ATIVIDADE SOMATIVA: SEMANAS 7 E 8

Detecção de Intrusão através da ferramenta Snort

Pré-requisitos:

1. Efetue download da máquina virtual Kali Linux. Link para download da VM: https://secplab.ppgia.pucpr.br/ftp/jgeremias/Kali-Linux.zip
   a. Login/senha: root/toor
2. Efetue o download da máquina virtual contendo o Snort instalado. Link para download da VM: https://secplab.ppgia.pucpr.br/ftp/jgeremias/Linux.zip
   a. Login/senha: user/user

Etapa 1: Configurar o snort para detectar ping

Nessa etapa, você irá configurar o snort para detectar ping a partir de qualquer máquina. Na etapa seguinte você irá configurar o snort para detectar DoS.

1. Verifique as configurações do Snort, para isso o seguinte comando deve ser utilizado:
   sudo snort -T -c /etc/snort/snort.conf -i ens33

```
++++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
0 Snort rules read
    0 detection rules
    0 decoder rules
    0 preprocessor rules
0 Option Chains linked into 0 Chain Headers
0 Dynamic rules
++++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       0       0       0       0
|     any       0       0       0       0
|      nc       0       0       0       0
|     s+d       0       0       0       0
+------------------------------------------------------------------------------
```

Figure 1 - A saída apresenta que nenhuma regra está em operação.

2. Crie uma regra simples no Snort para gerar um alerta sempre que uma mensagem ICMP (ping) for identificada. Para isto, utilizando o editor de texto de sua preferência, inserindo a seguinte linha no arquivo de configuração de regras.
   Local do arquivo: sudo gedit /etc/snort/rules/local.rules
   Comando para ser inserido no arquivo (salve o arquivo após inserir o comando):
   alert icmp any any -> any any (msg:"PING detectado"; sid:10000001;)

3. Verifique e valide as configurações do snort novamente, execute o comando abaixo:
   sudo snort -T -c /etc/snort/snort.conf -i ens33

```
+++++++++++++++++++++++++++++++++++++++++++++++++++
Initializing rule chains...
1 Snort rules read
    1 detection rules
    0 decoder rules
    0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       0       0       0       0
|     any       0       0       1       0
|      nc       0       0       1       0
|     s+d       0       0       0       0
+-----------------------------------------------------------------------------
```

Figure 2- A saída anterior mostra que a configuração foi aplicada e validada com sucesso (1 regra em operação).

4. Inicie o Snort para isso execute o seguinte comando:
   sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33

Após executar o comando acima, inicialmente não haverá nenhuma saída. O Snort está monitorando todos os pacotes que chegam na interface ens33. Quando um pacote corresponder a essa regra, será gerado um alerta na tela.

Para gerar o tráfego ICMP através de outro *host* execute um ping para o IP da máquina que executa o Snort. Exemplo de saída:

```
MP} 192.168.59.139 -> 192.168.59.132
05/05-08:34:48.052338  [**] [1:10000001:0] PING detectado [**] [Priority: 0] {IC
MP} 192.168.59.132 -> 192.168.59.139
05/05-08:34:49.062603  [**] [1:10000001:0] PING detectado [**] [Priority: 0] {IC
MP} 192.168.59.139 -> 192.168.59.132
05/05-08:34:49.062647  [**] [1:10000001:0] PING detectado [**] [Priority: 0] {IC
MP} 192.168.59.132 -> 192.168.59.139
05/05-08:34:50.065314  [**] [1:10000001:0] PING detectado [**] [Priority: 0] {IC
MP} 192.168.59.139 -> 192.168.59.132
```

Figure 3 - Exemplo do tráfego ICMP

Utilize "*ctrl+c*", para terminar o monitoramento Snort.

Informações complementares:

➔ Interface física da VM se chama **ens33** (pode variar e.g.: ens33, ens34, ensXX), distribuições mais antigas do linux tipicamente utilizam a nomenclatura de **eth0/eth1/etc** para as interfaces de rede.

Etapa 2: Ataque de negação de serviço

Nessa etapa você deverá analisar o impacto de um ataque de negação de serviço

5. Na máquina com SNORT, execute o seguinte comando:
   - htop
   - Esse comando apresenta o monitor de recursos do sistema operacional.
6. No Kali, execute o seguinte comando:
   - sudo hping3 -c 10000 -d 120 -S -p 80 --flood --rand-source **<IP_DESTINO>**
   - Esse comando realiza o ataque de negação de serviço no IP selecionado.
7. Na máquina com SNORT, visualize o consumo de CPU da máquina – Pressione "ctrl +c" para parar o ataque no Kali.

Etapa 3: Detecção de ataque negação de serviço

Nessa etapa você deverá configurar o snort para detectar ataque de negação de serviço. Essa atividade poderá ser realizada de forma individual ou em equipe (máximo três estudantes).

8. Pesquise e cadastre uma regra para monitoramento de ataque do tipo DDoS no Snort, e aplique o monitoramento da interface de rede.
9. No sistema operacional Kali realize um ataque de DDoS para o IP da VM Snort.
10. Produza um vídeo de captura de tela, de no máximo três minutos, apresentando:
    - Nome dos integrantes da equipe;
    - Configuração do snort para detectar ataque de negação de serviço;
    - Descrição do ataque e a respectiva detecção de intrusão, **narrando detalhes de cada execução**.
11. O estudante deverá entregar um arquivo ".txt" contendo o nome dos integrantes da equipe e o link do vídeo produzido.

Informações complementares:

Criar um vídeo demostrando o funcionamento da solução. Este vídeo deve estar postado no YouTube como não listado (visualização privada) até a data especificada, deve ter duração máxima de 3 min. Para gravar a tela e você falando ao mesmo tempo recomendo utilizar o "Screencast-o-matic" https://screencast-o-matic.com que é gratuito e fácil de usar.