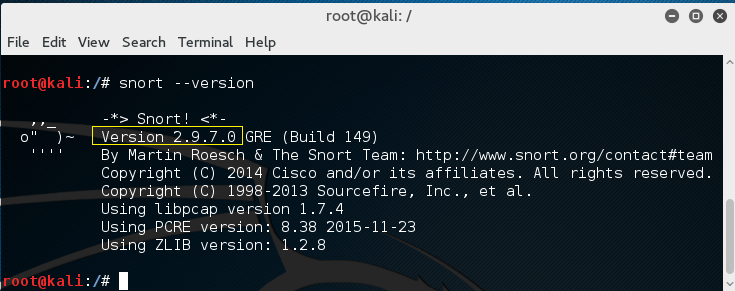
** INTRUSION DETECTION SYSTEM :**

**Components:**

* **Window device : ip@ 192.168.220.1**
* **Ubuntu device : ip@ 192.168.220.129**
* **Kali device : ip@ 192.168.220.128**

1. **Install *Snort* on KALI:**

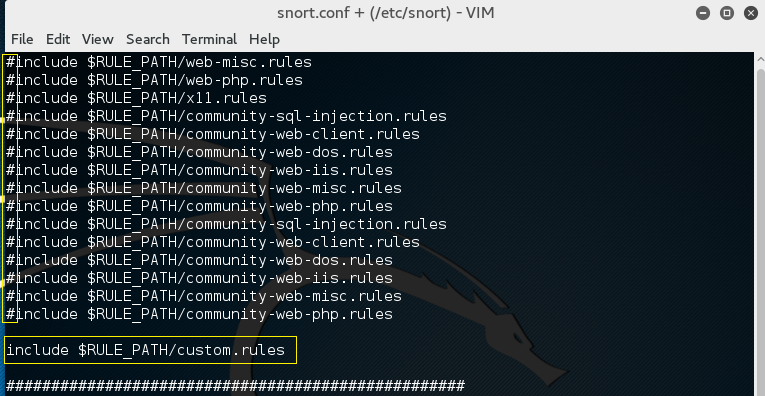
**:/# apt-get install snort**

****

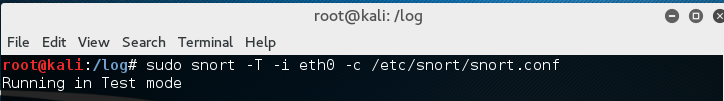
**Snort is lightweight intrusion detection for networks** that can just work as a packet sniffer. It means it captures and displays packets from the network with different levels of detail on the console. Or it can works as an alerting system like we will see below

1. **We Comment all the default rules in the configuration file**

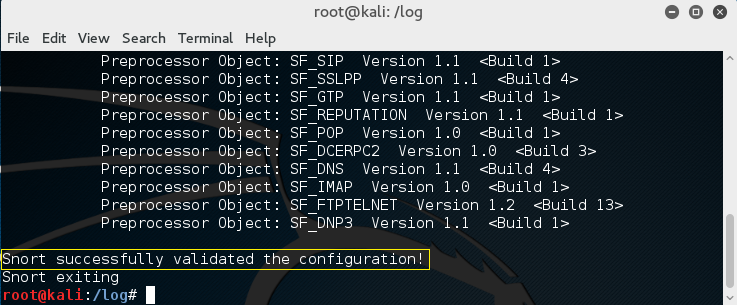
**then we ADD our OWN rules**

****

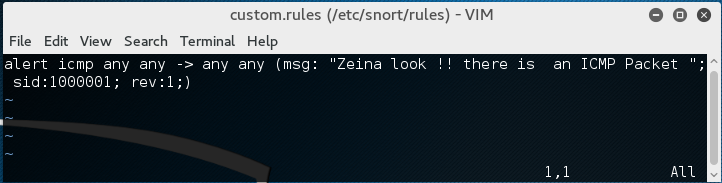
1. **Test it after the modification :**

****

**Result:**

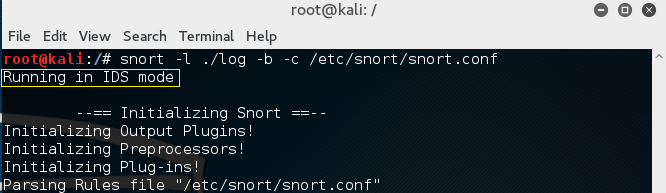
****

1. **Add the first rule in *custom.rules* :**

****

any any > any any means from any source to any destination IN OUR PROJECT there is 2 devices only -> the query means alert any ICMP packet transferred between these two

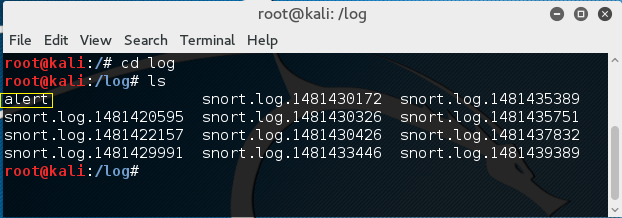
1. **Start *Snort* in IDS mode and tell it to save alerts in log Directory**

****

**One Rule Added:**

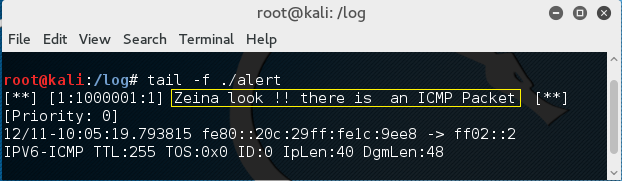
****

**All the alerts are saved here:**

****

1. **Ping ubuntu from window (Or the Inverse because we Wrote any any in the rule )**

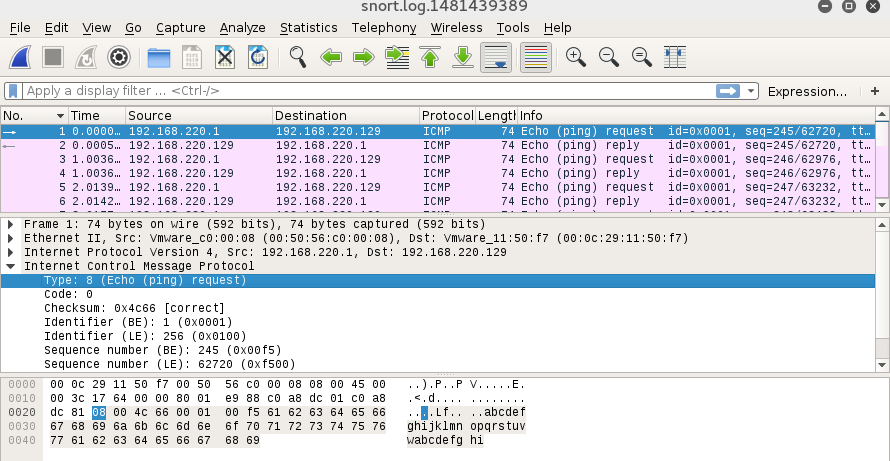
**We check our file :**

****

**YES YES! I can see it :P**

**Whatever let’s go back to work, So …**

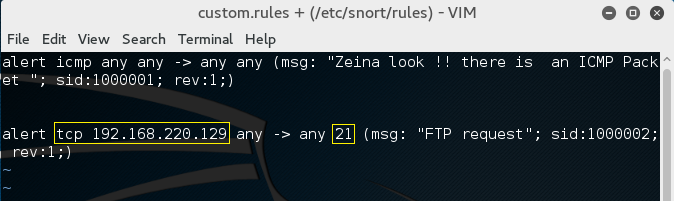
1. **We can Open *wireshark* to get more details**

****

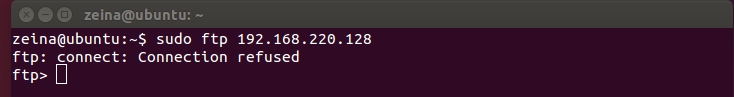
1. **Add a FTP rule:**

FTP protocol use TCP protocol and port 21

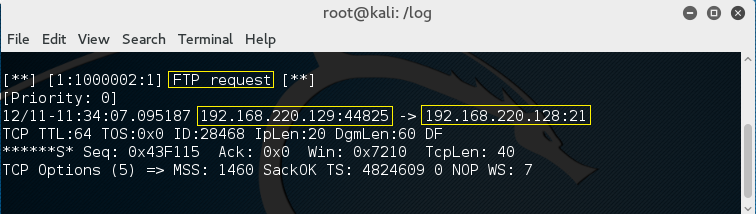
192.168.220.129 is our Ubuntu machine

****

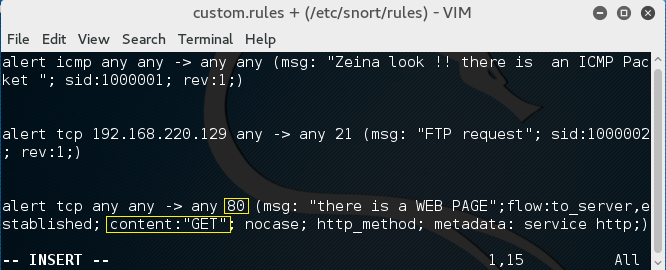
1. **Connect to FTP :**

****

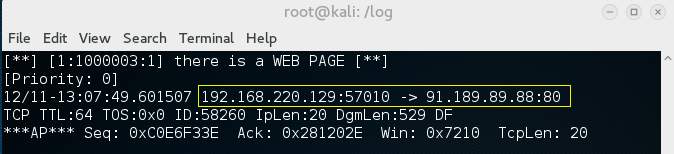
1. **Check the alert file:**

****

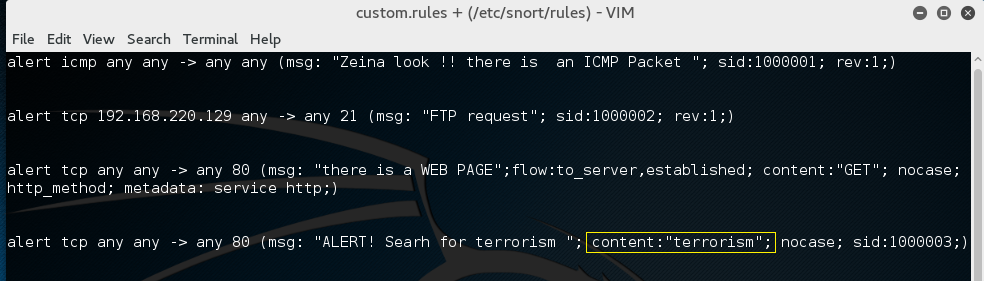
1. **Add a HTTP request rule based on content:**

****

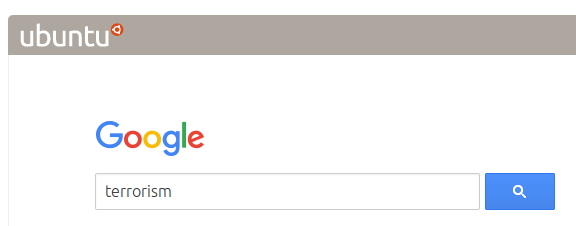
1. **When Opening a web page an HTTP alert appear :**

****

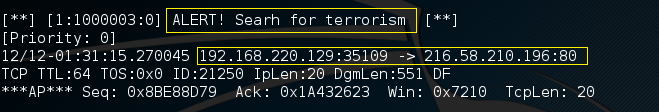
1. **Add a HTTP rule based on content=”*terrorism”:***

****

1. **Access a webpage named terrorism from ubuntu**

****

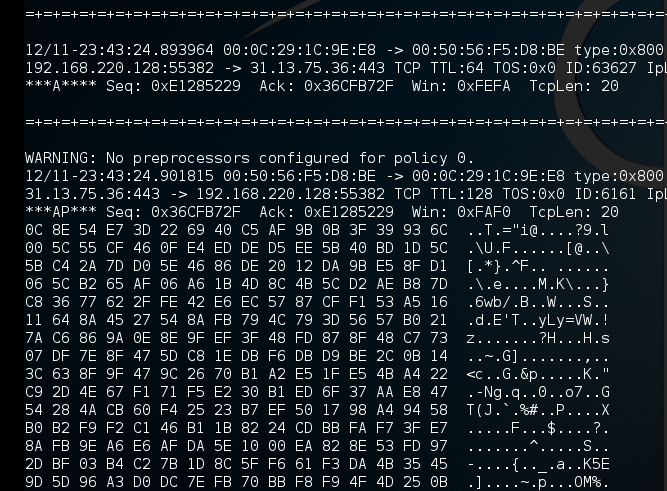
1. **View the alert :**

****

**Yes !! Well done**

* **Snort can work just in sniffer mode:**

**:/# Snort –vde**

****