Intrusion Protection System Lab

Ryan Coon

CYB-525

Dr. Emmett Ward

December 18, 2024

Part 1:

Screenshots:

A screenshot of a computer

Description automatically generated

Logged into pfsense firewall, click system, package manager. Then click available packages. Once it loads search for snort.

A screenshot of a computer

Description automatically generated

Click install then confirm. Snort will now begin the installation phase.

A screenshot of a computer

Description automatically generated

The installation phase was pretty quick. You will receive a success message upon a successful installation.

A screenshot of a computer

Description automatically generated

Once installation is finished, click services then click snort.

A screenshot of a computer

Description automatically generated

Click on global setting and check the box to enable download of rules. Then click to sign up for a free registered users account to obtain an oinkmaster code.

A screenshot of a computer

Description automatically generated

Fill out the registration page and sign up.

A screenshot of a computer

Description automatically generated

Once submitted, you must check your email and confirm your account.

A screenshot of a computer

Description automatically generated

After you confirm your account you will then login. It will take you to the account page.

A screenshot of a computer

Description automatically generated

Click on oinkcode and copy it. This will be what we need to enter into pfsence for snort.

A screenshot of a computer

Description automatically generated

Add in your oinkcode and click the enable snort GPLv2.

A screenshot of a computer

Description automatically generated

Click down on the checkboxes to enable emerging threats downloads, download sourcefire openappid detectors, download appid open text rules. Set to update daily and to never remove blocked hosts.

A screenshot of a computer

Description automatically generated

Scroll back to the top and click updates. Under update your rule set, click update rules.

A screenshot of a computer

Description automatically generated

Rules are being updated.

A screenshot of a computer

Description automatically generated

Successful update to the rules.

A screenshot of a computer

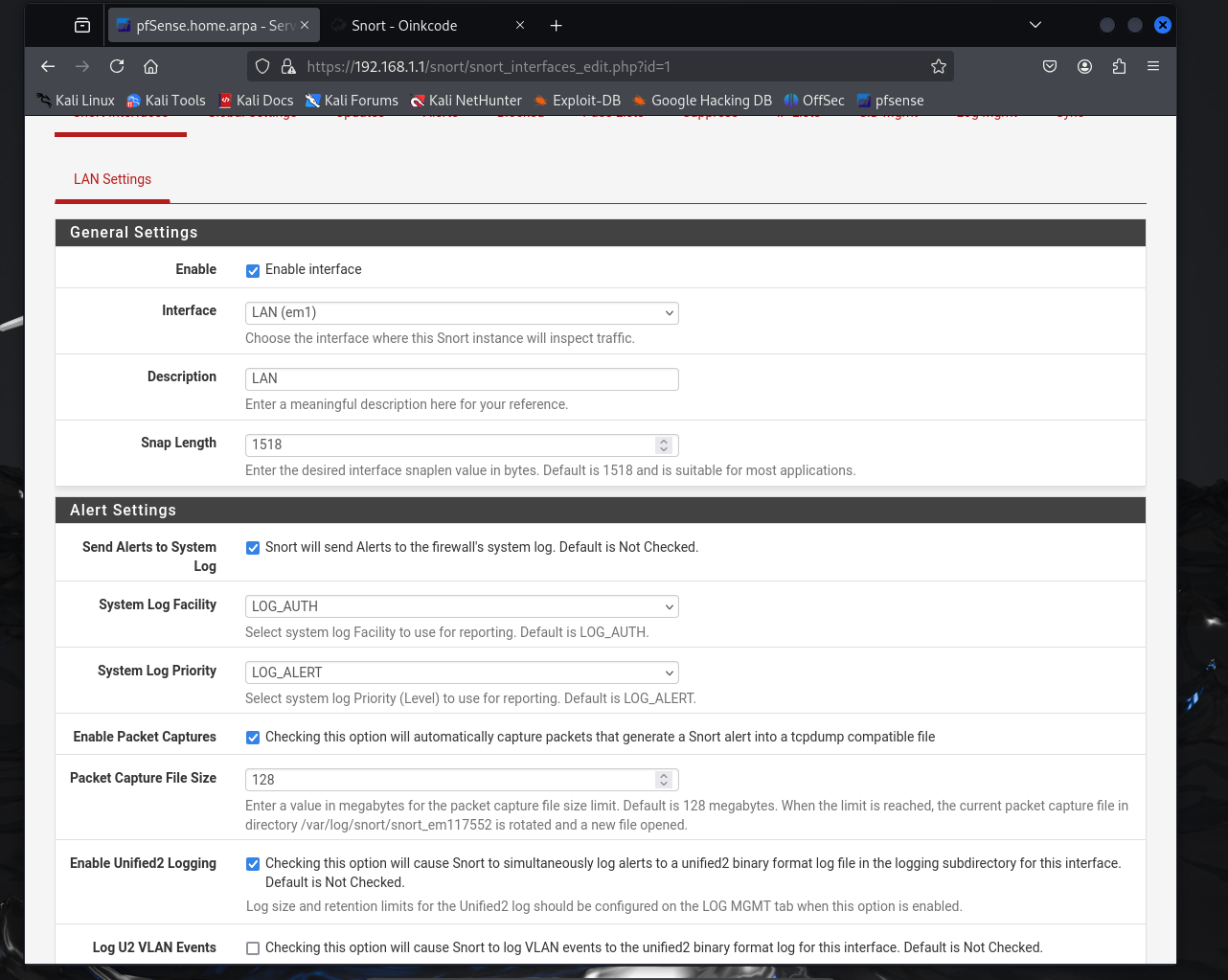
Description automatically generated

At the top click snort interfaces, then click add to add a new snort interface.

A screenshot of a computer

Description automatically generated

The first will be the WAN interface. Check to send alerts to the system log and leave the rest as default.



Next is the LAN interface. Check to send alerts to system log, enable packet captures and enable unified2 logging. The rest will be left default.

A screenshot of a computer

Description automatically generated

Click back to the snort interfaced and enable them both. Snort is now installed and enabled.

A screenshot of a computer

Description automatically generated

Here is the GVM full and fast scan results against the Pfsense ip. You can see there is one severe item in there. After looking through, I can see that it is because the admin login for pfsence is default. This can be easily fixed by changing the credentials.

A screenshot of a computer

Description automatically generated

Here are the LAN Snort logs that happened during the GVM scan. The main alert was for Webroot Directory Traversal. This happened over 30 times as it was trying different SPorts. To prevent unwanted access to files by traversal, developers must sanitize all user inputs and restrict the type of input that can be processed. By ensuring that all inputs follow a certain format — such as checking that the input is a valid filename and does not contain directory traversal sequences — these vulnerabilities can be effectively neutralized(Directory Traversal, n.d.).

**Lesson Learned**

* Configured Snort and start the Snort service.
* Updated Snort and download the latest community rules .
* Learned that Snort is an Intrusion Prevention System designed to provide network traffic analysis in real-time and data packet logging.

**Issues Encountered**

* There were no issues encountered, during and setting up snort.
* Ended up rushing as I got busy with work and life, thinking this assignment would be a breeze.

**How to make sure issues don’t happen again**

* First is to make sure time management is the key factor. This means to write out a schedule if need to.
* Don’t rush through your homework.

Snort Intrusion Protection System (IPS) is a fascinating technology that provides a robust layer of security. It can be implemented as either a dedicated device or software, actively monitoring network traffic for potential threats. IPS goes beyond detecting individual suspicious activities, analyzing patterns and combinations of events to identify potential threats that might otherwise go unnoticed. It's important to distinguish IPS from Intrusion Detection Systems (IDS), which primarily focus on alerting administrators to potential threats. While IDS passively monitors network traffic, IPS actively takes steps to prevent or mitigate threats, safeguarding systems from cyberattacks(*IPS vs IDS*, 2023). Making sure to prioritize items such as school, work, personal life, and leave time for possible unplanned situations.

Reference:

*Directory Traversal | Imperva. (n.d.). Learning Center. https://www.imperva.com/learn/application-security/directory-traversal/*

*IPS vs IDS: What’s the Difference and Why It Matters | Tech Impact. (2023, October 26). Techimpact.org. https://techimpact.org/news/ips-vs-ids-whats-difference-and-why-it-matters*