First Principles: Simplicity, Minimization, Layering

1. Time: 1-4
2. Lecture: No lecture
3. Activities
    a. Reference: OSSIM Overview - https://www.youtube.com/watch?v=wVxYiZ_Dl0Q
    b. Activity: Use the SIEM to push OSSIM client out to hosts
        i. https://www.youtube.com/watch?v=JVmvgLS81wk
    c. Activity: Log into the hosts and watch the activity on OSSIM
        i. Run a port-scan against a host on the floor and watch the activity
        ii. Run an exploit against OSSIM, and watch the activity.
        iii. Run a browser exploit against host on the floor and watch the activity
    d. Activity: Run vulnerability scan against clients on the floor
        i. Configure the Windows Firewall on some hosts and rerun the scan against the server
        ii. If OpenVAS is installed on Kali in the lab, use that as well. If not, use nmap's vulnerability scan scripts.
    e. Activity: Run a web application vulnerability scanner (OWASP ZAP) against the webserver