
DESEC®
INFORMATION SECURITY

Burlando Mecanismos de Defesa - IDS - Sistema de Detecção de Intrusos

tags: IDS, IPS, snort

O Kali Linux passou um tempo sem ter o Snort disponível no seu repositório. Recentemente voltou a incluí-lo , mas agora na versão 3. A aula do Novo Pentest Profissional - NPP que trata diretamente do Snort foi gravada com a versão 2.

Estaremos mostrando o que mudou, e como acompanhar as aulas usando o Snort v3.

> **Atenção**: Neste roteiro, quando utilizarmos os caracteres "$" ou "#" antes dos comandos, estaremos informando se o comando deve ser executado como usuário normal ($) ou como root (#). Esse símbolo não faz parte da execução, então não precisa escrevê-lo na hora de executar o referido comando.

Para help em linha de comando digite:

```
$ snort -?
```

Vamos executar todos os comandos como "root", então digite o comando abaixo se você estiver como um usuário comum:

```
$ sudo -s -H
```

Com o comando acima agora estamos como root (#).

Agora vamos aproveitar e verificar se nosso sistema encontra-se atualizado. Se não estiver esse comando abaixo já vai atualizá-lo:

```
# apt update ; apt dist-upgrade -y
```

Aproximadamente no minuto 1:20 o Longatto instala o snort com o comando abaixo. Podemos fazer o mesmo, não existe diferença entre as versões neste comando:

```
# apt install snort snort-common snort-common-libraries snort-rules-default
```

No minuto 2:10 o Longatto fala que vai estar com outro Kali que será usado como a máquina do atacante. Você pode usar a sua máquina hospedeira (real) para atacar a máquina virtualizada com Snort. Para isso você deve deixar a sua placa de rede da máquina virtualizada no modo "Bridge".

Aproximadamente no minuto 2:35 o Longatto fala sobre o arquivo de configuração do snort. No snort v2 é o "snort.conf" e no Snort v3 é o "snort.lua". Eles se encontram no diretório "/etc":

```
# cd /etc
```

Então todas as vezes que o Longatto falar sobre o "snort.conf", nós que estamos utilizando o Snort v3 vamos usar o "snort.lua".

Podemos usar o comando abaixo para validar o arquivo de configuração do Snort v3, e se estiver tudo correto ele retorna no final a mensagem "Snort successfully validated the configuration (with 0 warnings)."

```
# snort -c /etc/snort/snort.lua
```

Agora no minuto 3:50 (aproximadamente) o Longatto fala sobre o arquivo de configuração do snort v2 que é o "snort.conf". Você pode dar uma olhada rápida no conteúdo do arquivo "snort.lua". Logo no início dele temos a sessão "1. configure defaults" que faz referência para as configurações utilizadas como padrão que estão no arquivo "snort_defaults.lua" e que é incluído através da referência abaixo:

```
include 'snort_defaults.lua'
```

É interessante dar uma olhada também no conteúdo do arquivo "snort_defaults.lua" presente no mesmo diretório para se familiarizar com o novo formato.

No minuto 4:35 o Longatto fala sobre onde ficam as referências às regras (rules) no "snort.conf" do Snort v2. No Snort v3, vamos fazer um pouco diferente. Criamos inicialmente um diretório "rules" dentro do "/etc" com o comando abaixo:

```
# mkdir /etc/rules
```

Neste diretório "/etc/rules" vamos adicionar as regras que queremos que fiquem ativadas no momento de execução do Snort v3.

Todas as regras que vieram por padrão na instalação do Snort v3 estão no diretório "/etc/snort/rules". Vamos copiar inicialmente a regra "icmp-info.rules", que será utilizada nos nossos exemplos:

```
# cp /etc/snort/rules/icmp-info.rules /etc/rules/
```

Essa regra encontra-se no formato do snort v2. Vamos mudá-la para a sintaxe do Snort v3 com o comando abaixo:

```
# snort2lua -c /etc/snort/rules/icmp-info.rules -r
/etc/rules/icmp-info.rules
```

Com o comando acima adequamos a regra para funcionar no Snort v3.

No minuto 4:52 o temos a execução do comando snort. Se executarmos o mesmo comando no Snort v3 ele vai apenas verificar a sintaxe do arquivo de configuração "snort.lua".

No snort v3 para termos o mesmo retorno mostrado no vídeo, devemos digitar o comando abaixo:

```
# snort -c /etc/snort/snort.lua -A fast --tweaks snort.debian -i eth0
--rule-path=/etc/rules
```

Se você estiver com dúvidas qual a interface de rede que você tem que passar no parâmetro "-i" digite o comando abaixo para listá-las:

```
# ip -br a
```

Para executar o snort no modo silencioso usamos o parâmetro "-q" e o comando fica da forma abaixo:

```
# snort -c /etc/snort/snort.lua -A fast --tweaks snort.debian -i eth0
--rule-path=/etc/rules -q
```

Na nossa máquina atacante executamos o comando "ping" (negrito) abaixo:

```
$ ping -c1 192.168.15.8
PING 192.168.15.8 (192.168.15.8) 56(84) bytes of data.
64 bytes from 192.168.15.8: icmp_seq=1 ttl=64 time=0.399 ms

--- 192.168.15.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.399/0.399/0.399/0.000 ms
```

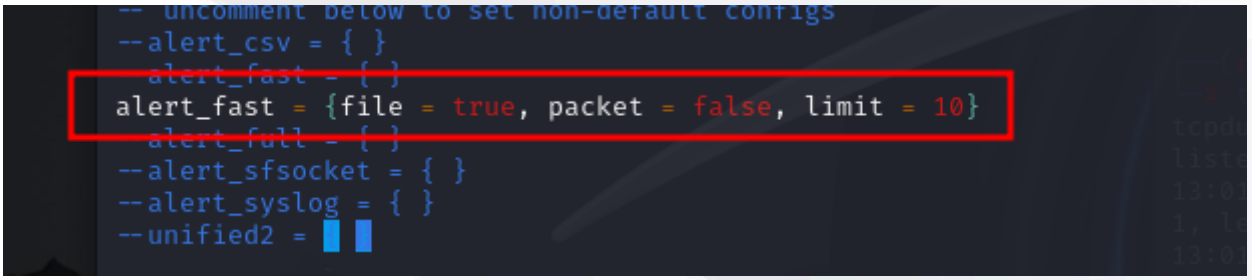
E obtemos um retorno do snort semelhante a este abaixo

```
03/26-13:28:56.141243 [**] [1:366:7] "ICMP PING *NIX" [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.15.3 -> 192.168.15.8
03/26-13:28:56.141243 [**] [1:384:5] "ICMP PING" [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.15.3 -> 192.168.15.8
03/26-13:28:56.141324 [**] [1:408:5] "ICMP Echo Reply" [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.15.8 -> 192.168.15.3
```

No minuto 6:00 aproximadamente é mostrado os arquivos de log do snort v2. Para termos o arquivo de log "alert" no snort v3 temos que adicionar na sessão "7. configure outputs" do arquivo "snort.lua" a linha abaixo:

```
alert_fast = {file = true, packet = false, limit = 10}
```

Fica assim :



Salve o arquivo e agora execute o comando abaixo:

```
# snort -c /etc/snort/snort.lua -i eth0 -A alert_fast -u snort -g snort -m
027 -l /var/log/snort --tweaks /etc/snort/snort.debian
--rule-path=/etc/rules -q
```

Execute novamente o ping a partir da máquina atacante, e verifique o diretório de logs do snort:

```
# ls -l /var/log/snort/
```

O resultado deve ser semelhante a este:

```
# ls -l /var/log/snort
total 4
-rw-r--r-- 1 snort adm 419 Mar 26 14:40 alert_fast.txt
```

Verificamos o conteúdo do arquivo "alert_fast.txt" gerado após o ping com o comando (em negrito) abaixo:

```
# cat  /var/log/snort/alert_fast.txt
03/26-14:40:49.546757 [**] [1:366:7] "ICMP PING *NIX" [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.15.3 -> 192.168.15.8
03/26-14:40:49.546757 [**] [1:384:5] "ICMP PING" [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.15.3 -> 192.168.15.8
03/26-14:40:49.546871 [**] [1:408:5] "ICMP Echo Reply" [**] [Classification:
Misc activity] [Priority: 3] {ICMP} 192.168.15.8 -> 192.168.15.3
```

Agora deixe um comando ping executando da máquina do atacante e verifique o log, em tempo real, com o comando abaixo:

```
# tail -f /var/log/snort/alert_fast.txt
```

No minuto 7:15 é mostrado como direcionar a saída apenas no terminal, alterando o parâmetro "-A fast" para "-A console".

Mas no Snort v3 quando for necessário ver a saída apenas no terminal primeiro comente a linha de referência ao log no arquivo "snort.lua", adicionando dois hifens antes dela, conforme abaixo:

```
--alert_fast = {file = true, packet = false, limit = 10}
```

Salve o arquivo após a modificação e em seguida execute novamente agora com a sintaxe abaixo:

```
# snort -c /etc/snort/snort.lua -i eth0 -A fast -u snort -g snort  --tweaks
snort.debian --rule-path=/etc/rules -q
```

Agora temos a saída apenas no terminal e não mais no arquivo de log.

Burlando Mecanismos de Defesa - Entendendo e criando regras de IDS

tags: IDS, IPS, snort

Vamos manter a configuração sem gerar log, da forma que configuramos no final do vídeo passado.

No minuto 00:40 o Longatto executa o comando para ativar o Snort v2, no Snort v3 vamos utilizar o comando abaixo:

```
# snort -c /etc/snort/snort.lua -i eth0 -A fast -u snort -g snort  --tweaks
snort.debian --rule-path=/etc/rules -q
```

A regra criada por Longatto no minuto 04:00 será a mesma que usaremos no Snort v3.

Depois de criada, no Snort v3 vamos colocá-la dentro do diretório "/etc/rules" para que seja lida pelo Snort. Não precisamos alterar nada no arquivo de configuração.

Em seguida paramos o Snort se ele estiver ativo, e ativamos ele novamente com o comando abaixo. Dessa forma a regra que criamos já vai estar funcionando:

```
# snort -c /etc/snort/snort.lua -i eth0 -A fast -u snort -g snort  --tweaks
snort.debian --rule-path=/etc/rules -q
```

Podemos utilizar o comando nmap abaixo:

```
# nmap -sS -Pn --top-ports=10 <ip-alvo> --open --max-retries=0 -r
```

Com o comando acima vamos escanear, apenas uma vez (--max-retries=0), as 10 portas (--top-ports=10) mais comuns, em ordem crescente (-r), do ip <ip-alvo> (informe aqui o IP do alvo).