

ACTIVIDAD 8 – INTENTOS DE PENETRACIÓN – TEMA 2

- a) **Honeypots.** Instalación , configuración , ejecución y prueba en Windows o GNU/Linux de **honeypd** www.honeyd.org

Nos descargamos la aplicación poniendo apt-get install honeyd

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~$ sudo su
[sudo] password for lales:
root@lales-virtual-machine:/home/lales# apt-get install honeyd
```

Ahora nos vamos al fichero de configuración que está en /etc/default/honeyd y lo configuramos

```
root@lales-virtual-machine: /etc/default
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.2.6 Archivo: honeyd Modificado

# Defaults for honeyd initscript
# Master system-wide honeyd switch. The initscript
# will not run if it is not set to yes.
RUN="yes"

# Default options.
# Interface to listen on (if unset honeyd will select
# an interface himself)
# note: Use only one! if you wish to use
# more than one use multiple -i in OPTIONS
INTERFACE="eth0"

# Network honeyd will listen for. IF this is not set
# Honeyd will claim all IP addresses set on the configured
# interface (this is probably not what you want)
# This "sane" default will prevent you from doing it.
NETWORK=192.168.249.0/24

^G Ver ayuda ^O Guardar ^R Leer Fich ^Y RePág. ^K Cortar Tex ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág. Sig. ^U PegarTxt ^T Ortografia
```

Y reiniciamos el servicio con /etc/init.d/honeyd start

```
root@lales-virtual-machine:/etc/default#
root@lales-virtual-machine:/etc/default# nano honeyd
root@lales-virtual-machine:/etc/default# /etc/init.d/honeyd start
* Starting Honeyd daemon honeyd [ OK ]
root@lales-virtual-machine:/etc/default#
```

Y ahora ponemos route -nNvee y podemos ver las tablas de enrutamientos

```
root@lales-virtual-machine:/etc/default# route -nNvee
Tabla de rutas IP del núcleo
Destino Puerta de Enlace Genmask Banderas Métrica Ref Uso Interfaz MSS Ventana i
rtt
192.168.249.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0
0 0 0
169.254.0.0 0.0.0.0 255.255.0.0 U 1000 0 0 eth0
0 0 0
0.0.0.0 192.168.249.2 0.0.0.0 UG 100 0 0 eth0
0 0 0
```

b) Sistema de detección de intrusos (IDS): HostIDS: - Linux: Integridad de un fichero: md5sum.

Creamos un fichero en el escritorio llamado integridad y ahora con el comando md5sum integridad, vamos a generar el hash del fichero

```
lales@lales-virtual-machine: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~/Escritorio$ md5sum integridad
d41d8cd98f00b204e9800998ecf8427e integridad
lales@lales-virtual-machine:~/Escritorio$
```

Vamos a copiar ese resultado en un fichero con extensión .md5 y vemos que la suma coincide

```
lales@lales-virtual-machine: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~/Escritorio$ md5sum integridad
d41d8cd98f00b204e9800998ecf8427e integridad
lales@lales-virtual-machine:~/Escritorio$ md5sum integridad > integridad.md5
lales@lales-virtual-machine:~/Escritorio$ md5sum -c integridad.md5
integridad: La suma coincide
lales@lales-virtual-machine:~/Escritorio$
```

Ahora vamos a modificar el fichero con unas líneas

```
*Integridad (~/.Escritorio) - gedit
Archivo Editar Ver Buscar Herramientas Documentos Ayuda
Abrir Guardar Deshacer
*Integridad x
la luna vino a la fragua con su polisión de nardos|
```

Si volvemos a ejecutar el mismo comando vemos que la integridad se ha perdido porque ya la suma no coincide

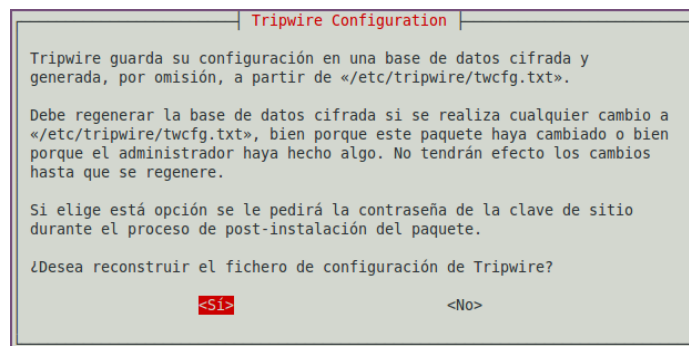
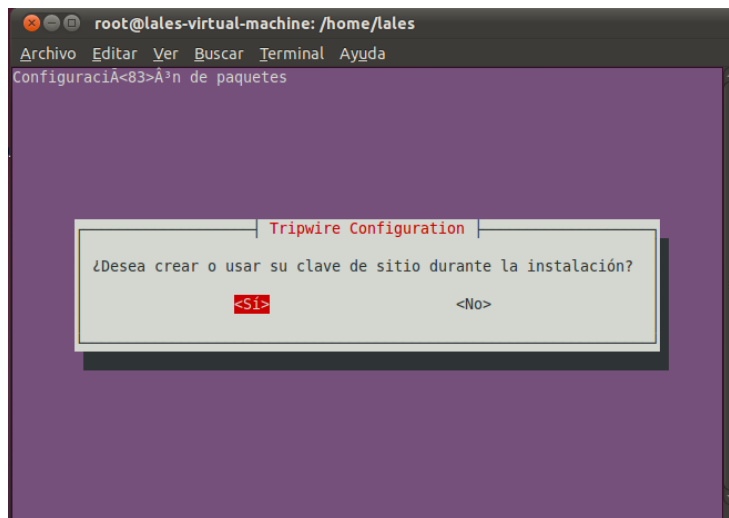
```
lales@lales-virtual-machine: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
lales@lales-virtual-machine:~/Escritorio$ md5sum integridad
d41d8cd98f00b204e9800998ecf8427e integridad
lales@lales-virtual-machine:~/Escritorio$ md5sum integridad > integridad.md5
lales@lales-virtual-machine:~/Escritorio$ md5sum -c integridad.md5
integridad: La suma coincide
lales@lales-virtual-machine:~/Escritorio$ md5sum -c integridad.md5
integridad: La suma no coincide
md5sum: AVISO: 1 de 1 suma de comprobación NO coincide
lales@lales-virtual-machine:~/Escritorio$
```

- Linux: Integridad de un sistema de ficheros: tripwire

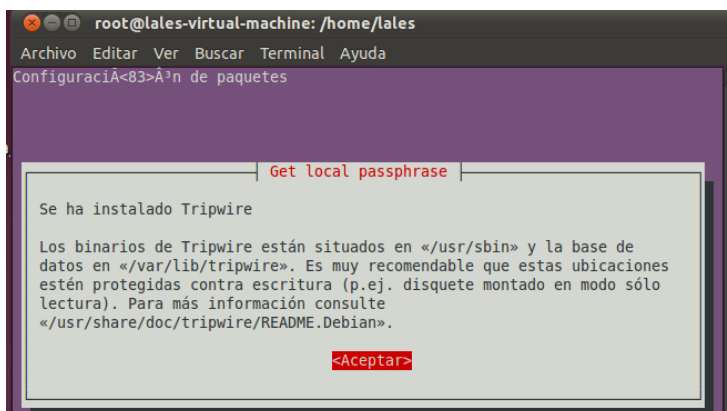
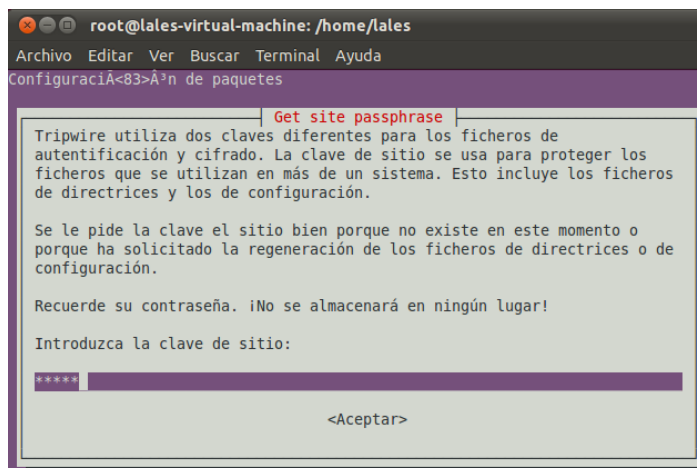
Vamos a instalar tripwire, para ello ponemos apt-get install tripwire

```
root@lales-virtual-machine:/home/lales# apt-get install tripwire
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-2.6.38-8 linux-headers-2.6.38-8-generic
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
  postfix
Paquetes sugeridos:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin
  dovecot-common resolvconf postfix-cdb
Se instalarán los siguientes paquetes NUEVOS:
  postfix tripwire
0 actualizados, 2 se instalarán, 0 para eliminar y 63 no actualizados.
Necesito descargar 4674 kB de archivos.
Se utilizarán 12,1 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?
```

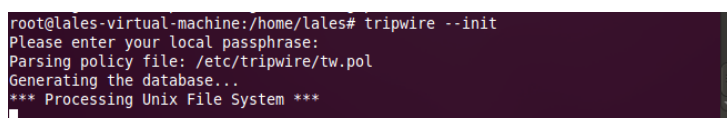
Nos sale un asistente, que vamos a ir dejando por defecto las opciones que nos da



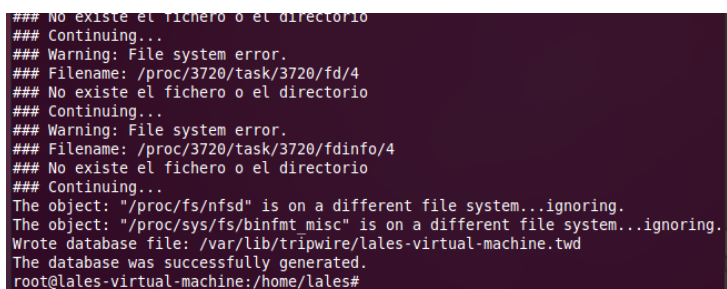
Nos pide una contraseña, vamos a poner inves



Ahora vamos a crear la base de datos con el comando tripwire --init



Y nos las crea correctamente



Una vez creado el archivo de configuración tendremos que crear un archivo de políticas, cuando lanzamos este comando luego nos pedirá nuestra contraseña. Nos creamos una base de datos para que se almacene todo lo del programa tripwire.

```
root@lales-virtual-machine:/home/lales# twadmin -m P /etc/tripwrite/twpol.txt
### Error: File could not be opened.
### Filename: /etc/tripwrite/twpol.txt
### No existe el fichero o el directorio
### Exiting...
root@lales-virtual-machine:/home/lales#
```

Y volvemos a poner el comando tripwire -init

```
### Continuing...
### Warning: File system error.
### Filename: /proc/3737/task/3737/fdinfo/4
### No existe el fichero o el directorio
### Continuing...
The object: "/proc/fs/nfsd" is on a different file system...ignoring.
The object: "/proc/sys/fs/binfmt_misc" is on a different file system...ignoring.
Wrote database file: /var/lib/tripwire/lales-virtual-machine.twd
The database was successfully generated.
root@lales-virtual-machine:/home/lales#
```

Ahora generamos un informe para ver si registra las modificaciones

```
root@lales-virtual-machine:/home/lales# tripwire --check | more
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

```
root@lales-virtual-machine: /home/lales
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Open Source Tripwire(R) 2.4.1 Integrity Check Report

Report generated by:      root
Report created on:       Mon Apr 16 03:06:14 2012
Database last updated on: Never

=====
Report Summary:
=====

Host name:                lales-virtual-machine
Host IP address:          127.0.1.1
Host ID:                   None
Policy file used:         /etc/tripwire/tw.pol
Configuration file used:  /etc/tripwire/tw.cfg
Database file used:       /var/lib/tripwire/lales-virtual-machine.twd
Command line used:        tripwire --check
```

```

root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
Section: Unix File System
-----
Rule Name                Severity Level  Added  Removed  Modified
-----
Invariant Directories    66             0      0         0
Tripwire Data Files      100            0      0         0
Other binaries           66             0      0         0
Tripwire Binaries        100            0      0         0
Other libraries          66             0      0         0
Root file-system executables 100            0      0         0
System boot changes      100            0      0         0
Root file-system libraries (/lib) 100            0      0         0
Critical system boot files 100            0      0         0
Other configuration files (/etc) 66             0      0         0
Boot Scripts             100            0      0         0
Security Control         66             0      0         0
Root config files        100            0      0         0
* Devices & Kernel information 100            431    190       0
Total objects scanned: 80078
--MAC--

```

```

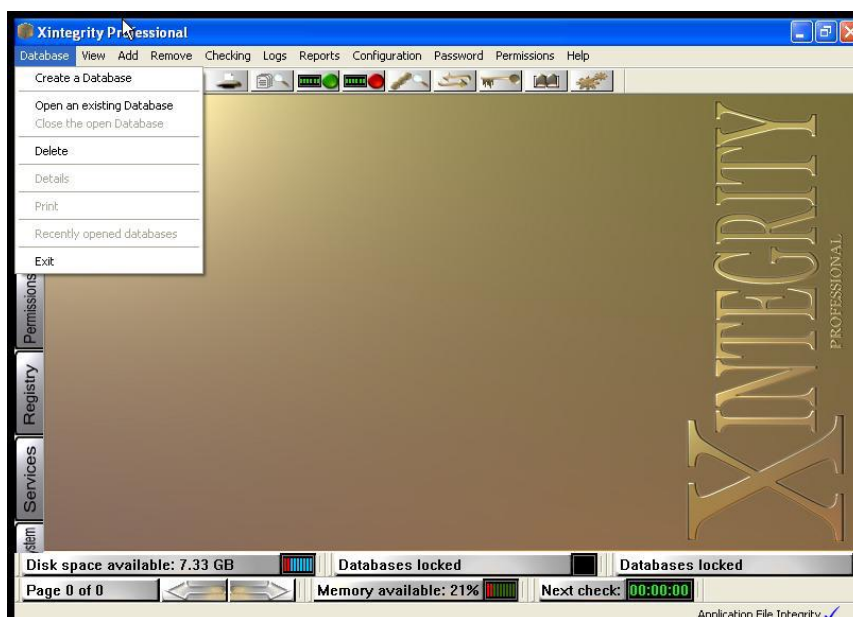
*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY; for details use --version. This is free software which may be redistributed or modified only under certain conditions; see COPYING for details.
All rights reserved.
Integrity check complete.
root@lales-virtual-machine:/home/lales#

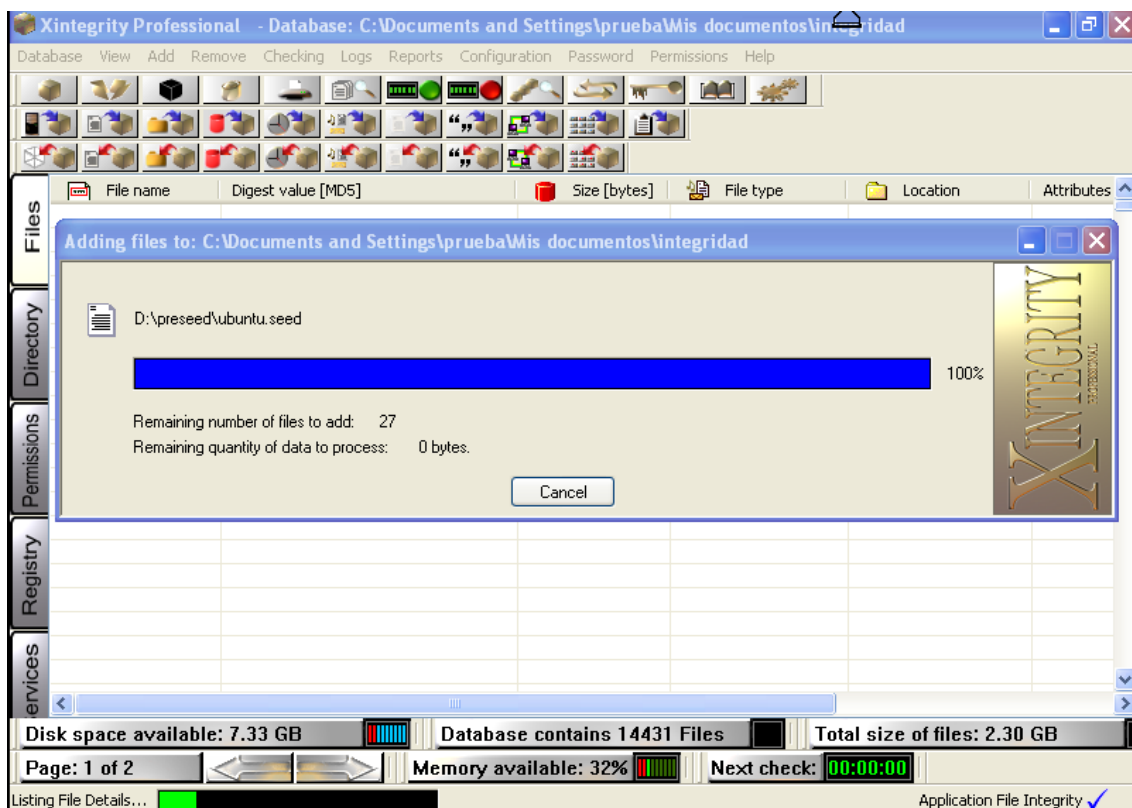
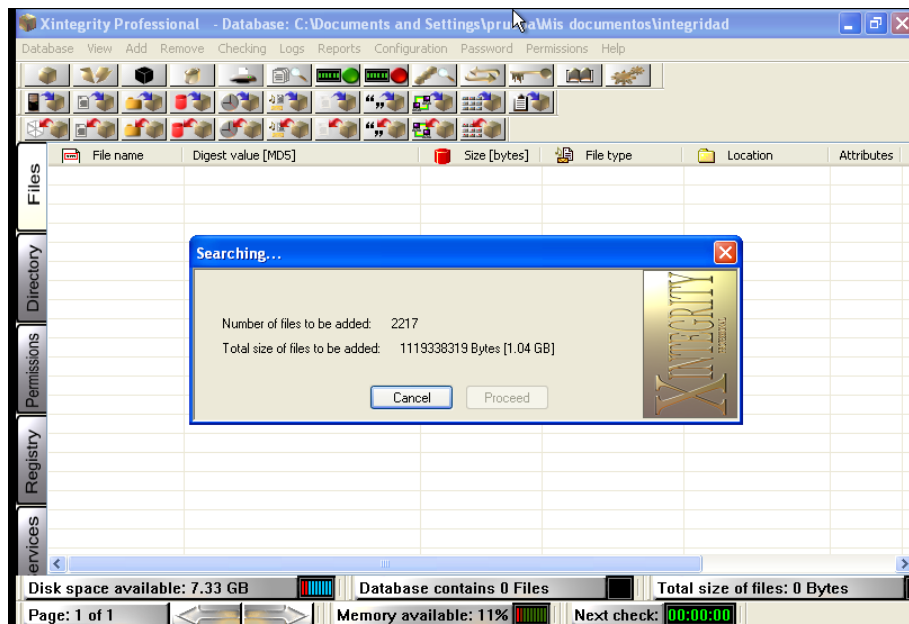
```

- Windows: Integridad del sistema de ficheros mediante Xintegrity.

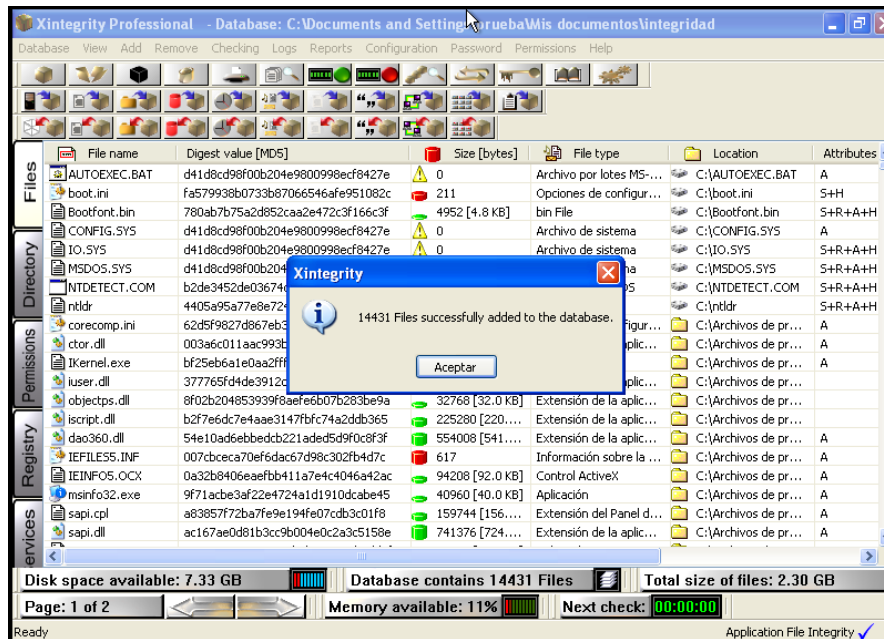
Nos descargamos el programa Xintegrity y en la pantalla principal creamos una base de datos



A continuación añadimos los archivos a nuestra base de datos



Y nos da correctamente todos los archivos que se han creado en la base de datos



c) Sistema de detección de intrusos (IDS): Net IDS:

- Instala y configura Snort en GNU/Linux.

www.snort.org

Instalamos con apt-get install snort

```
root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
root@lales-virtual-machine:/home/lales# apt-get install snort
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-2.6.38-8 linux-headers-2.6.38-8-generic
Utilice «apt-get autoremove» para eliminarlos.
Se instalarán los siguientes paquetes extras:
  libprelude2 oinkmaster snort-common snort-common-libraries
  snort-rules-default
Paquetes sugeridos:
  snort-doc
Se instalarán los siguientes paquetes NUEVOS:
  libprelude2 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 actualizados, 6 se instalarán, 0 para eliminar y 63 no actualizados.
Necesito descargar 1740 KB de archivos.
Se utilizarán 10,4 MB de espacio de disco adicional después de esta operación.
¿Desea continuar [S/n]?
```


Al final nos muestra un resumen de todas las escuchas que ha hecho

```
root@lales-virtual-machine: /etc
Archivo Editar Ver Buscar Terminal Ayuda
Received: 206
Analyzed: 206 (100.000%)
Dropped: 0 (0.000%)
Outstanding: 0 (0.000%)
=====
Breakdown by protocol (includes rebuilt packets):
  ETH: 206 (100.000%)
  ETHdisc: 0 (0.000%)
  VLAN: 0 (0.000%)
  IPV6: 7 (3.398%)
  IP6 EXT: 0 (0.000%)
  IP6opts: 0 (0.000%)
  IP6disc: 0 (0.000%)
  IP4: 173 (83.981%)
  IP4disc: 0 (0.000%)
  TCP 6: 0 (0.000%)
  UDP 6: 0 (0.000%)
  ICMP6: 0 (0.000%)
  ICMP-IP: 0 (0.000%)
  TCP: 11 (5.340%)
  UDP: 162 (78.641%)
  ICMP: 0 (0.000%)
  TCPdisc: 0 (0.000%)
  UDPdisc: 0 (0.000%)
```

MARÍA ÁNGELES PEÑASCO SÁNCHEZ – ACTIVIDAD 8 – TEMA 2 – SAD