Lab 10-2-1: Building a SCADA Honeypot

Lab Requirements

- Ubuntu virtual machine
- Docker

```
najd@ubuntu:~/Desktop$ sudo apt-get update
[sudo] password for najd:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
najd@ubuntu:~/Desktop$ sudo apt-get install ca-certificates curl gnupg lsb-rele
ase
Reading package lists... Done
Building dependency tree
Reading state information... Done
lsb-release is already the newest version (11.1.0ubuntu2).
lsb-release set to manually installed.
ca-certificates is already the newest version (20210119~20.04.2).
ca-certificates set to manually installed.
gnupg is already the newest version (2.2.19-3ubuntu2.1).
gnupg set to manually installed.
The following NEW packages will be installed:
  curl
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 161 kB of archives.
After this operation, 412 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 curl amd64 7
.68.0-1ubuntu2.7 [161 kB]
Fetched 161 kB in 1s (166 kB/s)
Selecting previously unselected package curl.
(Reading database ... 169638 files and directories currently installed.)
```

```
| sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
najd@ubuntu:~/Desktop$ echo \
>   "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docke
r-archive-keyring.gpg] https://download.docker.com/linux/ubuntu \
>   $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list >
 /dev/null
najd@ubuntu:~/Desktop$ sudo apt-get update
Get:1 https://download.docker.com/linux/ubuntu focal InRelease [57.7 kB]
Get:2 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages [13.
5 kB]
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:5 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:6 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Fetched 71.2 kB in 1s (76.8 kB/s)
Reading package lists... Done
najd@ubuntu:~/Desktop$ sudo apt-get install docker-ce docker-ce-cli containerd.
io
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  docker-ce-rootless-extras docker-scan-plugin pigz
  slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli
  docker-ce-rootless-extras docker-scan-plugin pigz
```

```
See 'docker run --help'.
najd@ubuntu:~/Desktop$ sudo docker run -it ubuntu bash
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
08c01a0ec47e: Pull complete
Digest: sha256:669e010b58baf5beb2836b253c1fd5768333f0d1dbcb834f7c07a4dc93f474be
Status: Downloaded newer image for ubuntu:latest
root@264dbaa5d5a5:/#
```

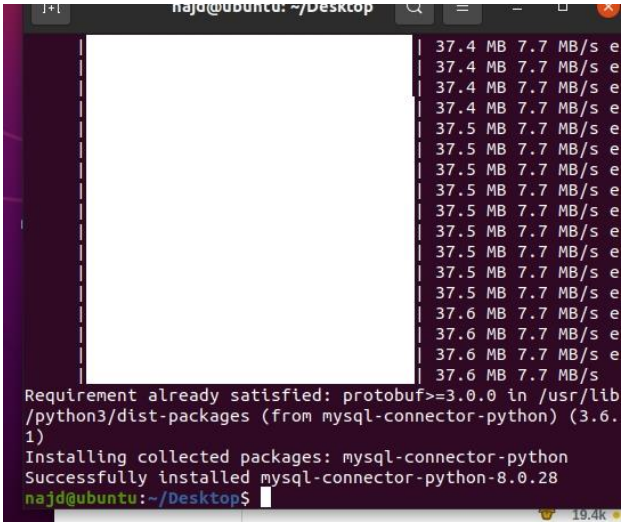
```
cker.sock: connect: permission denied
najd@ubuntu:~/Desktop$ sudo docker pull honeynet/conpot
Using default tag: latest
latest: Pulling from honeynet/conpot
Digest: sha256:cd93e88d9e44b020db691fc4c75cb29e76b5e90ddb
c408aca26e6c78c5646976
Status: Image is up to date for honeynet/conpot:latest
docker.io/honeynet/conpot:latest
```

```
najd@ubuntu:~/Desktop$ sudo apt-get install libsmi2ldbl s
nmp-mibs-downloader python-dev libevent-dev libxslt1-dev
libxml2-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'python-dev-is-python2' instead of 'pytho
n-dev'
The following additional packages will be installed:
  icu-devtools libevent-core-2.1-7 libevent-extra-2.1-7
  libevent-openssl-2.1-7 libevent-pthreads-2.1-7
  libicu-dev libpython2-dev libpython2-stdlib
  libpython2.7 libpython2.7-dev libpython2.7-minimal
  libpython2.7-stdlib python-is-python2 python2
  python2-dev python2-minimal python2.7 python2.7-dev
  python2.7-minimal smistrip
Suggested packages:
  icu-doc python2-doc python-tk python2.7-doc
  binfmt-support
The following NEW packages will be installed:
```

```
E: Package 'python-pip' has no installation candidate
najd@ubuntu:~/Desktop$ sudo apt-get install python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3-pip is already the newest version (20.0.2-5ubuntu
1.6).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgr
aded.
```

```
E: Unable to locate package libmysqlcl
najd@ubuntu:~/Desktop$ sudo apt-get install python-dev li
bmysqlclient-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'python-dev-is-python2' instead of 'pytho
n-dev'
python-dev-is-python2 is already the newest version (2.7.
t17-4).
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libmysqlclient-dev libssl-dev
0 upgraded, 2 newly installed, 0 to remove and 0 not upgr
aded.
Need to get 3,184 kB of archives.
After this operation, 18.1 MB of additional disk space wi
ll be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/m
ain amd64 libssl-dev amd64 1.1.1f-1ubuntu2.10 [1,584 kB]
```


```
E: Unable to locate package libmysqlcl
najd@ubuntu:~/Desktop$ sudo apt-get install python-dev li
bmysqlclient-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'python-dev-is-python2' instead of 'pytho
n-dev'
python-dev-is-python2 is already the newest version (2.7.
t17-4).
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libmysqlclient-dev libssl-dev
0 upgraded, 2 newly installed, 0 to remove and 0 not upgr
aded.
Need to get 3,184 kB of archives.
After this operation, 18.1 MB of additional disk space wi
ll be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/m
ain amd64 libssl-dev amd64 1.1.1f-1ubuntu2.10 [1,584 kB]
```




```
python3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
najd@ubuntu:~/Desktop$ sudo apt install python3-mysqldb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  default-mysql-server | virtual-mysql-server python3-mysqldb-dbg
The following NEW packages will be installed:
  python3-mysqldb
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 44.9 kB of archives.
After this operation, 181 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 python3-mysqldb amd6
4 1.4.4-2build1 [44.9 kB]
Fetched 44.9 kB in 1s (44.3 kB/s)
Selecting previously unselected package python3-mysqldb.
(Reading database ... 171855 files and directories currently installed.)
Preparing to unpack .../python3-mysqldb_1.4.4-2build1_amd64.deb ...
Unpacking python3-mysqldb (1.4.4-2build1) ...
Setting up python3-mysqldb (1.4.4-2build1) ...
najd@ubuntu:~/Desktop$
```

```
najd@ubuntu:~/Desktop$ sudo conpot --template default
[sudo] password for najd:
/usr/local/lib/python3.8/dist-packages/scapy/base_classes.
py:324: SyntaxWarning: Packet 'SPE' has a duplicated 'SL2'
 field ! If you are using several ConditionalFields, have
a look at MultipleTypeField instead ! This will become a S
yntaxError in a future version of Scapy !
  warnings.warn(war_msg, SyntaxWarning)

                     _
  ___ ___ ___ ___ ___| |_
 |  _| . |   | . | . |  _|
 |___|___|_|_|  _|___|_|
             |_|

 Version 0.6.0
 MushMush Foundation
```