

# Estudo Técnico - Bypass de Regras de IDS

+ O objetivo é que eu aprenda a fazer uma pesquisa para aprender a burlar as regras existentes de qualquer bypass que me apareça

+ Pelo menos nesse módulo eu entendi a importância de se saber a versão do Firewall usado pela empresa. Para que eu possa estudá-lo e realizar as adaptações adequadas aos meus teste afim de que se chegue ao bypass das regras.

+ O princípio é que se entenda o que os filtros buscam na interação para fazer a declaração ao administrador, para então modificar as interações que fazemos

+ É necessário que eu use o firewall em um ambiente controlado para verificar a ação dessas regras e os requisitos de cada uma

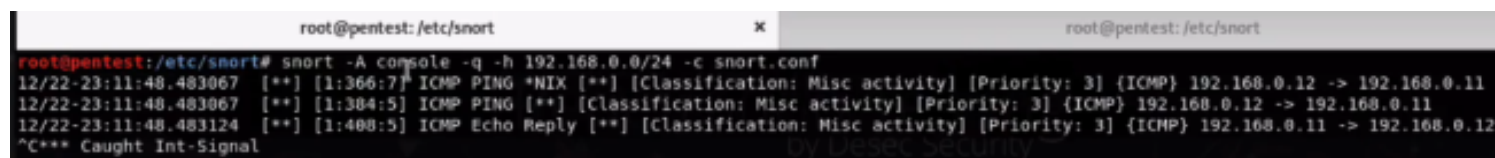
+ Vamos usar o exemplo dado em aula, do snort

[SITUAÇÃO]

+ Enviamos um simples pacote ping para o alvo

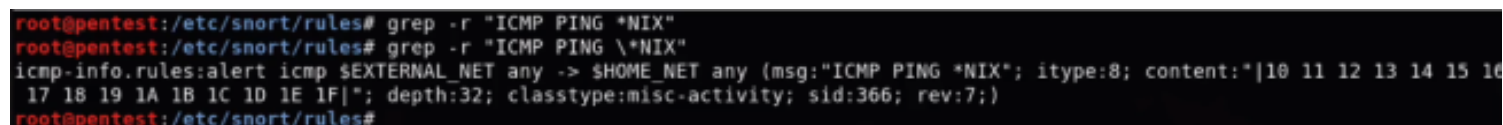
```
ping -c1 192.168.0.11
```

+ 3 Regras nos acusaram:



```
root@pentest: /etc/snort
root@pentest:/etc/snort# snort -A console -q -h 192.168.0.0/24 -c snort.conf
12/22-23:11:48.483067  [**] [1:366:7] ICMP PING *NIX [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.12 -> 192.168.0.11
12/22-23:11:48.483067  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.12 -> 192.168.0.11
12/22-23:11:48.483124  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 192.168.0.11 -> 192.168.0.12
^C*** Caught Int-Signal
```

+ Fizemos um grep no diretório das regras para encontrar a primeira regra:



```
root@pentest:/etc/snort/rules# grep -r "ICMP PING *NIX"
root@pentest:/etc/snort/rules# grep -r "ICMP PING *NIX"
icmp-info.rules:alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING *NIX"; itype:8; content:"|10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F|"; depth:32; classtype:misc-activity; sid:366; rev:7;)
```

→ Veja que a regra tem 3 requisições:

- 1 - itype: 8 (essa não dá pra mudar pois indica que é uma request) e
- 2 - content [conteúdo]: 11 12 13 ... 1F e
- 3 - depth: 32

+ O objetivo então é mudar o formato do ping para que ele não seja capturado por essa regra

→ Basta mudar uma das características mencionadas acima para que obtenhamos êxito

+ No caso, mudamos apenas o conteúdo do ping com o seguinte comando

```
ping -c1 -p "53461643461" 192.168.0.11
```

→ mudando apenas o corpo da mensagem, foi-se possível evadir a primeira regra

+ A partir disso, devemos sair olhando as demais regras para que se entenda o que elas requerem para que possamos passar por todas sem sermos detectados.