INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Rede
Aula 10: Instalação e Configuração do Snort no Ubuntu.

Olá, meus alunos!! Como é que vocês vão? Vamos lá!!! Preparados???

Snort

O Snort é um Sistema de Detecção de Intrusão de Rede (NIDS). Ele monitora os pacote enviados e recebidos em uma interface de rede específica. O snort pode detectar tentativas de ataques, malwares, sistemas comprometidos e violações de políticas de segurança usando assinatura e análise dos protocolos de rede.

O Snort é um dos IDS baseados em rede mais usados. Éle é gratuito, código fonte aberto, e disponível em várias plataformas. Embora o Snort seja capaz de muito mais do que apenas monitorar a rede, na aula de hoje iremos instalar, configurar e executar o Snort no modo NIDS nasua configuração básica de monitoramento.

Instalação

Antes de instalar o snort, você precisará:

01. Instalando alguns softwares pré-requisito:

```
sudo apt instale -y gcc libpcre3-
dev zlib1g-dev libluajit-5.1-
dev libpcap-dev openssl libssl-
dev libnghttp2-dev libdumbnet-
dev bison flex libdnet
```

Configurar o Snort no Ubuntu a partir do código-fonte consiste em alguns passos: baixar o código, configurá-lo, compilar, instalá-lo em um diretório apropriado e, finalmente, configurar as regras de detecção.

02. Criando uma pasta temporária e depois entrando nela.

```
mkdir ~/snort_src && cd ~/snort_src
```

O Snort usa o Data Acquisition Library (DAQ) para fazer captura de pacotes.

03. Faça o download do pacote fonte DAQ

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

04. Extraia o código-fonte e salte para o novo diretório.

```
tar -xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
```

05. Execute o script de configuração e, em seguida, compile o programa com make para instalar o DAQ.

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

06. Com o DAQ instalado, você pode voltar ao Snort, voltar para a pasta que criamos.

```
cd ~/snort_src
```

08. Baixe o código-fonte do Snort com wget. Caso dê algum problema, procure no site qual é a versão mais recente do Snort.

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

09. Quando o download estiver concluído, extraia a fonte e mude para o novo diretório.

```
tar -xvzf snort-2.9.13.tar.gz
cd snort-2.9.13
```

10. Agora iremos configurar e instalar o Snort.

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

Configuração

11. Depois da instalação deveremos atualizar as bibliotecas.

```
sudo ldconfig
```

12. Snort no Ubuntu é instalado no diretório /usr/local/bin/snort, é recomendado criar um link simbólico para /usr/sbin/snort, facilitando a localização do comando.

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

13. Para executar o Snort, iremos criar um novo usuário não privilegiado e um novo grupo de usuários.

```
sudo groupadd snort
sudo useradd snort -r -
s /sbin/nologin -c SNORT_IDS -g snort
```

14. Criando uma estrutura de pastas para colocar as configurações do Snort.

```
sudo mkdir -p /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
```

15. Defina as permissões para os novos diretórios.

```
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
```

16. Crie novos arquivos para as listas branca e negra, bem como as regras locais.

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

17. Copia os arquivos de configuração da pasta de download.

```
sudo cp ~/snort_src/snort-
2.9.13/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-
2.9.13/etc/*.map /etc/snort
```

Agora, precisamos baixar as regras de detecção do Snort para identificar possíveis ameaças. O Snort fornece três conjuntos de regras:

- Comunitárias: estão livremente disponíveis, embora ligeiramente limitadas.
- Usuários Registrados: ao registrar-se gratuitamente em seu site, você obtém acesso ao um outro conjuntos de regras.
- Assinantes: regras mais completas e atualizadas disponíveis para usuários com assinatura.

Iremos utilizar as regras comunitárias.

18. Baixando as regras comunitárias.

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

19. Extrair as regras e copiar para a pasta de configuração.

```
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-
rules/* /etc/snort/rules
```

20. Por padrão, o Snort no Ubuntu espera encontrar vários arquivos de regras diferentes que não estão incluídos nas regras da comunidade. Entretanto, burlar essa característica comentando as linhas desnecessárias usando o comando.

```
sudo sed -i 's/include \$RULE\_PATH/#include
\$RULE\_PATH/' /etc/snort/snort.conf
```

21. Agora iremos copiar e editar o snort.conf para modificar alguns parâmetros.

```
sudo cp /etc/snort/snort.conf /etc/snort/snort.conf
.bkp
```

```
sudo gedit /etc/snort/snort.conf
```

22. Encontre estas seções mostradas abaixo no arquivo de configuração e altere os parâmetros.

Os endereços de rede que você irá tentar identificar invasores.

```
ipvar HOME_NET 192.168.10.0/24
```

Caminho para seus arquivos de regras

```
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

Configure a saída do unified2 para registrar logs no arquivo snort.log

```
output unified2: filename snort.log, limit 128
```

Na parte inferior do arquivo encontre (removendo o comentário) ou acrescente a lista de regras local.rules para permitir que o Snort carregue quaisquer regras personalizadas.

```
include $RULE_PATH/local.rules
```

Agora iremos adicione o conjunto de regras da comunidade na parte final do arquivo.

```
include $RULE_PATH/community.rules
```

23. Configuração concluida, salve as alterações e saia do editor.

Validando a Configuração

24. Teste a configuração usando o parâmetro -T.

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

O resultado deverá ser algo do tipo:

```
Snort successfully validated the configuration!
Snort exiting
```

Testando

Para testar se o Snort está registrando alertas, adicione uma regra de alerta nas conexões ICMP de entrada ao arquivo local.rules. Para isso, abra suas regras locais em um editor de texto.

```
sudo gedit /etc/snort/rules/local.rules
```

Em seguida, adicione a seguinte linha ao arquivo.

```
alert icmp any any -
> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
```

A regra consiste nas seguintes partes:

- Ação: alertar;
- Protocolo: ICMP;
- Endereço de origem e porta: qualquer (any) para incluir todos os endereços e portas;
- Endereço de destino e porta: $HOME_NET, minha rede conforme declarado na configuração e qualquer porta;
- Registro de log: mensagem, identificador de regra (sid) para as regras locais precisa ser 1000001 ou superior e o número da versão.

Salve as regras locais e saia do editor.

Inicie o Snort com as opções -A para imprimir os alertas. Você precisará selecionar a interface de rede, usuário, grupo e arquivo de configuração.

```
sudo snort -A console -
i enp0s8 -u snort -g snort -
c /etc/snort/snort.conf
```

Execute um ping a partir de qualquer outro computador. Você deve ver um aviso para cada chamada ICMP no terminal executando o Snort.

```
05/19-15:37:33.191327  [**] [1:10000001:1]
ICMP test [**] [Priority: 0] {ICMP}
192.168.10.2 -> 192.168.10.1
```

O Snort registra os alertas em /var/log/snort/snort.log. Você pode ler os logs com o comando.

```
snort -r /var/log/snort/snort.log.
```

Atividades

01. Siga os passos da aula, faça a instalção, configuração e teste do Snort para mensagens ICMP.

02. Faça um registro no Snort e obtenha as regras de usuário registrado.

03. Escreva suas próprias regras de detecção e teste.