Lampiran 4 Konfigurasi

```
#prepare server

sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl
libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet

#install from the source

mkdir ~/snort_src && cd ~/snort_src

wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz

tar -xvzf daq-2.0.6.tar.gz

cd daq-2.0.6

./configure && make && sudo make install

cd ~/snort_src

wget https://www.snort.org/downloads/snort/snort-2.9.12.tar.gz

tar -xvzf snort-2.9.12.tar.gz

cd snort-2.9.12

./configure --enable-sourcefire && make && sudo make install


#configuring snort

sudo ldconfig

sudo ln -s /usr/local/bin/snort /usr/sbin/snort


#setting up username and folder structure

sudo groupadd snort

sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

sudo mkdir -p /etc/snort/rules

sudo mkdir /var/log/snort

sudo mkdir /usr/local/lib/snort_dynamicrules
```

```
#permission
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules

#rule
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
sudo cp ~/snort_src/snort-2.9.12/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-2.9.12/etc/*.map /etc/snort
wget https://www.snort.org/rules/community -O ~/community.tar.gz
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-rules/* /etc/snort/rules
wgethttps://www.snort.org/rules/snortrules-snapshot-
29120.tar.gz?oinkcode=oinkcode -O ~/registered.tar.gz

#configuring network and rules
sudo nano /etc/snort/snort.conf
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
```

```
ipvar EXTERNAL_NET !$HOME_NET

# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
include $RULE_PATH/local.rules
include $RULE_PATH/community.rules
```

Iptables.sh

```
#!/bin/bash
KEY="829332923:AAFDIxlD3316zO48H9R57K1sSOO5JQxZcQE"
data=$(mysql --login-path=local -e "use coba;select * from data") # | tail -n +2)
function alert() {
        URL="https://api.telegram.org/bot$KEY/sendMessage"
    text=$1
        curl -s --max-time 5 -d "chat_id=877801183&disable_web_page_preview=1&text=$text&parse_mode=Markdown" $URL
        curl -s --max-time 5 -d "chat_id=877801183&disable_web_page_preview=1&text=sudah terblokir&parse_mode=Markdown" $URL
}
```

```
isi_icmp=$(cat data.csv | awk 'BEGIN{FS=","} $4 != "192.168.1.2" {print $4, $5}'
| grep -v ":" | uniq)

isi_tcp=$(cat data.csv | awk 'BEGIN{FS=","} $4 != "192.168.1.2" {print $1,$4,
$5}' | grep ":" | uniq)


if [ ! -z "$isi_icmp" ]; then

        while IFS= read -r line; do

                sumber_icmp=$(echo $line | cut -d " " -f 1)

                tujuan_icmp=$(echo $line | cut -d " " -f 2)


                iptables -C INPUT -p icmp -s $sumber_icmp -d $tujuan_icmp -j
DROP

                if [ $? -eq 1 ]; then

                        iptables -I INPUT -p icmp -s $sumber_icmp -d $tujuan_icmp
-j DROP

                        echo "Rule berhasil ditambahkan"

                        alert "ada ping  dari $sumber_icmp"

                else

                        echo "Rule sudah ada"

                fi

        done <<< "$isi_icmp"

fi


if [[ ! -z "$isi_tcp" ]]; then

        echo "tcp"

        while IFS= read -r line; do
```

```
                sumber_tcp=$(echo $line | cut -d " " -f 2)
        tujuan_tcp=$(echo $line | cut -d " " -f 3)
                srca=$(echo $sumber_tcp | cut -d ":" -f 1)
                dsta=$(echo $tujuan_tcp | cut -d ":" -f 1)
                dstp=$(echo $tujuan_tcp | cut -d ":" -f 2)
                prt=$(echo $line | cut -d " " -f 1)
                iptables -C INPUT -p tcp --dport $dstp -s $srca -d $dsta -j DROP
                if [ $? -eq 1 ]; then
                        iptables -I INPUT -p tcp --dport $dstp -s $srca -d $dsta -j
DROP
                        echo "Rule berhasil ditambahkan"
                        alert "ada $prt dari $srca"
        else
                echo "Rule sudah ada"
                fi
        done <<< "$isi_tcp"
fi
```

Insert.sh

```
#!/bin/bash
res=$(cat data.csv | cut -d "," -f 2,3,4,5,6 )
#res_icmp=$(cat data.csv | grep "ICMP" | cut -d "," -f 2,3,4,5,6 )
#res=$(echo "$res_tcp""\n""$res_icmp")
while IFS= read loop
  do
        date=$(echo $loop | cut -d "," -f 1)
```

```
        tm=$(echo $loop | cut -d "," -f 2)
        srca=$(echo $loop | cut -d "," -f 3 | cut -d ":" -f 1)
        dst=$(echo $loop | cut -d "," -f 4)
        dsta=$(echo $dst | cut -d ":" -f 1)
        port=$(echo $loop | cut -d "," -f 5)
        if [ $port != "ICMP" ];then
                dstp=$(echo $dst | cut -d ":" -f 2)
        else
                dstp="0"
        fi
    echo "INSERT INTO data (date,time,source,dest,port,proto) VALUES ('$date','$tm','$srca', '$dsta', '$dstp', '$port');"

done <<< $res | mysql -u pmauser -proot coba;
```

File Parse.sh

```
#!/bin/bash
$(cat /var/log/snort/alert | grep -E "[1-9]/[1-9]|[TCPIM]{3,4}|\[\*" | grep -v "Options" | cut -d " " -f 1,2,3,4 | sed '$!N;$!N;s/\n/ /g' | cut -d " " -f 3,5,6,8,9 | sed 's/ /,/g' | sed 's/-/,/g' > data.csv && echo "" > /var/log/snort/alert)
```