Lab 4: Adding a Snort IDS to pfSense

Introduction

In this exercise, we'll integrate Snort into the pfSense firewall to add IPS functionality, focusing on prevention rather than just detection. This configuration will help block potential threats from both external and internal sources. By placing active controls between an untrusted zone (enterprise/IDMZ) and a trusted zone (industrial network), we mitigate the risk of compromises before they can affect production processes.

Objectives for this assignment:

1. Installation and Initial Setup
2. Configuration of Snort Interfaces
3. Test Snort Configuration

**Submission:** You need to submit a detailed lab report, with screenshots, to describe what you have done and observed. Questions will be defined as you progress through the lab. The lab report will be compiled as a Word document and submitted on Brightspace by **March 3rd at 12:59 PM.**

*Objective 1: Installation and Initial Setup*

***Instructions:***

1. Access the pfSense Web Portal:

* Open your browser and log in to the pfSense web portal

1. Navigate to the Package Manager:
   * Go to **System** > **Package Manager**.

**A screenshot of a computer

Description automatically generated**

1. **Install the Snort Package:**
   * + Click on the **Available Packages** tab and search for **Snort**.

A screenshot of a computer

Description automatically generated

* + - Click **Install** and confirm to begin the installation process.

1. **Configure Global Settings:**
   * Once installed, navigate to **Services** > **Snort** to access the Snort Interfaces Configuration page.
   * Switch to the **Global Settings** tab and configure the following:

* **Enable Snort VRT**: Enter your Oinkmaster code from Security Onion.
  + - **Enable Snort GPLv2**
    - **Enable ET Open**
    - **Enable OpenAppID**
    - **Enable AppID Open Text Rules**

**A screenshot of a computer

Description automatically generated**

Scroll down to set the following:

* + - **Update Interval**: 12 HOURS
    - **Update Start Time**: Set a random time (e.g., 00:14)
    - **Remove Blocked Hosts Interval**: 6 HOURS
    - **Startup/Shutdown Logging**

**A screenshot of a computer

Description automatically generated**

* Click **Save** to apply these configurations.

1. **Force Initial Rule Update:**

* Switch to the **Updates** tab and click **Force Update** to start the initial rule update.

A screenshot of a computer

Description automatically generated

* Verify the update by checking for an MD5 signature with the current time and date.

*Objective 2: Configuring Snort Interfaces*

1. **Add a New Snort Interface:**
   * Go to the **Snort Interfaces** tab and click **Add** to create a new interface.
   * Configure the initial screen as follows:
     + **Interface**: WAN (to protect the external network interface)
     + **Send Alerts to System Log**: Enable to forward alerts to the pfSense system log.
     + **System Log Priority**: LOG\_NOTICE (for more verbose alerting)
     + **Block Offenders**: Enable to convert Snort from an IDS to an IPS. Use **Legacy Mode** and block both source and destination IPs.

**A screenshot of a computer

Description automatically generated**

* + Leave other settings as default and click **Save**.

1. **Set IPS Policy:**
   * Switch to the **WAN Categories** tab and check the **Use IPS Policy** option.
   * Choose **Balanced** for the IPS Policy Mode.

**A screenshot of a computer

Description automatically generated**

* + Click **Save** to finalize the configuration.

1. **Start Snort:**
   * Navigate to **Services** > **Snort** > **Interfaces** and click **Start Snort on this interface**.
   * Verify that Snort is monitoring traffic on the WAN interface from the **Service Status** widget on the main pfSense screen.

**A screenshot of a computer

Description automatically generated**

*Objective 3: Testing Snort Configuration*

1. **Generate a Snort Alert:**
   * On a computer within the network protected by pfSense, open a browser and go to ‘**http://testmyids.ca’**
   * Initially, the page will load, but upon refresh, it will be blocked by pfSense.
   * This occurs because Snort is operating in Legacy Mode, inspecting packet copies rather than inline inspection. Switching to Inline Mode increases security but may have hardware requirements.

**A screenshot of a computer

Description automatically generated**

1. **View Snort Alerts:**
   * Alerts can be viewed on the main dashboard or by navigating to **Services** > **Snort** > **Alerts**.

**A screenshot of a computer

Description automatically generated**

* + Check the **Blocked** tab to see the IP addresses that have been blocked.

**A screenshot of a computer

Description automatically generated**

1. **Verify Alerts in Elasticsearch:**
   * Search for a **MALWARE-OTHER** message in Kibana's Discovery page to ensure the alert was logged in the Elasticsearch database.

**A screenshot of a computer

Description automatically generated**

Summary:

This exercise demonstrated how to integrate and configure Snort on a pfSense firewall, adding an IPS layer to protect the network's perimeter. With this setup, all detections from Snort are logged into the ELK event database, enabling correlation, visualization, and alerting on security events.