

Laboratorio 9

Deivis J. Castro

LABORATORIO: Prácticas de contraseña segura (creación y gestión)

Parte 1: Configuración de Políticas de Contraseñas Seguras

Paso 1: Revisión de la Configuración Actual

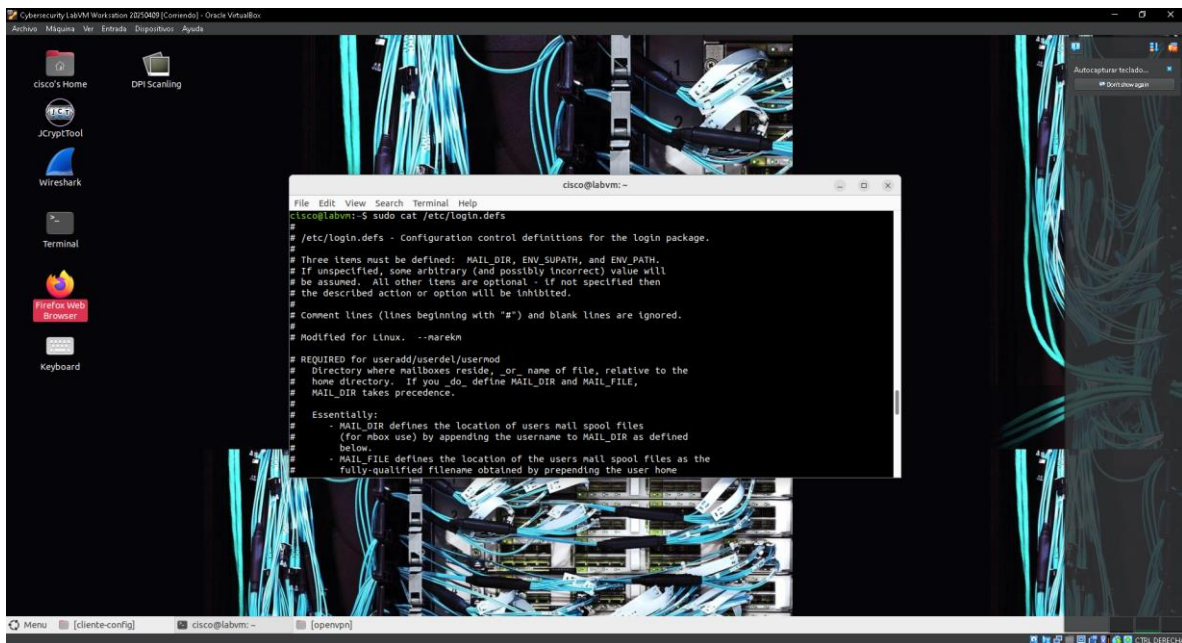
Linux:

1. Verificar la política de contraseñas actual en Linux se realiza revisando el archivo de configuración pam.d y el archivo /etc/login.defs:

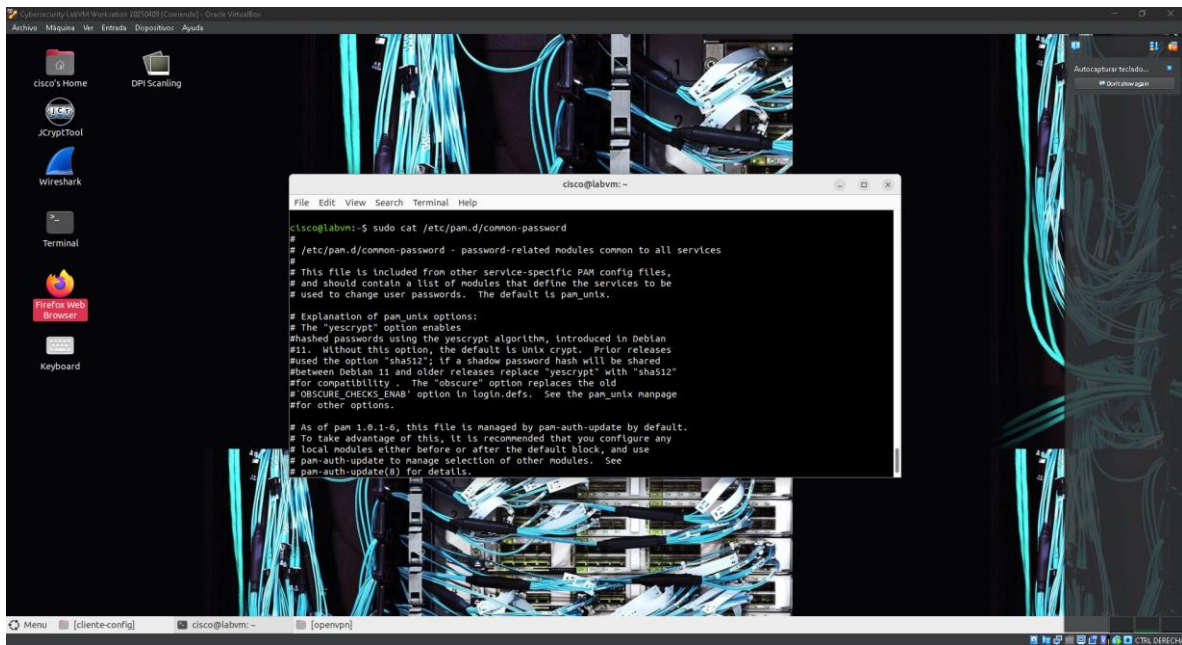
bash

Copiar código

sudo cat /etc/login.defs

A screenshot of a Linux desktop environment with a terminal window open. The terminal displays the output of the command 'sudo cat /etc/login.defs'. The output shows configuration control definitions for the login package, including requirements for MAIL_DIR, ENV_SUPATH, and ENV_PATH. It also mentions that comment lines and blank lines are ignored, and that the configuration was modified for Linux by --narekm. The desktop background features a network-themed wallpaper with glowing blue cables. Various application icons are visible on the left side of the desktop, including Cisco's Home, DPI Scanning, JCryptTool, Wireshark, Terminal, Firefox Web Browser, and Keyboard. The terminal window title is 'cisco@labvm:~'.

sudo cat /etc/pam.d/common-password



2. También puedes verificar el uso de políticas de contraseñas seguras con libpam
pwquality (en algunas distribuciones):

bash

Copiar código

```
sudo cat /etc/security/pwquality.conf
```

Windows:

1. En Windows, puedes revisar las políticas de contraseñas con Directiva de seguridad local.

- ☐ Ve a Inicio > Panel de control > Herramientas administrativas > Directiva de seguridad local.
- ☐ Navega a Políticas de cuenta > Política de contraseñas.
- ☐ Revisa la configuración actual para la longitud mínima, caducidad y complejidad de las contraseñas.

• Explicación: En este paso, revisamos la configuración actual para ver si hay políticas aplicadas en relación con la longitud mínima, complejidad y caducidad de contraseñas.

NO PUDE REALIZAR ESTOS DOS PASOS PORQUE LA DISTRIBUCION DEL LINUX NO TIENE INSTALADO EL PWQUALITY Y PARA REVISAR LAS

CONTRASEÑAS SE REQUIERE UN WINDOWS PRO O EDUCATION, PERO SOLO TENGO LA VERSION HOME

Paso 2: Configuración de la Longitud Mínima y Complejidad de las Contraseñas

Linux:

1. Instalar el paquete libpam-pwquality (si no está instalado):

bash

Copiar código

sudo apt install libpam-pwquality -y

2. Configurar la longitud mínima y la complejidad de las contraseñas en el archivo

/etc/security/pwquality.conf:

bash

Copiar código

sudo nano /etc/security/pwquality.conf

Añade o edita las siguientes líneas:

text

Copiar código

minlen = 12

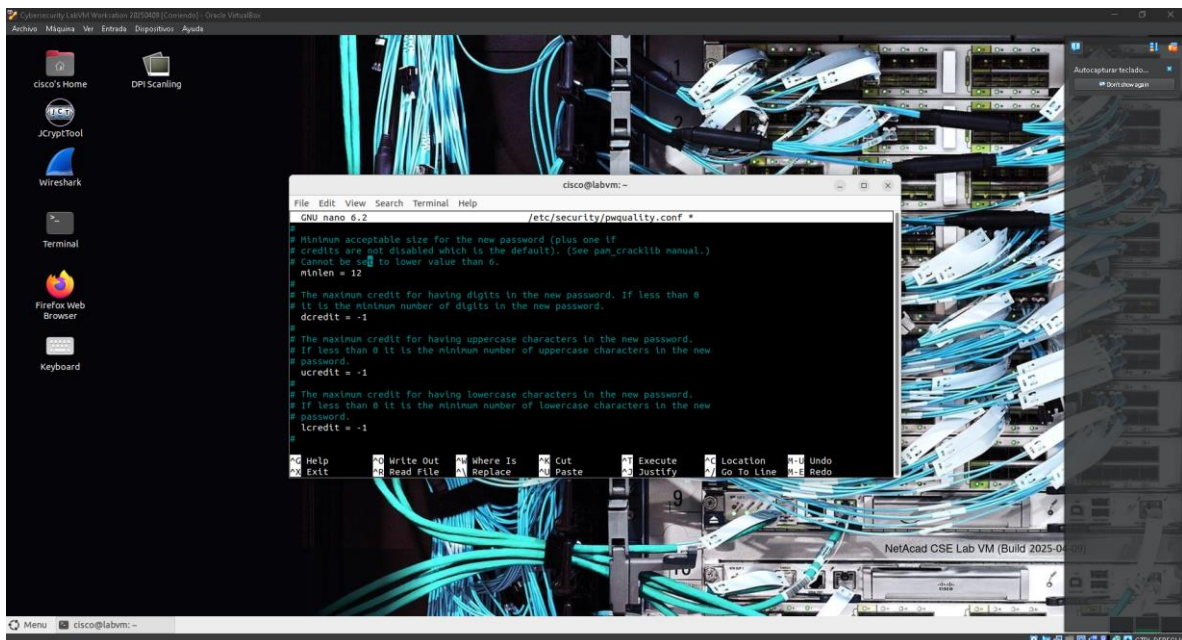
dcredit = -1

ucredit = -1

ocredit = -1

lcredit = -1

- ☐ minlen: Longitud mínima de la contraseña.
- ☐ dcredit: Número mínimo de dígitos.
- ☐ ucredit: Número mínimo de letras mayúsculas.
- ☐ lcredit: Número mínimo de letras minúsculas.
- ☐ ocredit: Número mínimo de caracteres especiales.



3. Aplicar las políticas modificando el archivo /etc/pam.d/common-password para que use el módulo pam_pwquality.so:

bash

Copiar código

password requisite pam_pwquality.so retry=3

Windows:

1. Configura la longitud mínima y complejidad de contraseñas en Directiva de seguridad local:

- ☐ Navega a Políticas de cuenta > Política de contraseñas.
- ☐ Configura Longitud mínima de la contraseña a 12 caracteres.
- ☐ Activa La contraseña debe cumplir con los requisitos de complejidad.

2. En Windows PowerShell, puedes revisar y establecer la longitud mínima con:

powershell

Copiar código

Get-ADDefaultDomainPasswordPolicy

Set-ADDefaultDomainPasswordPolicy -MinPasswordLength 12

• Explicación: Establecer la longitud mínima y los requisitos de complejidad asegura que las

contraseñas cumplan con un estándar de seguridad adecuado, incluyendo el uso de caracteres

especiales, letras mayúsculas y minúsculas, y números.

ESTE PASO NO SE PUDO HACER PORQUE ESTAMOS EN WINDOWS NORMAL Y NO UN SERVER CON DOMINIO

Parte 2: Configuración de Bloqueo de Cuenta tras Intentos Fallidos

Paso 3: Implementación del Bloqueo de Cuenta

Linux:

1. Para implementar el bloqueo de cuenta en Linux, puedes usar pam_tally2 o pam_faillock, dependiendo de la distribución.

☐ Con pam_faillock, abre el archivo /etc/pam.d/common-auth y añade:

bash

Copiar código

auth required pam_faillock.so preauth silent deny=5

unlock_time=900

auth [default=die] pam_faillock.so authfail deny=5

unlock_time=900

Esto bloqueará la cuenta tras 5 intentos fallidos durante 15 minutos (900 segundos).

Windows:

1. En Windows, para establecer el bloqueo de cuentas, accede a Política de seguridad local:

☐ Navega a Políticas de cuenta > Política de bloqueo de cuenta.

☐ Configura:

☐ Umbral de bloqueo de cuenta a 5 intentos.

☐ Duración del bloqueo de cuenta a 15 minutos.

2. Alternativamente, en PowerShell:

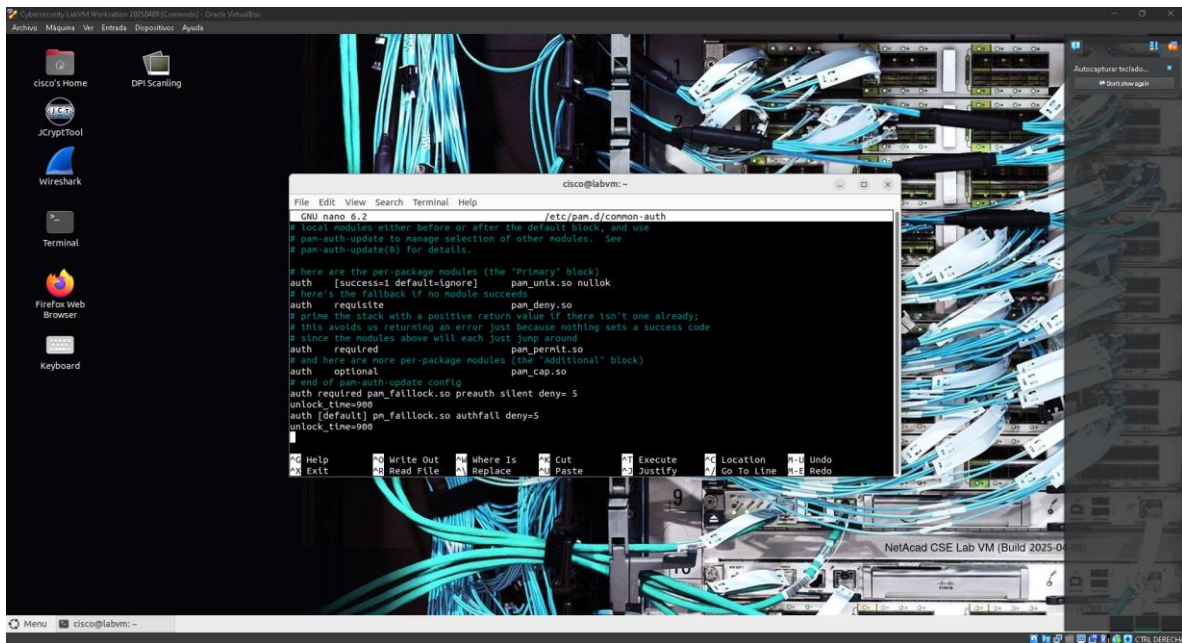
powershell

Copiar código

Set-ADAccountLockoutPolicy -LockoutThreshold 5 -LockoutDuration 15 -

ObservationWindow 30

- Explicación: El bloqueo de cuenta tras varios intentos fallidos reduce la posibilidad de ataques de fuerza bruta al bloquear la cuenta temporalmente.



Parte 3: Verificación y Documentación de la Configuración

Paso 4: Verificación de la Configuración de Contraseñas

Linux:

1. Puedes verificar la política de contraseñas probando crear o cambiar una contraseña

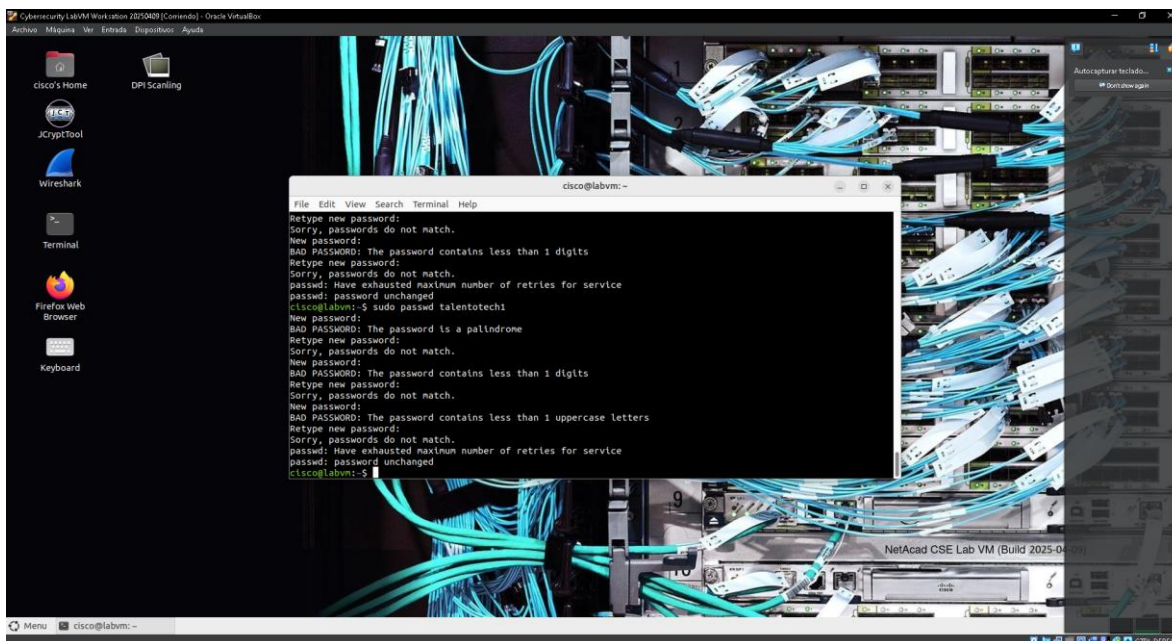
con passwd:

bash

Copiar código

passwd [usuario]

Introduce contraseñas que no cumplan con los requisitos para verificar que el sistema las rechaza.



Windows:

1. Intenta crear o cambiar contraseñas para usuarios desde el Administrador de usuarios locales o usando:

powershell

Copiar código

net user [usuario] *

Paso 5: Verificación del Bloqueo de Cuenta

Linux:

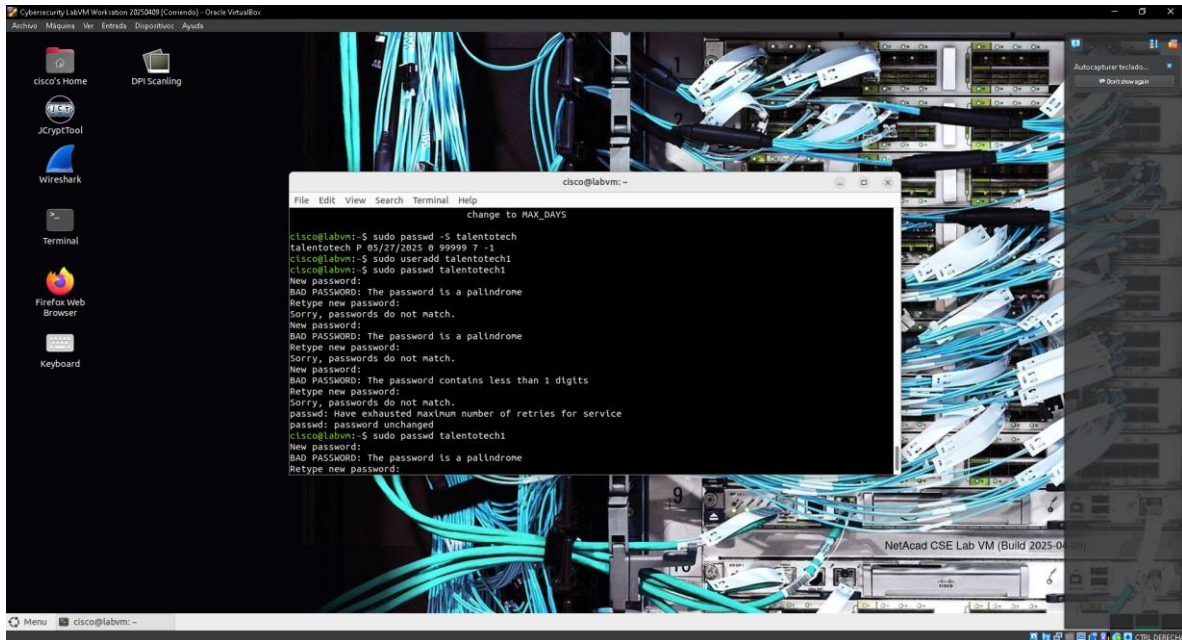
1. Para verificar el bloqueo de cuenta en Linux, intenta iniciar sesión varias veces con una contraseña incorrecta:

bash

Copiar código

su - [usuario]

Después de 5 intentos fallidos, la cuenta debería estar bloqueada.



Windows:

1. Intenta iniciar sesión con una contraseña incorrecta en Windows para el usuario varias veces (5 intentos). Después de los intentos fallidos, el sistema debería bloquear la cuenta.

- Explicación: Estas verificaciones aseguran que las políticas de seguridad están correctamente aplicadas y funcionando según lo configurado.

Paso 6: Documentación del Proceso

1. Documenta los pasos realizados:

- ☐ Incluye capturas de pantalla o comandos utilizados durante la configuración de políticas de contraseñas y bloqueo de cuenta.
- ☐ Describe cómo has verificado que las políticas están funcionando correctamente.

2. Esquema de configuración final:

- ☐ Longitud mínima de contraseña: 12 caracteres.

☐ Requisitos de complejidad de contraseñas: Incluyen números, letras mayúsculas, minúsculas y caracteres especiales.

☐ Bloqueo de cuenta tras 5 intentos fallidos, duración del bloqueo: 15 minutos.

Explicación: Documentar todo el proceso permite que otros administradores o tú mismo puedan replicar o revisar la configuración en el futuro.