

M6 – P1: Aplicación del Benchmark CIS en Sistemas Operativos

El Center for Internet Security (CIS) ofrece estándares de configuración segura ("benchmarks") para distintos sistemas. En esta práctica, los alumnos aprenderán a auditar y reforzar la configuración de un sistema operativo siguiendo uno de estos benchmarks.

Objetivos específicos

- Comprender qué es un benchmark CIS y por qué es relevante.
- Auditar un sistema Linux o Windows con herramientas especializadas.
- Aplicar las recomendaciones básicas y volver a auditar para comprobar mejoras.

Requisitos técnicos

- Máquina virtual con Ubuntu 20.04 o Windows 10
- Acceso a internet
- Terminal con permisos de administrador (sudo/administrador)
- Herramientas: Lynis para Linux o CIS-CAT Lite para Windows

1. Introducción al Benchmark

1. Ingresar a la web oficial:

<https://www.cisecurity.org/cis-benchmarks>

2. Descargar el benchmark correspondiente:

- Ubuntu 20.04: CIS Ubuntu Linux 20.04 LTS Benchmark v1.1.0
- Windows 10: CIS Microsoft Windows 10 Benchmark

2. Auditoría con herramienta automatizada

Linux: Lynis



1. Instalación de Lynis

```
sudo apt update && sudo apt install lynis -y
```

Descargar e instalar Lynis desde los repositorios oficiales de Linux.

2. Ejecución de la auditoría

```
sudo lynis audit system
```

```
#####
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.

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

[+] Initializing program
-----
- Detecting OS ... [ DONE ]
- Checking profiles ... [ DONE ]

Program version: 3.1.4
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.12.38+kali
Hardware platform: x86_64
Hostname: kali

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: en
Test category: all
Test group: all

- Program update status ... [ NO UPDATE ]

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

- Lynis ejecutará una serie de pruebas de seguridad sobre el sistema operativo, servicios y configuraciones.
- Al finalizar, mostrará un resumen en la terminal.
- El **informe detallado** se guarda en:
 - /var/log/lynis.log → registro completo de la ejecución.
 - /var/log/lynis-report.dat → informe resumido con resultados clave.

```
-[ Lynis 3.1.4 Results ]-  
  
Warnings (2):  
! Couldn't find 2 responsive nameservers [NETW-2705]  
  https://cisofy.com/lynis/controls/NETW-2705/  
  
! iptables module(s) loaded, but no rules active [FIRE-4512]  
  https://cisofy.com/lynis/controls/FIRE-4512/  
  
Suggestions (49):  
* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]  
  - Related resources  
    * Website: https://cisofy.com/lynis/controls/LYNIS/  
  
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]  
  - Related resources  
    * Website: https://cisofy.com/lynis/controls/DEB-0280/  
  
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]  
  - Related resources  
    * Website: https://cisofy.com/lynis/controls/DEB-0810/  
  
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]  
  - Related resources  
    * Website: https://cisofy.com/lynis/controls/DEB-0811/  
  
* 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]  
  - Related resources  
    * Website: https://cisofy.com/lynis/controls/DEB-0831/
```

3. Revisión del informe

Para revisar directamente el informe con los hallazgos principales:

```
less /var/log/lynis-report.dat
```

Dentro verás entradas como:

- [WARNING] vulnerabilidades o configuraciones inseguras que requieren atención inmediata.
- [SUGGESTION] recomendaciones de endurecimiento (hardening), no críticas, pero que mejoran la seguridad.

Ejemplo de líneas típicas:

```
[WARNING] No password set for GRUB bootloader. [AUTH-9232]  
[SUGGESTION] Install a PAM module for password strength testing [AUTH-9262]
```

4. Identificar advertencias y sugerencias

Puedes extraer rápidamente advertencias y sugerencias con:

```
grep "warning" /var/log/lynis-report.dat  
  
grep "suggestion" /var/log/lynis-report.dat
```

Esto facilita crear una lista de **prioridades**:

- **Primero atender los [WARNING] riesgos inmediatos** (por ejemplo, falta de parches de seguridad, permisos inseguros, configuraciones críticas sin protección).

- **Después los [SUGGESTION]** buenas prácticas (mejoras en logging, endurecimiento de SSH, configuración de firewall, etc.).

1. Ejemplo de [WARNING]

```
[WARNING] No password set for GRUB bootloader. [BOOT-5122]
```

Qué significa: El gestor de arranque **GRUB** no tiene contraseña. Esto permitiría que alguien con acceso físico a la máquina modifique parámetros del kernel o arranque en modo de rescate sin control.

Cómo solucionarlo: Configurar una contraseña para GRUB:

```
sudo grub-mkpasswd-pbkdf2
```

Pega la contraseña en `/etc/grub.d/40_custom` de esta forma:

```
set superusers="root"  
password_pbkdf2 root <hash_generado>
```

Y actualiza GRUB:

```
sudo update-grub
```

2. Ejemplo de [SUGGESTION]

```
[SUGGESTION] Install a PAM module for password strength testing [AUTH-9262]
```

Qué significa: Tus contraseñas pueden ser demasiado simples porque no hay un módulo PAM (Pluggable Authentication Module) que obligue a usar complejidad mínima.

Cómo solucionarlo: Instalar el módulo de calidad de contraseñas:

```
sudo apt install libpam-pwquality
```

Y configurarlo en `/etc/security/pwquality.conf` (ejemplo):

```
minlen = 12  
ucredit = -1  
dcredit = -1  
ocredit = -1  
lcredit = -1
```

Esto fuerza mínimo 12 caracteres con mayúsculas, minúsculas, números y símbolos.

3. Ejemplo de [SUGGESTION]

```
[SUGGESTION] Enable process accounting [LOGG-2190]
```

Qué significa: No tienes activada la contabilidad de procesos (accounting), lo que dificulta auditar qué comandos ejecutan los usuarios.

Cómo solucionarlo: Instalar el paquete `acct`:

```
sudo apt install acct
```

Activar el servicio:

```
sudo systemctl enable acct --now
```

Windows: CIS-CAT Lite



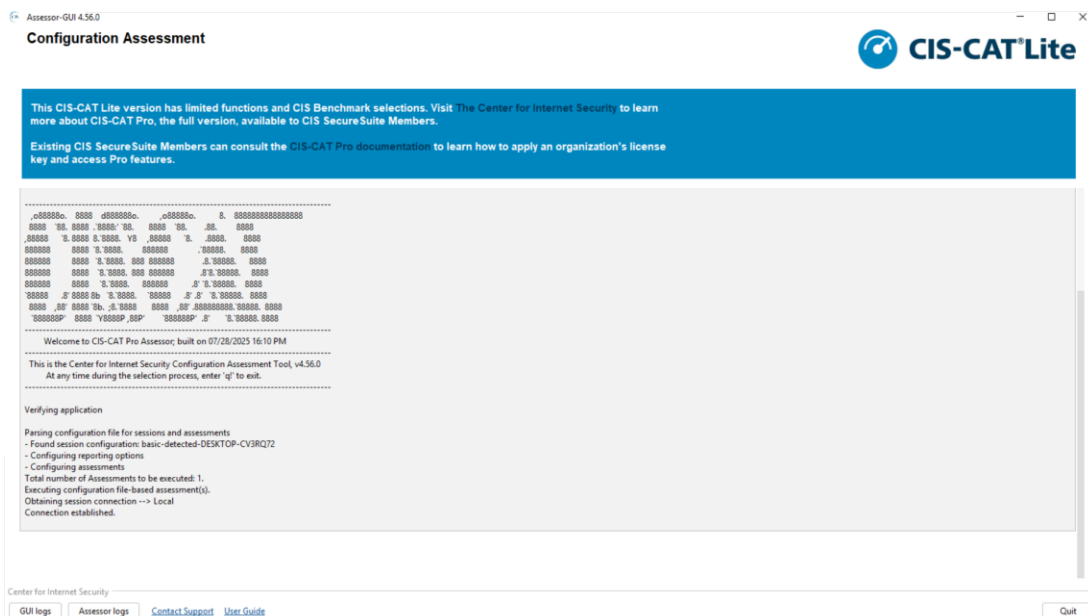
1. Descargar el zip desde la web oficial.

<https://learn.cisecurity.org/cis-cat-lite>
<https://github.com/skylens/CIS?tab=readme-ov-file>

2. Ejecutar como administrador el `.bat` o `.jar`:

```
java -jar CIS-CAT-Lite.jar
```

3. Elegir perfil de evaluación: Windows 10.





Security Configuration Assessment Report for DESKTOP-CV3RQ72

Target IP Address: 10.0.0.136

CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0

Level 1 (L1)
Monday, September 29 2025 11:00:22
Assessment Duration: 3 minutes, 23 seconds

Activar
We a Confi
Windows.

Summary

Description	Tests						Scoring		
	Pass	Fail	Error	Unkn	Man.	Exc.	Score	Max	Percent
1 Account Policies	7	3	0	0	1	0	7.0	10.0	70%
1.1 Password Policy	5	2	0	0	0	0	5.0	7.0	71%
1.2 Account Lockout Policy	2	1	0	0	1	0	2.0	3.0	67%
2 Local Policies	61	37	0	0	1	0	61.0	98.0	62%
2.1 Audit Policy	0	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	27	10	0	0	0	0	27.0	37.0	73%
2.3 Security Options	34	27	0	0	1	0	34.0	61.0	56%
2.3.1 Accounts	4	1	0	0	0	0	4.0	5.0	80%
2.3.2 Audit	1	1	0	0	0	0	1.0	2.0	50%
2.3.3 DCOM	0	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	0	0	0	0	0	0	0.0	0.0	0%
2.3.5 Domain controller	0	0	0	0	0	0	0.0	0.0	0%
2.3.6 Domain member	6	0	0	0	0	0	6.0	6.0	100%
2.3.7 Interactive logon	1	6	0	0	0	0	1.0	7.0	14%
2.3.8 Microsoft network client	2	1	0	0	0	0	2.0	3.0	67%
2.3.9 Microsoft network server	2	3	0	0	0	0	2.0	5.0	40%
2.3.10 Network access	9	3	0	0	0	0	9.0	12.0	75%
2.3.11 Network security	2	9	0	0	1	0	2.0	11.0	18%
2.3.12 Recovery console	0	0	0	0	0	0	0.0	0.0	0%
2.3.13 Shutdown	0	0	0	0	0	0	0.0	0.0	0%
2.3.14 System cryptography	0	0	0	0	0	0	0.0	0.0	0%
2.3.15 System objects	2	0	0	0	0	0	2.0	2.0	100%
2.3.16 System settings	0	0	0	0	0	0	0.0	0.0	0%
2.3.17 User Account Control	5	3	0	0	0	0	5.0	8.0	62%
3 Event Log	0	0	0	0	0	0	0.0	0.0	0%
4 Restricted Groups	0	0	0	0	0	0	0.0	0.0	0%
5 System Services	9	12	0	0	0	0	9.0	21.0	43%

2.3.1.1 (L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

Fail

Description:

This policy setting prevents users from adding new Microsoft accounts on this computer.

The recommended state for this setting is: `Users can't add or log on with Microsoft accounts`.

Note: Due to the way Windows 10 version 1607 (and older) handles the process for adding Microsoft Accounts, this legacy setting will remain in the Windows 10 Benchmarks until extended support for LTSC 1607 ends in [October of 2026](#). Applying this setting to newer versions of the OS will not cause an issue, and the OS will ignore the setting. For newer versions of the OS, this setting has been replaced with *Block all consumer Microsoft account user authentication*. For more information please visit: [Accounts Block Microsoft accounts - Windows 10 | Microsoft Learn](#).

Rationale:

Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Users can't add or log on with Microsoft accounts`:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts
```

Impact:

Users will not be able to log onto the computer with their Microsoft account.

Assessment:

[Show Assessment Evidence](#)

[Show Rule Result XML](#)

References:

- URL: <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-block-microsoft-accounts>
- URL: <https://learn.microsoft.com/en-us/lifecycle/products/windows-10-2016-ltsc>
- URL: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/accounts-block-microsoft-accounts>
- URL: GRID: MS-00000053

CIS Controls V7.0:

Activar
ve a Confi
Windows.

3. Análisis de hallazgos

- Documentar mínimo 5 recomendaciones del benchmark que **no se cumplen**.
- Clasificar por criticidad (alta, media, baja).
- Investigar el impacto de cada una.

4. Aplicar correcciones manuales

Ejemplos en Linux:

- Deshabilitar servicios innecesarios:

```
sudo systemctl disable avahi-daemon  
sudo systemctl disable cups
```


- Reforzar contraseñas:

Editar `/etc/login.defs`:

```
PASS_MAX_DAYS 90  
PASS_MIN_DAYS 10  
PASS_WARN_AGE 7
```

- Activar bloqueo por intentos fallidos:

```
sudo apt install libpam-faildelay  
sudo pam-auth-update
```

5. Re-auditar el sistema

- Ejecutar nuevamente Lynis o CIS-CAT.
- Comparar los resultados con la auditoría inicial.
- Documentar el puntaje antes y después de aplicar mejoras.

Consejos y buenas prácticas

- Leer siempre la descripción de cada recomendación: muchas tienen dependencias o riesgos.
- Documentar todos los cambios realizados.
- Comprobar si los servicios desactivados no afectan al uso esperado del sistema.