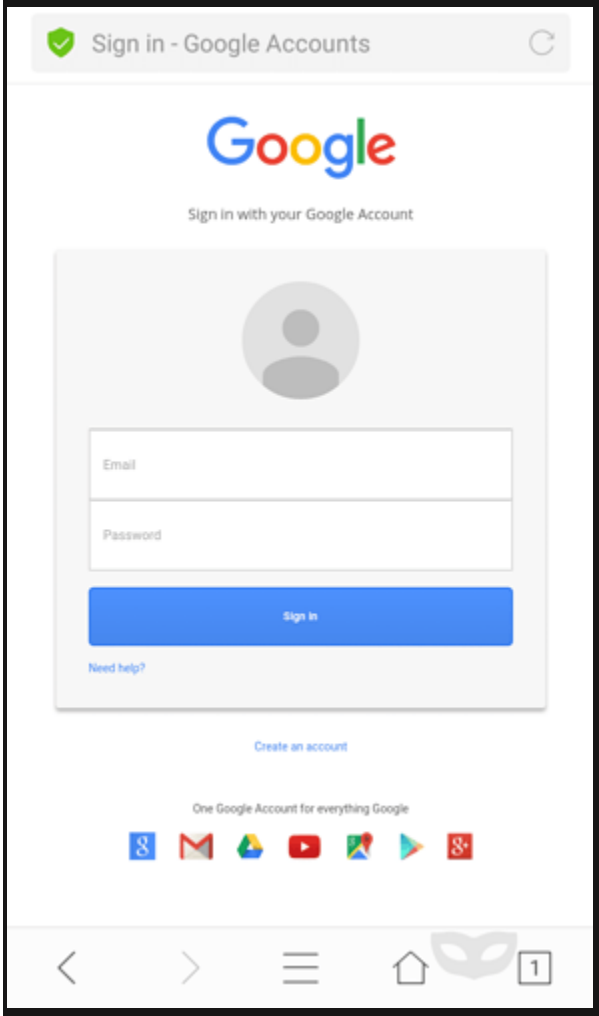
Hello everyone! This is a continuation of part 1 of the Using Social Engineer Toolkit tutorial. Lets continue!

The purpose why i am the use of mobile phone (android)? Let see how the web page displayed in my integrated android browser. So, I am gaining access to my Kali Linux webserver on 192.168.43.99 in the browser. And here is the page:



See? It seems so real, there aren't any security problems displayed on it. The URL bar displaying the title alternatively the URL itself. We understand the silly will apprehend this as the original Google page. So, i bring my cell smartphone, and stroll into my buddy, and communicate to him as though i failed to login to Google and act if I am thinking if Google crashed or errored. I deliver my telephone and ask him to try to login the usage of his account. He doesn't trust my phrases and at once starts offevolved typing in his account statistics as though not anything will manifest badly here. Haha.

He already typed all the required forms, and let me to click the Sign in button. I click the button... Now It is loading... And then we got Google search engine main page like this.

Once the victim clicks the Sign in button, it will send the authentication information to our listener machine, and it is logged.

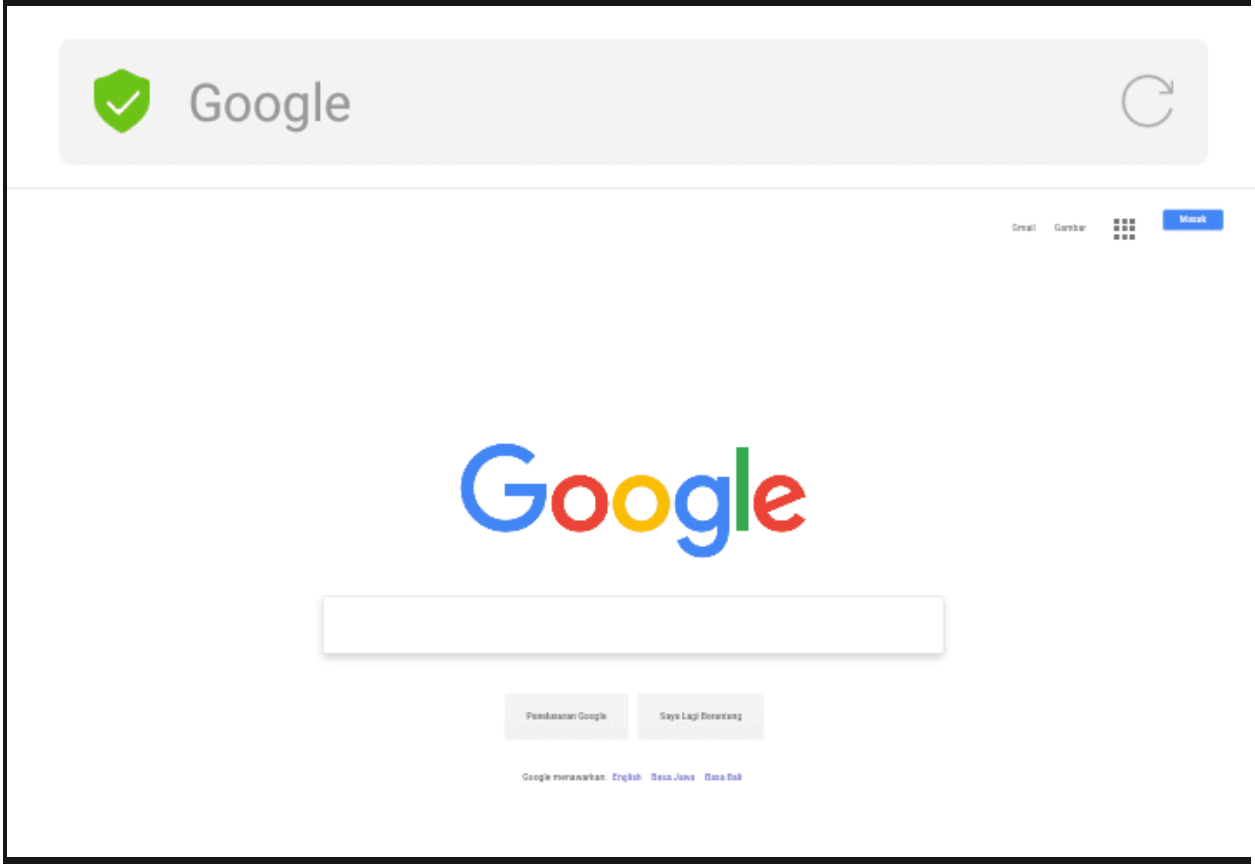


image717×488 6.39 KB

Nothing is going on, i tell him, the Sign In button remains there, you did not login even though. And then i'm beginning again the phising page, at the same time as some other friend of this silly coming to us. Nah, we were given every other sufferer.

Until i cut the communicate, then i go returned to my table and check the log of my SEToolkit. And if you followed it correctly you should have a username and password highlighted in red.

And we are done! Thank you for viewing this tutorial.