

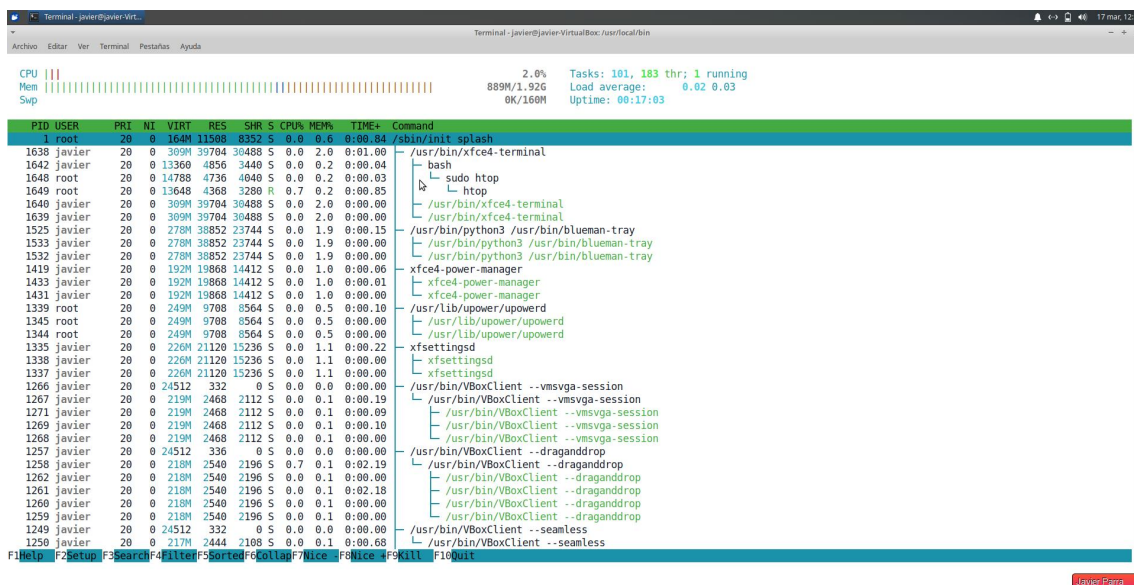
UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

En la UD 07 hay un criterio de evaluación que dice lo siguiente: “Se han tomado medidas de seguridad ante la aparición de procesos no identificados”

¿Qué harías en tu servidor Linux?

Ante la aparición de procesos no identificados es recomendable realizar las siguientes acciones:

1º Verificar la autenticidad de los procesos, utilizando herramientas como ps, top, htop o pstree, identificamos los procesos que están en ejecución en el sistema. De esta manera podremos identificar procesos que no reconozcamos o parezcan sospechosos.



2º Realizar una investigación de la actividad del sistema, revisando los ficheros logs en las rutas /var/log/syslog, /var/log/auth.log o /var/log/messages, en busca de cualquier actividad que nos sea inusual. Estos logs nos pueden proporcionar pistas sobre que procesos se ejecutaron recientemente.

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

```
Terminal - javier@javier-Virt...
javier@javier-VirtualBox: /usr/local/bin$ cat /var/log/syslog | tail -n 10
Mar 17 12:40:12 javier-VirtualBox systemd[1]: run-user-114.mount: Succeeded.
Mar 17 12:40:12 javier-VirtualBox systemd[1]: user-runtime-dir@114.service: Succeeded.
Mar 17 12:40:12 javier-VirtualBox systemd[1]: Stopped User Runtime Directory /run/user/114.
Mar 17 12:40:12 javier-VirtualBox systemd[1]: Removed slice User Slice of UID 114.
Mar 17 12:40:27 javier-VirtualBox pulseaudio[1141]: GetManagedObjects() failed: org.freedesktop.DBus.Error.NoReply: Did not receive a reply. Possible causes include: the remote application d
id not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.
Mar 17 12:40:36 javier-VirtualBox systemd[1]: Condition check resulted in Run anacron jobs being skipped.
Mar 17 12:40:36 javier-VirtualBox systemd[1]: blueman-mechanism.service: Succeeded.
Mar 17 12:54:08 javier-VirtualBox systemd[1]: Starting Cleanup of Temporary Directories...
Mar 17 12:54:08 javier-VirtualBox systemd[1]: systemd-tmpfiles-clean.service: Succeeded.
Mar 17 12:54:08 javier-VirtualBox systemd[1]: Finished Cleanup of Temporary Directories.
javier@javier-VirtualBox: /usr/local/bin$
```

3º Realizar un análisis del sistema, utilizando herramientas de análisis de seguridad como rkhunter, chkrootkit o clamav para buscar signos de intrusiones de malware o rootkits escondidos en el sistema.

Podemos usar el antimalware clamav para analizar los procesos y ficheros del sistema.

Instalamos clamav con su interfaz gráfica.

```
Terminal - javier@javier-Virt...
javier@javier-VirtualBox: /usr/local/bin$ sudo apt install clamav clamtk
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  clamav-base clamav-freshclam gnome-icon-theme libclamav9 libcommon-sense-perl libencode-perl libjson-perl libjson-xs-
  libtypes-serialiser-perl
Paquetes sugeridos:
  libclamunrar clamav-docs cabextract clamtk-gnome libclamunrar9
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-freshclam clamtk gnome-icon-theme libclamav9 libcommon-sense-perl libencode-perl libjson-pe
  libtftm1 libtypes-serialiser-perl
0 actualizados, 15 nuevos se instalarán, 0 para eliminar y 16 no actualizados.
Se necesita descargar 12,8 MB de archivos.
Se utilizarán 32,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

Paramos el servicio de clamav y actualizamos la base de datos de virus.

```
$ sudo systemctl stop clamav-freshclam.service
```

```
$ sudo freshclam
```

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)



```
Terminal - javier@javier-Virt...
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
Terminal - javier@javier-VirtualBox: /usr/local/bin

javier@javier-VirtualBox: /usr/local/bin$ sudo systemctl stop clamav-freshclam.service
javier@javier-VirtualBox: /usr/local/bin$ sudo freshclam
Sun Mar 17 13:03:25 2024 -> ClamAV update process started at Sun Mar 17 13:03:25 2024
Sun Mar 17 13:03:25 2024 -> daily.cvd database is up-to-date (version: 27217, sigs: 2055524, f-level: 90, builder: raynman)
Sun Mar 17 13:03:25 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Sun Mar 17 13:03:25 2024 -> bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
javier@javier-VirtualBox: /usr/local/bin$
```

Javier Parra

Volvemos a iniciar el servicio de ClamAV.

```
Terminal - javier@javier-Virt...
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
Terminal - javier@javier-VirtualBox: /usr/local/bin

javier@javier-VirtualBox: /usr/local/bin$ sudo systemctl start clamav-freshclam.service
javier@javier-VirtualBox: /usr/local/bin$ sudo systemctl status clamav-freshclam.service
● clamav-freshclam.service - ClamAV virus database updater
   Loaded: loaded (/lib/systemd/system/clamav-freshclam.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-03-17 13:04:08 CET; 5s ago
     Docs: man:freshclam(1)
           man:freshclam.conf(5)
           https://docs.clamav.net/
   Main PID: 2693 (freshclam)
     Tasks: 1 (limit: 2261)
    Memory: 2.0M
   CGroup: /system.slice/clamav-freshclam.service
           └─2693 /usr/bin/freshclam -d --foreground=true

mar 17 13:04:08 javier-VirtualBox systemd[1]: Started ClamAV virus database updater.
mar 17 13:04:08 javier-VirtualBox freshclam[2693]: Sun Mar 17 13:04:08 2024 -> ClamAV update process started at Sun Mar 17 13:04:08 2024
mar 17 13:04:08 javier-VirtualBox freshclam[2693]: Sun Mar 17 13:04:08 2024 -> daily.cvd database is up-to-date (version: 27217, sigs: 2055524, f-level: 90, builder: raynman)
mar 17 13:04:08 javier-VirtualBox freshclam[2693]: Sun Mar 17 13:04:08 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
mar 17 13:04:08 javier-VirtualBox freshclam[2693]: Sun Mar 17 13:04:08 2024 -> bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
javier@javier-VirtualBox: /usr/local/bin$
```

Javier Parra

Analizamos un directorio en concreto para encontrar procesos o ficheros sospechosos.

```
Terminal - javier@javier-Virt...
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
Terminal - javier@javier-VirtualBox: /usr/local/bin

javier@javier-VirtualBox: /usr/local/bin$ sudo clamscan -r /usr/local/bin
[sudo] contraseña para javier:
/usr/local/bin/test_tfn.sh: OK
/usr/local/bin/correo_spam_2.sh: OK
/usr/local/bin/usuarios.txt: OK
/usr/local/bin/comprobar_mac.sh: OK
/usr/local/bin/probar_servicio.sh: OK
/usr/local/bin/fl1.txt: OK
/usr/local/bin/procesosPesados.sh: OK
/usr/local/bin/pckInstalado.sh: OK
/usr/local/bin/passwdToHTML.sh: OK
/usr/local/bin/array_asociativo.sh: OK
/usr/local/bin/revisar_logs.sh: OK
/usr/local/bin/getusuario.sh: OK
/usr/local/bin/esNumero10.sh: OK
/usr/local/bin/practical.sh: OK
/usr/local/bin/eq_mac.txt: OK
/usr/local/bin/monitorizar_espacio.sh: OK
/usr/local/bin/check_tfn_3.sh: OK
/usr/local/bin/test_matricula.sh: OK
/usr/local/bin/tablas1.sh: OK
/usr/local/bin/check_tfn_funciones.sh: OK
/usr/local/bin/backup_27-11-2023.tar.gz: OK
/usr/local/bin/n: Symbolic link
/usr/local/bin/escanear_puertos.sh: OK
/usr/local/bin/funciones2.sh: OK
/usr/local/bin/cortesia.sh: OK
/usr/local/bin/addusuariosv2.sh: OK
/usr/local/bin/saludo.sh: OK
/usr/local/bin/eq_mac_ok: OK
/usr/local/bin/ocupacion.sh: OK
/usr/local/bin/tab_aso_1.sh: OK
/usr/local/bin/serviciosV2.sh: OK
/usr/local/bin/check_dni.sh: OK
/usr/local/bin/mac_log: OK
/usr/local/bin/addusuarios.sh: OK
/usr/local/bin/monitorizar_espacio_V2.sh: OK
/usr/local/bin/check_tfn_5_1.sh: OK
/usr/local/bin/funciones/validar: OK
/usr/local/bin/red_ok.sh: OK
```

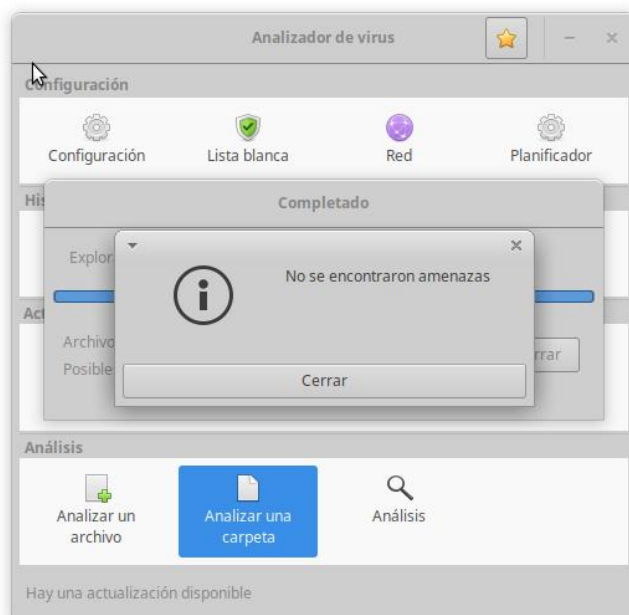
Javier Parra

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

```
Terminal - javier@javier-VirtualBox: /usr/local/bin
Archivo  Editor  Ver  Terminal  Pestañas  Ayuda
/usr/local/bin/fecha.sh: OK
/usr/local/bin/check_tfn_4.sh: OK
/usr/local/bin/.vscode/prueba.txt: OK
/usr/local/bin/check_tfn_5_2.sh: OK
/usr/local/bin/correo_spam_1.sh: OK
/usr/local/bin/f2.txt: OK
/usr/local/bin/corepack: Symbolic link
/usr/local/bin/check_tfn_2.sh: OK
/usr/local/bin/eje14_fraude_copla.sh: OK
/usr/local/bin/nombre_servicios.txt: OK
/usr/local/bin/args.sh: OK
/usr/local/bin/check_tfn_1.sh: OK
/usr/local/bin/crontab-ui: Symbolic link
/usr/local/bin/npz: Symbolic link
/usr/local/bin/prueba_remoto_vscode.txt: Empty file
/usr/local/bin/npm: Symbolic link
/usr/local/bin/monitorizar_espacio_V3.sh: OK
/usr/local/bin/ps_pesados.sh: OK
/usr/local/bin/llamadas.txt: OK
/usr/local/bin/fecha.sh.save: OK
/usr/local/bin/grupos.txt: OK
/usr/local/bin/plantilla_menu.sh: OK
/usr/local/bin/addgrupos_v1.sh: OK
/usr/local/bin/servicios.sh: OK
/usr/local/bin/script9.sh: OK
/usr/local/bin/pckInstaladoV2.sh: OK

----- SCAN SUMMARY -----
Known viruses: 8687223
Engine version: 0.103.11
Scanned directories: 3
Scanned files: 76
Infected files: 0
Data scanned: 0.00 MB
Data read: 274.19 MB (ratio 0.00:1)
Time: 16.023 sec (0 m 16 s)
Start Date: 2024-03-17 13:36:18
End Date: 2024-03-17 13:36:34
javier@javier-VirtualBox: /usr/local/bin
```

También podremos hacer uso de la interfaz gráfica ClamTK de ClamAV para analizar directorios.



Javier Parra

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

4º Verificar la integridad del sistema, comprobando la integridad de los archivos que son críticos en el sistema, utilizando herramientas como tripwire, AIDE o ossec. Estas herramientas pueden detectar cambios no autorizados en archivos del sistema que pueden indicar una intrusión.

5º Revisar los permisos y accesos, verificando los permisos de los archivos y directorios más importantes del sistema, para asegurarse de que solo usuarios autorizados puedan acceder o modificarlos.

```
Terminal - javier@javier-Virt...
javier@javier-VirtualBox: /usr/local/bin$ ls -l /
total 104
drwxr-xr-x 2 root root 4096 mar 12 18:32 actividades
drwxr-xr-x 5 root root 4096 nov 29 09:22 analizar
drwxr-xr-x 3 javier javier 4096 mar 12 19:22 backups
lrwxrwxrwx 1 root root 7 sep 14 2023 bin -> usr/bin
drwxr-xr-x 3 root root 4096 ene 22 12:54 boot
drwxrwxr-x 2 root root 4096 sep 14 2023 cdrom
drwxr-xr-x 2 root root 4096 dic 8 20:25 copias
drwxr-xr-x 19 root root 4160 mar 17 13:35 dev
drwxr-xr-x 147 root root 12288 mar 17 13:42 etc
drwxr-xr-x 22 root root 4096 mar 13 09:55 home
lrwxrwxrwx 1 root root 7 sep 14 2023 lib -> usr/lib
lrwxrwxrwx 1 root root 9 sep 14 2023 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 sep 14 2023 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 sep 14 2023 libx32 -> usr/libx32
drwx----- 2 root root 16384 sep 14 2023 lost+found
drwxr-xr-x 3 root root 4096 sep 14 2023 media
drwxr-xr-x 4 root root 4096 ene 23 10:58 mnt
drwxr-xr-x 4 root root 4096 sep 27 09:21 opt
dr-xr-xr-x 285 root root 0 mar 17 13:35 proc
-rw-r--r-- 1 root root 598 nov 23 12:34 procesos_pesados.txt
drwx----- 8 root root 4096 mar 12 18:47 root
drwxr-xr-x 35 root root 1060 mar 17 13:42 run
lrwxrwxrwx 1 root root 8 sep 14 2023/sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 dic 10 12:57 shared
drwxr-xr-x 2 root root 4096 sep 14 2023 snap
drwxr-xr-x 2 root root 4096 ago 31 2022 srv
dr-xr-xr-x 13 root root 0 mar 17 13:35 sys
drwxr-xr-x 2 root root 4096 nov 27 13:00 temporales
drwxrwxrwt 16 root root 4096 mar 17 13:47 tmp
drwxr-xr-x 14 root root 4096 ago 31 2022 usr
drwxr-xr-x 15 root root 4096 ago 31 2022 var
javier@javier-VirtualBox: /usr/local/bin$
```

Javier Parra

6º Realizar una actualización del sistema para parchear errores y vulnerabilidades de los que los ciberdelincuentes se puedan aprovechar utilizando diferentes exploits conocidos.

```
Terminal - javier@javier-Virt...
javier@javier-VirtualBox: /usr/local/bin$ sudo apt upgrade
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
linux-headers-5.15.0-89-generic linux-hwe-5.15.0-89 linux-image-5.15.0-89-generic linux-modules-5.15.0-89-generic linux-modules-extra-5.15.0-89-generic
Utllice #sudo apt autoremove para eliminarlos.
Get more security updates through Ubuntu Pro with 'esm-apps' enabled:
vlc-bin vlc-plugin-video-output libavformat58 exo-utils libavfilter7
libwireshark13 libwsutil11 vlc-plugin-samba node-hosted-git-info
libswresample3 vlc-plugin-qt libgegl-0.4-0 libzmq5 libmagickwand-6.q16-6
libwiretap10 vlc-plugin-skins2 libgegl-common vlc-plugin-visualization
vlc-libn libexo-1.0 vlc-plugin-notify libvlc5 libexo-2.0 libpostproc55
libvlccore9 libvlc-bin wireshark node-tar wireshark-common libavcodec58
libexo-common vlc libavutil56 vlc-data libswscale5 node-ip libopenexr24
libstdl2-2.0-0 libmysofa libmagickcore-6.q16-6 vlc-plugin-video-splitter
libwireshark-data vlc-plugin-base wireshark-qt libexo-helpers
imagenagick-6-common
Learn more about Ubuntu Pro at https://ubuntu.com/pro
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
javier@javier-VirtualBox: /usr/local/bin$ uname -r
5.15.0-91-generic
javier@javier-VirtualBox: /usr/local/bin$
```

Javier Parra

UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

7º Aplicación de medidas de seguridad para la red, utilizando cortafuegos para realizar un filtrado de paquetes, utilizar sistemas de identificación de intrusos (IDS) o sistemas para la prevención de intrusiones basados en firmas (IPS).

Nos podemos instalar un cortafuegos, para crear reglas y protegernos ante conexiones maliciosas que provoquen la entrada de procesos sospechosos.

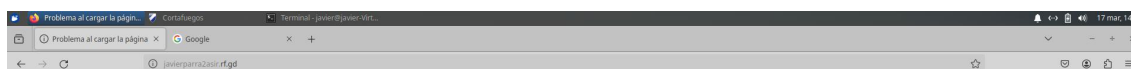
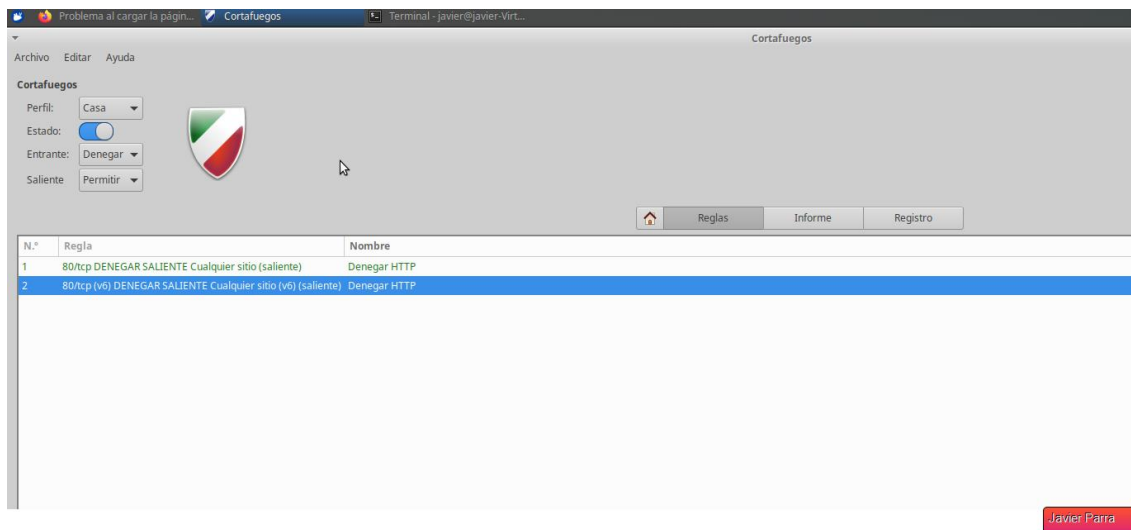
\$ sudo apt install gufw

```
Terminal - javier@javier-VirtualBox: /usr/local/bin$ sudo apt install gufw
javier@javier-VirtualBox: /usr/local/bin$ sudo apt install gufw
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
linux-headers-5.15.0-89-generic linux-hwe-5.15.0-headers-5.15.0-89 linux-image-5.15.0-89-generic linux-modules-5.15.0-89-generic linux-modules-extra-5.15.0-89-generic
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
 gufw
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 860 kB de archivos.
Se utilizarán 3.539 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu focal-updates/universe amd64 gufw all 20.04.1-lubuntu1 [860 kB]
Descargados 860 kB en 1s (869 kB/s)
Seleccionando el paquete gufw previamente no seleccionado.
(Leyendo la base de datos ... 251615 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../gufw.20.04.1-lubuntu1_all.deb ...
Desempaquetando gufw (20.04.1-lubuntu1) ...
Configurando gufw (20.04.1-lubuntu1) ...
Procesando disparadores para desktop-file-utils (0.24-lubuntu3) ...
Procesando disparadores para mime-support (3.64ubuntu1) ...
Procesando disparadores para hicolor-icon-theme (0.17-2) ...
Procesando disparadores para gnome-menus (3.36.0-lubuntu1) ...
Procesando disparadores para man-db (2.9.1-1) ...
```



UD 07: GESTIÓN DE PROCESOS. ACTIVIDADES (II)

Podemos crear una regla, por ejemplo voy a crear una para no permitir el acceso mediante HTTP, para conexiones no seguras.



La conexión ha caducado

The server at javierparra2asir.rf.gd is taking too long to respond.

- El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

Reintentar

Timed Out

Javier Parra