THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Collector Configuration

OpenLI Training: Chapter Nine

Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

The Collector

- Intercepts network traffic and encodes into ETSI format
  - Receives instructions from the provisioner
  - Monitors session management protocols for target identities
  - Intercepts packets that belong to an intercept target
  - Labels and sequences intercepted packets
  - Forwards encoded records to mediator

The Collector

- Get a shell on your collector container

```
$ docker exec -i -t openli-collector /bin/bash

root@cd488a97a8e7:/home/openli-coll#
```

Configuration

- Open the collector configuration file in a text editor

```
# vim /etc/openli/collector-config.yaml

operatorid: <OPID>
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: <PROVIP>
provisionerport: <COLLECTORPORT>
```

Configuring Provisioner Connection

- Replace <PROVIP> with the correct IP address
  - This will be the IP address you used in the provisioner lesson

```
operatorid: <OPID>
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: 172.19.0.3
provisionerport: <COLLECTORPORT>
```

Configuring Provisioner Connection

- Replace <PROVIP> with the correct IP address
  - This will be the IP address you used in the provisioner lesson

```
operatorid: <OPID>
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddress: 172.19.0.3
provisionerport: <COLLECTORPORT>
```

Configuring Provisioner Connection

- Replace all instances of <COLLECTORPORT>
  - Use the port you chose for collector connections

```
operatorid: <OPID>
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: 172.19.0.3
provisionerport: 9001
```

Configuring Provisioner Connection

- Replace all instances of <COLLECTORPORT>
  - Use the port you chose for collector connections

```
operatorid: <OPID>
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: 172.19.0.3
provisionerport: 9001
```

Configuring Identity

- Replace <OPID> with your operator ID string

```
operatorid: WAND
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: 172.19.0.3
provisionerport: 9001
```

Configuring Identity

- Replace <OPID> with your operator ID string

```
operatorid: WAND
networkelementid: openli-lab
interceptpointid: col001

encoderthreads: 2

inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:

etsitls: no
provisioneraddr: 172.19.0.3
provisionerport: 9001
```

Configuring Identity

- Network Element ID
  - Identifies the location of the collector within your network
  - 16 characters max
  - Suggestion: name it after the traffic source

Configuring Identity

- Interception Point ID
  - Distinguish between multiple collectors at the same location
  - 8 characters max
  - Optional
    - Use when operator and network element IDs are not unique

Configuring Capture Interfaces

- Inputs
  - Each capture interface appears as a list item here
- URIs
  - Describes the capture method and interface to capture on
  - In this case: AF_PACKET on interface eth2

```
inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:
```

Configuring Capture Interfaces

- URIs for other capture methods
  - XDP: `xdp:<interface>`
  - DPDK: `dpdk:<PCI address>`
  - PF_RING: `pfring:<interface>`

```
inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:
```

Configuring Capture Interfaces

- Threads
  - Number of threads to dedicate to packet capture
  - Don’t forget to leave CPU cores for encoding as well!

```
inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:
```

Configuring Capture Interfaces

- Hasher
  - Defines how packets should be distributed among threads
  - Use “radius” for interfaces that will see RADIUS traffic
    - Ensure RADIUS sessions go to a consistent thread
  - Other options: “bidirectional”, “balanced”.

```
inputs:
   - uri: eth2
     threads: 2
     hasher: radius
     #filter:
```

Configuration Complete!

- We’re done -- save and exit your text editor

Logging with rsyslog

- Copy the provided rsyslog config to `/etc/rsyslog.d/`
  - Restart rsyslog service
  - OpenLI logs will now appear in `/var/log/openli/`

```
# cp /etc/openli/rsyslog.d/10-openli-collector.conf /etc/rsyslog.d/

THIS STEP IS NEEDED ONLY WHEN USING THE LAB CONTAINER
# stop_rsyslog.sh

# service rsyslog restart
```

Starting the Collector

- Now we can start the collector service
  - Examine logs for any obvious error messages

```
# service openli-collector start

 * Starting OpenLI collector /etc/openli/collector-config.yaml          [ OK
]


# less /var/log/openli/collector.log
```

Starting the Collector

- Example of “good” looking logs

```
openlicollector[2811]: OpenLI: not using OpenSSL TLS for internal communications
openlicollector[2811]: OpenLI: collector is using a RADIUS-session hasher for input eth2
openlicollector[2811]: OpenLI: collector has started reading packets from eth2 using 2
threads.
openlicollector[2811]: openli-collector: all processing threads have reported for duty
openlicollector[2811]: OpenLI: new mediator announcement for 172.19.0.4:12009
openlicollector[2811]: OpenLI: adding new mediator 1 at 172.19.0.4:12009
openlicollector[2811]: OpenLI: collector has connected to mediator 172.19.0.4:12009 using a
non-TLS connection
```

Starting the Collector

- Example of “good” looking logs

```
openlicollector[2811]: OpenLI: not using OpenSSL TLS for internal communications
openlicollector[2811]: OpenLI: collector is using a RADIUS-session hasher for input eth2
openlicollector[2811]: OpenLI: collector has started reading packets from eth2 using 2
threads.
openlicollector[2811]: openli-collector: all processing threads have reported for duty
openlicollector[2811]: OpenLI: new mediator announcement for 172.19.0.4:12009
openlicollector[2811]: OpenLI: adding new mediator 1 at 172.19.0.4:12009
openlicollector[2811]: OpenLI: collector has connected to mediator 172.19.0.4:12009 using a
non-TLS connection
```

Starting the Collector

- Example of “good” looking logs

```
openlicollector[2811]: OpenLI: not using OpenSSL TLS for internal communications
openlicollector[2811]: OpenLI: collector is using a RADIUS-session hasher for input eth2
openlicollector[2811]: OpenLI: collector has started reading packets from eth2 using 2
threads.
openlicollector[2811]: openli-collector: all processing threads have reported for duty
openlicollector[2811]: OpenLI: new mediator announcement for 172.19.0.4:12009
openlicollector[2811]: OpenLI: adding new mediator 1 at 172.19.0.4:12009
openlicollector[2811]: OpenLI: collector has connected to mediator 172.19.0.4:12009 using a
non-TLS connection
```

Starting the Collector

- Example of logs where an error has occurred
  - Using wrong interface name

```
openlicollector[2860]: OpenLI: not using OpenSSL TLS for internal communications
openlicollector[2860]: OpenLI: Failed to create trace for input eth3: Unable to find URI
(eth3)
openlicollector[2860]: OpenLI: failed to start input eth3
```

Starting the Collector

- Example of logs where an error has occurred
  - Error when specifying provisioner IP or port

```
openlicollector[2900]: OpenLI: not using OpenSSL TLS for internal communications
openlicollector[2900]: OpenLI: collector is using a RADIUS-session hasher for input eth2
openlicollector[2900]: OpenLI: Failed to connect to 172.19.0.4:9001 -- Connection refused.
openlicollector[2900]: OpenLI: Will retry connection periodically.
openlicollector[2900]: OpenLI: collector has started reading packets from eth2 using 2
threads.
```

Starting the Collector

- Check provisioner logs for a successful connection

```
openliprovisioner[2715]: OpenLI: connection accepted from collector 172.19.0.5-34896
openliprovisioner[2715]: OpenLI provisioner: collector 172.19.0.5-34896 is now active
```

Starting the Collector

- Check mediator logs for a successful connection

```
openlimediator[2799]: OpenLI Mediator: accepted connection from collector 172.19.0.5.
```

Stopping the Collector

- Normally, you would use systemd to halt the service
  - Can't normally stop processes with systemd inside docker
  - I've added a script to the container to do it for you

```
DO THIS NORMALLY
# service openli-collector stop

ON THE LAB CONTAINER, DO THIS INSTEAD
# stop_collector.sh
```

Next Time

- Simulating a dummy LEA