

PARTE PRÁCTICA

Usando SNORT

Instalamos snort y definimos una regla de mensaje que nos debería mostrar al realizar un ping en el Ip.

```
ades  Editor de textos  16 de jun 16:49
local.rules [Solo lectura]
/etc/snort/rules
Guardar

1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures.  Put your local
6 # additions here.
7 alert icmp 192.168.0.0/24 any -> any any (msg:"ALERTA alguien esta haciendo ping";sid:19910316;rev:1;)
```

Realizamos un ping a la ip desde otro dispositivo.

```
C:\Users\Usuario1>ping 192.168.0.11

Haciendo ping a 192.168.0.11 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Respuesta desde 192.168.0.11: bytes=32 tiempo=3183ms TTL=64
Respuesta desde 192.168.0.11: bytes=32 tiempo=2350ms TTL=64
Respuesta desde 192.168.0.11: bytes=32 tiempo=3836ms TTL=64

Estadísticas de ping para 192.168.0.11:
    Paquetes: enviados = 4, recibidos = 3, perdidos = 1
    (25% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2350ms, Máximo = 3836ms, Media = 3123ms

C:\Users\Usuario1>
```

En la consola de snort nos notificará sobre los intentos de intrusión.

```
camila@camila:/$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i wlo1
[sudo] contraseña para camila:
06/16-10:26:39.989034 192.168.0.27 -> 192.168.0.11 [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:39.989034 192.168.0.27 -> 192.168.0.11 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:39.989034 192.168.0.27 -> 192.168.0.11 [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:39.989138 192.168.0.11 -> 192.168.0.27 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:39.989138 192.168.0.11 -> 192.168.0.27 [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:42.553456 192.168.0.27 -> 192.168.0.11 [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:42.553456 192.168.0.27 -> 192.168.0.11 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:42.553456 192.168.0.27 -> 192.168.0.11 [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:42.553556 192.168.0.11 -> 192.168.0.27 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:42.553556 192.168.0.11 -> 192.168.0.27 [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:46.616803 192.168.0.27 -> 192.168.0.11 [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:46.616803 192.168.0.27 -> 192.168.0.11 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:46.616803 192.168.0.27 -> 192.168.0.11 [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:46.616881 192.168.0.11 -> 192.168.0.27 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:46.616881 192.168.0.11 -> 192.168.0.27 [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:48.126379 192.168.0.27 -> 192.168.0.11 [1:382:7] ICMP PING Windows [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:48.126379 192.168.0.27 -> 192.168.0.11 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:48.126379 192.168.0.27 -> 192.168.0.11 [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP}
06/16-10:26:48.126458 192.168.0.11 -> 192.168.0.27 [1:19910316:1] ALERTA alguien esta haciendo ping [**] [Priority: 0] {ICMP}
06/16-10:26:48.126458 192.168.0.11 -> 192.168.0.27 [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP}
```