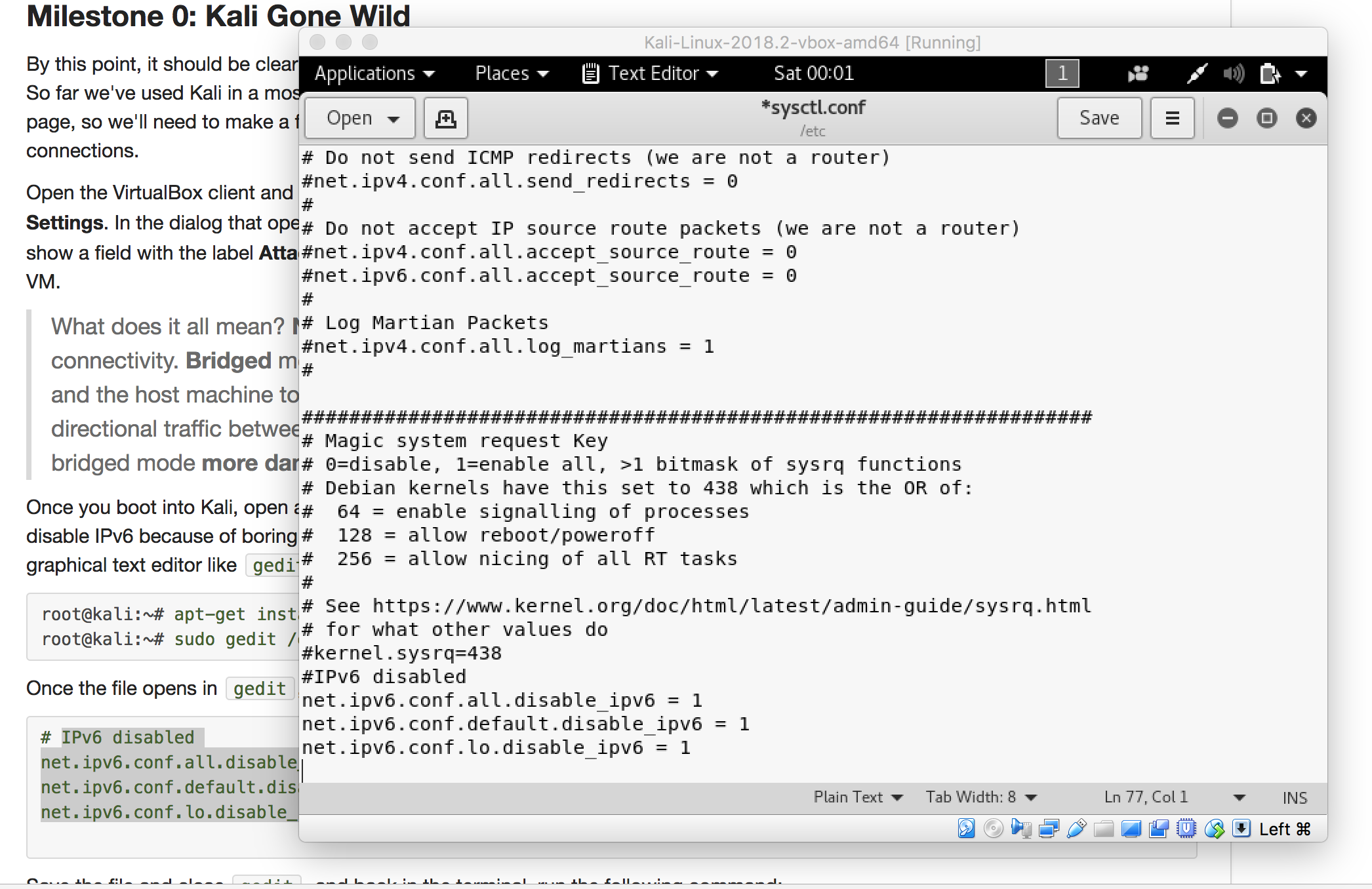
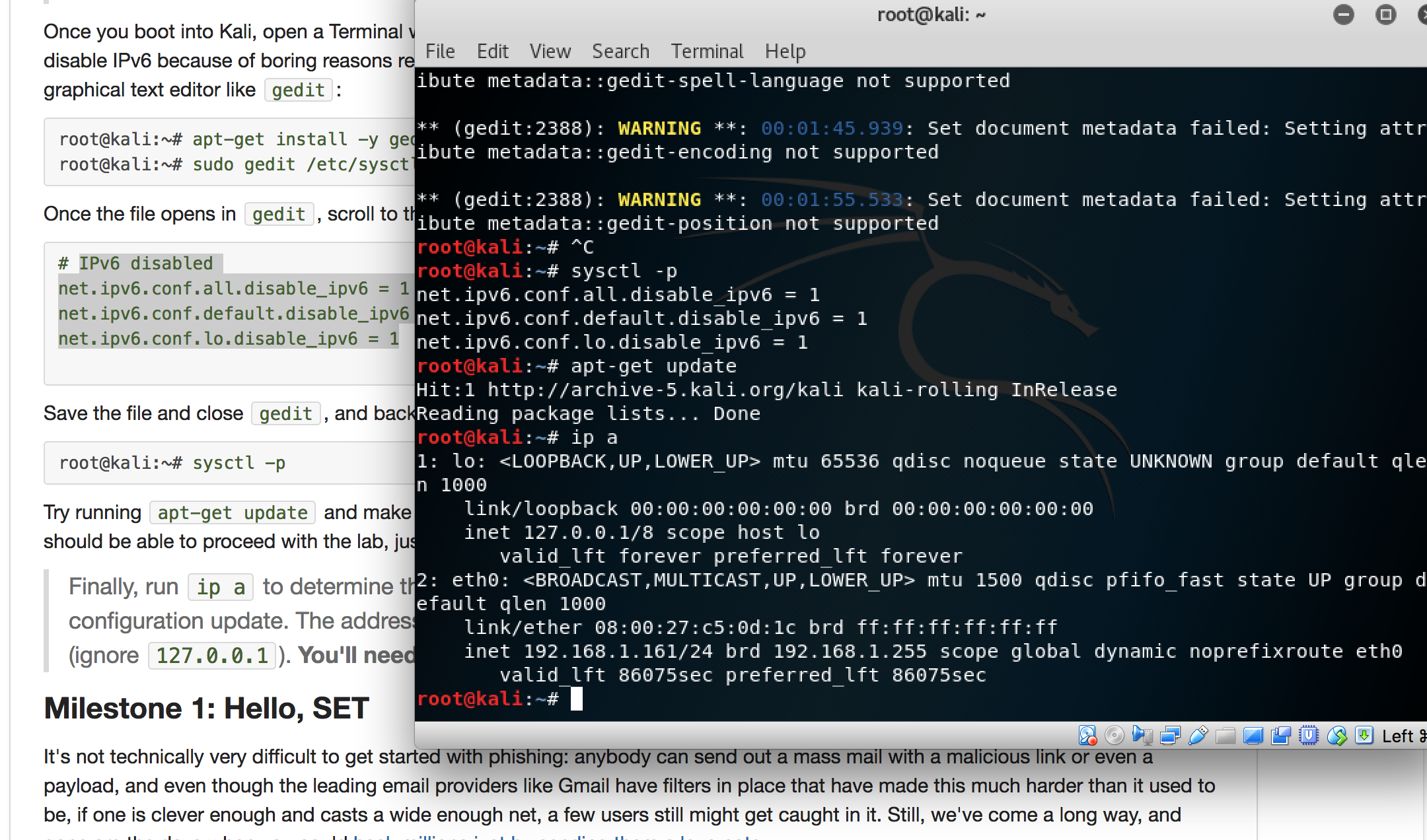
Kristen Trunnelle

IST 590

Week 10 Lab

**Milestone 0: Kali Gone Wild**





In Milestone 0, I had no problems. The few steps worked easily.

### Milestone 1: Hello, SET

### 

### 

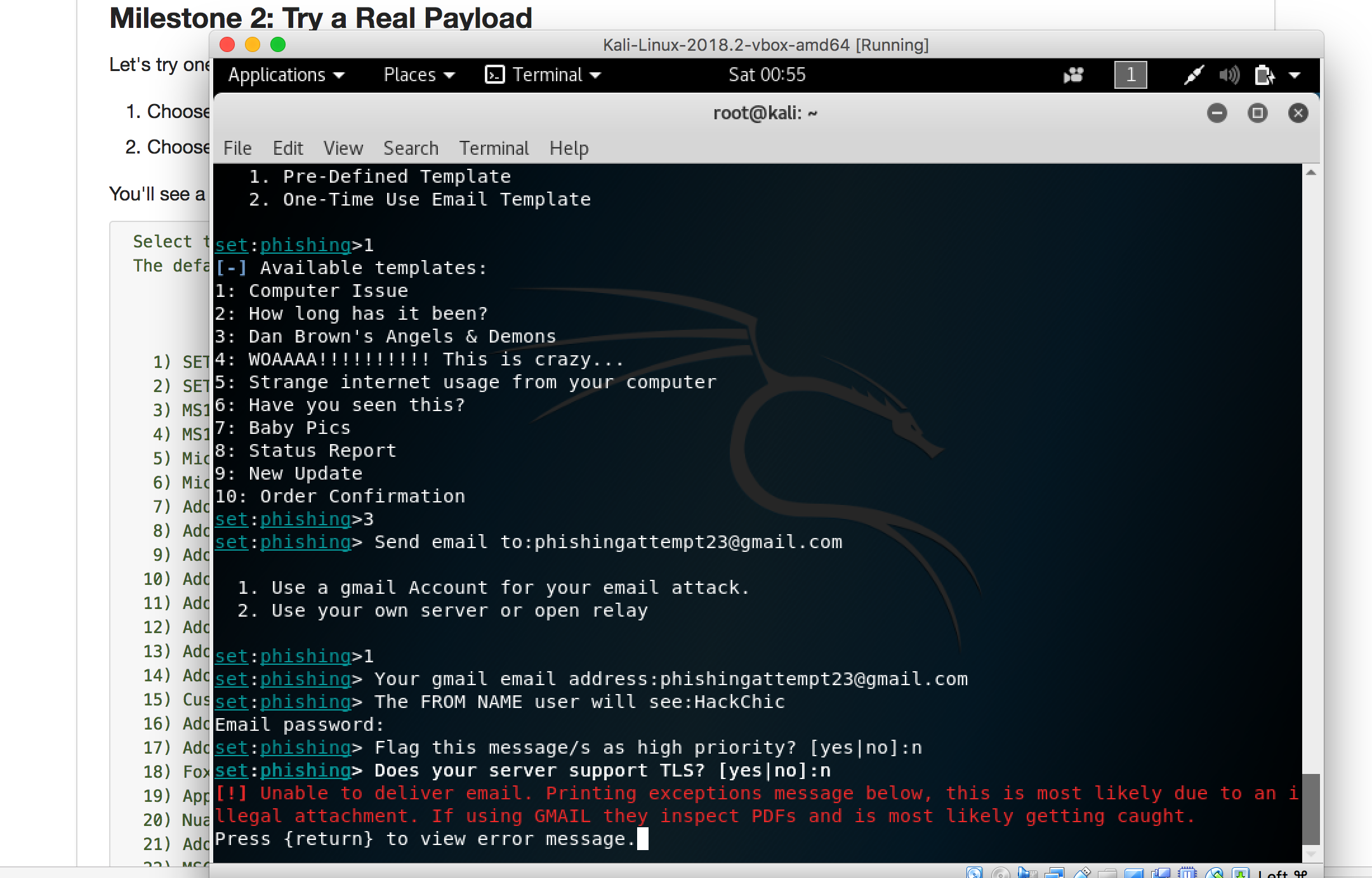
### 

### In milestone 1, I was able to run the set tool set with the given commands. When I made a fake email though and tried the commands, they worked on Kali but I didn’t get any email on the fake account like I was supposed to.

### Milestone 2: Try a Real Payload

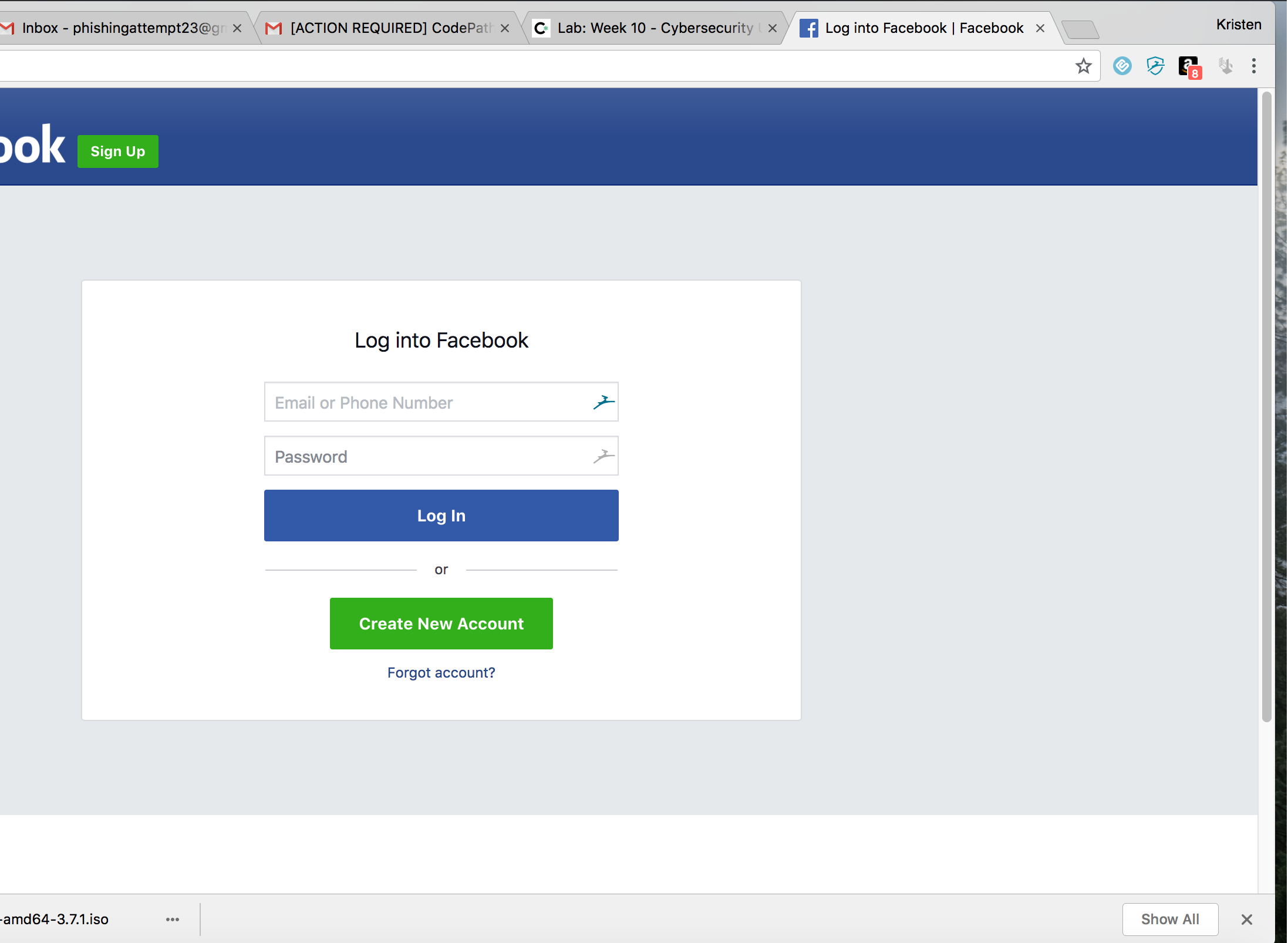
* Which two software companies are heavily represented on this list? Microsoft and Adobe

Which operating system would most of these exploits require? All versions of Microsoft Office prior to the release of the MS10-087 security patch



In milestone 2, all the steps worked.

### Milestone 3: Fakebook



I saw this page on both my laptop side and on the vm side.

### Milestone 6: SE In Situ

* What vulnerabilities were beyond the control of the user? Apple and Amazon having given partial credit card numbers (data management policies).
* What if anything could have been done by the user to mitigate the severity of the attack? Users could have not had all their accounts linked together, could have backed up their devices, and could have used two-factor authentication.

Now, think back to the fake Facebook login scenario above. Assuming a successful compromise, in which the user's Facebook username and password were successfully intercepted, answer the following:

* 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) use two form authentication such as something you have instead of just something you know. They can use a token of some sort.
* 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). A hacker can try them on tons of other sites that they are bound to work on, either the username or password, or both.