

**PC Hardening**

**Introduction and/or Background**

Alyx has researched the threats to her PC and wants to take the first steps at hardening, or securing it.

**Objectives**

In this project/lab the student will:

* Harden a Desktop PC

**Equipment/Supplies Needed**

* Windows 10 Virtual Machine

**Assignment**

*Secure the BIOS*

1. In VMware Workstation Pro, locate your Win10-xx Virtual Machine. Right click it, then click Settings.
2. In the Virtual Machine Settings window, click the Options Tab. In the Advanced Setting, change the Firmware Type from UEFI to BIOS. Ensure Enable Secure Boot is not selected. Click Ok.
3. In the Library pane, right click the VM, mouse over Power, then click Power On to Firmware to enter the BIOS.
4. In the PhoenixBIOS Setup Utility, move to the Security tab, select Set Supervisor Password, then press Enter.
5. Enter your desired password twice, then press Enter. At the Setup Notice confirmation popup, take a screenshot.
6. Move to Password on boot, press Enter, and select Enable. Press Enter again. Take a screenshot.
7. Move to the Exit menu, move to Exit Saving Changes, and press Enter. At the Setup Confirmation popup, select Yes and Press Enter.
8. Your VM will reboot and should require you to type in a password to continue.
9. Before continuing the lab, change your firmware type back from BIOS to UEFI as indicated previously.

*Disable Autoplay*

1. In Windows Search, type Autoplay, then choose AutoPlay settings.
2. Slide the switch under “Use AutoPlay for all media and devices” to the Off position. Take a Screenshot.

*Encrypt a Virtual Machine*

1. Power off your VM again. Right click your VM name and click Settings.
2. In the Virtual Machine Settings window, click the Options tab.
3. Click the Access Control setting, then click the Encrypt button.
4. In the Encrypt Virtual Machine window, enter a memorable password in both fields, then click Encrypt.
5. When the process completes, you’ll see a message on the Virtual Machine Settings window indicating the VM is encrypted. Take a screenshot.

*Enable BitLocker*

1. In the Virtual Machine Settings Window, click the Hardware tab, then click Add.
2. In the Add Hardware Wizard, click Trusted Platform Module, then click Finish.
3. Click Ok, then start the VM again.
4. Open Control Panel, click System and Security, then click BitLocker Drive Encryption.
5. Click Turn on BitLocker. Insert your USB drive into your host PC and Connect it to your VM.
6. In the BitLocker Drive Encryption wizard, specify you’d like to Save your recovery key to a file. Choose a location on the USB drive to save the key, then click Save. Click Next.
7. In the “Choose how much of your drive to encrypt” screen, click “Encrypt entire drive” and click Next.
8. In the “Choose which encryption mode to use” screen, click “New encryption mode” and click Next.
9. In the “Are you ready to encrypt this drive?” screen, check Run BitLocker system check, then click Continue.
10. Restart your VM to complete the encryption process.
11. Open the BitLocker Drive Encryption screen again and show that your drive is now encrypted. Take a screenshot.

*Review Privacy Settings*

1. Right click the Windows menu and click Settings.
2. In the Windows Settings menu, click Privacy.
3. Review and turn off the privacy options in the General screen. Take a screenshot.
4. In the App permission section on the left, click Location.
5. Review the location permissions, then turn them all off. Take a screenshot.
6. Scroll down and Clear location history on the device. You should see a checkbox appear by the Clear button. Take a screenshot.
7. In the App permission section on the left, click Camera.
8. Review the camera permissions, then turn them all off. Take a screenshot.
9. In the App permission section on the left, click Microphone.
10. Review the microphone permissions, then turn them all off. Take a screenshot.

*Update the Operating System*

1. Right click the Windows menu and click Settings.
2. Click Update & Security.
3. Your Operating System may need some Windows Updates. Download and install all current updates by pressing the Download button. This may take some time and may require some restarts.
4. When the updates are complete, you should see a confirmation message. Take a screenshot.

**Rubric**

Checklist/Single Point Mastery

|  |  |  |
| --- | --- | --- |
| Concerns  Working Towards Proficiency | Criteria  Standards for This Competency | Accomplished  Evidence of Mastering Competency |
|  | Criteria #1: Student correctly completed step 5 on Secure the BIOS#1  (10 points) |  |
|  | Criteria #2: Student correctly completed step 6 on Secure the BIOS (10 points) |  |
|  | Criteria #3: Student correctly completed step 2 on Disable AutoPlay (5 points) |  |
|  | Criteria #4: Student correctly completed step 5 on Encrypt a VM (10 points) |  |
|  | Criteria #5: Student correctly completed step 11 on Enable BitLocker (10 points) |  |
|  | Criteria #6: Student correctly completed step 3 on Review Privacy Settings (5 points) |  |
|  | Criteria #7: Student correctly completed step 5 on Review Privacy Settings (10 points) |  |
|  | Criteria #8: Student correctly completed step 6 on Review Privacy Settings (10 points) |  |
|  | Criteria #9: Student correctly completed step 8 on Review Privacy Settings (10 points) |  |
|  | Criteria #10: Student correctly completed step 10 on Review Privacy Settings (10 points) |  |
|  | Criteria #11: Student correctly completed step 4 on Update the Operating System (10 points) |  |