32mOK#[0m ]
#[2C- Determining default umask#[32C
#[4C- umask (/etc/profile)#[35C [ #[1;33mNO ENCONTRADO#[0m ]
#[4C- umask (/etc/login.defs)#[32C [ #[1;33mSUGERENCIA#[0m ]
#[2C- LDAP authentication support#[30C [ #[1;37mNO HABILITADO#[0m ]
#[2C- Logging failed login attempts#[28C [ #[1;32mHABILITADO#[0m ]
```

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

#[2C- Checking shells from /etc/shells#[25C

```
#[4CResult: found 8 shells (valid shells: 8).#[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- ACL support root file system#[29C [ #[1;32mHABILITADO#[0m ]
#[2C- Mount options of /#[39C [ #[1;33mNO POR DEFECTO#[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:7 noexec:25 nosuid:19 ro or noexec (W\X): 10 of total 42#[0C
#[2C- Disable kernel support of some filesystems#[15C
[+] #[1;33mDispositivos USB#[0m
#[2C- Checking usb-storage driver (modprobe config)#[12C [ #[1;37mNO
DESHABILITADO#[0m]
#[2C- Checking USB devices authorization#[23C [ #[1;33mHABILITADO#[0m ]
#[2C- Checking USBGuard#[40C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mAlmacenamiento#[0m
#[2C- Checking firewire ohci driver (modprobe config)#[10C [ #[1;32mDESHABILITADO#[0m ]
[+] #[1;33mNFS#[0m
#[2C- Check running NFS daemon#[33C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1:33mServicios de nombres#[0m
#[2C- Checking search domains#[34C [ #[1;32mENCONTRADO#[0m ]
#[2C- Checking /etc/resolv.conf options#[24C [ #[1;32mENCONTRADO#[0m ]
#[2C- Searching DNS domain name#[32C [ #[1;33mDESCONOCIDO#[0m ]
#[2C- Checking /etc/hosts#[38C
#[4C- Duplicate entries in hosts file#[24C [ #[1;32mNINGUNO#[0m ]
#[4C- Presence of configured hostname in /etc/hosts#[10C [ #[1;32mENCONTRADO#[0m ]
#[4C- Hostname mapped to localhost#[27C [ #[1;32mNO ENCONTRADO#[0m ]
#[4C- Localhost mapping to IP address#[24C [ #[1;32mOK#[0m ]
```

```
[+] #[1;33mPuertos y paquetes#[0m
#[2C- Searching package managers#[31C
#[4C- Searching dpkg package manager#[25C [ #[1;32mENCONTRADO#[0m ]
#[6C- Querying package manager#[29C
#[4C- Query unpurged packages#[32C [ #[1;32mNINGUNO#[0m ]
#[2C- Checking security repository in sources.list file#[8C [ #[1;32mOK#[0m ]
#[2C- Checking APT package database#[28C [ #[1;32mOK#[0m ]
#[2C- Checking vulnerable packages#[29C [ #[1;32mOK#[0m ]
#[2C- Checking upgradeable packages#[28C [ #[1;37mOMITIDO#[0m ]
#[2C- Checking package audit tool#[30C [ #[1;32mINSTALADO#[0m ]
#[4CFound: apt-check#[41C
#[2C- Toolkit for automatic upgrades (unattended-upgrade)#[6C [ #[1;32mENCONTRADO#[0m ]
[+] #[1;33mConectividad#[0m
#[2C- Checking IPv6 configuration#[30C [ #[1;37mHABILITADO#[0m ]
#[6CConfiguration method#[35C [ #[1;37mAUTO#[0m ]
#[6CIPv6 only#[46C [ #[1;37mNO#[0m ]
#[2C- Checking configured nameservers#[26C
#[4C- Testing nameservers#[36C
#[8CNameserver: 127.0.0.53#[31C [ #[1;32mOK#[0m ]
#[4C- DNSSEC supported (systemd-resolved)#[20C [ #[1;33mNO#[0m ]
#[2C- Getting listening ports (TCP/UDP)#[24C [ #[1;32mHECHO#[0m ]
#[2C- Checking promiscuous interfaces#[26C [ #[1;32mOK#[0m ]
#[2C- Checking status DHCP client#[30C
#[2C- Checking for ARP monitoring software#[21C [ #[1;33mNO ENCONTRADO#[0m ]
#[2C- Uncommon network protocols#[31C [ #[1;33m0#[0m ]
[+] #[1;33mImpresoras y spools#[0m
_____
#[2C- Checking cups daemon#[37C [ #[1;32mCORRIENDO#[0m ]
#[2C- Checking CUPS configuration file#[25C [ #[1;32mOK#[0m ]
#[4C- File permissions#[39C [ #[1;31mPELIGRO#[0m ]
#[2C- Checking CUPS addresses/sockets#[26C [ #[1;32mENCONTRADO#[0m ]
#[2C- Checking lp daemon#[39C [ #[1;37mNO ESTÁ CORRIENDO#[0m ]
[+] #[1:33mSoftware: correo electrónico y mensajería#[0m
[+] #[1;33mSoftware: firewalls#[0m
#[2C- Checking iptables kernel module#[26C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking iptables policies of chains#[19C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking for empty ruleset#[29C [ #[1;31mPELIGRO#[0m ]
#[4C- Checking for unused rules#[30C [ #[1;32mOK#[0m ]
#[2C- Checking host based firewall#[29C [ #[1;32mACTIVO#[0m ]
[+] #[1;33mSoftware: servidor web#[0m
#[2C- Checking Apache#[42C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Checking nginx#[43C [ #[1;37mNO ENCONTRADO#[0m ]
```

```
[+] #[1;33mSoporte SSH#[0m
#[2C- Checking running SSH daemon#[30C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mSoporte SNMP#[0m
#[2C- Checking running SNMP daemon#[29C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mBases de datos#[0m
-----
#[4CNo database engines found#[32C
[+] #[1;33mServicios LDAP#[0m
_____
#[2C- Checking OpenLDAP instance#[31C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mPHP#[0m
#[2C- Checking PHP#[45C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mSoporte Squid#[0m
#[2C- Checking running Squid daemon#[28C [ #[1;37mNO ENCONTRADO#[0m ]
[+] #[1;33mLogging y ficheros#[0m
#[2C- Checking for a running log daemon#[24C [ #[1;32mOK#[0m ]
#[4C- Checking Syslog-NG status#[30C [ #[1;37mNO ENCONTRADO#[0m ]
#[4C- Checking systemd journal status#[24C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking Metalog status#[32C [ #[1;37mNO ENCONTRADO#[0m ]
#[4C- Checking RSyslog status#[32C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking RFC 3195 daemon status#[24C [ #[1;37mNO ENCONTRADO#[0m ]
#[4C- Checking minilogd instances#[28C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Checking logrotate presence#[30C [ #[1;32mOK#[0m ]
#[2C- Checking remote logging#[34C [ #[1;33mNO HABILITADO#[0m ]
#[2C- Checking log directories (static list)#[19C [ #[1;32mHECHO#[0m ]
#[2C- Checking open log files#[34C [ #[1;32mHECHO#[0m ]
#[2C- Checking deleted files in use#[28C [ #[1;33mARCHIVOS ENCONTRADOS#[0m ]
[+] #[1;33mServicios inseguros#[0m
#[2C- Installed inetd package#[34C [ #[1;32mNO ENCONTRADO#[0m ]
#[2C- Installed xinetd package#[33C [ #[1;32mOK#[0m ]
#[4C- xinetd status#[42C
#[2C- Installed rsh client package#[29C [ #[1;32mOK#[0m ]
#[2C- Installed rsh server package#[29C [ #[1;32mOK#[0m ]
#[2C- Installed telnet client package#[26C [ #[1;32mOK#[0m ]
#[2C- Installed telnet server package#[26C [ #[1;32mNO ENCONTRADO#[0m ]
#[2C- Checking NIS client installation#[25C [ #[1:32mOK#[0m ]
#[2C- Checking NIS server installation#[25C [ #[1;32mOK#[0m ]
#[2C- Checking TFTP client installation#[24C [ #[1;32mOK#[0m ]
```

```
[+] #[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;33mNO ENCONTRADO#[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;32m30s#[0m ]
[+] #[1;33mCriptografía#[0m
#[2C- Checking for expired SSL certificates [0/151]#[12C [ #[1;32mNINGUNO#[0m ]
#[30;43m[WARNING]#[0m: Test CRYP-7902 had a long execution: 15.183253 seconds#[0m
#[2C- Kernel entropy is sufficient#[29C [ #[1;32mSÍ#[0m ]
#[2C- HW RNG & rngd#[44C [ #[1;33mNO#[0m ]
#[2C- SW prng#[50C [ #[1;33mNO#[0m ]
#[2C- MOR variable not found#[35C [ #[1;37mDÉBIL#[0m ]
[+] #[1;33mVirtualización#[0m
_____
[+] #[1;33mContenedores#[0m
[+] #[1;33mFrameworks de seguridad#[0m
#[2C- Checking presence AppArmor#[31C [ #[1;32mENCONTRADO#[0m ]
#[4C- Checking AppArmor status#[31C [ #[1;32mHABILITADO#[0m ]
#[8CFound 124 unconfined processes#[23C
#[2C- Checking presence SELinux#[32C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Checking presence TOMOYO Linux#[27C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Checking presence grsecurity#[29C [ #[1;37mNO ENCONTRADO#[0m ]
#[2C- Checking for implemented MAC framework#[19C [ #[1;32mOK#[0m ]
```

#[2C- Checking TFTP server installation#[24C [#[1;32mOK#[0m]

```
[+] #[1:33mSoftware: integridad de ficheros#[0m
#[2C- Checking file integrity tools#[28C
#[2C- Checking presence integrity tool#[25C [ #[1;33mNO ENCONTRADO#[0m ]
[+] #[1;33mSoftware: Herramientas del sistema#[0m
#[2C- Checking automation tooling#[30C
#[2C- Automation tooling#[39C [ #[1;33mNO ENCONTRADO#[0m ]
#[2C- Checking for IDS/IPS tooling#[29C [ #[1;33mNINGUNO#[0m ]
[+] #[1;33mSoftware: Malware#[0m
 -----
#[2C- Malware software components#[30C [ #[1;33mNO ENCONTRADO#[0m ]
[+] #[1:33mPermisos de ficheros#[0m
#[2C- Starting file permissions check#[26C
#[4CFile: /boot/grub/grub.cfg#[32C [ #[1;33mSUGERENCIA#[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 ]
[+] #[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;32mOK#[0m ]
#[4C- kernel.ctrl-alt-del (exp: 0)#[27C [ #[1;32mOK#[0m ]
#[4C- kernel.dmesg_restrict (exp: 1)#[25C [ #[1;32mOK#[0m ]
```

```
#[4C- kernel.kptr_restrict (exp: 2)#[26C [ #[1;31mDIFERENTE#[0m ]
#[4C- kernel.modules disabled (exp: 1)#[23C [ #[1;31mDIFERENTE#[0m ]
#[4C- kernel.perf_event_paranoid (exp: 3)#[20C [ #[1;31mDIFERENTE#[0m ]
#[4C- kernel.randomize va space (exp: 2)#[21C [ #[1;32mOK#[0m ]
#[4C- kernel.sysrq (exp: 0)#[34C [ #[1;31mDIFERENTE#[0m ]
#[4C- kernel.unprivileged_bpf_disabled (exp: 1)#[14C [ #[1;31mDIFERENTE#[0m ]
#[4C- kernel.yama.ptrace_scope (exp: 1 2 3)#[18C [ #[1;32mOK#[0m ]
#[4C- net.core.bpf_jit_harden (exp: 2)#[23C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.all.accept redirects (exp: 0)#[12C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.all.accept_source_route (exp: 0)#[9C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.all.bootp_relay (exp: 0)#[17C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.all.forwarding (exp: 0)#[18C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.all.log_martians (exp: 1)#[16C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.all.mc forwarding (exp: 0)#[15C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.all.proxy_arp (exp: 0)#[19C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.all.rp_filter (exp: 1)#[19C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.all.send_redirects (exp: 0)#[14C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.default.accept_redirects (exp: 0)#[8C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.conf.default.accept source route (exp: 0)#[5C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.conf.default.log_martians (exp: 1)#[12C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)#[10C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)#[4C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.tcp_syncookies (exp: 1)#[23C [ #[1;32mOK#[0m ]
#[4C- net.ipv4.tcp_timestamps (exp: 0 1)#[21C [ #[1;32mOK#[0m ]
#[4C- net.ipv6.conf.all.accept_redirects (exp: 0)#[12C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv6.conf.all.accept source route (exp: 0)#[9C [ #[1;32mOK#[0m ]
#[4C- net.ipv6.conf.default.accept redirects (exp: 0)#[8C [ #[1;31mDIFERENTE#[0m ]
#[4C- net.ipv6.conf.default.accept_source_route (exp: 0)#[5C [ #[1;32mOK#[0m ]
[+] #[1;33mBastionado#[0m
#[4C- Installed compiler(s)#[34C [ #[1;32mNO ENCONTRADO#[0m ]
#[4C- Installed malware scanner#[30C [ #[1;31mNO ENCONTRADO#[0m ]
#[4C- Non-native binary formats#[30C [ #[1;31mENCONTRADO#[0m ]
[+] #[1;33mPruebas personalizadas#[0m
_____
#[2C- Running custom tests... #[33C [ #[1;37mNINGUNO#[0m ]
[+] #[1;35mPlugins (fase 2)#[0m
 -[ #[1;37mLynis 3.0.7 Results#[0m ]-
 #[1;31mWarnings#[0m (1):
 #[1;37m-----#[0m
 #[1;31m!#[0m iptables module(s) loaded, but no rules active [FIRE-4512]
   https://cisofy.com/lynis/controls/FIRE-4512/
```

- #[1;33mSuggestions#[0m (39):
- #[1;37m-----#[0m
- #[1;33m*#[0m This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]
 - #[0;37mhttps://cisofy.com/lynis/controls/LYNIS/#[0m
- #[1;33m*#[0m Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions [DEB-0280] #[0;37mhttps://cisofy.com/lynis/controls/DEB-0280/#[0m
- #[1;33m*#[0m Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
 - #[0;37mhttps://cisofy.com/lynis/controls/DEB-0810/#[0m
- #[1;33m*#[0m Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
 - #[0;37mhttps://cisofy.com/lynis/controls/DEB-0811/#[0m
- #[1;33m*#[0m Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]
 - #[0;37mhttps://cisofy.com/lynis/controls/DEB-0831/#[0m
- #[1;33m*#[0m Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
 - #[0;37mhttps://cisofy.com/lynis/controls/DEB-0880/#[0m
- #[1;33m*#[0m Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
 - #[0;37mhttps://cisofy.com/lynis/controls/BOOT-5122/#[0m
 - #[1;33m*#[0m Consider hardening system services [BOOT-5264]
 - Details: #[0;36mRun'/usr/bin/systemd-analyze security SERVICE' for each service#[0m#[0;37mhttps://cisofy.com/lynis/controls/BOOT-5264/#[0m
- #[1;33m*#[0m If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]
 - #[0;37mhttps://cisofy.com/lynis/controls/KRNL-5820/#[0m
 - #[1;33m*#[0m Configure password hashing rounds in /etc/login.defs [AUTH-9230] #[0;37mhttps://cisofy.com/lynis/controls/AUTH-9230/#[0m
 - #[1;33m*#[0m When possible set expire dates for all password protected accounts [AUTH-9282] #[0;37mhttps://cisofy.com/lynis/controls/AUTH-9282/#[0m
 - #[1;33m*#[0m Configure minimum password age in /etc/login.defs [AUTH-9286] #[0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/#[0m
 - #[1;33m*#[0m Configure maximum password age in /etc/login.defs [AUTH-9286] #[0;37mhttps://cisofy.com/lynis/controls/AUTH-9286/#[0m
 - #[1;33m*#[0m Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328] #[0;37mhttps://cisofy.com/lynis/controls/AUTH-9328/#[0m

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

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

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

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

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

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

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

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

#[1;33m*#[0m Check DNS configuration for the dns domain name [NAME-4028] #[0;37mhttps://cisofy.com/lynis/controls/NAME-4028/#[0m

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

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

- #[1;33m*#[0m Install package apt-show-versions for patch management purposes [PKGS-7394] #[0;37mhttps://cisofy.com/lynis/controls/PKGS-7394/#[0m
- #[1;33m*#[0m Determine if protocol 'dccp' is really needed on this system [NETW-3200] #[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/#[0m
- #[1;33m*#[0m Determine if protocol 'sctp' is really needed on this system [NETW-3200] #[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/#[0m
- #[1;33m*#[0m Determine if protocol 'rds' is really needed on this system [NETW-3200] #[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/#[0m
- #[1;33m*#[0m Determine if protocol 'tipc' is really needed on this system [NETW-3200] #[0;37mhttps://cisofy.com/lynis/controls/NETW-3200/#[0m
- #[1;33m*#[0m Access to CUPS configuration could be more strict. [PRNT-2307] #[0;37mhttps://cisofy.com/lynis/controls/PRNT-2307/#[0m
- #[1;33m*#[0m Check CUPS configuration if it really needs to listen on the network [PRNT-2308] #[0;37mhttps://cisofy.com/lynis/controls/PRNT-2308/#[0m
- #[1;33m*#[0m Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

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

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

```
#[1;33m*#[0m Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
   #[0;37mhttps://cisofy.com/lynis/controls/BANN-7126/#[0m
 #[1;33m*#[0m Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
   #[0;37mhttps://cisofy.com/lynis/controls/BANN-7130/#[0m
 #[1;33m*#[0m Enable process accounting [ACCT-9622]
   #[0;37mhttps://cisofy.com/lynis/controls/ACCT-9622/#[0m
 #[1;33m*#[0m Enable sysstat to collect accounting (no results) [ACCT-9626]
   #[0;37mhttps://cisofy.com/lynis/controls/ACCT-9626/#[0m
 #[1;33m*#[0m Enable auditd to collect audit information [ACCT-9628]
   #[0;37mhttps://cisofy.com/lynis/controls/ACCT-9628/#[0m
 #[1;33m*#[0m Install a file integrity tool to monitor changes to critical and sensitive files [FINT-
4350]
   #[0;37mhttps://cisofy.com/lynis/controls/FINT-4350/#[0m
 #[1;33m*#[0m Determine if automation tools are present for system management [TOOL-5002]
   #[0;37mhttps://cisofy.com/lynis/controls/TOOL-5002/#[0m
 #[1;33m*#[0m Consider restricting file permissions [FILE-7524]
  - Details: #[0;36mSee screen output or log file#[0m
  - Solution : Use chmod to change file permissions
   #[0;37mhttps://cisofy.com/lynis/controls/FILE-7524/#[0m
 #[1;33m*#[0m One or more sysctl values differ from the scan profile and could be tweaked
[KRNL-6000]
  - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)
   #[0;37mhttps://cisofy.com/lynis/controls/KRNL-6000/#[0m
 #[1;33m*#[0m Harden the system by installing at least one malware scanner, to perform periodic
file system scans [HRDN-7230]
  - Solution: Install a tool like rkhunter, chkrootkit, OSSEC
   #[0;37mhttps://cisofy.com/lynis/controls/HRDN-7230/#[0m
 #[0:36mFollow-up#[0m:
 #[1:37m-----#[0m
 #[1;37m-#[0m Show details of a test (lynis show details TEST-ID)
 #[1;37m-#[0m Check the logfile for all details (less /var/log/lynis.log)
 #[1;37m-#[0m Read security controls texts (https://cisofy.com)
 #[1;37m-#[0m Use --upload to upload data to central system (Lynis Enterprise users)
```

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

#[0;36mHardening index#[0m:#[1;37m65#[0m [#[1;33m##########[0m 1

#[0;36mTests performed#[0m:#[1;37m248#[0m #[0;36mPlugins enabled#[0m:#[1;37m1#[0m

```
#[1;37mComponents#[0m:
 - Firewall
                [#[1;32mV#[0m]
- Malware scanner
                    [#[1;31mX#[0m]
#[1;33mScan mode#[0m:
Normal [V] Forensics [] Integration [] Pentest []
#[1;33mLynis modules#[0m:
 - Compliance status
                    [#[1;33m?#[0m]
 - Security audit
                  [#[1;32mV#[0m]
- Vulnerability scan
                  [#[1;32mV#[0m]
#[1;33mFiles#[0m:
 - Test and debug information
                           : #[1;37m/var/log/lynis.log#[0m
- Report data
                      : #[1;37m/var/log/lynis-report.dat#[0m
=======
#[1;37mLynis#[0m 3.0.7
Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)
2007-2021, CISOfy - https://cisofy.com/lynis/
#[1;37mEnterprise support available (compliance, plugins, interface and tools)#[0m
______
=======
```

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

VirtualBox

Javi

5

C:

No

10.0.22631

11.1.22621.0

22631

Javi

34

0c0a

3082

SP

Sí

10.0.2.2

Configuración del equipo/Componentes de Windows/Biometría/Permitir el uso de biometría

información acerca de inicios de sesión anteriores durante inicio de sesión de usuario

el servidor de inicio de sesión no está disponible durante el inicio de sesión del usuario

Configuración del equipo/Componentes de Windows/Biometría/Permitir que los usuarios de dominio inicien

Configuración del equipo/Componentes de Windows/Biometría/Permitir que los usuarios inicien sesión

Configuración del equipo/Componentes de Windows/Opciones de inicio de sesión de Windows/Mostrar

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

Configuración del equipo/Componentes de Windows/Opciones de inicio de sesión de Windows/Informar cuando No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Privacidad de la aplicación/Permitir que las aplicaciones de No configurado

Configuración del equipo/Componentes de Windows/Contenido en la nube/No mostrar sugerencias de Windows No configurado

Configuración del equipo/Componentes de Windows/Recopilación de datos y versiones preliminares/No volver a No configurado

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de navegación/Evitar No configurado

Configuración del equipo/Componentes de Windows/Informe de errores de Windows/Deshabilitar el informe de No configurado

80.73.148.121

① Recoge el conjunto de adaptadores de red presentes en el sistema

12.0.22621.2506

innotek GmbH

x64-based PC

WORKGROUP

3,98 GB's

AT/AT COMPATIBLE

Cliente independiente

Microsoft Windows 11 Pro

C:\Windows\system32

No hay Service Pack instalado

00330-80000-00000-AA307

(UTC+01:00) Bruselas, Copenhague, Madrid, París

Intel(R) PRO/1000 MT Desktop Adapter

10.0.2.15 - fe80::1a94:e91f:34f7:6bbd

08:00:27:4F:0E:D3

255.255.255.0 / 64

Cumplimiento (41,56%)

04/10/2024 18:09:16

① Recopila la información de los diferentes medios de almacenamiento del sistema, evaluando el tipo de formato de almacenamiento

Modelo

Discos

Nombre

Tamaño

Nombre

Servidor

Versión

Instalación core

Organización

Directorio del sistema

Versión de Service Pack

Número de compilación

Configuración regional

Lenguaje del sistema operativo

Puerta de enlace predeterminada

Orden de búsqueda servidor DNS

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

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

Windows accedan a la información de la cuenta

Windows accedan al historial de llamadas

Windows tengan acceso a los contactos

Windows accedan al correo electrónico

Windows accedana la ubicación

Windows accedan a los mensajes

Windows accedan al movimiento

Windows accedan al calendario

Windows accedan a la cámara

Windows controlen las radios

Windows accedan a las tareas

Windows se ejecuten en el fondo

mostrar notificaciones de comentarios

Internet en Search

archivos

telemetría

digital

adicionales

soporte técnico

Messenger

4.0

Windows

Entrada

Entrada

Antivirus

Nombre

Nombre

contraseña

Nombre

Windows 10 [version 1507])

del sistema operativo:

de datos fijas:

de datos extraibles:

memoria al reiniciar

Otro firewall

Firewall de Windows

Nivel de actualización

Reproducción automática

errores de Windows

Windows Media Center

aplicaciones de escritorio)

consumidor de Microsoft

Windows accedan a dispositivos de confianza

Windows se sincronicen con dispositivos

Windows accedan a las notificaciones

Windows realicen llamadas telefónicas

Windows accedan a la información de diagnóstico sobre otras aplicaciones

Configuración del equipo/Componentes de Windows/Asistencia en línea/Desactivar la ayuda activa

Configuración del equipo/Componentes de Windows/Buscar/No buscar en Internet o mostrar resultados de

Configuración del equipo/Componentes de Windows/Internet Explorer/Permitir a los servicios de Microsoft

Configuración del equipo/Componentes de Windows/One drive/Impedir el uso de OneDrive para almacenar

Configuración del equipo/Componentes de Windows/Recopilación de datos y versiones preliminares/Permitir

Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar scripting de ubicación

Configuración del equipo/Componentes de Windows/Windows Media Center/No permitir que se ejecute

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

Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar sensores

Configuración del equipo/Componentes de Windows/Ubicación y sensores/Desactivar ubicación

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

la eliminación de datos de filtrado ActiveX, protección de rastreo y No realizar seguimiento

Configuración del equipo/Componentes de Windows/Internet Explorer/Eliminar el historial de

Configuración del equipo/Componentes de Windows/Internet Explorer/Activar sitios sugeridos

Configuración del equipo/Componentes de Windows/Almacén Digital/No permitir que se ejecute el Almacén

Configuración del equipo/Componentes de Windows/Informe de errores de Windows/No enviar datos

Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de

comunicaciones de Internet/Desactivar informe de errores de reconocimiento de escritura a mano

Configuración del equipo/Sistema/Administración de comunicaciones de Internet/Configuración de

Configuración del equipo/Componentes de Windows/Administración de derechos digitales de Windows

Configuración del equipo/Componentes de Windows/Directivas de Reproducción automática/Desactivar

Configuración del equipo/Componentes de Windows/Tienda/Desactivar la aplicación Tienda

Configuración del equipo/Sistema/Perfiles de usuario/Desactivar el identificador de publicidad

Configuración del equipo/Componentes de Windows/Internet Explorer/Configuración de

Configuración del equipo/Componentes de Windows/Buscar/Permitir el uso de Cortana

mano/Desactivar el aprendizaje automático (recopilación manuscrita)

mano/Desactivar el aprendizaje automático (recopilación escritura)

Internet/Autocompletar/Desactivar las sugerencias de direcciones URL

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

SmartScreen. Seleccionar modo de filtro SmartScreen:

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

OP.EXP.5 - Gestión de cambios (100%)

comunicaciones de Internet/Desactivar la tarea de imágenes 'Pedir copias fotográficas'

comunicaciones de Internet/Desactivar los vínculos 'Events.asp' del Visor de eventos

comunicaciones de Internet/Desactivar el informe de errores de Windows

comunicaciones de Internet/Desactivar el acceso a la tienda

Media/Impedir el acceso a Internet de Windows Media DRM

predeterminado para la ejecución automática

comunicaciones de Internet/Desactivar el Programa para la mejora de la experiencia del usuario de Windows

comunicaciones de Internet/Desactivar el contenido '¿Sabía que...?' del Centro de ayuda y soporte técnico

comunicaciones de Internet/Desactivar la búsqueda en Microsoft Knowledge Base del Centro de ayuda y

comunicaciones de Internet/Desactivar la actualización de archivos de contenido del Asistente para búsqueda

comunicaciones de Internet/Desactivar el Programa para la mejora de la experiencia del usuario de Windows

Configuración del equipo/Componentes de Windows/Directivas de Reproducción automática/Comportamiento

Configuración del equipo/Componentes de Windows/Shell remoto de Windows/Permitir acceso a shell remoto

Configuración del equipo/Sistema/Net Logon/Permitir algoritmos de criptografía compatibles con Windows NT

Configuración del equipo/Componentes de Windows/Tienda/Deshabilitar todas las aplicaciones de la Tienda

Configuración del equipo/Panel de control/Configuración regional y de idioma/Personalización de escritura a

Configuración del equipo/Panel de control/Configuración regional y de idioma/Personalización de escritura a

Configuración del equipo/Componentes de Windows/Internet Explorer/Impedir administración del filtro

Configuración del equipo/Componentes de Windows/Endpoint Protection/Desactivar Endpoint Protection

Configuración del equipo/Componentes de Windows/Explorador de archivos/Configurar Windows SmartScreen

Configuración del equipo/Componentes de Windows/Microsoft Edge/Desactivar el filtro SmartScreen

Configuración de usuario/Panel de control/Personalización/Proteger el protector de pantalla mediante

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,

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e

Configuración del equipo/Componentes de Windows/Cifrado de unidad BitLocker/Elegir método de cifrado e

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

extraíbles/Controlar el uso de BitLocker en unidades extraíbles. Permitir que los usuarios apliquen la protección

extraíbles/Controlar el uso de BitLocker en unidades extraíbles. Permitir que los usuarios suspendan y descifren

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

operativo/Configurar perfil de validación de plataforma del TPM. PCR 13: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 14: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 15: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 16: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 17: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 18: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 19: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 20: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 21: Reservado para uso futuro

operativo/Configurar perfil de validación de plataforma del TPM. PCR 22: Reservado para uso futuro

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

Directivas de servicios del sistema (0%)

No hay datos relevantes que mostrar en esta sección.

operativo/Configurar perfil de validación de plataforma del TPM. PCR 11: Control de acceso de BitLocker

operativo/Configurar perfil de validación de plataforma del TPM. PCR 10: Administrador de arranque

operativo/Configurar perfil de validación de plataforma del TPM. PCR 9: Bloque de arranque de NTFS

operativo/Configurar perfil de validación de plataforma del TPM. PCR 8: Sector de arranque de NTFS

operativo/Configurar perfil de validación de plataforma del TPM. PCR 5: Tabla de participaciones de registro de

operativo/Configurar perfil de validación de plataforma del TPM. PCR 6: Eventos de activación y transición de

operativo/Configurar perfil de validación de plataforma del TPM. PCR 7: Específico del fabricante del equipo

operativo/Configurar perfil de validación de plataforma del TPM. PCR 3: Configuración y datos de ROM de

operativo/Configurar perfil de validación de plataforma del TPM. PCR 2: Código ROM de opció

operativo/Configurar perfil de validación de plataforma del TPM. PCR 1: Configuración y datos de placa base y

operativo/Configurar perfil de validación de plataforma del TPM. PCR 0: CRTM (Core Root of Trust of

operativo/Requerir autenticación adicional al iniciar. Configurar la clave de inicio y el PIN del TPM:

operativo/Requerir autenticación adicional al iniciar. Configurar clave de inicio del TPM:

operativo/Requerir autenticación adicional al iniciar. Configurar PIN de inicio con TPM:

operativo/Requerir autenticación adicional al iniciar. Configurar inicio del TPM:

operativo/Configurar perfil de validación de plataforma del TPM

Measurement), BIOS y extensiones de la plataforma

plataforma

opción

estado

maestro (MBR)

arranque maestro (MBR)

intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades

intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades

intensidad de cifrado de unidad (Windows 10 [version 1511] y posteriores). Método de cifrado de las unidades

Configuración de usuario/Panel de control/Personalización/Habilitar protector de pantalla

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

extraíbles/Controlar el uso de BitLocker en unidades extraíbles

la protección de BitLocker en unidades de datos extraibles

operativo/Configurar longitud mínima de PIN para el inicio

operativo/Permitir los PIN mejorados para el inicio

operativo/Requerir autenticación adicional al iniciar

contraseña o clave de inciio en unidad flash USB):

de BitLocker en unidades de datos extraibles

navegación/Permitir que se elimine el historial de exploración al salir

navegación/Impedir que se eliminen los datos de formularios

navegación/Impedir que se elimine el historial de descarga

navegación/Impedir que se eliminen los sitios web que el usuario visitó

navegación/Impedir que se eliminen los archivos temporales de Internet

navegación/Impedir que se eliminen los datos de filtrado InPrivate

navegación/Impedir que se eliminen datos del sitio de favoritos

navegación/Impedir que se eliminen contraseñas

navegación/Impedir que se eliminen cookies

Configuración del equipo/Componentes de Windows/Contenido en la nube/Desactivar experiencias del

ofrecer sugerencias mejoradas mientras el usuario escribe en la barra de direcciones

accedan al micrófono

Servidor primario WINS

Servidor secundario WINS

Usuario registrado

Número de serie

Último arranque

Zona horaria

Localización

Descripción

MAC

DHCP

Subred

Análisis ENS

Nombre

Nombre

Nombre

sesión mediante biometría

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

mediante biometría

Resultados

Valor de criticidad

IP

Teclado

Código de país

Adaptadores de red

Versión de Internet Explorer

Versión de Windows Media Player

① Recoge información sobre la configuración de región

Fabricante

Descripción

Tipo de sistema

Memoria física

Rol del dominio

Letra de unidad

Sistema de ficheros

Sistema operativo

Recoge información del sistema operativo

Nombre del propietario

Dominio / Grupo de trabajo

Versión de PowerShell

Mostrar todo

Ocultar

Resultado

Resultado

Resultado

No configurado

Resultado

Inconcluso

Correcto

Correcto

Resultado

Resultado

Correcto

Resultado

Resultado

No configurado

0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F7

Ocultar

Correcto

Ocultar

Ocultar

Ocultar

Ocultar

Valor esperado

Valor esperado

Valor esperado

Forzar denegación

Habilitada

Deshabilitada

Habilitada

Todas las unidades

Deshabilitada

Deshabilitada

Deshabilitada

Deshabilitada

Habilitada

Habilitada

Habilitada

Habilitada

Valor esperado

Habilitada

Deshabilitada

Valor esperado

Valor esperado

XTS-AES 256 bits

XTS-AES 256 bits

AES-CBC 256 bits

Deshabilitada

Deshabilitada

Deshabilitada

Deshabilitada

Habilitada

Habilitada

No permitir TPM

Habilitada

Habilitada

Deshabilitada

Habilitada

Habilitada

Habilitada

Deshabilitada

Deshabilitada

Habilitada

Habilitada

Habilitada

Habilitada

Deshabilitada

Desactivado/Deshabilitado

No permitir clave de inicio con TPM

No permitir clave y PIN de inicio con TPM

Requerir PIN de inicio con TPM

8

AES 256 bits

Habilitada

Habilitada

No configurada/Deshabilitada

software desconocido descargado

Requerir la aprobacion de un administrador antes de ejecutar un

No hay ningún firewall. Los siguientes firewalls han sido analizados de forma automatizada: McAfee, Norton, Trend Micro, F-Secure, Microsoft.

Habilitada

No ejecutar ningún comando de ejecución automática

No configurada/Deshabilitada

Siempre desactivado

Básico

Habilitada

Habilitada

Habilitada

Habilitada

Habilitada

Habilitada

Centro Criptológico Nacional

Unidad: SAD Categoría del sistema: ALTA Auditado por Javi Informes generados el día 04/10/2024 17:11:03 UTC Versión de CLARA: 2.0 0418ae14-50d4-40f0-99e5-1647218f2953-09504d03-81c9-4de8-a235-3b5bdc3239e1-2F74

Nombre del sistema: FJBP Organización: Asir

Datos del sistema

Valor de criticidad

Sistema ① Recoge la información de datos básicos del sistema Nombre del sistema FJBP

Valor actual

No configurado

No configurado

No configurado

Valor actual

No configurado

Valor actual

No configurado

El sistema está actualizado dentro de los últimos 30 días.

Los siguientes antivirus han sido detectados: Windows Defender

Valor actual

No configurado

No configurado

No configurado

No configurado

Valor actual

No configurado

No configurado

Valor actual

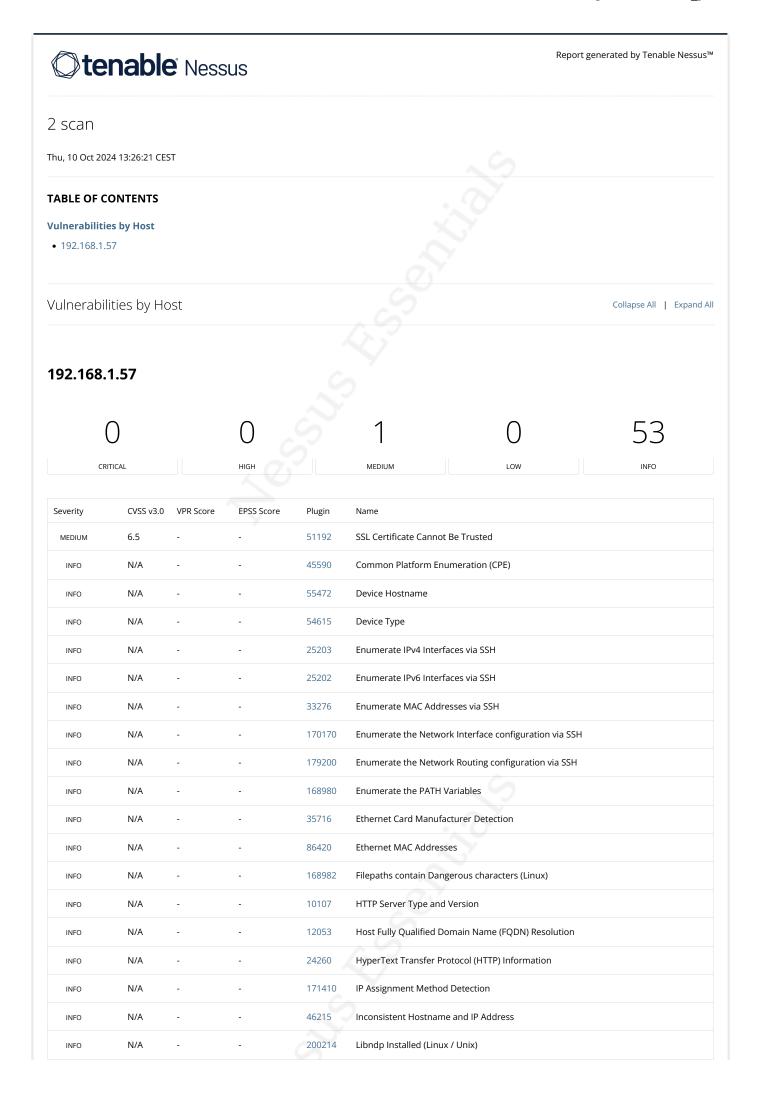
No configurado

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

Notas

Notas

Los perfiles están habilitados



1 of 3 10/10/24, 16:18

INFO	N/A	-		157358	Linux Mounted Devices
INFO	N/A	-	~(0)	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	-	-	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	-	ON	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	-	-	186361	VMWare Tools or Open VM Tools Installed (Linux)
INFO	N/A	-	-	189731	Vim Installed (Linux)
INFO	N/A	-	-	198234	gnome-shell Installed (Linux / UNIX)
INFO	N/A	-	-	182848	libcurl Installed (Linux / Unix)
INFO	N/A	-	-	204828	libexiv2 Installed (Linux / Unix)
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

2 of 3 10/10/24, 16:18

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

© 2024 Tenable™, Inc. All rights reserved.

3 of 3 10/10/24, 16:18

10/10/24, 16:15 2 scan



Report generated by Tenable Nessus™

2 scan

Thu, 10 Oct 2024 13:20:04 Romance Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.1.55

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.55

\bigcirc	0 8	2	0	30	
CRITICAL	HIGH	MEDIUM	LOW	INFO	

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
MEDIUM	6.5	<u>.</u>	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	57608	SMB Signing not required
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	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	1-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A		-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	1-	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
				4.74	

INFO	N	/A	-	- 6	64582	Netstat Connection Information
INFO	N	/A	-	- 65	14272	Netstat Portscanner (SSH)
INFO	N	/A	-	20	11936	OS Identification
INFO) N	/A	-	4	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	-	Æ	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	ia .	-	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	1-	1-	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

© 2024 Tenable $^{\text{\tiny{TM}}}$, Inc. All rights reserved.