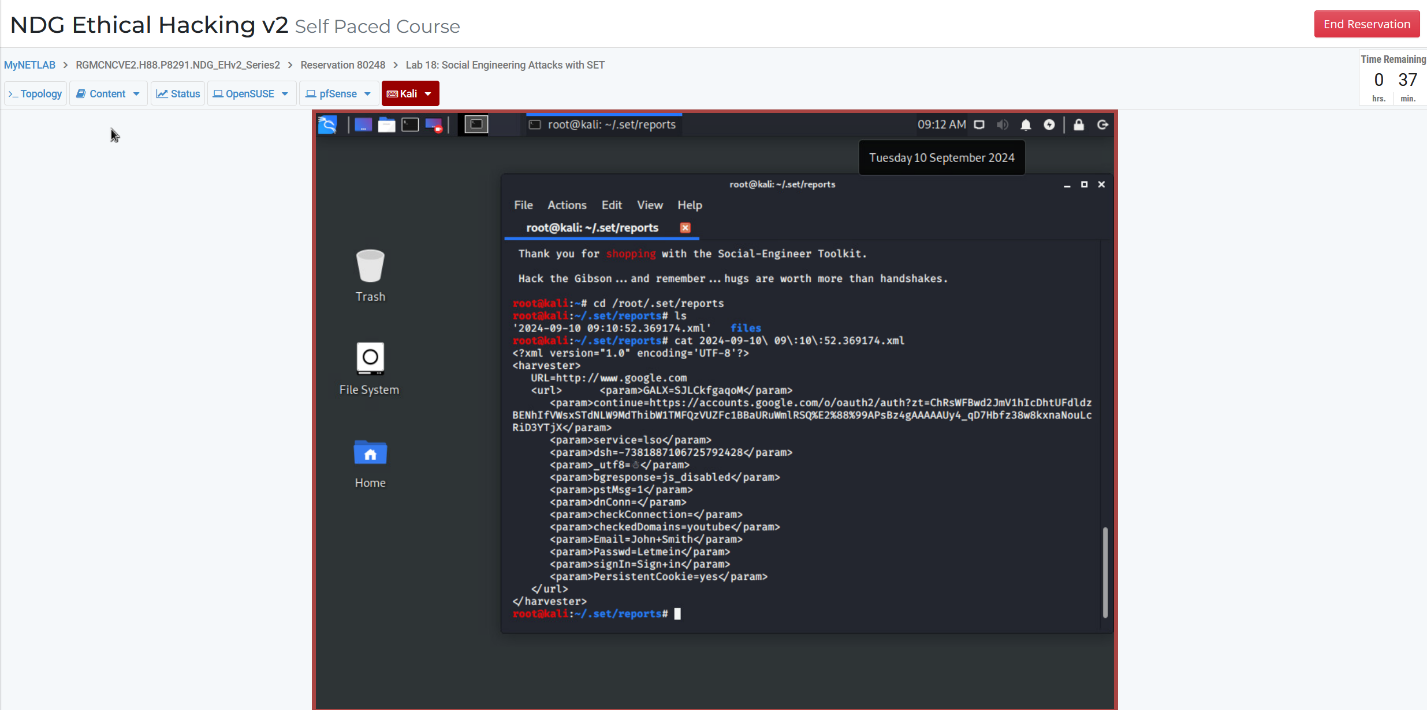
**Section 3, Step 17**– Take a Screenshot of the credentials you were able to steal and paste it below

*Paste screenshot of credentials from Section 3, Step 11 here*

A screenshot of a computer

Description automatically generated

**

**Questions**

1. What type of Phishing or Internet-Based Technique from LabSim section 3.1.8 does this attack most closely resemble? The attack done in this lab most closely resembles a Spear Phishing attack. While we did not send an email, this website is meant to have someone input their google account credentials, and then redirect them back to their gmail account so they have no clue their information has been stolen.
2. Do some research on the HTTPS Everywhere browser extension (Link to description: <https://www.websecurity.digicert.com/security-topics/https-everywhere>)
   1. How could using this extension help combat hacking techniques like the one you completed in this activity? The extension HTTPS everywhere would ensure the authentication of the website’s identity, so a user of HTTPS everywhere would know if they are going to a real or fake website.
3. In this lab, we as the attacker were able to just jump on the OpenSUSE machine on the internal network. Obviously this is probably not possible in the real world.
   1. What social engineering technique(s) could we use to get a user on the internal network to come to our false page and enter their credentials? In the real world, the most likely scenario for getting a user on the internal network to our false page would be a type of phishing scam.