SECUESTRO DE SESIONES WEB

Rubén O. Nacho Paucara
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas de Información
Nacho5972653@gmail.com

RESUMEN

Un secuestro de sesiones se da cuando un atacante logra colocarse entre dos máquinas, y apoderarse de la sesión establecida entre ambas. Los atacantes pueden hacerse de nuestras cuentas capturando las contraseñas que viajan por el aire, tanto en texto plano como encriptados, la comunicación sucede en tiempos diferidos. De esta forma, el cliente envía una petición, el servidor la recibe y envía una respuesta con las cabeceras **HTTP**.

Los ordenadores no sólo sirven para procesar información almacenada en soportes físicos en cualquier formato digital, sino también como herramienta para acceder a información, a recursos y servicios prestados por ordenadores remotos, como sistema de publicación y difusión de la información

Palabras Clave

Sesión, Secuestro, wifi, Mozilla Firefox, Ataques, Ferret, Hamster,Fireshepp, Cookies

1. INTRODUCCIÓN

Las redes sociales han sido víctimas de diferentes ataques desde su creación. La suplantación de identidades es algo común, alguien puede darse de alta en una red social a nombre de otra persona. También es posible implementar un ataque de phishing, en el que el usuario entre a un sitio falso y proporcione sus datos de autenticación a otras personas.

Un *secuestro de sesión*es una técnica que consiste en interceptar una sesión iniciada entre dos equipos para secuestrarla. Como la comprobación de autentificación se hace sólo al abrir la sesión, un pirata que inicie su ataque con éxito puede controlar la conexión durante toda la sesión.

Esta modalidad no se trata estrictamente de un secuestro, ya que no implica una restricción a la libertad ambulatoria. Consiste en el engaño dirigido a los familiares o allegados de una presunta víctima, para lograr de ellos una disposición patrimonial, haciéndoles creer falsamente que ésta se encuentra privada de su libertad.

La inadecuada gestión de sesiones en aplicaciones web empresariales se ha convertido en la terceravulnerabilidad en aplicaciones web. El impacto de explotar esta vulnerabilidad es crítico debido a la exposición de informaciónrestringida para el negocio.

2. FUNCIONAMIENTO DEL SECUESTRO DE SESIONES

Cuando se inicia una sesión, se genera una “cookie” en el navegador del usuario entregada por el servidor. En cada petición hecha por el usuario, se incluye la cookie para que el servidor sepa que este ya ha iniciado la sesión.

Aunque no se ingrese las credenciales sobre una red pública o privada pero de baja seguridad, un atacante sigue siendo capaz de capturar el tráfico de red y ver las cookies de sesión. El hecho es que, quien posea esa información, posee una cuenta mientras la sesión exista, mientras no se cierre la sesión actual, la cookie capturada por nuestro atacante, sigue siendo útil.

El atacante encuentra un mecanismopara averiguar el identificador de *SESIÓN* y realizar el secuestro de la sesión del usuario.

El usuario (la víctima) no se entera que su sesión de aplicación web ha sido vulnerada.

Existe un botón que aparece abajo de los checkbox donde se ingresa las credenciales al inicio de sesión que dice “No cerrar sesión”. Este checkbox implica que, aunque cerremos nuestro navegador, las cookies van a seguir estando en memoria de la maquina hasta que ***MANUALMENTE*** se cierre la sesión.

3. HERRAMIENTAS PARA REALIZAR EL SECUESTRO DE SESIÓN

- Ferret, es una herramienta que captura toda la información hecha disponible por los equipos conectados a una red wifi. Esta herramienta genera un archivo de log llamado hamster.txt en el que va almacenando toda la información obtenida de la red, algo similar a lo que se podría hacer de forma manual con Etercap o Dsniff.

- Hamster, se trata de un servidor proxy que trabaja sobre el archivo hamster.txt generado por Ferret. Para acceder a él es recomendable utilizar otro navegador, o bien otro

perfil de usuario si utilizamos firefox, y configurar el puerto servido por Hamster como proxy.

- Fireshepp, coge el identificador de sesión y permite ingresar a la aplicación de manera más fácil y sencilla, utiliza Plugin de Mozilla Firefox, automatiza de manera muy rápida el robo de sesiones, a la fecha el plugin está descontinuado.

- Greasemonkey, utiliza Plugin de Mozilla Firefox, permite ingresar la cookie capturada mediante MITM.

4. MÉTODOS DE ATAQUE

- Ataque a ciegas, si se deshabilita el enrutamiento de origen, que es lo que sucede actualmente con la mayoría de los equipos, un segundo método consiste en enviar paquetes como "ataques a ciegas", sin recibir repuesta, tratando de predecir una secuencia numérica.

- Ataque MitM es cuando un pirata está en la misma programación de red que sus dos contactos, puede supervisar la red y "silenciar" a uno de los participantes al irrumpir en su equipo o al congestionar la red para tomar su lugar.

5. CONCLUSIÓN

Tener en cuenta que navegar en redes públicas pone en riesgo nuestra privacidad de la información. Utilizar siempre firewalls para publicar la mínima información, y cerrar siempre las sesiones al finalizar la conexión al sitio al que accedemos. Utilizar las herramientas como el HTTP, conexiones VPN para evitar el secuestro de sesión cuando ingresamos a alguna red social.

6. REFERENCIAS

[28] Gomez R. Secuestro de sesiones web. 2010. [Disponible en:]. http://www.bsecure.com.mx/opinion/arearestringida/secuestro-de-sesiones-web/. [Fecha de búsqueda:] 14/04/13

[29] Ogawa G. Session Hijacking. [Disponible en:].http://www.mkit.com.ar/blog/tag/secuestro-de-sesion/. [Fecha de búsqueda:] 25/04/13

[30] Secuestro de sesión. 2013. [Disponible en:]. http://es.kioskea.net/contents/42-secuestro-de-sesion-tcp. [Fecha de búsqueda:] 27/04/13

Secuestro de sesiones de aplicaciones web – Session Hijacking. 2012. [Disponible en:].http://www.el-palomo.com/2012/04/secuestro-de-sesiones-de-aplicaciones-web-session-hijacking/. [Fecha de búsqueda:] 27/04/13