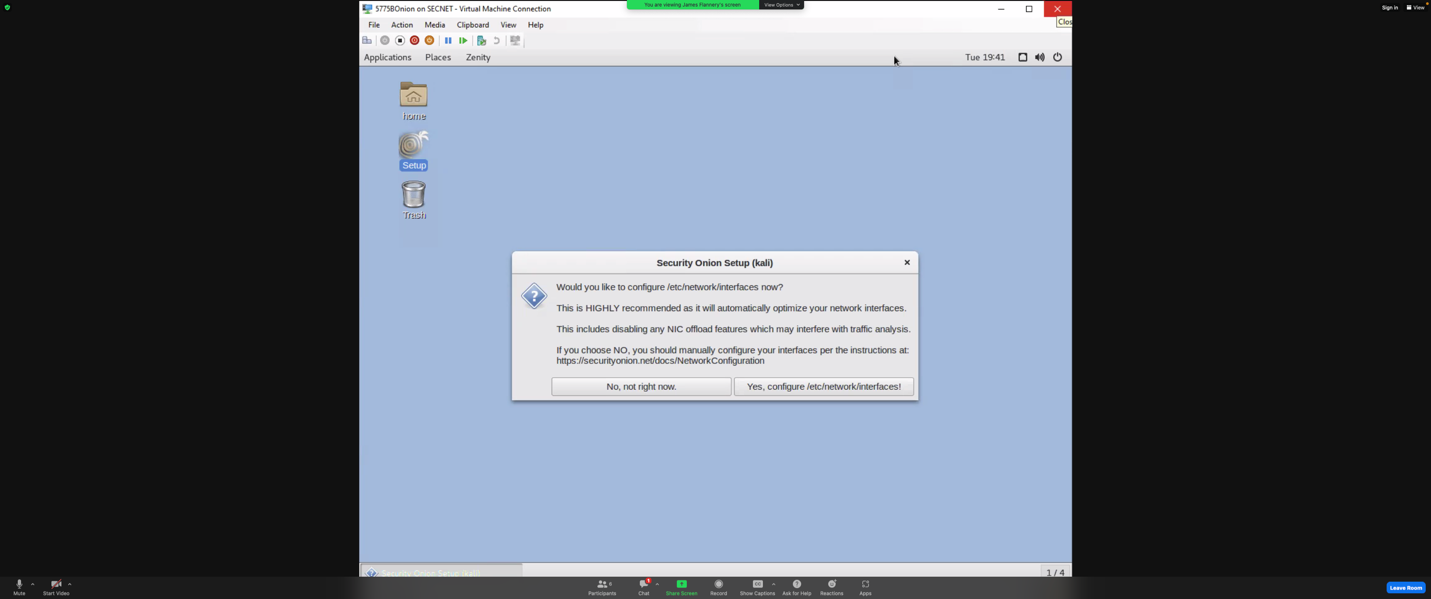
Team Buffalo

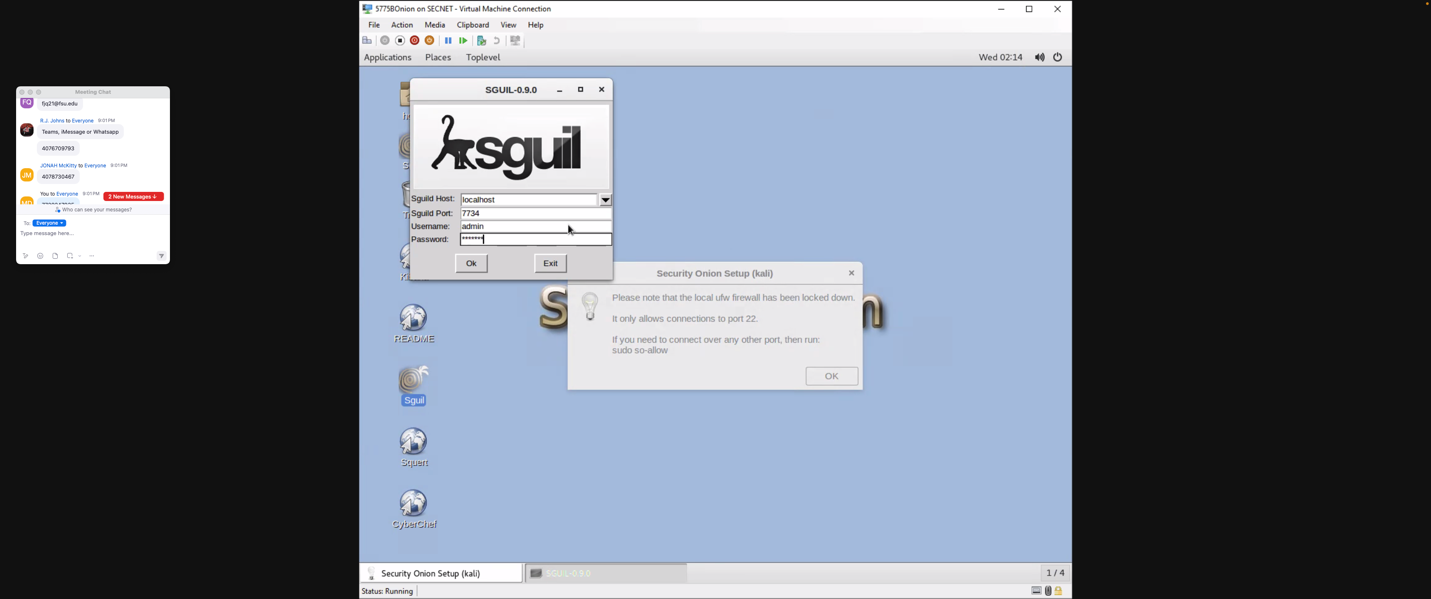
LIS5775

SecurityOnion Setup

Above is the first screen shot we took as a group. This shows the process of what steps to take to set up security onion. First it had us configure network interfaces.

A screenshot of a computer

Description automatically generatedThis screen shot shows that the network configuration was successful, and the step of configuring network interfaces is done. For the sguil interface to advance it also made us reboot which is what the pop-up textbox is stating.

This is where we needed to log into sguil. We used the standard FSU password for VM’s to keep sguil uniform in this process. (password not provided to protect university’s integrity)

A screenshot of a computer

Description automatically generatedThis is the sguil home menu. This is where you are able to look at the network interface you configure into sguil to monitor their traffic and see what takes place, when and where.