WIRESHARK

SAD

2ºASIR
I.E.S. ANTONIO MACHADO
ANA OROZCO ASENSIO

Contenido

Introducción.

En esta práctica vamos a usar Wireshark para monitorear la red usando Wordpress con MySQL y Apache con PHP.

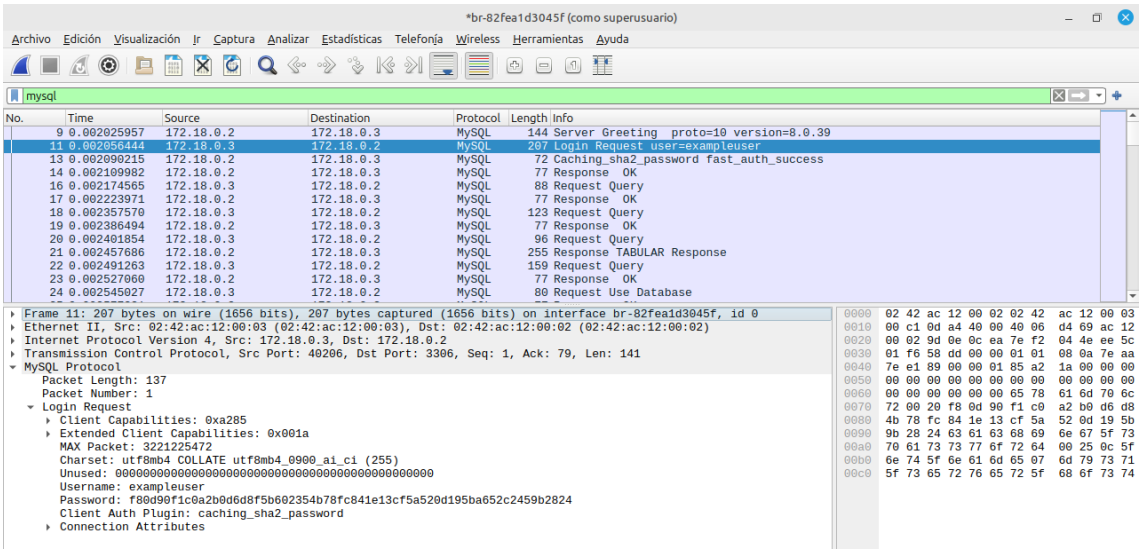
Comprobaremos lo que podemos ver al buscar en los paquetes que monitoreamos y buscaremos la contrseña y usuario de Wordpress.

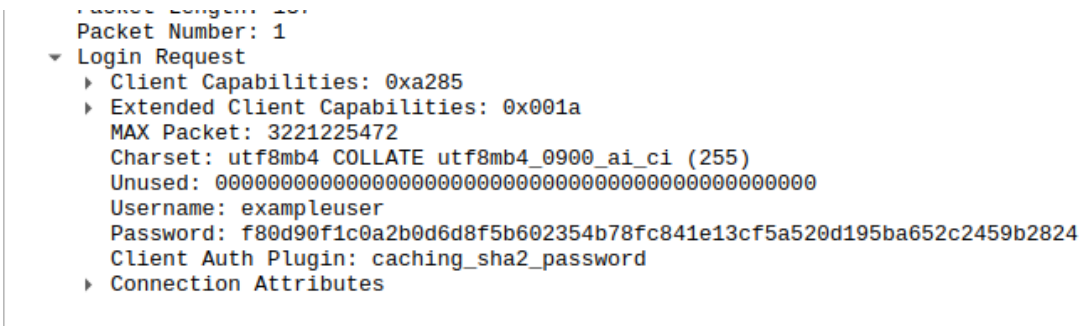
Monitoreo.

Voy a dividir en 2 este monitoreo.

MySQL

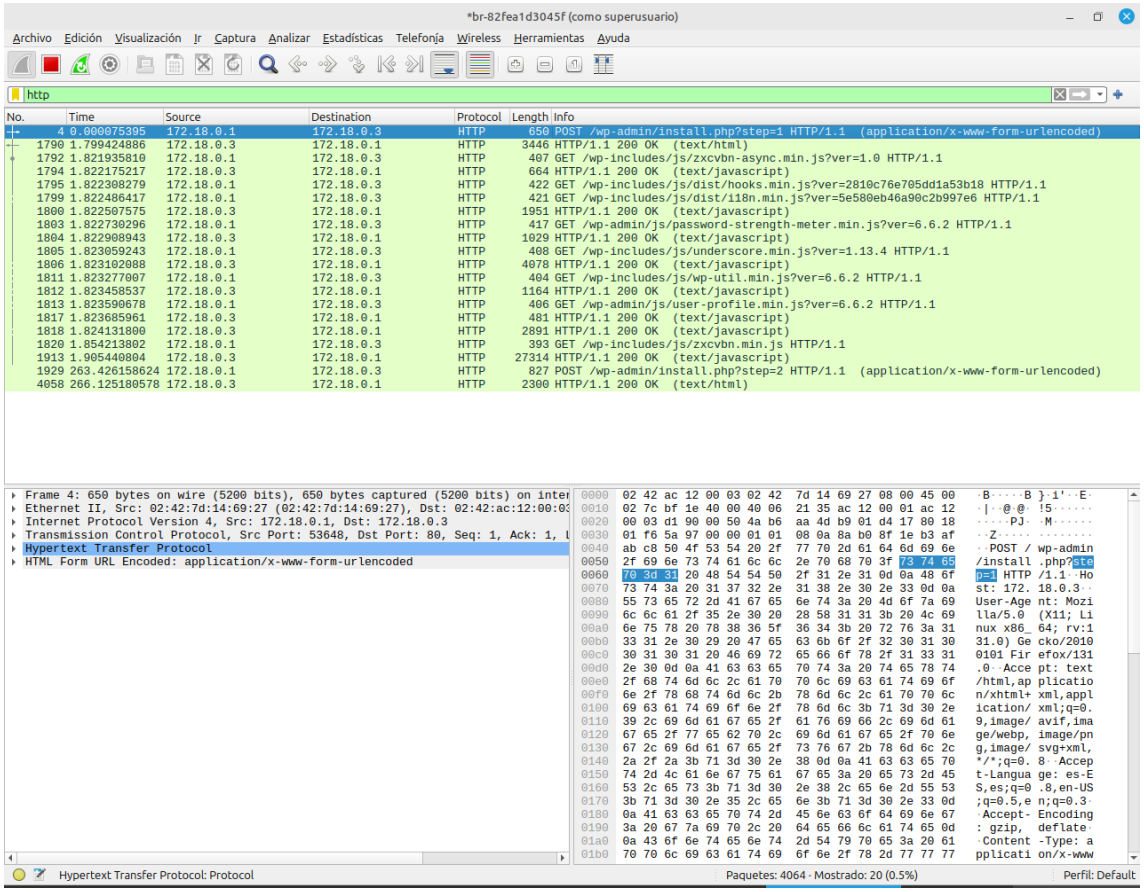
En esta captura podemos ver el trafico de la red filtrando con el protocolo MySQL, al entrar en los login resquest podemos ver que la contraseña está cifrada, por lo que de estos paquetes podemos sacar poca información.





HTTP.

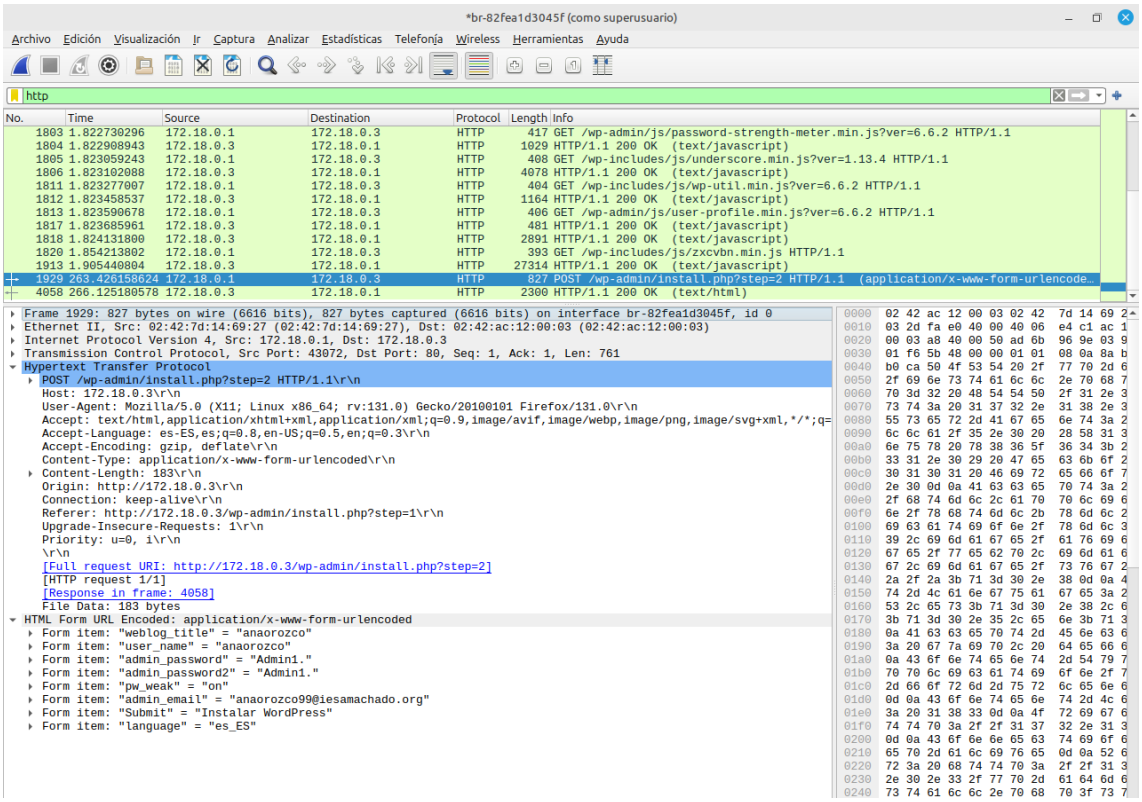
Con el protocolo HTTP vemos varios tipos de paquetes como GET que solicita los recursos al servidor o POST que envía datos al servidor (se suele usar para los formularios)



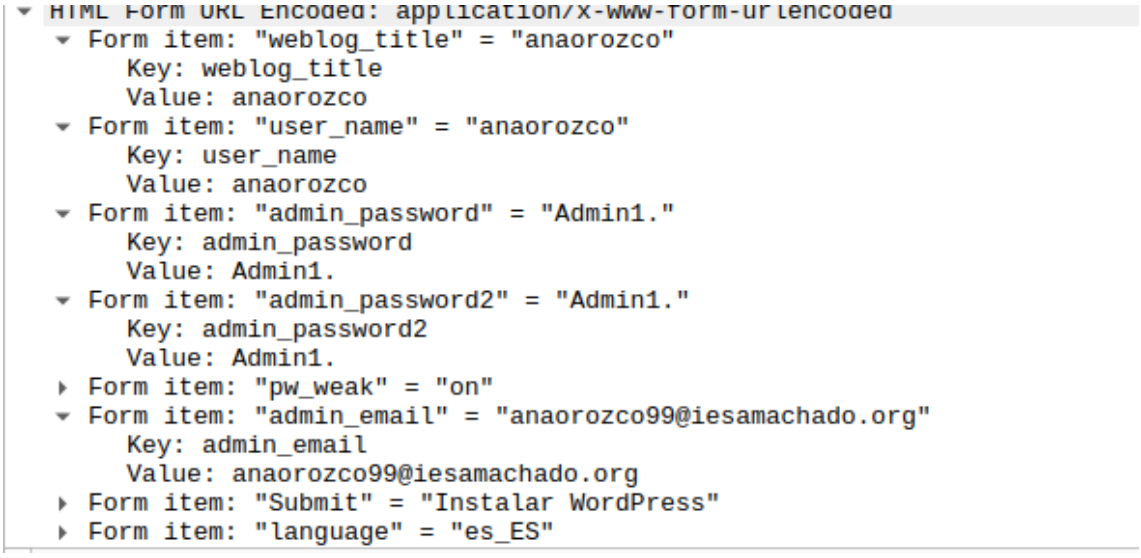
En esta captura vemos que solo tenemos códigos del estado del HTTP como 200 OK que significa que la solicitud se ha procesado correctamente, también tenemos el 500 Internal Server Error que dice que ha ocurrido un error en el servidor y el famoso 404 Not Found, que lo que nos dice es que no se encuentra el recurso que hemos solicitado. Además de estos hay más errores pero esto son los más comunes.

Seguimos buscando podemos encontrar información como el navegador que se utiliza en el tipo POST, el sistema operativo e incluso el idioma.

En los paquetes GET suele estar la información de la versión de HTTP utilizada, la url del recurso, la versión del PHP, el tipo de contenido, etc.



Además, podemos ver el usuario y la contraseña usados en el formulario de creación, por lo que no hay cifrado y por lo tanto no es seguro.



Conclusión

Después de esta práctica me he dado cuenta de por qué no es seguro el protocolo HTTP y deberíamos usar el HTTPS (aunque no todo el contenido de HTTPS está cifrado).

La diferencia que veríamos en wireshark sería que al hacer el monitoreo veríamos los paquetes, pero estos tendrían la información encriptada y autenticada