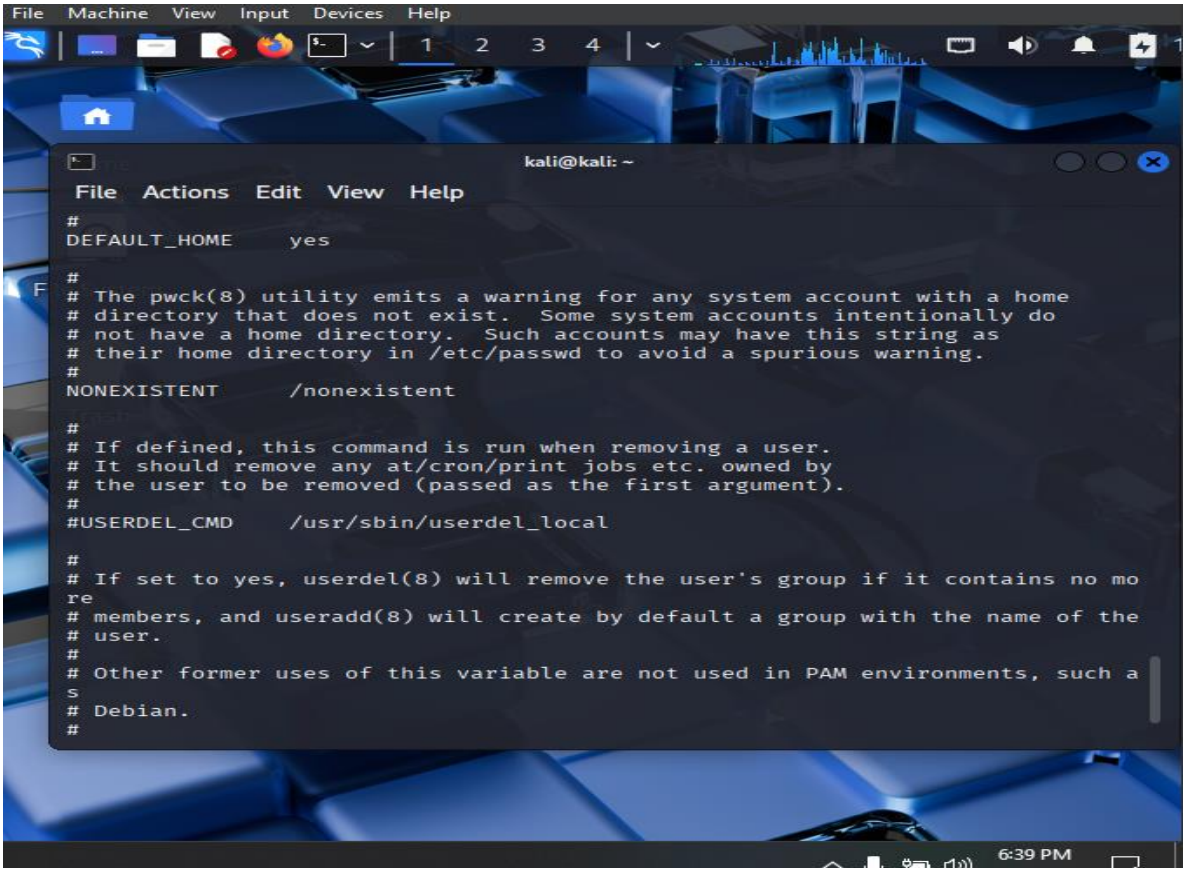
LABORATORIO 9

1 PARTE:

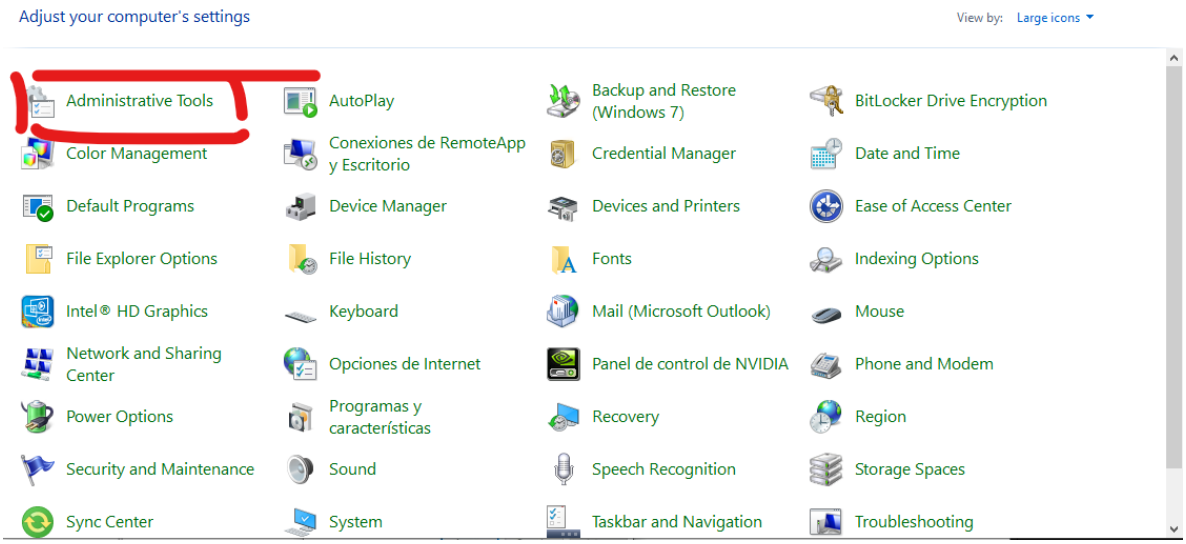
1 PASO : Revision de la configuración actual

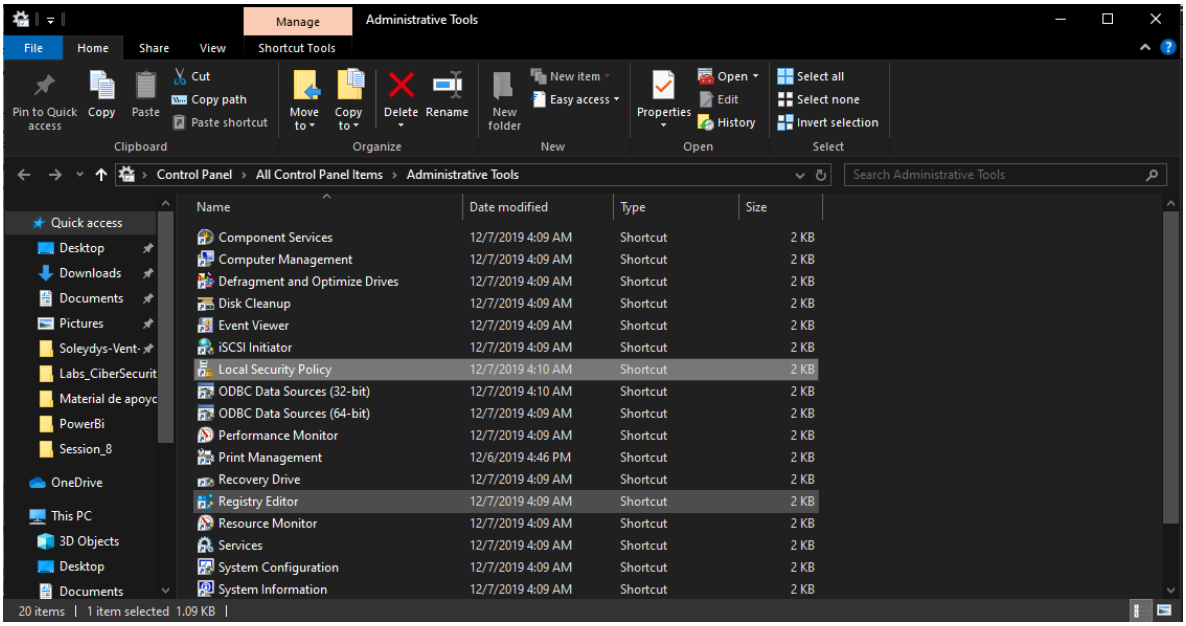


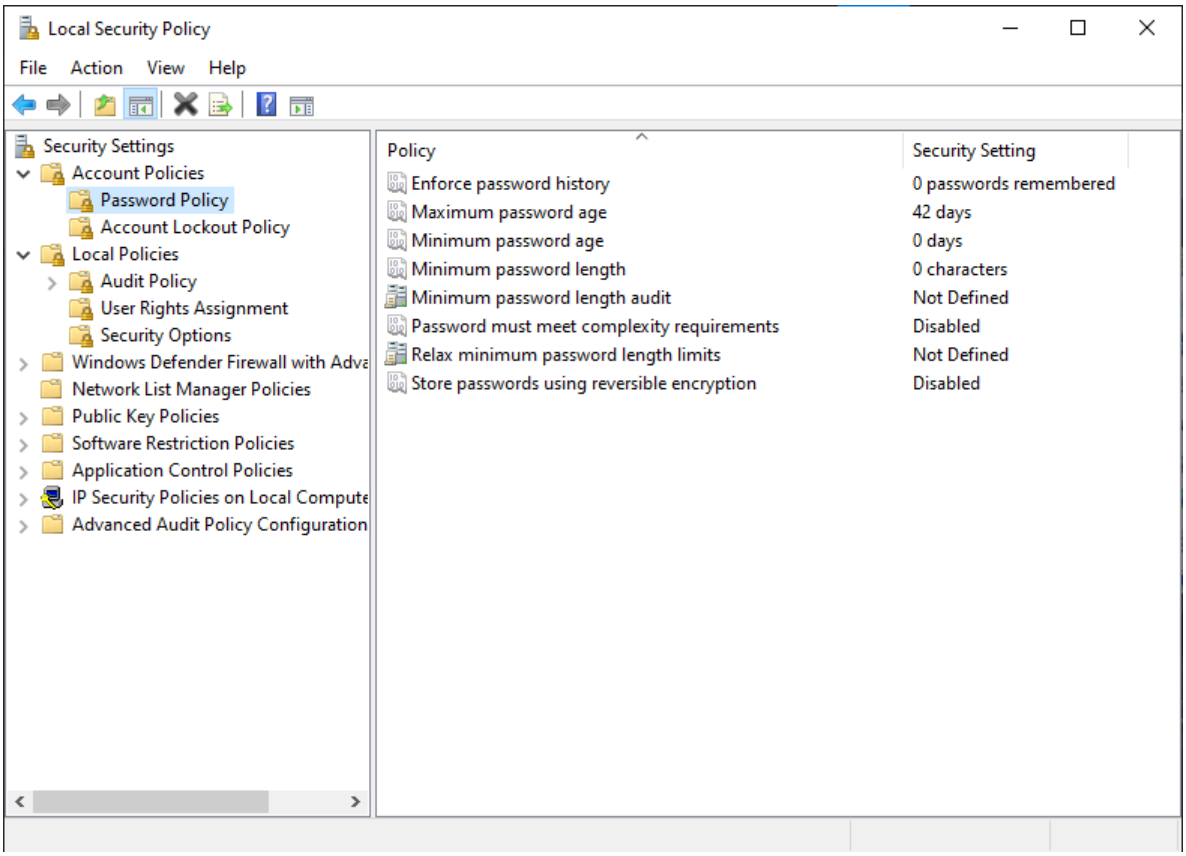
```
File  Machine  View  Input  Devices  Help
1  2  3  4
kali@kali: ~
File  Actions  Edit  View  Help
/etc/ssl/certs/ is a directory

┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all service
s
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        [success=2 default=ignore]      pam_unix.so obscure yescrypt
password        [success=1 default=ignore]      pam_winbind.so try_authtok tr
y_first_pass
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
```

```
1  2  3  4
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/security/pwquality.conf
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = 0
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = 0
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
CTRL DERECHA
```

En Windows


Adjust your computer's settings
View by: Large icons
Administrative Tools
AutoPlay
Backup and Restore (Windows 7)
BitLocker Drive Encryption
Color Management
Conexiones de RemoteApp y Escritorio
Credential Manager
Date and Time
Default Programs
Device Manager
Devices and Printers
Ease of Access Center
File Explorer Options
File History
Fonts
Indexing Options
Intel® HD Graphics
Keyboard
Mail (Microsoft Outlook)
Mouse
Network and Sharing Center
Opciones de Internet
Panel de control de NVIDIA
Phone and Modem
Power Options
Programas y características
Recovery
Region
Security and Maintenance
Sound
Speech Recognition
Storage Spaces
Sync Center
System
Taskbar and Navigation
Troubleshooting

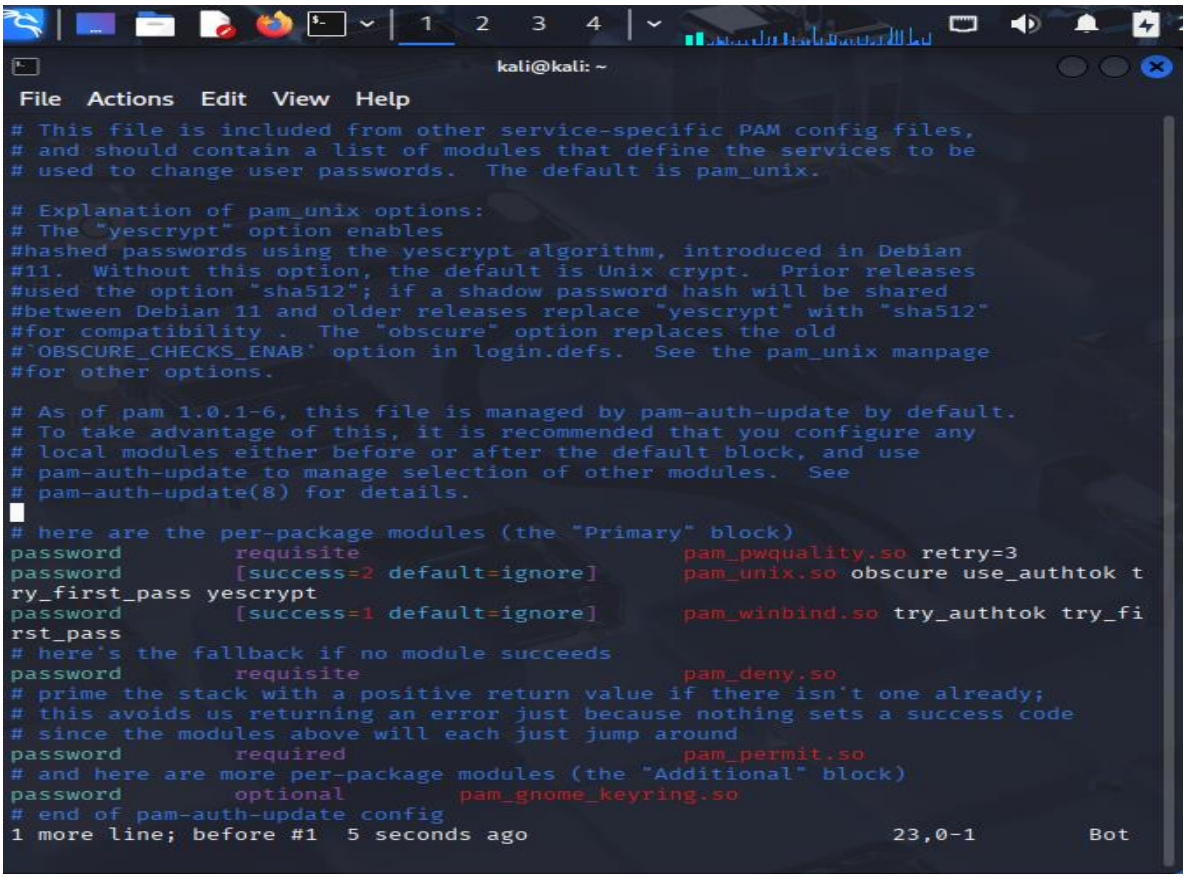

Manage
Administrative Tools
File
Home
Share
View
Shortcut Tools
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Select all
Select none
Invert selection
Select
Control Panel › All Control Panel Items › Administrative Tools
Search Administrative Tools
Quick access
Desktop
Downloads
Documents
Pictures
Soleydys-Vent
Labs_CiberSecurit
Material de apoyo
PowerBi
Session_8
OneDrive
This PC
3D Objects
Desktop
Documents
Name
Date modified
Type
Size
Component Services 12/7/2019 4:09 AM Shortcut 2 KB
Computer Management 12/7/2019 4:09 AM Shortcut 2 KB
Defragment and Optimize Drives 12/7/2019 4:09 AM Shortcut 2 KB
Disk Cleanup 12/7/2019 4:09 AM Shortcut 2 KB
Event Viewer 12/7/2019 4:09 AM Shortcut 2 KB
iSCSI Initiator 12/7/2019 4:09 AM Shortcut 2 KB
Local Security Policy 12/7/2019 4:10 AM Shortcut 2 KB
ODBC Data Sources (32-bit) 12/7/2019 4:10 AM Shortcut 2 KB
ODBC Data Sources (64-bit) 12/7/2019 4:09 AM Shortcut 2 KB
Performance Monitor 12/7/2019 4:09 AM Shortcut 2 KB
Print Management 12/6/2019 4:46 PM Shortcut 2 KB
Recovery Drive 12/7/2019 4:09 AM Shortcut 2 KB
Registry Editor 12/7/2019 4:09 AM Shortcut 2 KB
Resource Monitor 12/7/2019 4:09 AM Shortcut 2 KB
Services 12/7/2019 4:09 AM Shortcut 2 KB
System Configuration 12/7/2019 4:09 AM Shortcut 2 KB
System Information 12/7/2019 4:09 AM Shortcut 2 KB
20 items | 1 item selected 1.09 KB



PASO 2: CONFIGURACIÓN DE LONGITUD MINIMA Y COMPLEJIDAD DE CONTRASEÑAS

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo apt install libpam- pwquality
Error: Unable to locate package libpam
Error: Unable to locate package pwquality

┌──(kali㉿kali)-[~]
└─$ sudo apt install libpam-pwquality
Installing:
  libpam-pwquality

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 6
  Download size: 13.1 kB
  Space needed: 41.0 kB / 63.5 GB available

Get:1 http://kali.mirror.rafal.ca/kali kali-rolling/main amd64 libpam-pwquality a
md64 1.4.5-5 [13.1 kB]
Fetched 13.1 kB in 2s (5,447 B/s)
Selecting previously unselected package libpam-pwquality:amd64.
(Reading database ... 416654 files and directories currently installed.)
Preparing to unpack .../libpam-pwquality_1.4.5-5_amd64.deb ...
Unpacking libpam-pwquality:amd64 (1.4.5-5) ...
Setting up libpam-pwquality:amd64 (1.4.5-5) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(kali㉿kali)-[~]
└─$
```

```
kali@kali: ~
File  Actions  Edit  View  Help
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 12
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
dcredit = -1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 0
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
# maxrepeat = 0
                                                        33,1          6%
```

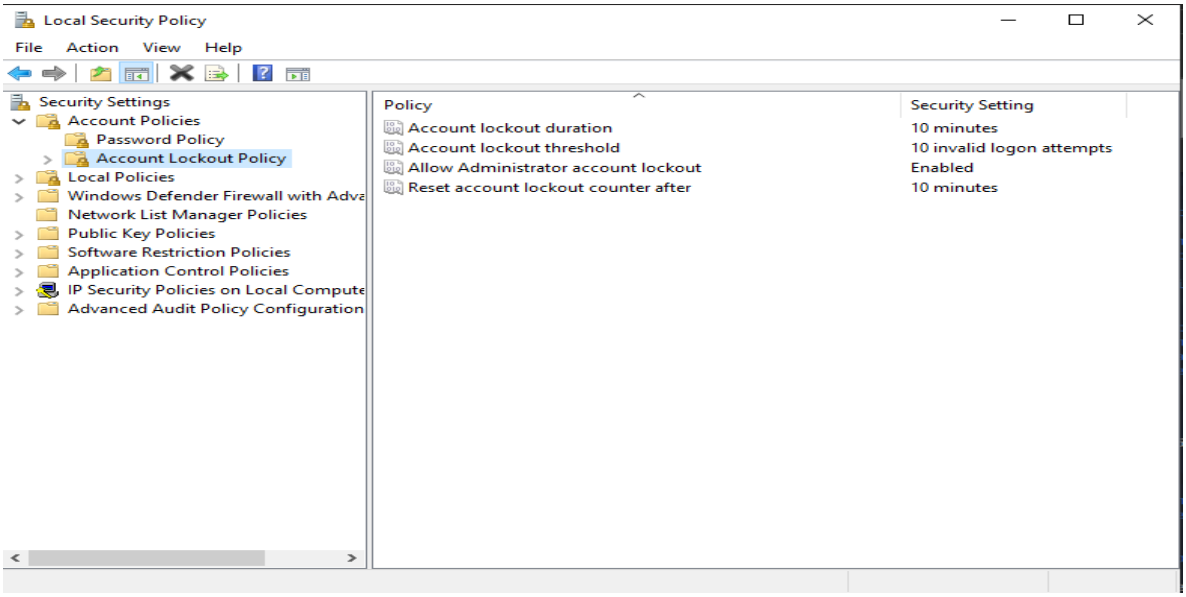

kali@kali: ~
File Actions Edit View Help
This file is included from other service-specific PAM config files,
and should contain a list of modules that define the services to be
used to change user passwords. The default is pam_unix.
Explanation of pam_unix options:
The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11. Without this option, the default is Unix crypt. Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility . The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
#for other options.
As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
To take advantage of this, it is recommended that you configure any
local modules either before or after the default block, and use
pam-auth-update to manage selection of other modules. See
pam-auth-update(8) for details.
here are the per-package modules (the "Primary" block)
password requisite pam_pwquality.so retry=3
password [success=2 default=ignore] pam_unix.so obscure use_authtok try_first_pass yescrypt
password [success=1 default=ignore] pam_winbind.so try_authtok try_first_pass
here's the fallback if no module succeeds
password requisite pam_deny.so
prime the stack with a positive return value if there isn't one already;
this avoids us returning an error just because nothing sets a success code
since the modules above will each just jump around
password required pam_permit.so
and here are more per-package modules (the "Additional" block)
password optional pam_gnome_keyring.so
end of pam-auth-update config
1 more line; before #1 5 seconds ago
23,0-1 Bot

En Windows

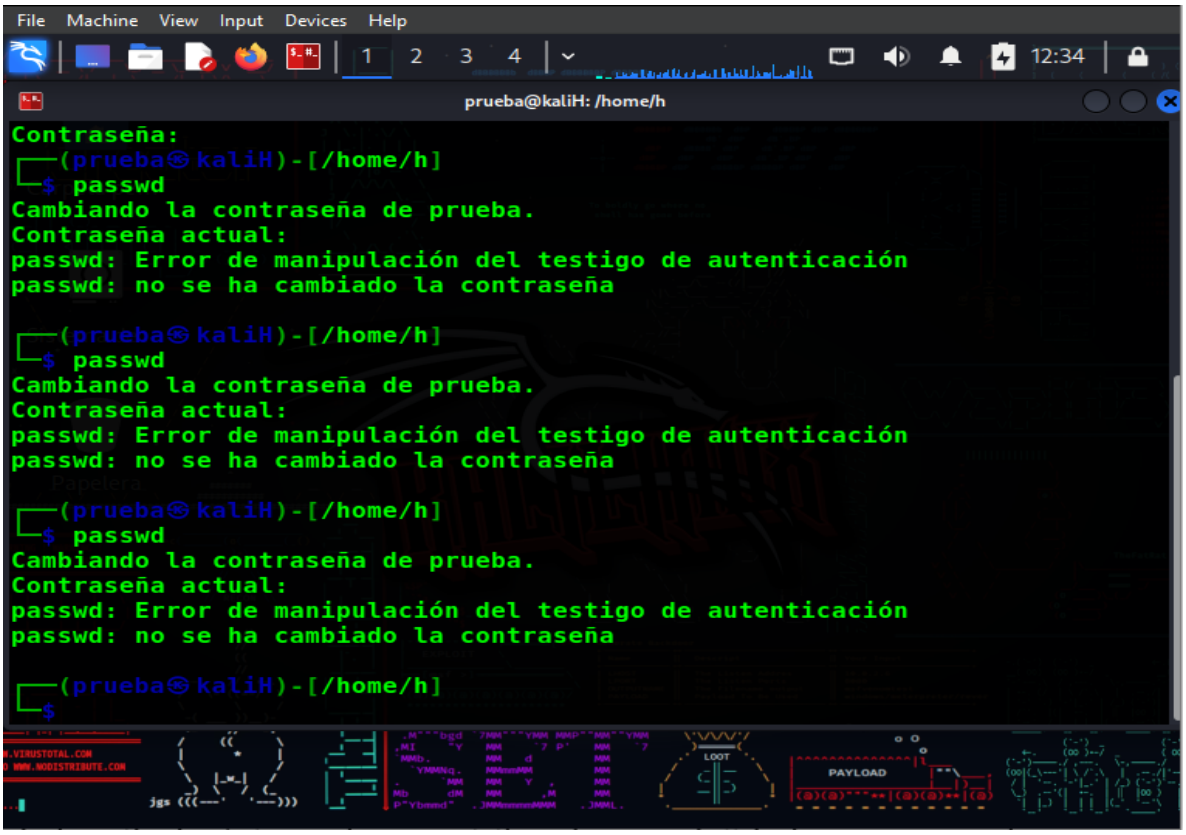
Paso 3: implementación de bloque de cuenta por fallo

```
kali@kali: ~
File  Actions  Edit  View  Help
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=2 default=ignore]      pam_unix.so nullok
auth    [success=1 default=ignore]      pam_winbind.so krb5_auth krb5_ccache_type
=FILE cached_login try_first_pass
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
aut     required                        pam_faillock.so preauth silent deny=7
unlock_time=420
auth    [default=die]                   pam_faillock.so authfail deny=7
unlock_time=900
~
~
~
~
~
-- INSERT --                                                    30,16         Bot
```

en Windows:



PASO 4: Verificación de las contraseñas



Paso 5 : Verificación de bloqueo de cuenta