**Hardening pfSense**

Open your pfSense virtual machine (path should be something like *v:\pfsense\pfsense.vmx*)

1. Navigate to the **System>Advanced>Admin Access** area in the pfSense webConfigurator page.

Look over the following settings. For each, provide:

* 1. A short description
  2. Your recommended setting
  3. If adjusting the setting would considered *reducing exposure* or *implementing protections* (or both)
  4. Screenshot of the adjusted setting

Note: If you need more information on a particular setting, refer to the **Configuration** section of the pfSense book.

* Protocol
* Max Processes
* WebGUI Login Autocomplete

Enable *Secure Shell Server* by making sure the box is checked.

* Do some quick research about SSH. Why would it be a good protocol to use when managing the firewall?
* Open *putty.exe* on the desktop.
  + Make sure it is set to SSH in the “Connection type” section.
  + Type the management IP address of your firewall (this should be the IP address assigned to your firewalls LAN interface), then click “Open”
* Take a screenshot of the putty window showing the pfSense console and paste it below:

*paste screenshot here*

1. Navigate to the **System>User Manager** area in the pfSense webConfigurator page

When installing pfSense the default password was left in place for ease of getting started. This is not good!

* Click the  icon to edit the account and set a more complex password of *Cnt262@admin*

Using “anonymous” accounts like ‘admin’ makes it difficult to track who made certain changes to a firewall’s settings.

* Create a new account using your first initial and last name. Use a password only you know.
* After you have created the account, take a screenshot of the Users page showing this account and paste it below:

*paste screenshot here*

1. Navigate to the **System>Advanced>Firewall & NAT** area in the pfsense webConfigurator page

Read the summary for the *IP Random id generation* setting.

* Which step in the hacking process would this setting make more difficult for an attacker?

1. Navigate to the **System>Update>System Update** area in the pfSense webconfigurator page

* What is the *Current Base System* version?
* What is the *Latest Base System* version?
* If there is a newer version, should you update as part of hardening pfSense? Why or why not?

1. Navigate to the **Diagnostics>Backup & Restore** area in the pfSense webconfigurator page

* Would backing up the configuration be an essential part of securing the firewall? Why or why not?
* Leave the “Encrypt this configuration file” box unchecked and then click the “Download configuration as XML”
  + Locate this .xml file in your Downloads folder and open it with Wordpad.
  + What type of information is in this file? (be sure to scroll all the way through the file)
* Assume someone copied a firewall configuration backup file to a USB drive and forgot it at Starbucks.
  + How would this file assist a potential attacker shortcut the scanning and enumeration portions of the hacking process?
* Configure the appropriate setting to implement protection for these file contents. Take a screenshot of your recommended backup settings and paste it below.

*paste screenshot here*

* After applying your backup settings from the previous step, download the configuration again.
  + Open the new backup file with Wordpad and take a screenshot of the contents. Paste the screenshot below.

*paste screenshot here*

* + How does this reduce your exposure in the event you inadvertently left the configuration on a USB at Starbucks, or in any other insecure location?
* Navigate the pfSense webconfigurator interface and locate at least one other setting (from any menu area) that would be beneficial to use (or change) at part of hardening the firewall (and include how/why it helps improve security)