Network Security

Assignment: Threat Intelligence

Introduction

You are a Threat Intelligence analyst and are asked to identify the organizational threat landscape. To this end, you have collected application layer traces of attackers targeting your network. These files are stored in PCAP format on the Weblab platform. To better understand the attacks facing your organization, you will run an IDS (Snort) on this data to obtain more information about the threats. As your organization does not have its own IDS ruleset, you will rely on the community ruleset of Snort. Your objective is to understand the attack traffic aimed at your organization, and to investigate how well the Snort community rules will protect you against adversaries.

NOTE: These files are recent, which means that many of the malware samples collected in the network data are still active. Please stick to the analysis of the network data and do not download anything from other sources.

PCAP Files

We cannot upload a large file in weblab. To make it easier to work with the data, we suggest to merge the individual PCAP files together after downloading using the `mergecap` command line utility.

Running Snort

To install and run Snort **3** you can refer to: `https://hackertarget.com/snort-tutorial-practical-examples/#install-snort-29`. In this document we show how to run it using Docker. You are free to run it in every way that suits you, but we will not be able to help with the setup unless you use the method described below.

For this project, we will be using Snort 3. The following commands should work on OSX and Linux. For Windows, please refer to the docker manual. To run Snort 3 in a Docker instance, you can use the following commands:

```
:-$ sudo docker pull ciscotalos/snort3
:-$ sudo docker run --name snort3 -h snort3 -u snorty -w /home/snorty -d -it \
    ciscotalos/snort3 bash
```

The rules can be downloaded from the Weblab. This is a version of the community rules.

To run Snort using the rules, the easiest method is to copy the files into the docker home directory as follows:

```
:-$ sudo docker cp snort3-community.rules snort3:/home/snorty/local.rules
:-$ sudo docker cp <PCAP_FILE> snort3:/home/snorty
```

Running Snort requires you to connect to the docker and run the Snort command:

```
:-$ sudo docker exec -it snort3 bash
<YOU SHOULD NOW BE INSIDE THE DOCKER CONTAINER>
:-$ snort --talos -r <PCAP_FILE>

<To obtain alertations line-by-line you can use the following>
:-$ snort --talos -A alert_fast -r dataset_netsec.pcap
```

For other commands for Snort, please refer to the Snort documentation.

To easily search through the PCAP files you can use `tshark` or `tcpdump` and filter the files.

Assignment

1. **Data Analysis (55 Points)**
   - How many packets would the system have blocked? (5 points)
   - List the top **5** alerts by number of hits, and for every alerts comment on the severity of the alert (10 points)
   - You know that your company is running a "Linksys E-series HNAP". Which IP addresses are trying to attack this device? (5 points)
   - Analyze the rule that detects attacks on the "Linksys E-series HNAP" and explain step by step what the rule triggers on. (5 points)
   - For the earliest hit on the "Linksys E-series HNAP" rule, deconstruct the attack packet and explain step by step what the attack packet does. (10 points)
   - Analyze the rule "MALWARE-CNC Win.Trojan.Gh0st variant outbound connection". Which IP addresses does it hit on, what does it check, and which of the hits are true positives (if any)? (10 points)
   - Analyze the rule "INDICATOR-SHELLCODE x86 inc ecx NOOP". Comment on the correctness of this rule from an adversarial perspective. Could you circumvent detection on this rule? (5 points)
   - Analyze the packets that hit on the "INDICATOR-SHELLCODE x86 inc ecx NOOP" rule. What is the content of the packet, which service is targeted, and what would be the goal of these packets? (5 points)
2. **New Threats (30 Points)**
   - Your company learns of a new malware that requests `/board.cgi`. Write a Snort rule that identifies this malware. (5 points)
   - What is the name of the malware and which type of devices are targeted by the malware? (5 points)
   - You know that the malware spreads in multiple ways. To detect more exploit attempts of this malware, you should write a Snort rule that detects these other attempts as well. Explain the rule and what it detects. (10 points)
   - List all different ways in which this malware tries to spread and the device types that are targeted. (10 points)
3. **Report and Visualization (15 points)**
   - Plot a time series for every rule with at most 1,500 alerts in the same diagram. Choose a plot type that you think will clearly show the data. (15 points)

Submission

Please submit all questions through the inputs on Weblab. This document is there for ease of reading.