SNORT

Ary Felipe Farah e Silva

1 Configuração Inicial

Feito

2 Endereços IP

`ifconfig`

IP Kali: 192.168.236.130

IP Linux: 192.168.236.128

3 Configuração e Testes das Regras

3.1 Verificar as regras do snort já existentes:

`sudo snort -T -c /etc/snort/snort.conf -i ens33`

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

3.2 Adicionar regras no snort por meio da edição do arquivo de regras locais:

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

Inserir a regra para identificar o ping (ICMP):

`alert icmp any any -> $HOME_NET any (msg:"Ping detectado!"; GID:1; sid:10000001;rev:001; classtype:icmp-event;)`

```
  nano 2.6.3          Arquivo: /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg:"Ping detectado!";
```

3.3 Gravar o arquivo, finalizando a edição.

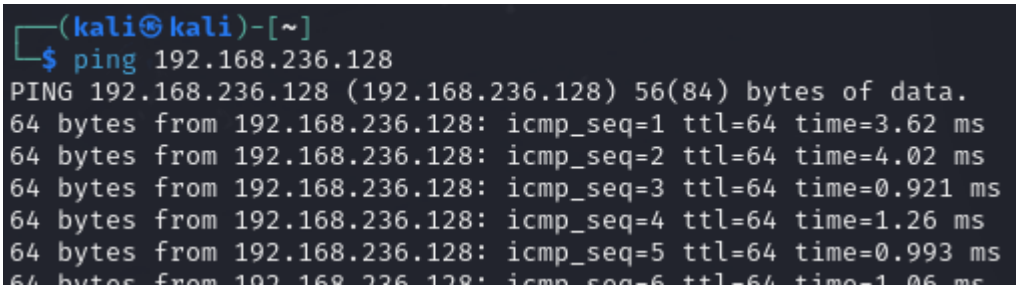
Validar as configurações do snort:

```
sudo snort -T -c /etc/snort/snort.conf -i ens33
```

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

Efetuar um ping à partir do Kali Linux para testar:

```
ping 192.168.236.128
```




```
06/17-08:50:00.754995  [**] [1:10000001:1] Ping detectado! [**] [Classification:
 Generic ICMP event] [Priority: 3] {ICMP} 192.168.236.128 -> 192.168.236.130
```

Inicializar o snort como NIDS

```
sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i
ens33 &
```

```
user@virtual-machine:~$ sudo /usr/local/bin/snort -A console -q -u snort -g snor
t -c /etc/snort/snort.conf -i ens33 &
[2] 4246
```

```
user@virtual-machine:~$ sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/
snort.conf -i ens33 &
[5] 5406
```

Inserir a regra para identificar acesso às páginas web (HTTP):

```
alert tcp any any -> any 80 (msg:"Tentativa de acesso web –porta 80"; sid:1000002;)
```

```
alert tcp any any -> any 80 (msg:"Tentativa de acesso web –porta 80";
                                                                    ...
```

Para testar a detecção de acesso HTTP, abrir o browser do Kali Linux e inserir o endereço da VM Linux:

```
http://192.168.236.128
```

```
user@virtual-machine:~$ 06/17-08:52:53.279560  [**] [1:1000002:0] Tentativa de acesso web –porta
 80 [**] [Priority: 0] {TCP} 192.168.236.130:47706 -> 192.168.236.128:80
```

Inserir a regra para identificar acesso FTP:

```
alert tcp any any -> $HOME_NET 21 (msg:"FTP connection attempt"; sid:1000003; rev:1;)
```

```
alert tcp any any -> $HOME_NET 21 (msg:"FTP connection attempt"; sid:1000003; rev:1;)
```

Para testar a detecção de acesso FTP, executar, no Kali Linux:

```
ftp 192.168.236.128
```

```
user@virtual-machine:~$ 06/17-08:56:51.131441  [**] [1:1000003:1] FTP connection attempt [**] [P
riority: 0] {TCP} 192.168.236.130:46122 -> 192.168.236.128:21
```

```
nmap -sS 192.168.236.128
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.236.128
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 07:57 EDT
Nmap scan report for 192.168.236.128
Host is up (0.0023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:0B:D4:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.91 seconds
```

```
06/17-08:57:53.409305  [**] [1:1000002:0] Tentativa de acesso web –porta 80 [**] [Priority: 0] {
TCP} 192.168.236.130:41457 -> 192.168.236.128:80
06/17-08:57:53.411969  [**] [1:1000002:0] Tentativa de acesso web –porta 80 [**] [Priority: 0] {
TCP} 192.168.236.130:41457 -> 192.168.236.128:80
```

port scan com TCP:

```
alert tcp any any -> any any (msg: "Scan Detect TCP"; sid:1000005; rev:2;)
```

```
alert tcp any any -> any any (msg: "Scan Detect TCP"; sid:1000005; rev:2;)
```

Para testar a detecção de port scan TCP, usar o nmap no Kali Linux:

```
nmap -sS 192.168.236.128
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.236.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 07:59 EDT
Nmap scan report for 192.168.236.128
Host is up (0.0024s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:0B:D4:D5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

```
user@virtual-machine:~$ 06/17-09:00:20.544260  [**] [1:1000003:1] FTP connection attempt [**] [P
riority: 0] {TCP} 192.168.236.130:49839 -> 192.168.236.128:21
06/17-09:00:20.552080  [**] [1:1000002:0] Tentativa de acesso web –porta 80 [**] [Priority: 0] {
TCP} 192.168.236.130:49839 -> 192.168.236.128:80
06/17-09:00:20.552554  [**] [1:1000002:0] Tentativa de acesso web –porta 80 [**] [Priority: 0] {
TCP} 192.168.236.130:49839 -> 192.168.236.128:80
```

A mensagem que apareceu não é a mesma pedida, mesmo deletando as outras regras

Inserir a regra para identificar port scan com UDP:

```
alert udp any any -> any any (msg: "Scan Detect UDP"; sid:1000003; rev:2;)
```

```
alert udp any any -> any any (msg: "Scan Detect UDP"; sid:1000003; rev:2;)
```

Para testar a detecção de port scan UDP, usar o nmap no Kali Linux:

`nmap -sU 192.168.236.128`

```
06/17-09:07:57.661121  [**] [1:10000001:1] Ping detectado! [**] [Classification: Generic ICMP ev
ent] [Priority: 3] {ICMP} 192.168.236.128 -> 192.168.236.130
```

A mensagem que apareceu não é a mesma pedida, mesmo deletando as outras regras

Inserir a regra para identificar acesso ao banco de dados MySql:

`alert tcp any any -> any 3306 (msg:"Tentativa de acessar o MySql"; sid:1000003;)`

```
alert tcp any any -> any 3306 (msg:"Tentativa de acessar o MySql"; sid:1000003;)
```

Para testar, executar na VM Kali Linux:

`mysql -u root -p -h 192.168.236.128`

pediu senha e não consegui terminar