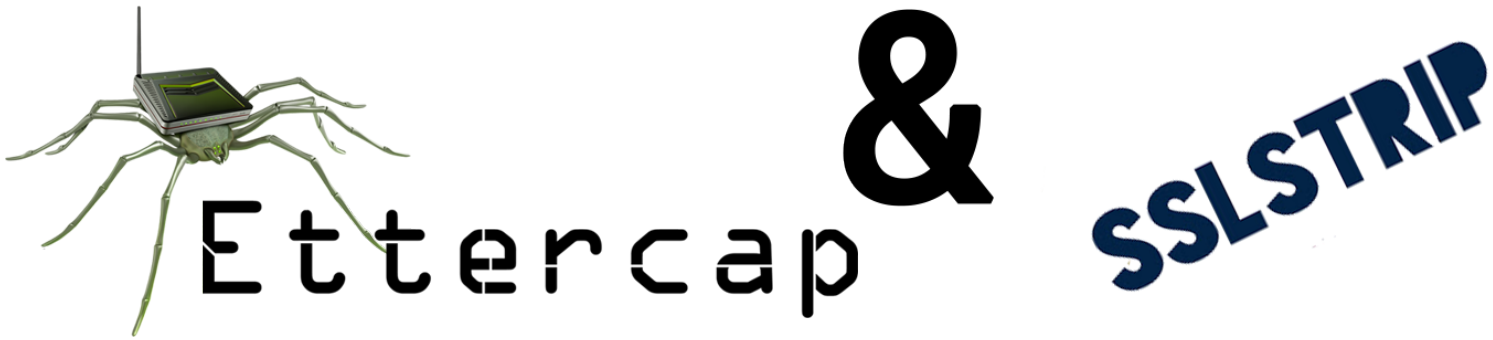
Ettercap y SSLStrip

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia

Vulnerabilidades en redes

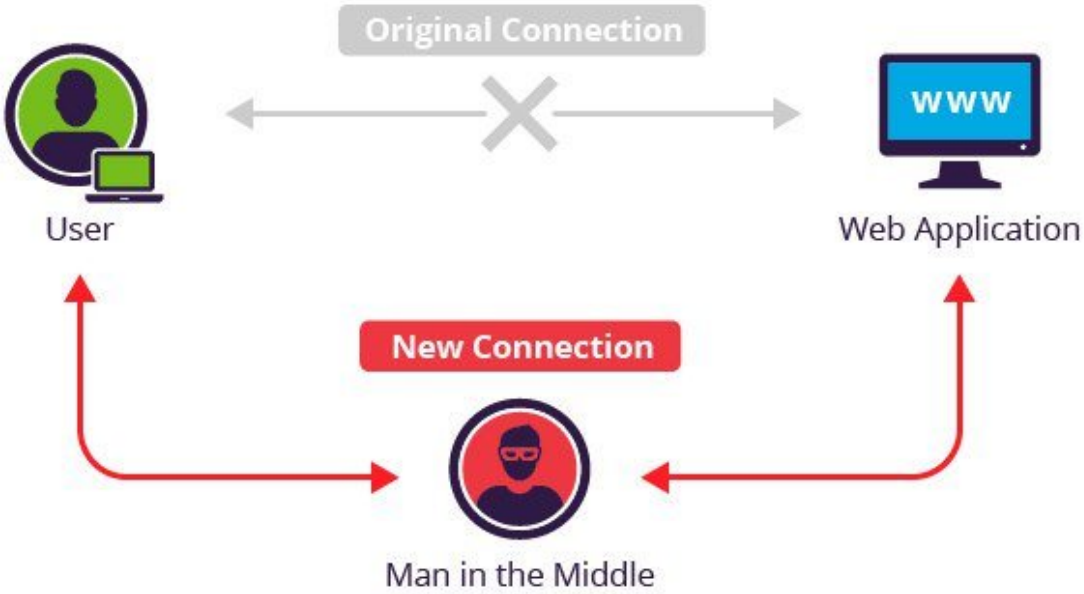


Índice

Man-in-the-Middle

Definición

Es un ataque donde el atacante puede leer, insertar y modificar los datos recibidos de una víctima a voluntad. Dicho atacante se coloca entre el emisor original del mensaje y el receptor original del mismo sin que ninguno de ellos sepa de la existencia del atacante. Debido a esto, ninguna de las partes sabe que el mensaje enviado/recibido ha sido violado por el atacante.



¿Qué es Ettercap?

Definición

Es un sniffer para redes LAN que permite la lectura, inyección y modificación de datos en una conexión establecida gracias a un ataque "Man-in-the-middle".

¿Cómo funciona Ettercap?

Funcionamiento

Para el ejemplo en el que nos vamos a centrar, simplemente usaremos un ataque "Man-in-the-middle" para la lectura de las credenciales de usuario en una página web con protocolo HTTP debido a que las páginas que usan HTTPS tienen un cifrado de credenciales y no podemos acceder a dichas credenciales de usuario.

Ejemplo práctico con Ettercap

Requisitos

- Una red.
- Un host usuario.
- Un host atacante.
- Ettercap.

¿Qué es SSLStrip?

Definición

Es una aplicación capaz de descifrar el tráfico HTTPS que viaja a través de una red dejándolo visible en "texto plano".

¿Cómo funciona SSLStrip?

Funcionamiento

SSLStrip no descifra el protocolo HTTPS. Su función es engañar al servidor y convertir todo el mensaje HTTPS cifrado de una web en un mensaje HTTP (sin cifrar). Esto solo funciona cuando la víctima llega la página web mediante una redirección o un link.

Ejemplo práctico con SSLStrip

Requisitos

- Una red.
- Un host usuario.
- Un host atacante.
- Ettercap.
- Script SSLStrip.

¿Qué ha pasado?

Resultado del ataque

Parece ser que el ataque no ha funcionado sin motivo alguno.

¿Por qué?

Debido a que los navegadores hoy día disponen de una contramedida a los sslstrip llamada HSTS.

¿Qué es HSTS?

Definición

Es un protocolo de seguridad que deniega las conexiones HTTP y solo posibilita las comunicaciones HTTPS entre el cliente y el servidor.

¿Cómo funciona?

Para poder activar esta utilidad, el usuario debe ser capaz de haber establecido una conexión al menos una vez de forma exitosa con dicha web.