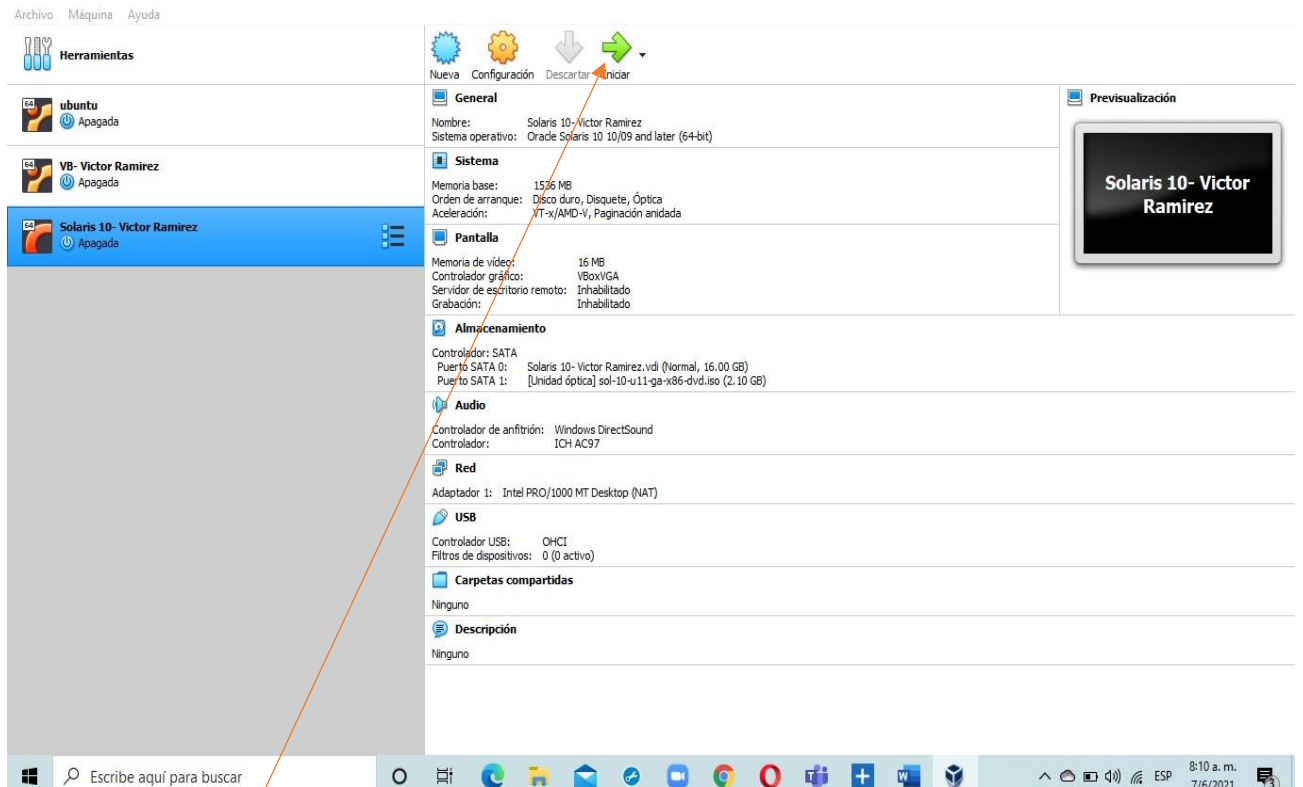


Configuración de Seguridad Solaris 10



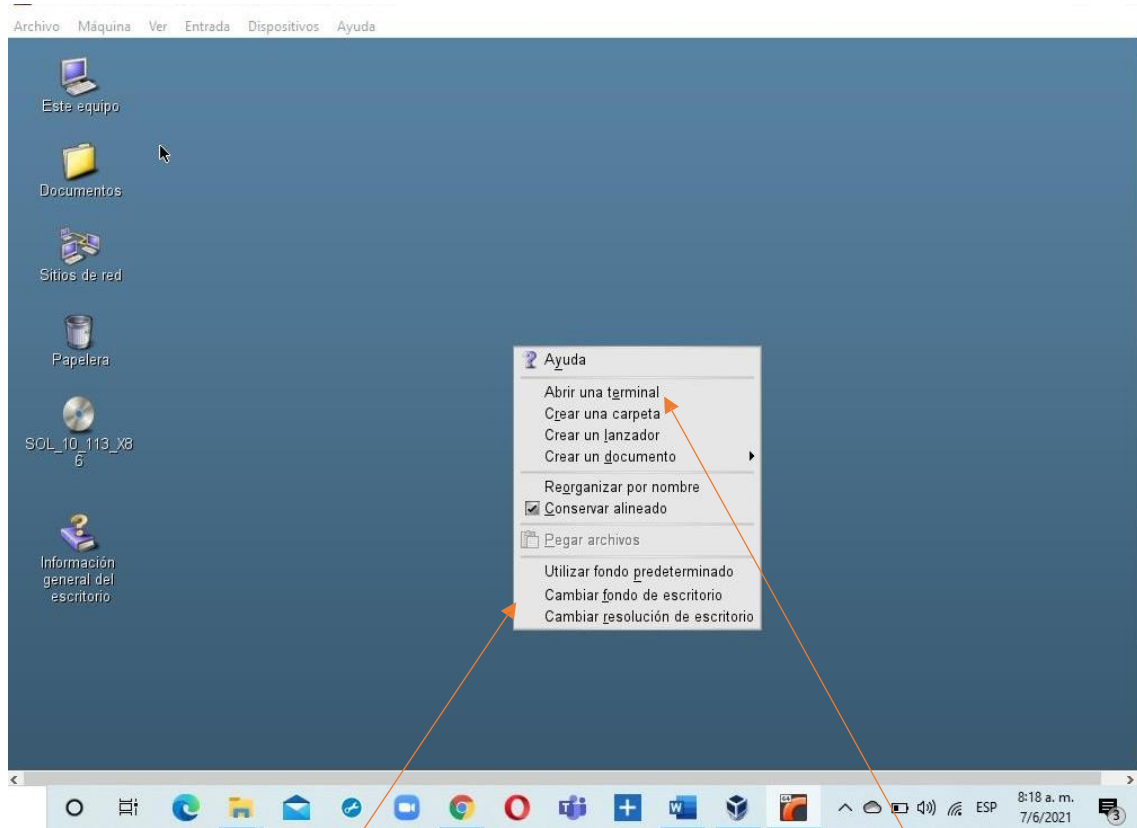
BY: JOSE CUSTODIO

Paso 1



Iniciamos nuestra maquina virtual como nuestro sistema operativo solaris 10.

Paso 2



Primero hacemos clic derecho para abrir este recuadro de opciones.

Clic aquí para abrir una nueva terminal.

Paso 3

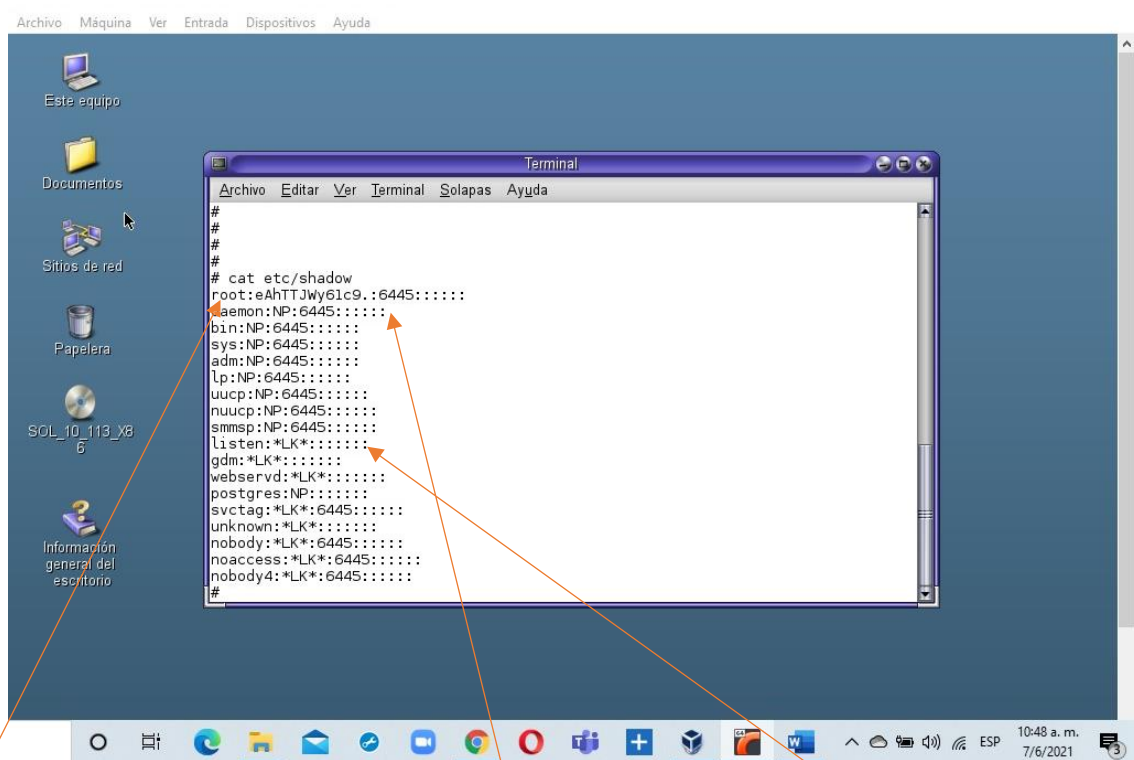
```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

# cat /etc/passwd
root:x:0:0:Super-User:/sbin/sh
daemon:x:1:1:/:
bin:x:2:2:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smmsp:x:25:25:SendMail Message Submission Program:/
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/
webservd:x:80:80:WebServer Reserved UID:/
postgres:x:90:90:PostgreSQL Reserved UID:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/
unknown:x:96:96:Unknown Remote UID:/
nobody:x:60001:60001:NFS Anonymous Access User:/
noaccess:x:60002:60002:No Access User:/
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/
#
```

En la terminal digitamos: cat
etc/passwd

Debemos de asegurarnos de que el parámetro
“x” sea el que le prosiga al nombre del usuario
separado por “:” en medio.

Paso 4



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

#
#
#
# cat etc/shadow
root:eAhTTJWy61c9.:6445::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
smmsp:NP:6445::::::
listen:*LK*:::::::
gdm:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
unknown:*LK*:::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
#
```

Para poder ver la contraseña encriptada digitamos: cat

Desde Daemon hasta smmsp es relacionado. NP: No Password

Desde listen hasta nobody es relacionado. LK: Locked

Paso 5

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
# cat etc/default/login
#ident "@(#)login.dfl 1.14 04/06/25 SMI"
#
# Copyright 2004 Sun Microsystems, Inc. All rights reserved.
# Use is subject to license terms.
#
# Set the TZ environment variable of the shell.
#
#TIMEZONE=ESTSEDT
#
# ULIMIT sets the file size limit for the login. Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0
#
# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console
#
# PASSREQ determines if login requires a password.
#
PASSREQ=YES
#
# ALTSHELL determines if the SHELL environment variable should be set
#
ALTSHELL=YES
#
# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:
#
# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin
#
# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
#TIMEOUT=300
```

Digitamos: cat
etc/default/login

Revisamos que este parámetro no tenga un signo de # delante, si lo tiene significa que no se requiere de contraseña para entrar al sistema.

Paso 6

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
#
# cat etc/default/passwd
#ident "@(#)passwd.dfl 1.7      04/04/22 SMI"
#
# Copyright 2004 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
MAKWEELS=
MINWEELS=
PASSLENGTH=6
#
# NAMECHECK enables/disables login name checking.
# The default is to do login name checking.
# Specifying a value of "NO" will disable login name checking.
#
#NAMECHECK=NO
#
# HISTORY sets the number of prior password changes to keep and
# check for a user when changing passwords.  Setting the HISTORY
# value to zero (0), or removing/commenting out the flag will
# cause all users' prior password history to be discarded at the
# next password change by any user.  No password history will
# be checked if the flag is not present or has zero value.
# The maximum value of HISTORY is 26.
#
# This flag is only enforced for user accounts defined in the
# local passwd(4)/shadow(4) files.
#
#HISTORY=0
#
# Password complexity tunables.  The values listed are the defaults
# which are compatible with previous releases of passwd.
# See passwd(1) and pam_authok_check(5) for use warnings and
# discussion of the use of these options.
#
#MINDIFF=3
#MINALPHA=2
#MINNONALPHA=1
#MINUPPER=0
#MINLOWER=0
#MAXREPEATS=0
#MINSPECIAL=0
#MINDIGIT=0
```

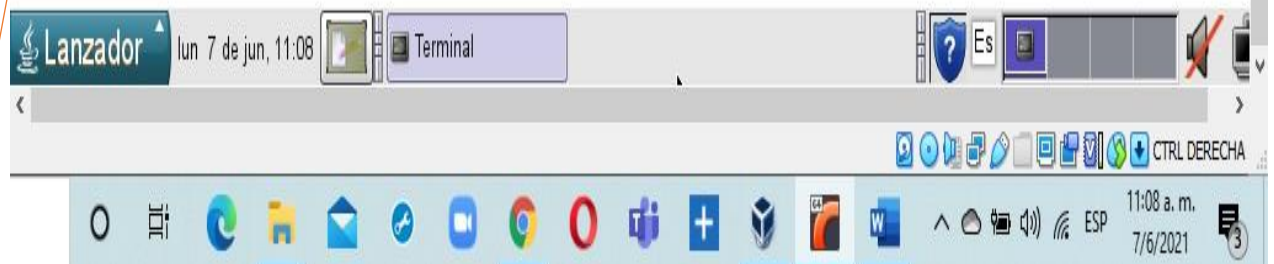
Digitamos cat
etc/default/passwd

Significado de los parámetros en la siguiente página.

- MAXWEEKS= máximo tiempo en semanas de la validez de la contraseña.
- MINWEEKS= mínimo tiempo en semanas en que la contraseña puede ser cambiada.
- PASSLENGTH= longitud de la contraseña.
- NAMECHEK= se comprueba si el nombre de usuario y contraseña son iguales.
- HISTORY= Número de contraseñas guardadas para evitar que se repitan.
- MINDIFF= Diferencia mínima entre la nueva contraseña y las antiguas.
- MINALPHA= Número mínimo de caracteres alfanuméricos.
- MINNONALPHA= Número mínimo de caracteres no alfanuméricos.
- MINUPPER= Número mínimo de mayúsculas.
- MINLOWER= Número mínimo de minúsculas.
- MAXREPEAT= Número de veces que se puede repetir un carácter.
- MINSPECIAL= Número mínimo de caracteres especiales (@#%).
- MINDIGIT = Número mínimo de dígitos.
- WHITESPACE= Si se permiten espacio en blanco o tabs en las contraseñas.

Paso 7

```
π  
# cat etc/hosts  
#  
# Internet host table  
#  
::1      localhost  
127.0.0.1 localhost  
10.0.2.15 unknown # Added by DHCP  
#
```



Digitamos `cat etc/hosts` para verificar que solo el host local y el protocolo que asigna los parámetros de la configuración de red de manera automática (DHCP) se encuentran definidos.



FIN