# Windows Unit 3 Lab Guide

Practice what you’ve just learned!

* [3.1 - Task Scheduler](#_3fhplj46hm74) 1
* [3.2 - GPEDIT](#_cmc3vmlhotpy) 1
* [3.3 - Event Logs](#_mncfvo7rlzbg) 1
* [3.4 - Backdoors](#_8wont0srhefm) 2

While you go through the exercises, make sure you understand why these topics are important in a security standpoint.

If you have any questions at any point, don’t hesitate to Google it or raise your hand!

### 3.1 - Task Scheduler

1. Try turning on firewall - after a while, it will turn off automatically. Fix this issue!
2. After finding out which task is causing the issue, try and find it in C:\Windows\System32\Tasks, then delete the task and observe the change in Task Scheduler
3. Try making a task of your own. Have it open Firefox every 5 minutes, or whatever you like!

### 3.2 - GPEDIT

1. Configure the settings that you’ve learned in the powerpoint. Assume that remote desktop is *required*.
2. Check out firewall, remote settings, and anything else you have configured. They should be grayed out.
3. Explore <https://www.stigviewer.com/> and <https://gpsearch.azurewebsites.net/> for a bit.
4. Try creating a backup of your settings using LGPO. You can download it here: [LGPO](https://www.microsoft.com/en-us/download/details.aspx?id=55319). Once you download the toolkit, unzip the LGPO file.
5. Once your backup is created, change those previous settings and save them. Try implementing your LGPO script, and check if they were changed back.

### 3.3 - Event Logs

1. Which account was the last to log in successfully to the system, other than you (should be a user who is part of the Users group)?
   1. What’s the Event ID for this event?
   2. Pro tip: if you aren’t sure of the exact ID, you can supply multiple event IDs and filter for Audit Success or Audit Failure. A successful login would be Audit Success; a failed login attempt would be Audit Failure.
2. Find the user who last failed a login attempt and when it occurred (should be a user who is part of the Users group).
   1. What’s the Event ID for this event?

### 3.4 - Backdoors

1. There is something listening on your computer… find out which port it is listening on, and delete it!
2. Something was causing it to start up when you logged in. Have you stumbled upon the reason in the last exercises?

If you have already finished, experiment with adding and removing roles/features. You may also check out the Windows Admin Center.

Credentials for Windows Admin Center

* Username: Administrator
* Password: <blank, don’t supply a password>