11.3.5 Implement Intrusion Prevention

Your Performance

Your Score: 5 of 5 (100%) Pass Status: **Pass**

Elapsed Time: 2 minutes 14 seconds Required Score: 100%

Task Summary

Required Actions

✓ Configure Snort rules Hide Details

- ➕ Enable Snort VRT
- ➕ Enter the Snort Oinkmaster Code of 359d00c0e75a37a4dbd70757745c5c5dg85aa
- ➕ Enable Snort GPLv2
- ➕ Enable ET Open

✓ Configure Sourcefire OpenAppID Detectors Hide Details

- ➕ Enable OpenAppID
- ➕ Enable RULES OpenAppID

✓ Configure the Rules Update Settings Hide Details

- ➕ Use the Update Interval of 1 Day
- ➕ Use an Update Start Time of 01:00
- ➕ Hide Deprecated Rules Categories

✓ Configure General Settings Hide Details

- ➕ Use the Remove Blocked Hosts Interval of 1 HOUR
- ➕ Enable Startup/Shutdown Logging

✓ Configure the Snort Interface settings for the WAN interface Hide Details

- ➕ WAN interface is enabled
- ➕ Description: WANSnort
- ➕ Send Alerts to System Log enabled
- ➕ Block offenders enabled
- ➕ Snort started on the WAN interface

Explanation

Complete this lab as follows:

1. Sign into 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 the 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 *Sort Oinkmaster Code* field, enter **359d00c0e75a37a4dbd70757745c5c5dg85aa**. 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 **1 Day**.
   b. For Update Start Time, change to **01:00**.
   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 HOUR**.
   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 (PFSense port 1)**.
   d. For Description, use **WANSnort**.
   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**.
   b. Wait for a checkmark to appear, indicating that Snort was started successfully.