11.3 Lab: Implement Intrusion Prevention

Candidate: COMPTIA COMPTIA ()
Time Spent: 00:55

Score: 0%

Task Summary

Required Actions

- ✕ Configure Snort rules Show Details
- ✕ Configure Sourcefire OpenAppID Detectors Show Details
- ✕ Configure the Rules Update Settings Show Details
- ✕ Configure General Settings Show Details
- ✕ Configure the Snort Interface settings for the WAN interface Show Details

Explanation

Complete this lab as follows:

1. Sign in to the pfSense management console.
   a. In the Username field, enter **admin**.
   b. In the Password field, enter **P@ssw0rd** (zero).
   c. Select **SIGN IN** or press **Enter**.
2. Access Snort Global Settings.
   a. From the pfSense menu bar, select **Services** > **Snort**.
   b. Under the *Services* breadcrumb, select **Global Settings**.
3. Configure the required rules to be downloaded.
   a. Select **Enable Snort VRT**.
   b. In the Snort Oinkmaster Code field, enter **992acca37a4dbd7**. You can copy and paste this from the scenario.
   c. Select **Enable Snort GPLv2**.
   d. Select **Enable ET Open**.
4. Configure the Sourcefire OpenAppID Detectors to be downloaded.
   a. Under Sourcefire OpenAppID Detectors, select **Enable OpenAppID**.
   b. Select **Enable RULES OpenAppID**.
5. Configure when and how often the rules will be updated.
   a. Under Rules Update Settings, use the **Update Interval** drop-down menu to select **4 DAYS**.
   b. For Update Start Time, change to **00:10** (12:10 a.m. in 24-hour format).

c. Select **Hide Deprecated Rules Categories**.

6. Configure Snort General Settings.
   a. Under General Settings, use the **Remove Blocked Hosts Interval** drop-down menu to select **1 Day**.
   b. Select **Startup/Shutdown Logging**.
   c. Select **Save**.
7. Configure the Snort Interface settings for the WAN interface.
   a. Under the *Services* breadcrumb, select **Snort Interfaces** and then select **Add**.
   b. Under General Settings, make sure **Enable interface** is selected.
   c. For Interface, use the drop-down menu to select **WAN (CorpNet_pfSense_L port 1)**.
   d. For Description, use **Snort-WAN**.
   e. Under Alert Settings, select **Send Alerts to System Log**.
   f. Select **Block Offenders**.
   g. Scroll to the bottom and select **Save**.
8. Start Snort on the WAN interface.
   a. Under the Snort Status column, select the ***arrow*** to start Snort.
   b. Wait for a checkmark to appear, indicating that Snort was started successfully.