VERSAO SNORT: 2.9.7.0 GRE (build 149)

Computador alvo:

-Ambiente virtualizado(Oracle VM VirtualBox Manager)

-SO: Ubuntu 20.04.1 LTS

Computador teste:

-Ambiente virtualizado(Oracle VM VirtualBox Manager)

-SO: Kali GNU/LINUX ROLLING, 2020.4

Tarefa 2)

Ex.2 Em particular anote a função das opções -v, -d, -e, -l, -c e -T.

Uma imagem com texto

Descrição gerada automaticamente

Opção -v : Output mais detalhado

Opção -d : Largar a camada de aplicação

Opção -e : Apresentar o cabeçalho da informação da segunda camada

Opção -l : Ficheiro log para a diretoria

Opção -c : Usar o ficheiro de regras

Opção -T : Testar e reportar a atual configuração do Snort

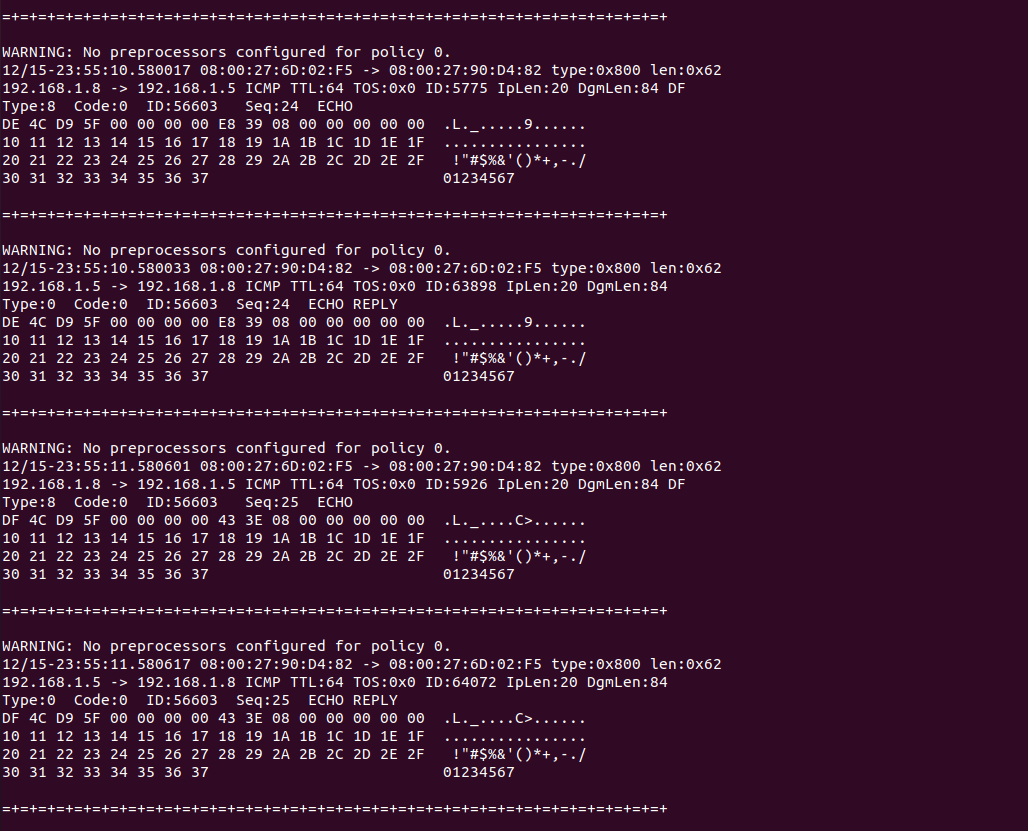
EX.3 a) Anote o que observa no ecrã, procurando justificar a atividade.

Uma imagem com texto

Descrição gerada automaticamente

Tráfego na rede captado pelo SNORT

EX.4 a) Anote o que observa no ecrã do computador alvo, procurando justificar a atividade.



Snort deteta o ping(ICMP) feito a partir do computador teste

EX.5 a) Anote o que observa no ecrã.

Uma imagem com texto

Descrição gerada automaticamente

Resultado do modo Sniffer do Snort

Tarefa 4)

Ex 6 a) Quantos pacotes o Snort recebeu e qual a distribuição desses pacotes por protocolos fudamentais (TCP, UDP, ICMP e ARP)? Justifique a observação com base na atividade criada.

Uma imagem com mesa

Descrição gerada automaticamente

Relativamente aos pacotes TCP, UDP e ICMP, podem ser justificados por trafego na rede não relevante, tal como aceder a algum website, stream, pings, entre outros. Os pacotes arp detetados resultam da tentativa de arp-poisinig por parte do computador teste

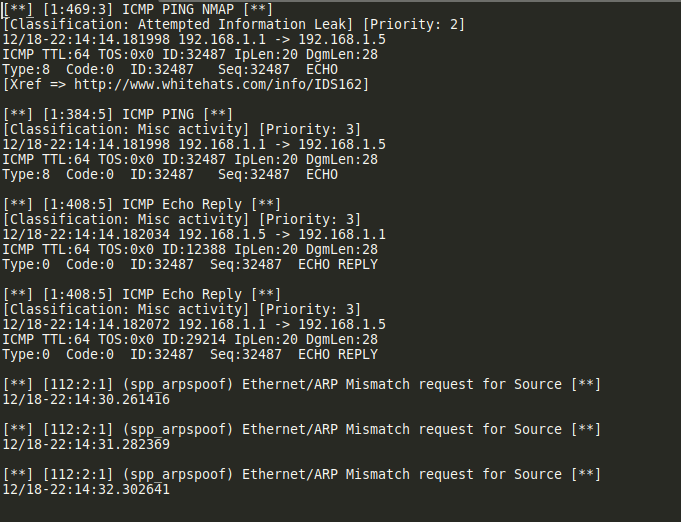
b) Quantos alertas foram registados (se tudo correu bem, devem ter sido registados vários alertas)?

Uma imagem com texto

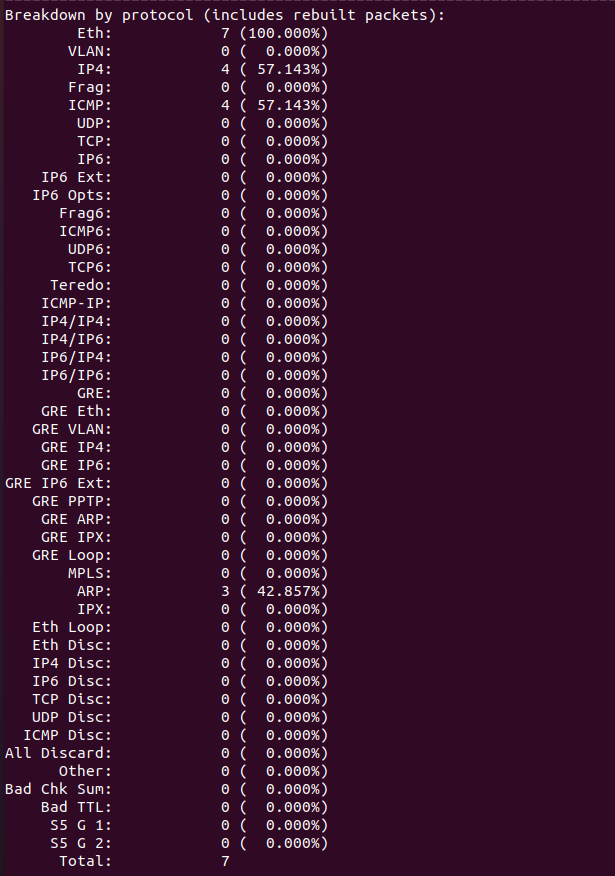
Descrição gerada automaticamente

Foram detetados 7 alertas.

Copie para o relatório o conteúdo do ficheiro de alertas, juntamente com o conteúdo do ficheiro “snort.log.\*” e comente o seu conteúdo.



As primeiras quatro entradas são as tentativas de ping do computador teste para o computador alvo. As três ultimas representam o alerta de arp-poisining



Pacotes que deram origem aos alertas. Os três Arp’s representam os 3 alertas de arp -poisining.

Tarefa 5)

siga as instruções do seu servidor para o ativar, registando o processo no seu logbook.

Uma imagem com texto

Descrição gerada automaticamente

É necessário ter em atenção que ao usar as regras que ditam o ficheiro “snort\_detection.conf” foram detetados 0 alertas. Posto isto, o ficheiro utilizado passou a ser o ficheiro original, “snort.conf”

Ex-7 a. Quantos pacotes o Snort recebeu?

Uma imagem com texto

Descrição gerada automaticamente

Recebeu 537

b. Qual o número de pacotes TCP?



391 pacotes TCP

c. Quantos alertas foram gerados?

Uma imagem com texto

Descrição gerada automaticamente

Foram gerados 18 alertas

Anote todos os alertas detetados e justifique-os à luz da atividade criada. Consegue localizar os alertas gerados pelo ataque ARP poisoning? Justifique.

Alertas relativos ao arp-poisonigUma imagem com texto

Descrição gerada automaticamente

Uma imagem com texto, placa, captura de ecrã

Descrição gerada automaticamente

Alertas relativos à conexão Telnet.

Tarefa 6)

Ex2) Alertar, quando existir trafego TCP, de qualquer porta para a porta 27374

EX 6 a. Quantos pacotes recebeu o Snort?

Uma imagem com texto

Descrição gerada automaticamente

Recebeu 1968 pacotes

b. Quantos alertas foram gerados?



Foram registados quatro alertas.

EX 7 a. Anote todos os alertas detetados.

Uma imagem com texto

Descrição gerada automaticamente

b. Consegue localizar os alertas gerados pela atividade que acabou de gerar?

Todos os alertas apresentados acima são relativos à tentativa, sem sucesso, de conexão telnet para a porta 27374

c. Acha que o alerta gerado está de acordo com o objectivo da regra, anteriormente enunciado (ver 2, acima)?

Sim

Classificaria este alerta como um “Falso Positivo”?

Sim, uma vez que uma tentativa de conexão para uma porta fechada não deve ser relevante.

Uma imagem com desporto, jogo atlético, jogador

Descrição gerada automaticamente