# Instructions

In this lab, students will learn about Machine/Virtual Machines (VMs) and the importance of Windows 10 Security Technical Implementation Guide (STIG), which is published as a tool to improve the security of Department of Defense (DoD) information systems.

# Assignment & Instructions

## Part I: Windows 10 Hardening

Download the Excel sheet provided on BeachBoard, go through the 25 items to harden your machine. Some cells have questions or will ask you to take screenshots (See Cell F). Please label those as per their respective cell (e.g row 2) just simply put a #2 or 2, etc. and include the screenshot or whatever work you are being asked to do. Once you are done, do the following to create a report file.

1. Open a CMD prompt as Administrator
2. Type the following à gpresult /r /v > <Enter Location Path of your file to be created>\<LastName.txt>

## Upload this file along with your report

## **Note: If you do not upload this file. Your lab will be incomplete, and you will receive a ZERO for this lab.**

## Part II:

1. Create a group policy to prevent all Users from Shut Down, Restart, Sleep and Hibernate commands
2. Create a group policy to prevent all Users from being able to access any type of removable media
3. Create a group policy to enforce password history, complexity, age
   1. Set it to remember the last 24 passwords you entered
   2. Set complexity requirements to enable
   3. Set the maximum password age to 30 days
4. Now create a group policy to remove all CLT+ALT+DEL options
5. Set settings to whole disk encrypt your VM.
6. Now create a Local User. Name it “**BugKiller**”. Make sure **BugKiller** is not part of the Administrators group, then take a screenshot.
7. Restart your machine, and log in using with user: **BugKiller**
8. Now shutdown the VM. Were you able to Shut Down the VM? If yes, explain how you did it? If not, explain why not?

**Hint: You will need to do some googling**