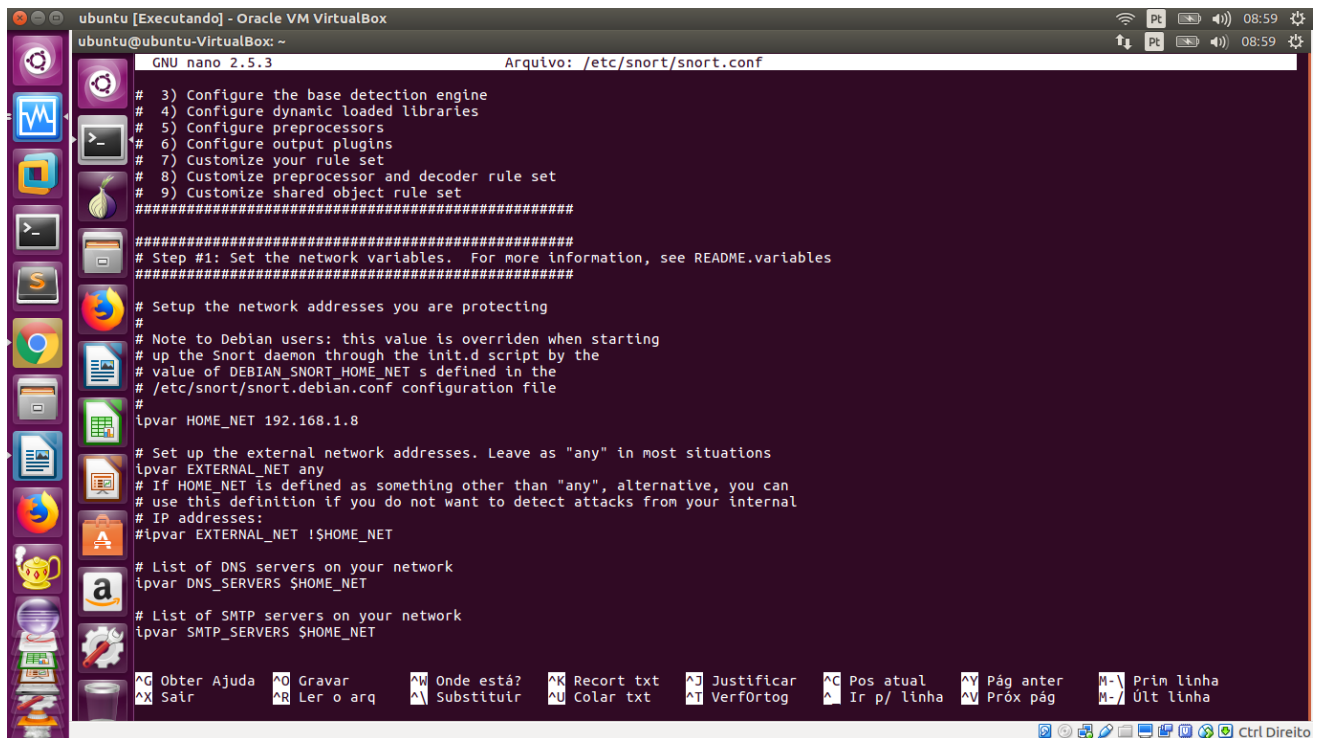


Pratica IDS

Nessa pratica instalei configurei duas Vm um com linux e uma com windows, na Vm linux utilizei os comandos :

sudo apt install snort

Comando para instalar o snort, no qual após a instalação pedi algumas configurações, como a interface no qual o snort vai escutar e um faixa de ip. Também foi preciso configurar o arquivo /etc/snort/snort.conf para colocar o ip da maquina.



```
ubuntu [Executando] - Oracle VM VirtualBox
ubuntu@ubuntu-VirtualBox: ~
GNU nano 2.5.3                               Arquivo: /etc/snort/snort.conf

# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####

#####
# Step #1: Set the network variables.  For more information, see README.variables
#####

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 192.168.1.8

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

Obter Ajuda  Gravar  Onde está?  Recort txt  Justificar  Pos atual  Pág anter  Prim linha
Sair  Ler o arq  Substituir  Colar txt  VerFórtog  Ir p/ linha  Próx pag  Últ linha
Ctrl Direito
```

Após o termino da configuração da Vm Linux iniciei a Vm windows , porem minha maquina não suportou rodar as duas Vms juntas , por isso não conclui a pratica.