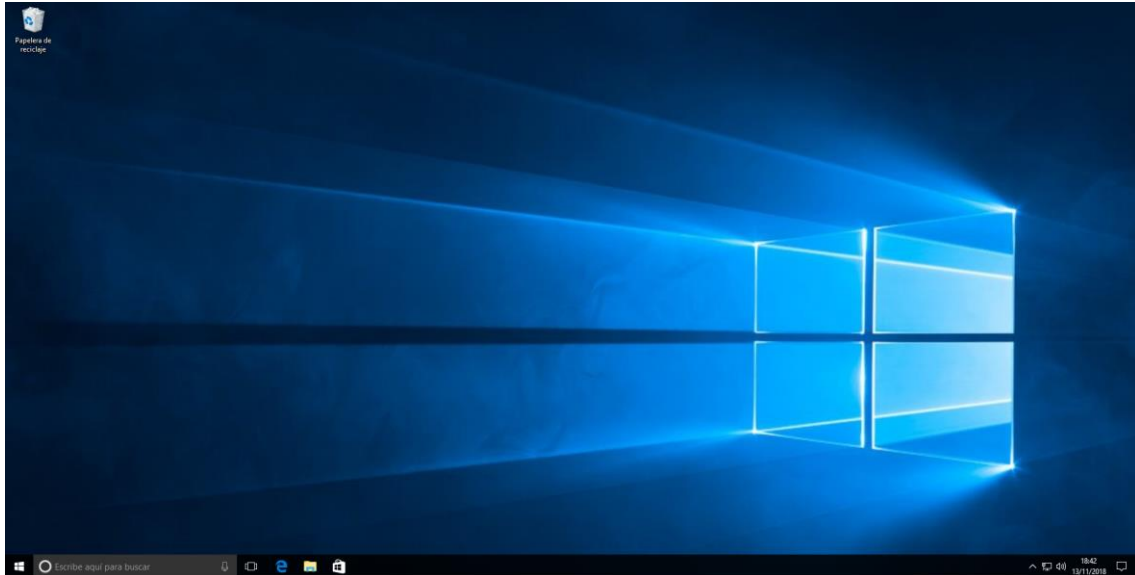
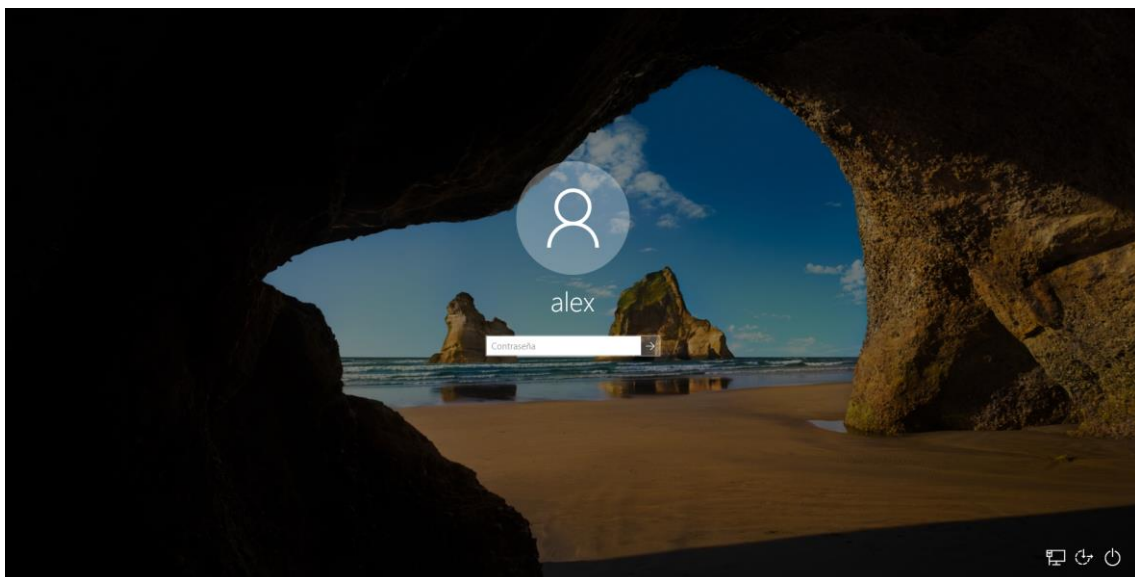


Destruir contraseñas de Windows y Linux

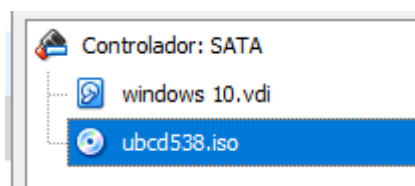
Vamos a romper la contraseña de un sistema operativo Windows. Para eso vamos a usar Ultimate boot CD. Esta herramienta nos permite romper contraseñas para poder acceder al ordenador, en este caso la utilizaremos para entrar en un sistema Windows en concreto un Windows 10.



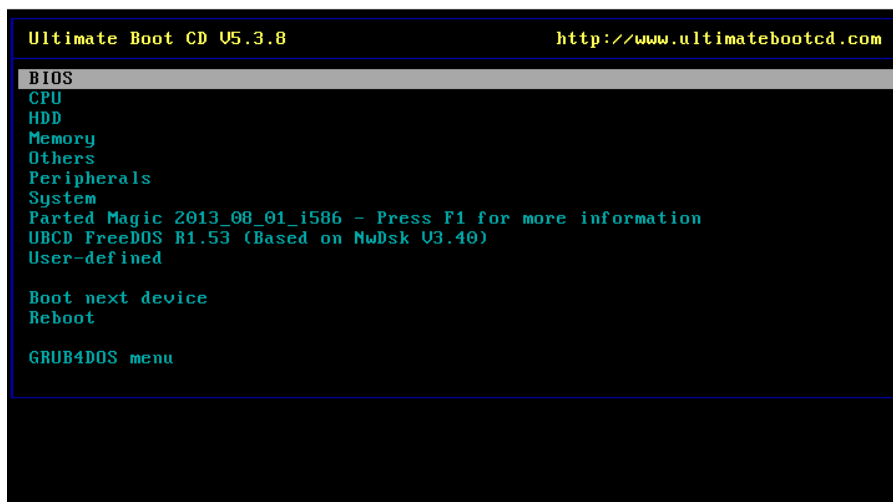
Como podemos ver este equipo tiene contraseña por lo que vamos a quitársela con el Ultimate boot CD.



Debemos arrancar el de desde el BIOS para que se inicie, ya que es un CD arrancable

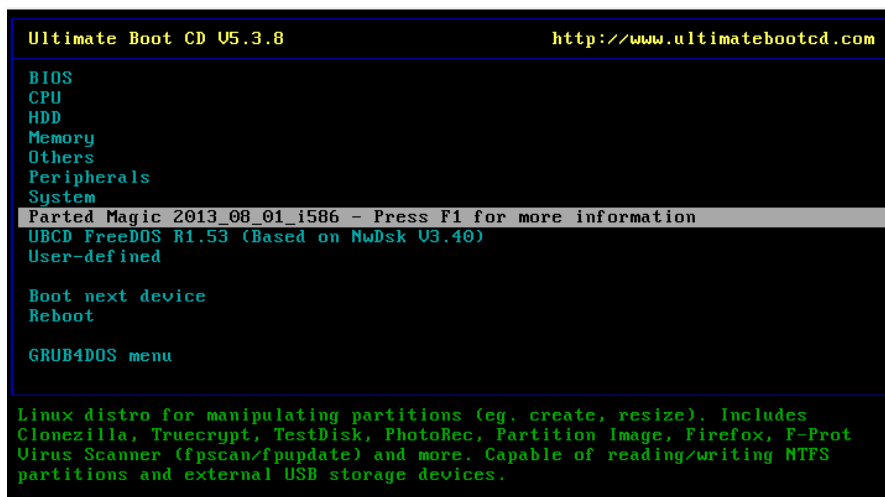


Una vez arrancado veremos este menú.

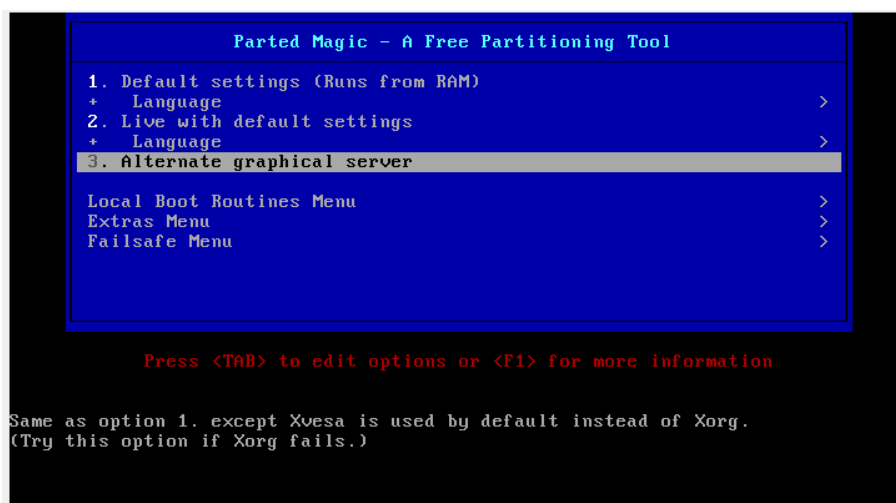


Vamos a arrancar el entorno grafico para que sea más cómodo.

Le damos a Parted magic.

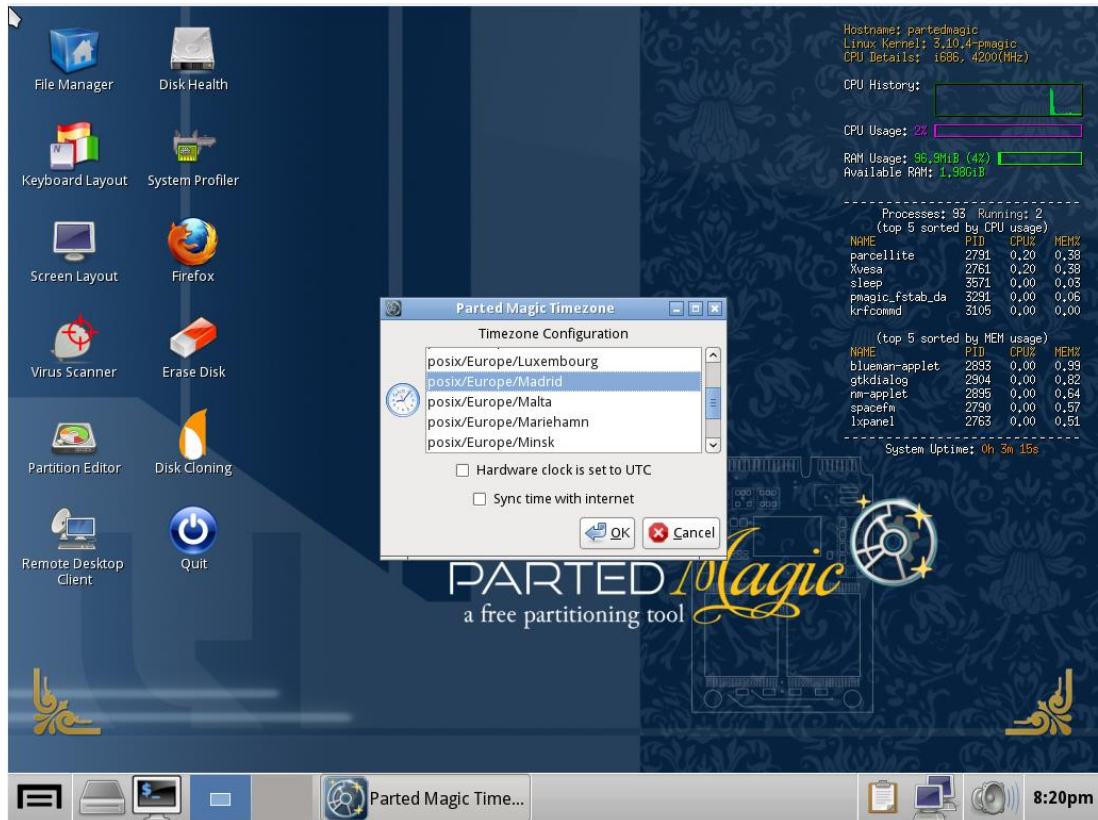


Y alternate grafical server.

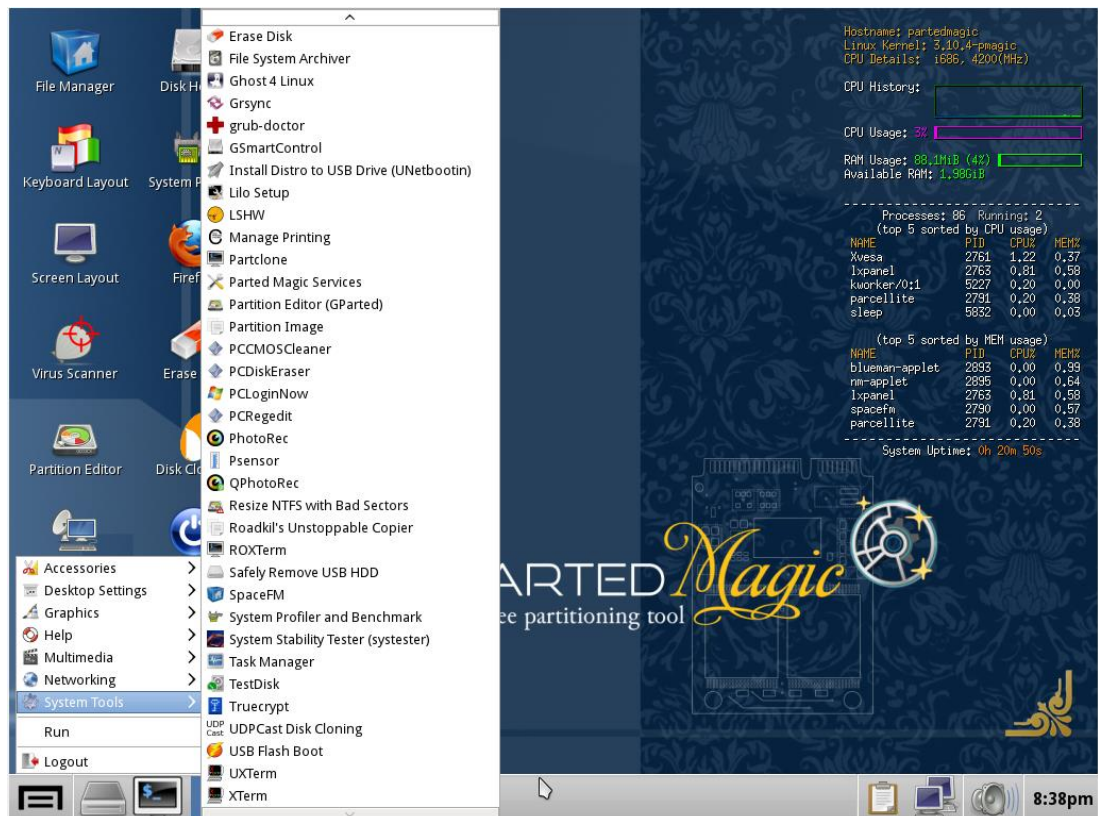


Ahora nos entrara en modo gráfico.

Nos da a elegir la zona horaria y todo.

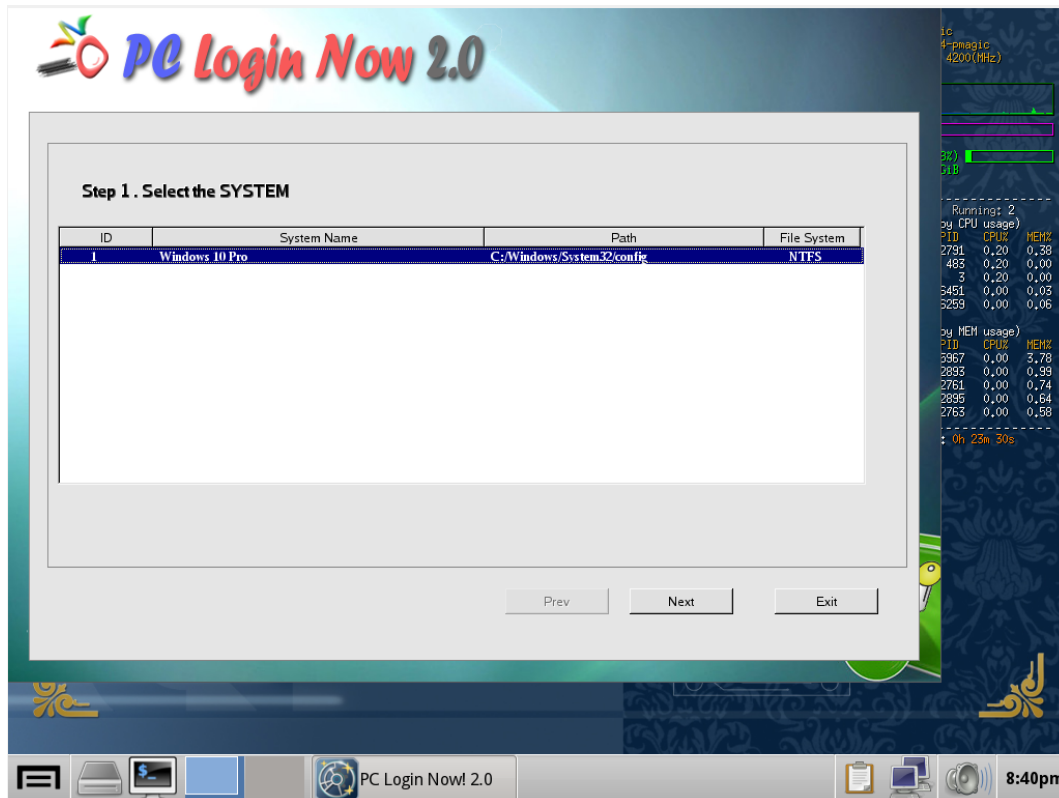


Nos metemos en la parte que estaría el inicio de Windows, system tool, y PCLogin now.

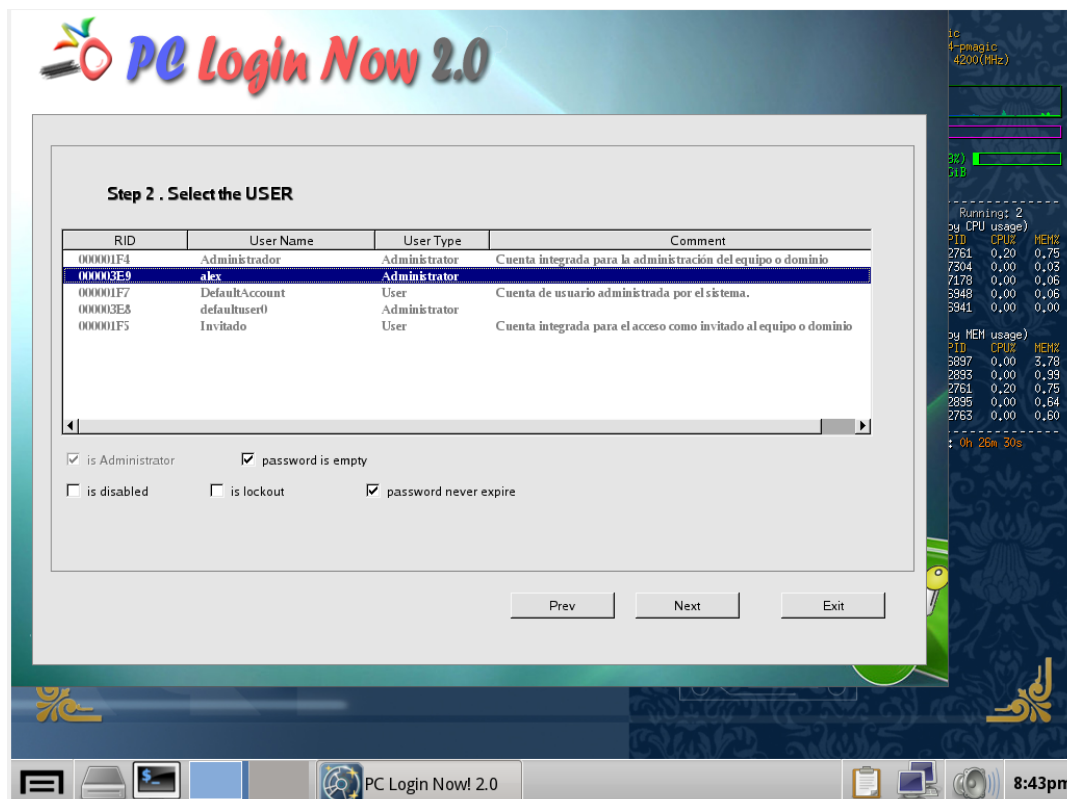


En cuanto se nos inicie le damos a siguiente.

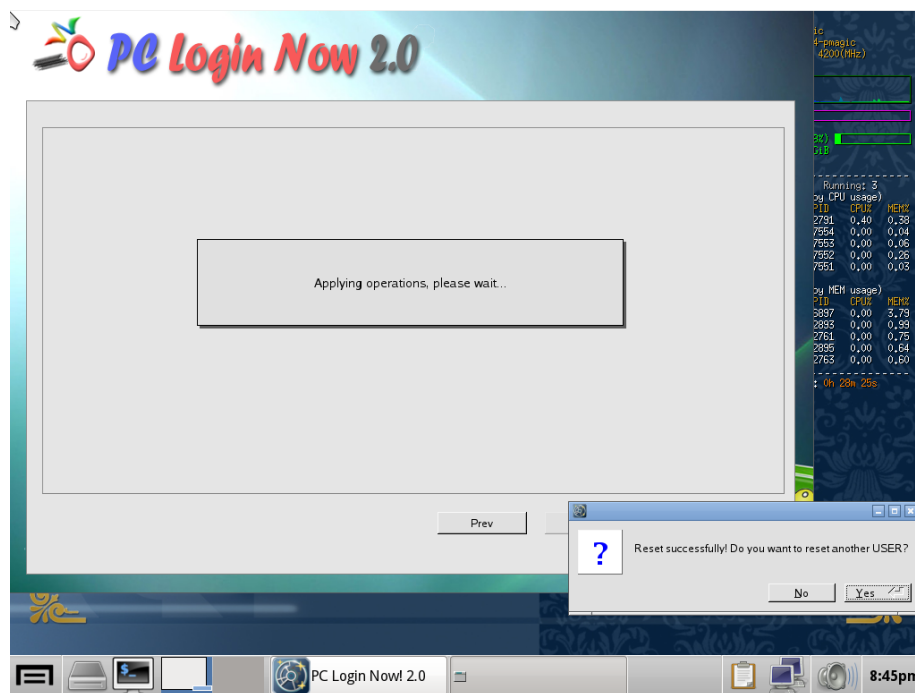
Seleccionamos el sistema operativo (no hay muchos que seleccionar la verdad).



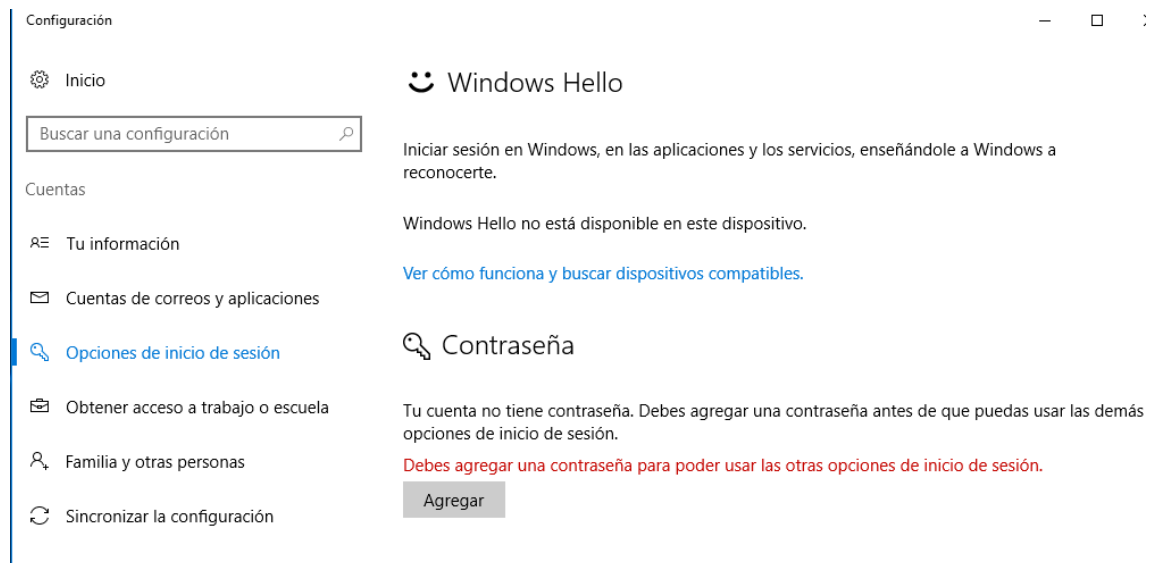
Seleccionamos la cuenta a la que queremos quitar la contraseña (importante, debemos marcar la casilla de la contraseña esta vacía).



Le damos que si para confirmar.



Y al iniciar veremos que nuestro usuario no tiene contraseña.



Actividad 5.

Vamos a ver como des encriptar las contraseñas de Linux.

Antes se usaba una distribución llamada BackTrack pero actualmente esta obsoleta



Por lo que utilizaremos Kali Linux.



Y usaremos el programa John the Ripper que esta herramienta viene con el Kali Linux



Bueno este método sería en caso de que nosotros seamos root y tengamos un usuario en nuestro equipo que queremos saber su contraseña

```
root@kali:~# cd /home
root@kali:/home# ls
matias_el_del_seguro
root@kali:/home#
```

Si nos vamos al archivo passwd veremos que la contraseña esta cifrada.

```
root@kali: /etc
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 2.9.8                                passwd

inetsim:x:122:129::/var/lib/inetsim:/usr/sbin/nologin
sshd:x:123:65534:./run/sshd:/usr/sbin/nologin
speech-dispatcher:x:124:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
couchdb:x:125:132:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
gluster:x:126:133:./var/lib/glusterd:/usr/sbin/nologin
geoclue:x:127:134:./var/lib/geoclue:/usr/sbin/nologin
colord:x:128:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
saned:x:129:137:./var/lib/saned:/usr/sbin/nologin
avahi:x:130:138:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
pulse:x:131:139:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
dradis:x:132:141:./var/lib/dradis:/usr/sbin/nologin
king-phisher:x:133:142:./var/lib/king-phisher:/usr/sbin/nologin
beef-xss:x:134:143:./var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:x:135:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:./sbin/nologin
matias_el_del_seguro:x:1000:1000:Matias,,,:/home/matias_el_del_seguro:/bin/bash

^G Ver ayuda  ^O Guardar  ^W Buscar  ^K Cortar txt  ^J Justificar  ^C Posición
^X Salir      ^R Leer fich.  ^_ Reemplazar  ^U Pegar txt  ^T Ortografía  ^_ Ir a línea
```

También podemos intentar ver la contraseña en el fichero shadow (pero saldrá cifrada).

```
Aplicaciones ▾ Lugares ▾ Terminal ▾ mié 19:29
root@kali: /etc
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.8 shadow

Debian-snmp:!:17785:0:99999:7:::
stunnel4:!:17785:0:99999:7:::
rtkit:!:17785:0:99999:7:::
ssllh:!:17785:0:99999:7:::
inetsim:!:17785:0:99999:7:::
sshd:!:17785:0:99999:7:::
speech-dispatcher:!:17785:0:99999:7:::
couchdb:!:17785:0:99999:7:::
gluster:!:17785:0:99999:7:::
geoclue:!:17785:0:99999:7:::
colord:!:17785:0:99999:7:::
saned:!:17785:0:99999:7:::
avahi:!:17785:0:99999:7:::
pulse:!:17785:0:99999:7:::
dradis:!:17785:0:99999:7:::
king-phisher:!:17785:0:99999:7:::
beef-xss:!:17785:0:99999:7:::
Debian-gdm:!:17785:0:99999:7:::
systemd-coredump:!:17838:!:!:!:
matias_el_del_seguro:$6$7Mb1d.ZP$AsHASr0Wayb/cTjpJ1YQfsqx14RrkChGA5HC4TxCXk2ep7nwnjW4$

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

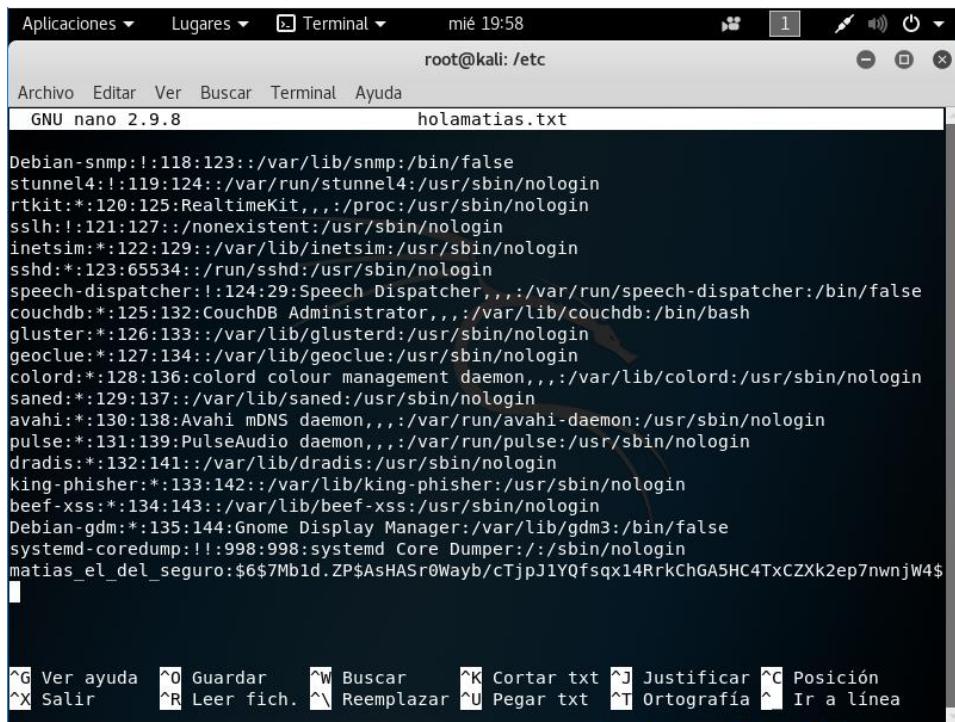
Vamos a mezclar estos dos archivos con el comando unshadow.

```
root@kali: /etc# unshadow /etc/passwd /etc/shadow > holamatias.txt
```

Y comprobamos

```
root@kali: /etc# ls
adduser.conf      gdm3             mime.types        rsyslog.d
adjtime           geoclue          minicom          rygel.conf
aliases          ghostscript      miredo           samba
alternatives     glvnd            miredo.conf      sane.d
amap             gnome            mke2fs.conf      scalpel
anacrontab       groff            modprobe.d       screenrc
apache2          group            modules           sddm.conf
apg.conf         group-           modules-load.d   searchsploit_rc
apm              grub.d           motd              securetty
apparmor         gshadow          mtab             security
apparmor.d       gshadow-        mysql            selinux
appstream.conf   gss              nagios-plugins   sensors3.conf
apt              gssapi_mech.conf nanorc            sensors.d
arpwatch         gtk-2.0          netsniff-ng      services
avahi            gtk-3.0          NetworkManager   sgml
bash.bashrc      hdparm.conf     networks         shadow
bash_completion  holamatias.txt  newt             shadow-
bash_completion.d
```

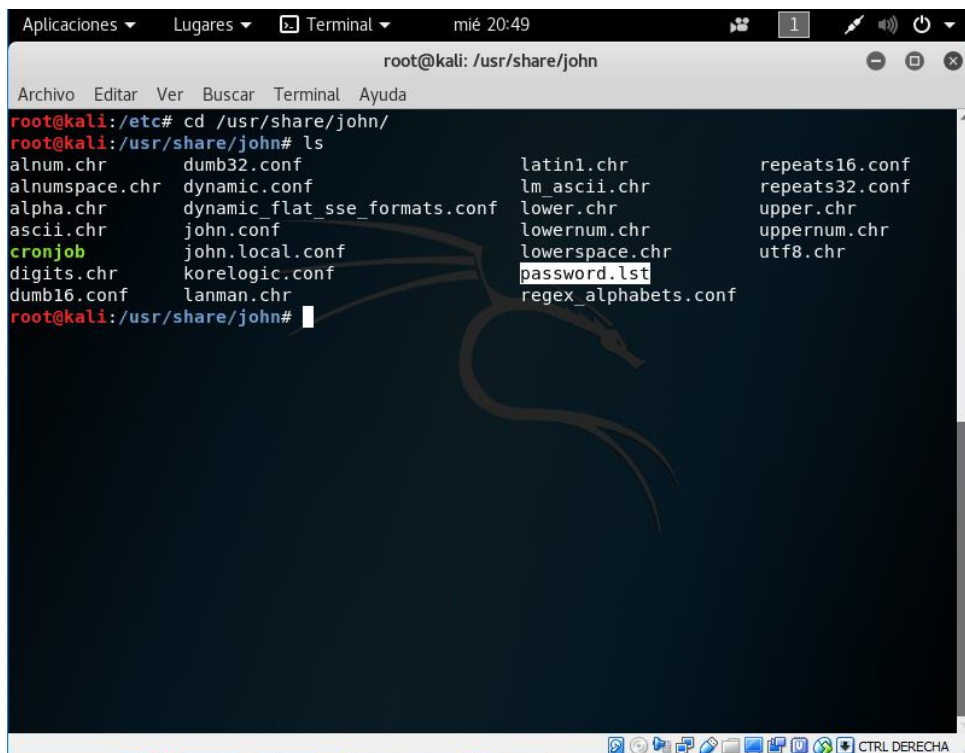

Ahora si miramos dentro del fichero, y veremos que donde nos aparecía antes la x ahora nos aparece toda la contraseña.



```
root@kali: /etc
GNU nano 2.9.8 holamatias.txt
Debian-snmp:!:118:123::/var/lib/snmp:/bin/false
stunnel4:!:119:124::/var/run/stunnel4:/usr/sbin/nologin
rtkit:!:120:125:RealtimeKit,,,:/proc:/usr/sbin/nologin
sshd:!:121:127::/nonexistent:/usr/sbin/nologin
inetsim:!:122:129::/var/lib/inetsim:/usr/sbin/nologin
sshd:!:123:65534::/run/sshd:/usr/sbin/nologin
speech-dispatcher:!:124:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
couchdb:!:125:132:CouchDB Administrator,,,:/var/lib/couchdb:/bin/bash
gluster:!:126:133::/var/lib/glusterd:/usr/sbin/nologin
geoclue:!:127:134::/var/lib/geoclue:/usr/sbin/nologin
colord:!:128:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
saned:!:129:137::/var/lib/saned:/usr/sbin/nologin
avahi:!:130:138:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
pulse:!:131:139:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
dradis:!:132:141::/var/lib/dradis:/usr/sbin/nologin
king-phisher:!:133:142::/var/lib/king-phisher:/usr/sbin/nologin
beef-xss:!:134:143::/var/lib/beef-xss:/usr/sbin/nologin
Debian-gdm:!:135:144:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:!:998:998:systemd Core Dumper:/:/sbin/nologin
matias_el_del_seguro:$6$7Mb1d.ZP$AsHASr0Wayb/cTjpJ1YQfsqx14RrkChGA5HC4TxCXk2ep7nwnjW4$
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^E Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Ahora vamos al directorio donde se encuentra John.

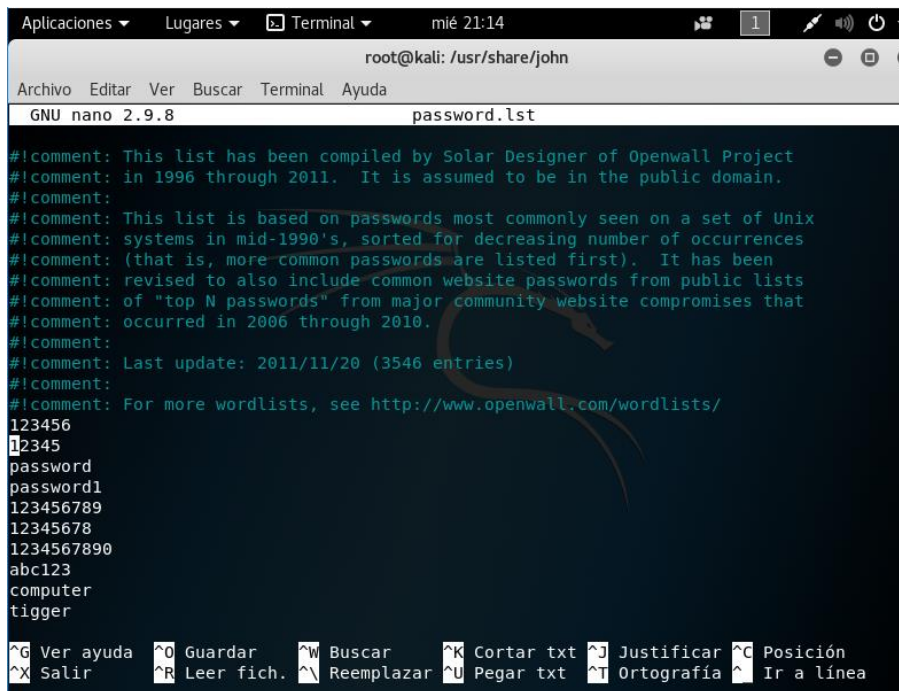
Miramos dentro del directorio y veremos que tenemos un fichero llamado password.lst.



```
root@kali: /usr/share/john
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:/etc# cd /usr/share/john/
root@kali:/usr/share/john# ls
alnum.chr          dumb32.conf        latin1.chr          repeats16.conf
alnumspace.chr     dynamic.conf       lm_ascii.chr        repeats32.conf
alpha.chr          dynamic_flat_sse_formats.conf lower.chr            upper.chr
ascii.chr           john.conf           lowernum.chr         uppernum.chr
cronjob             john.local.conf     lowerspace.chr        utf8.chr
digits.chr          korelogic.conf      regex_alphabets.conf
dumb16.conf         lanman.chr
root@kali:/usr/share/john#
```

Nos metemos en ese fichero.

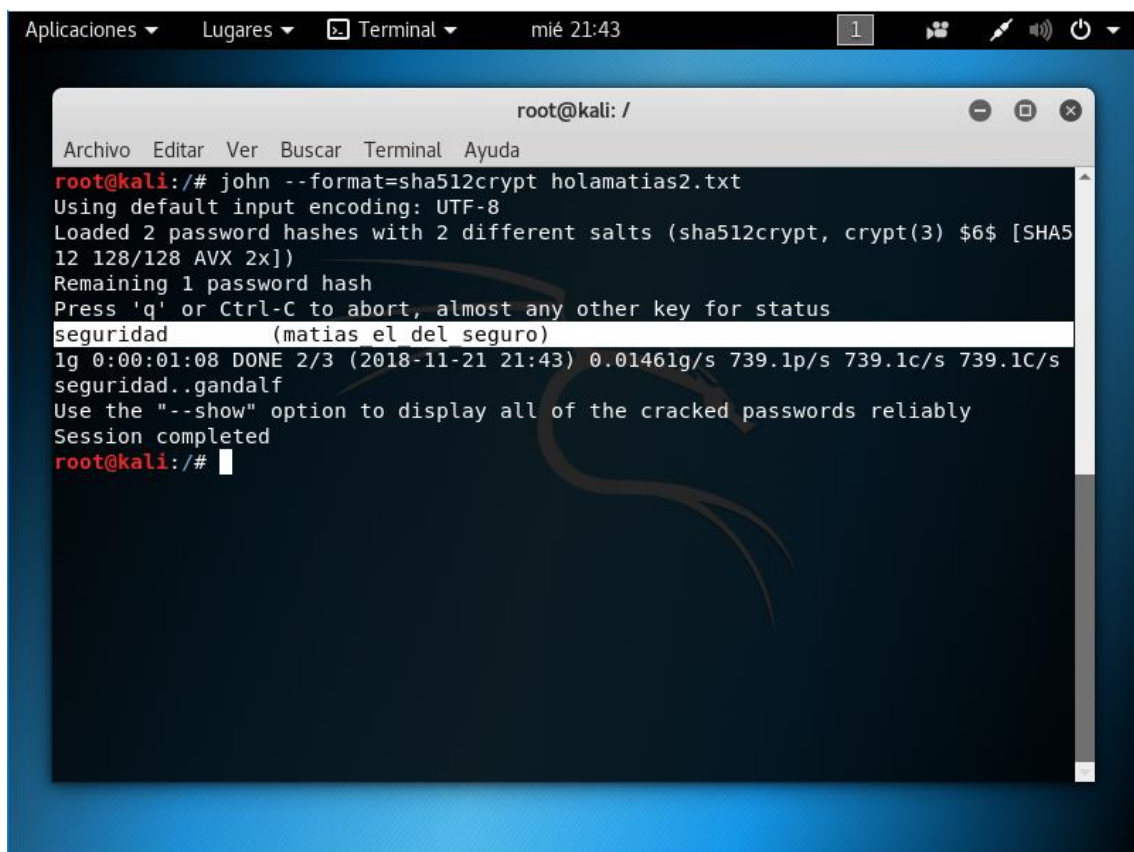
Y nos aparecerá una lista con distintas contraseñas (si nuestra contraseña estuviera en esta lista sería de las más inseguras que puede haber).



```
root@kali: /usr/share/john
GNU nano 2.9.8 password.lst
#!/comment: This list has been compiled by Solar Designer of Openwall Project
#!/comment: in 1996 through 2011. It is assumed to be in the public domain.
#!/comment:
#!/comment: This list is based on passwords most commonly seen on a set of Unix
#!/comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!/comment: (that is, more common passwords are listed first). It has been
#!/comment: revised to also include common website passwords from public lists
#!/comment: of "top N passwords" from major community website compromises that
#!/comment: occurred in 2006 through 2010.
#!/comment:
#!/comment: Last update: 2011/11/20 (3546 entries)
#!/comment:
#!/comment: For more wordlists, see http://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tiger
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^N Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

El gran defecto de esta aplicación es ese.

Ejecutamos John y podremos cual es la contraseña de Matías.



```
root@kali: /
Archivo Editar Ver Buscar Terminal Ayuda
root@kali: /# john --format=sha512crypt holamatias2.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 AVX 2x])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
seguridad (matias el del seguro)
lg 0:00:01:08 DONE 2/3 (2018-11-21 21:43) 0.01461g/s 739.1p/s 739.1c/s 739.1C/s
seguridad..gandalf
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali: /#
```