THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

University of Waikato
Network Research Group

openLI

Mediator Configuration

OpenLI Training: Chapter Eight

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

The Mediator

- Delivers intercepted traffic to the LEAs
    - Receives the intercepts from the collectors
    - Establishes and maintains handovers to LEAs
    - Ensure that the intercepted traffic goes to the right LEA

The Mediator

- Get a shell on your mediator container

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

root@b22dba6e6361:/home/openli-med#
```

The Mediator

- Query the container’s IP address on the openli-lab network

```
# ip addr list eth1

844: eth1@if845: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default
    link/ether 02:42:ac:13:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.19.0.4/16 brd 172.19.255.255 scope global eth0
    valid_lft forever preferred_lft forever
```

The Mediator

- Query the container’s IP address on the openli-lab network

```
# ip addr list eth1

844: eth1@if845: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default
    link/ether 02:42:ac:13:00:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.19.0.4/16 brd 172.19.255.255 scope global eth0
    valid_lft forever preferred_lft forever
```

Configuration

- Open the mediator configuration file in a text editor

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: <MEDIP>

provisioneraddr: <PROVIP>
provisionerport: <MEDIATORPORT>

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Listening IP

- Replace all instances of <MEDIP> with the correct IP address

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: <PROVIP>
provisionerport: <MEDIATORPORT>

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Listening IP

- Replace all instances of <MEDIP> with the correct IP address

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: <PROVIP>
provisionerport: <MEDIATORPORT>

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Provisioner Connection

- Replace all instances of <PROVIP> with the correct IP address
  - This will be the IP address you used in the previous lesson

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: <MEDIATORPORT>

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Provisioner Connection

- Replace all instances of <PROVIP> with the correct IP address
    - This will be the IP address you used in the previous lesson

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: <MEDIATORPORT>

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Provisioner Connection

- Replace all instances of <MEDIATORPORT>
  - Use the port you chose for mediator connections previously

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Provisioner Connection

- Replace all instances of <MEDIATORPORT>
  - Use the port you chose for mediator connections previously

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

operatorid: <OPID>

listenport: <MEDLISTENPORT>
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: <MEDIDNUM>

etsitls: no
```

Listening for Collectors

- Choose a distinctive port for the listening service
  - Collectors will connect to this mediator on this port

Configuring Listener

- Replace <MEDLISTENPORT> with your chosen port number

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

operatorid: <OPID>

listenport: 12009
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: <MEDIDNUM>

etsitls: no
```

Configuring Listener

- Replace <MEDLISTENPORT> with your chosen port number

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

operatorid: <OPID>

listenport: 12009
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: <MEDIDNUM>

etsitls: no
```

Mediator Identity Fields

- Operator ID
  - A string that uniquely identifies your network to the agencies
  - Maximum of 16 characters
- Mediator ID
  - A number that uniquely identifies this mediator in your deployment
  - Most deployments have just one mediator
  - Minimum: 0
  - Maximum: 1,000,000

Configuring Identity

- Replace <OPID> with your operator ID string
- Replace <MEDIDNUM> with your mediator ID

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

operatorid: WAND

listenport: 12009
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: 1

etsitls: no
```

Configuring Identity

- Replace <OPID> with your operator ID string
- Replace <MEDIDNUM> with your mediator ID

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

operatorid: WAND

listenport: 12009
listenaddr: 172.19.0.4

provisioneraddr: 172.19.0.3
provisionerport: 9002

mediatorid: 1

etsitls: no
```

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-mediator.conf /etc/rsyslog.d/

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

# service rsyslog restart
```

Starting the Mediator

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

```
# service openli-mediator start

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


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

Starting the Mediator

- Example of “good” looking logs

```
openlimediator[2799]: OpenLI: not using OpenSSL TLS for internal communications
openlimediator[2799]: OpenLI Mediator: '1' has started.
openlimediator[2799]: OpenLI: Mediator listening on 172.19.0.4:12009 successfully.
openlimediator[2799]: OpenLI Mediator: pcap trace file directory has been set to NULL
openlimediator[2799]: OpenLI Mediator: pcap trace files are named using the default
template
openlimediator[2799]: OpenLI Mediator: pcap output file rotation frequency is set to 30
minutes.
openlimediator[2799]: OpenLI Mediator: changing pcap trace compression level to 1 (from
next file onwards)
openlimediator[2799]: OpenLI mediator has connected to provisioner at 172.19.0.3:9002
```

Starting the Mediator

- Example of “good” looking logs

```
openlimediator[2799]: OpenLI: not using OpenSSL TLS for internal communications
openlimediator[2799]: OpenLI Mediator: '1' has started.
openlimediator[2799]: OpenLI: Mediator listening on 172.19.0.4:12009 successfully.
openlimediator[2799]: OpenLI Mediator: pcap trace file directory has been set to NULL
openlimediator[2799]: OpenLI Mediator: pcap trace files are named using the default
template
openlimediator[2799]: OpenLI Mediator: pcap output file rotation frequency is set to 30
minutes.
openlimediator[2799]: OpenLI Mediator: changing pcap trace compression level to 1 (from
next file onwards)
openlimediator[2799]: OpenLI mediator has connected to provisioner at 172.19.0.3:9002
```

Starting the Mediator

- Example of logs where an error has occurred

```
openlimediator[2758]: OpenLI: not using OpenSSL TLS for internal communications
openlimediator[2758]: OpenLI Mediator: '1' has started.
openlimediator[2758]: OpenLI: Mediator listening on 172.19.0.4:12009 successfully.
openlimediator[2758]: OpenLI Mediator: pcap trace file directory has been set to NULL
openlimediator[2758]: OpenLI Mediator: pcap trace files are named using the default
template
openlimediator[2758]: OpenLI Mediator: changing pcap trace compression level to 1 (from
next file onwards)
openlimediator[2758]: OpenLI Mediator: pcap output file rotation frequency is set to 30
minutes.
openlimediator[2758]: OpenLI mediator has connected to provisioner at 172.19.0.3:9001
openlimediator[2758]: OpenLI Mediator: Disconnecting from provisioner.
```

Starting the Mediator

- Example of logs where an error has occurred

```
openlimediator[2758]: OpenLI: not using OpenSSL TLS for internal communications
openlimediator[2758]: OpenLI Mediator: '1' has started.
openlimediator[2758]: OpenLI: Mediator listening on 172.19.0.4:12009 successfully.
openlimediator[2758]: OpenLI Mediator: pcap trace file directory has been set to NULL
openlimediator[2758]: OpenLI Mediator: pcap trace files are named using the default
template
openlimediator[2758]: OpenLI Mediator: changing pcap trace compression level to 1 (from
next file onwards)
openlimediator[2758]: OpenLI Mediator: pcap output file rotation frequency is set to 30
minutes.
openlimediator[2758]: OpenLI mediator has connected to provisioner at 172.19.0.3:9001
openlimediator[2758]: OpenLI Mediator: Disconnecting from provisioner.
```

Starting the Mediator

- Check provisioner logs for a successful connection

```
openliprovisioner[2715]: OpenLI: mediator 172.19.0.4-41364 on fd 14 auth success.
```

Stopping the Mediator

- 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-mediator stop

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

Next Time

- Configuring the Collector