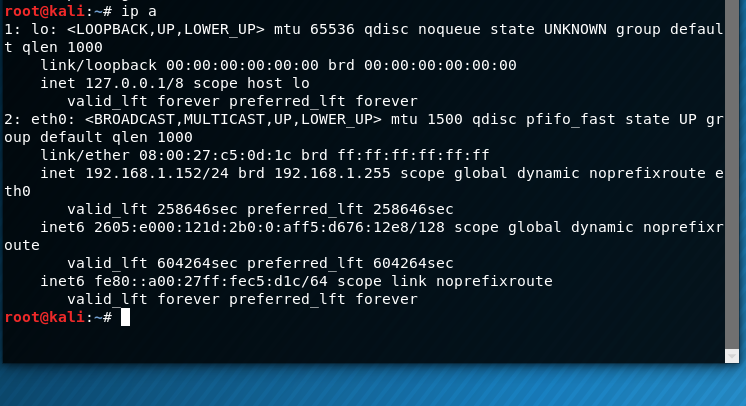
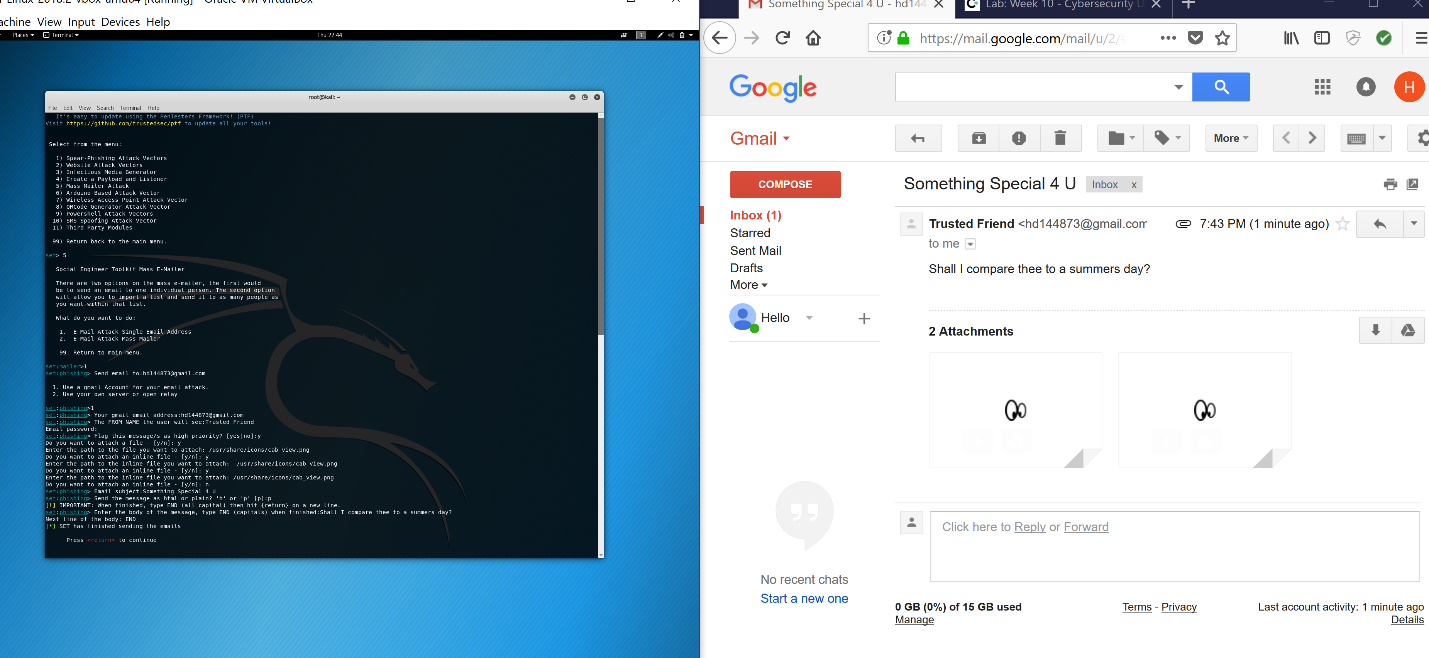
**Milestone 0: Kali Gone Wild**



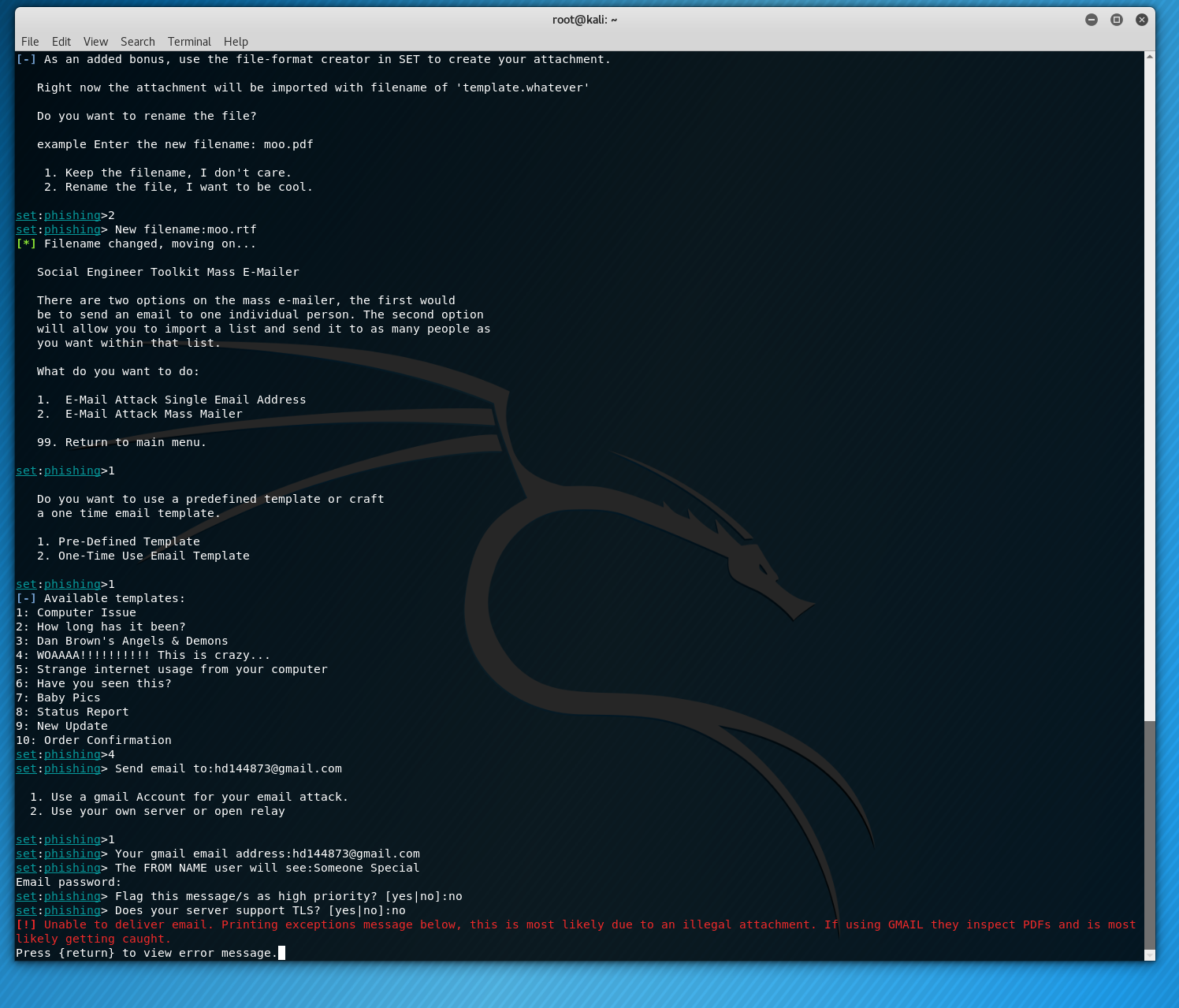
* Need to know the new IP address before going to Milestone 4: 192.168.1.152

**Milestone 1: Hello, SET**

****

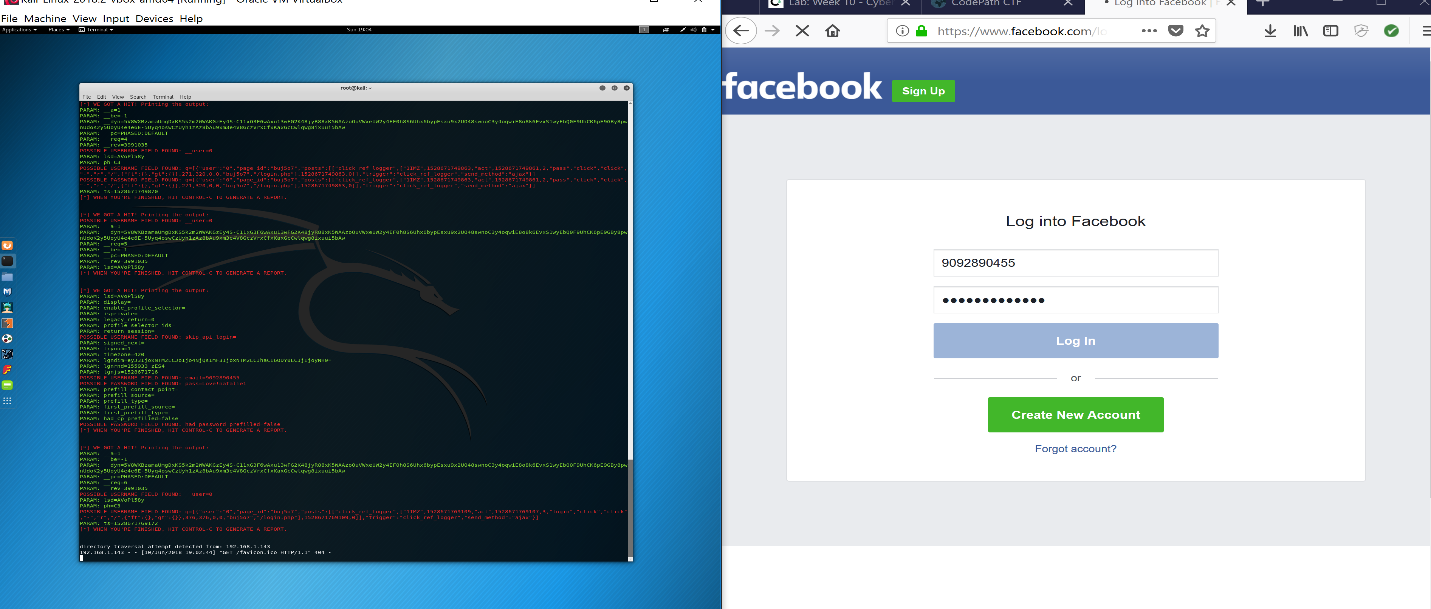
* After following the steps from Milestone 1 you will get this answer.

**Milestone 2: Try a Real Payload**



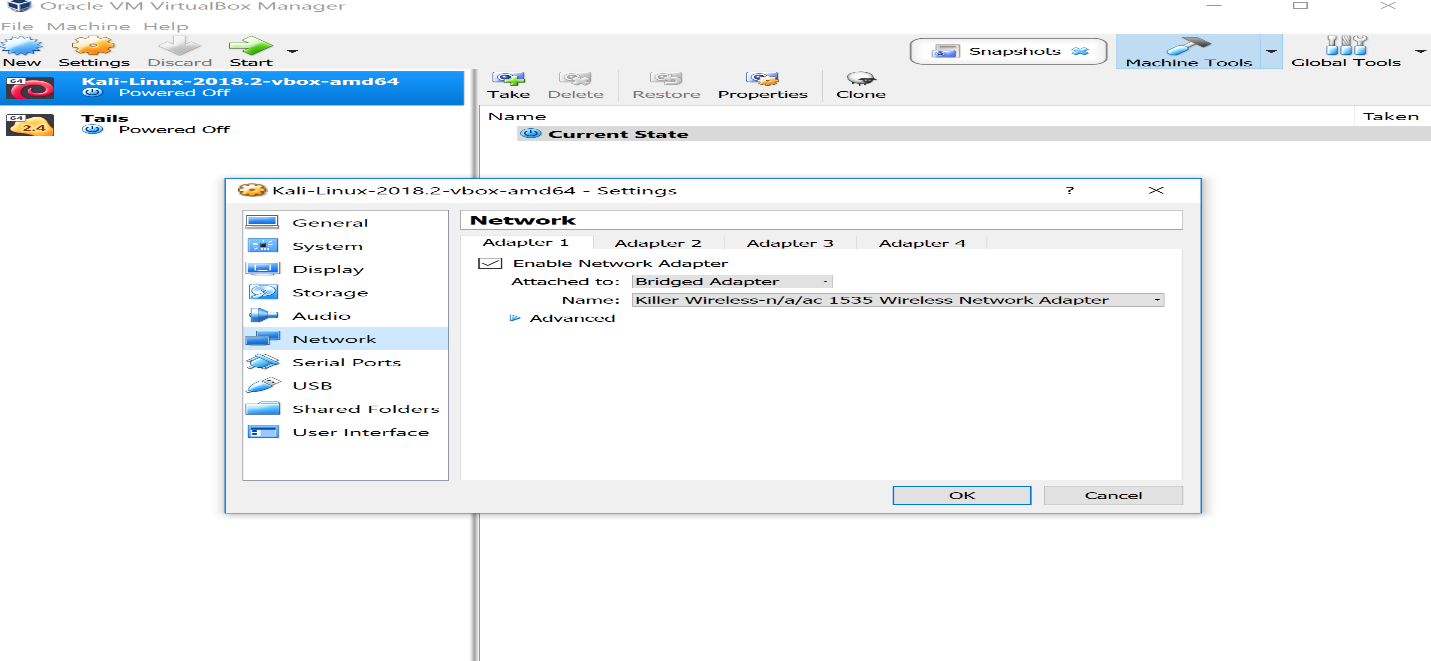
* The following step will give you the error messages.
* This error messages stop the payload from being sent to the email.

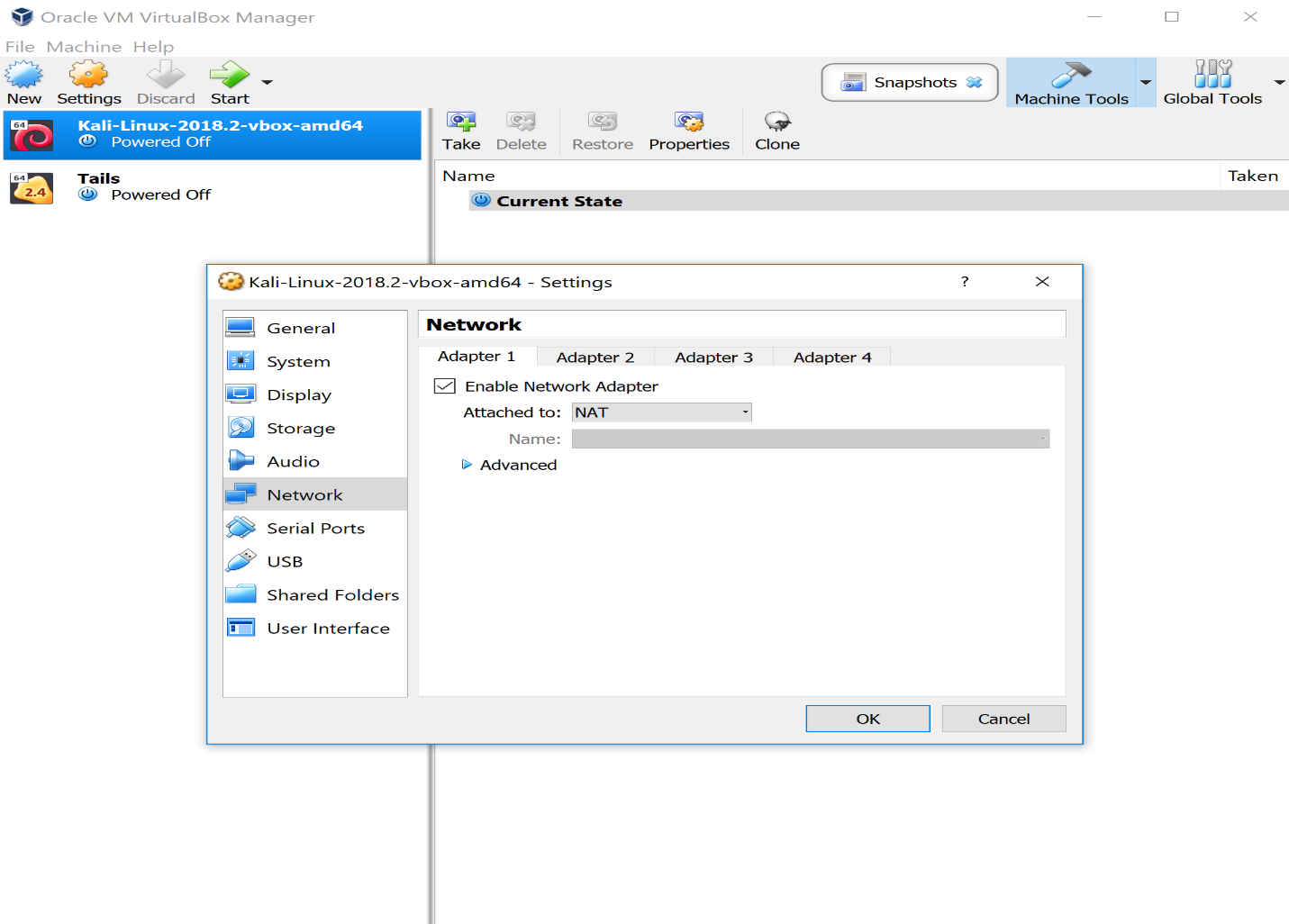
**Milestone 3: Fakebook**



* I was able to connect to my facebook, but as you can see I was receiving information back to my Kail.

**Milestone 5: Cleanup**





* Returning my setting back to NAT on my Kail, following steps.

**Milestone 6: SE In Situ**

 What vulnerabilities were beyond the control of the user? **Human being/Pushing.**

 What if anything could have been done by the user to mitigate the severity of the attack? **More training into these types of attack dealing with pushing attack.**

 What could the user do to mitigate this, making a successful login impossible for the attacker even with the credentials? **The user could have use a second authentication key or automatic text to his or her phone.**

 Why might the username/password still be of value to the attacker even if she can't use them to login to Facebook? **The hacker could’ve put malicious malware that could monitors his or her keystrokes into other accounts.**