INSTALACIÓN DE KISMET

INSTALACIÓN DE KISMET

Para la instalar kismet en Linux solo es escribir los siguientes comandos en la terminal:

- **Sudo apt-get update**
- **Sudo apt-get Install kismet**

Como el IDS Kismet fue instalado en una Raspberry Pi 3, es importarte saber que la tarjeta de red de este dispositivo no se deja cambiar a modo monitor, por lo tanto fue necesario implementarle la siguiente antena USB:

Imagen 1.

Configuración de la antena: Para cambiar la tarjeta a modo monitor se escriben los siguientes comandos en la consola:

- **sudo ifconfig wlan0 down**
- **sudo iwconfig wlan0 mode monitor**
- **sudo ifconfig wlan0 up**

***La interface es a la que está conectada la antena, para mirar escriba el comando: ifconfig

Configuración de kismet:

Vamos al archivo de configuración de kismet kismet.conf que generalmente se encuentra en la ruta /etc/kismet/kimet.conf y la abrimos con el siguiente comando:

- **nano kismet.conf**

Añadimos al final del archivo “ncsource = wlan0” sin las “”, para que kismet reconozca por de interface se va hacer el escaneo.

Corriendo Kismet:

Para correr kismet ese escribe el comando:

- **kismet**

Se abrirá una ventana de kismet:

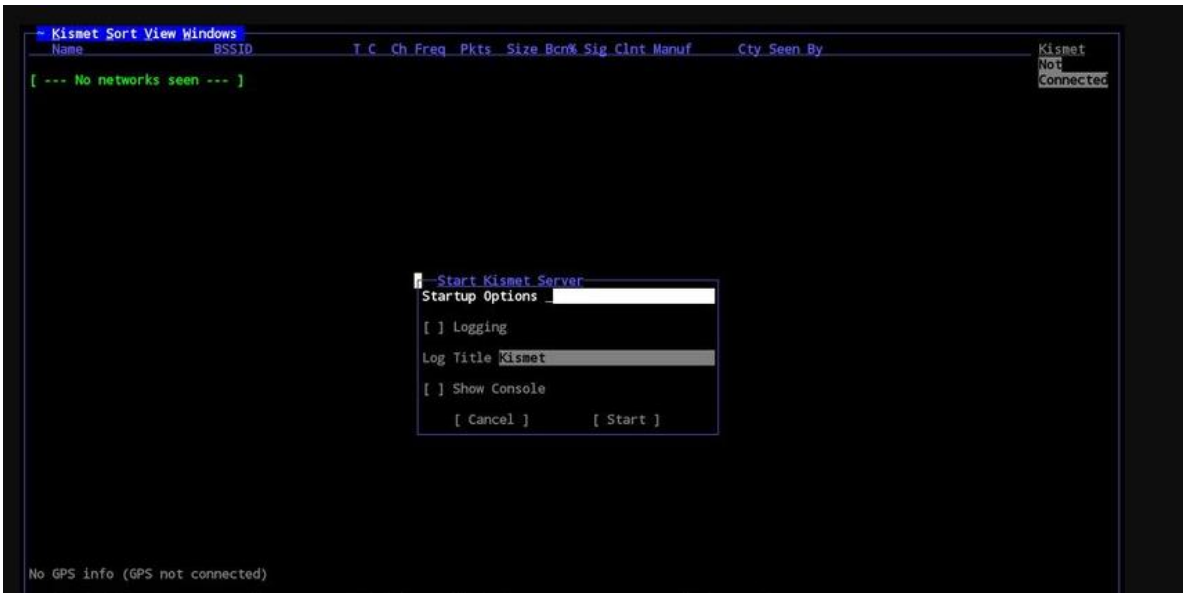


Imagen 2.

Si queremos ver la información por la consola de kismet le damos click en **[]Show Console**

Le damos click en **Start.**

Y kismet empieza a monitorear las redes WIFI.

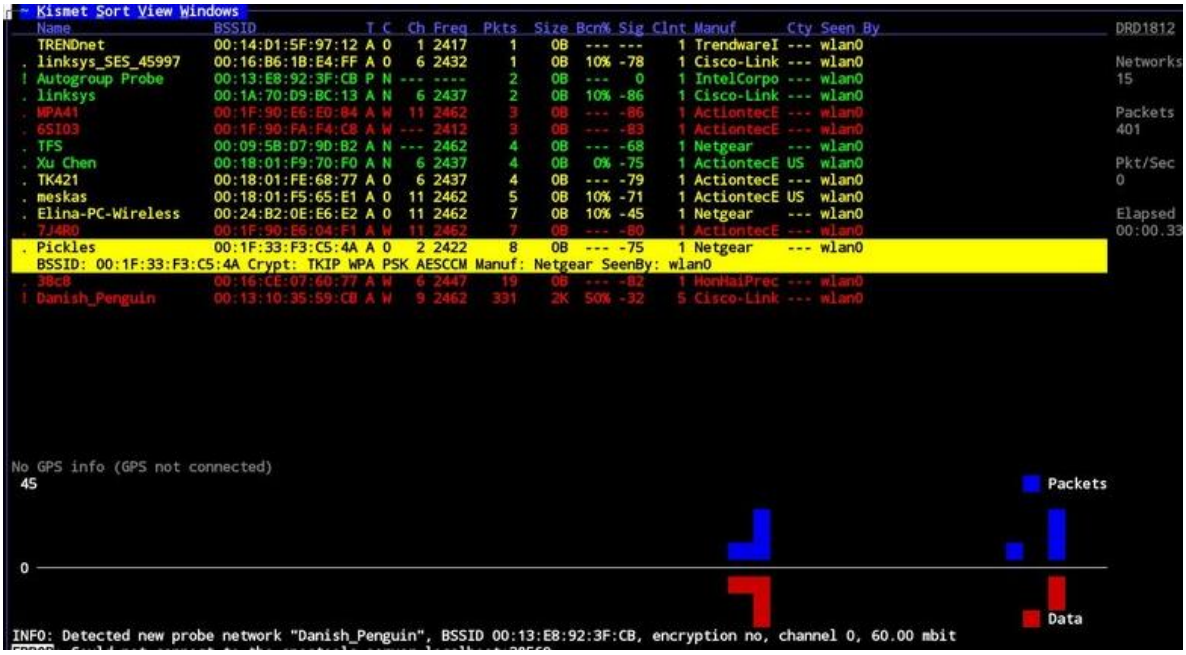


Imagen 3.

CONFIGURACIÓN KISMET EN OSSIM

Para cuando Kismet genere la alerta generalmente la guarda en la siguiente ruta **etc/kismet** y la envia al OSSIM y para esto se debe tener corriendo el programa que está en el siguiente Github https://github.com/andresvega82/SIEM-IoT/tree/master/Software/Kismet

en el archivo Syslogkismet.zip, el cual envía el syslog al OSSIM para que este pueda recibir el evento.

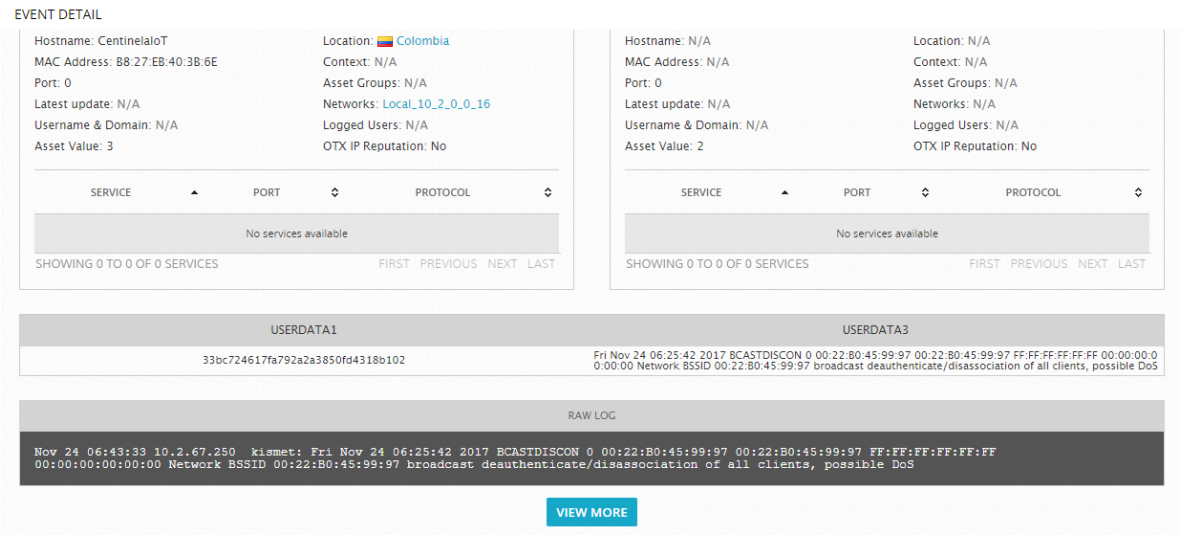
En la siguiente imagen podemos ver en color amarillo el código donde se envía el syslog:

```
        // Initialise sender
UdpSyslogMessageSender messageSender = new UdpSyslogMessageSender();
        messageSender.setDefaultMessageHostname(""); // some syslog cloud services may use this field to t
        messageSender.setDefaultAppName("kismet");
        messageSender.setDefaultFacility(Facility.USER);
        System.out.println("lo que tiene USER"+Facility.USER.name());
        messageSender.setDefaultSeverity(Severity.ALERT);
        //messageSender.setSyslogServerHostname("10.2.78.8");
        messageSender.setSyslogServerHostname("192.168.0.5");
        messageSender.setSyslogServerPort(514);
        messageSender.setMessageFormat(MessageFormat.RFC_3164);

         try {
      FileReader fr = new FileReader(fichero);
      BufferedReader br = new BufferedReader(fr);

      String linea;
      while((linea = br.readLine()) != null){
          lineas.add(linea);
          //System.out.println(linea);
      }

      for(int i= 0; i<lineas.size(); i++){
           System.out.println(lineas.get(i));
          // send a Syslog message

          try{
              messageSender.sendMessage(lineas.get(i));
                  System.out.println("el mensaje enviado fue:"+ lineas.get(i));}catch (IOException ex) {
        Logger.getLogger(ex.getMessage());
        }
```

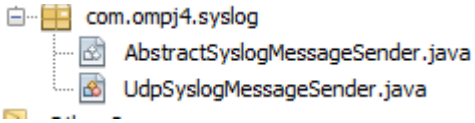
Imagen 4.

Este programa lee los nuevos archivos que se van creando en la carpeta ect/kismet y los envía al ossim.

La forma en que llega el evento al OSSIM es la siguiente:



**Es necesario incluir las clases:



**Para correr el programa se genera un .jar

** y se ejecuta con el conmando **java -jar <el nombre del archivo >.Jar.**

Ya con lo anterior se envía el syslog al OSSIM , pero para indicarles que campos del syslog queremos que se vea en el evento, es necesario agregar en la plataforma de OSSIM le plugin kismetIoTPlugin.cfg, el cual se encuentra en el Github mencionado anteriormente, el cual contiene la expresión regular:

```
[syslog - KimsteSyslog]
event_type=event
regexp="([\s\S]+) (?P<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}) (kismet: )([\s\S]+)(?P<date>\w+ \d\d \d\d:\d\d:\d\d)([\s\S]+)(BCASTDISCON
plugin_sid=1
src_ip={resolv($src_ip)}
username={$date}
userdata2={$channel}
userdata3={$src_mac}
userdata4={$dest_mac}
userdata5={$chan}
```

Imagen 5.

Continuación de la expresión regular

```
(?P<channel>\d+) (?P<src_mac>\w\w(:)\w\w(:)\w\w(:)\w\w(:)\w\w(:)\w\w) (?P<dest_mac>\w\w(:)\w\w(:)\w\w(:)\w\w(:)\w\w(:)\w\w)(?P<chan>[\s\S]+)"
```

Imagen 6.

La cual hará que el OSSIM reciba y muestre el evento de la siguiente forma:

```
Nov 25 11:45:57 10.2.67.240  -: Nov 25 16:10:53 10.2.67.240  kismet: Sat Nov 25 16:10:53 2017 BCASTDISCON 0 90:F6:52:89:7C:B2 90:F6:52:89:7C:B2
FF:FF:FF:FF:FF:FF 00:00:00:00:00:00 Network BSSID 90:F6:52:89:7C:B2 broadcast deauthenticate/disassociation of all clients, possible DoS
```

Imagen 7.

PRUBAR KISMET

Generar una alerta en Kismet:

En este escenario vamos a generar la alerte **BCASTDISCON** la cual se dispara cuando detecta que hay un ataque de desasociación de la red de un cliente o de varios, causando una posible denegación de servicio.

Debemos tener el Kismet corriendo:

Comando : **Kismet**

Para generar el ataque vamos a utilizar la herramienta **aireplay-ng,** en nuestro caso vamos a desconectar a todos los clientes conectados a la red:

Escribimos el siguiente comando:

- **aireplay-ng –deauth 0 –a < BSSID> wlan1**

  *el 0(cero) indica que va a realizar el ataque indefinidamente, si queremos que solo se realice 1 vez, cambiamos el 0 por 1.
  * wlan1 es la interface de red.
  * El BSSID es el punto de acceso por el cual se va a realizar el ataque.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER
BC:CA:B5:D2:A5:B0	-63	590	63 0	7	54e	WPA2	CCMP
98:68:3D:1D:94:F0	-67	583	503 0	8	54e	WPA2	CCMP
A4:7E:39:AA:00:AB	-77	514	26 0	6	54e	WPA	CCMP
58:23:8C:83:CE:34	-81	513	5211 0	6	54e	WPA2	CCMP
5C:89:01:6E:13:4E	-73	465	0 0	6	54e.	WPA2	CCMP
CC:96:A0:02:B5:48	0	450	3 0	11	54	WPA	TKIP

Imagen 8.

Cualquiera que se encuentre en la red para visualizar mejor estas BSSID podemos utilizar el comando: **airodump-ng wlan1**
, utilizando la interface de red que tengamos en el momento.

Luego le damos Enter y se empieza el ataque, se demora un poco ya que tiene que coincidir el canal(CH) del BSSID con el de la interface de red(wlan1).

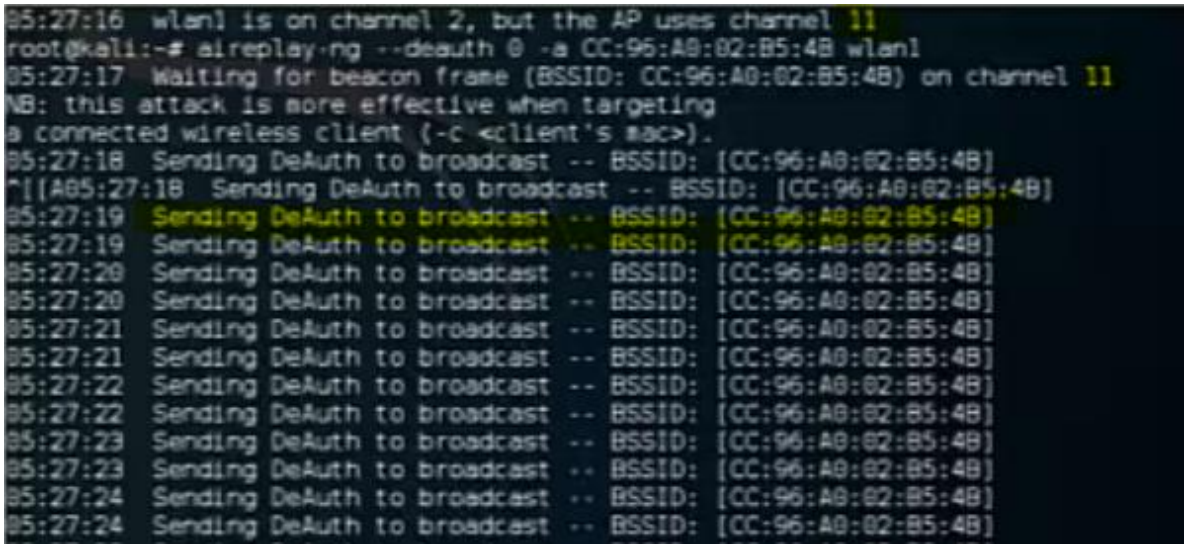


Imagen 9.

En la imagen anterior ponemos ver que empieza a enviar paquetes de desasociación por el punto que acceso que definimos y de este modo generar una denegación de servicio.

Kismet detecta el ataque:

```
INFO: Detected new probe network "HOLLYWOOD", BSSID 7C:BB:C6:FA:9F:FA,
      encryption no, channel 0, 72.20 mbit
ALERT: BCASTDISCON Network BSSID CC:96:A0:02:B5:4B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID CC:96:A0:02:B5:4B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID CC:96:A0:02:B5:4B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID CC:96:A0:02:B5:4B broadcast deauthenticate
       /disassociation of all clients, possible DoS
ALERT: BCASTDISCON Network BSSID CC:96:A0:02:B5:4B broadcast deauthenticate
       /disassociation of all clients, possible DoS
```

Imagen 10.

Informado que tipo de ataque es, por donde se está generando el ataque y cual la consecuencia de este.

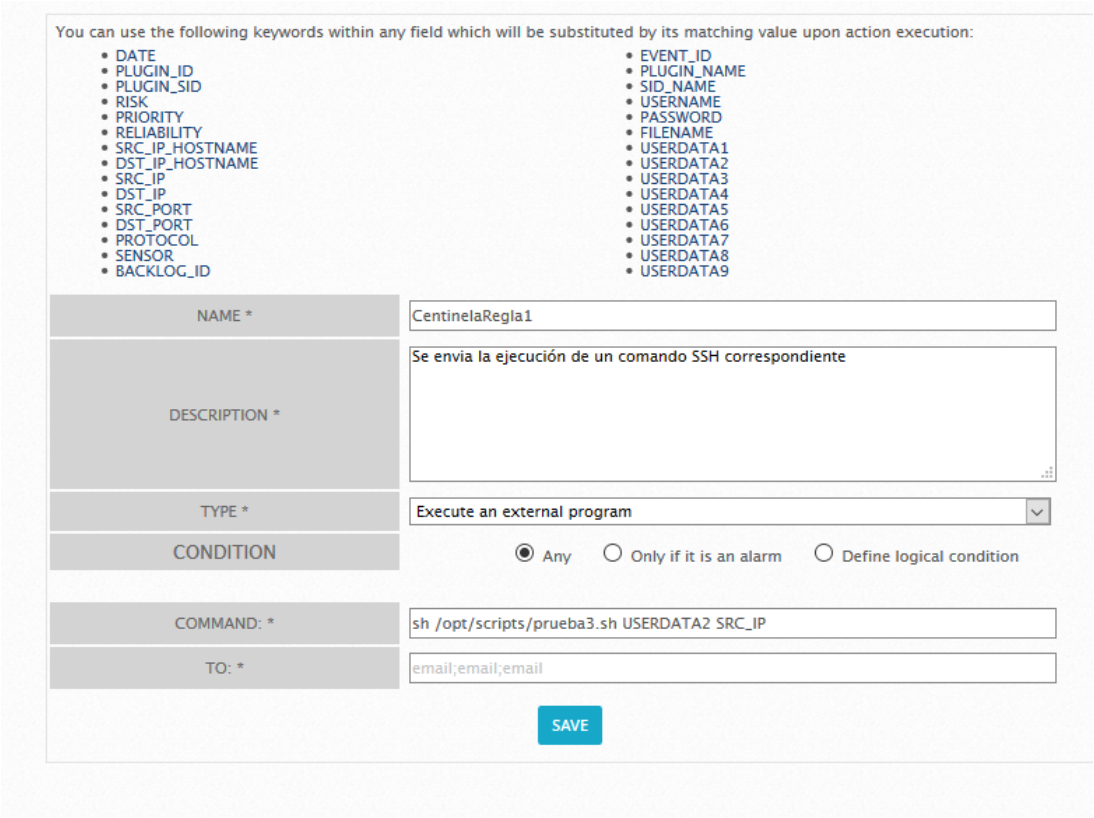
Cuando kismet recibe la alerta esta es reportada al OSSIM y el OSSIM por medio del siguiente script, realiza una acción:

```
import paramiko
import sys
def sshCommand(hostname,port,username,password,command):
    sshClient = paramiko.SSHClient()

    sshClient.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    sshClient.load_system_host_keys()
    sshClient.connect(hostname,port,username,password)
    stdin, stdout, stderr = sshClient.exec_command(command)
    print(stdout.read())

if __name__=='__main__':
    sshCommand(sys.argv[0],22,'root','toor','reboot')
```

Imagen 11.

En nuestro caso lo que hace el reiniciar el equipo cerrando el punto de acceso del atacante (se debe tener en cuenta que para este paso se deben tener permisos de administrador). En el OSSIM se programa de la siguiente manera:

INSTALACIÓN DE KISMET



COMMAND:* se indica el scripts que se va a utilizar.

En TO* se puede poner un correo para informar al administrador de que ocurrió el evento.