

## ACTIVIDAD 5 – AMENAZAS Y ATAQUES EN REDES CORPORATIVAS – TEMA 2

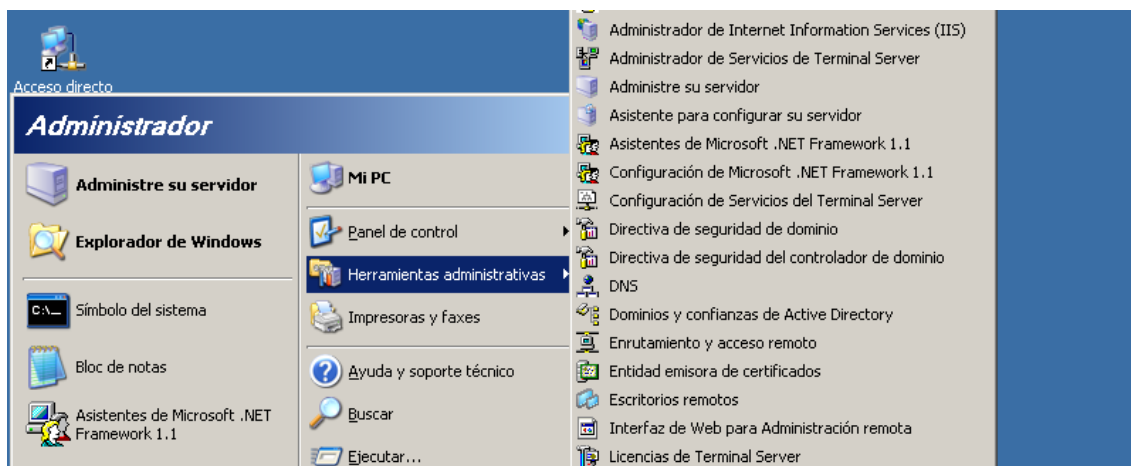
### a) Identidad digital.

¿Qué diferencias existen entre la instalación de un certificado en un servidor web y un servidor de certificaciones?

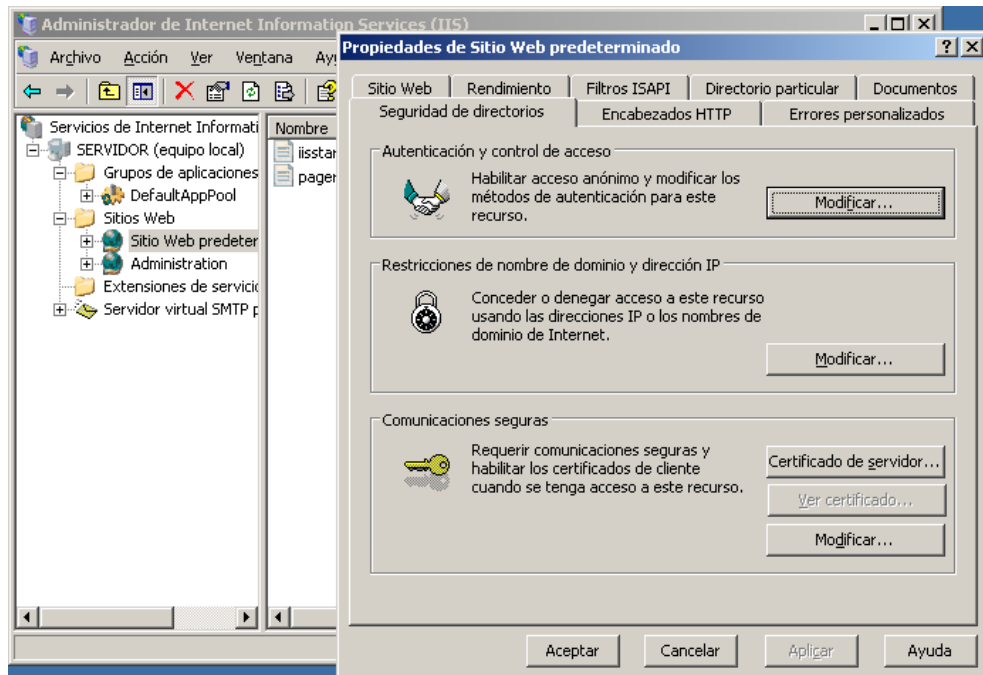
- Cifrado de datos: Los datos intercambiados entre el navegador del usuario y el servidor se cifrarán, con lo que no serían directamente inteligibles en caso de interceptación en su tránsito por la red. Esta característica es muy útil si se utilizan formularios para que el usuario envíe datos críticos o personales, o si el contenido del web o parte del mismo es un área privada cuyos datos son confidenciales y deben ser únicamente accesibles por un grupo cerrado de personas.
- Autenticación del servidor: El visitante podrá saber que el propietario de la web indicada en el certificado ha seguido un proceso de identificación ante un tercero (autoridad de certificación) que es quien emite el certificado. Este proceso de identificación varía según el emisor del certificado y el tipo de certificado, y puede ir desde la validación por correo electrónico del propietario del dominio hasta la validación documental de la existencia de la organización propietaria del dominio.

**Busca cómo se instala y qué opciones ofrece el servidor de certificados integrados en el servidor IIS de Microsoft. Realiza una petición por parte de un cliente de un certificado digital.**

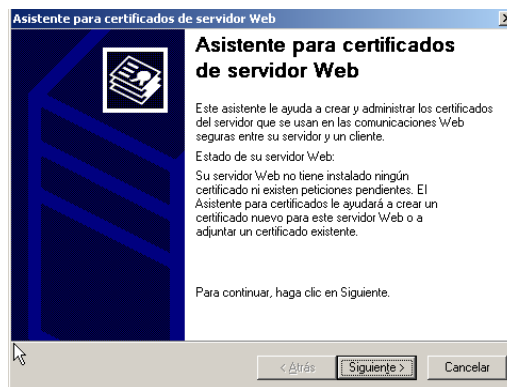
En WS2003 vamos a ir hasta herramientas administrativas y le damos al menú y elegimos Administrador de Internet Information Services (IIS)



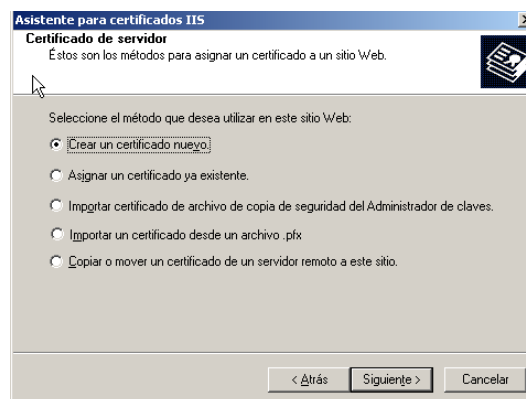
En propiedades de Sitio Web predeterminado le damos a Certificado de servidor y nos aparecerá un asistente



Y lo seguimos para crear el certificado de servidor



Le damos a crear un certificado nuevo



Aquí seguimos el asistente con la opción que nos viene por defecto

**Asistente para certificados IIS**

**Petición demorada o inmediata**

Puede preparar una petición para enviarla más tarde o inmediatamente.

¿Desea preparar una petición de certificado para enviarla más tarde o prefiere enviarla inmediatamente a una entidad emisora de certificados en línea?

Preparar la petición ahora pero enviarla más tarde

Enviar la petición inmediatamente a una entidad emisora de certificados en línea

< Atrás    Siguiente >    Cancelar

Aquí le ponemos nombre al certificado

**Asistente para certificados IIS**

**Nombre y configuración de seguridad**

Su nuevo certificado debe tener un nombre y una longitud en bits determinada.

Escriba un nombre para el nuevo certificado. El nombre debe ser fácil de usar y recordar.

Nombre:

La longitud en bits de la clave de cifrado determina el nivel de cifrado del certificado. Cuanto mayor sea la longitud, mayor será el nivel de seguridad aunque se corre el riesgo de que disminuya el rendimiento.

Longitud en bits:

Seleccionar el proveedor de servicios criptográficos (CSP) para este certificado

< Atrás    Siguiente >    Cancelar

Y una organización para lo que lo queremos

**Asistente para certificados IIS**

**Información de la organización**

El certificado debe incluir información que permita diferenciar su organización de otras.

Seleccione o escriba el nombre de su organización y de su unidad organizativa. Suele ser el nombre jurídico de su organización y el nombre de su división o departamento.

Para obtener más información, consulte el sitio Web de la entidad emisora del certificado.

Organización:

Unidad organizativa:

< Atrás    Siguiente >    Cancelar

El nombre del servidor lo dejamos por defecto

**Asistente para certificados IIS**

**Nombre común de su sitio Web**  
El nombre común de su sitio Web es su nombre de dominio completo.

Escriba el nombre de su sitio Web. Si el servidor está en Internet, utilice un nombre DNS válido. Si el servidor está en la intranet puede que prefiera utilizar el nombre NetBIOS del equipo.

Si cambia el nombre común, deberá obtener un nuevo certificado.

Nombre común:

< Atrás    Siguiete >    Cancelar

Y ponemos los datos de la localidad

**Asistente para certificados IIS**

**Información geográfica**  
La entidad emisora de certificados necesita la información geográfica siguiente.

País o región:

Estado o provincia:

Ciudad o localidad:

Los nombres de estado, provincia, ciudad y localidad deben ser nombres oficiales completos que no contengan abreviaturas.

< Atrás    Siguiete >    Cancelar

El nombre de archivo lo dejamos también por defecto

**Asistente para certificados IIS**

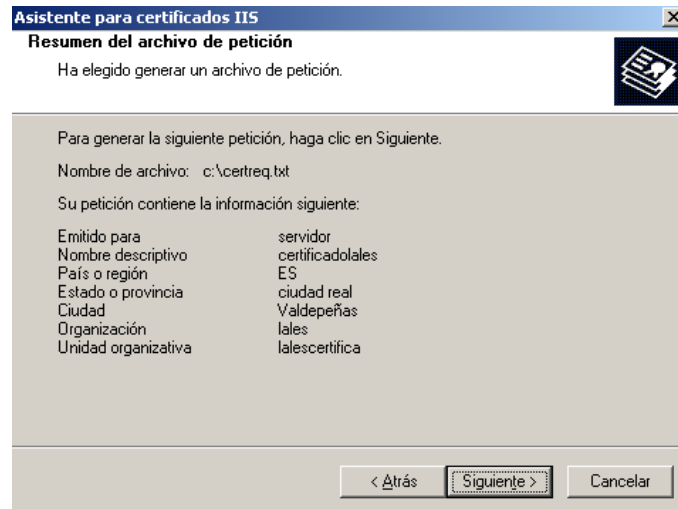
**Nombre de archivo de la petición de certificado**  
Su petición de certificado se ha guardado en un archivo de texto con el nombre de archivo que especificó.

Escriba un nombre de archivo para la petición de certificado.

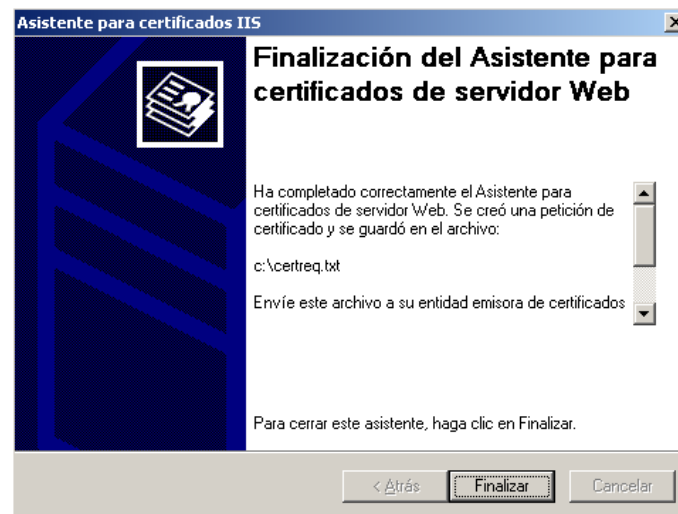
Nombre de archivo:  
    Examinar...

< Atrás    Siguiete >    Cancelar

Este es el resumen de la solicitud de certificado



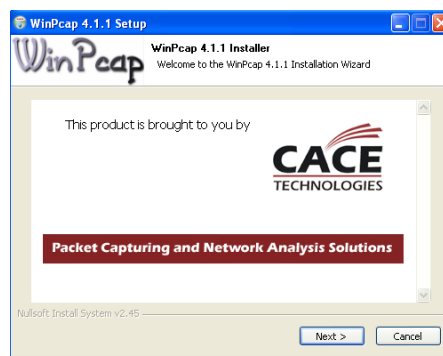
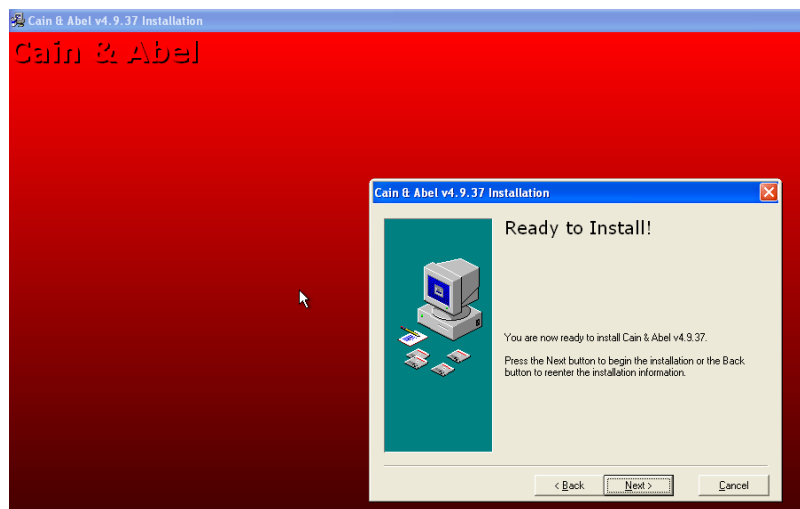
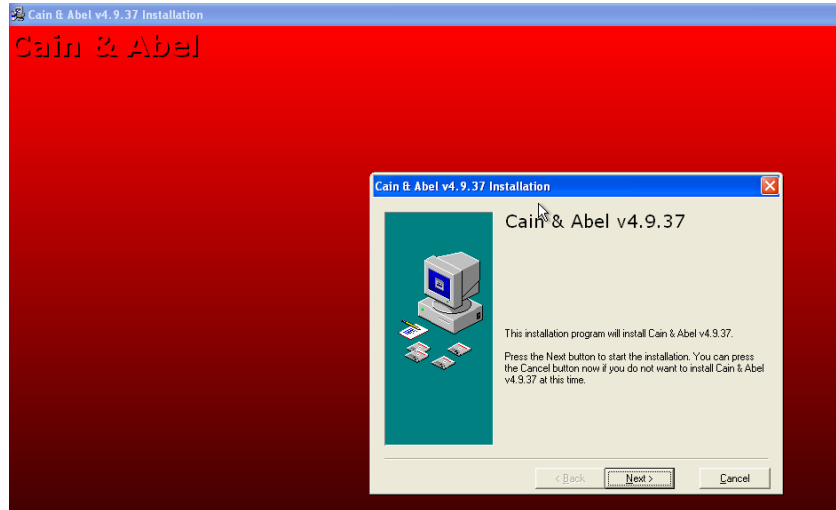
Y ya tenemos solicitado el certificado de servidor Web



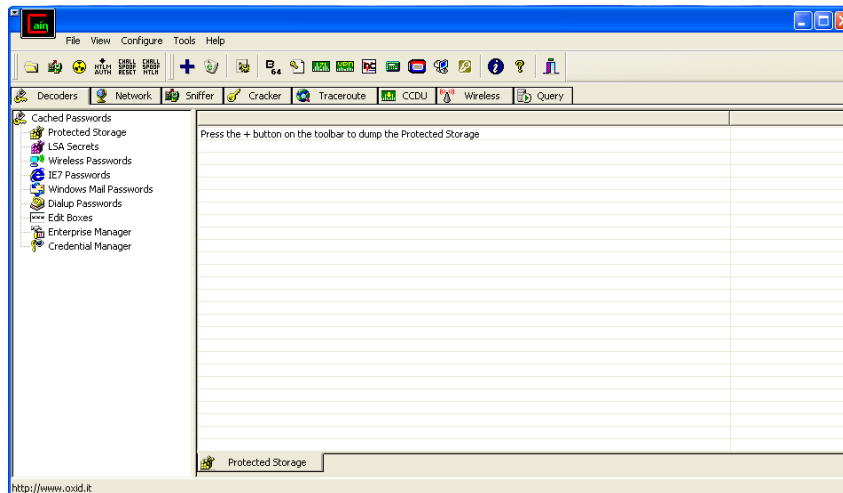
## b) Seguridad en redes corporativas

- Windows: Uso de Caín & Abel como Sniffing – MitM- ARP Spoofing – Pharming.

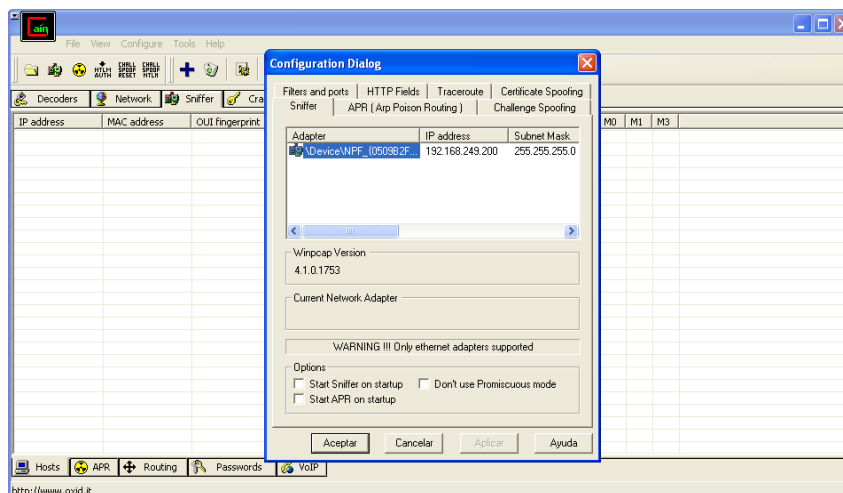
Nos descargamos la aplicación Caín & Abel



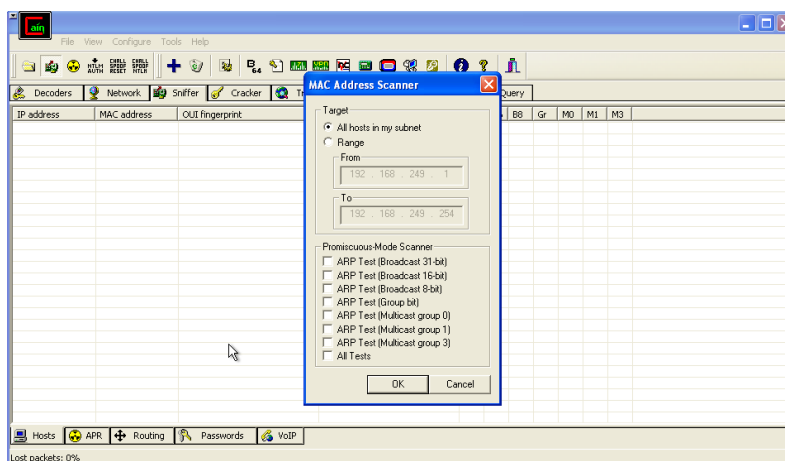
Esta es la pantalla principal del programa, le vamos a dar a Configure



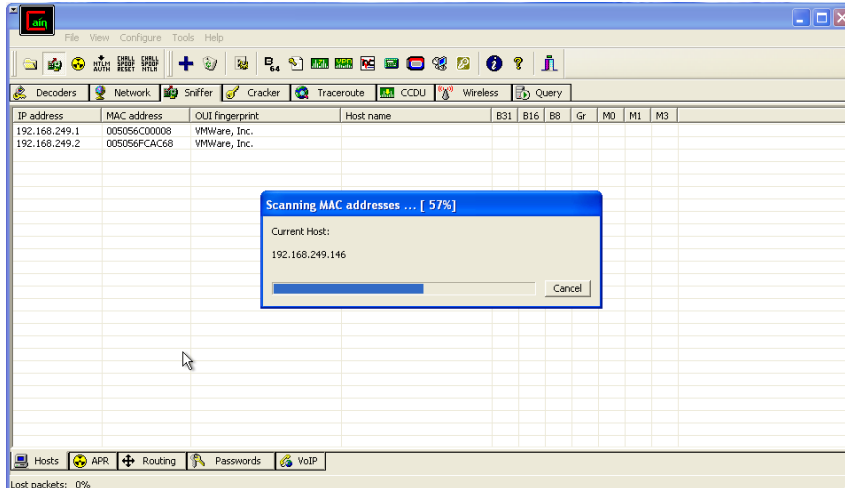
Aquí nos muestra las tarjetas que ha detectado, vamos a elegir la única que nos sale



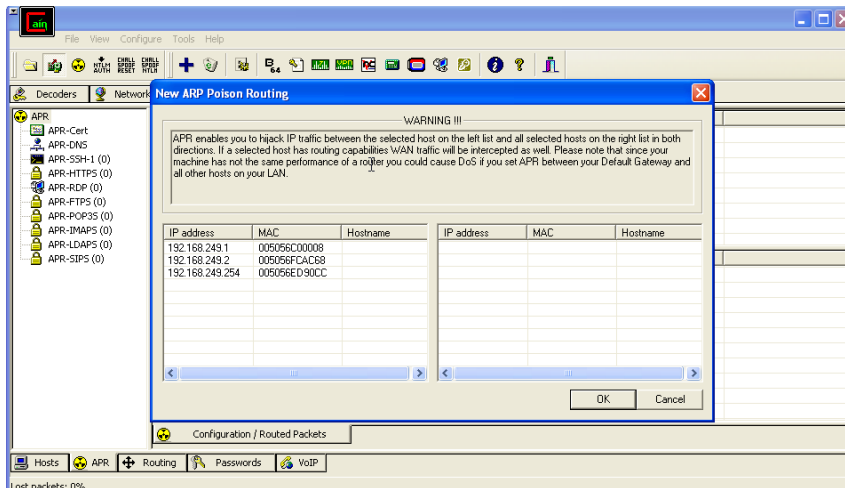
Ahora en el rango vamos a poner todos los hosts que encuentre y que haga el test de todo lo que encuentre



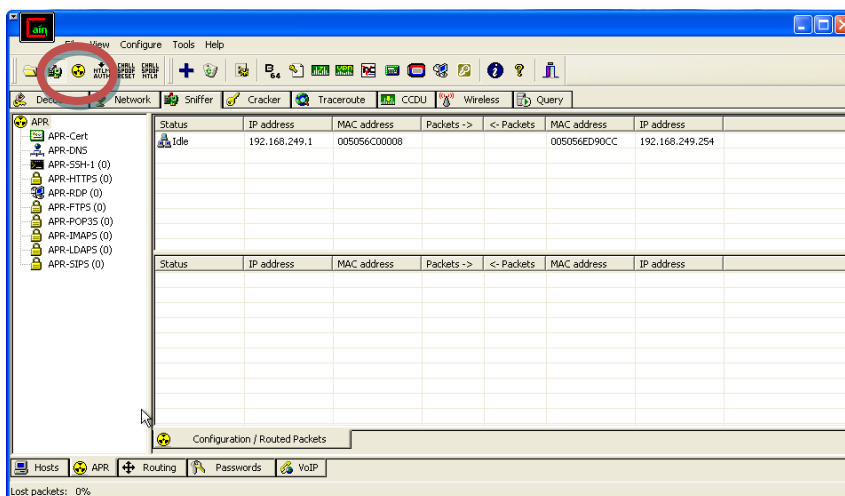
Y empieza a buscar las direcciones ip



Y nos muestra las que ha encontrado, vamos a elegir una de ellas

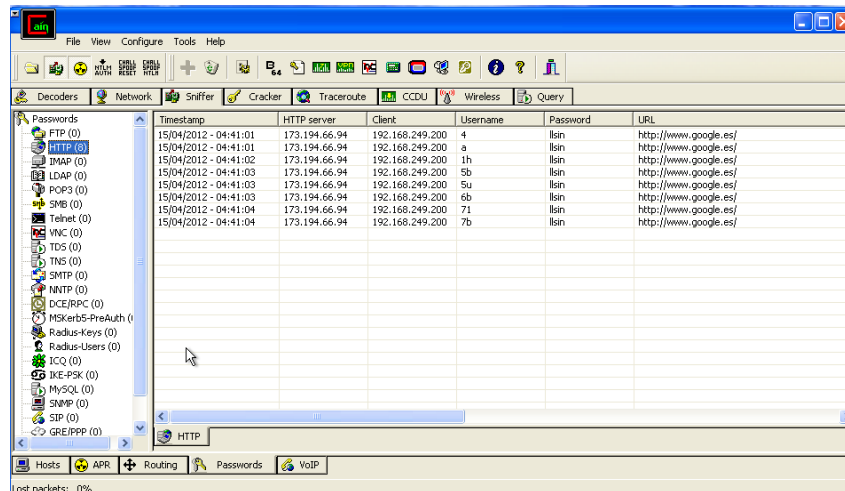


La elegimos y le damos al botón de Start/stop ARP





Si nos vamos al navegador de este equipo y nos metemos en cualquier página va saliendo todo donde vamos a entrar y lo que hacemos desde este equipo



## GNU/Linux: Uso de ArpWatch.

Lo primero que vamos a hacer es instalar arpwatc, para ello ponemos apt-get install arpwatc

```
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 arpwatc
```

Con el comando **arp -a** comprobamos si nos están atacando, ya que si la Ip y la MAC no se corresponden a las nuestras, podemos estar siendo víctimas de un ataque.

```
root@lales-virtual-machine:/home/lales# arp -a
? (192.168.249.2) en 00:50:56:fc:ac:68 [ether] en eth0
? (192.168.249.254) en 00:50:56:f0:3b:ac [ether] en eth0
root@lales-virtual-machine:/home/lales#
```

Con el comando **arp -nv -i eth0** le indicamos la interfaz que usaremos y nos muestra las conexiones existentes.

```
root@lales-virtual-machine:/home/lales# arp -nv -i eth0
Dirección      TipoHW  DirecciónHW      Indic Máscara      Inter
faz
192.168.249.2  ether  00:50:56:fc:ac:68  C                   eth0
192.168.249.254 ether  00:50:56:f0:3b:ac  C                   eth0
Entradas: 2 Ignoradas: 0 Encontradas: 2
root@lales-virtual-machine:/home/lales#
```

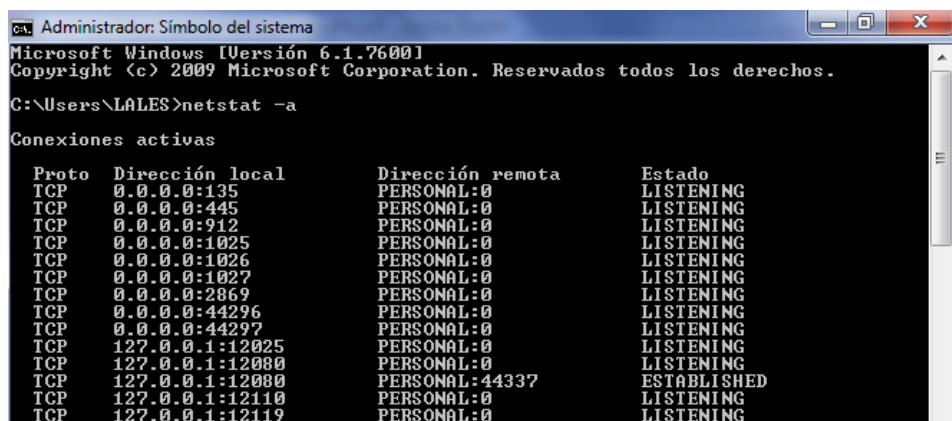
## c) Seguridad en redes corporativas

### - Uso de netstat para análisis de puertos en Windows y GNU/Linux.

#### NETSTAT

- **-a** Visualiza todas las conexiones y puertos TCP y UDP, incluyendo las que están "en escucha" (listening).
- **-b** En los sistemas recientes, visualiza el binario (ejecutable) del programa que ha creado la conexión.
- **-e** Estadísticas Ethernet de las visualizaciones, como el número de paquetes enviados y recibidos. Se puede combinar con la opción **-s**.
- **-n** Se muestran los puertos con su identificación en forma numérica y no de texto.
- **-o** En sistemas Windows XP y 2003 Server, muestra los identificadores de proceso (PID) para cada conexión. Se puede verificar los identificadores de proceso en el Administrador de Tareas de Windows (al agregarlo a las columnas de la pestaña procesos)
  
- **-p** Muestra las conexiones para el protocolo especificado; el protocolo puede ser TCP o UDP. Si se utiliza con la opción de **-s** para visualizar la estadística por protocolo; el protocolo (Proto) puede ser TCP, UDP o IP.
- **-r** Visualiza la tabla de enrutamiento o encaminamiento. Equivale al comando **route print**.
- **-s** Estadística por protocolo de las visualizaciones. Por el valor por defecto, la estadística se muestra para TCP, UDP e IP; la opción **-p** se puede utilizar para especificar un subconjunto del valor por defecto.
- **-v** En sistemas Windows XP y 2003 Server, y usado en conjunto con **-b**, muestra la secuencia de componentes usados en la creación de la conexión por cada uno de los ejecutables.
  
- **Intervalo:** Vuelve a mostrar la información cada intervalo (en segundos). Si se presiona CTRL+C se detiene la visualización. si se omite este parámetro, netstat muestra la información solo una vez.
- **/?** Help: aparecerán los caracteres y su función.

#### EN WINDOWS



```
ca. Administrador: Símbolo del sistema
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\LALES>netstat -a

Conexiones activas

Proto  Dirección local      Dirección remota      Estado
TCP    0.0.0.0:135           PERSONAL:0            LISTENING
TCP    0.0.0.0:445           PERSONAL:0            LISTENING
TCP    0.0.0.0:912           PERSONAL:0            LISTENING
TCP    0.0.0.0:1025          PERSONAL:0            LISTENING
TCP    0.0.0.0:1026          PERSONAL:0            LISTENING
TCP    0.0.0.0:1027          PERSONAL:0            LISTENING
TCP    0.0.0.0:2869          PERSONAL:0            LISTENING
TCP    0.0.0.0:44296         PERSONAL:0            LISTENING
TCP    0.0.0.0:44297         PERSONAL:0            LISTENING
TCP    127.0.0.1:12025       PERSONAL:0            LISTENING
TCP    127.0.0.1:12080       PERSONAL:0            LISTENING
TCP    127.0.0.1:12080       PERSONAL:44337        ESTABLISHED
TCP    127.0.0.1:12110       PERSONAL:0            LISTENING
TCP    127.0.0.1:12119       PERSONAL:0            LISTENING
```

```

C:\Users\LALES>netstat -b
Conexiones activas

    Proto Dirección local           Dirección remota           Estado
    TCP    127.0.0.1:12080           PERSONAL:44337            ESTABLISHED
    [AvastSvc.exe]
    TCP    127.0.0.1:44335           PERSONAL:44336            ESTABLISHED
    [umware.exe]
    TCP    127.0.0.1:44336           PERSONAL:44335            ESTABLISHED
    [umware.exe]
    TCP    127.0.0.1:44337           PERSONAL:12080            ESTABLISHED
    [umnat.exe]
    TCP    192.168.30.113:44295      72.5.58.53:http           ESTABLISHED
    [AvastSvc.exe]
    TCP    192.168.30.113:44322      a173-222-35-51:https      CLOSE_WAIT
    [umware.exe]
    TCP    192.168.30.113:44323      a173-222-35-51:https      CLOSE_WAIT
    [umware.exe]
    TCP    192.168.30.113:44324      a173-222-35-51:https      CLOSE_WAIT
    [umware.exe]
    TCP    192.168.30.113:44325      a173-222-35-51:https      CLOSE_WAIT
    [umware.exe]
    TCP    192.168.30.113:44338      ubuntu:http                ESTABLISHED
    [AvastSvc.exe]

C:\Users\LALES>_

```

```

C:\Users\LALES>netstat -e
Estadísticas de interfaz

                Recibidos           Enviados
Bytes           365662081           8894543
Paquetes de unidifusión 243285           144725
Paquetes no de unidifusión 3                2599
Descartados     0                 0
Errores         0                 0
Protocolos desconocidos 0

C:\Users\LALES>

```

```

C:\Users\LALES>netstat -r
=====
Lista de interfaces
15...1c 65 9d 1f 0b 36 .....Realtek RTL8191SE 802.11b/g/n WiFi Adapter
11...1c c1 de 9f 3a 34 .....Realtek PCIe FE Family Controller
16...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
17...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
1.....Software Loopback Interface 1
26...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft #8
20...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft #2
14...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
28...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft #10
63...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft #43
21...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft #3
19...00 00 00 00 00 00 e0 Adaptador 6to4 de Microsoft

```

```

IPv4 Tabla de enrutamiento
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace    Interfaz  Métrica
 0.0.0.0            0.0.0.0             192.168.30.1        192.168.30.113  25
127.0.0.0          255.0.0.0           En vínculo          127.0.0.1       306
127.0.0.1          255.255.255.255    En vínculo          127.0.0.1       306
127.255.255.255    255.255.255.255    En vínculo          127.0.0.1       306
192.168.0.0        255.255.255.0      En vínculo          192.168.0.1     276
192.168.0.1        255.255.255.255    En vínculo          192.168.0.1     276
192.168.0.255      255.255.255.255    En vínculo          192.168.0.1     276
192.168.30.0       255.255.255.0      En vínculo          192.168.30.113  281
192.168.30.113     255.255.255.255    En vínculo          192.168.30.113  281
192.168.30.255     255.255.255.255    En vínculo          192.168.30.113  281
192.168.249.0      255.255.255.0      En vínculo          192.168.249.1   276
192.168.249.1      255.255.255.255    En vínculo          192.168.249.1   276
192.168.249.255    255.255.255.255    En vínculo          192.168.249.1   276
224.0.0.0          240.0.0.0           En vínculo          127.0.0.1       306
224.0.0.0          240.0.0.0           En vínculo          192.168.0.1     276
224.0.0.0          240.0.0.0           En vínculo          192.168.249.1   276
224.0.0.0          240.0.0.0           En vínculo          192.168.30.113  281
255.255.255.255    255.255.255.255    En vínculo          127.0.0.1       306
255.255.255.255    255.255.255.255    En vínculo          192.168.0.1     276
255.255.255.255    255.255.255.255    En vínculo          192.168.249.1   276
255.255.255.255    255.255.255.255    En vínculo          192.168.30.113  281
=====
Rutas persistentes:
Ninguno

IPv6 Tabla de enrutamiento
=====
Rutas activas:
Cuando destino de red métrica      Puerta de enlace
 1 306 ::1/128                        En vínculo
16 276 fe80::/64                       En vínculo
17 276 fe80::/64                       En vínculo
15 281 fe80::/64                       En vínculo
17 276 fe80::3cc0:470:3866:6030/128    En vínculo
16 276 fe80::794f:e8ce:43d9:192d/128    En vínculo
15 281 fe80::e528:6ba5:c962:566/128     En vínculo
 1 306 ff00::/8                        En vínculo
16 276 ff00::/8                        En vínculo
17 276 ff00::/8                        En vínculo
15 281 ff00::/8                        En vínculo
=====
Rutas persistentes:
Ninguno

```

```

C:\Users\LALES>netstat -o
Conexiones activas

Proto Dirección local      Dirección remota      Estado      PID
TCP    127.0.0.1:12000      PERSONAL:44337        ESTABLISHED 1456
TCP    127.0.0.1:44335     PERSONAL:44336        ESTABLISHED 2776
TCP    127.0.0.1:44336     PERSONAL:44335        ESTABLISHED 2776
TCP    127.0.0.1:44337     PERSONAL:12000        ESTABLISHED 1860
TCP    192.168.30.113:44295 72.5.58.53:http       ESTABLISHED 1456
TCP    192.168.30.113:44322 a173-222-35-51:https  CLOSE_WAIT  2776
TCP    192.168.30.113:44323 a173-222-35-51:https  CLOSE_WAIT  2776
TCP    192.168.30.113:44324 a173-222-35-51:https  CLOSE_WAIT  2776
TCP    192.168.30.113:44325 a173-222-35-51:https  CLOSE_WAIT  2776
TCP    192.168.30.113:44338 ubuntu:http           ESTABLISHED 1456

```

```

C:\Users\LALES>netstat -v
Conexiones activas

Proto Dirección local      Dirección remota      Estado
TCP    127.0.0.1:12000      PERSONAL:44337        ESTABLISHED
TCP    127.0.0.1:44335     PERSONAL:44336        ESTABLISHED
TCP    127.0.0.1:44336     PERSONAL:44335        ESTABLISHED
TCP    127.0.0.1:44337     PERSONAL:12000        ESTABLISHED
TCP    192.168.30.113:44295 72.5.58.53:http       ESTABLISHED
TCP    192.168.30.113:44322 a173-222-35-51:https  CLOSE_WAIT
TCP    192.168.30.113:44323 a173-222-35-51:https  CLOSE_WAIT
TCP    192.168.30.113:44324 a173-222-35-51:https  CLOSE_WAIT
TCP    192.168.30.113:44325 a173-222-35-51:https  CLOSE_WAIT
TCP    192.168.30.113:44338 ubuntu:http           ESTABLISHED

```

## EN LINUX

- r, --route Muestra la tabla de enrutamiento.
- i, --interfaces Muestra la tabla de interfaces
- g, --groups Muestra los miembros del grupo de multidifusión
- s, --statistics Muestra estadísticas de red (como SNMP)
- M, --masquerade Muestra conexiones enmascaradas
- v, --verbose Muestra más información en la salida
- n, --numeric No resuelve nombres en general
- numeric-hosts No resuelve el nombre de los hosts
- numeric-ports No resuelve el nombre de los puertos
- numeric-users No resuelve los nombres de usuarios
- N, --symbolic Muestra los nombres del hardware de red
- e, --extend Muestra otra/mas información.
- p, --programs Muestra PID o nombre del programa por cada socket
- c, --continuous Muestra continuamente las estadísticas de red (hasta que se interrumpa el programa)
- l, --listening Muestra los server sockets que están es modo escucha
- a, --all, --listening Muestra todos los sockets (por defecto únicamente los que están en modo conectado)
- o, --timers Muestra los timers
- F, --fib Muestra el Forwarding Information Base (por defecto)

```
root@lales-virtual-machine:/home/lales# netstat -i
Tabla de la interfaz del núcleo
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0    1500 0      511    0      0 0      553    0      0      0 B
MRU
lo      16436 0      1163   0      0 0      1163   0      0      0 L
RU
root@lales-virtual-machine:/home/lales#
```

```

root@lales-virtual-machine:/home/lales# netstat -l
Conexiones activas de Internet (solo servidores)
Proto Recib Enviad Dirección local Dirección remota Estado
tcp 0 0 *:39937 *: * ESCUCHAR
tcp 0 0 *:nfs *: * ESCUCHAR
tcp 0 0 *:sunrpc *: * ESCUCHAR
tcp 0 0 *:35728 *: * ESCUCHAR
tcp 0 0 *:ftp *: * ESCUCHAR
tcp 0 0 *:ssh *: * ESCUCHAR
tcp 0 0 localhost:ipp *: * ESCUCHAR
tcp 0 0 *:46527 *: * ESCUCHAR
tcp6 0 0 [::]:ssh [::]: * ESCUCHAR
tcp6 0 0 ip6-localhost:ipp [::]: * ESCUCHAR
udp 0 0 *:bootpc *: * ESCUCHAR
udp 0 0 *:sunrpc *: * ESCUCHAR
udp 0 0 lales-virtual-machi:ntp *: * ESCUCHAR
udp 0 0 localhost:ntp *: * ESCUCHAR
udp 0 0 *:ntp *: * ESCUCHAR
udp 0 0 *:43658 *: * ESCUCHAR
udp 0 0 *:mdns *: * ESCUCHAR
udp 0 0 *:850 *: * ESCUCHAR
udp 0 0 *:59251 *: * ESCUCHAR
udp 0 0 *:38272 *: * ESCUCHAR

```

```

udp6 0 0 [::]:53090 [::]: *
Activar zócalos de dominio UNIX (solo servidores)
Proto RefCnt Flags Type State I-Node Ruta
unix 2 [ ACC ] FLUJO ESCUCHANDO 12901 /tmp/orbit-lales/linc
-664-0-62de0725aef9f
unix 2 [ ACC ] FLUJO ESCUCHANDO 13023 /tmp/orbit-lales/linc
-668-0-54a3d14f2fe5
unix 2 [ ACC ] FLUJO ESCUCHANDO 13055 /tmp/orbit-lales/linc
-66c-0-7946c8354c3bd
unix 2 [ ACC ] FLUJO ESCUCHANDO 13404 /tmp/orbit-lales/linc
-67f-0-1560ab7b3f843
unix 2 [ ACC ] FLUJO ESCUCHANDO 10970 /tmp/ssh-dlllEvmQ1494
/agent.1494
unix 2 [ ACC ] FLUJO ESCUCHANDO 13821 /tmp/orbit-lales/linc
-697-0-6ccab94c9d1a6
unix 2 [ ACC ] FLUJO ESCUCHANDO 11009 /tmp/.ICE-unix/1494
unix 2 [ ACC ] FLUJO ESCUCHANDO 11008 @/tmp/.ICE-unix/1494
unix 2 [ ACC ] FLUJO ESCUCHANDO 17145 /tmp/orbit-lales/linc
-8ec-0-73f64abfc02b9
unix 2 [ ACC ] FLUJO ESCUCHANDO 11045 /tmp/orbit-lales/linc
-600-0-2e11431bb5913
unix 2 [ ACC ] FLUJO ESCUCHANDO 13895 /tmp/orbit-lales/linc
-69c-0-65cf5614ba3f6
unix 2 [ ACC ] FLUJO ESCUCHANDO 13958 /tmp/orbit-lales/linc

```

```

root@lales-virtual-machine: /home/lales
Archivo Editar Ver Buscar Terminal Ayuda
unix 3 [ ] FLUJO CONECTADO 13249
unix 2 [ ] DGRAM 13238
unix 3 [ ] FLUJO CONECTADO 13223 @/tmp/dbus-k90YytFTGe
unix 3 [ ] FLUJO CONECTADO 13222
unix 3 [ ] FLUJO CONECTADO 13221 @/tmp/dbus-k90YytFTGe
unix 3 [ ] FLUJO CONECTADO 13220
unix 3 [ ] FLUJO CONECTADO 13211 @/dbus-vfs-daemon/soc
ket-rxap9KvD
unix 3 [ ] FLUJO CONECTADO 13210
unix 3 [ ] FLUJO CONECTADO 13212 @/dbus-vfs-daemon/soc
ket-ZgWHyIiw
unix 3 [ ] FLUJO CONECTADO 13209
unix 3 [ ] FLUJO CONECTADO 13208 @/tmp/.X11-unix/X0
unix 3 [ ] FLUJO CONECTADO 13207
unix 3 [ ] FLUJO CONECTADO 13197 /var/run/dbus/system_
bus_socket
unix 3 [ ] FLUJO CONECTADO 13196
unix 3 [ ] FLUJO CONECTADO 13193 @/tmp/.X11-unix/X0
unix 3 [ ] FLUJO CONECTADO 13192
unix 3 [ ] FLUJO CONECTADO 13189 @/tmp/dbus-k90YytFTGe
unix 3 [ ] FLUJO CONECTADO 13188
unix 3 [ ] FLUJO CONECTADO 13185 @/tmp/.X11-unix/X0
unix 3 [ ] FLUJO CONECTADO 13184 @/tmp/.X11-unix/X0
unix 3 [ ] FLUJO CONECTADO 13183

```

```

root@lales-virtual-machine:/home/lales# netstat -r
Tabla de rutas IP del núcleo
Destino          Pasarela          Genmask          Indic  MSS Ventana irtt Interfa
Z
192.168.249.0    *                 255.255.255.0   U      0 0          0 eth0
link-local       *                 255.255.0.0     U      0 0          0 eth0

```

## Uso de un análisis de puertos on line:

<http://www.internautas.org/w-scanonline.php>

Entramos a la página web y vamos a elegir escanear los puertos

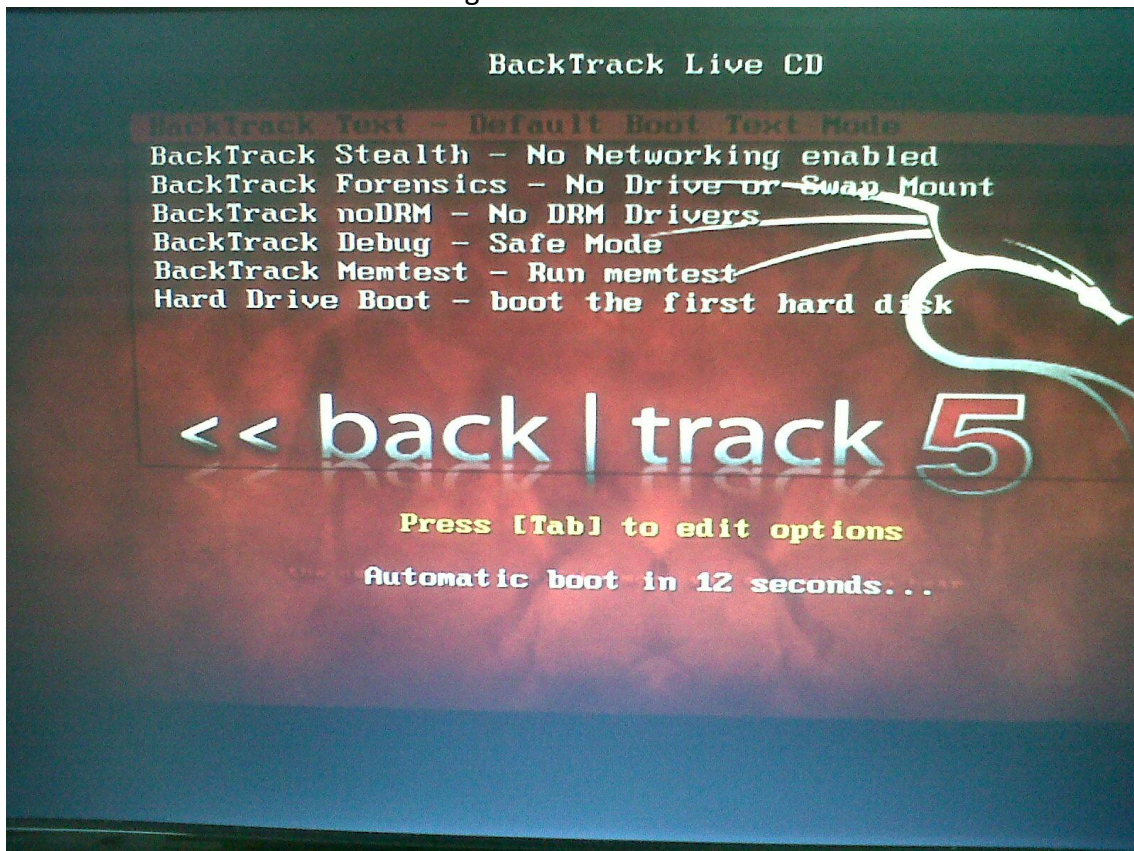
Puerto	Desc.	Estado	Observaciones
20	FTP	cerrado	Utilizado por FTP
21	FTP	cerrado	Utilizado por FTP
22	SSH	abierto	Secure Shell.
23	TELNET	cerrado	Acceso remoto
25	SMTP	cerrado	Servidor de correo SMTP
53	DNS	abierto	Servidor DNS
79	FINGER	cerrado	Servidor de información de usuarios de un PC
80	HTTP	abierto	Servidor web
110	POP3	cerrado	Servidor de correo POP3
119	NNTP	cerrado	Servidor de noticias
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
135	DCOM-scm	cerrado	Solo se puede cerrar a través de un cortafuegos
139	NETBIOS	cerrado	Compartición de Ficheros a través de una red
143	IMAP	cerrado	Servidor de correo IMAP
389	LDAP	cerrado	LDAP. Tambien Puede ser utilizado por Neetmeting
443	HTTPS	abierto	Servidor web seguro
445	MSFT DS	cerrado	Server Message Block.
631	IPP	cerrado	Servidor de Impresion
1433	MS SQL	cerrado	Base de Datos de Microsoft
3306	MYSQL	cerrado	Base de Datos. MYSQL
5000	UPnP	cerrado	En windows está activado este puerto por defecto.

d) Uso de la distribución Backtrack de GNU/Linux con la finalidad de investigar sobre la inyección de código SQL (SQL Injection) con la finalidad de obtener las tablas de usuarios y contraseñas de las bases de datos de sitios web.

Nos descargamos la imagen de Backtrack

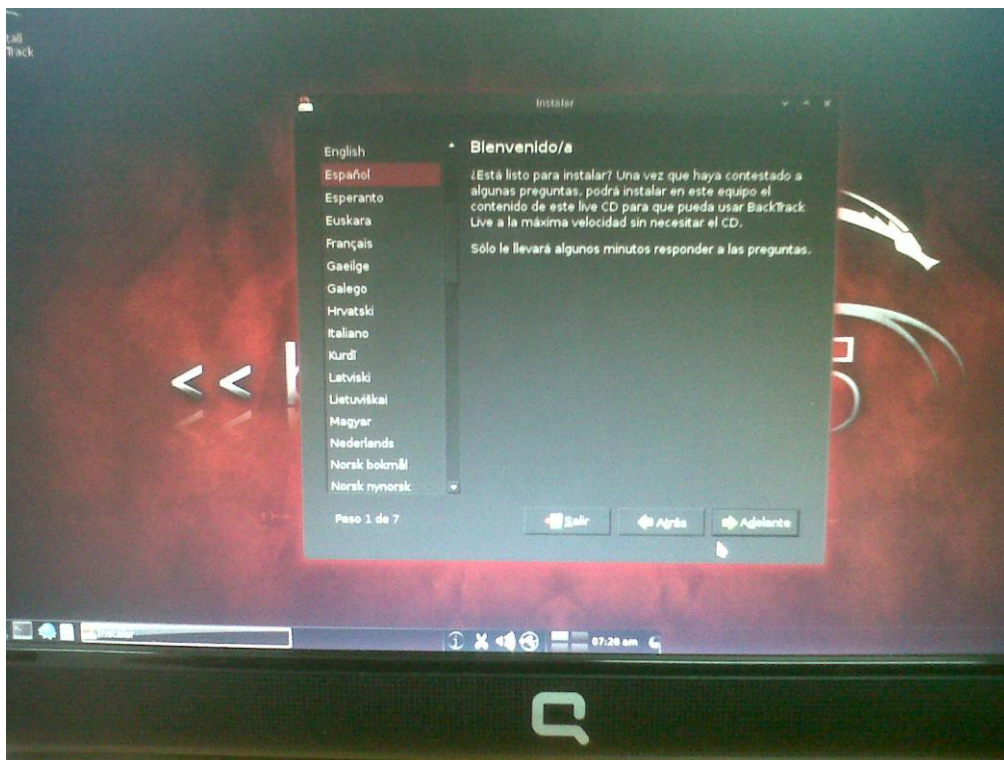


Y cargamos desde Live CD

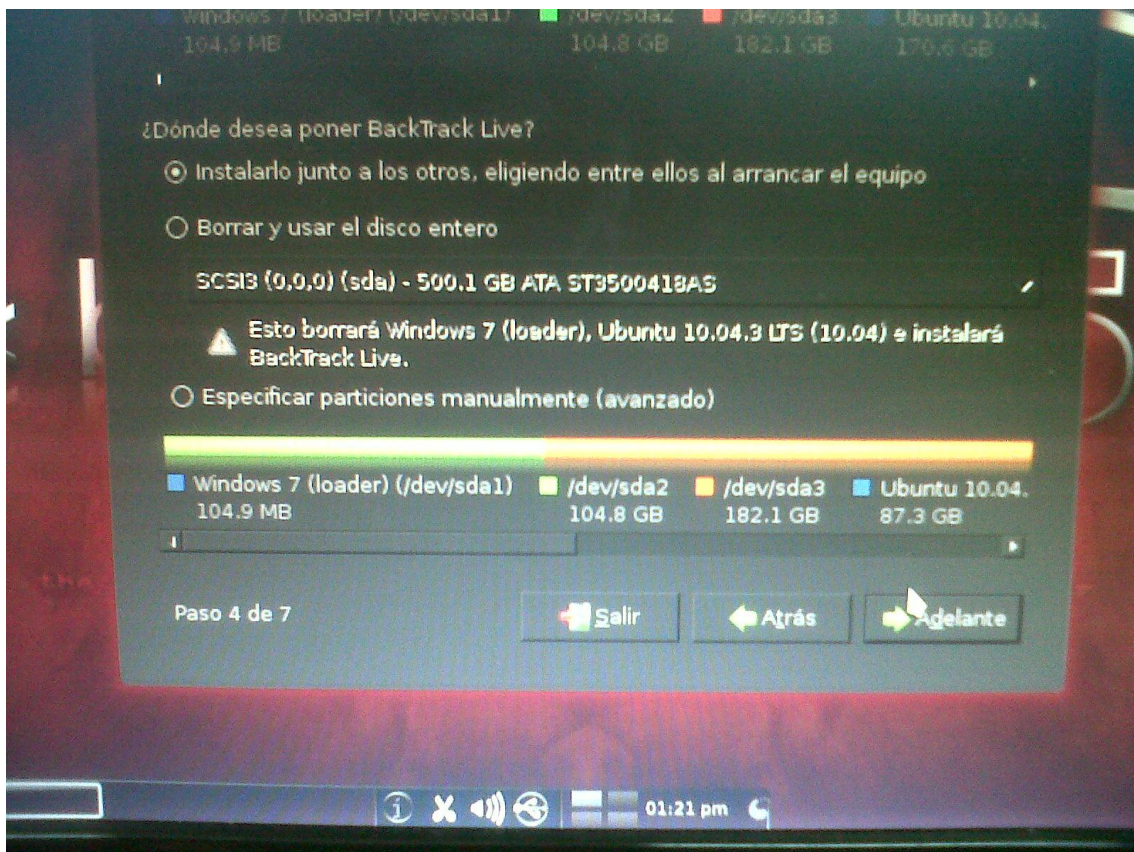




Elegimos el idioma



Y elegimos donde lo vamos a instalar



Y esta es la ventana principal de Backtrack y vamos a ir hasta la consola



Aquí tenemos la consola donde vamos a trabajar

```
root@bt: /pentest/web/scanners/sqlmap
File Edit View Terminal Help
General:
  These options can be used to set some general working parameters.

-t TRAFFICFILE      Log all HTTP traffic into a textual file
-s SESSIONFILE     Save and resume all data retrieved on a session file
--flush-session    Flush session file for current target
--fresh-queries    Ignores query results stored in session file
--eta              Display for each output the estimated time of arrival
--update          Update sqlmap
--save            Save options on a configuration INI file
--batch          Never ask for user input, use the default behaviour

Miscellaneous:
--beep            Alert when sql injection found
--check-payload  IDS detection testing of injection payloads
--cleanup        Clean up the DBMS by sqlmap specific UDF and tables
--forms         Parse and test forms on target url
--gpage=GOOGLEPAGE Use Google dork results from specified page number
--page-rank      Display page rank (PR) for Google dork results
--parse-errors   Parse DBMS error messages from response pages
--replicate      Replicate dumped data into a sqlite3 database
--tor            Use default Tor (Vidalia/Privoxy/Polipo) proxy address
--wizard        Simple wizard interface for beginner users
root@bt: /pentest/web/scanners/sqlmap#
```

**Prueba en un sitio web en el que sea necesario registrarse.  
¿Qué tipo de precauciones tendrías como administrador web  
para evitar inyecciones SQL?**

<http://www.backtrack-linux.org/>

Hay algunas precauciones que pueden tomarse para evitar este tipo de ataques. Por ejemplo, es una buena práctica agregar una capa entre un formulario visible y la base de datos.

En PHP, la extensión PDO se usa a menudo para trabajar con parámetros en lugar de incrustar el contenido del usuario en la declaración. Otra técnica muy fácil es escapar caracteres, donde todos los caracteres peligrosos que pueden tener un efecto directo sobre la estructura de base de datos se escapan. Por ejemplo, cada comilla simple [''] en un parámetro se debe sustituir por dos comillas simples ['] para formar una cadena literal de SQL válida. Estas son sólo dos de las acciones más comunes que puedes tomar para mejorar la seguridad de un sitio web y evitar las inyecciones SQL. En Internet puedes encontrar muchos recursos que se ajustan a tus necesidades (lenguajes de programación, aplicaciones web específicas, etc).

**MARÍA ÁNGELES PEÑASCO SÁNCHEZ – PRÁCTICA 5 – TEMA 2 - SAD**