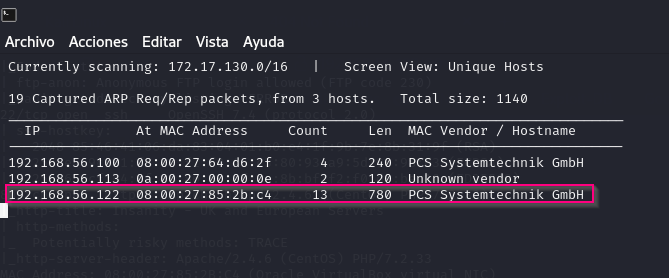
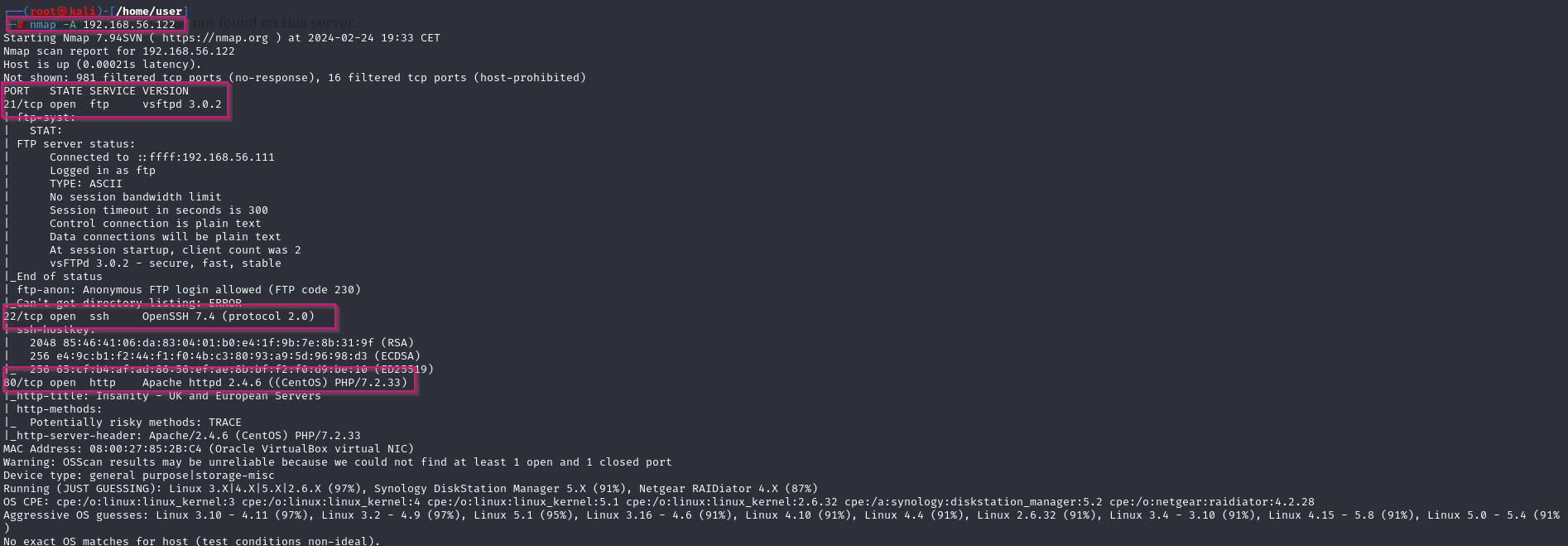
# **Insanity: 1 Vulnhub Walkthrough**

Primero haremos un netdiscorver para saber la Ip de nuestra máquina Objetivo:

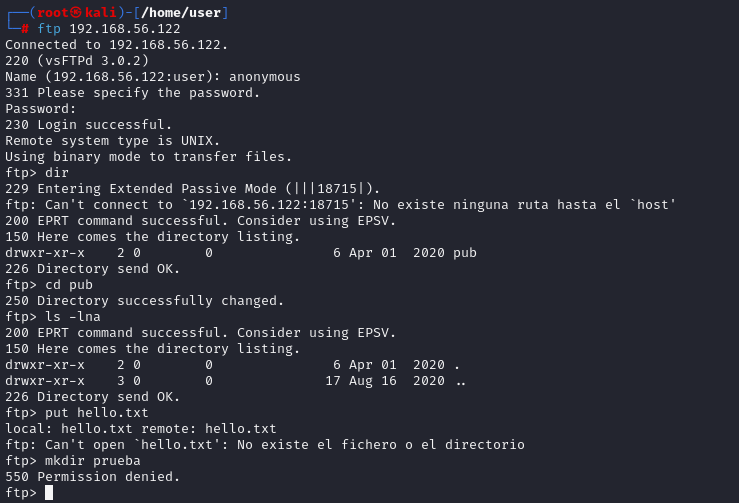
IP: 192.168.56.122



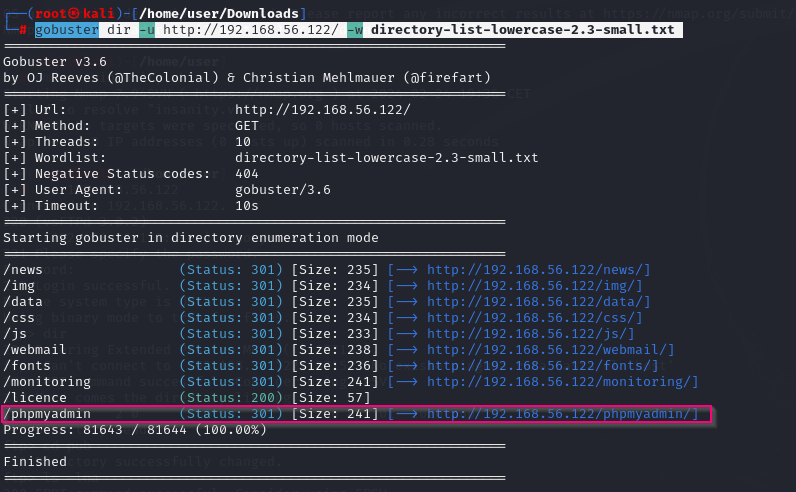
NMAP para ver los puertos:



Entramos por el Servidor FTP: y nos da permiso denegado al crear una carpeta

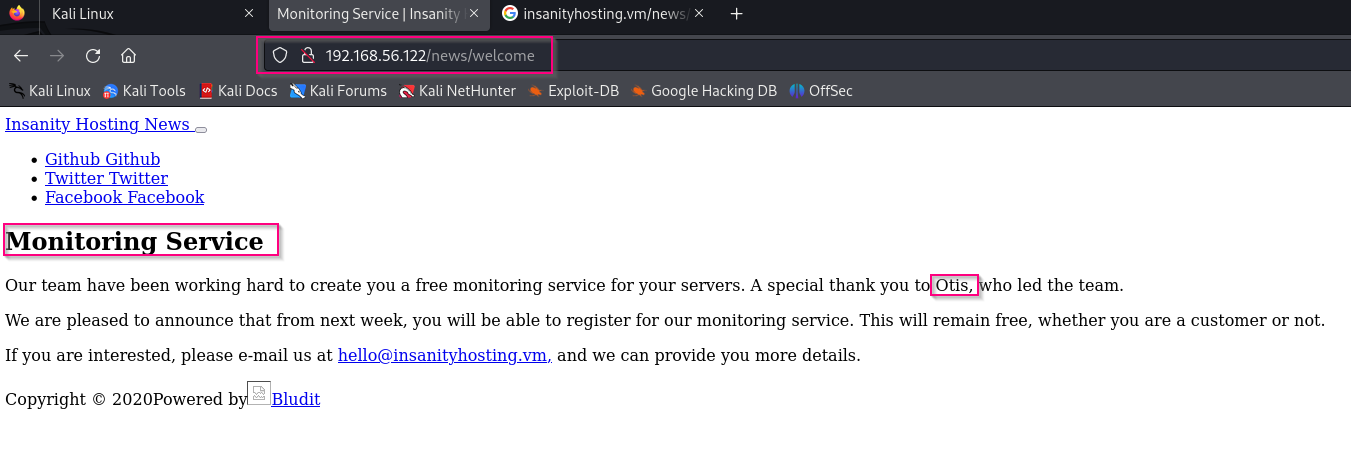


Con un comando llamado: **gobuster dir -u http://192.168.56.122/ -w directory-list-lowercase-2.3-small.txt** Podemos ver una enumeración de la página web:

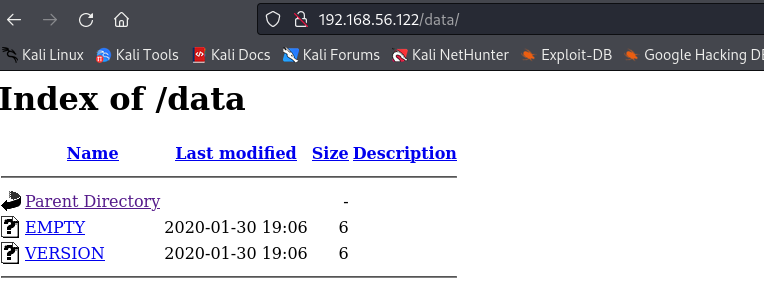


/news

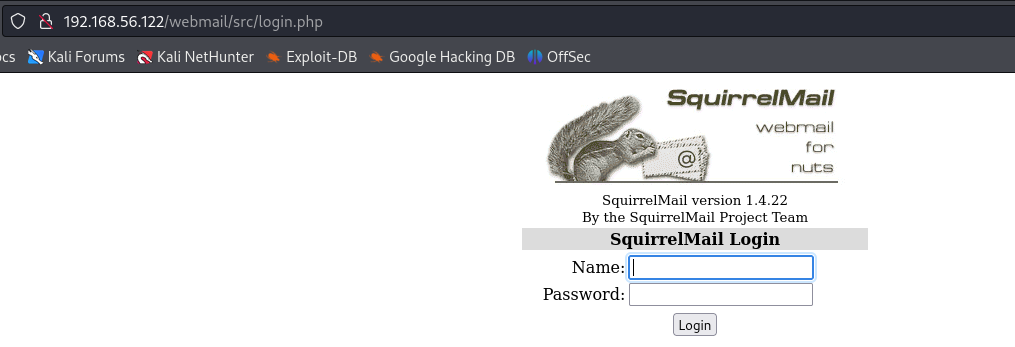
**Obtenemos un nombre.**



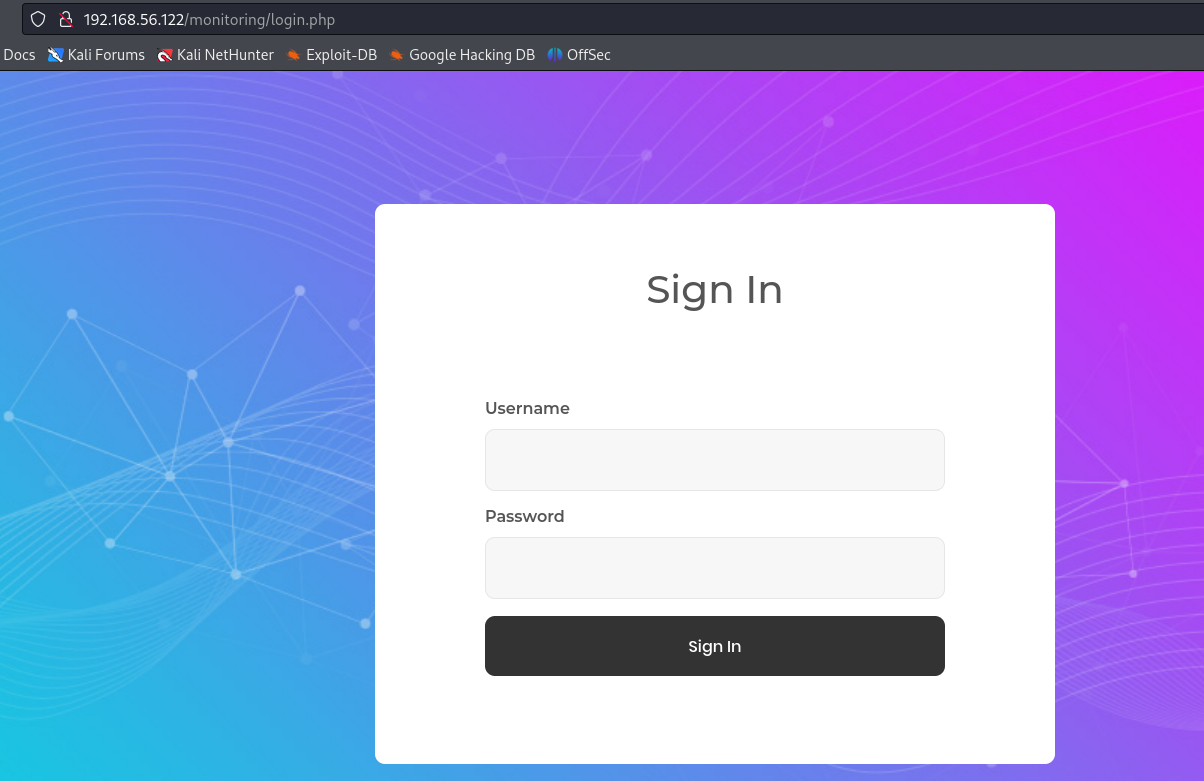
/data:



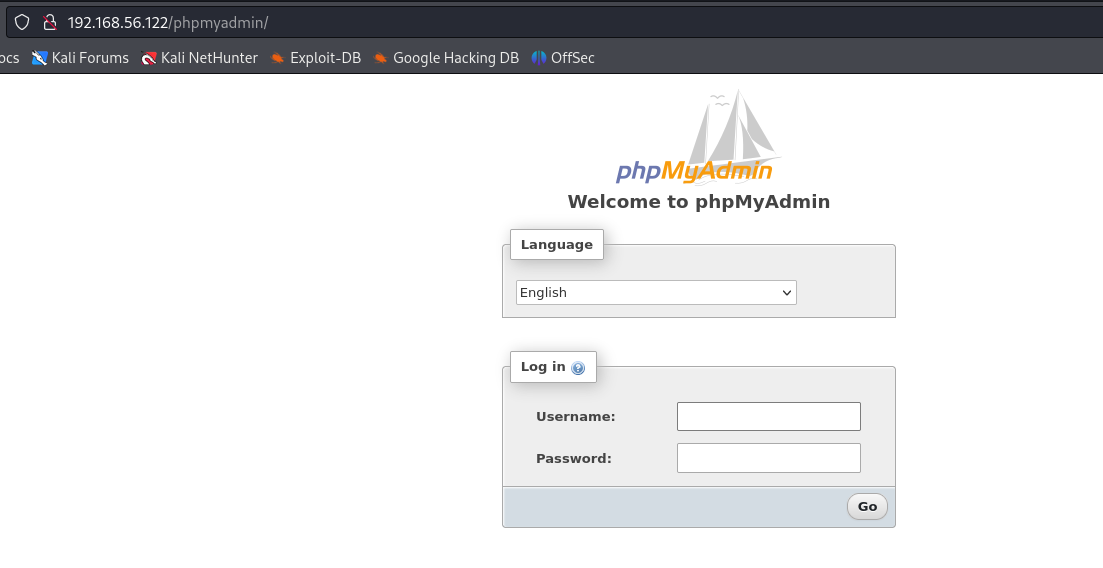
/webmail:



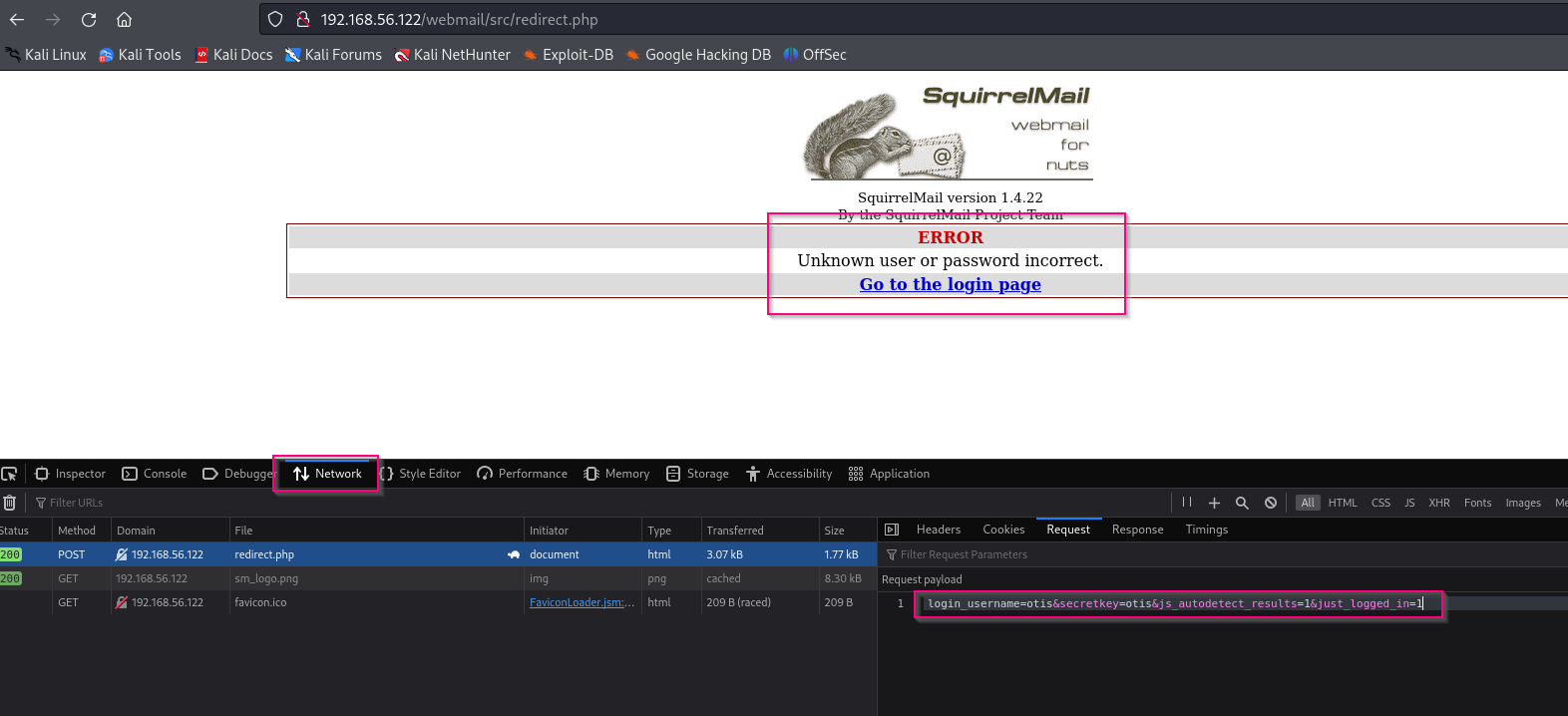
/monitoring:



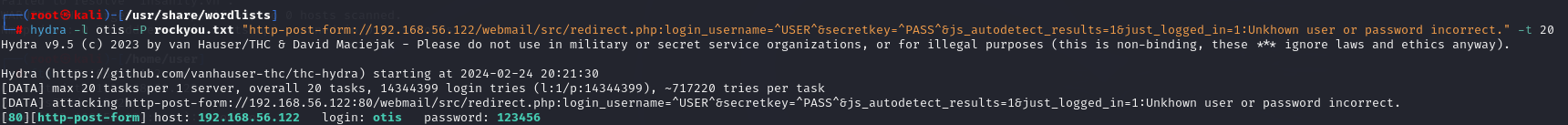
/Phpmyadmin:

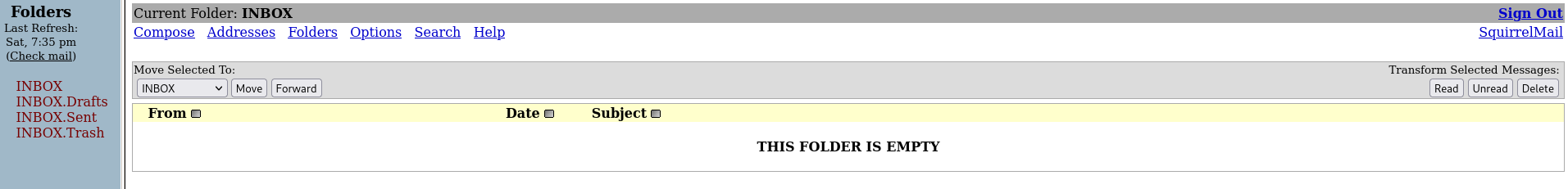


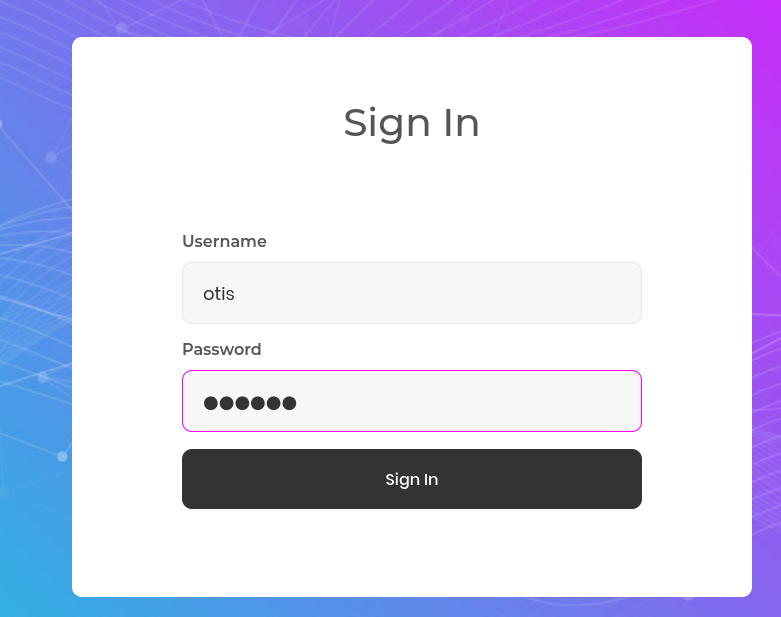
Nos iríamos por ejemplo a la página de webmail y haríamos una fuerza bruta con el usuario Otis, le damos a F12:

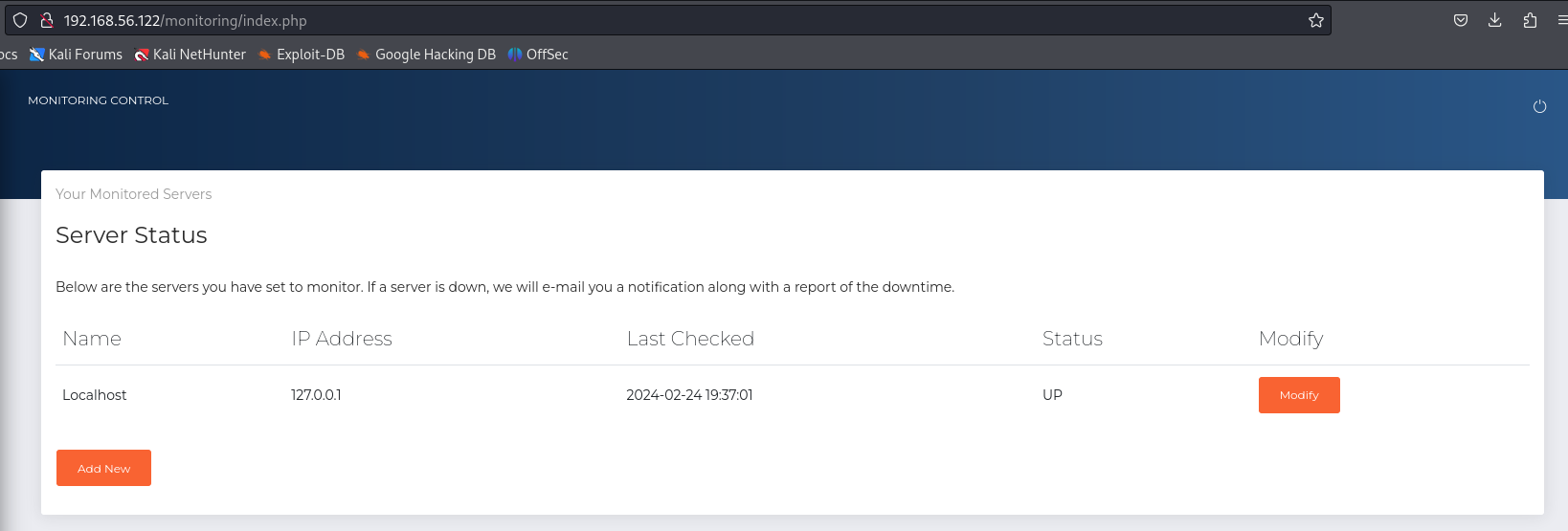


Nos da un error y nos tenemos que fijar en el Request, con esta respuesta nos vamos al comando de hydra: nos da la contraseña 123456

Y podemos entrar al email con Otis:

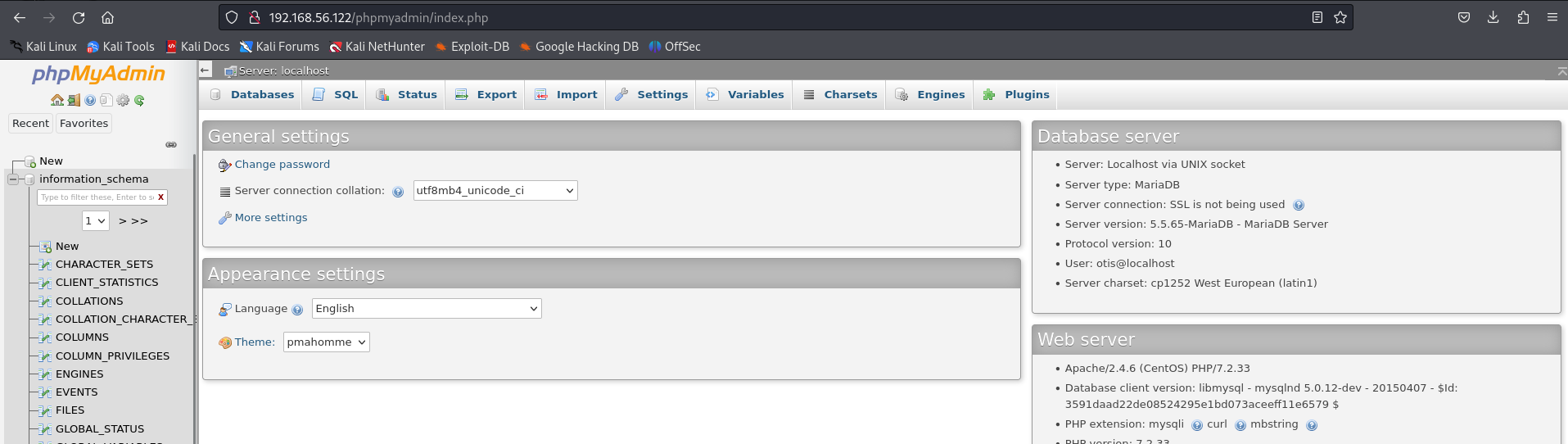
Tambien funciona en el apartado de /monitoring:



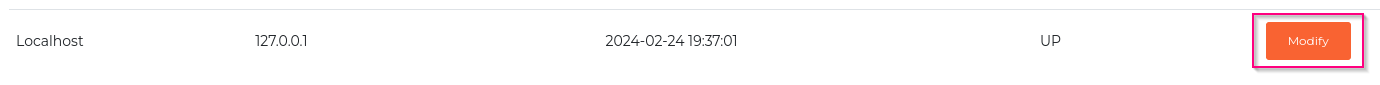


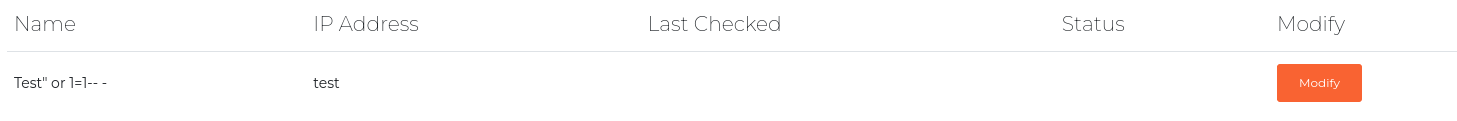
En /phpmyadmin podemos entrar solo con el username=Otis:

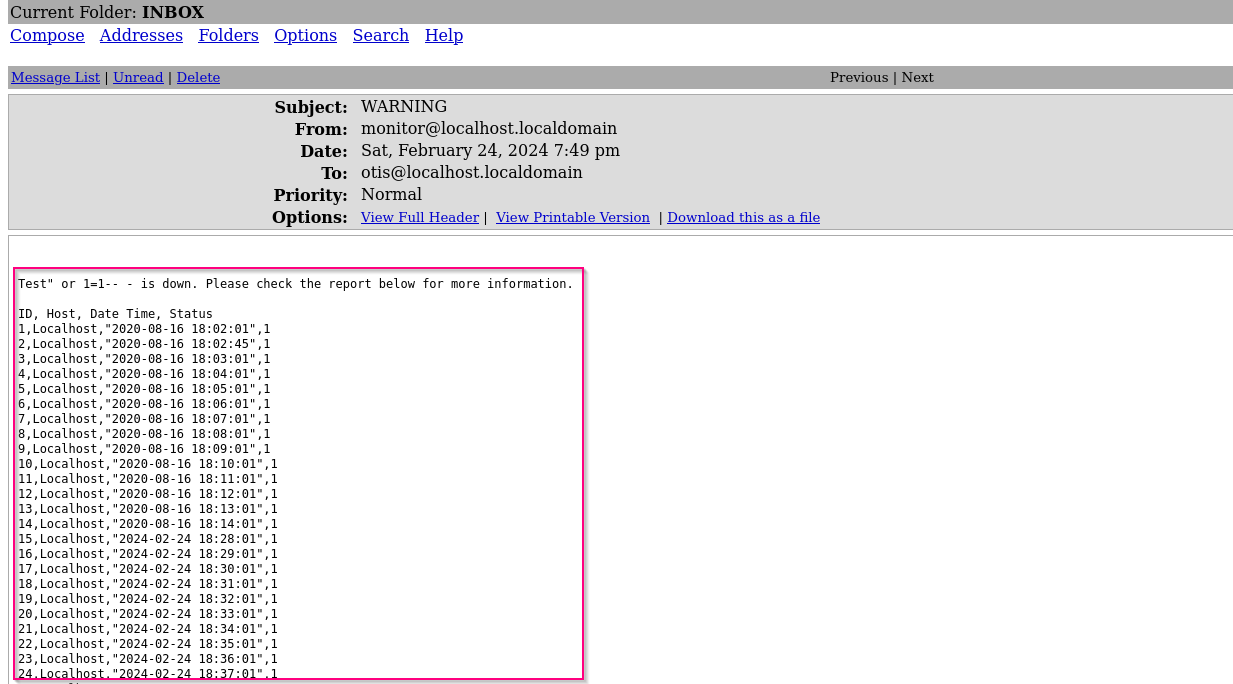




Vamos a irnos a la parte de monitoring y vamos a probar la inyección sql modificando el que ya está y ver si nos envía un email con el error:

Quedaria así: Test” or 1=1-- -

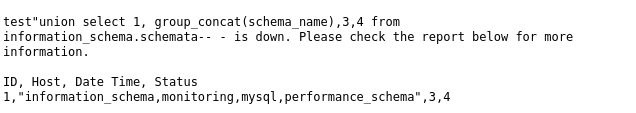
Nos sale lo siguiente y podemos deducir que es vulnerable:



Ahora bien, con esto podemos conseguir datos importantes como son las tablas de los usuarios, bases de datos y contraseñas.

SQL:





Tablas de monitoring:



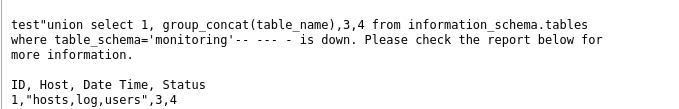
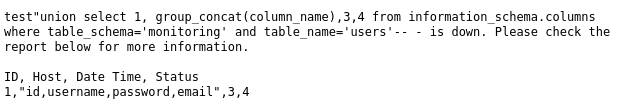


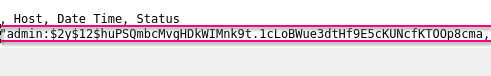
Tabla de usuarios:

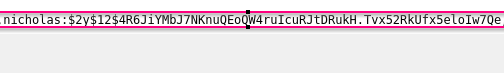




Usuarios con las contraseñas:



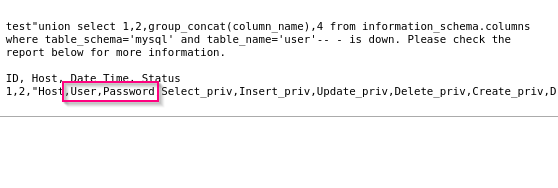






Vamos a enumerar las tablas de la BD mysql: y nos interesa la tabla user





Asi podemos sacar Root:



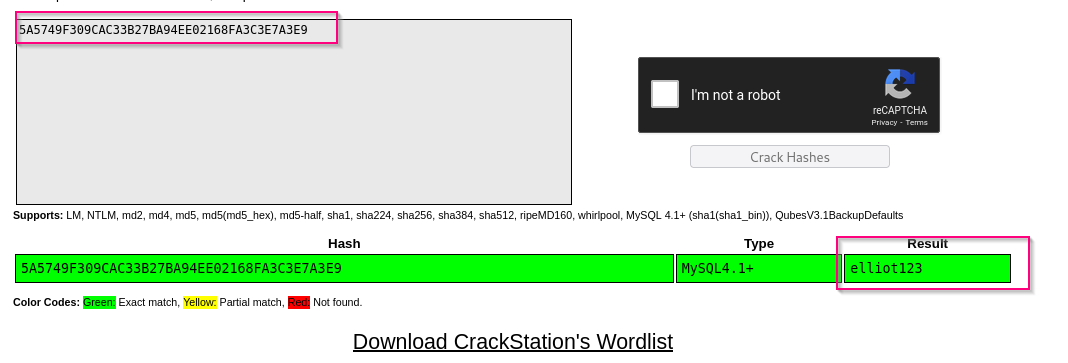






Nos interesa la de ellitot asique la desencriptamos: elliot123

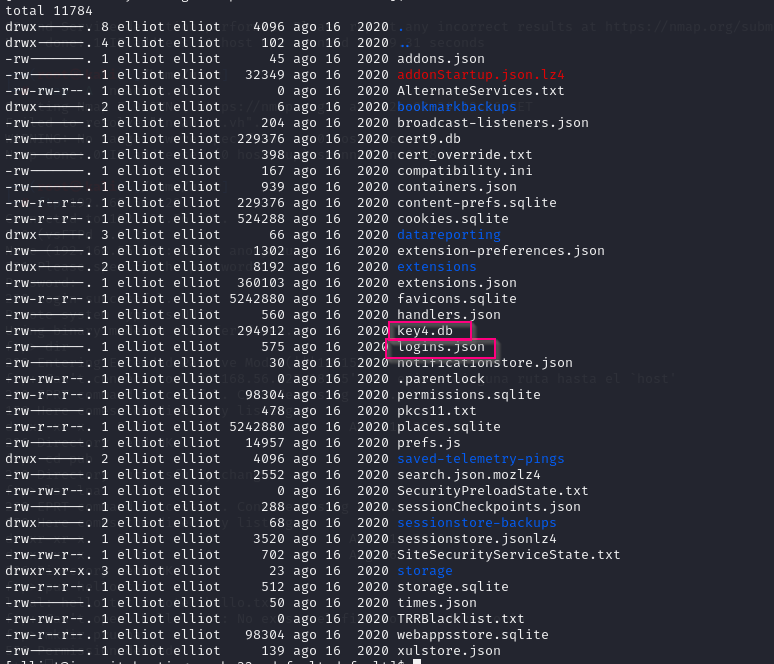




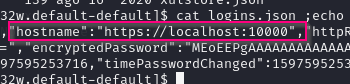
Nos conectaremos por ssh:

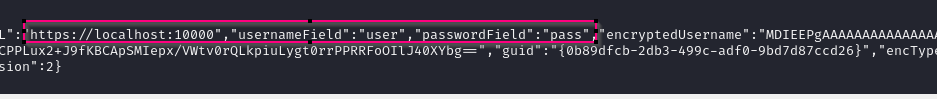


Nos vamos al directorio de .mozilla/firefox/ esmhp32w.default-default/ y nos interesa: key4.db y logins.json

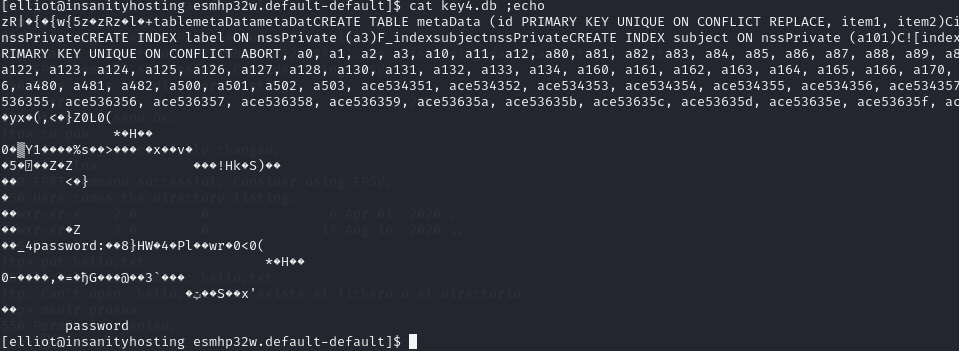


Logins.json: pero las password están encryptadas



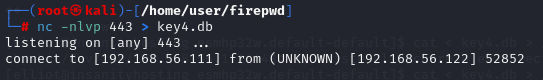


Key4.db:

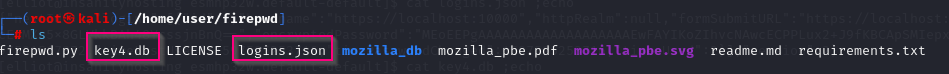


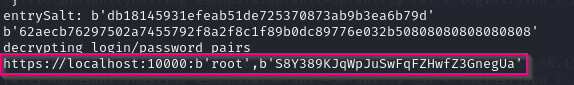
Nos transferimos los dos últimos archivos y con un script llamado firepwd daremos con la solución:

Con el puerto de escucha 443:





Y lo resolvemos con firepwd.py:



Ahora podemos acceder con root sabiendo la contraseña: S8Y389KJqWpJuSwFqFZHwfZ3GnegUa

