Document d’architecture :

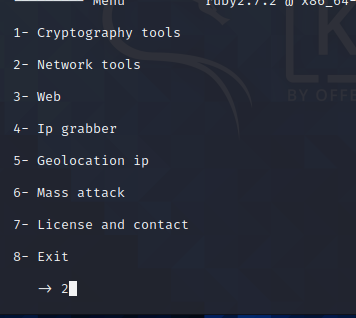
Projet UF

* Denys Delaunay
* Yohan Stoeckle
* Bastien Bruyez

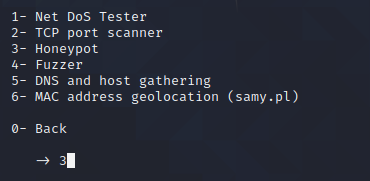
SOMMAIRE :

1. Test du honeypot
2. Test du firewall
3. Test récupération fichier supprimer
4. Test de la détection d’intrusion
5. Test du honeypot :

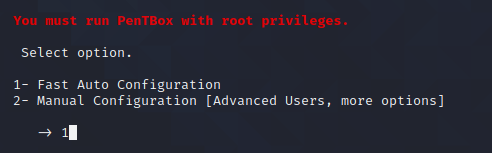
Sur l’interface ci-dessous, il faut choisir le 2 :



Sur la fenêtre suivante nous devons choisir le 3, le honeypot :



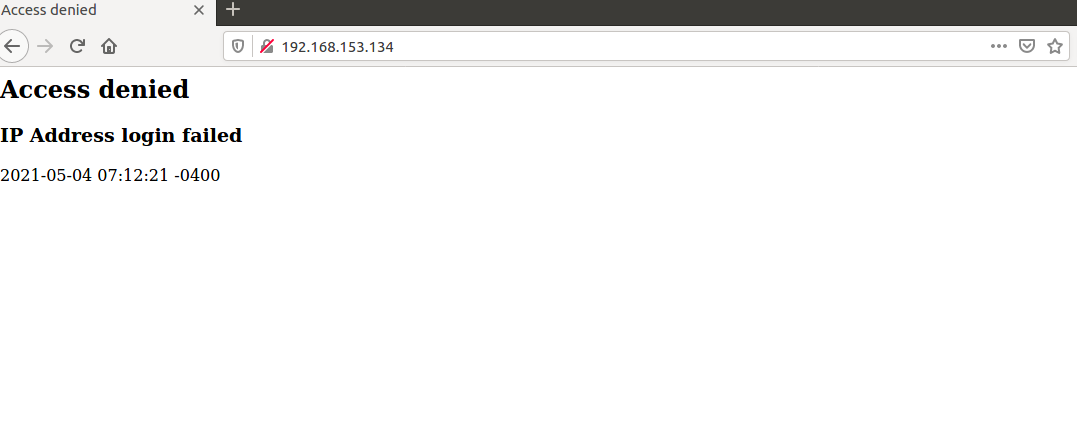
Sur le choix suivant nous pouvons choisir la 1ère option, qui permet de se connecter automatiquement au port en question :



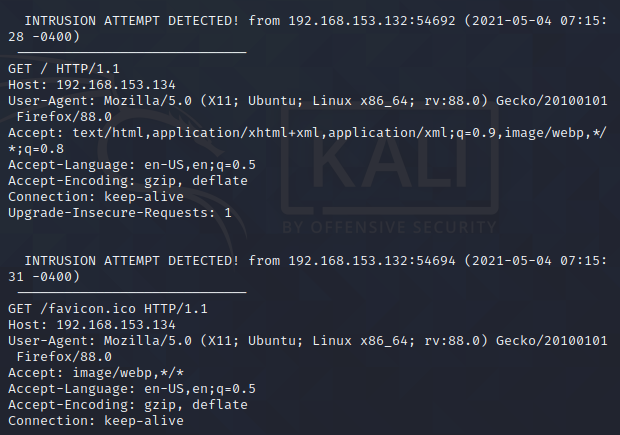
Après avoir fait le choix ci-dessus, nous avons lancé le honeypot :



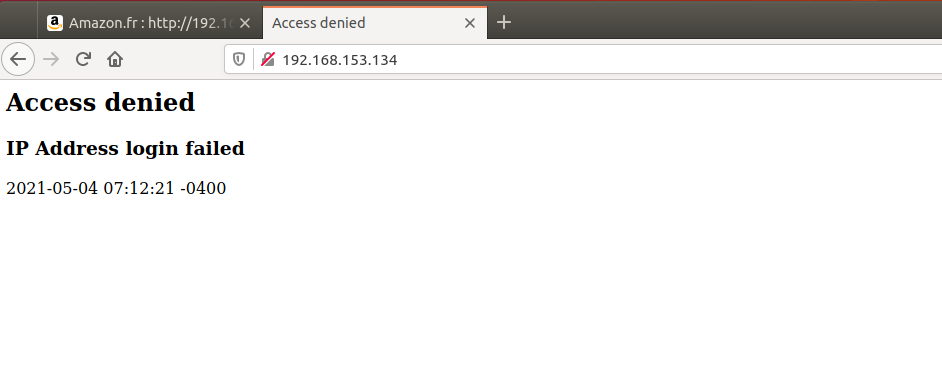
Nous essayons de nous connecter à l’ip du serveur souhaité :



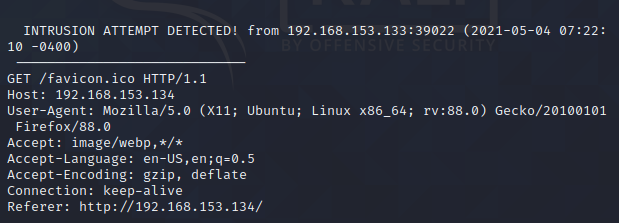
Nous avons un retour sur le serveur cible de l’intrusion :



Nous essayons avec un autre serveur linux :



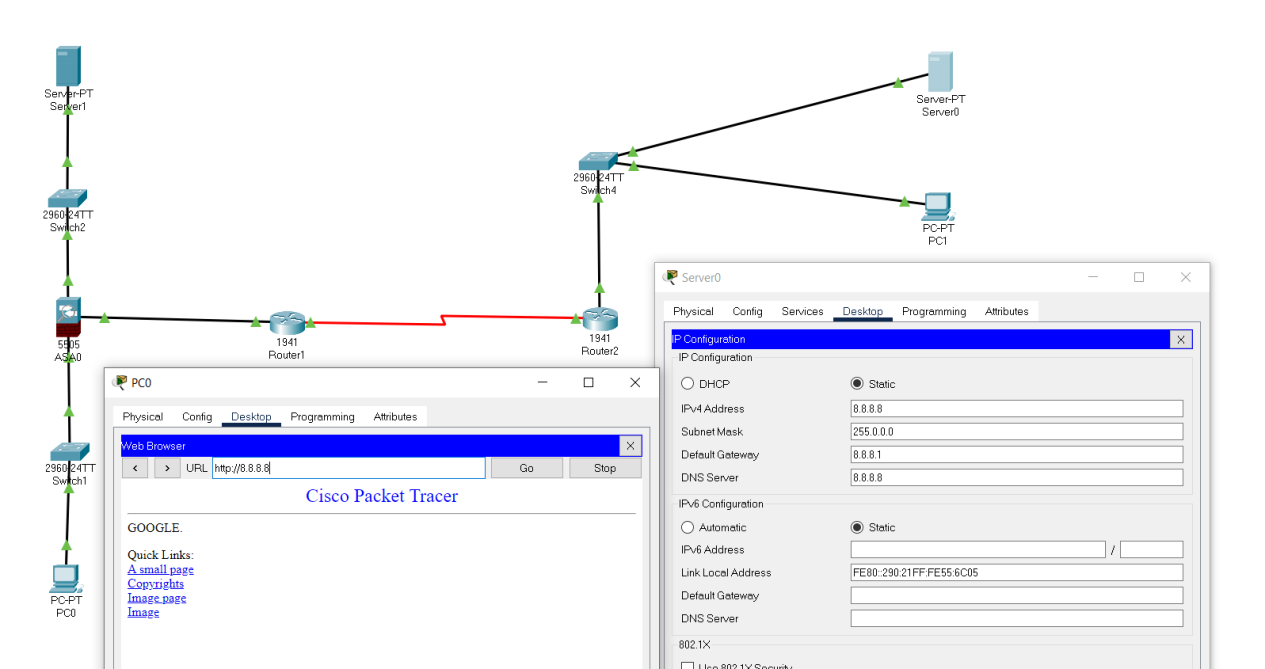
Nous voyons l’intrusion sur le kali :

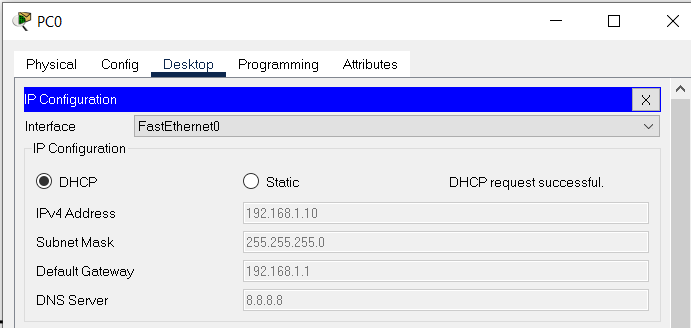


1. Test du firewall:

Configuration dns dhcp sur vlan 1 (inside)



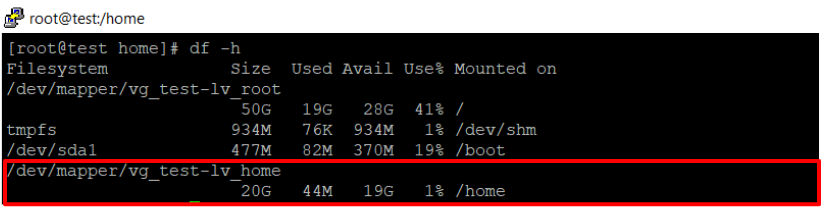




1. Test récupération fichier supprimer :

Suivez les étapes ci-dessous afin de récupérer le fichier supprimé.

* Utilisez la commande **[df -h]** afin de voir la valeur d'espace disque disponible des systèmes de fichier dont l'utilisateur possède l'accès en lecture.

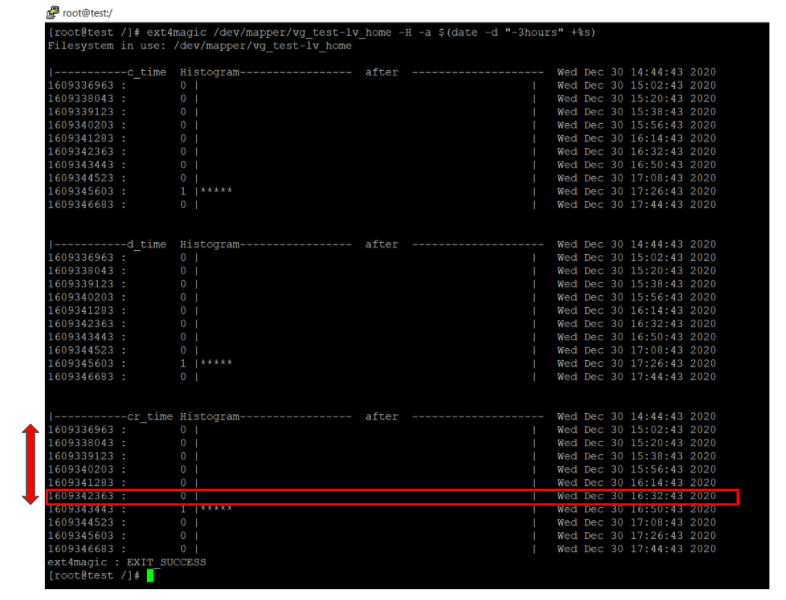


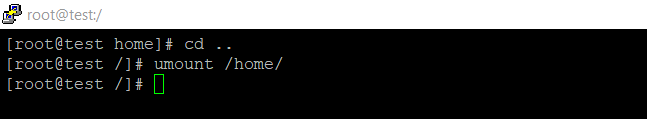
Dans ce cas c’est l’espace disque **vg\_test-lv\_home** qui est utilisé, **à adapter selon votre cas**

Démontez le système de fichiers en spécifiant le chemin du répertoire dans lequel il a été monté.

* Utilisez la commande suivante :

**[umount *chemin\_du\_répertoire]***

****



Créez un répertoire de récupération dans /tmp

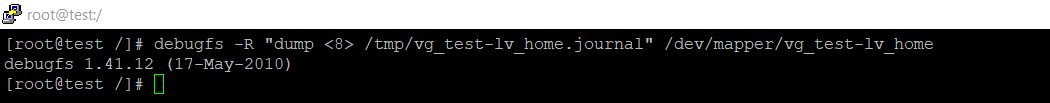
* Utilisez la commande suivante :

**[mkdir /tmp/recovery]**

Sauvegardez votre table d'inodes, vous en aurez besoin pour la restauration

* Utilisez la commande suivante

**[debugfs -R "dump <8> /tmp/vg\_test-lv\_home.journal" /dev/mapper/vg\_test-lv\_home]**

****

Vérifiez à quel moment vos fichiers/dossiers étaient encore là

* Utilisez la commande suivante :

**[ext4magic /dev/mapper/vg\_test-lv\_home -H -a $(date -d "-3hours" +%s)]**

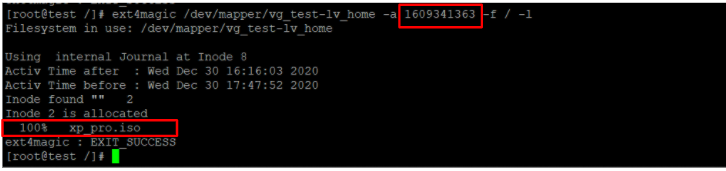
Cette commande permet de voir la liste de tous les fichiers supprimés au cours des trois dernières heures. **A adapter selon votre cas.**

Nous pouvons voir une suite de chiffres représentant les fichiers supprimés.

Copiez la suite de chiffres représentant le fichier supprimé.

* Utilisez la commande suivante :

**[ext4magic /dev/mapper/vg\_test-lv\_home -a 1609341363 -f / -l]**

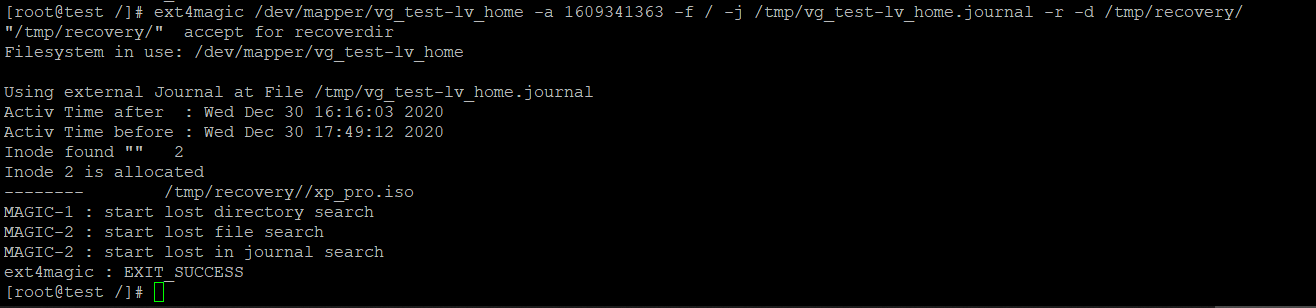
****

Cette commande permet de lister les fichiers/dossiers dans le délai souhaité. Ici, nous retrouvons le fichier supprimé en question.

Restaurez le fichier dans le répertoire de récupération créée en début de procédure.

* Utilisez la commande suivante :

**[ext4magic /dev/mapper/vg\_test-lv\_home -a 1609341363 -f / -j /tmp/vg\_test-lv\_home -r -d *répertoire\_de\_dossier]***

****

Dans ce cas, il a été restauré dans **/tmp/recovery.**

Une fois la commande lancée, celle-ci prend du temps à s'exécuter.

**Patientez quelques minutes** avant de pouvoir récupérer votre fichier.

Une fois la commande exécutée, vous pourrez retrouver votre fichier dans le répertoire spécifié

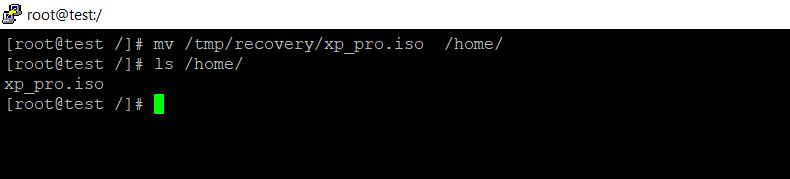
****

**/! Voilà, nous avons réussi à récupérer le fichier !\**

Une fois l’opération terminée, n’oubliez pas de remonter le système de fichiers démonté au début de la procédure.

****

Et, si vous le souhaitez, déplacer le fichier restauré à partir du répertoire “recovery” dans le répertoire initial.

****

Fin de la procédure

1. Test de la détection d’intrusion :

Maintenant que nous avons tout qui fonctionne comme il le faut, allons tester notre règle. Prenons une deuxième machine qui servira de ping. (La machine physique peut servir si tout est bien configurer pour que le réel et le virtuel communique). Entrons la commande suivante afin de faire fonctionner snort et notre règle :

snort -A console -q -i ens33 -c /etc/snort/snort.conf -K ascii

snort= calls the program

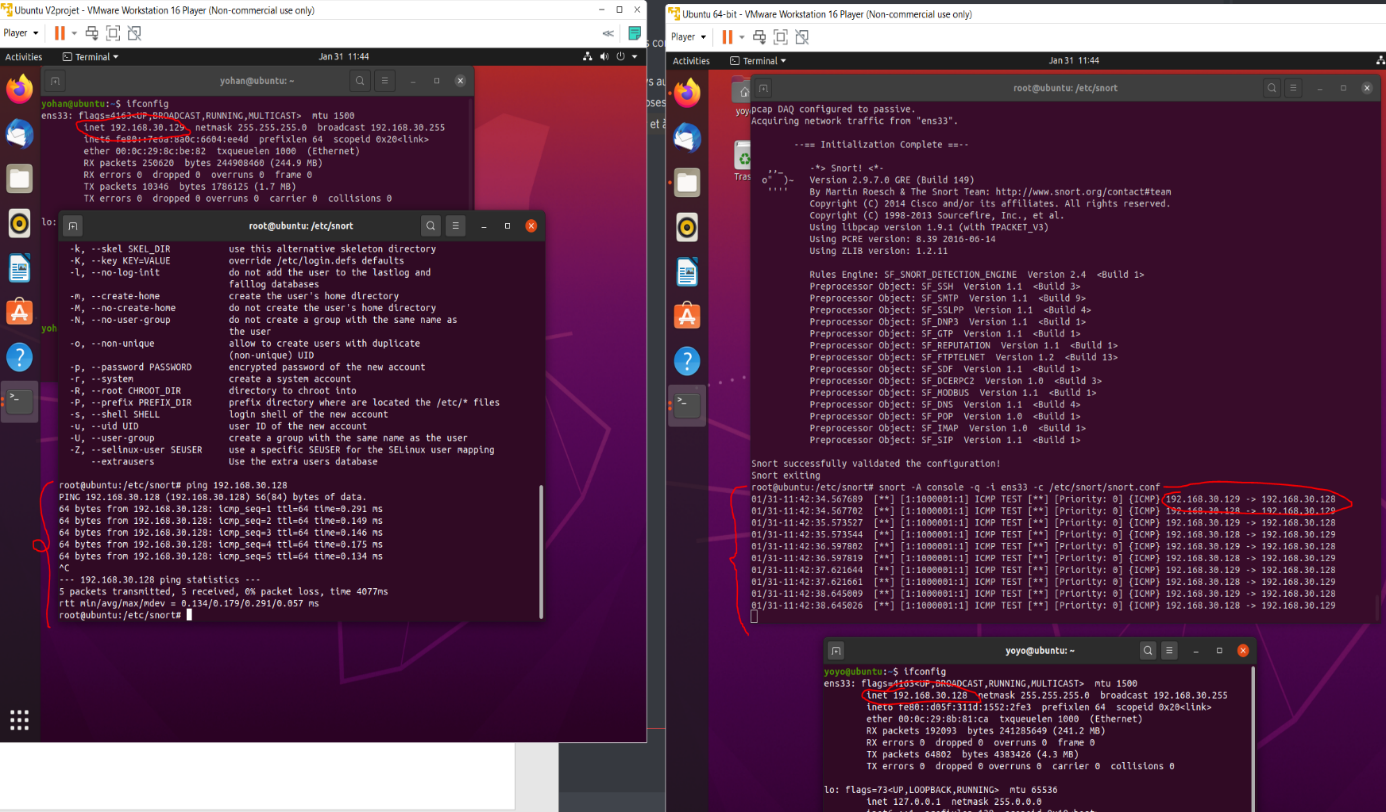
-c= path to config file (/etc/snort/snort.conf)

-q= prevents snort from displaying initial information

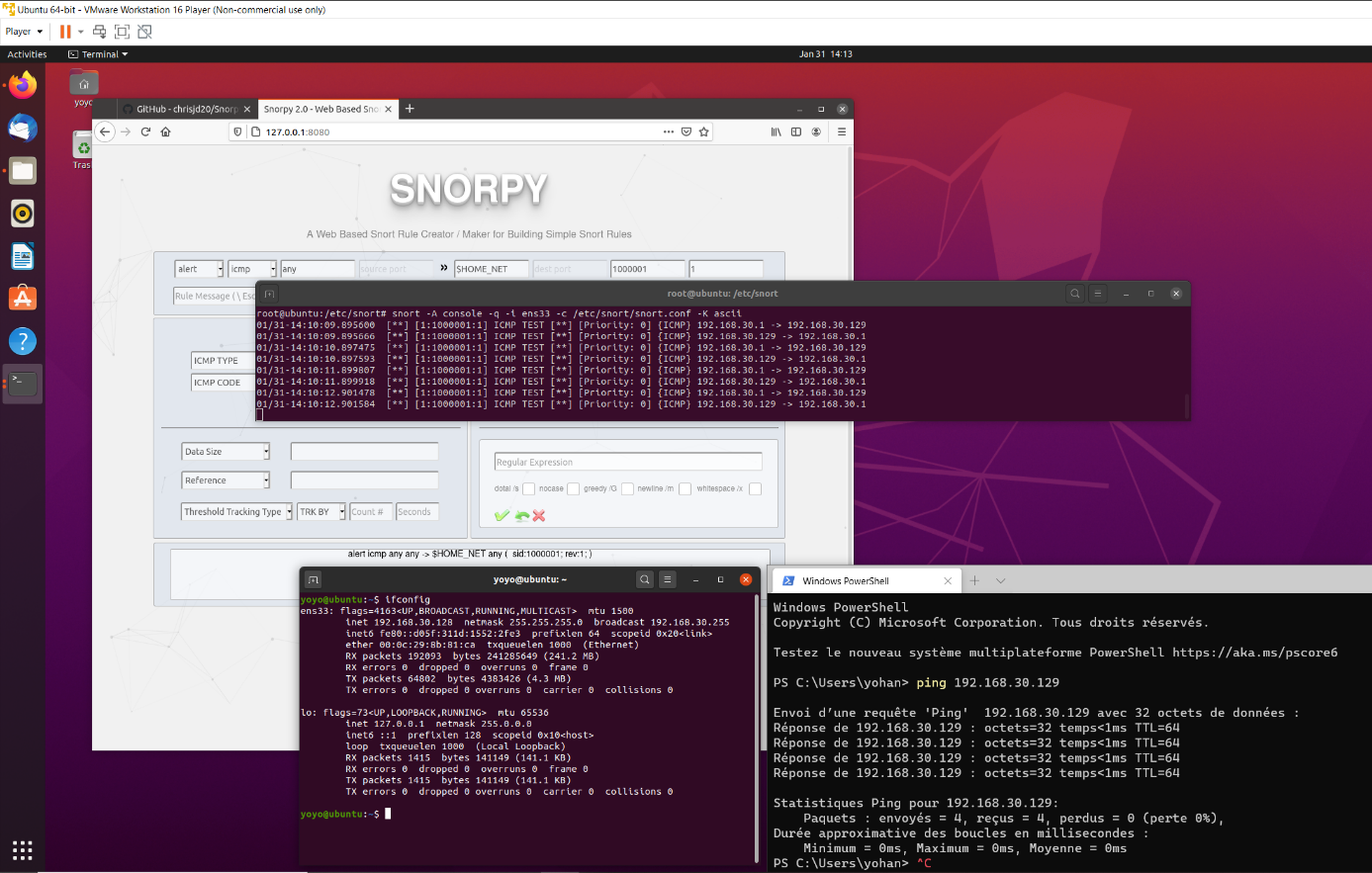
-A= defines the alert mode. Dans notre cas la console.

-K ascii= Write events in a log file in (/var/log/snort/)

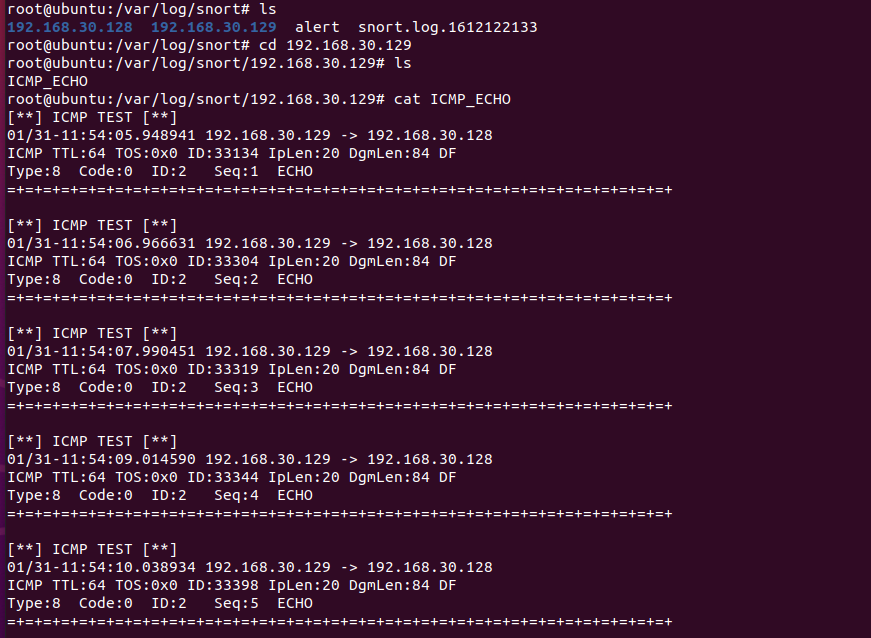
Dans ces screens nous pouvons voir que la règle réagie quand on lui fait une requête PING.

2 machines virtuelles Ubu

1 machine virtuelle ubuntu avec l’IDS Snort activé et une machine physique Windows 10 Pro



Voici maintenant le contenu des logs des évènements de Snort et donc de notre règle. Elle est bien recensée et nous indique l’évènement avec le message que nous avons configuré avec l’alerte (ICMP TEST) ainsi que d’autres détailles comme l’IP source, la date et l’heure…



**Pour aller plus loin :**

* Mettre en place un VPN.
* Mettre en place de la redondance sur tout l’infra pour minimiser le risque.