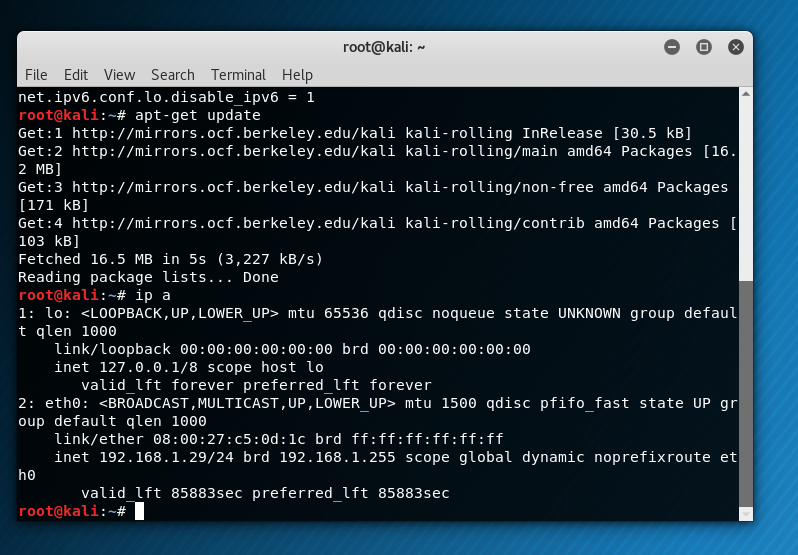
**Lab 10**

Milestone 0:



The first few parts of this milestone worked, but when I went to change the file it would give me an error message when I tried to save the file. Then I continued on with the steps and found the ip address of my vm.



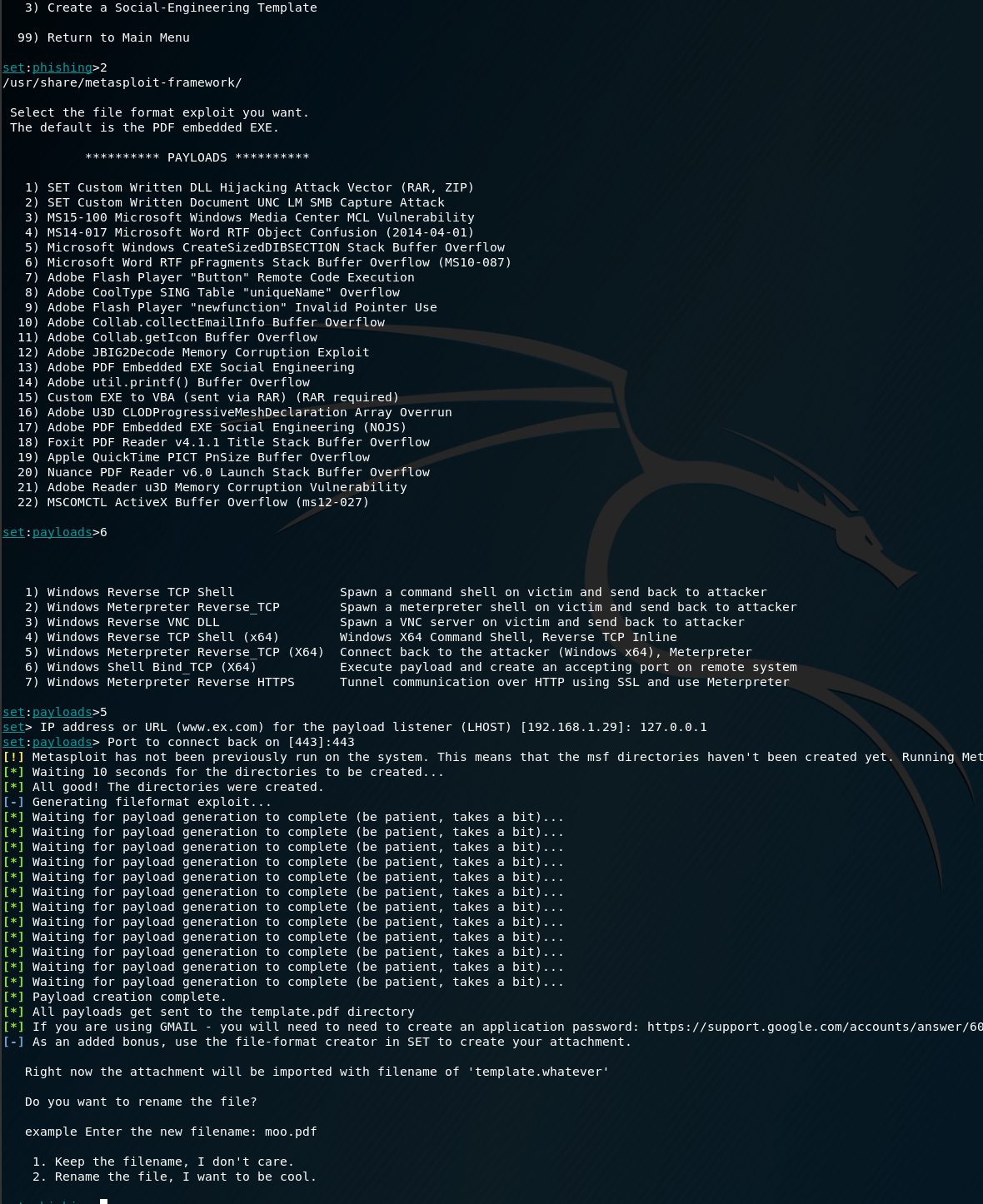
Milestone 1:

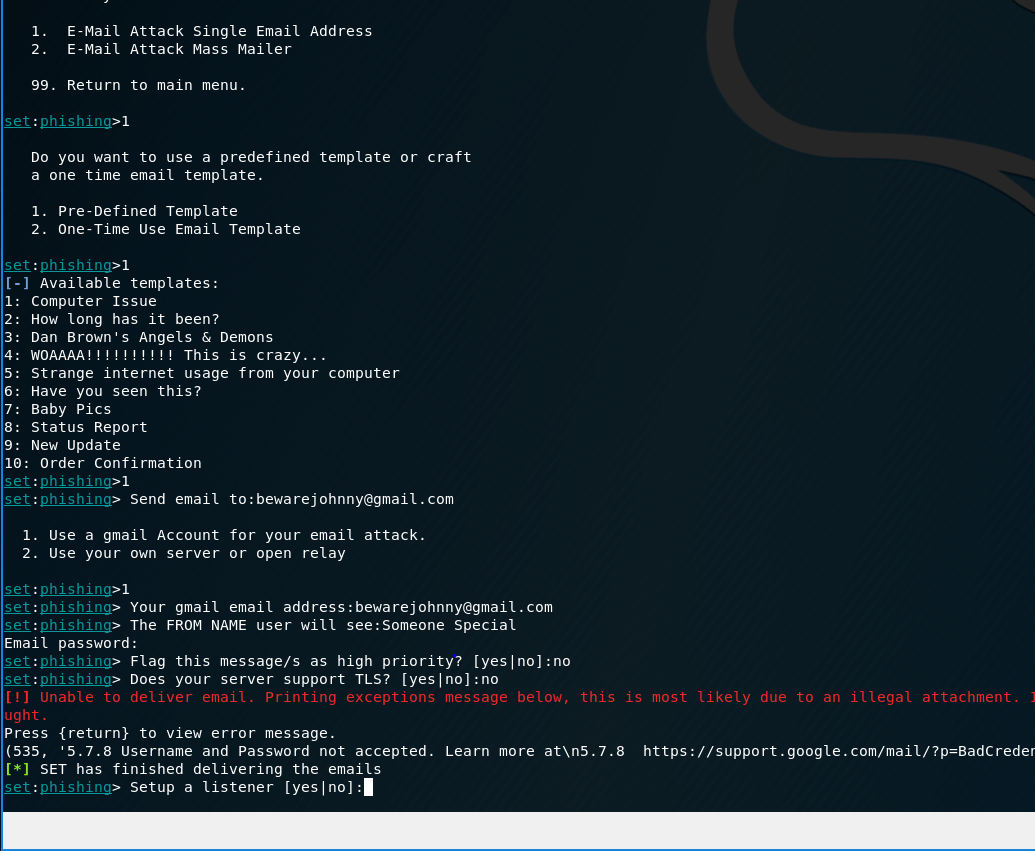
I created a fake gmail account and updated social engineer toolkit in Kali. I then followed the steps listed for this milestone.



Milestone 2:

For milestone 2 the following questions:

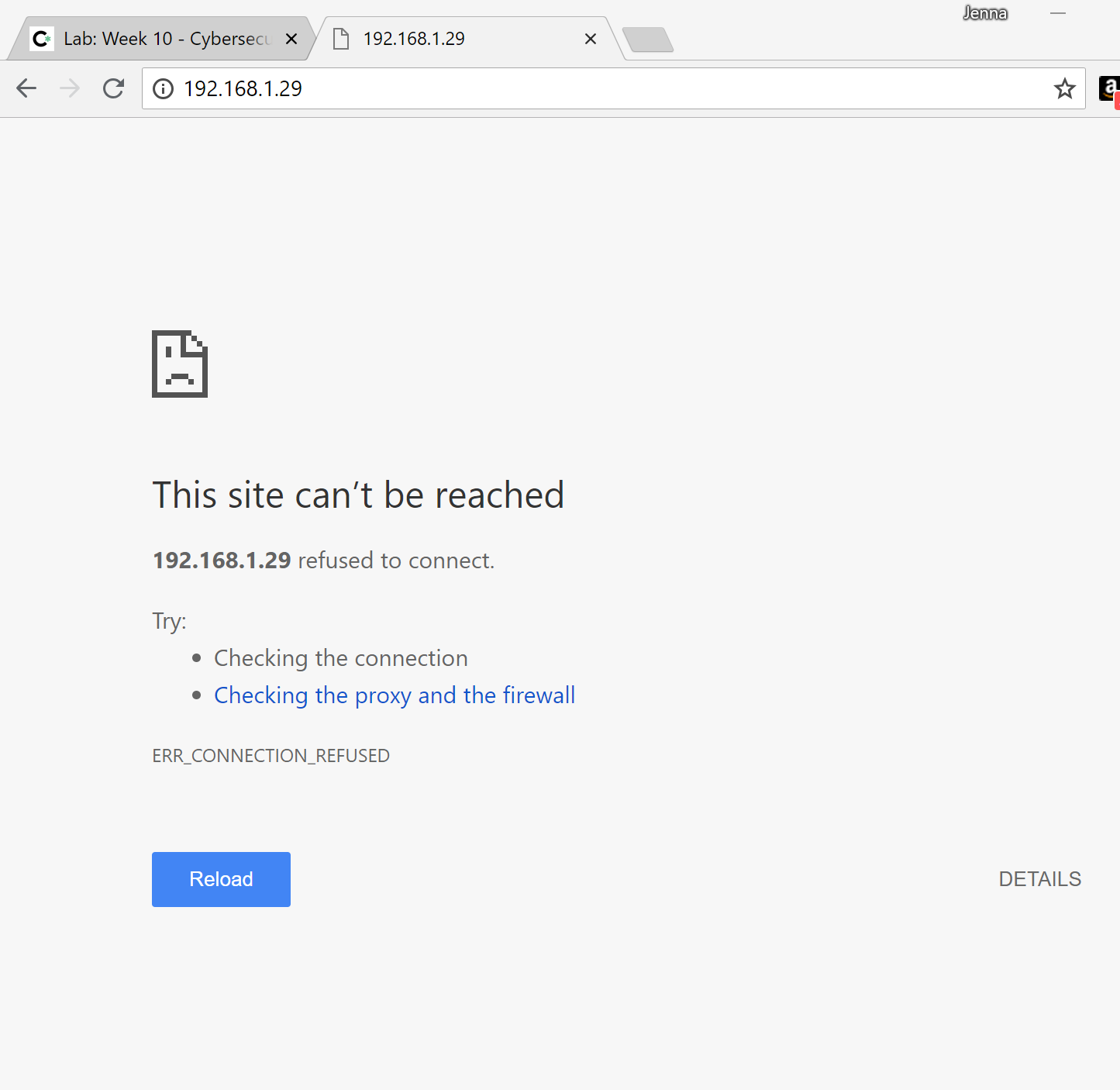
* Which two software companies are heavily represented on this list? Adobe, Microsoft
* Which operating system would most of these exploits require? windows 
* 



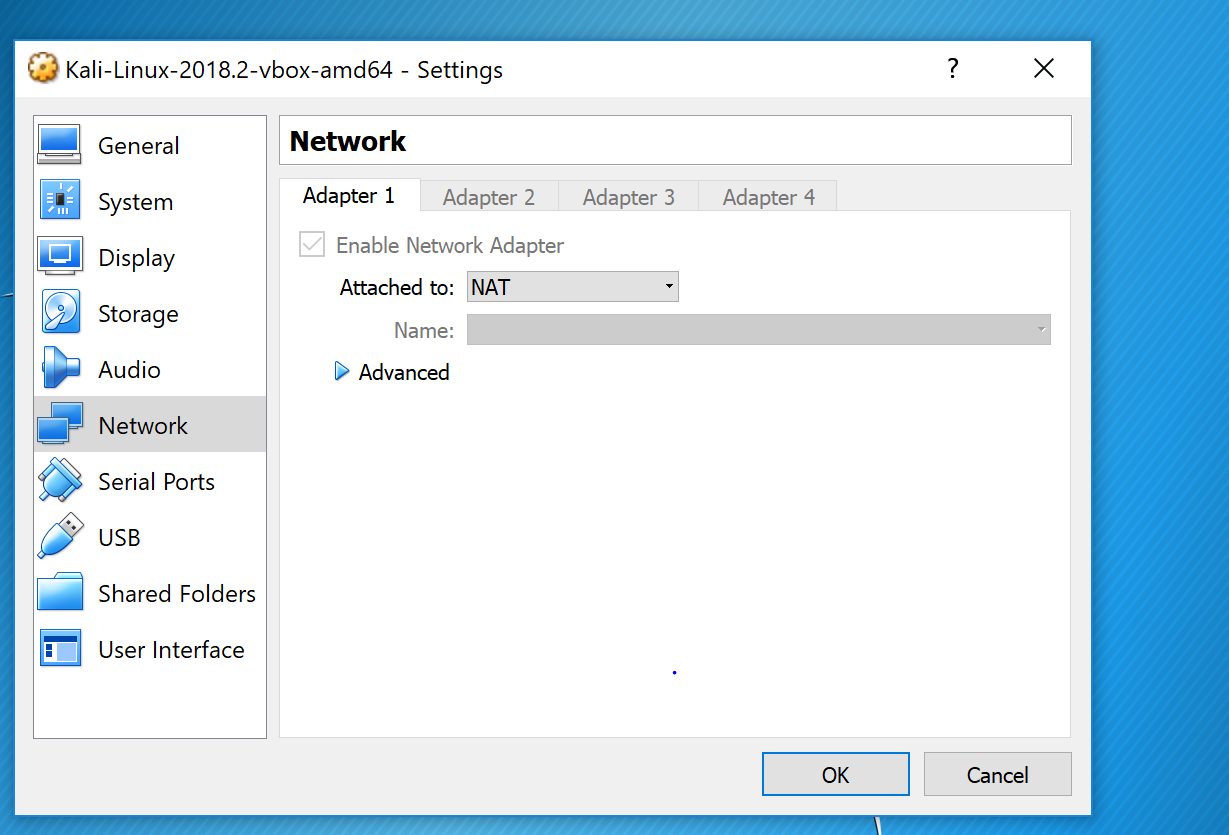
Everything worked in this step.

Milestone 3:

This step didn’t work for me. When I typed localhost into a web browser on my Kali I would get an error message. The IP of my kali wouldn’t load anything from my host computer browser.



Milestone 5:



In this step, I switched the VM from Bridged mode to NAT.

Milestone 6:

* What vulnerabilities were beyond the control of the user?

Apple’s tech support gave the hackers access to the user’s icloud account. They revealed a partial credit card number-that apple used to release information. These numbers were what was required for apple’s identity verification.

The tech support in the phone provider situation was a vulnerability as well. The girl was able to edit the guy’s account and find out his email address.

* What if anything could have been done by the user to mitigate the severity of the attack?

The user could have had a webcam cover.

The user could have not clicked on the link in the phishing email.

The user shouldn’t have had all their accounts linked.

* What could the user do to mitigate this, making a successful login impossible for the attacker even with the credentials? (Hint: FB offers this as an option; not all sites do)

If the user had a usb for authentication as part of their log in. This way the security key usb is entered into the computer as well as the password.



* Why might the username/password still be of value to the attacker even if she can't use them to login to Facebook? (Hint: think about how users come up with passwords)

They might contain information for other passwords or security questions.