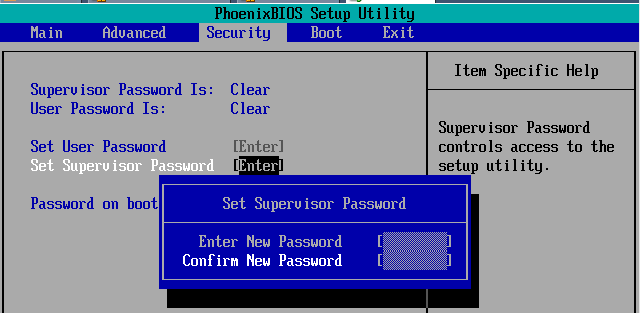
**Lab 8: Bypassing a BIOS Password**

**What You Need for this lab**

**•** VMware Workstation or VMware Player.

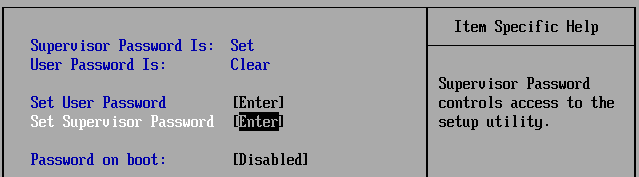
## Assigning a BIOS Password

1. Open a virtual machine (VM), but don't start it. It doesn't matter what OS is installed on the VM. If you don't have a VM handy, just create a new one.
2. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power ON to BIOS**". If that menu item is not there, you may have an old version of VMware, or VMware Player. You can probably still do the project by starting the machine, clicking quickly in it, and pressing F2 to open the BIOS. If the machine boots up too quickly for you to get into the BIOS, power the virtual machine down, find its .vmx file, and add this line to the end of it:

bios.bootdelay = 5000

Complete instructions for the process are here:

http://www.howtogeek.com/howto/16876/how-to-increase-the-vmware-boot-screen-delay/

1. When the "PhoenixBIOS Setup Utility" screen appears, click in the VM to capture the keyboard. Then use the keyboard arrow keys to select the **Security** menu. Press **Enter** to "**Set Supervisor Password**".
2. Enter a BIOS password of **12345678** in both boxes, as shown to the right on this page. Use the **Enter** key to move from one box to the other.
3. After entering the password in both fields, press **Enter**. A "Setup Notice" box appears saying "Changes have been saved.". Press **Enter** again.
4. Your BIOS screen should now show that the "Supervisor Password" is "Set", as shown to the right on this page.
5. Press F10 and then Enter to save changes.
6. When the VM restarts, from the VMware Workstation menu bar, click **VM**, **Power**, "**Power Off**"

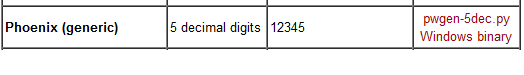
## Entering the Wrong Password Three Times

1. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power ON to BIOS**".
2. A blue box asks you to "Enter Password". Enter something wrong, like **X**, and press Enter. Repeat the process three times.
3. A "System Disabled" box appears, as shown to the right on this page, with a code number visible.

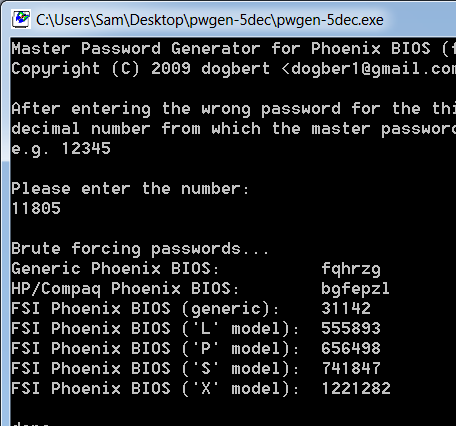
## Saving a Screen Image

1. Make sure your screen shows the "System Disabled" box, with the code number visible.
2. Press Ctrl+Alt to release the keyboard from the VM. Press the PrntScrn key to save the screen image. Open Paint and paste in the image. Save it as **Lab-Proj 8a from YOUR NAME**.

## Downloading the BIOS Keygen

1. Open a Web browser and go to **dogber1.blogspot.com/2009/05/table-of-reverse-engineered-bios.html**
2. In the "Phoenix (generic) line, download the "**Windows binary**" link (or Lab-Proj.08\_pwgen-5dec.zip from the instructor).
3. On your desktop, right-click the **pwgen-5dec.zip** and click "**Extract All…**". Click **Extract**.

## Using the Keygen

1. A box pops up showing a **pwgen-5dec.exe** file. Double-click that file. If a warning box pops up, click **Run**.
2. A command prompt window opens. Click in that box and enter the number from your "System Disabled" message.
3. It finds a series of passwords. Notice that the passwords you get are not the same ones I got, and don't include the password is not the one you entered--but it will probably still work.

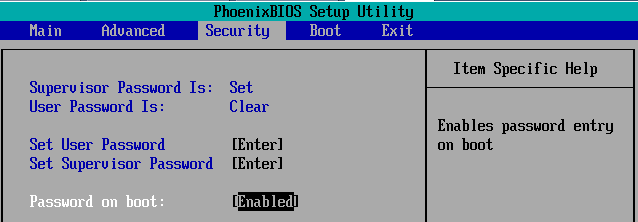
## Saving a Screen Image

1. Make sure your screen shows the "**Generic Phoenix BIOS**" line, with a generated password visible that is different from the example above.
2. Press Ctrl+Alt to release the keyboard from the VM. Press the PrntScrn key to save the screen image. Open Paint and paste in the image. Save it as **Lab-Proj 8b from YOUR NAME**.

## Testing the Generated Password

1. Press Ctrl+Alt to release the keyboard from the VM.
2. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power Off**". Click "**Power off**".
3. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power On to BIOS**".
4. A blue box asks you to "Enter Password". Enter the password from the "Generic Phoenix BIOS" line in the keygen--when I did it, it was **fqhrzg**
5. If the password works, you will see the BIOS open. If it fails, run the keygen again. Every time you run it, it finds different passwords, and they don't all work. But it worked for me two out of three times.

## Setting a Boot Password

1. In the Security menu, press the down-arrow to select the "**Password on boot**" item. Press **Enter** to select it. A blue box pops up. Press the down-arrow key to highlight **Enabled** and press **Enter**.
2. Your BIOS screen should now show that the "Password on boot" is "Enabled", as shown to the right on this page.
3. Press F10 and then Enter to save changes.

## Entering the Wrong Password Three Times

1. A blue box asks you to "Enter Password". Enter something wrong, like **X**, and press Enter. Repeat the process three times.
2. A "System Disabled" box appears, as shown to the right on this page, but this time the code number is 00000.

## Saving a Screen Image

1. Make sure your screen shows the "**System Disabled**" box, with a number of **00000**.
2. Press Ctrl+Alt to release the keyboard from the VM. Press the PrntScrn key to save the screen image. Open Paint and paste in the image. Save it as **Lab-Proj 8c from YOUR NAME**.

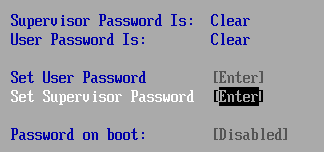
## Using the Keygen

1. Run the keygen and enter the code of **00000**. It generates a password.

## Testing the Generated Password

1. Press Ctrl+Alt to release the keyboard from the VM.
2. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power Off**". Click "**Power off**".
3. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power On** ".
4. A blue box asks you to "Enter Password". Enter the password from the "Generic Phoenix BIOS" line in the keygen. It won't work--obviously 00000 is not the real code. This keygen works for BIOS passwords, but not for boot passwords.

## Clearing the Passwords

1. Press Ctrl+Alt to release the keyboard from the VM.
2. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power Off**". Click "**Power off**".
3. From the VMware Workstation menu bar, click **VM**, **Power**, "**Power On to BIOS**".
4. A blue box asks you to "Enter Password". Enter the password you chose originally: **12345678**
5. Use the arrow keys to get to the Security page. Highlight "**Password on Boot**" and press **Enter**. Use the arrow keys to highlight **Disabled** and press **Enter**.
6. In the Security menu, set the "Password on boot" to **Disabled**.
7. Use the arrow keys to highlight "**Set Supervisor Password**" and press **Enter**.
8. In the blue "Set Supervisor Password" box, enter **12345678** in the first line. Press **Enter** four times.
9. Your BIOS screen should now show that both passwords are Clear, as shown to the right on this page.
10. Press F10 and then Enter to save changes.

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 8.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 8 From YOUR NAME**", replacing "YOUR NAME" with your real name.