CHALLENGE – UNIDAD DOS – SPRINT CINCO

CHALLENGE - IDS/IPS: SNORT

BOOTCAMP DE CIBERSEGURIDAD – THE BRIDGE

1.- INTRODUCCIÓN

Snort es un potente sistema de detección y prevención de intrusiones (IDS/IPS) que se utiliza para monitorizar el tráfico de red y detectar actividades sospechosas, que proporciona análisis de tráfico de red en tiempo real y registro de datos.

2.- INSTALACIÓN Y CONFIGURACION EN MAQUINA UBUNTU

La instalación de snort se ha llevado en un entorno controlado conformado por 3 máquinas: PfSense, Kali-LAN y Ubuntu, estando conectado esta ultima como DHCP y la LAN sin él, instalándose la herramienta Snort en la maquina WAN.

La configuración Snort se ha realizado siguiendo las siguientes premisas:

- Se procede a abrir uno de los archivos de instalación, concretamente en *"/etc/snort/snort.conf",* declarando una nueva variable donde se asigna un rango de direcciones IPs: *"ipvar HOME_NET 10.0.2.14/24"*
- Se Crea un archivo de reglas personalizadas en la ruta *"/etc/snort/rules/local.rules*":

1

```
 GNU nano 6.2                                                local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

#regla detectar ping
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Ping detected"; itype:8; sid:1000001; rev:1;)

#regla detectar FTP
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"FTP anonymous login attempt"; flow:to_server,established; content:"USER anonymous"; nocase>

#regla para escaneo SYN
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SYN scan detected"; flags:S; threshold:type both, track by_dst, count 5, seconds 5; sid:1>

#regla multiples conexiones SSH
alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"Multiple SSH connections detected"; flags:S; threshold:type both, track by_src, count 5, s>

#regla peticón al servedor web
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"Request for /test.html detected"; flow:to_server,established; content:"GET /test.html"; ht>
```

[1] Los finales de las reglas están cortados, correspondiendo el faltante, al *"sid*" y el *"riv",* que van consecutivos desde arriba hacia abajo.

.

- Finalmente, se abre nuevamente el archivo *"snort.conf"* para confirmar que las reglas locales creadas están incluidas en el *"$RULE_PATH"*

3.- MONITORIZACIÓN Y PRUEBA DE LAS REGLAS

Se ejecuta en una terminal el modo monitorización de Snort para que vaya detectando el tráfico generado y las alertas creadas con las reglas customizadas y otras incluidas en los archivos de configuración de snort, usando el comando: "*sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3".*

Las pruebas efectuadas sobre cada una de las 5 reglas, han dado los siguientes resultados:

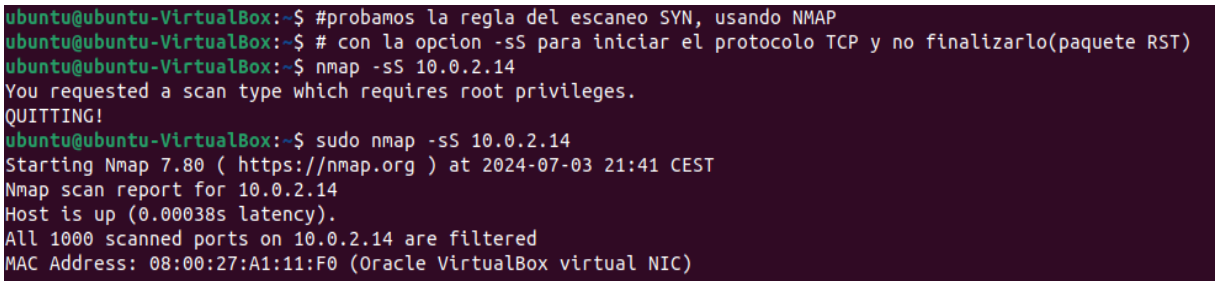
- Regla que detecta cuando se hace ping a una máquina de la red. – Se realiza un ping hacia la Ip 10.0.2.14, con resultado positivo.

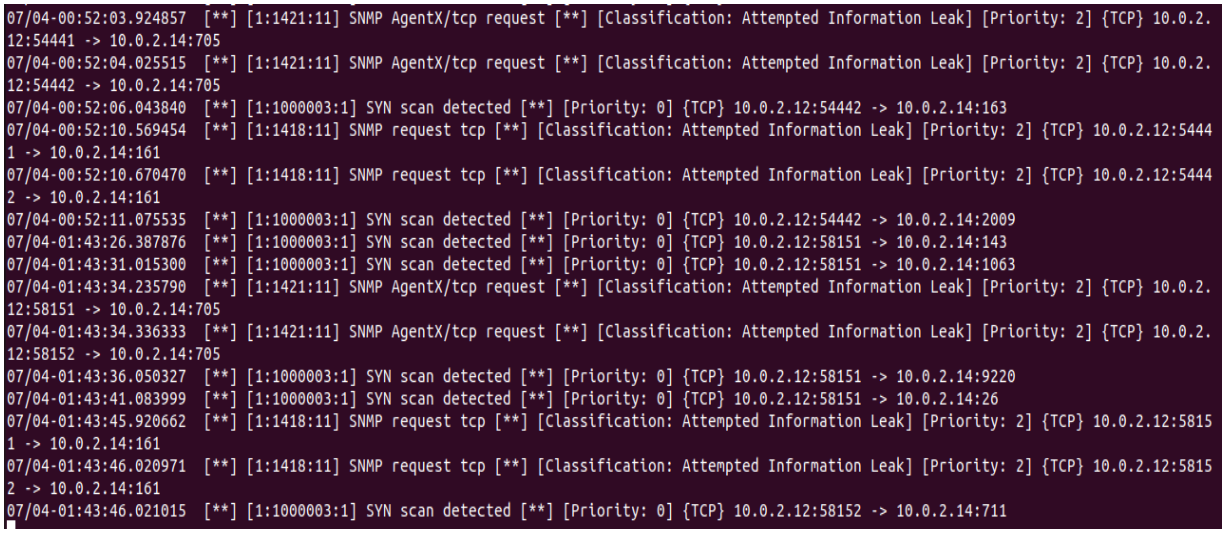
```
ubuntu@ubuntu-VirtualBox:~$ #iniciamos modo alerta snort   enp0s3
ubuntu@ubuntu-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.conf
-i enp0s3
07/03-21:22:07.868020  [**] [1:1000001:1] ICMP Ping detected [**] [Priority: 0
] {ICMP} 10.0.2.12 -> 10.0.2.14
07/03-21:22:08.871229  [**] [1:1000001:1] ICMP Ping detected [**] [Priority: 0
] {ICMP} 10.0.2.12 -> 10.0.2.14
07/03-21:22:09.895231  [**] [1:1000001:1] ICMP Ping detected [**] [Priority: 0
] {ICMP} 10.0.2.12 -> 10.0.2.14
07/03-21:22:10.919716  [**] [1:1000001:1] ICMP Ping detected [**] [Priority: 0
] {ICMP} 10.0.2.12 -> 10.0.2.14
07/03-21:22:11.943339  [**] [1:1000001:1] ICMP Ping detected [**] [Priority: 0
```

- Regla que detecta si alguien se ha autenticado con usuario anónimo por ftp hacia la red. - Tras numerosos intentos de configuración tanto de la regla como del entorno, el resultado es infructuoso.

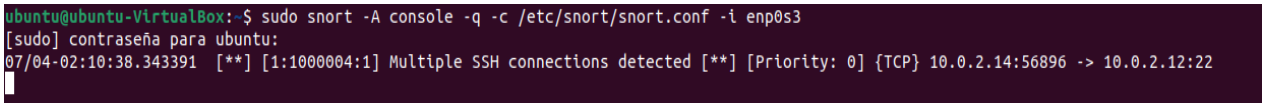
```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.12
Connected to 10.0.2.12.
220 (vsFTPd 3.0.5)
Name (10.0.2.12:kali): anonymous
331 Please specify the password.
Password:
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
ftp: Login failed
ftp>
```

- Regla que detecta cuando se hace un escaneo para detectar puertos abiertos, concretamente TCP de la red. - Se realiza un ataque mediante el comando *"nmap -sS 10.0.2.14",* el cual ejecuta un falso intento de conexión TCP, pero finalmente no cierra el "shakehand" enviando un paquete RST. EL resultado de regla ha sido positivo:

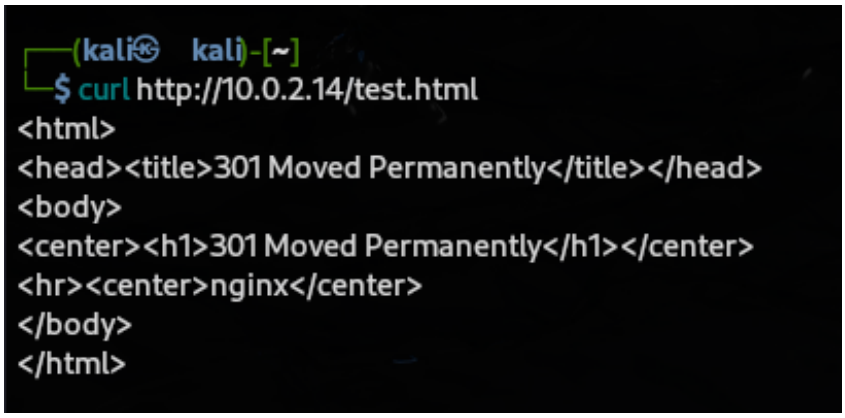




- Regla que detecta más de 5 conexiones seguidas al servicio SSH del mismo cliente. - Se realizan 6 conexiones seguidas desde la maquina LAN (Kali) a la WAN (Ubuntu) mediante el protocolo SSH, obteniendo respuesta positiva en la consola de Snort:



- Regla que detecta cuando se recibe una petición al servidor Web solicitando el recurso /test.html en la red WAN. - Tras varios intentos y cambios en la regla creada, todos han sido infructuoso.



EXTRA:

Mientras se realizaban los análisis ha saltado esta alerta en la consola de Snort, que una vez analizada se deduce que puede ser provocada por el cliente DHCP que usa el protocolo UDP, ya que la Ip de origen es la 0.0.0.0:68, que representa a este cliente y la dirección de destino 255.255.255.255:67 representa una transmisión de datos a todos los hosts de la red, dirigida por el puerto 67, por lo que es un falso positivo, no es tráfico potencialmente peligroso.