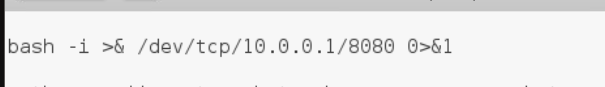
**ISEC 500 - Information Security Overview**

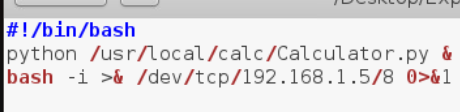
**Assignment 6 – Lab 5: RemoteShell: Pentesting and Understanding Vulnerabilities - Embedding Client-side Code into a Package**

The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

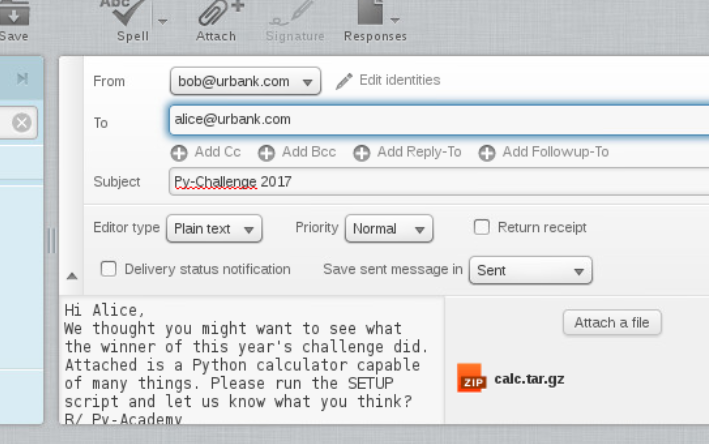
**INSERTING CODE INTO A PROGRAM**





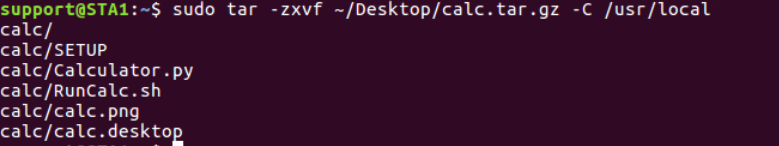


**SPEAR PHISHING**



**FALLING VICTIM: REMOTE SHELL**





**PART 2**

This week’s virtual lab was interesting, informative and related to real world like all other virtual labs.

I liked how we mixed our malicious inside a harmless program that target was interested in. Social engineering + trojan. The trojan was a good trojan too. It not only looked like a harmles program at first, it continued working as a harmless program. Therefore the target didn’t get suspicious.  
  
Those were the good criticism I had for this attack. Now lets start talking about negative criticism.  
  
The email we send wont come from that website she uses. It will come from us. Which will alert some targets. But unfortunately some email services such as outlook are designed in such as way that the email subject is where sender is supposed to be and is bold. So when someone send an email with a subject [help@paypal.com](mailto:help@paypal.com) it actually looks like that is the sender, not the subject.  
  
Another thing that will alert some of the users is the fact that we email the user an executable file for the user to download and execute. Which is a huge red flag.  
  
Another thing that will alert some of the users is that users will extract the file and than check its contents. They wont use cmd commands to extract the file to some folder in the background and execute it using commands.