Day-8 LAB

Running IDS using Snort and BarnYard

Snort for IDS

BarnYard for Logging

- Install dependencies:

```
  sudo apt-get install -y  autoconf automake default-libmysqlclient-dev
dos2unix libmariadb-dev-compat libmariadb-dev libtool mariadb-client
mariadb-server unzip
```

- Check the version of libpcap:

```
dpkg -s libpcap0.8 | grep Version
dpkg -s libpcap0.8-dev | grep Version
```

- Uninstall libpcap0.8 and libpcap0.8-dev
- Download and install the libpcap deb file

```
sudo dpkg -i lib........deb11
```

- Go to

```
sudo nano /etc/snort/snort.conf
```

- add the line bellow unified2:

```
output unified2: filename snort.u2, limit 128
```

- Download and install barnyard:

```
./autogen.sh
sudo ln -s /usr/include/dumbnet.h /usr/include/dnet.h
sudo ldconfig
./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-
gnu/
sudo make
sudo make install
```

-
  ```
  sudo cp etc/barnyard2.conf /etc/snort/
  sudo mkdir /var/log/barnyard2/
  sudo chown snort:snort /var/log/barnyard2/
  sudo touch /var/log/snort/barnyard2.waldo
  sudo chown snort:snort /var/log/snort/barnyard2.waldo
  ```

- Create a database in mariadb name= snort

  ```
  source /tmp/barnyard2-master/schemas/create_mysql
  ```

- Create a user in Database and give permissions:

  ```
  CREATE USER 'snort'@'localhost' IDENTIFIED BY 'toor';
  GRANT CREATE, INSERT, SELECT, DELETE, UPDATE ON snort.* TO
  'snort'@'localhost';
  ```

- sudo nano /etc/snort/barnyard2.conf:

  ```
  output database: log, mysql, user=snort password=toor dbname=snort
  host=localhost
  ```

-
  ```
  sudo chmod o-r /etc/snort/barnyard2.conf
  ```

- run a perl script:

  ```
  sudo sh -c "./create-sidmap.pl /etc/snort/rules/ > /etc/snort/sid-
  msg.map"
  ```

- run snort:

  ```
  sudo snort -q -i ens33 -u snort -g snort -c /etc/snort/snort.conf
  ```

- run barnyard:

  ```
  sudo barnyard2 -c /etc/snort/barnyard2.conf -d /var/log/snort/ -f
  snort.u2 -w /var/log/snort/barnyard2.waldo -g snort -u snort
  ```

GEOIP

-
  ```
  sudo apt install python3-systemd fail2ban
  ```

-
  ```
  sudo nano /etc/fail2ban/jail.local

  [sshd]
  backend = systemd
  enable = true
  port = 22
  filter = sshd
  maxretry = 3
  bantime = 3600
  findtime = 600
  ```