NFS Lab 7: Introduction to IPS

I Introduction

This optional session provides a guided first contact with Intrusion Prevention Systems (IPS) by exploring Snort 3, following the official examples and tutorials published by the Snort 3 development team.

I.1 Prerequisites

For this lab, we will be using a prebuilt docker from the Snort development team.

```
~$ docker pull ciscotalos/snort3
~$ docker run --name snort3 -h snort3 -u snorty -w /home/snorty -d -it ciscotalos/
snort3 bash
~$ docker exec -it snort3 bash
```

II Getting Familiar with IPS Concepts

Watch the short guided introduction video on Snort 3 fundamentals.

Keep the container open while viewing, you will reproduce selected commands and behaviors as you progress.

Take a look as the rule file within ~/snort3/etc/rules/.

II.1 Rule Writing

Continue with the rule creation walkthrough.

At this stage, treat rule writing as interactive pattern matching exercises to observe detection and prevention behavior.

II.2 Now on your own

In the same fashion, write your own rules to trigger warnings to detect icmp packages, and flag a basic SQL injection. The documentation of snort can also help you.

You can download the two pcap files for these here and here.

Acknowledgements

This lab is part of the Snort 3 Cisco Talos dev team.