# Social Engineering



* **What is Social Engineering?**

# Types of Social Engineering Attacks

## ★ Phishing

★ *Vishing*

## ★ Pretexting

★ *Baiting*

# How to Prevent Social Engineering Attacks

## ★ Delete any request for personal information or passwords.

★ *Reject requests for help or offers of help.*

## ★ Set your spam filters to high.

★ *Secure your devices.*

# Set Up Lab Environment

### Download and Install Kali Linux and Ubuntu Virtual Environments

Kali Linux: <https://www.kali.org/get-kali/#kali-virtual-machines>

Credential

### Username: kali Password: kali

Ubuntu: <https://www.osboxes.org/ubuntu/>

* Select “Ubuntu 12.04 Precise Pangolin” 64 bit VDI

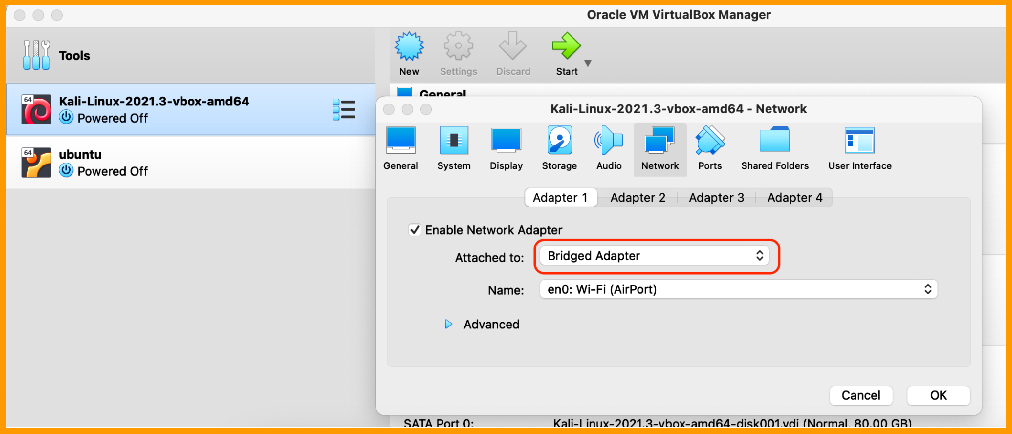
Credential

**Username: osboxes.org Password: osboxes.org**

# Part 01 - Set up Attacker’s Virtual Machine (Kali Linux)

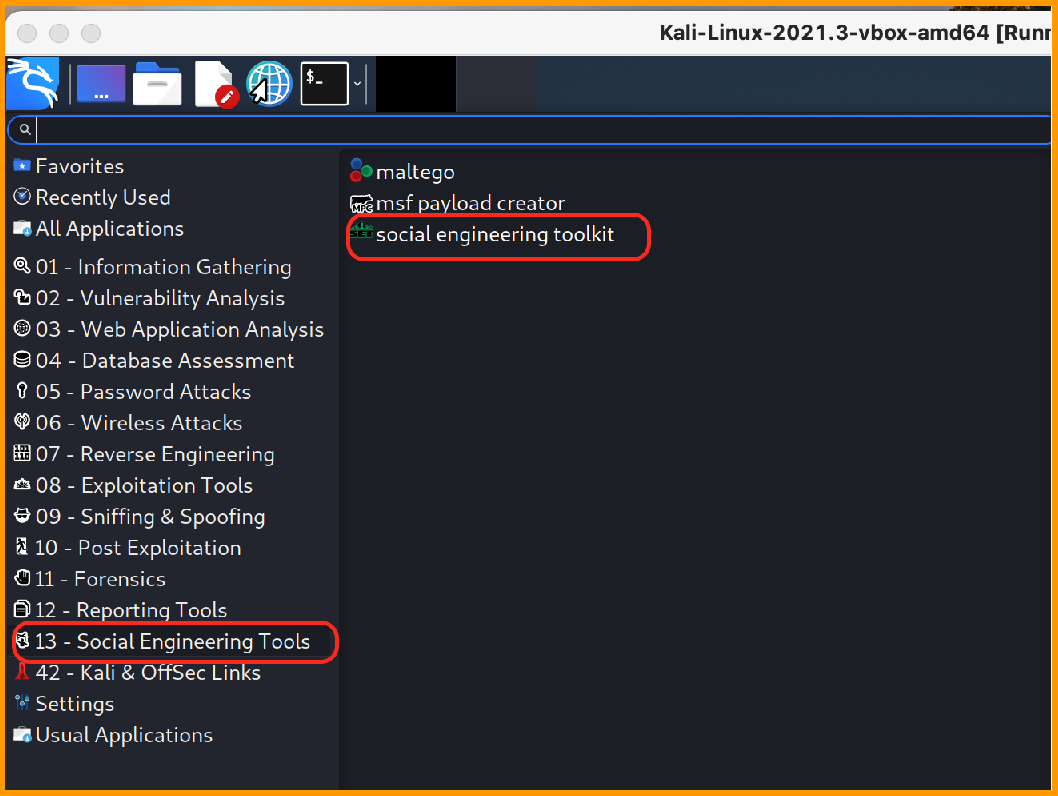
1. *Configure Kali Linux Virtual Machine Settings*
   * *Edit Network Adapter*

#### Settings > Network > Bridged Adapter



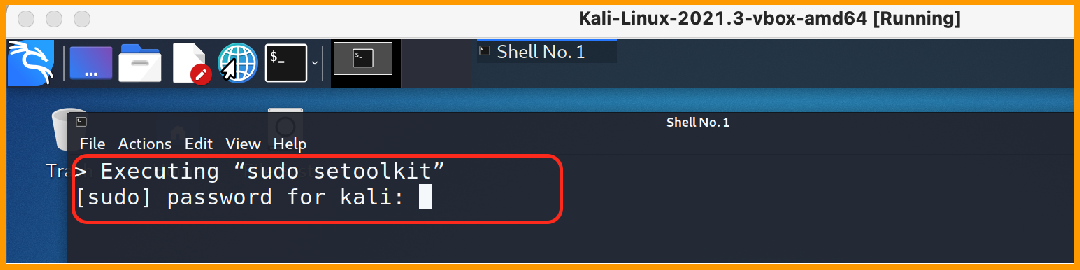
1. *Start Kali Linux Virtual Machine*
2. *Open Console Terminal and Retrieve IP Address (use* ***ifconfig*** *command)*
3. *Start the Social Engineering ToolKit in Kali Linux*

#### Applications > Social Engineering Tools > Social Engineering toolkit

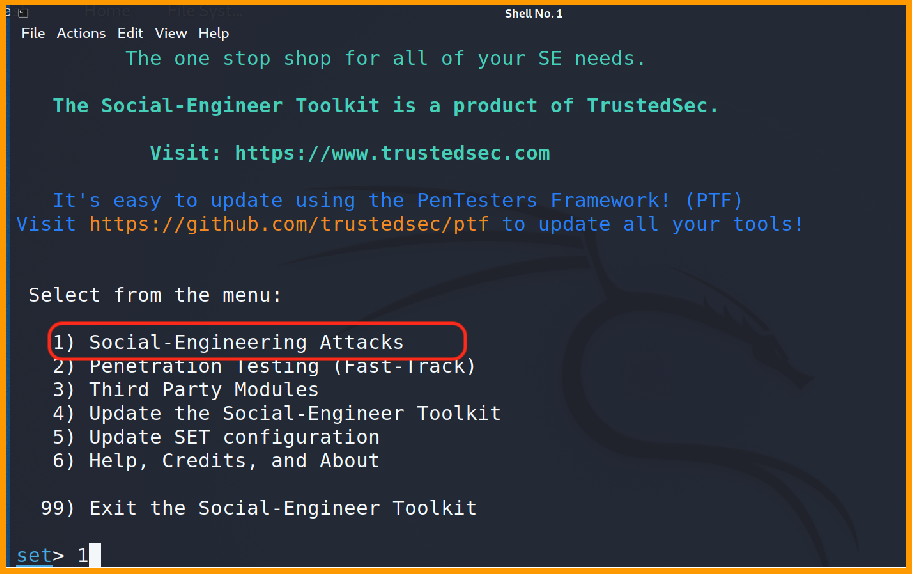


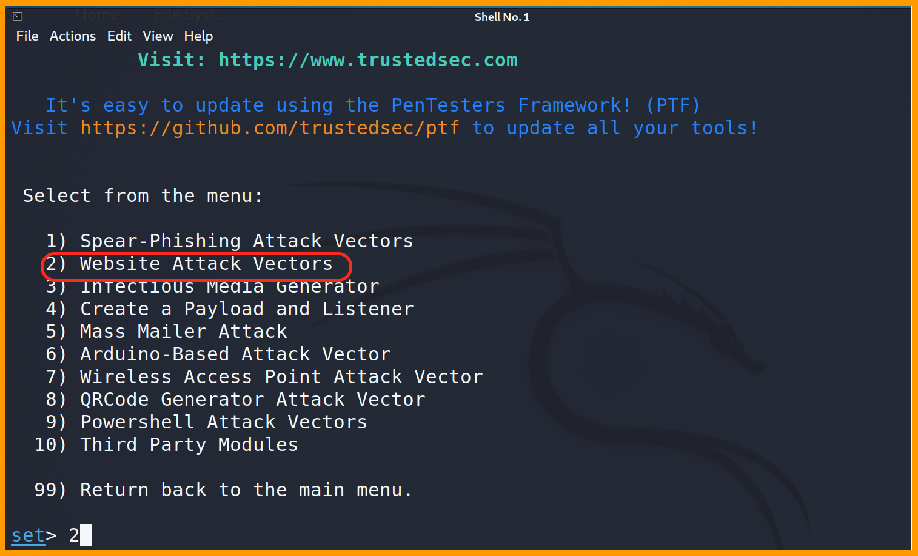
1. *Give your Kali Linux credential (current user password) to access the social engineering toolkit.*

**Current User Password - kali**

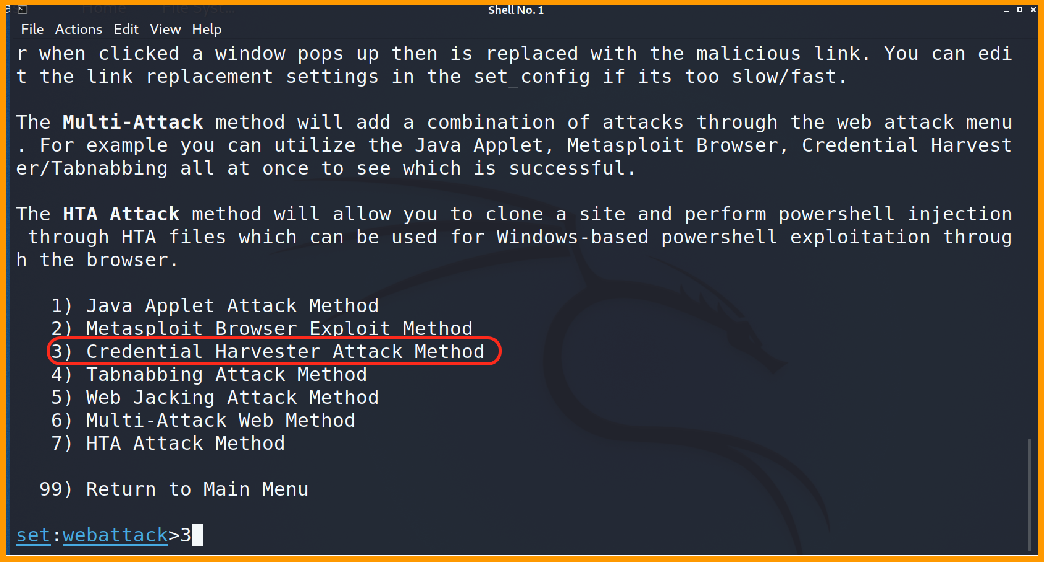


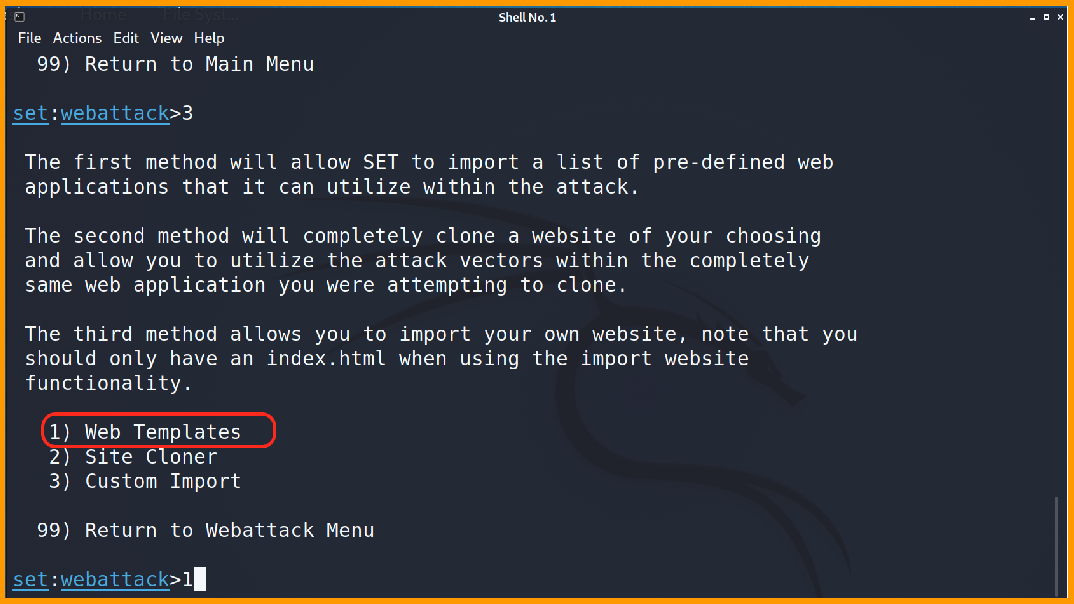
1. *Select “Social-Engineering Attacks” from the menu*
   * *Type “1” in the terminal.*



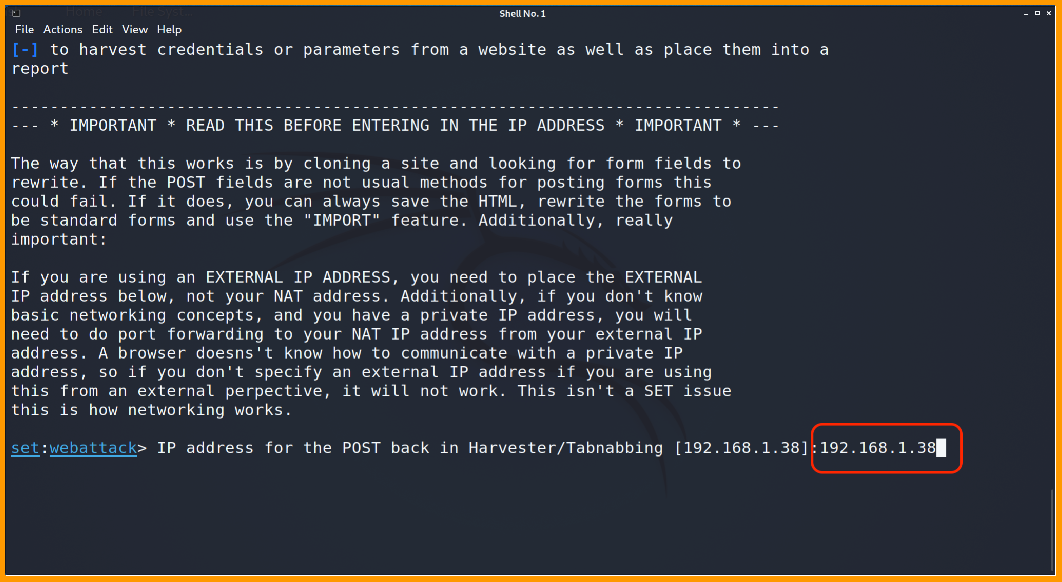
1. *Select “Website Attack Vectors” from the vectors menu Type “2” in the terminal*
2. *Select “Credential Havester Attack Methods” from the Attack methods menu*

Type “3” in the terminal

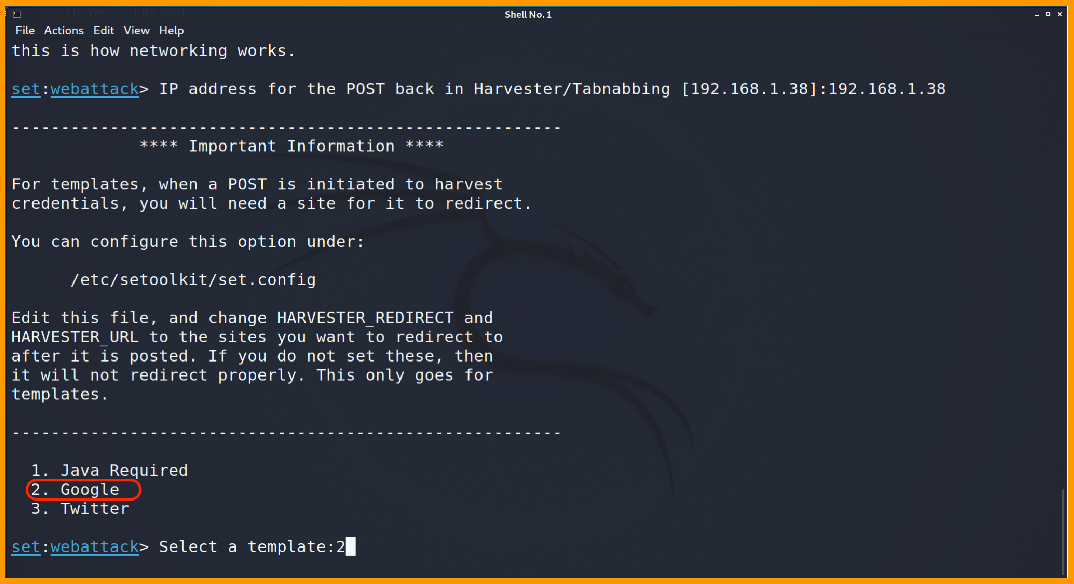


1. *Select “Web Templates” from the Imports menu Type “1” in the terminal*
2. *Put kali linux IP Address for the POST back in Harvest/Tabnabbing*
   * *To get the IP Address of your kali linux type “ifconfig” in separate terminal then you’ll get your kali linux virtual machine IP address.*

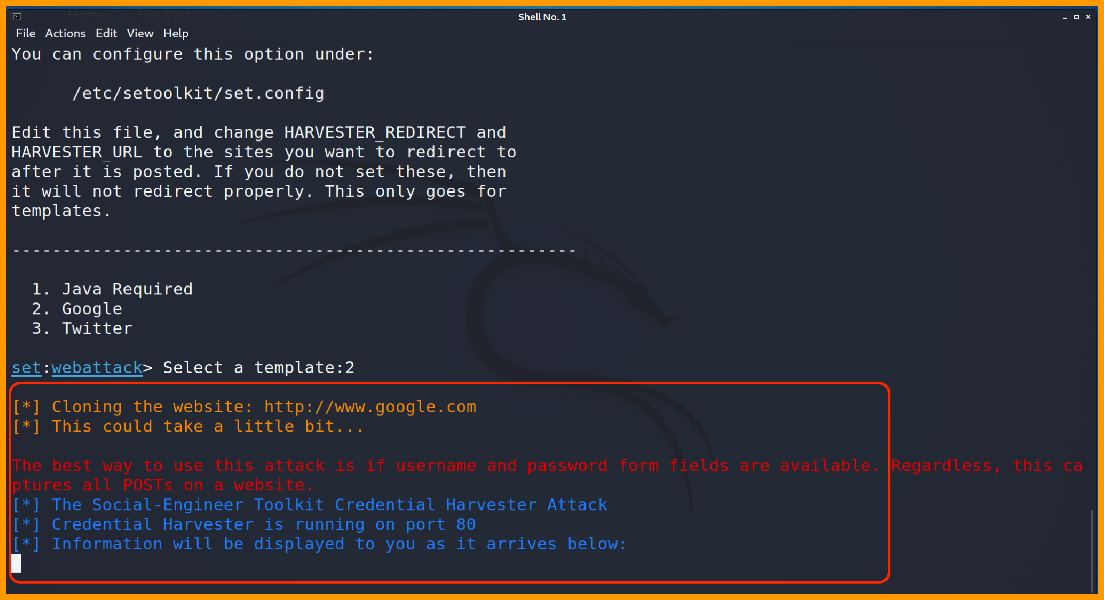
**Example** : In here kali linux IP Address is 192.168.1.38



1. *Select “Google” from the Templates menu Type “2” in the terminal*



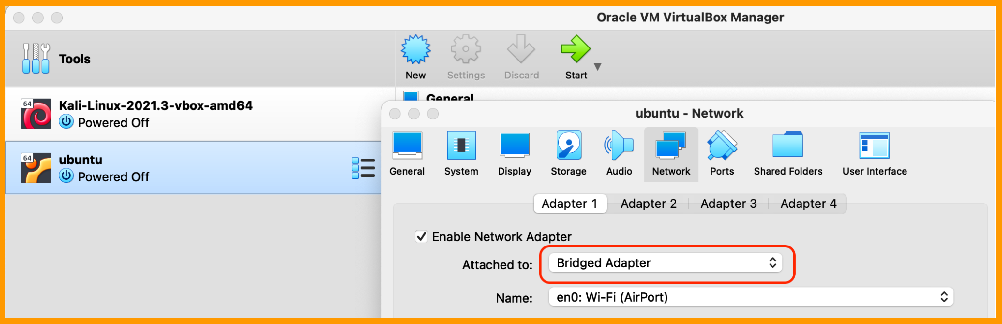
1. *After you enter template (“Google”) you can see Website Cloning. It may take a while to clone, meanwhile you can start up your ubuntu virtual machine.*



# Part 02 - Set up Victim’s Virtual Machine (Ubuntu)

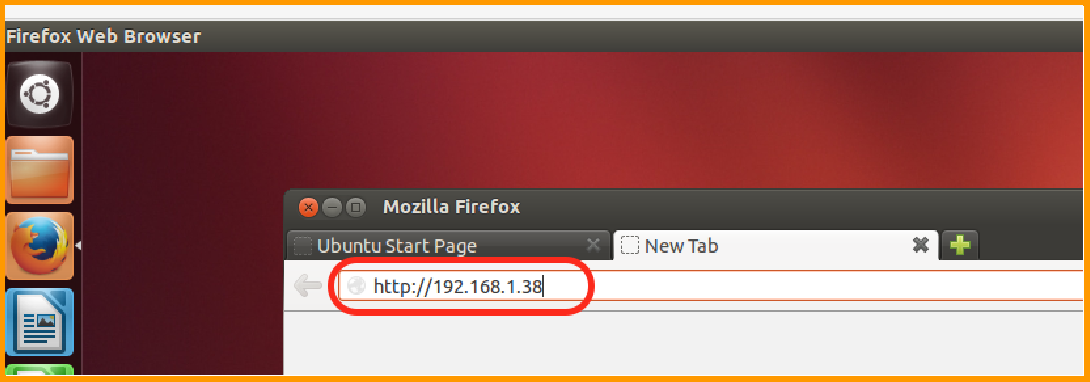
1. *Configure Ubuntu Virtual Machine Settings*
   * *Edit Network Adapter*

#### Settings > Network > Bridged Adapter

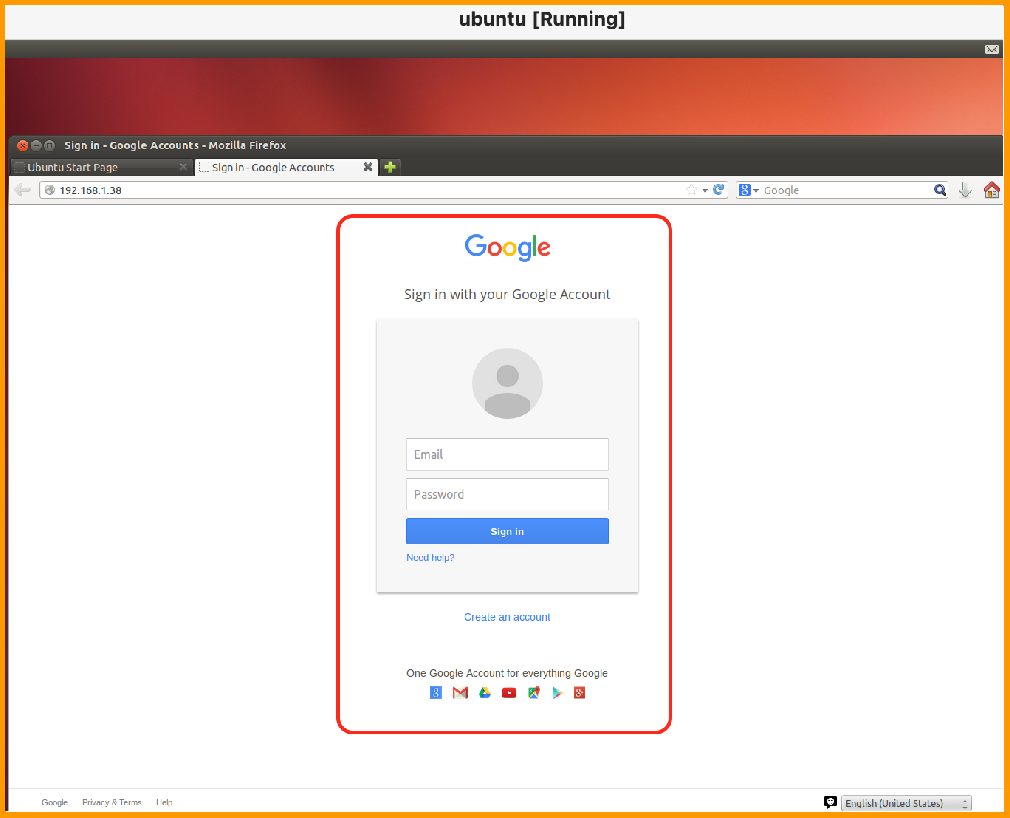


1. *Start Ubuntu Virtual Machine*
2. *Open Console Terminal and Retrieve IP Address (use* ***ifconfig*** *command)*
3. *Start the Web Browser (Mozilla Firefox) in ubuntu virtual machine*
4. *Open new tab and place the kali linux machine IP address in address bar*

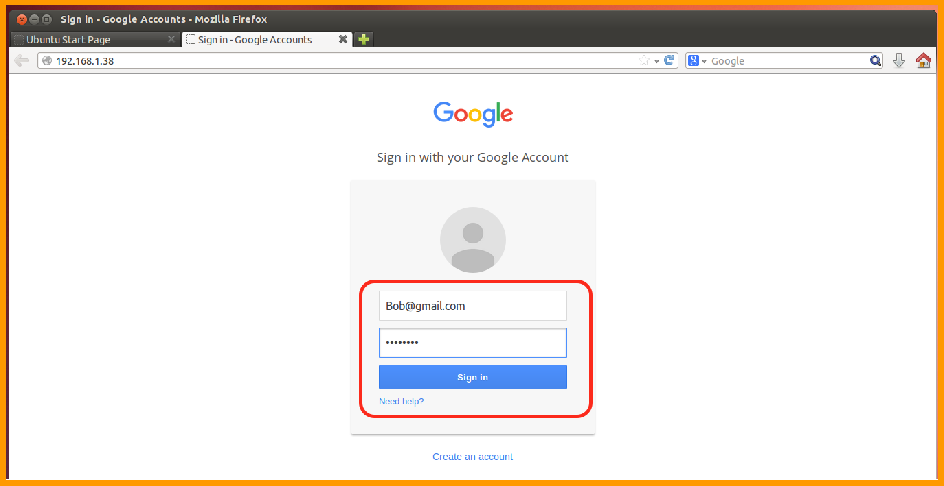
*Example :* [***http://192.168.1.38***](http://192.168.1.38/)



1. *After you enter above URL you’ll redirect to google account*



1. *Enter Email and Password (you can enter any email address or password that you like)*
2. *Click “Sign In”*



1. *After you sign in go to the kali linux virtual machine.*
2. *Observe that now you have data showing the victim's username and password in kali Social Engineering toolkit shell.*

