TP1 – Info0605

Rapport, au format PDF uniquement, et au maximum 3 jours après la fin de votre TP sur moodle

- **Besoin d'un linux (en VM Virtualbox avec réseau en NAT et de Wireshark sous linux ou sur Windows)**
- **Distribution Kali ou une Ubuntu server (interface graphique non nécessaire)**
- **Configuration minimale : un Linux invité (VM Ubuntu Server sans interface graphique), un Windows hôte avec Wireshark, connexion ssh depuis votre Windows vers votre VM**

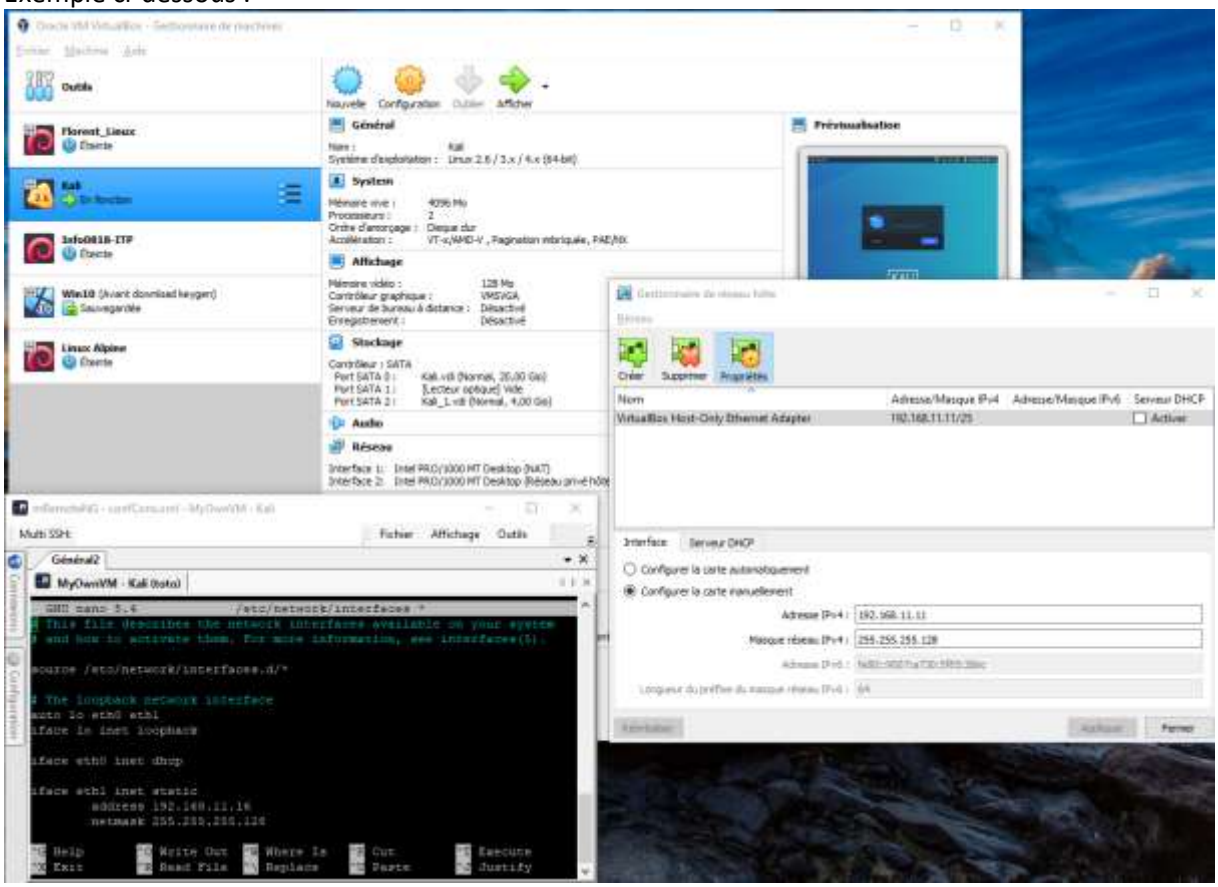
Pour configurer votre Linux et y avoir un accès simple, sans interface graphique, configurer 2 cartes réseaux :

1ère carte en NAT pour l'accès à internet

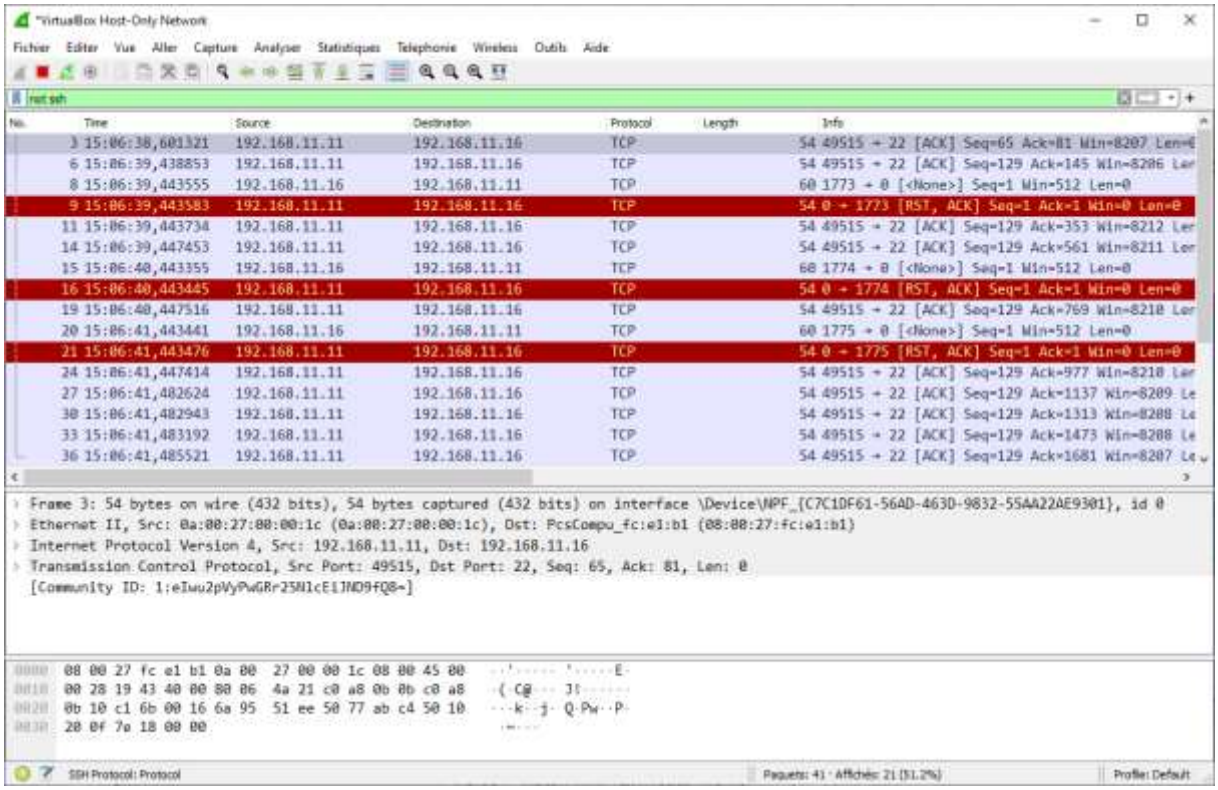
2ème carte en Host only (réseau privé hôte) pour l'accès ssh depuis votre windows à votre VM

- Configuration de l'IP hôte : dans virtualbox, Fichier -> Gestionnaire de réseau hôte
  - Ajouter une carte si aucun n'est présente
  - Définir une IP statique à votre carte
- Sur votre VM, configurer une IP fixe dans ce même réseau afin de pouvoir communiquer depuis Windows avec votre Linux

Exemple ci-dessous :



Pour capturer, dans Wireshark, que les paquets intéressants, sans avoir les échanges SSH entre votre windows et votre Linux : utiliser les filtres : `not ssh` sur votre carte « `VirtualBox host-Only Network` » Dans cet exemple, j'ai fait un « `hping3 192.168.11.11` » depuis Linux vers Windows en utilisant pour `IP_cible`, l'IP de la carte « `VirtualBox Host-Only` »



Partie 1 :

Découvrez l'IP de `www.certifiedhacker.com`
Trouvez la taille maximale autorisée des paquets grâce à la commande `ping`.
Quelles options faut-il utiliser ?
Simuler un `traceroute`, via la commande `ping`. Quels option et paramètre faut-il donner à à la commande `ping` pour changer le TTL pour atteindre le serveur qui gère le site web `www.certifiedhacker.com` ?
Via la commande `dig`, identifiez l'IP du serveur mail sur le domaine univ-reims.fr ainsi que le mail du responsable du serveur DNS.

Partie 2 :

Il vous faudra pour la suite utiliser 2 machines : un linux pour les commandes, votre windows comme cible et Wireshark sous windows pour visualiser les paquets qui sortent de votre VM.

Exécutez un `hping3 -c 3 IP_target`
Sur la cible, exécutez Wireshark afin d'examiner les paquets reçus.
`hping3 --scan 1-3000 -S IP_target`
Sur la cible, exécutez Wireshark afin d'examiner les paquets reçus.
Comparez les 2 résultats obtenus et interprétez-les.
`hping3 IP_target --udp -rand-source --data 500`
Sur la cible, exécutez Wireshark afin d'examiner les flux UDP.
`hping3 -S IP_target -p 80 -c 5`
Sur la cible, exécutez Wireshark afin d'examiner les flux TCP.
`hping3 IP_target --flood`
Grâce à la commande nmap et l'option -O, découvrez toutes les IP actives.
En prenant pour cible un windows, exécutez un `nmap` avec l'option `–packet-trace` et expliquez les informations retournées.
Effectuer 2 différents scans de port, sur la plage 1-3000, l'un en utilisant le protocole TCP et l'autre le protocole UDP.
Sur le protocole TCP, effectuez un scan avec la commande nmap en positionnant le flag SYN à 1 puis un autre avec le flag ACK à 1. Comparez les résultats et interprétez-les.
Exécutez la commande `nmap -sT -T3 -A IP_VM_Windows_8.1`
Interprétez les résultats et expliquez ce que fait cette commande
Activez le firewall de Windows puis exécutez la commande `nmap -sX -T4 -A IP_VM_Windows`
Exécutez la même commande mais en désactivant le firewall de Windows.
Quelles différences obtenez-vous et quelles en sont les raisons ?
Que fait la commande `nmap -Pn -p 80 -sI IP_host IP_VM_Windows` ?
En activant le firewall de votre invité Windows 8.1, à la fois sur les réseaux publiques et privées, exécutez la commande `nmap -f IP_VM_Windows`
Puis la commande `nmap -mtu 8 IP_VM_Windows` puis la commande `nmap -D RND :10 IP_VM_Windows`
Pour ces 3 commandes, exécutez en même temps un wireshark sur votre Windows. Interprétez les résultats obtenus.