

Experto Universitario en Ethical Hacking

Módulo 3:

Hardening (Windows Servers o Linux Servers)

Unidad 3:

Configuraciones y servicios (Parte 02)



Presentación

En esta tercer Unidad del módulo, se conocerán las configuraciones de seguridad principales, pero en este caso, se avanza con los servicios relacionados a SO Linux.

También se aprenderá que tener en cuenta con respecto a un buen Hardening en los servidores.



Objetivos

Que los participantes logren...

- Conocer sobre el mundo de los servidores informáticos, existentes en toda infraestructura informática de mediana y alta gama.
- Conocer las herramientas esenciales y las buenas prácticas necesarias para obtener el máximo nivel de seguridad en una red de servidores de arquitectura Microsoft Windows Server o Linux Server, protegiéndola de potenciales amenazas.
- Comprender los conceptos básicos referentes a la implementación, configuración, mantenimiento y soporte de servidores de infraestructura en tecnologías Windows o Linux.



Bloques temáticos

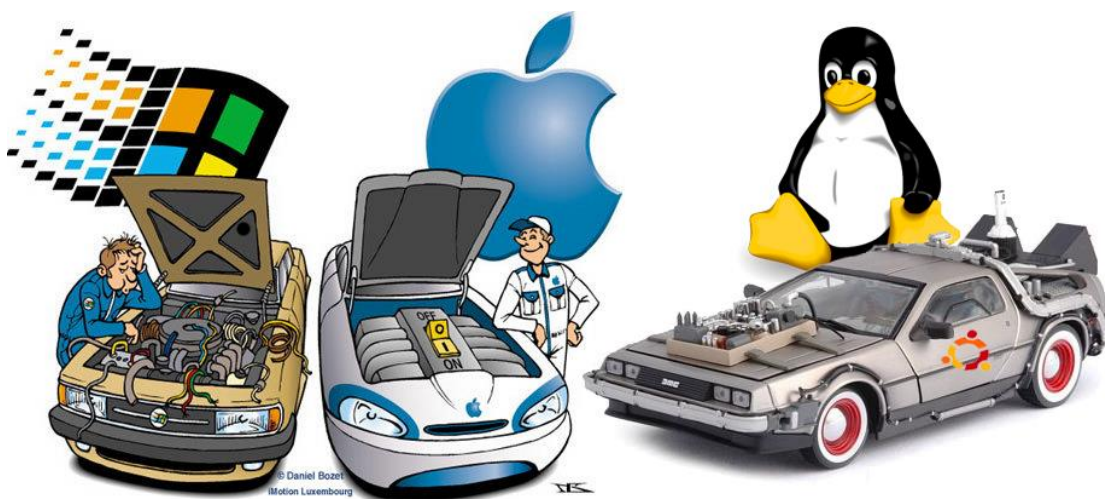
1. Hardening en Linux
2. Ejemplos
3. Material obsequio: Hardening en PHP

Hardening en Linux



En esta unidad hablaremos de un sistema operativo, cuya funciones son las mismas que se utilizan en otros sistemas, pero más accesible cuando se habla de la configuración.

Muchos pensaron que Linux, es muy complicado de configurar, asegurar y hasta el entorno de “mantenerlo”, sin embargo hoy en día está considerado como uno de los más seguros, aun pensando que se trata de “código abierto”.



¿Será tan así o es más que nada nuestro pensamiento de acuerdo a la experiencia que se tenga en el sistema operativo?

Arranquemos con unos comandos sencillos, para los que recién se inicien en este SO.

Comando CAT

Utilizado para mostrar los datos de un archivo o más en la pantalla y/o unir varios archivos juntos en un solo archivo y hasta crear un archivo de cero.

```
(root@kali)-[/home/kali]
# cat > test.txt
Prueba de crear archivo
^Z
```

cat > test.txt

Crea un archivo llamado “test.txt”, al darle **ENTER**, nos permite escribir su contenido y para salir y grabar, se puede utilizar la combinación de las teclas **CTRL y Z**.

```
(root@kali)-[/home/kali]
# cat test.txt
Prueba de crear archivo
```

cat test.txt

Muestra en la pantalla el contenido del archivo seleccionado llamado “test.txt”.

```
(root@kali)-[/home/kali]
# cat test.txt prueba.txt
Prueba de crear archivo
Segunda prueba de archivo
```

cat test.txt prueba.txt

Muestra en la pantalla el contenido de ambos archivos seleccionados, habiendo creado anteriormente uno llamado “prueba.txt”.



```
(root@kali)-[/home/kali]
# cat test.txt prueba.txt > resultado.txt

(root@kali)-[/home/kali]
# cat resultado.txt
Prueba de crear archivo
Segunda prueba de archivo
```

cat test.txt prueba.txt > resultado.txt

Combina los archivos test.txt y prueba.txt en un nuevo archivo llamado resultado.txt.

```
(root@kali)-[/home/kali]
# cat test1.txt >> resultado.txt

(root@kali)-[/home/kali]
# cat resultado.txt
Prueba de crear archivo
Segunda prueba de archivo
Tercera prueba
```

cat test1.txt >> resultado.txt

Adjuntar el archivo test1.txt al archivo resultado.txt.

```
(root@kali)-[/home/kali]
# cat >> resultado.txt
Prueba final
^Z
zsh: suspended cat >> resultado.txt

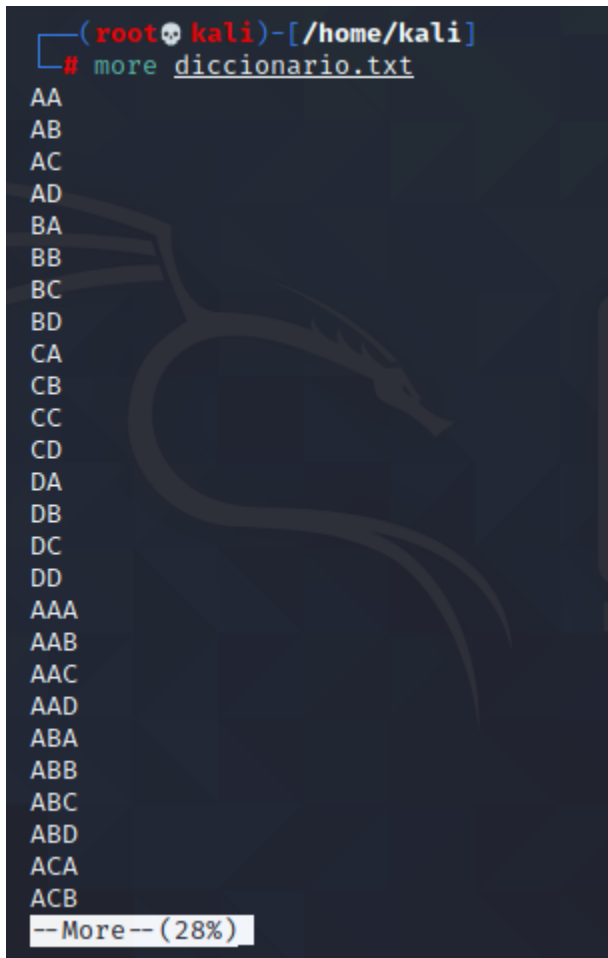
(root@kali)-[/home/kali]
# cat resultado.txt
Prueba de crear archivo
Segunda prueba de archivo
Tercera prueba
Prueba final
```

cat >> resultado.txt

Añade datos adicionales al archivo resultado.txt.

Comando MORE

Muestra en pantalla un archivo de texto seleccionado, visualizandolo por página, presionando la barra de espacio para ir a la página siguiente o por línea presionando el **ENTER**.



```
(rootkali)-[/home/kali]
# more diccionario.txt
AA
AB
AC
AD
BA
BB
BC
BD
CA
CB
CC
CD
DA
DB
DC
DD
AAA
AAB
AAC
AAD
ABA
ABB
ABC
ABD
ACA
ACB
--More-- (28%)
```

more diccionario.txt

Muestra en la consola el documento de una página a la vez, debido a que el contenido completo no se puede exponer en la pantalla, por una cuestión de espacio.

Tener en cuenta que este comando, es de visualización, se puede ver cualquier archivo, sin importar su contenido.

```
(root@kali)-[/home/kali]
# more -10 diccionario.txt
AA
AB
AC
AD
BA
BB
BC
BD
CA
CB
--More-- (9%)
```

more -num diccionario.txt

Muestra las primeras líneas seleccionadas del documento como se especifique en (**num**).

Ejemplo: **more -10 diccionario.txt** (muestra las 10 primeras líneas del archivo especificado).

```
(root@kali)-[/home/kali]
# more -10 diccionario.txt
AA
AB
AC
AD
BA
BB
BC
BD
CA
CB
CC
CD
DA
DB
DC
DD
AAA
AAB
AAC
AAD
ABA
ABB
ABC
ABD
ACA
ACB
ACC
--More-- (30%)
```

Al presionar la tecla **ENTER**, se puede bajar línea a línea.



Ejercicio Número 1 Unidad 3



Ejercicio de aprendizaje y ejercitación.

Averiguar el uso de los siguientes comandos: *LESS – TAIL - HEAD*

Postearlos en el foro, exponiendo una captura de ejemplo de uso de cada uno.

TIP: Al escribir en Linux, el comando “man” junto al comando que necesitamos saber, nos expondrá mucha información de ayuda del mismo.

Ejemplo:

```
(root@kali)-[/home/kali]
# man cat
```

```
CAT(1)                                User Commands
NAME
    cat - concatenate files and print on the standard output
SYNOPSIS
    cat [OPTION] ... [FILE] ...
DESCRIPTION
    Concatenate FILE(s) to standard output.
    With no FILE, or when FILE is -, read standard input.
    -A, --show-all          equivalent to -vET
    -b, --number-nonblank    number nonempty output lines, overrides -n
    -e                      equivalent to -vE
    -E, --show-ends          display $ at end of each line
    -n, --number             number all output lines
    -s, --squeeze-blank      suppress repeated empty output lines
Manual page cat(1) line 1 (press h for help or q to quit)
```

Seguridad física

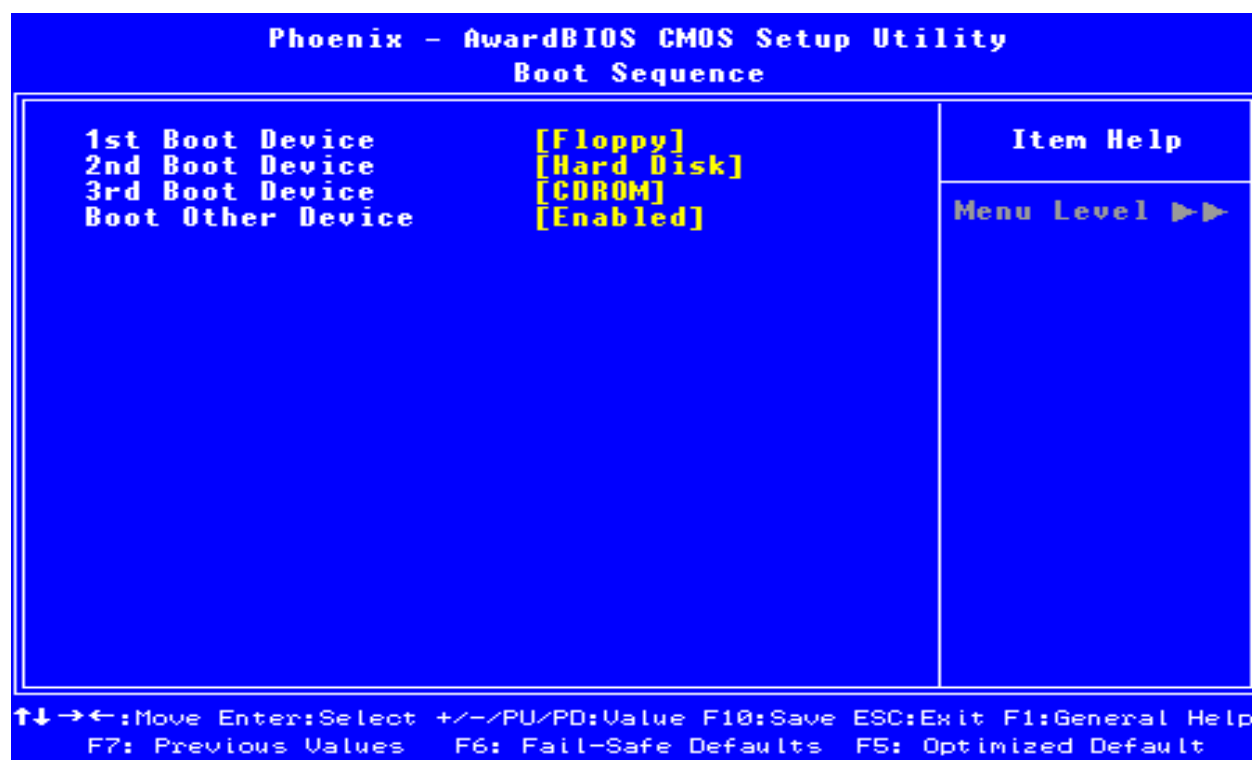
Se recomienda configurar el BIOS para deshabilitar el arranque desde CD / DVD, dispositivos externos, unidades de USB, de esa manera se evita que inserten un SO en formato Live (arrancar desde una unidad externa).

A continuación, se expone cómo habilitar la contraseña del BIOS y también como proteger el **GRUB** (es un gestor de arranque) con contraseña para restringir el acceso físico de su sistema.

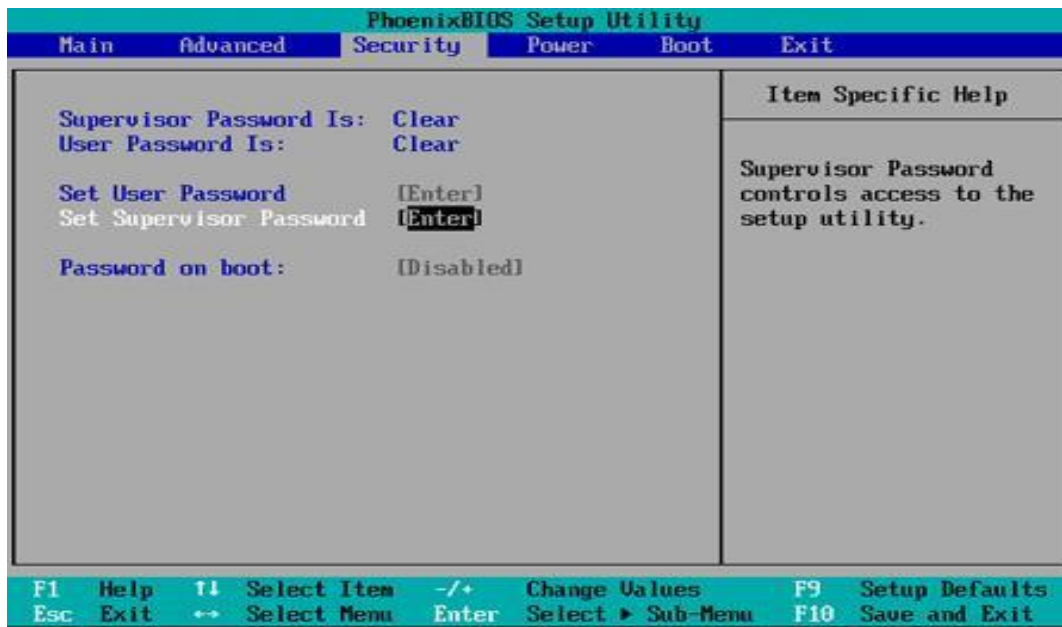
Antes: Que es GRUB?: http://es.wikipedia.org/wiki/GNU_GRUB

El BIOS de nuestros equipos, suele ser diferente de acuerdo a los **Vendors** y modelos, pero no cambia mucho generalmente el nombre de las opciones.

En primer medida, hay que cambiar el orden de booteo de los dispositivos, o sea indicar que queremos que bootee primero por nuestra unidad de disco primario.

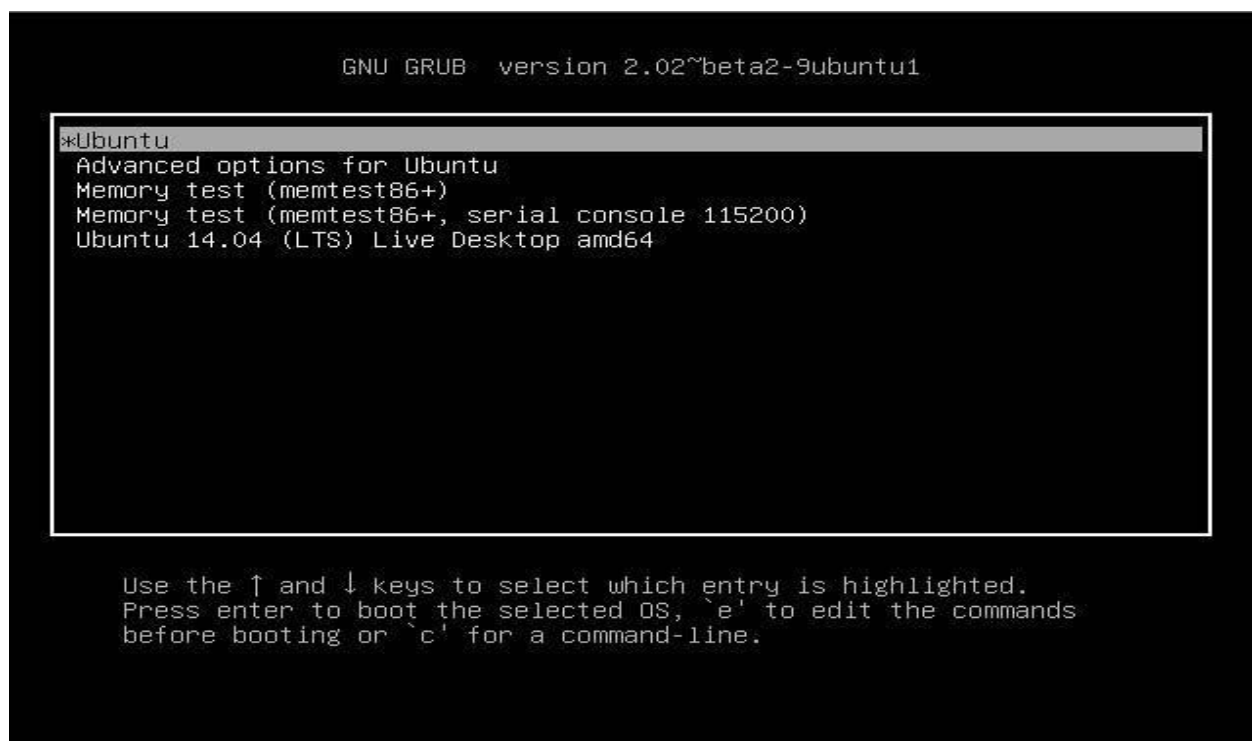


Para poder acceder al **BIOS**, consulte el manual de su equipo, pero generalmente puede ser presionando cuando arranca el equipo, algunas de las teclas de función.



En este caso, se configura para poder tener dos tipos de password, la de usuario interno y la de usuario supervisor (uno es de lectura, el otro de escritura)

Volviendo a GRUB, si un intruso llegara a tener acceso físico al equipo, podría reiniciar y **cambiar los parámetros de GRUB** para conseguir acceso como administrador al equipo.



Con insertar un 'l' o una 's' al final de la línea 'kernel' de GRUB para conseguir esa clase de acceso.

```
(root@kali)-[/home/kali]
# grub
Probing devices to guess BIOS drives. This may take a long time.

GNU GRUB  version 0.97  (640K lower / 3072K upper memory)

[ Minimal BASH-like line editing is supported.  For
  the first word, TAB lists possible command
  completions.  Anywhere else TAB lists the possible
  completions of a device/filename. ]

grub> md5crypt
md5crypt
Password: esto es una prueba
esto es una prueba
Encrypted: $1$KrEOH1$M6GRHjYeJ31N2xvNftvss1
grub> 
```

Abrimos una consola, y escribimos “**grub**” y le añadimos una contraseña, usando el comando “**md5crypt**”, donde nos devuelve la password cifrada.

Preguntará la contraseña que quieren utilizar.

Obtendrán una contraseña cifrada, que tendrán que guardar con mucho cuidado.

Si por algún motivo no lo tenemos instalado o disponemos de otra distribución, tendremos que escribir: “**apt install grub**” y de esa manera se instalará en el sistema (recordar, siempre depende de qué tipo de distribución se encuentran utilizando, hay comandos que no son los mismos)

```
(root@kali)-[/home/kali]
# apt install grub
Reading package lists... Done
Building dependency tree
```

De querer ver cómo queda todo configurado:

```
(root@kali)-[/home/kali]
# nano /boot/grub/grub.cfg
```

En otras distros:

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE: You have a /boot partition. This means that
#           all kernel and initrd paths are relative to /boot/, eg.
#           root (hd0,0)
#           kernel /vmlinuz-version ro root=/dev/sda3
#           initrd /initrd-[generic-]version.img
#boot=/dev/sda
default=0
timeout=5
password --md5 $1$TNUB/1$TwroGJn4eCd4xsYeGiBYq.
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-279.5.2.el6.i686)
    root (hd0,0)
    kernel /vmlinuz-2.6.32-279.5.2.el6.i686 ro root=UUID=d06b9517-8bb3-44db
    initrd /initramfs-2.6.32-279.5.2.el6.i686.img
title centos (2.6.32-71.el6.i686)
    root (hd0,0)
    kernel /vmlinuz-2.6.32-71.el6.i686 ro root=UUID=d06b9517-8bb3-44db-b8c5
    initrd /initramfs-2.6.32-71.el6.i686.img
```

- Editamos el archivo de configuración del menú de arranque de GRUB:

```
$ sudo gedit /boot/grub/menu.lst
```

Buscamos la siguiente línea:

```
#password topsecret
```

- Borramos la almohadilla o numeral (#) de la línea, haciendo esto la descomentaremos. Debe quedar así:

```
password topsecret
```

- Guardamos el archivo y cerramos el editor.

Editamos el archivo menu.lst, buscamos la línea correspondiente a #password, le sacamos el signo de # para que quede sin el mismo, y a continuación ponemos la password que seleccionamos antes (la contraseña en formato cifrado).


A tener en cuenta:

Lo que antes se conocía como menu.lst ahora se genera automáticamente con el comando update-grub2, el cual escribe el **grub.cfg**

Una buena práctica es poner esto en un archivo **custom**, para no mezclar lo nuestro con lo nativo.

Se recomienda crear y hacer todo en **/etc/grub.d/40_custom** para separar las aguas, y no tocar el header.

Esta técnica que hablamos anteriormente, fue actualizada, por GRUB 2, lo cual nos permite un mayor control, por ejemplo, definir un usuario privilegiado para esos cambios que hablamos anteriormente.



```
DesdeLinux : bash - Terminal
sudo nano /etc/grub.d/00_header

Al final pegá lo siguiente:

DesdeLinux : bash - Terminal
cat < < EOF
set superusers="user1"
password user1 password1
EOF

Donde user1 es el superusuario, ejemplo:

DesdeLinux : bash - Terminal
cat < < EOF
set superusers="superusuario"
password superusuario 123456
EOF
```

Creación de particiones

Es importante tener diferentes particiones para obtener mayor seguridad de los datos en caso de que ocurra cualquier accidente.

Mediante la creación de diferentes particiones, los datos pueden ser separados y agrupados. Cuando se produce un accidente inesperado, sólo los datos de la partición se dañarán, mientras que los datos en otras particiones podrán salvarse.

Asegurar de que dispone de las siguientes particiones separadas y de que las aplicaciones de terceros se deban instalar en los sistemas de archivos independientes en **/ opt**.


```

lab_utm@labutn-desktop: /
Archivo Editar Ver Terminal Ayuda
total 96
drwxr-xr-x  2 root 4096 2013-09-05 20:09 bin
drwxr-xr-x  3 root 4096 2013-09-05 20:10 boot
drwxr-xr-x  2 root 4096 2013-09-05 19:52 cdrom
drwxr-xr-x 16 root 3600 2013-09-05 20:52 dev
drwxr-xr-x 128 root 12288 2013-09-05 20:58 etc
drwxr-xr-x  3 root 4096 2013-09-05 19:57 home
lrwxrwxrwx  1 root  33 2013-09-05 20:09 initrd.img -> boot/initrd.img-2.6.32-24-generic
drwxr-xr-x 20 root 12288 2013-09-05 20:09 lib
drwx----- 2 root 16384 2013-09-05 19:50 lost+found
drwxr-xr-x  3 root 4096 2013-09-05 20:58 media
drwxr-xr-x  2 root 4096 2010-04-23 07:11 mnt
drwxr-xr-x  2 root 4096 2010-08-16 06:32 opt
dr-xr-xr-x 142 root  0 2013-09-05 20:52 proc
drwx-----  9 root 4096 2013-09-05 20:47 root
drwxr-xr-x  2 root 4096 2013-09-05 20:16 sbin
drwxr-xr-x  2 root 4096 2009-12-05 18:55 selinux
drwxr-xr-x  2 root 4096 2010-08-16 06:32 srv
drwxr-xr-x 12 root  0 2013-09-05 20:52 sys
drwxrwxrwt 13 root 4096 2013-09-05 20:58 tmp
drwxr-xr-x 10 root 4096 2010-08-16 06:32 usr
drwxr-xr-x 15 root 4096 2010-08-16 06:48 var
lrwxrwxrwx  1 root  30 2013-09-05 20:09 vmlinuz -> boot/vmlinuz-2.6.32-24-generic
lab_utm@labutn-desktop:/$
  
```

Estructura raíz (principal)

```

(root@kali)-[/home/kali]
# fdisk -l
Disk /dev/sda: 80 GiB, 85899345920 bytes, 167772160 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe7875fa7

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *          2048    165771263    165769216    79G 83 Linux
/dev/sda2             165773310    167770111    1996802     975M  5 Extended
/dev/sda5             165773312    167770111    1996800     975M 82 Linux swap / Solaris
  
```

Usar el comando “**fdisk -l**” para poder ver las particiones en uso

Minimizar paquetes para minimizar vulnerabilidad

¿Es necesario tener todo tipo de servicios instalados?

Se recomienda evitar la instalación de paquetes obsoletos para evitar vulnerabilidades en los mismos y de esa manera minimizar el riesgo que puede llegar a comprometer otros servicios.

Encontrar y eliminar o deshabilitar los servicios no deseados del servidor para minimizar la vulnerabilidad. Utilizar el comando “**chkconfig**” para averiguar los servicios que se ejecutan en el nivel de ejecución 3.

```

lab_utn@labutn-desktop: /
Archivo Editar Ver Terminal Ayuda
lab_utn@labutn-desktop:/$ chkconfig --list | grep '3:on'
acpi-support          0:off 1:off 2:on 3:on 4:on 5:on 6:off
binfmt-support        0:off 1:off 2:on 3:on 4:on 5:on 6:off
bluetooth             0:off 1:off 2:on 3:on 4:on 5:on 6:off
cups                  0:off 1:off 2:on 3:on 4:on 5:on 6:off
dns-clean             0:off 1:off 2:on 3:on 4:on 5:on 6:off
fancontrol            0:off 1:off 2:on 3:on 4:on 5:on 6:off
grub-common           0:off 1:off 2:on 3:on 4:on 5:on 6:off
kerneloops            0:off 1:off 2:on 3:on 4:on 5:on 6:off
ondemand              0:off 1:off 2:on 3:on 4:on 5:on 6:off
pppd-dns              0:off 1:off 2:on 3:on 4:on 5:on 6:off
pulseaudio            0:off 1:off 2:on 3:on 4:on 5:on 6:off
rc.local              0:off 1:off 2:on 3:on 4:on 5:on 6:off
rsync                 0:off 1:off 2:on 3:on 4:on 5:on 6:off
saned                 0:off 1:off 2:on 3:on 4:on 5:on 6:off
speech-dispatcher     0:off 1:off 2:on 3:on 4:on 5:on 6:off
lab_utn@labutn-desktop:/$
  
```

Escribimos: **chkconfig –list | grep ‘3:on’**

Una vez seleccionado el servicio: **“chkconfig “servicename seleccionado” off”**

En Kali Linux el comando a utilizar es **“systemctl”**

```

(root@kali)~[/home/kali]
# systemctl list-units
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
proc-sys-fs-binfmt-misc.automount  loaded active running Arbitrary Executable File Formats File System Auto>
sys-devices-pci0000:00-0000:00:01.1-ata2-host2-target2:0:0-2:0:0-0-block-sr0.device loaded active plugged VBOX_CD-ROM
sys-devices-pci0000:00-0000:00:03.0-net-eth0.device loaded active plugged 82540EM Gigabit Ethernet Controller (PRO/1000 MT D>
sys-devices-pci0000:00-0000:00:05.0-sound-card0.device loaded active plugged 82801AA AC'97 Audio Controller
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0-0-block-sda-sda1.device loaded active plugged VBOX_HARDDISK 1
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0-0-block-sda-sda2.device loaded active plugged VBOX_HARDDISK 2
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0-0-block-sda-sda5.device loaded active plugged VBOX_HARDDISK 5
sys-devices-pci0000:00-0000:00:0d.0-ata3-host1-target1:0:0-1:0:0-0-block-sda-sda6.device loaded active plugged VBOX_HARDDISK
sys-devices-platform-serial8250-tty-ttyS0.device loaded active plugged /sys/devices/platform/serial8250/tty/ttyS0
sys-devices-platform-serial8250-tty-ttyS1.device loaded active plugged /sys/devices/platform/serial8250/tty/ttyS1
sys-devices-platform-serial8250-tty-ttyS2.device loaded active plugged /sys/devices/platform/serial8250/tty/ttyS2
sys-devices-platform-serial8250-tty-ttyS3.device loaded active plugged /sys/devices/platform/serial8250/tty/ttyS3
sys-devices-virtual-misc-rfkill.device loaded active plugged /sys/devices/virtual/misc/rfkill
sys-module-configfs.device loaded active plugged /sys/module/configfs
sys-module-fuse.device loaded active plugged /sys/module/fuse
sys-subsystem-net-devices-eth0.device loaded active plugged 82540EM Gigabit Ethernet Controller (PRO/1000 MT D>
  
```

Listar servicios: **systemctl list-units**

Chkconfig vs Systemctl

chkconfig: # **chkconfig --list**

systemd: # **systemctl list-units**

Enable a service

chkconfig: # chkconfig <servicename> on

systemd: # systemctl enable <servicename>.service

Disable a service

chkconfig: # chkconfig <servicename> off

systemd: # systemctl disable <servicename>.service

Start a service

chkconfig: # service <servicename> start

systemd: # systemctl start <servicename>.service

Stop a service

chkconfig: # service <servicename> stop

systemd: # systemctl stop <servicename>.service

Check the status of a service

chkconfig: # service <servicename> status

systemd: # systemctl status <servicename>.service

Utilizar el gestor de paquetes RPM, herramientas como "yum" o "apt-get" para listar todos los paquetes instalados del sistema y eliminarlos

```
# yum -y remove package-name
```

```
# sudo apt-get remove package-name
```

Recordar (nuevamente) cada distro tiene comandos específicos y de nombre distintos para cumplir mismas funciones, para este caso:

- ☐ RPM: \$ rpm -qa --last.



- ☐ RedHat / CentOS: \$ dnf list installed.
- ☐ OpenSuSE: \$ zypper se --installed-only.
- ☐ Debian / Ubuntu via DPKG: \$ dpkg -l.

```
(root@kali)-[/home/kali]
# apt list --installed
Listing ... Done
acl/kali-rolling,now 2.2.53-8 amd64 [installed,automatic]
adduser/kali-rolling,now 3.118 all [installed]
adwaita-icon-theme/kali-rolling,now 3.38.0-1 all [installed,automatic]
aircrack-ng/kali-rolling,now 1:1.6+git20201206.8259703-1 amd64 [installed]
amass-common/kali-rolling,now 3.10.5-0kali1 all [installed,automatic]
amass/kali-rolling,now 3.10.5-0kali1 amd64 [installed]
amd64-microcode/kali-rolling,now 3.20191218.1 amd64 [installed,automatic]
apache2-bin/kali-rolling,now 2.4.46-2 amd64 [installed,automatic]
apache2-data/kali-rolling,now 2.4.46-2 all [installed,automatic]
apache2-utils/kali-rolling,now 2.4.46-2 amd64 [installed,automatic]
apache2/kali-rolling,now 2.4.46-2 amd64 [installed]
apparmor/kali-rolling,now 2.13.5-1+b2 amd64 [installed,automatic]
apt-utils/kali-rolling,now 2.1.12 amd64 [installed]
apt/kali-rolling,now 2.1.12 amd64 [installed]
arj/kali-rolling,now 3.10.22-24 amd64 [installed,automatic]
arp-scan/kali-rolling,now 1.9.7-1 amd64 [installed]
arping/kali-rolling,now 2.21-1 amd64 [installed]
asleap/kali-rolling,now 2.2-1kali7 amd64 [installed]
aspell-en/kali-rolling,now 2018.04.16-0-1 all [installed,automatic]
aspell/kali-rolling,now 0.60.8-1 amd64 [installed,automatic]
at-spi2-core/kali-rolling,now 2.38.0-2 amd64 [installed,automatic]
atftpd/kali-rolling,now 0.7.git20120829-3.1+b1 amd64 [installed]
atril-common/kali-rolling,now 1.24.0-1 all [installed,automatic]
atril/kali-rolling,now 1.24.0-1 amd64 [installed,automatic]
attr/kali-rolling,now 1:2.4.48-6 amd64 [installed,automatic]
autopsy/kali-rolling,now 2.24-5 all [installed]
avahi-daemon/kali-rolling,now 0.8-3 amd64 [installed,automatic]
axel/kali-rolling,now 2.17.10-1 amd64 [installed]
```

- ☐ Debian / Kali Linux: \$ apt list --installed

Comprobar Puertos de “escucha” de red

La ayuda de comandos como '**netstat**' nos mostrará todos los puertos abiertos y los programas asociados.

```
(root@kali)-[/home/kali]
# netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.36:59020      eze06s02-in-f3.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:60486      eze06s05-in-f10.1:https ESTABLISHED
tcp        0      0 192.168.1.36:46966      eze04s08-in-f2.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:39144      eze06s01-in-f2.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:36062      ec2-52-35-213-209:https ESTABLISHED
tcp        0      0 192.168.1.36:50624      eze06s02-in-f4.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:43632      eze06s02-in-f4.1e1:http ESTABLISHED
tcp        0      0 192.168.1.36:46058      eze04s06-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.1.36:43150      eze04s08-in-f3.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:50714      eze04s08-in-f14.1:https ESTABLISHED
tcp        0      0 192.168.1.36:32856      192.16.58.8:http        ESTABLISHED
tcp        0      0 192.168.1.36:50612      server-13-227-69-:https ESTABLISHED
tcp        0      0 192.168.1.36:32864      192.16.58.8:http        ESTABLISHED
tcp        0      0 192.168.1.36:43132      eze04s08-in-f3.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:43630      eze06s02-in-f4.1e1:http TIME_WAIT
tcp        0      0 192.168.1.36:43902      eze06s01-in-f3.1e1:http ESTABLISHED
tcp        0      0 192.168.1.36:41888      eze04s09-in-f3.1e1:http ESTABLISHED
tcp        0      0 192.168.1.36:50614      server-13-227-69-:https ESTABLISHED
tcp        0      0 192.168.1.36:39142      eze06s01-in-f2.1e:https ESTABLISHED
tcp        0      0 192.168.1.36:52856      ec2-34-216-80-151:https ESTABLISHED
tcp        0      0 192.168.1.36:43900      eze06s01-in-f3.1e1:http ESTABLISHED
tcp        0      0 192.168.1.36:36698      server-13-227-69-:https ESTABLISHED
tcp        0      0 192.168.1.36:43888      eze06s01-in-f3.1e1:http ESTABLISHED
tcp        0      0 192.168.1.36:48500      eze06s06-in-f14.1:https ESTABLISHED
```

Ejemplo: **netstat -t** (nos muestra todos los puertos activos en escucha)

Los datos más importantes que uno puede observar son:

Tipo de protocolo: (**TCP/UDP**)

Local Address: generalmente la **IP** de la máquina local

Foreign Address: la IP destino, sesión abierta entre nuestra máquina y esa **IP** remota.

State: estado de la sesión (por ende, **ESTABLISHED**, significa conexión establecida)

```
(root@kali)-[/home/kali]
# netstat -anlp | grep LISTEN
unix 2      [ ACC ]     STREAM    LISTENING  16644    918/ssh-agent      /tmp/ssh-x0eH07nj7iiY/agent.844
unix 2      [ ACC ]     STREAM    LISTENING  16708    844/xfce4-session  /tmp/.ICE-unix/844
unix 2      [ ACC ]     STREAM    LISTENING  14064    553/Xorg            /tmp/.X11-unix/X0
unix 2      [ ACC ]     STREAM    LISTENING  14063    553/Xorg            @/tmp/.X11-unix/X0
unix 2      [ ACC ]     STREAM    LISTENING  16502    815/systemd        /run/user/1000/systemd/private
unix 2      [ ACC ]     STREAM    LISTENING  16511    815/systemd        /run/user/1000/bus
unix 2      [ ACC ]     STREAM    LISTENING  16513    815/systemd        /run/user/1000/gnupg/S.dirmngr
unix 2      [ ACC ]     STREAM    LISTENING  12642    1/init             /run/systemd/private
unix 2      [ ACC ]     STREAM    LISTENING  16515    815/systemd        /run/user/1000/gnupg/S.gpg-agent.browser
unix 2      [ ACC ]     STREAM    LISTENING  16517    815/systemd        /run/user/1000/gnupg/S.gpg-agent.extra
unix 2      [ ACC ]     STREAM    LISTENING  12644    1/init             /run/systemd/userdb/io.systemd.DynamicUser
unix 2      [ ACC ]     STREAM    LISTENING  16519    815/systemd        /run/user/1000/gnupg/S.gpg-agent.ssh
unix 2      [ ACC ]     STREAM    LISTENING  12645    1/init             /run/systemd/io.system.ManagedOOM
unix 2      [ ACC ]     STREAM    LISTENING  16521    815/systemd        /run/user/1000/gnupg/S.gpg-agent
unix 2      [ ACC ]     STREAM    LISTENING  16523    815/systemd        /run/user/1000/pulse/native
unix 2      [ ACC ]     STREAM    LISTENING  11041    1/init             /run/systemd/fsck.progress
unix 2      [ ACC ]     STREAM    LISTENING  11049    1/init             /run/systemd/journal/stdout
unix 2      [ ACC ]     SEQPACKET LISTENING  11051    1/init             /run/udev/control
unix 2      [ ACC ]     STREAM    LISTENING  16707    844/xfce4-session  @/tmp/.ICE-unix/844
unix 2      [ ACC ]     STREAM    LISTENING  15857    935/dbus-daemon    @/tmp/dbus-30Ayad0C4T
unix 2      [ ACC ]     STREAM    LISTENING  11106    285/systemd-journal /run/systemd/journal/io.systemd.journal
unix 2      [ ACC ]     STREAM    LISTENING  14479    1/init             /run/dbus/system_bus_socket
```

netstat -anlp | grep LISTEN (revisa los servicios que se están corriendo)

Aquí dos datos muy interesantes:

En la sexta columna, el nombre del **PID** (process **ID**) y la columna posterior, la ruta del servicio/programa que se está ejecutando.

```
(root@kali)-[/home/kali]
# netstat -i
Kernel Interface table
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500    648427 0      2139 0        10091 0      0      0 BMRU
lo         65536   70      0      0 0         70    0      0      0 LRU
```

Netstat -i

Por último, se puede verificar estadísticas de las interfaces de red, de esa manera uno puede observar si tenemos errores.

Usar Secure Shell (SSH)

Servicios de conexión como **Telnet** y **rlogin** utiliza protocolos de texto plano, sin formato cifrado.

SSH es un protocolo de seguridad que utiliza tecnología de cifrado durante la comunicación con el servidor.

Algunas recomendaciones:

- Nunca entrar directamente como root a menos que sea necesario.
- Utilizar "sudo" para ejecutar comandos .sudo (se especifican en /etc / sudoers) o también puede ser editado con la utilidad "visudo" (de acuerdo a la distribución), que se abre en el editor VI.
- Es recomendable cambiar el número de puerto 22 por defecto SSH por otro número de puerto de más alto nivel (dado que es un servicio de los más conocidos).

```
# vi /etc/ssh/sshd_config
```

Disable root Login

```
PermitRootLogin no
```

Only allow Specific Users

```
AllowUsers username
```

Use SSH Protocol 2 Version

```
Protocol 2
```

En el ejemplo, se puede observar cómo abrir el archivo principal de configuración de SSH y tener la posibilidad de realizar algunos cambios en los parámetros para evitar que los intrusos tengan acceso.

Hay distribuciones, que uno puede configurar números de intentos de login:

vi /etc/login.defs

LOGIN_RETRIES 3

LOGIN_TIMEOUT 30

LOG_UNKFAIL_ENAB yes

Otra opción es bloquear las TTY para no acceder directamente como root.

Se accedes al archivo y se ejecuta el siguiente comando:

vi /etc/securetty

:1,\$s/tty/#tty

Mantener actualizado el sistema

Siempre mantener el sistema actualizado con los últimos parches de versiones, revisiones de seguridad y de núcleo cuando estén disponibles.

En la distribución que se recomienda (Kali Linux):

```
(root@kali)-[/home/kali]
# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [17.5 MB]
Get:3 http://kali.download/kali kali-rolling/contrib amd64 Packages [106 kB]
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [202 kB]
Fetched 17.8 MB in 5s (3,731 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
395 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

#apt update (verifica en el repositorio, cantidad de paquetes a instalar/actualizar)


```
(root@kali)-[/home/kali]
# apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  grub-pc-bin libcapstone3 libcrypt++6 libradare2-4.3.1 qt5-gtk2-platformtheme ruby-connection-pool ruby-molinillo ruby-net-http-persistent ruby-thor
  xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  apt-file command-not-found gir1.2-xfconf-0 libapt-pkg-perl libbcb729-0 libbpf0 libcrypt++8 libexporter-tiny-perl libfmt7 liblist-moreutils-perl
  liblist-moreutils-xs-perl libradare2-5.0.0 librexp-assemble-perl liburing1 python3-h2 python3-hpack python3-hyperframe ruby-rubygems
The following packages have been kept back:
  libopenconnect5
The following packages will be upgraded:
  acl apache2 apache2-bin apache2-data apache2-utils apparmor apt apt-utils aspell atftpd bash binutils binutils-common binutils-x86-64-linux-gnu bluez
  bluez-hcidump bluez-obexd bsdxtrautils bsduutils bubblewrap bundler burpsuite catfish cherrytree console-setup console-setup-linux cpp-10 curl diffutils eject
  espeak espeak-data exploitable faraday fdisk firebird3.0-common firebird3.0-common-doc firmware-amd-graphics firmware-atheros firmware-brcm80211
  firmware-intel-sound firmware-iwlwifi firmware-libertas firmware-linux firmware-linux-nonfree firmware-misc-nonfree firmware-realtek firmware-ti-connectivity flac
  fuse3 g++-10 gcc-10 gcc-10-base gdal-data geoclue-2.0 geoupdate gettext-base gir1.2-nm-1.0 grub-common grub-pc-bin gtk2-engines-pixbuf gvfs gvfs-backends
  gvfs-common gvfs-daemons gvfs-fuse gvfs-libs hwloc ieee-data intel-media-va-driver intel-microcode ipp-usb iproute2 ipython3 kali-defaults kali-defaults-desktop
  kali-desktop-base kali-desktop-core kali-desktop-xfce kali-linux-core kali-themes kali-themes-common kali-tools-top10 kali-undercover kali-wallpapers-2019.4
  kali-wallpapers-2020.4 keyboard-configuration lib32gcc-s1 lib32stdc++6 libacl1 libaio1 libapparmor1 libapr1 libapt-pkg6.0 libasan6 libasound2 libasound2-data
  libaspell15 libatk-wrapper-java libatk-wrapper-java-jni libatkmm-1.6-1v5 libatomic1 libaudio2 libaudit-common libaudit1 libbinutils libblkid1 libbluetooth3
  libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 libcairo-gobject2 libcairo2 libcc1-0 libcrypt-random-seed-perl libctf-nobfd0 libctf0 libcupst
  libcurl3-gnutls libcurl4 libdebconfclient0 libdeflate0 libdigest-bubblebabble-perl libdw1 libegl-mesa0 libelf1 libespeak1 libfbclient2 libfdisk1 libflac8
  libflite1 libfuse3-3 libgail-common libgail18 libgbm1 libgcc-10-dev libgcc-s1 libgdal28 libgfortran5 libgl1-mesa-dri libglapi-mesa libglv2.0-0 libglv2.0-bin
```

Luego realizar un “apt upgrade”

Actualizará e instalará lo encontrado con el “apt update”.

Por último se recomienda el uso de: “apt dist-upgrade”, para que actualice todo lo relacionado al sistema.

```
(root@kali)-[/home/kali]
# apt dist-upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  grub-pc-bin libcapstone3 libcrypt++6 libradare2-4.3.1 qt5-gtk2-platformtheme ruby-connection-pool ruby-molinillo ruby-net-http-persistent ruby-thor
  xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  libtss2-esys0
The following NEW packages will be installed:
  libtss2-esys-3.0.2-0 libtss2-mu0 libtss2-sys1
The following packages will be upgraded:
  libopenconnect5
1 upgraded, 3 newly installed, 1 to remove and 0 not upgraded.
Need to get 443 kB of archives.
After this operation, 1,026 kB disk space will be freed.
Do you want to continue? [Y/n]
```

Desactivar la detección de memoria USB

Muchas veces sucede que se quiere restringir a otros usuarios el uso de una memoria USB en los sistemas para proteger y asegurar los datos de que sean robados.

Una manera sería crear un archivo en “/etc/modprobe.d/no-usb” y añadiendo a continuación la línea no se detectará el almacenamiento USB.

“install usb-storage /bin/true”

Cuentas con contraseñas vacías

Cualquier cuenta con una contraseña vacía significa que queda abierta para el acceso no autorizado de cualquier persona.

Por lo tanto, hay que asegurarse de que todas las cuentas tengan contraseñas seguras y con acceso autorizado.

Las cuentas con contraseñas vacías son riesgos de seguridad

Para comprobar si tiene cuentas con contraseña vacías, utiliza el comando:

Cat / etc / shadow | awk-F: '(\$ 2 == "") {print \$ 1}'

Revisar los registros con regularidad

Mover los registros de log del servidor dedicado, esto evitará que los intrusos puedan modificar fácilmente los registros locales.

- / var / log / auth.log - Registros de autenticación.
- / var / log / kern.log - logs del kernel.
- / var / log / cron.log - logs crond (cron).
- / var / log / maillog - los registros del servidor de correo.
- / var / log / boot.log - registro de arranque del sistema.
- / var / log / mysqld.log - archivo de registro del servidor de bases de datos MySQL.
- / var / log / secure - registro de autenticación.
- / var / log / utmp o / var / log / wtmp: Login archivo de registros.
- / var / log / yum.log: archivos de registro de Yum.

Material obsequio: Hardening en PHP

La siguiente es una lista de directivas que se pueden configurar en el archivo de configuración de php (/etc/php.ini, o /etc/php5/apache2/php.ini, dependiendo la distribución) para mejorar la seguridad del servidor:

- **Restringir el acceso al sistema de archivos**

Dado que los sites se alojarán en /var/www, salvo casos excepcionales, los scripts PHP no necesitan acceso al resto del sistema de archivos, a excepción del directorio /tmp que es donde se alojan los archivos cuando el usuario hace un upload. Es posible restringir los directorios a los que se puede acceder, mediante la opción:

open_basedir = /var/www:/tmp

Esta configuración se puede cambiar por site en el correspondiente Virtual Host, utilizando la directiva:

php_admin_value open_basedir /var/www/[nombre site]/

- **Deshabilitar funciones riesgosas**

Hay funciones que deben ser permitidas sólo en casos particulares, debido a que se usan raramente y representan un gran riesgo.

Esta configuración se realiza con la directiva `disable_functions`:

disable_functions = show_source, system, shell_exec, passthru, exec, phpinfo, popen, proc_open

- **No revelar información de PHP en los headers**

Esto le permitiría a un atacante saber que el servidor posee PHP, además de la versión instalada, y así poder realizar un ataque más específico:

expose_php = Off

- **No exponer errores de scripts al cliente**

Los errores de programación no deben quedar expuestos a los clientes, sino que deben loggarse en archivos para que el programador los pueda depurar:

display_errors = Off

display_startup_errors = Off

Loggear errores permiten detectar cuál fue la falla que causó que el programa no funcione o lo haga de forma imprevisible

log_errors = On

- **No utilizar register_globals**

Esta funcionalidad se considera extremadamente peligrosa y por default viene desactivada en toda configuración actual, pero por las dudas se debe chequear que el valor sea el siguiente

register_globals = 0

- **Para realizar upload de archivos desde el cliente, utilizar el directorio tmp correspondiente al site, es decir /var/www/[nombre site]/tmp**

Esta configuración se realiza en el virtual host con la sentencia:

php_admin_value upload_tmp_dir /var/www/[nombre site]/tmp

- **No tratar las URLs (como http:// o ftp://) como archivos.**

En caso de encontrar un error en la programación, un atacante podría realizar remote file inclusion si esto se encuentra activado:

allow_url_fopen = Off

allow_url_include = Off

- **Cambiar el nombre de la variable de sesión. Por defecto esta variable se llama PHPSESSID y demuestra que el servidor ejecuta PHP, y que la página actual está escrita en PHP. Si bien esto agrega poca seguridad, agrega una traba más al atacante:**

`session.name = SESSION_ID`

Conclusión

Recomendaciones en el hardware

Algunas recomendaciones esenciales en el hardware de nuestro equipo pasaría por ser compatible con SecureBoot, de esta forma estaremos protegidos frente a malware como rootkits.

Asimismo también sería recomendable si no tenemos SecureBoot, la instalación de Anti Evil Maid que nos ofrecería la misma protección contra los tipos de ataques que SecureBoot se encarga de parar.

Si además nuestro sistema no tiene Firewire, Thunderbolt ni puerto ExpressCard mucho mejor para que no tengan acceso a la memoria, asimismo es recomendable incorporar un dispositivo TPM para aumentar aún más la seguridad física.

Recomendaciones en el boot (arranque)

Algunas recomendaciones básicas que debemos configurar en la BIOS es el arranque en modo UEFI, además es necesario incorporar una contraseña de administrador para acceder a la configuración de UEFI y protegernos de accesos no autorizados.

Por último, y con el objetivo de aumentar la seguridad, si incorporamos una contraseña al arranque del ordenador para posteriormente arrancar el sistema operativo sería perfecto.

Recomendaciones en el sistema operativo y software

Por último, el checklist de seguridad se centra principalmente en la elección de un sistema operativo Linux robusto y fiable, compatible con tecnologías MAC/RBAC como SELinux/AppArmor/GrSecurity, que se actualice continuamente y lo antes posible así como que tenga soporte para UEFI y SecureBoot.

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU

Links complementarios

Te recomendamos visitar el siguiente sitio:

<https://github.com/lfit/itpol/blob/master/linux-workstation-security.md>

Te animas a probar la herramienta: checklistlinux.pl?

En caso de que si, expone en el foro la experiencia

<http://checklistlinux.sourceforge.net/>

Todo lo último en UBUNTU en español:

<http://www.ubuntu-es.org/>

Herramientas de seguridad para linux:

<http://blog.desdelinux.net/las-11-mejores-aplicaciones-de-hacking-y-seguridad-para-linux/>

El mejor sitio para chequear todos los comandos de LINUX:

<https://www.hscripts.com/es/tutoriales/linux-commands/index.php>

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado).