Kringlecon Lessonized

# Note to instructors

These lessons are available as one large file or broken down into individual lesson files so that you don’t have to hand out spoilers. I recommend against using the solutions as graded items, however; solutions to all Holiday Hack challenges are available on the Internet. Questions for the students to answer that require thought should be gradable.

Many of the lessons can be done in Windows, but some require the use of a Linux OS. If your lab allows VMware Workstation Player (free for educational use) or another hypervisor like Virtual Box, students should have no trouble doing these lessons. They do require Internet access, but other than that and access to Windows and Linux, nothing else is required.

These lessons do not have to be run straight through, as many can be standalone lessons. The Badge Manipulation lesson on SQL Injection is a good example. Data Repo Analysis and Dev Ops Fail could be combined for some interested in security of GitHub repositories. The only lessons that rely on previous lessons (other than for hints, which you can fix) are the Snort Terminal and PowerShell malware analysis lessons (Stop the Malware, Recover Alabaster’s Password, and Who Is Behind it All.)

Feel free to use any or all these lessons in your classes or texts. If you do use them, I ask that you let me know how it went. If you make improvements or run into problems, please contact me at [johnyork807@gmail.com](mailto:johnyork807@gmail.com) or @JohnYork\_r2 on Twitter.

I haven’t had a chance to teach these to my own class yet. I plan to do that this spring (2019). As I teach using them, I’m sure I will find things that need to be corrected and I will update this copy.