**ISEC 500 - Information Security Overview**

**Assignment 2 - Lab 2: Implementing Security Policies on Windows and Linux**

The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document.

**Part 1**

**challenge #1**



**challenge #2**



**challenge #3**



**challenge #4**

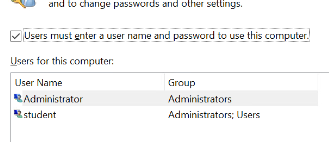


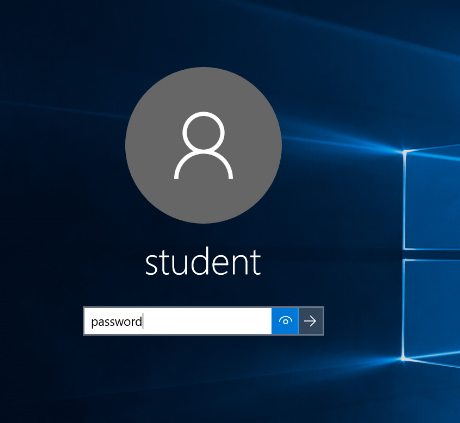
**challenge #5**

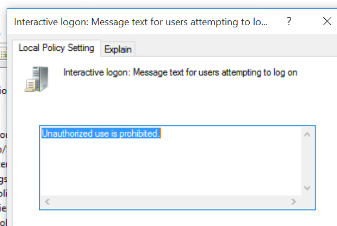


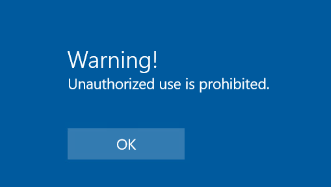
**challenge #6**

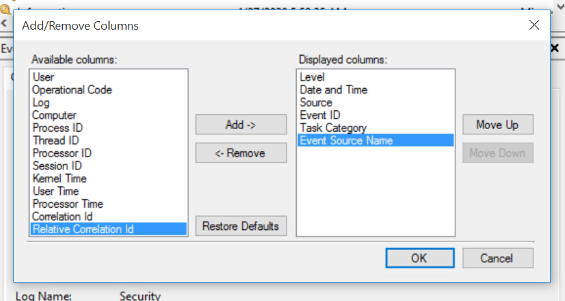
**Screenshots**

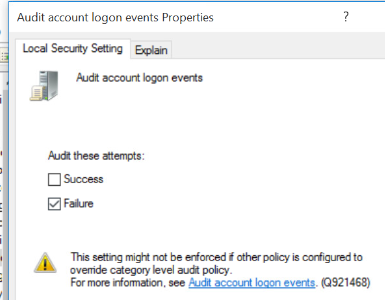


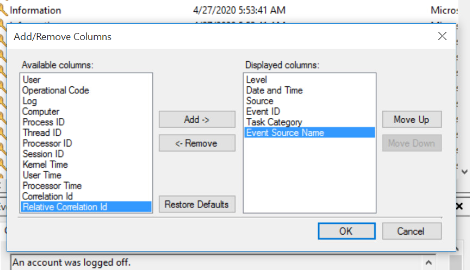


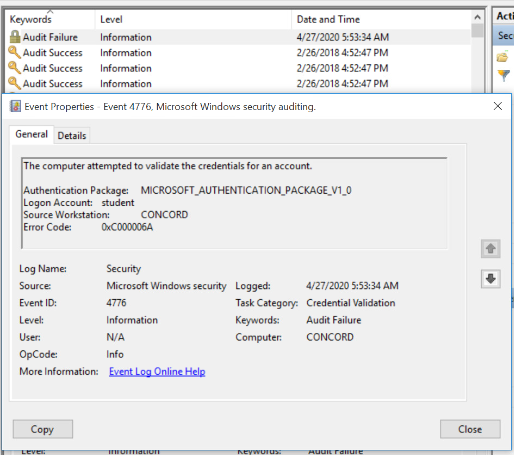


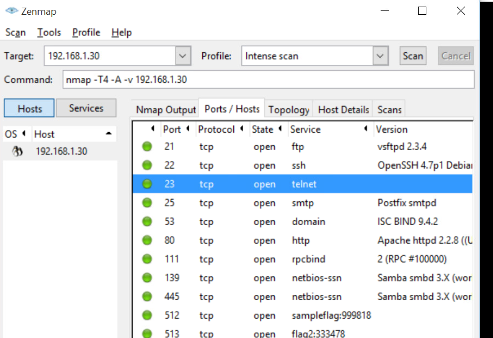


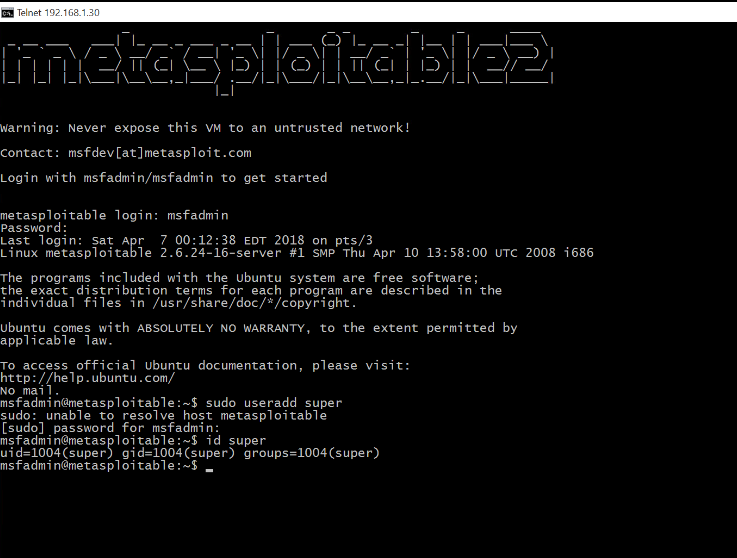


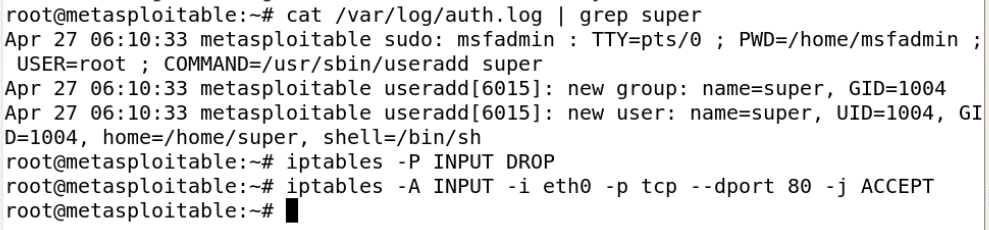


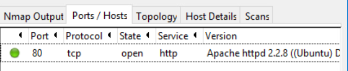












**PART 2**

I used netplwiz in the past when I wanted to disable the logon screen. Unchecking the option on netplwiz and then going to settings, accounts, sign in options, and choosing “never” for require sign-in allows you to go straight to the desktop. But I do use the password now.

This audit log feature can be really useful for tracking who is working on an insider attack without even letting them know they are being tracked.

And nmap is a very useful program for seeing which ports are active basically instantly. We were even able to drop all connection and open only port 80 and check it using nmap.

I appreciate how informative and related to real world these virtual labs are.