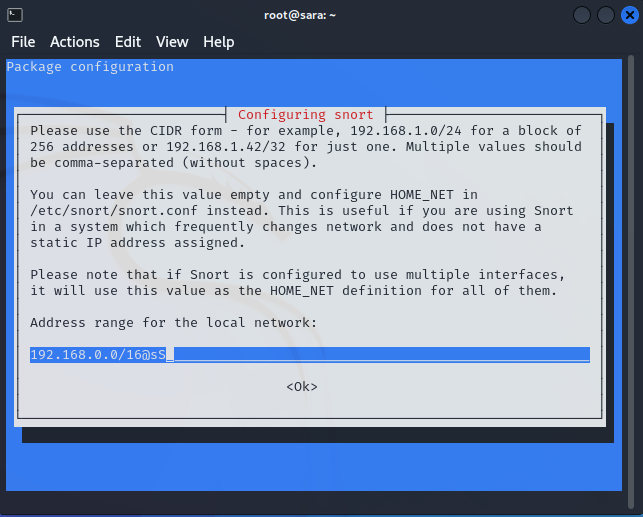
**Snort step**

<https://drive.google.com/file/d/1m10ylJhYg4RJDHMzy1n5qnT58LM6K3wk/view?usp=sharing>

رابط الفيديو للشرح

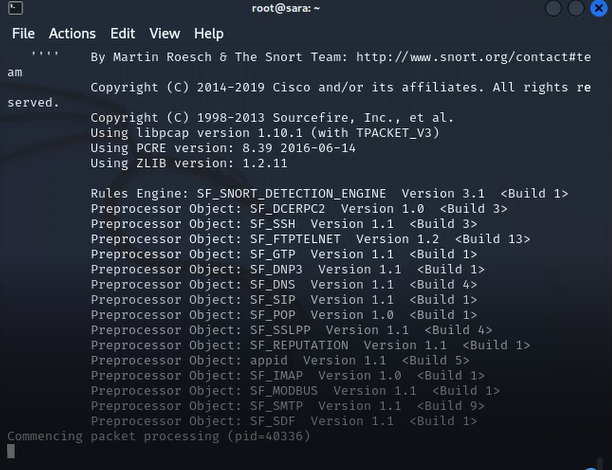
**المطلوب انشاء snort rule يعمل تنبيه عند ارسال ping من المصدر 192.168.0.0/24**

1. **تحميل snort بالامر apt-get install snort**
2. ****
3. **نعدل الامتداد ل 192.168.0.0/24**
4. **touch /etc/snort/rules/sara.rules عمل ملف اسمه sara**
5. **vi /etc/snort/snort.conf للدخول لملف snort.conf**
6. **نصبح داخل الملف snort.conf ننزل بالسهم ونضيف امتداد ملف sara.rules ثم نعدل ال $EXTERNAL\_NET 192.168.0.0/24 وال $HOME\_NET الى any**
7. **mkdir log انشاء مجلد log**
8. **vi /etc/snort/rules/sara.rules**
9. **ندخل في ملف sara.rules نكتب جملة التحذير حسب المطلوب من الواجب**

alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (sid:100006927; msg:'PING'; itype:8;)

**يجب الانتباه للسينتاكس كل مسافة او فاصلة** لاحظ **سابقا عدلنا $EXTERNAL\_NET لانها تمثل المصدر وال $HOME \_NET تمثل الواجهه**

1. snort -d -l ./log -h 192.168.0.0/24 -A console -c /etc/snort/snort.conf



اذا ظهرت هذه الشاشة يعني ان الsnort يعمل بشكل صحيح