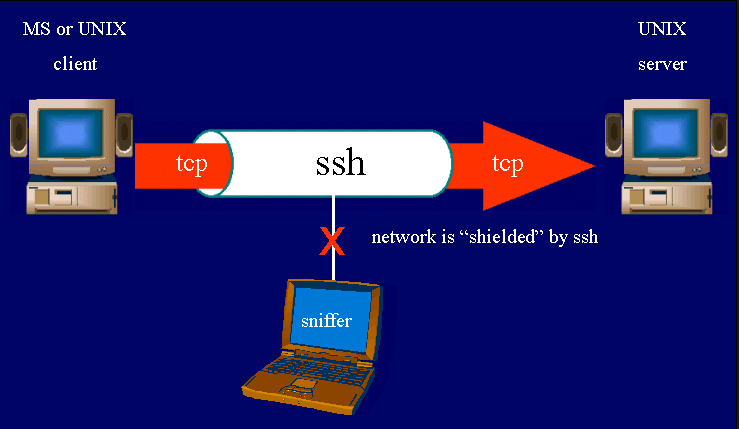
SSH

SSH (Secure Shell) es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas.

El protocolo SSH proporciona los siguientes tipos de protección:

* Después de la conexión inicial, el cliente puede verificar que se está conectando al mismo servidor al que se conectó anteriormente.
* El cliente transmite su información de autentificación al servidor usando una encriptación.
* Todos los datos enviados y recibidos durante la sesión se transfieren por medio de encriptación, lo cual los hacen extremamente difícil de descifrar y leer.
* El cliente tiene la posibilidad de reenviar aplicaciones gráficas desde el servidor. Esta técnica proporciona un medio seguro para usar aplicaciones gráficas sobre una red.



SSH reduce considerablemente la amenaza de una intercepción de la comunicación entre dos sistemas. También se reduce la amenaza de personificación de un determinado host; esto se produce cuando un sistema interceptor finge ser el receptor a quien está destinado un mensaje. Ambas amenazas son combatidas por el protocolo SSH debido a que cliente y servidor usan firmas digitales pare verificar su identidad y, adicionalmente, toda la comunicación entre los sistemas cliente y servidor es encriptada.