**Hardening pfSense**

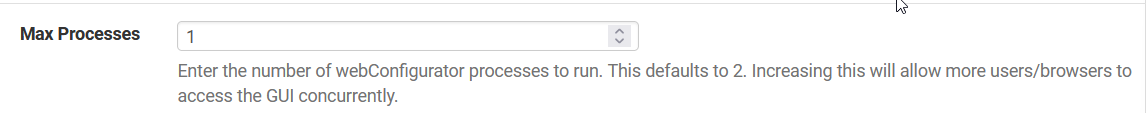
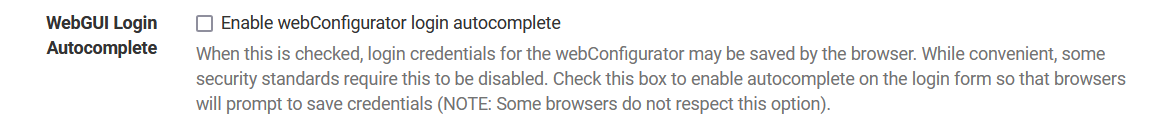
Open your pfSense virtual machine (path should be something like *v:\pfsense\pfsense.vmx*)

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
  1. Allows either the use of HTTP or HTTPS
  2. My recommended setting would be HTTPS if the Webgui is being accessed remotely. Otherwise, HTTP is fine.
  3. The default is HTTPS, so if the user decided to switch to HTTP, then ensuring only trusted connections are allowed is important.
  4. 
* Max Processes
  1. This setting determines how many instances of the web-gui allowed to be active.
  2. The recommended setting should be 1, I think any changes should try to be done through the terminal and not through the gui.
  3. I would enforce a MFA method to ensure that whoever is using the web-gui is trusted.
  4. 
* WebGUI Login Autocomplete
  1. This allows the users web browser to save the login credentials so it can auto login.
  2. My recommended setting would be to disable this option.
  3. Similar to the previous answer, enforcing a MFA method to ensure that even if credentials are stolen, an attacker would need something else.
  4. 

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? SSH would be a good protocol to use when managing a firewall due to the efficiency that can come from making changes through a command line interface.
* 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:

A computer screen shot of a computer program

Description automatically generated

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:

A screenshot of a computer

Description automatically generated

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? In the hacking process, this would make the reconnaissance phase more difficult as the traffic leaving is obscured.

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

* What is the *Current Base System* version? 2.7.0
* What is the *Latest Base System* version? 2.7.0
* If there is a newer version, should you update as part of hardening pfSense? Why or why not? You should update, only after reading the patch notes and determining if the changes made warrant an upgrade. For example, there could be changes that cause your current configuration to break so reading the patch notes before updating is crucial.

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? Backing up the configuration is not an essential part of securing the firewall, however, backing up the configuration gives the firewall admins the peace of mind that if something happens, the configuration file is saved.
* 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) The .XML is the configuration file, and when changes are made through the web-gui, the .XML file is being modified. It contains everything.
* 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? This file would give an attacker all of the information they need about the firewall. If the attacker can communicate with the firewall, they gain access. The attacker would also know what kind of rules are setup on the firewall, and could configure their attacks to work against the firewall.
* Configure the appropriate setting to implement protection for these file contents. Take a screenshot of your recommended backup settings and paste it below.

A screenshot of a computer

Description automatically generated

* 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.

A screen shot of a computer

Description automatically generated

* + 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? The attacker would need to decrypt the encrypted file, this reduces my exposure by adding an extra layer of security to my plain text file.
* 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) I found an option at the bottom of System > Advanced called “Password protect the console menu.” This feature adds an additional password to the console menu that is different from the web-gui logins. Maybe the admin account password is compromised, but because your console password is different, the attacker cannot access the console.