Faculdade de Tecnologia de Ourinhos

| **Segurança em Sistemas Operacionais e Redes de Computadores I** | | Professor: Robson Parmezan Bonidias | |
|---|---|---|---|
| **Nome**: Jeanne Dalio Oliveira<br>**Nome**: Lais Camarini Moura<br>**Nome**: Rafael Santos Santini<br>**Nome**: Ralph Schutez Muraro | | **RA**: 0210971921037<br>**RA**: 0210971921035<br>**RA**: 0210972113043<br>**RA**: 0210971921018 | |
| **Curso**: Segurança da Informação | **Turma**: 5º Semestre | **Período**: Noite | **Data**: 07SET2021 |

# Avaliação Contínua: Desafio 05

# IDS(Intrusion Detection System) e IPS (Intrusion Prevention System)


**Vence 28SET2021.**

## INSTRUÇÕES

Os detalhes do trabalho estão nos comentários do script:
Implementar a solução:

**Snort:**
REFERÊNCIAS
1 - https://www.snort.org/
2 - https://www.cloudsavvyit.com/6424/how-to-use-the-snort-intrusion-detection-system-on-linux/
3 - https://e-tinet.com/linux/snort-guia-instalacao/
4 - https://linuxhint.com/snort-ubuntu-tutorial/
5 - https://upcloud.com/community/tutorials/installing-snort-on-debian/

## SCRIPT DE INSTALAÇÃO

```
Chmod +x InstallSnort.sh
sudo ./InstallSnort.sh
```

```
#!/bin/bash
# Script de instalacao do Snort
#Autores: Ralph Muraro (Zappier) e equipe técnica do trabalho


# buscando arquivos necessarios para instalação
clear

#INSTALANDO BIBLIOTECAS NECESSARIAS

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 autoconf libtool

#CRIANDO DIRETORIOS NECESSARIOS

sudo mkdir /etc/snort

sudo mkdir /etc/snort/rules

sudo mkdir /etc/snort/preproc_rules

sudo touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules /etc/snort/rules/local.rules

sudo mkdir /var/log/snort

sudo mkdir /usr/local/lib/snort_dynamicrules


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

# informe a versao do snort a instalar conforme sua necessidade

wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz

wget https://www.snort.org/downloads/snort/snort-2.9.18.1.tar.gz


sudo tar xvzf daq-2.0.7.tar.gz

cd daq-2.0.7

sudo autoreconf -f -i

sudo ./configure && make && sudo make install

cd ..

sudo tar xvzf snort-2.9.18.1.tar.gz

cd snort-2.9.18.1

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

cd ..

# configuração previa do snort

sudo ldconfig

#Snort no Debian é instalado no diretório / usr / local / bin / snort , é uma boa prática criar um link

# simbólico para / usr / sbin / snort .

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

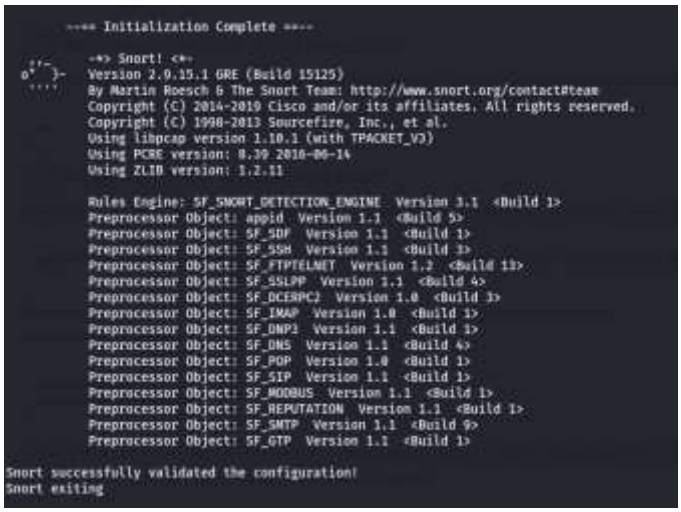
```
# Criando base de regras

wget https://www.snort.org/downloads/community/community-rules.tar.gz -O community-rules.tar.gz

sudo tar -xvzf community-rules.tar.gz -C /etc/snort/rules


sudo snort

sudo ldconfig

sudo snort –version
```

**ANTENÇÃO ALGUMS SISTEMAS JÁ POSSUEM O SNORT NATIVO** QUE PODEM SER INSTALADO COM O SEGUINTE COMANDO

```
sudo apt install snort
snort -V
```


COMANDO DE TESTE DO SNORT

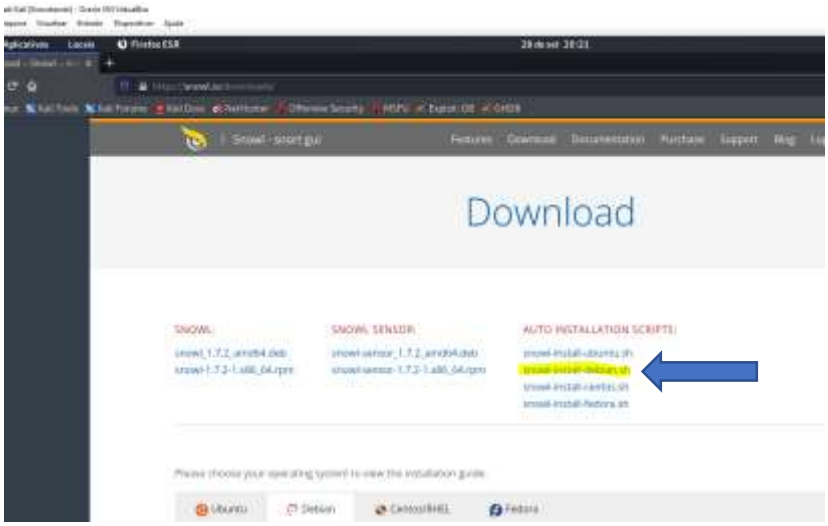
```
snort  -T -c /etc/snort/snort.conf
```



# INSTALAÇÃO DO AMBIENTE GRÁFICO DO SNORT

https://snowl.io/downloads/

Guia de Instalação




Execute a instalação do script disponível no site

```
sudo wget https://snowl.io/download/snowl-install-debian.sh
Chmod +x snowl-install-debian.sh
sudo ./snowl-install-debian.sh
sudo apt install apache2
```

FEITO ISSO PODEMOS IR DIRETO PRA ETAPA 5 DO GUIA DE INSTALAÇÃO DO SITE DIRECIONADO AO DEBIAN