Conpot: Deployment and Case Study

*CODE EXECUTION MANUAL*

Bennett University

Greater Noida, Uttar Pradesh

***The paper briefly describe the methodologies, design and how we have done the conpot deployment in the research project. First approach is to install the conpot on docker using prebuilt image file, building image from source or via github.***

Via pre-built image

Step 1- Install Docker

Step 2- Run docker pull honeynet/conpot

Step 3- Run docker run -it -p 80:80 -p 505:505 -p 302:302/udp –network=bridge honeynet/conpot:latest /bin/sh (the ports can be different but they should be available)

Building image from source

Step 1- Install Docker

Step 2- Clone this git clone <https://github.com/mushorg/conpot.git>

Step 3- Run sudo make run-docker

Building image from source via docker-compose

Step 1- Install Docker-Compose

Step 2- Clone this git clone <https://github.com/mushorg/conpot.git> and cd conpot/docker

Step 3- Build the image with docker-compose build

Step 4- Check if the Docker Compose is intalled properly docker-compose up

Step-5 Permanently run as a daemon with docker-compose up -d

*If you want to specify some particular ports in the github pull methods run docker run -it -p (#ports) honeynet/conpot:latest /bin/sh (make sure that the ports are available)*

*To confirm the setup search for the ports assigned*

***Second approach is to install the conpot on your local network through linux or virtual machine.***

Raw Conpot Installation

*This method installs and deploy the conpot from your linux system for local implementation by building a virtualized enviroment. Install any linux operating system on your virtual machine or VM player if u don’t have linux as your default operating system.*

Task 1- Installing conpot on linux :--

Step 1- Update linux

* sudo apt-get update

Step 2- Installing required dependencies

* sudo apt-get install git libsmi2ldbl smistrip libxslt1-dev python3.6-dev libevent-dev defaultlibmysqlclient-dev

Step 3- Creating, installing and activating the virtual environment (venv)

* sudo apt-get install python3-pip
* pip3 install virtualenv
* virtualenv --python=python3.6 conpot
* source conpot/bin/activate

Step 4- Upgrading pip with the needed tools dependencies

* pip install --upgrade pip
* pip install --upgrade setup tools pip
* pip install cffi

if any dependency is not install you can install it using pip install command within the virtual environment.

Step 5- Installing conpot, testing the default conpot

* pip install conpot
* conpot -f --template default

verify conpot is running- go to “127.0.0.1:8800” on your web browser

Task 2- Building the configuration file:--

Step 1- Look out for the “testing.cfg” file in the conpot directory installed previously.

Step 2- Make a copy of that file at /home/conpot as “conf.cfg”.

* cd /conpot/
* nano conf.cfg

Step 3- Make the following changes to the file

* data fs url = /tmp/
* fs\_url = tar:///home/conpot/conpot/lib/python3.6/site- packages/conpot/data.tar

Step 4- Test the conpot with conf.cfg file and verify the setup by looking at :8800 port

* conpot –c /conpot/config.cfg --template default

Task 3- Install and configure Authbind:--

Step 1- Install Authbind

* sudo apt-get install authbind

Step 2- Conduct the below steps for ports: 21, 69, 80, 102, 161, 502, 623

* sudo touch /etc/authbind/byport/(#port)
* sudo chown conpot:conpot /etc/authbind/byport/(#port)
* sudo chmod 755 /etc/authbind/byport/(#port)

for port “623” use format- /etc/authbind/byport/!623

Step 3- Correct the port numbers within template

Update every “.xml” file with given ports:

- BACNET: 47808

- ENIP: 44818

- FTP: 21

- HTTP: 80

- IPMI: 623

- MODBUS: 502

- S7COM: 102

- SNMP: 161

- TFTP: 69

Step 4- Booting conpot using Authbind

* authbind conpot -c /conpot/conf.cfg –template default

goto “127.0.0.1” to see the webpage

Task 4- Verify the conpot outside your home network:

* Ensure that your network is bridged on your VM
* Go to <http://ip4.me> to know your outfacing IP.
* Boot conpot
* source conpot/bin/activate
* authbind conpot -c /conpot/conf.cfg –template default

Contributors-

Priyanshu Sharma ([e21cseu0955@bennett.edu.in](mailto:e21cseu0955@bennett.edu.in)) [Bachelor of Technology(CSE), Bennett 2021-25]

Sachchit Bhasin ([e21cseu0021@bennett.edu.in](mailto:e21cseu0021@bennett.edu.in)) [Bachelor of Technology(CSE), Bennett 2021-25]

Akshit Verma ([e21cseu0167@bennett.edu.in](mailto:e21cseu0167@bennett.edu.in)) [Bachelor of Technology(CSE), Bennett 2021-25]