

TP1 – Info0605

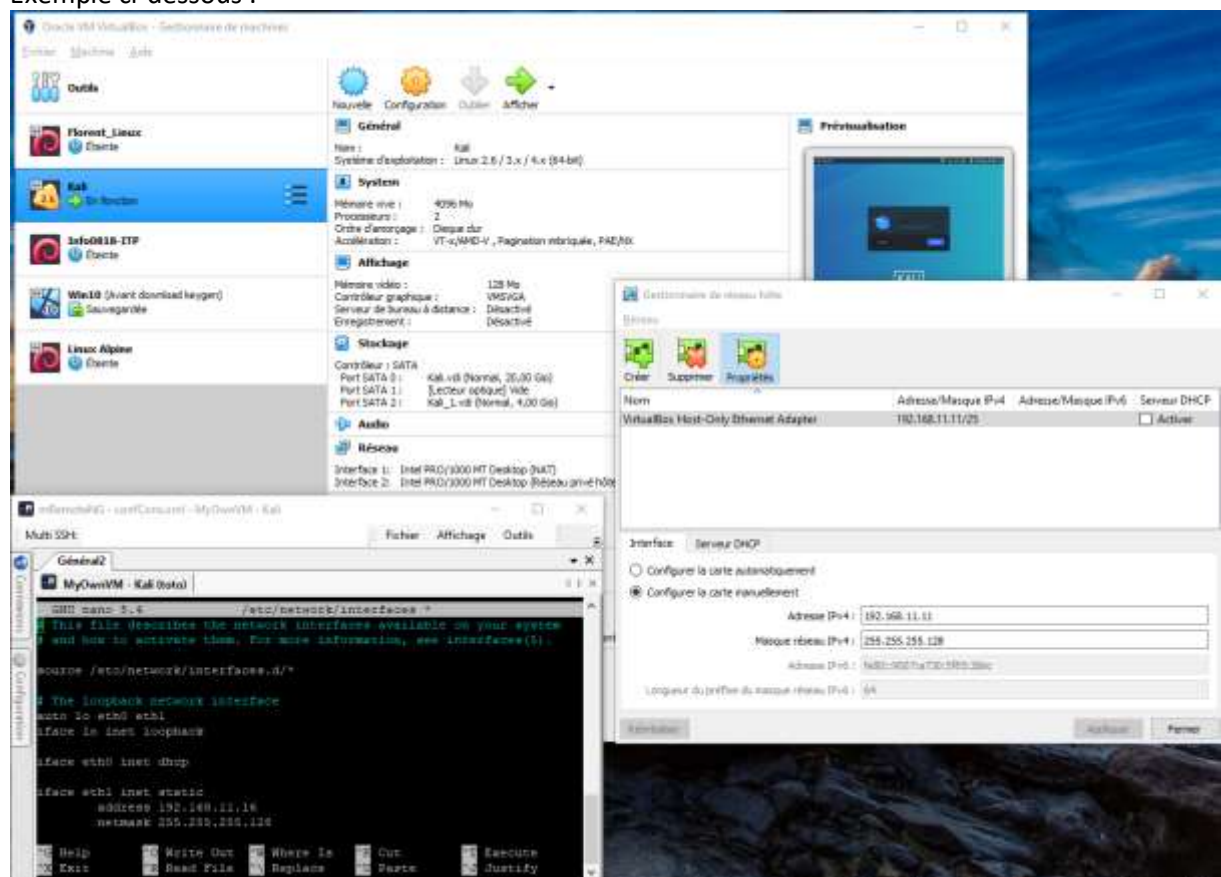
Rapport, au format PDF uniquement, et au maximum 3 jours après la fin de votre TP sur moodle

- 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 :

- 1^{ère} carte en NAT pour l'accès à internet
 - 2^{ème} 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
 - o Ajouter une carte si aucun n'est présente
 - o 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 »

No.	Time	Source	Destination	Protocol	Length	Info
3	15:06:38,601321	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=65 Ack=81 Win=8207 Len=0
6	15:06:39,438853	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=145 Win=8206 Len=0
8	15:06:39,443555	192.168.11.16	192.168.11.11	TCP	60	1773 → 0 [<None>] Seq=1 Win=512 Len=0
9	15:06:39,443583	192.168.11.11	192.168.11.16	TCP	54	0 → 1773 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11	15:06:39,443734	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=353 Win=8212 Len=0
14	15:06:39,447453	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=561 Win=8211 Len=0
15	15:06:40,443355	192.168.11.16	192.168.11.11	TCP	60	1774 → 0 [<None>] Seq=1 Win=512 Len=0
16	15:06:40,443445	192.168.11.11	192.168.11.16	TCP	54	0 → 1774 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	15:06:40,447516	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=769 Win=8210 Len=0
20	15:06:41,443441	192.168.11.16	192.168.11.11	TCP	60	1775 → 0 [<None>] Seq=1 Win=512 Len=0
21	15:06:41,443476	192.168.11.11	192.168.11.16	TCP	54	0 → 1775 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	15:06:41,447414	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=977 Win=8210 Len=0
27	15:06:41,482624	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=1137 Win=8209 Len=0
30	15:06:41,482943	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=1313 Win=8208 Len=0
33	15:06:41,483192	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=1473 Win=8208 Len=0
36	15:06:41,485521	192.168.11.11	192.168.11.16	TCP	54	49515 → 22 [ACK] Seq=129 Ack=1681 Win=8207 Len=0

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{C7C1DF61-56AD-463D-9832-55AA22AE9301}, id 0
 Ethernet II, Src: 0a:00:27:00:00:1c (0a:00:27:00:00:1c), Dst: PcsCompu_fc:e1:b1 (08:00:27:fc:e1:b1)
 Internet Protocol Version 4, Src: 192.168.11.11, Dst: 192.168.11.16
 Transmission Control Protocol, Src Port: 49515, Dst Port: 22, Seq: 65, Ack: 81, Len: 0
 [Community ID: 1:eIuu2pYyPwGRz25u1cE17MD9fQ8~]

```

0000  08 00 27 fc e1 b1 0a 00 27 00 00 1c 08 00 45 00  ...E-
0010  00 28 19 43 40 00 08 06 4a 21 c0 a8 0b c0 a8    -Cg...Jf...
0020  0b 10 c1 6b 00 16 6a 95 51 ee 50 77 ab c4 50 10  -k--j-Q-Pw-P-
0030  20 0f 7a 18 00 00                                -m-
  
```

SSH Protocol: Protocol Paquets: 41 - Affiché: 21 (51.2%) Profil: Default

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 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.