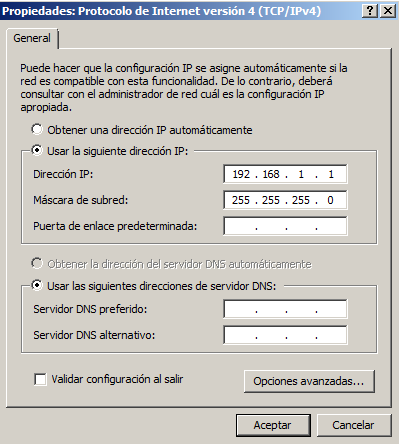
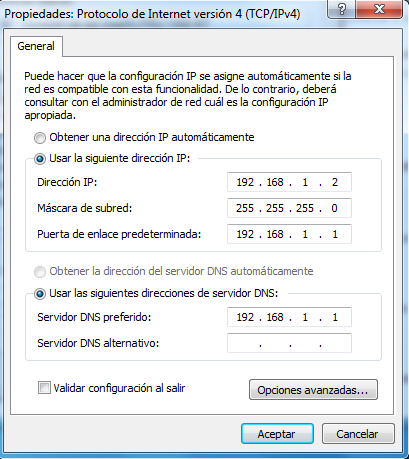
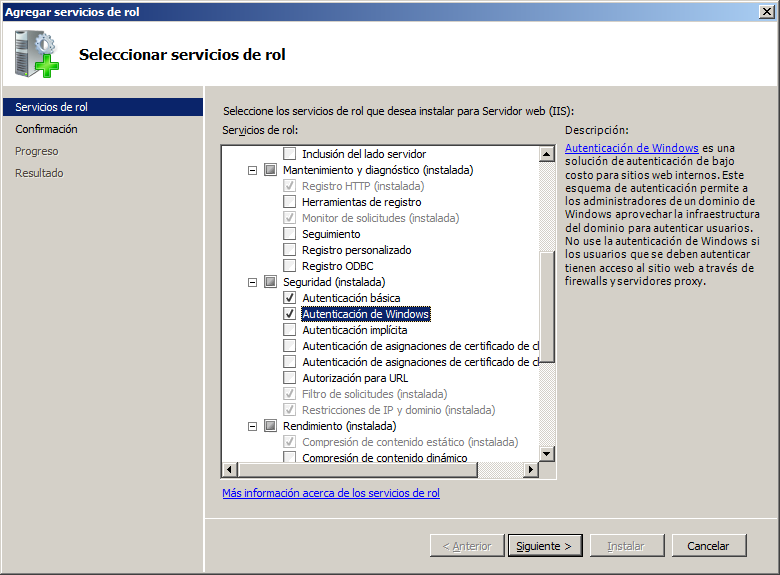
1. Configuración de red.

Servidor Cliente



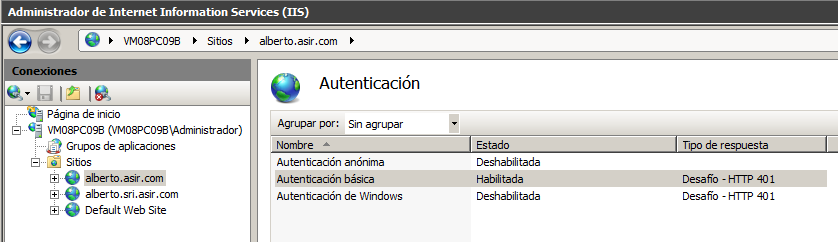
1. Configuración.

Instalamos los servicios de rol de autenticación de Windows y la básica para comprobar su funcionamiento a la hora de acceder a una página web.

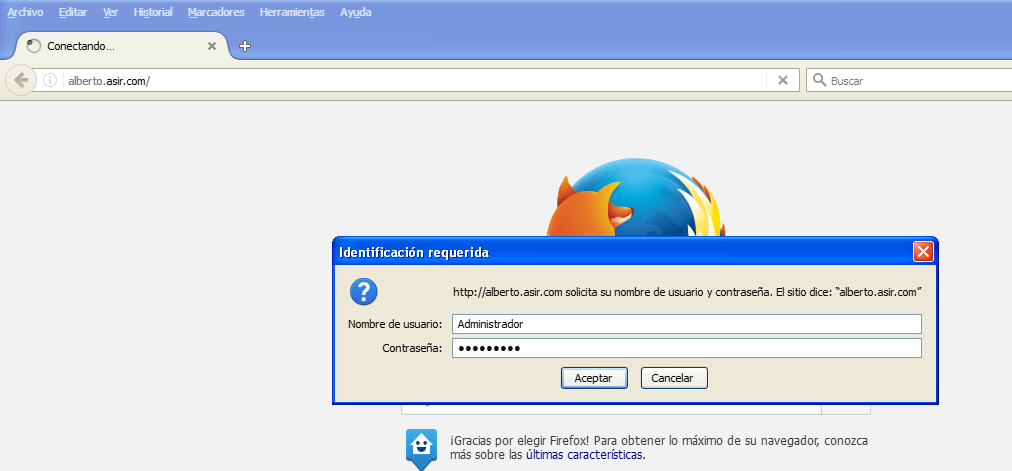


1. Básica.

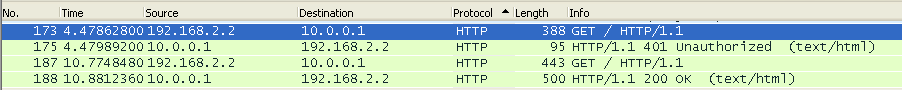
Configuramos para la web Alberto.asir.com la autenticación básica y deshabilitamos la autenticación anónima que viene configurada por defecto.



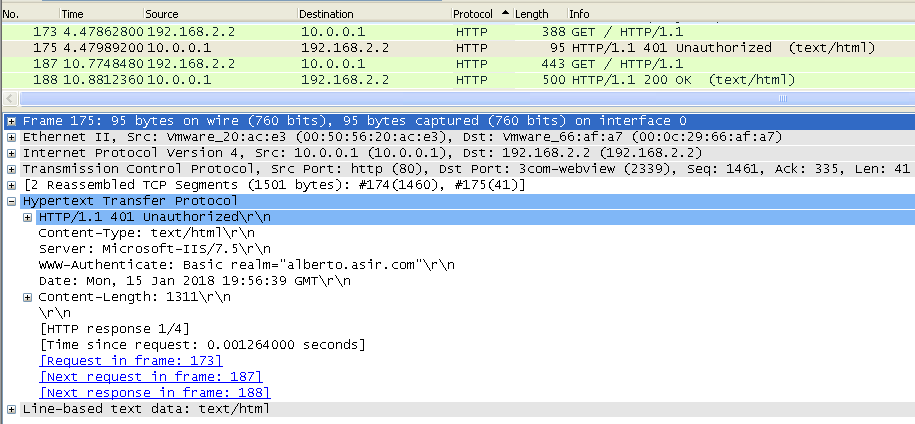
Como podemos comprobar en la imagen al acceder desde un cliente a la web nos solicita un usuario y contraseña, para lo cual ingresamos el usuario y contraseña del servidor.



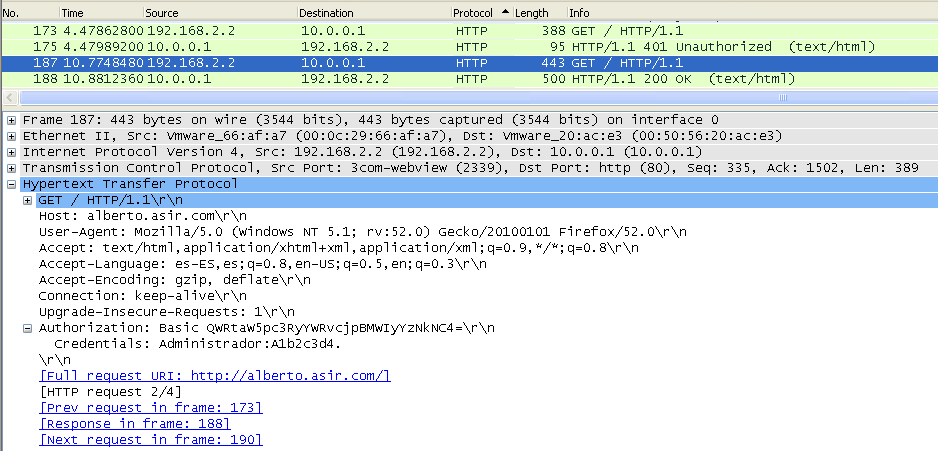
Ahora vamos a visualizar los paquetes que se intercambian entre el cliente y el servidor. Como se ve en la imagen el cliente solicita la web, a lo que el servidor le contesta con un 401 que no esta autorizado el acceso y le solicita usuario y contraseña, en el siguiente get el cliente envia los datos y después el servidor le da el 200 ok de acceso.



Como podemos observar, al desplegar las diferentes capas del paquete que envía el servidor al cliente, le envía un 401 de no autorizado y le comunica que la web tiene habilitada la autenticación básica.

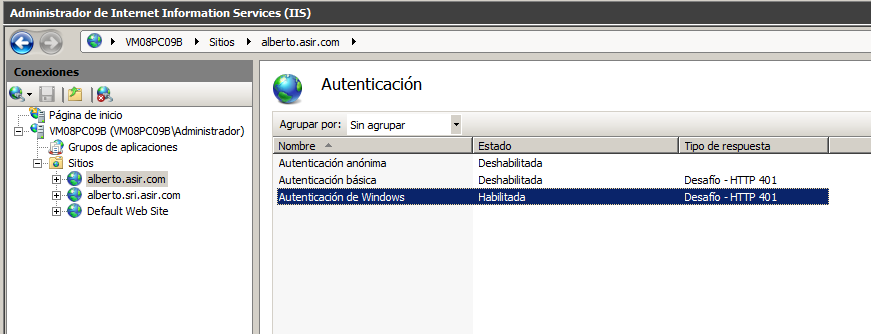


El siguiente paquete observamos como el cliente envía los datos de usuario y contraseña al servidor para validar el acceso a la web.

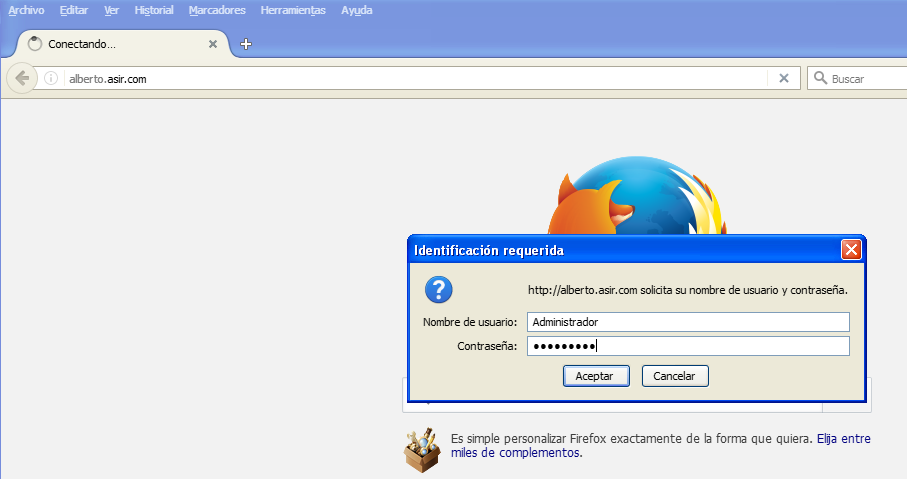


1. Windows.

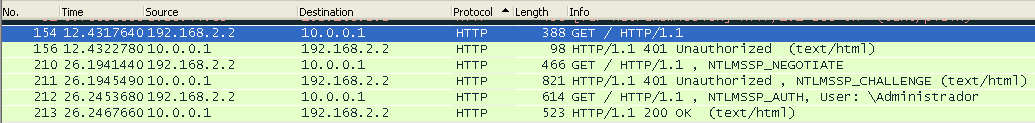
Ahora habilitamos para la misma página la autenticación de Windows y deshabilitamos la autenticación básica.



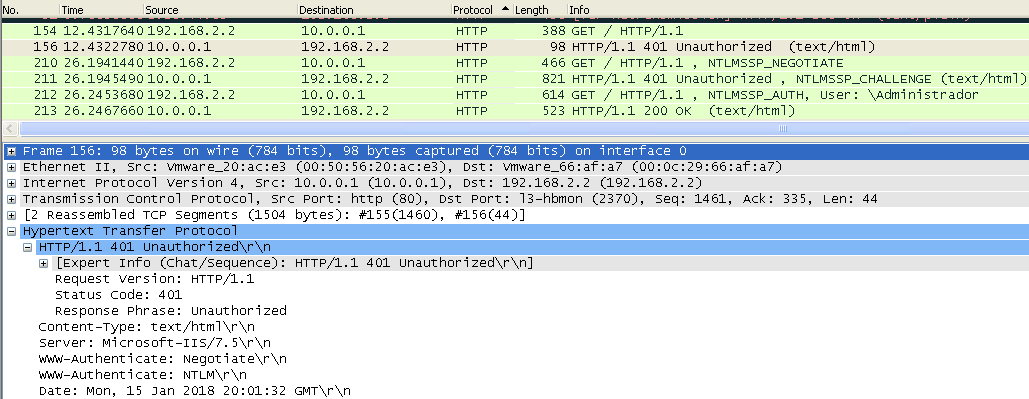
Como podemos observar en esta ocasión nos vuelve a solicitar el usuario y la contraseña para poder acceder.



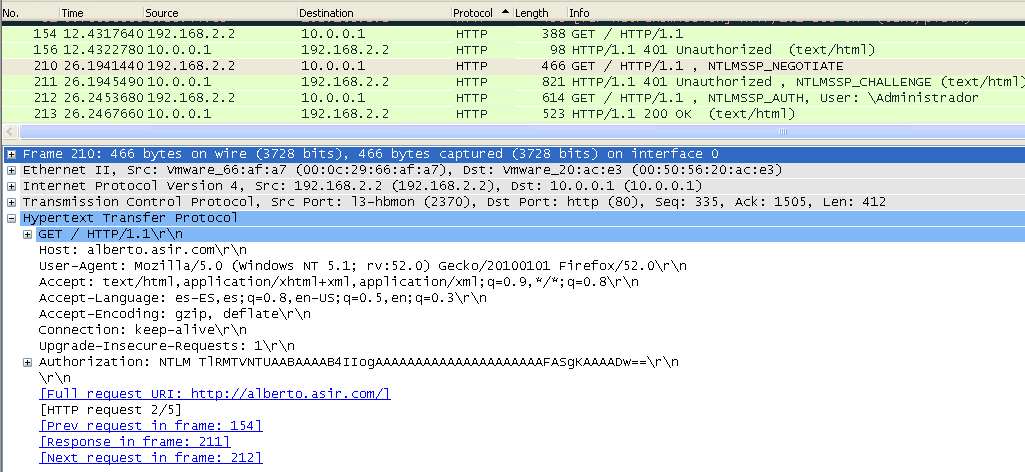
Volvemso al whiresark y vemos que en esta ocasión el servidor y el cliente intercambian 6 paquetes hasta que el servidor envia la web.



Como podemos ver el servidor envía un primer paquete indicando que no está autorizado el acceso a la web con un 401.



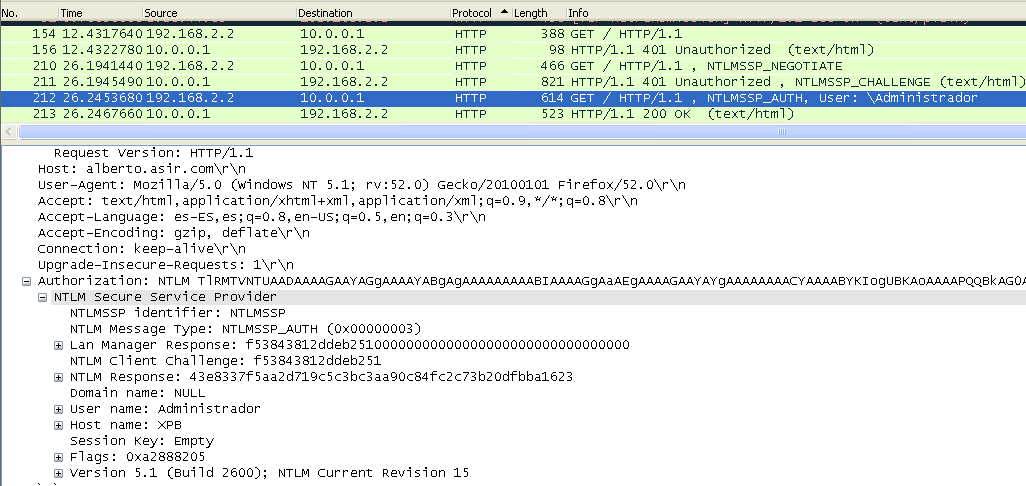
En el siguiente paquete el cliente le envía una petición para negociar el acceso a la web.



El servidor le responde con el modo de negociación necesario para que pueda acceder a la web.

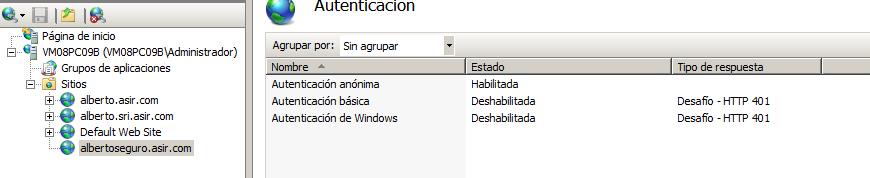


Por último el cliente le envía el nombre de usuario y la contraseña encriptada al servidor para validarse en la web y que el servidor le responda con un 200 ok y le sirva dicha web.

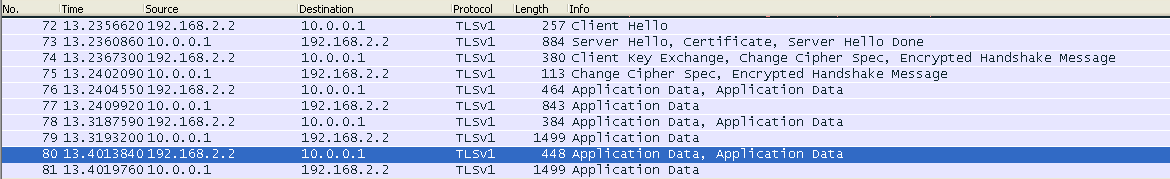


1. Anónima en https.

Configuramos la autenticación anónima para una web segura.



Al realizar el acceso a la web vemos los paquetes que intercambian entre el cliente y el servidor. Vemos los saludos y el envió de los certificados autoafirmados que tenemos en la web.



El último paquete debemos intuir que llevara el nombre de usuario y la contraseña de autorización que tiene el documento para poder validarse en la web. No se puede saber con certeza cuál de los paquetes que envía el servidor es dado que envía todos los datos encriptados.

