

Introduction to IDS & Suricata

Network Security Monitoring with Suricata



Suricata Installation

- For this training, Suricata has already been installed for you using the OISF supported package for Ubuntu LTS:
 - These installation instructions can be found in the Suricata user guide under “Binary Packages -> Ubuntu”
 - <https://suricata.readthedocs.io/en/suricata-6.0.2/install.html#ubuntu>
- Expect minor differences between all installation methods.

Suricata Installation Con't

- Other installation methods include:
 - OISF supported RPM repositories for RHEL, CentOS, Fedora
 - OISF supported installer for Windows
 - From source (./configure && make install)
 - Or even the package manager for your favorite operating system (Arch Linux, FreeBSD, OpenBSD, etc)

Note: This course is based around Suricata on Ubuntu Linux as installed with OISF's support packages via the Ubuntu personal package archive (PPA) system.

The Suricata Training Virtual Machine (VM)

- The Suricata training VM is an Ubuntu 20.04 LTS installation with Suricata installed from the OISF support PPA.
- Suricata configuration is stored in `/etc/suricata`:
 - `suricata.yaml` being the primary configuration file
- The logging location for the Suricata daemon process running on “live” traffic is `/var/log/suricata`.
- Suricata-Update is ready for use with the Emerging Threats Open ruleset and Suricata will load these rules by default from:
 - `/var/lib/suricata/rules/suricata.rules`

Note: When running Suricata in PCAP files, Suricata will log to the current directory rather than the system logging directory.

Dummy Networking

- To provide a “live” like experience Suricata is configured to listen on a fake ethernet device known as “dummy0”.
- Provide “live” like behavior without depending on proper network configuration and Suricata placement within a network.
- The VM provides a way to “replay” packet captures into the live dummy interface.
- Suricata can also be used directly on PCAP files in an offline mode:
 - Both live and offline modes will be discussed during this training.

Other Tools

- The VM provides a full Ubuntu LTS desktop environment.
- Popular editors such as `vi` and `nano` are installed.
- `Jq` is installed for viewing and processing JSON files as JSON is Suricata's primary logging method.
- EveBox is installed and pre-configured to visualize logs produced by Suricata in the web browser.

Suricata Output

- Suricata generates output (or log files) from network traffic such as alerts and other network metadata like DNS requests.
 - This is why we run Suricata: to generate this output.
- In a basic production installation of Suricata this output can be seen in `/var/log/suricata`.
- Check this directory out on the training VM as it comes with some files already in this directory.

/var/log/suricata

- In `/var/log/suricata`, note the following files:
 - eve.json - This is the primary Suricata log file for alerts and other network events.
 - fast.log - A simple text log file containing only alerts that may be familiar to those coming to Suricata from other intrusion detection systems.
 - stats.log - A text log file in a tabular format containing various metrics about the Suricata engine itself such as number of packets seen.
 - suricata.log - A log file containing output from the Suricata application itself such as startup errors.
 - filestore - The directory where extracted files can be found if file extraction is enabled - a topic that will be covered later on in the training.

Suricata Common Operations

Suricata Common Operations

- In most installation scenarios you will need to know how to:
 - Start Suricata
 - Stop Suricata
 - Update the rules
 - Reload the rules

Starting and Stopping the Suricata Service

- The Suricata service is started and stopped using *systemd*:
 - To start:
 - `systemctl start suricata`
 - To stop:
 - `systemctl stop suricata`
- To stop Suricata from starting on boot:
 - `systemctl disable suricata`
- To enable Suricata to start on boot:
 - `systemctl enable suricata`
- If you are familiar with *systemd*, Suricata is no different than any other service.

Note: The training VM has Suricata configured to start on boot.

Running Suricata on a PCAP File

- A common function of Suricata while learning, testing and experimenting is to run Suricata over a PCAP file.
- Most of the time a command like the following is enough:
 - `suricata -r /path/to/filename.pcap`
- This will place the log files in your current directory so it will not cause conflict with an instance of Suricata you may have running as a service.

Note: This mode of running Suricata is often referred to as “user mode”, as it’s usually done interactively by a user.

Running Suricata on a Live Network Interface

- While the training VM is already configured to start Suricata on a fake live interface on boot, it is sometimes an operation you may need to do interactively.
- Example:
 - `suricata -i dummy0 -l .`
- This will run Suricata on the live network interface named “dummy0”.
- Running Suricata on a live network interface is also known as “system” mode.

Running Suricata on a Live Network Interface

- Example:

- `suricata -i dummy0 -l .`

Note: The example command line above uses the “-l .” to put log files in the current directory. System mode by default will put the log files in `/var/log/suricata`, and we don’t want to conflict with the Suricata instances that are already running as a service.

Note: For most of this training, we’ll make use of the Suricata service and replay PCAPs, or operate on PCAP files directly using Suricata’s user-mode.

Network Variables

- To help detection accuracy, it is suggested to tell Suricata a little about your network with network variables in your `suricata.yaml`.
- The most important variable here is the “HOME_NET”.
 - By default, it is configured for private network address space and can be left alone for training purposes. However, remember to set this variable when doing a live deployment.
- Also considering other variables like HTTP_SERVERS, SMTP_SERVERS, and so to help with performance.

```
vars:  
  # more specific is better for alert accuracy and performance  
  address-groups:  
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"  
    #HOME_NET: "[192.168.0.0/16]"  
    #HOME_NET: "[10.0.0.0/8]"  
    #HOME_NET: "[172.16.0.0/12]"  
    #HOME_NET: "any"  
  
    EXTERNAL_NET: "!$HOME_NET"  
    #EXTERNAL_NET: "any"  
  
    HTTP_SERVERS: "$HOME_NET"
```

Updating Rules

Updating Rules

- The training VM along with most default installations of Suricata comes pre-configured to use the Emerging Threats Open ruleset.
 - https://rules.emergingthreats.net/OPEN_download_instructions.html
- The Emerging Threats teams update the rules about once a day so it makes sense to update your rules about once a day as well.
- To update your rules the following command can be used:
 - `suricata-update`

Updating Rules Con't

- The *Suricata-Update* tool will download the rules if they are newer than the last downloaded rule:
 - Apply any user specific configuration (such as enabling and disabling rules), test that Suricata can load them, then write them out to **`/var/lib/suricata/rules/suricata.rules`**.

Note: Suricata-Update by default will NOT trigger Suricata to reload the new rules.

- The following command will trigger Suricata to reload the rules:
 - `suricatasc -c reload-rules`

Configuring “suricata-update”

- Suricata-update can be configured to add, remove, disable and modify any existing rule sources.
- Run suricata-update periodically to update the rules to the latest as provided by the enabled sources.
- Suricata-update can simply be launched and run with the command:
 - `$ suricata-update`
- Check out the option `-h` for the available options and commands.

Useful Commands for Ruleset Management

- `suricata-update list-sources` :
 - List all the rule sources made available by `suricata-update` via the intel index.
- Example:

```
└─ $ ▶ suricata-update list-sources
19/5/2021 -- 17:50:27 - <Info> -- Using data-directory /var/lib/suricata.
19/5/2021 -- 17:50:27 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
19/5/2021 -- 17:50:27 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
19/5/2021 -- 17:50:27 - <Info> -- Found Suricata version 7.0.0-dev at /usr/bin/suricata.
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: ptresearch/attackdetection
  Vendor: Positive Technologies
  Summary: Positive Technologies Attack Detection Team ruleset
  License: Custom
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
```

Useful Commands for Ruleset Management Con't

- `suricata-update add-source <name> <url>:`
 - Add a new source to the list of rule sources.
- Example:

```
└─ $ ► suricata-update add-source test-source https://abc.xyz
19/5/2021 -- 17:52:10 - <Info> -- Using data-directory /var/lib/suricata.
19/5/2021 -- 17:52:10 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
19/5/2021 -- 17:52:10 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
19/5/2021 -- 17:52:10 - <Info> -- Found Suricata version 7.0.0-dev at /usr/bin/suricata.
```

Useful Commands for Ruleset Management Con't

- `suricata-update disable-source <name>:`
 - Disable rule source to avoid downloading rulesets from it.
- Example:

```
└─ $ ► suricata-update disable-source et/open
19/5/2021 -- 17:53:50 - <Info> -- Using data-directory /var/lib/suricata.
19/5/2021 -- 17:53:50 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
19/5/2021 -- 17:53:50 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
19/5/2021 -- 17:53:50 - <Info> -- Found Suricata version 7.0.0-dev at /usr/bin/suricata.
19/5/2021 -- 17:53:50 - <Info> -- Source et/open has been disabled
```

Useful Commands for Ruleset Management Con't

- `suricata-update update-sources:`
 - Updates sources to their latest.
- Example:

```
└─ $ ► suricata-update update-sources
19/5/2021 -- 17:54:55 - <Info> -- Using data-directory /var/lib/suricata.
19/5/2021 -- 17:54:55 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
19/5/2021 -- 17:54:55 - <Info> -- Using /usr/share/suricata/rules for Suricata provided rules.
19/5/2021 -- 17:54:55 - <Info> -- Found Suricata version 7.0.0-dev at /usr/bin/suricata.
19/5/2021 -- 17:54:55 - <Info> -- Downloading https://www.openinfosecfoundation.org/rules/index.yaml
19/5/2021 -- 17:54:56 - <Info> -- Saved /var/lib/suricata/update/cache/index.yaml
```

Suricata Rules and Intel Index

