

<b>Segurança em Sistemas Operacionais e Redes de Computadores I</b>		Professor: Robson Parmezan Bonidias	
Nome: Jeanne Dalio Oliveira Nome: Lais Camarini Moura Nome: Rafael Santos Santini Nome: Ralph Schutez Muraro		RA: 0210971921037 RA: 0210971921035 RA: 0210972113043 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
```

## Faculdade de Tecnologia de Ourinhos

```
#!/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 libpcap-dev zlib1g-dev liblua5.1-dev \
libpcap-dev openssl libssl-dev libnet2-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 775 /etc/snort

sudo chmod -R 775 /var/log/snort

sudo chmod -R 775 /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 xvfz daq-2.0.7.tar.gz

cd daq-2.0.7

sudo autoreconf -f -i

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

cd ..

sudo tar xvfz 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
```

## Faculdade de Tecnologia de Ourinhos

# 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
```

**ATENÇÃO** ALGUNS SISTEMAS JÁ POSSUEM O SNORT NATIVO QUE PODEM SER INSTALADO COM O SEGUINTE COMANDO

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

```
(zappier@Lab-Desec) ~/Downloads/Snort  
$ snort -V  
--> Snort! <--  
Version 2.9.15.1 GRE (Build 15125)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
(zappier@Lab-Desec) ~/Downloads/Snort  
$  
wget -O - https://raw.githubusercontent.com/62 sudo ldconfig  
echo 'deb [arch=amd64] http://deb.debian.org/debian/ bullseye main' | sudo tee /etc/apt/sources.list.d/snort.list  
63 sudo snort --version
```

COMANDO DE TESTE DO SNORT

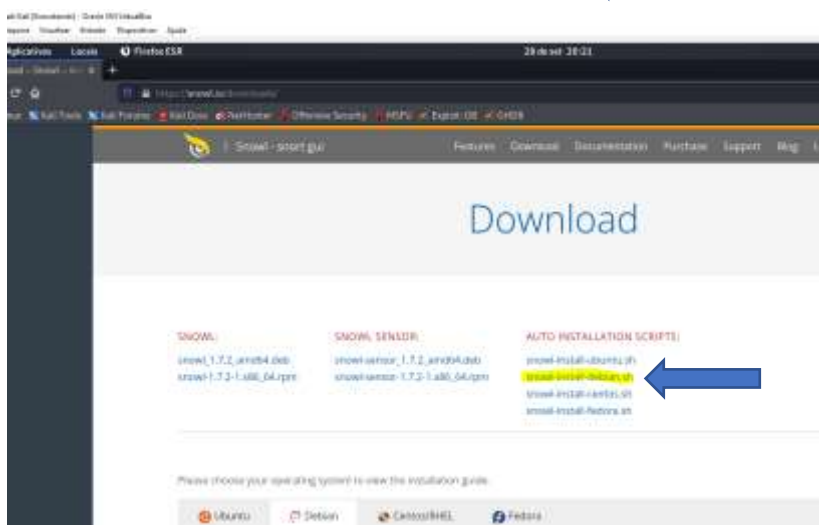
```
snort -T -c /etc/snort/snort.conf
```

```
==== Initialization Complete ====  
  
--> Snort! <--  
Version 2.9.15.1 GRE (Build 15125)  
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team  
Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.  
Copyright (C) 1998-2013 Sourcefire, Inc., et al.  
Using libpcap version 1.10.1 (with TPACKET_V3)  
Using PCRE version: 8.39 2016-06-14  
Using ZLIB version: 1.2.11  
  
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.1 <Build 1>  
Preprocessor Object: appid Version 1.1 <Build 5>  
Preprocessor Object: SF_SDP Version 1.1 <Build 1>  
Preprocessor Object: SF_SSH Version 1.1 <Build 1>  
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 11>  
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>  
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 1>  
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>  
Preprocessor Object: SF_DNP1 Version 1.1 <Build 1>  
Preprocessor Object: SF_DNS Version 1.1 <Build 4>  
Preprocessor Object: SF_POP Version 1.0 <Build 1>  
Preprocessor Object: SF_SIP Version 1.1 <Build 1>  
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>  
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>  
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>  
Preprocessor Object: SF_GTP Version 1.1 <Build 1>  
  
Snort successfully validated the configuration!  
Snort exiting
```

## 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

