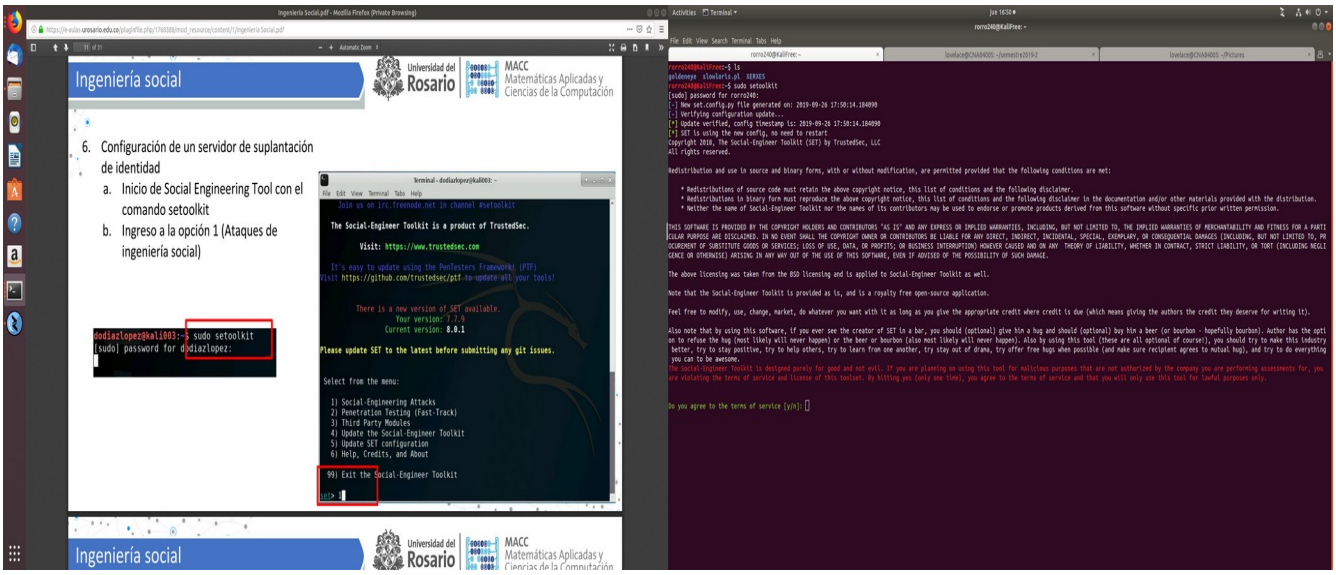
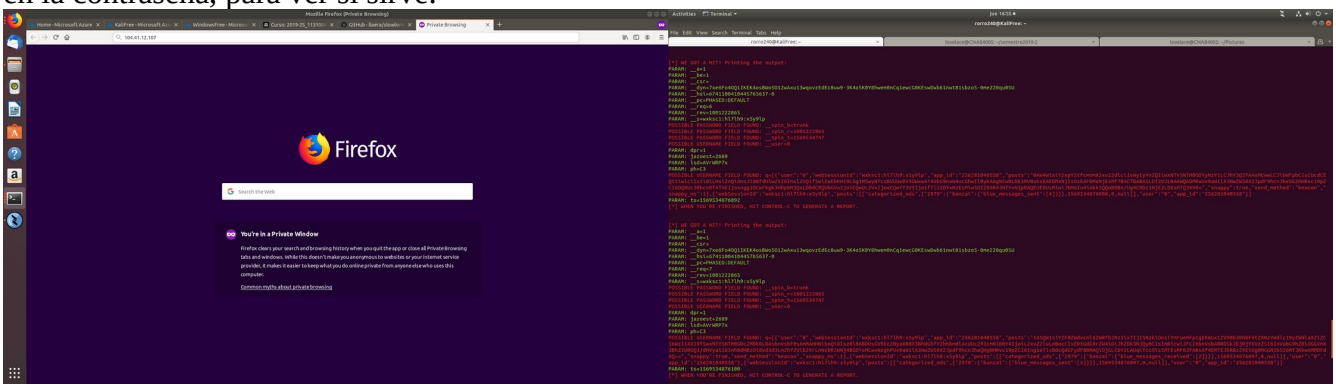
Rodrigo Castillo Camargo
Laboratorio 6: Ingeniería social

Para el laboratorio de Ingeniería social, me propuse a usar el framework llamado “Setoolkit” o Social Engineering Toolkit el cual es elaborado por la compañía TrustedSec, cuenta con una gran variedad de vectores de ataque para ingeniería social.

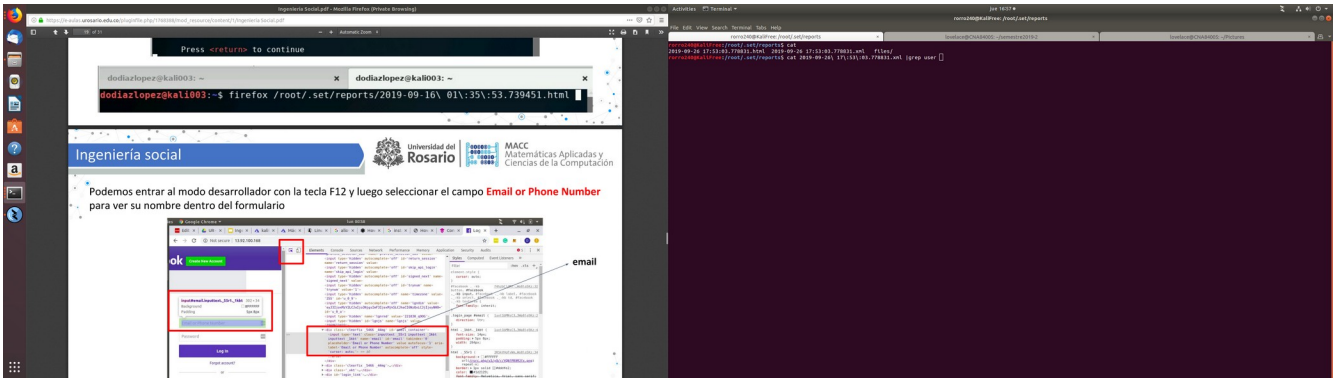


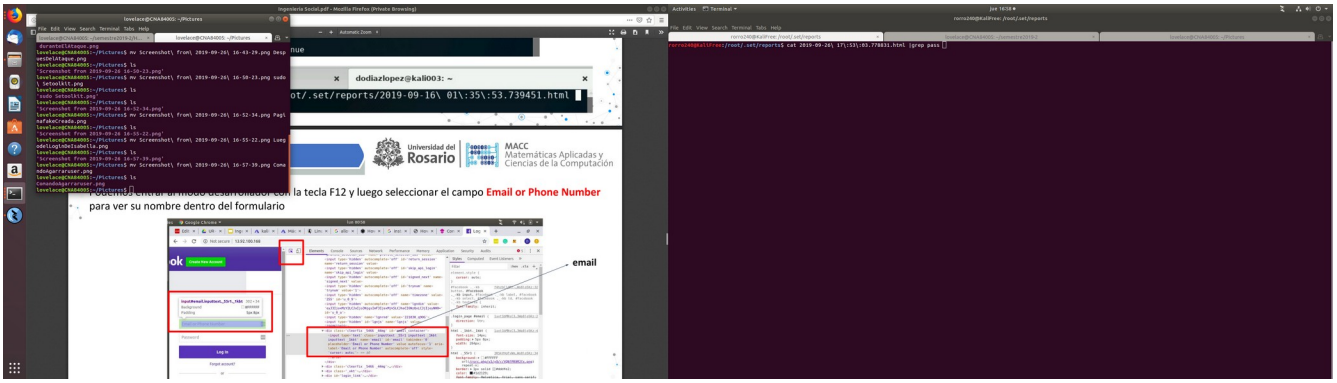
La idea del ataque, será atacarme a mi mismo con fines académicos, lo que haré será crear un servidor de phishing suplantando a la pagina de login del siar del rosario, y luego, escribirme un correo suplantando a la coordinación académica.

Una vez la pagina creada, le pediré a Isabella que abra mi servidor y digite cualquier input en el user y en la contraseña, para ver si sirve.

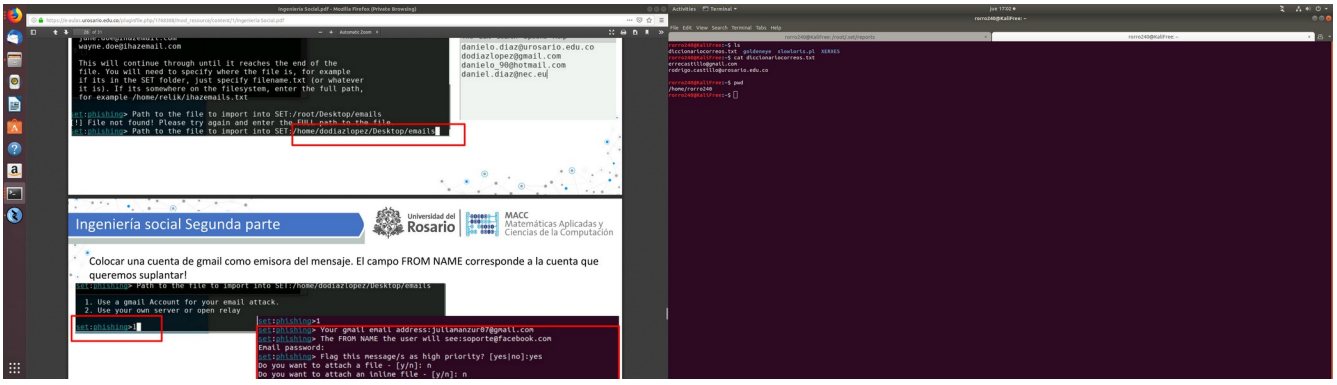


Ahora, voy a buscar dentro del registro generado por el framework a ver que escribió Isabella, para esto, usaré el comando |grep user y | grep pass en el registro



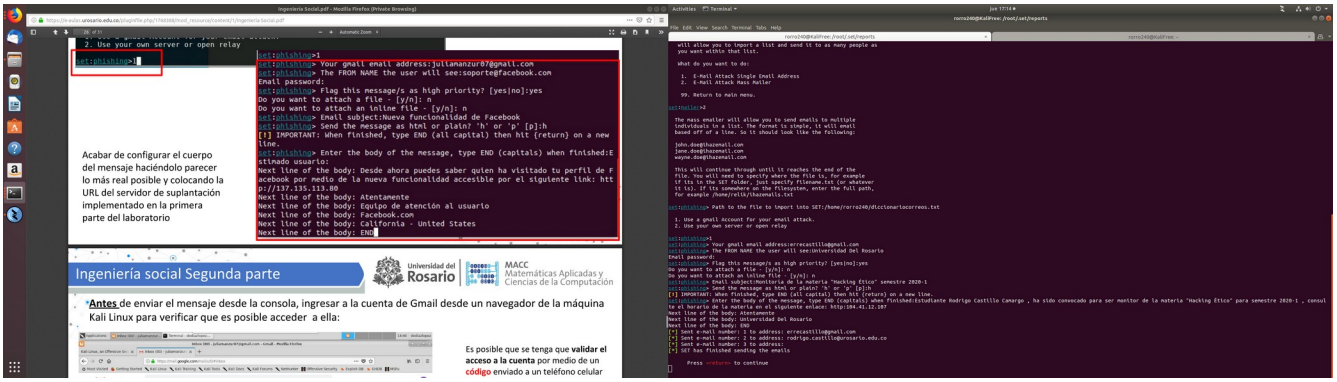


Una vez verificado que el ataque si funciona correctamente, me dispondré a redactar un correo engañoso a mi correo electrónico personal, como quiero que la víctima reciba el correo, crearé un archivo txt con los correos de la víctima (osea , mis correos).



Ahora, usaré la herramienta Setoolkit nuevamente para redactar un correo malicioso a los correos listados en el archivo txt generado.

Escribiré un correo suplantando a la Universidad Del Rosario, diciendo que se me está ofertando la monitoría de ésta asignatura para el siguiente semestre, entonces, que por favor, consulte el horario de la asignatura el siguiente semestre en el link de Phishing que creé



Con este ataque, espero que la víctima abra el correo, ingrese a la página del Siar para loguear pensando que va a consultar la asignatura, pero que al loguear al siar, lo que haga sea mandarme su cuenta del siar sin saberlo.