
11. Session HiJacking
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

# Introducción

Session HiJacking ocurre después de que se establece una sesión válida. El atacante roba una ID de una sesión válida que es utilizada para ingresar dentro del sistema y curiosear dentro del sistema. En TCP session Hijacking, un atacante roba una sesión TCP entre dos equipos. Ya que la autenticación solo ocurre al inicio de la sesión TCP, esto permite al usuario obtener acceso al equipo.

# Riesgos planteados por Hijacking

- La mayoría de las contramedidas no funcionan a menos que se utilice encriptación.
- Es simple de realizar.
- Amenaza de robos de identidad, pérdida de información, fraude, etc.
- La mayoría de los equipos que utilizan TCP/IP son vulnerables.
- Se puede hacer muy poco para protegerse a menos que se cambie a un protocolo más seguro.

# ¿Por que las sesiones Hijacking son exitosas?

- No hay bloqueo de cuentas para las ids de sesiones inválidas.
- Manipulación insegura.
- Ids de sesiones pequeñas.
- Transmisión en texto claro.
- Expiración de tiempo de sesión indefinida.
- Algoritmo de generación de IDs débil.

# Técnicas clave para la sesión Hijacking

- Fuerza Bruta: Un atacante intenta con IDs diferentes hasta que ocurre.
- Robo: Un atacante utiliza distintas técnicas para robar IDs de sesión.
- Calculando: Utilizando IDs generados de manera NO aleatoria, un atacante intenta calcular las IDs de las sesiones.

# Ejemplo de fuerza bruta

www.mysite.com/view/VW30422101518909

www.mysite.com/view/VW30422101518803

www.mysite.com/view/VW30422101518507

# Ataque HTTP Referrer

Un ataque intenta atraer a un usuario a hacer clic a un vínculo de otro sitio. Por ej: GET /index.html HTTP/1.0 Host: www.mysite.com Referrer: www.mywebmail.com/viewmsg, asp?msgid=6896646&SID2556x54VA75. El navegador envía la referrer URL conteniendo la ID de sesión al sitio del atacante www.hostile.com y el atacante ahora tiene la sesión ID del usuario.

# Spoofing vs. Hijacking

El spoofing pretende ser otro usuario, robando credenciales.

El Hijacking toma una sesión activa existente. Depende de un usuario legítimo para realizar la conexión

# Proceso de Session Hijacking

1. Sniff. Colocarse entre la victima y el blanco.
2. Monitor. Monitorear el flujo de paquetes y predecir la secuencia numérica.
3. Session Desynchronization. Romper la conexión al equipo de la víctima.
4. Session ID prediction. Robar la sesión.
5. Command injection. Comenzar a inyectar paquetes al servidor objetivo.

# Análisis de paquetes de una sesión local Hijacking

Se observa el intercambio de datos entre dos nodos, y si lo vemos podemos predecir la secuencia numérica.

# Tipos de Session Hijacking

- Activa: Un atacante encuentra una sesión activa y la roba.
- Pasiva: Un atacante hijackea una sesión, pero se sienta y observa los registros del tráfico que están siendo enviados.

# Session Hijacking en el modelo OSI

- Network Level Hijacking: Puede ser definido como la intercepción de paquetes durante la transmisión entre el cliente y el servidor en una sesión TCP y UDP.
- Application Level Hijacking: Obtener el control de una sesión HTTP de un usuario, obteniendo su ID de sesión.

# Application Level Session Hijacking

- Un token de sesión es robado o una sesión válida es predicha para obtener acceso no autorizado al servidor Web. Un token de sesión puede ser comprometido de varias maneras:
  - Session sniffing.
  - Man-in-the-browser attack.
  - Tokens de sesión precedible.
  - Ataques del lado del cliente.
  - Ataque man-in-the-middle

# Session Sniffing

El atacante usa un sniffer para capturar un token de sesión válida llamada "Session ID". Luego utiliza ese token para obtener acceso al servidor web.

# Tokens de sesión predecible

Es un método que se utiliza para predecir un ID de sesión o hacerse pasar por un usuario de sitio web. También se lo denomina Sesiono Hijacking. Utilizando esta técnica, el atacante consigue hacer ping a las solicitudes del sitio web. Adivinando un valor de sesión o deduciéndolo se realiza el ataque.

# ¿Cómo predecir una Session Token?

El atacante capturará varias IDs de sesión y analizará el patrón:

http://www.juggyboy.com/view/JBEX21092010152820
http://www.juggyboy.com/view/JBEX21092010153020
http://www.juggyboy.com/view/JBEX21092010160020
http://www.juggyboy.com/view/JBEX21092010164020

JBEX: Constante
25092010: Fecha
162555: Hora

# Ataque man-in-the-middle

Es utilizado para entrometerse dentro de una conexión existente entre los sistemas e interceptar los mensajes intercambiados.

Los atacantes utilizan distintas técnicas para dividir la conexión TCP en dos conexiones:

1. Conexión Client-to-attacker
2. Conexión Attacker-to-server

Luego de la intercepción, un atacante puede leer, modificar e insertar datos fraudulentos en la comunicación.

# Man-in-the-browser attack

Utiliza un caballo de troya para interceptar llamadas entre el navegador y su mecanismo de seguridad o librerías. Trabaja con un caballo de troya ya instalado y actúa entre el navegador y su mecanismo de seguridad. Su objetivo principal es de causar fraude financiero manipulando las transacciones de los sistemas de los bancos por internet.

# Pasos para realizar un ataque man-in-the-browser

1. Infectar al equipo con un troyano (S.O. o aplicación)
2. El troyano instala código malicioso (archivos de extensión) y lo guarda dentro de la configuración del navegador.
3. Luego de que el usuario reinicia el navegador, el código malicioso en el form de los archivos de extensión es cargado.
4. Los archivos de extensión registran un controlador para cada visita a una pagina web.
5. Cuando la página es cargada, la extensión utiliza la URL y la compara con una lista de sitios conocidos para el ataque.

# Pasos para realizar un ataque man-in-the-browser

6. El usuario se loguea de manera segura al sitio.
7. Registra un botón de controlador de eventos cuando la carga de una página específica es detectada por un patrón específico y la compara con su lista.
8. El navegador envía el form y modifica los valores al servidor.
9. Cuando el usuario hace clic en el botón, la extensión utiliza una interfaz DOM y extrae todos los datos desde los campos del form y modifica los valores.

# Pasos para realizar un ataque man-in-the-browser

10. El servidor recibe los valores modificados pero no puede distinguir entre los valores originales y modificados.
11. Luego de que el servidor realiza la transacción, un recipiente es generado.
12. Ahora, el navegador recibe el recipiente para la transacción modificada.
13. El navegador muestra el recipiente con los detalles originales.
14. El usuario piensa que la transacción  original fue recibida por el servidor sin ninguna intercepción.

# Ataques del lado del cliente

- XSS: Los ataques Cross-Site Scripting son un tipo de ataques de inyección, en el cual los scripts maliciosos son inyectados a los sitios Web.
- Malicious JavaScript Codes: Un script malicioso puede ser embebido en un sitio Web y no genera ningún tipo de advertencias cuando la página es vista en cualquier navegador.
- Troyanos: Programas aparentemente inofensivos pero pueden obtener control y causar daño.

# Cross-site Script Attack

El atacante puede comprometer el token de la sesión enviando código o programas maliciosos a los programas del lado del cliente.

# Fijación de sesión

Es un ataque que permite al atacante hijackear una sesión válida de un usuario. El atacante intenta atraer a usuario a autentificarse el mismo con una ID de sesión conocida y luego hijackear la sesión válida del usuario por el conocimiento de la ID de sesión utilizada. El atacante tiene que proveer una aplicación web legítima y atraer al navegador del usuario a utilizarla.

Muchas técnicas para ejecutar ataques de fijación de sesión son:

- Un token de sesión en el argumento URL.
- Un token de sesión en un campo de formulario oculto.
- Un ID de sesión en una cookie.

# Ataque de fijación de sesión

- El atacante explota una vulnerabilidad de un servidor que permite al usuario utilizar un SID fijo.
- El atacante provee un SID válido a la víctima y la atrae para que se autentifique a él mismo utilizando ese SDI.

# Ataque de fijación de sesión

Ejemplo:

1. Manda por correo, Hola Lolita mira esto: http://.....
2. La víctima hace clic ahí. Cookie: 0D644....
3. Atacante inicia sesión
4. Inicia sesión con el mismo SID (de la cookie)
5. Postea account.php. Cookie: la misma

# Session Hijacking a nivel de red

Es implementada en el flujo de datos del protocolo compartido por todas las aplicaciones web. El atacante puede obtener información crítica que es utilizada para atacar sesiones a nivel de aplicación.

- Blind Hijacking es una situación que no se puede monitorear el flujo de tráfico entre dos hosts.
- UDP Hijacking no necesita predecir secuencia de números porque no hay secuencia de números, se inyecta el paquete al listener UDP y esperar que los datos sean aceptados.

# Session Hijacking a nivel de red

- Man in the Middle Packet Sniffer
- TCP/IP Hijacking compromete la capa red del modelo OSI.
- RST Hijacking para desincronizar los nodos y tomar la conexión.
- IP Spoofing: Source routed packets detectando la ruta de los paquetes hacia la red.

# 3-Way Handshake

Si un atacante puede anticipar la siguiente secuencia y el número ACK que envió el usuario, el podrá spoofear la dirección del usuario y comenzar la comunicación con servidor. Si se puede ver la transmisión y el número de secuencia, predecir el número de secuencia no es tan difícil.

# Sequence Numbers

Son importantes en proveer una comunicación segura y también son cruciales para las hijacking sessions. Tienen un contador de 32 bits. Por tanto, las combinaciones pueden ser mas de 4 billones. Son utilizados para decir a la máquina receptora en que orden los paquetes deben ir cuando son recibidos. Por tanto, un atacante debe adivinar la secuencia si quiere hacer una sesión hijacking.

# Predicción de la secuencia de números

Luego de que un cliente envía un paquete de solicitud de conexión SYN al servidor, el servidor responde con una secuencia de números de elección SYN-ACK, que debe ser conocido por el cliente. Esta secuencia es predecible, el ataque conecta al servidor primero con su propia IP, registra la secuencia elegida, y luego abre una segunda conexión desde una IP falsa. El ataque no ve el SYN-ACK (o ningún otro paquete) desde el servidor, pero puede adivinar la respuesta correcta. Si la IP fuente es utilizada para autentificación, entonces el atacante puede utilizar una comunicación desigual para entrar al servidor.

# TCP/IP Hijacking

Es una técnica hacking que utiliza paquetes spoofeados para tomar una conexión entre la víctima y la maquina objetivo. La conexión de la víctima se cuelga y el atacante es capaz de comunicarse con la máquina host como si el atacante fuera la víctima. Para realizar este tipo de ataques, el atacante necesariamente debe estar en la misma red que la víctima. El blanco y la víctima pueden estar en cualquier otro lado.

# TCP/IP Hijacking Paso a paso

1. El atacante snifea la conexión de la víctima y utiliza la IP de la víctima para enviar paquetes spoofeados con la secuencia de número predicha.
2. El host procesa el paquete spoofeado, incrementa la secuencia del número y envía ACK a la dirección de la víctima.
3. La máquina de la víctima está inconsciente del paquete spoofeado, así que ignora el paquete ACK del equipo host y apaga el contador del número de secuencia.
4. Por tanto, el host recibe el paquete con la secuencia de número incorrecta.

# TCP/IP Hijacking Paso a paso

5. El atacante fuerza la conexión de la víctima con el equipo host a un estado desincronizado.
6. El atacante sigue la secuencia de número y continuamente spoofea paquetes que vienen desde la IP de la víctima.
7. El atacante continúa comunicándose con el equipo host mientras la conexión de la víctima se cuelga.

# IP Spoofing: Source Routed Packets

Es una técnica utilizada para obtener acceso no autorizado al equipo con la ayuda de un IP de un host de confianza. Cuando la sesión se establece, el hijacker inyecta el paquete falsificado antes de que el cliente responda. El paquete original es perdido cuando el servidor recibe el paquete con una secuencia distinta. La IP de destino puede ser especificada por el atacante.

# RST Hijacking

1. Consiste en inyectar un paquete authentic-looking reset (RST) utilizando una fuente spofeada y prediciendo el número ACK.
2. La víctima cree que la fuente está mandando el paquete RST y resetea la conexión.
3. Enciende la flag ACK en tcpdump para snifear paquetes.
4. RST Hijacking puede ser llevado a cabo utilizando una herramienta de elaboración de paquetes como Colasoft's Packet Builder y herramientas de análisis TCP/IP como tcpdump.

# Blind Hijacking

El acatante puede inyectar comandos o datos maliciosos dentro de las comunicaciones interceptadas en la sesión TCP incluso si la source-routing está deshabilitada.

El atacante puede enviar los datos o comentarios pero no tiene acceso para ver la respuesta.

# Ataque Man-in-the-Middle utilizando Packet Sniffer

En este ataque, el packet sniffer es utilizado como una interfaz entre el cliente y el servidor. Los paquetes entre el cliente y el servidor son enrutados a través del host hijacker utilizando dos técnicas.

Utilizando ICMP falso. Es una extensión IP que envía mensajes de error donde el atacante puede enviar mensajes para engañar al cliente y al servidor.

# Ataque Man-in-the-Middle utilizando Packet Sniffer

Utilizando ARP Spoofing. ARP es utilizado para mapear la IP local a la dirección MAC. El ARP Spoofing engaña al host difundiendo la solicitud ARP y almacenando el caché las tablas ARP enviando respuestas ARP falsas.

# UDP Hijacking

1. El atacante envía una respuesta de servidor falsa a la solicitud UDP del cliente antes de que el servidor la responda.
2. El atacante utiliza un ataque Man-in-the-Middle para interceptar la respuesta del servidor al cliente y enviar su propia respuesta falsa.

# Herramientas de sesión Hijacking

- Paros, es un proxy Man-in-the-Middle y un escáner de vulnerabilidades. Permite al atacante interceptar, modificar y depurar datos HTTP y HTTPS entre un servidor web y un navegador cliente.
- Burp Suite, permite al atacante inspeccionar y modificar tráfico entre el navegador y la aplicación objetivo. Analiza todo tipo de contenidos.
- Firesheep es una extensión de Firefox que permite robar un ID de sesión a un atacante para facebook.

# Contramedidas

- Utilizar SSL para crear un canal de comunicación seguro.
- Pasar las cookies de autenticación por una conexión HTTPS.
- Implementar la funcionalidad logout a los usuarios para finalizar sesiones.
- Generar un ID de sesión luego de iniciar sesión.
- Utilizar cadenas o números largos aleatorios como una clave de sesión.
- Pasar los datos encriptados entre los usuarios y los servidores web.

# Protección contra las sesiones Hijacking

- Utilizar encriptación.
- Utilizar protocolos seguros.
- Limitar las conexiones entrantes.
- Minimizar el acceso remoto.
- Educar a los empleados.
- Regenerar el ID de la sesión luego de iniciar sesión.

# Métodos para prevenir las sesiones Hijacking: Para ser seguidos por los desarrolladores Web.

- Reducir la duración de la vida de sesión de una cookie.
- Expirar las sesiones en cuanto el usuario cierra sesión.
- Regenerar la ID de sesión luego de un inicio de sesión correcto para prevenir ataque de fijación de sesión.
- Prevenir Eavesdropping entre la red.
- Cifrar los datos y la clave de sesión que fue transferida entre el usuario y los servidores Web.
- Crear claves de sesión con cadenas largas o números aleatorios para que sea difícil para el atacante adivinar una clave válida.

# Métodos para prevenir las sesiones Hijacking: Para ser seguidos por usuarios Web.

- No hacer clic en los vínculos que se reciben por correo o mensajería.
- Utilizar firewalls para prevenir contenido malicioso de toda la red.
- Utilizar firewalls y opciones de navegador para restringir las cookies.
- Asegurarse de que el sitio web está certificado por C.A.
- Asegurarse de que se limpia el historial, el contenido offline, y las cookies de su navegador luego de cada transacción sensible y confidencial.
- Preferir https, una transmisión segura para transmitir datos confidenciales y sensibles.
- Cerrar sesión del navegador haciendo clic en el botón logout en vez de cerrar directamente el navegador.

# Defensa contra ataques de sesión Hijacking

- Utilizar protocolos disponibles en la suite OpenSSH.
- Utilizar autenticación fuerte como Kerberos o VPNs punto a punto.
- Configurar reglas internas y externas spoof apropiadas en los gateways.
- Utilizar productos IDS o ARPwatch para monitorear ARP cache poisoning.

# Remediación de Sesión Hijacking

1. Defenderse a fondo es una clave importante de un plan de seguridad comprensible.
2. Defenderse a fondo es también un componente clave en la protección de la red de ataques de sesión hijacking.
3. Defenderse a fondo es definido como la práctica de utilización de sistemas o tecnologías de seguridad múltiple para prevenir intrusiones en la red.
4. La idea central detrás del concepto es que si una contramedida falla, hay niveles adicionales de protección para salvaguardar la red.

# IPSec

Es un conjunto de protocolos desarrollado por la IETF para soportar la el intercambio de paquetes en la capa IP de manera segura. Está desarrollada extensamente para implementar VPNs.

# Modos IPSec

- Modo Transporte
  - Autentifica dos equipos conectados.
  - Tiene una opción de cifrar la transferencia de datos.
  - Compatible con NAT.
- Modo Túnel
  - Encapsula paquetes para ser transferidos.
  - Tiene la opción de cifrar la transferencia de datos.
  - No es compatible con NAT.

# Arquitectura IPSec

El Protocolo AH trabaja con un algoritmo de autenticación (MD5 o SHA1). Es un protocolo de revisión de integridad.

El protocolo ESP trabaja con algoritmo de encriptación (DES o 3DES).

# Autenticación IPSec y confidencialidad

Utiliza dos distintos servicios de seguridad para la autenticación y confidencialidad

- Authentiction Header provee autenticación de datos para el que envía los datos.
- Encaptulation Security Payload (ESP) provee ambos, autenticación de datos y encriptación (confidencialidad) del que envía los datos.

# Componentes del IPSec

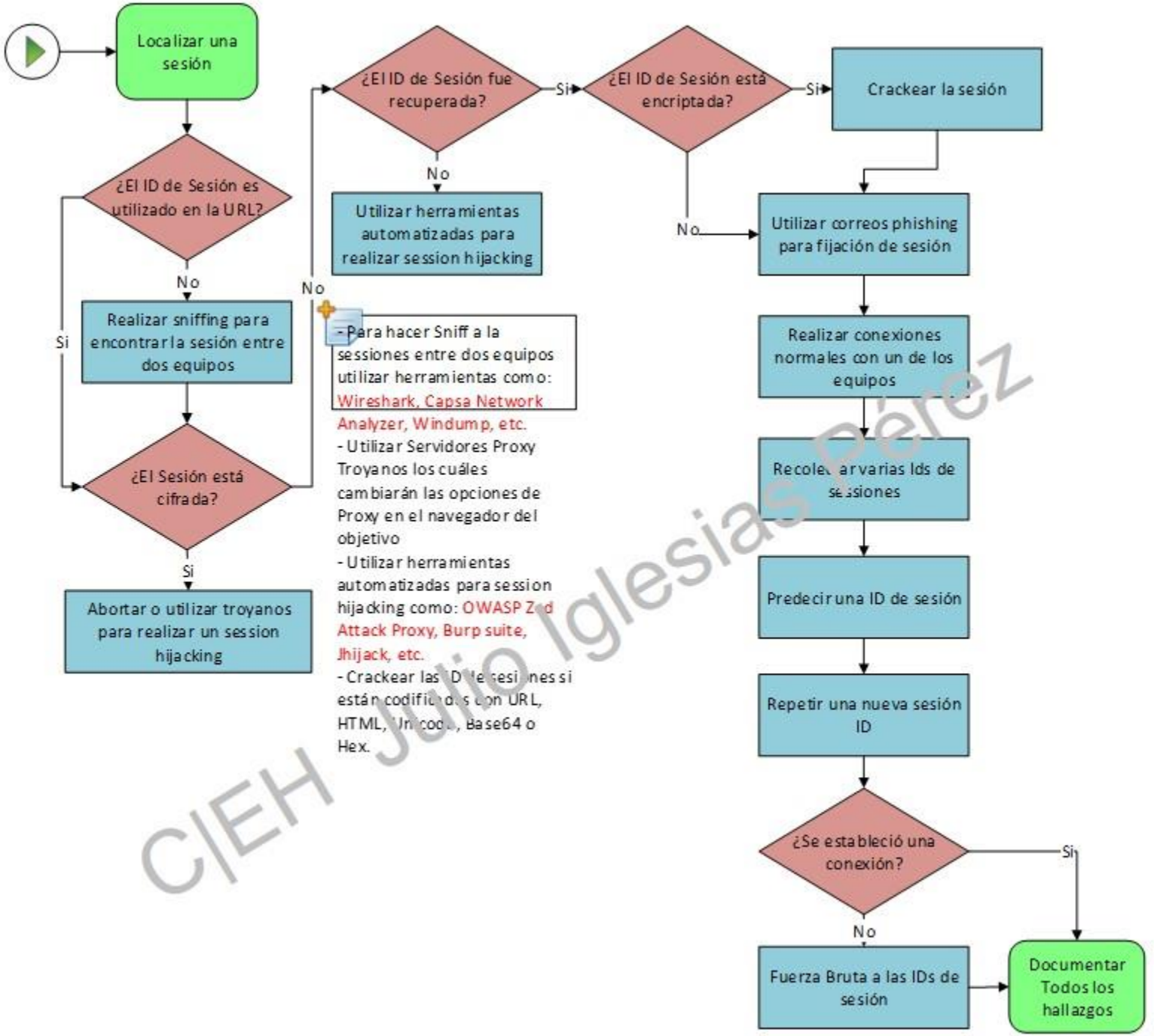
- IPSec Polivy Agent: Un servicio de Windows 2000 recolecta opciones de políticas de seguridad IPSec desde Active Directory y establece la configuración al sistema cuando inicia.
- Oakley: Un protocolo que utiliza el algoritmo Diffie-Hellman para crear una clave maestra, y una clave que es específica para cada sesión en la transferencia de datos IPSec.
-

# Componentes del IPSec

- - Internet Security Association Key Management Protocol: Un software que permite a dos equipos comunicarse encriptado los datos que son intercambiados entre ellos.
- - Internet Key Exchange (IKE): Protocolo IPSec que produce claves de seguridad para IPSec y otros protocolos.

**Nota.-** Se puede implementar IPSec por directivas de seguridad local en Windows.


Test de Intrusión para
Session Hijacking
C|EH
Julio




¡Muchas Gracias!
C|EH Julio Iglesias Perez