

## 1 Rappel important

**Il est complètement interdit de pratiquer les techniques vues dans ce cours sur un réseau ou une machine qui ne vous appartient pas, y compris le réseau de l'université et les machines qui ne sont pas dans le laboratoire prévu pour cette fin. Vous risquez la prison et ni votre professeur, ni votre université ne peuvent vous protéger. La loi c'est la loi !**

Le piratage (Hacking) c'est criminel. Principalement, la loi définit comme crimes informatiques : L'accès illégal aux ordinateurs et à leurs données (cc.342.1) ; le vols de données informatiques (cc.342.1) ; le méfaits aux données (cc.430). Pour plus de détails sur le code criminel : [laws-lois.justice.gc.ca/PDF/C-46.pdf](https://laws-lois.justice.gc.ca/PDF/C-46.pdf)

## 2 Objectif

L'objectif principal de ce laboratoire est de permettre à l'étudiant de comprendre et de manipuler des machines et des réseaux virtuels ainsi que Wireshark, le fameux outil d'analyse des trafics réseau.

## 3 VMware et VirtualBox : modes de connexions

VMware et VirtualBox permettent de créer des machines et de les connecter entre elles, avec la machine hôte et à Internet via différents modes de connexion tels que :

- **Bridged** : (pont) Ce mode donne la possibilité à une machine virtuelle d'accéder à son réseau local ainsi qu'à Internet. La machine aura sa propre adresse réseau IP et elle sera visible de l'extérieur. La machine connectée via ce mode obtient généralement son adresse d'une manière dynamique en exécutant le protocole DHCP (Dynamic Host Configuration Protocol). La machine hôte est par défaut connectée à ce mode via une des ses cartes réseaux réelles.
- **Host-only** : (hôte seulement) Ce mode permet à des machines virtuelle de se communiquer entre elles et avec la machine hôte. Les adresses IPs utilisées dans ce mode ne sont pas accessibles à partir de l'extérieur et nous pouvons les choisir par nous même.
- **Gest-only** : (invité seulement) Ce mode permet d'avoir un environnement complètement fermé. Les machines virtuelles ne peuvent se communiquer qu'entre elles.
- **NAT** : Ce mode permet à une machine virtuelle d'accéder au monde extérieur (réseau local ou Internet) en utilisant l'adresse IP de la machine hôte conformément au service NAT (Network Address Translation). .

## 4 Description du réseau utilisé

Le scénario de notre première aventure est comme le montre la figure 3. Le réseau de test est composé de trois ordinateurs bleu, rouge et vert connectés en mode Host-only ((hôte seulement) ).

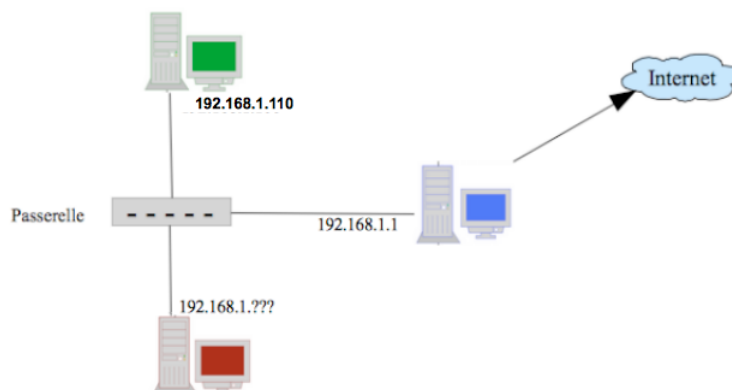


Fig. 3 Configuration du réseau

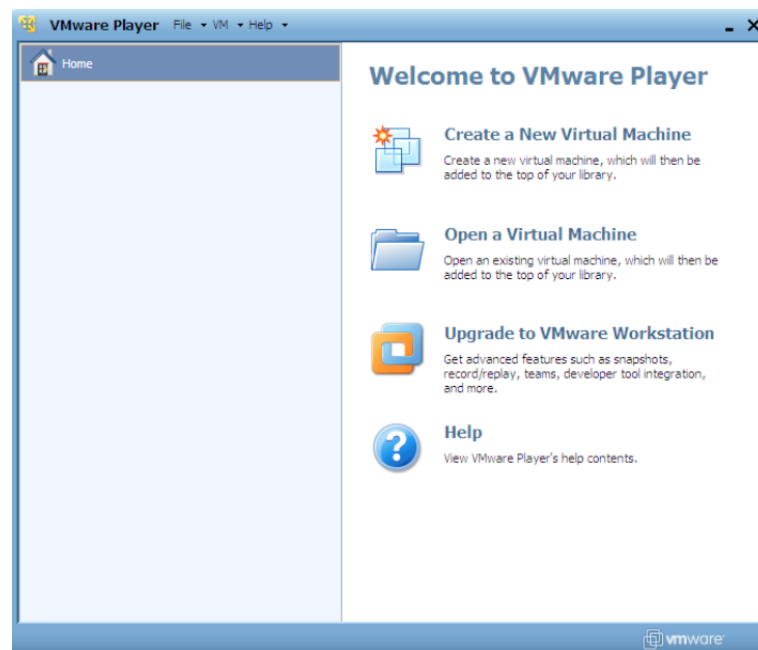
- La machine verte est la cible dont on ne connaît pas son mot de passe et elle sera notée dans ce qui suit par M110. On l'active via VMware (ou virtualBox) et on la laisse allumée sans essayer d'ouvrir une session via un nom d'utilisateur et un mot de passe (ces informations sont pour le moment inconnus).
  - Cette machine a été préconfigurée avec les adresses suivantes : : @IP=192.168.1.110 et masque = 255.255.255.0
- La machine rouge Kali est munie d'un ensemble d'outils (wireshark, nmap, etc.) très utiles pour analyser ou attaquer une machine ou un réseau. On active cette machine via VMware ou virtualBox et on y ouvre une session via le nom d'utilisateur `root` et le mot de passe `toor`. Cette machine devrait appartenir au réseau 192.168.1.0, mais chaque étudiant aura son propre numéro de machine qui est disponible sur le site web du cours. Par exemple, l'adresse IP d'un étudiant qui a 17 comme numéro de machine sera 192.168.1.17.
- La machine bleue est l'hôte : c'est votre machine habituelle et sa carte réseau virtuelle du mode host-only (Vmnet1 pour Vmware) doit être configurée avec l'adresse IP=192.168.1.1

## 5 Travail demandé

Le travail consiste à faire certaines opérations et de prendre des copies d'écrans montrant vos résultats. Les étapes et les détails sont décrits dans ce qui suit. Les copies d'écrans qu'il faut prendre sont indiquées par le signe suivant :

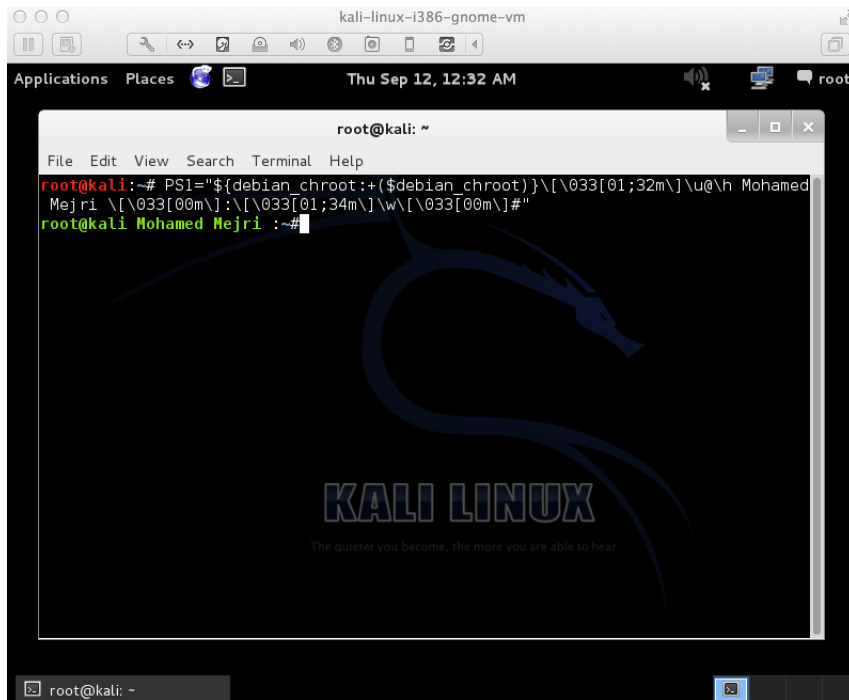


### 1. Lancer VMware Player



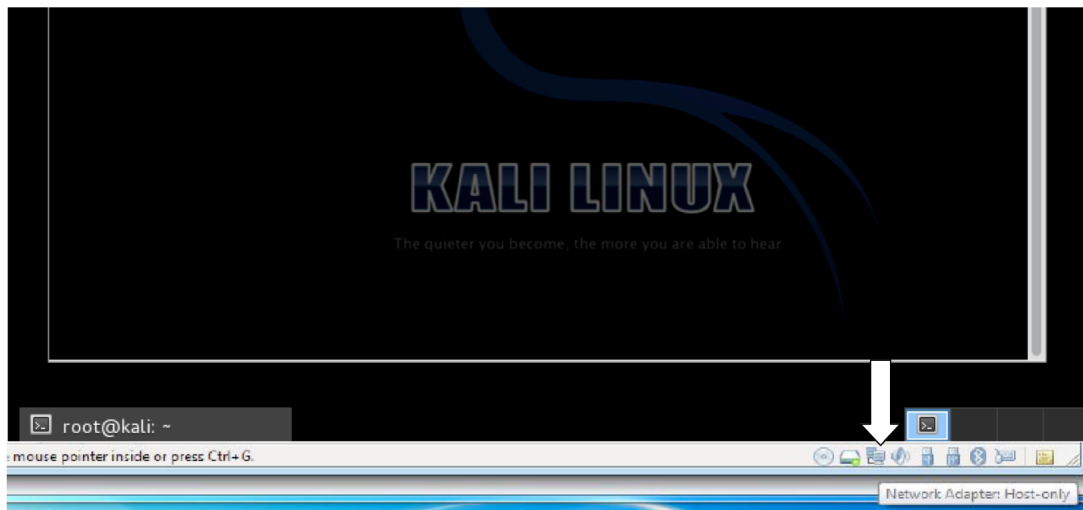
2. Lancer la machine Kali à partir de VMware et ouvrir une session
3. Personnaliser le prompt de votre machine Kali avec la commande suivante en remplaçant Nom et Prenom par votre nom et votre prénom :

```
PS1="${debian_chroot:+($debian_chroot)}\[\033[01;32m\]\u@h Prenom Nom \[\033[00m\]:\[\033[01;34m\]\w\[\033[00m\] #"
```

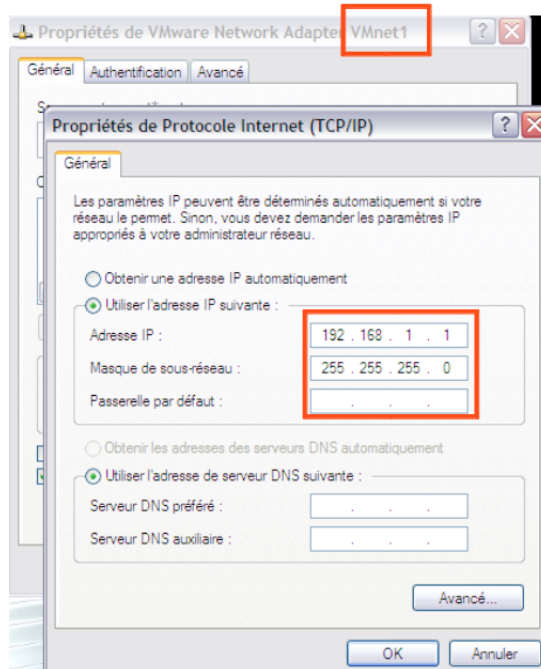


**Remarque :** Toutes les copies d'écrans demandées doivent montrer votre nom (sur un interpréteur de commande) ou votre adresse IP (sur une capture Wireshark par exemple)

4. Configurer la carte réseau de la machine Kali en mode *host-only* (hôte seulement)



5. Configurer l'interface VMnet1 de la machine hôte avec l'adresse 192.168.1.1 et le masque 255.255.255.0

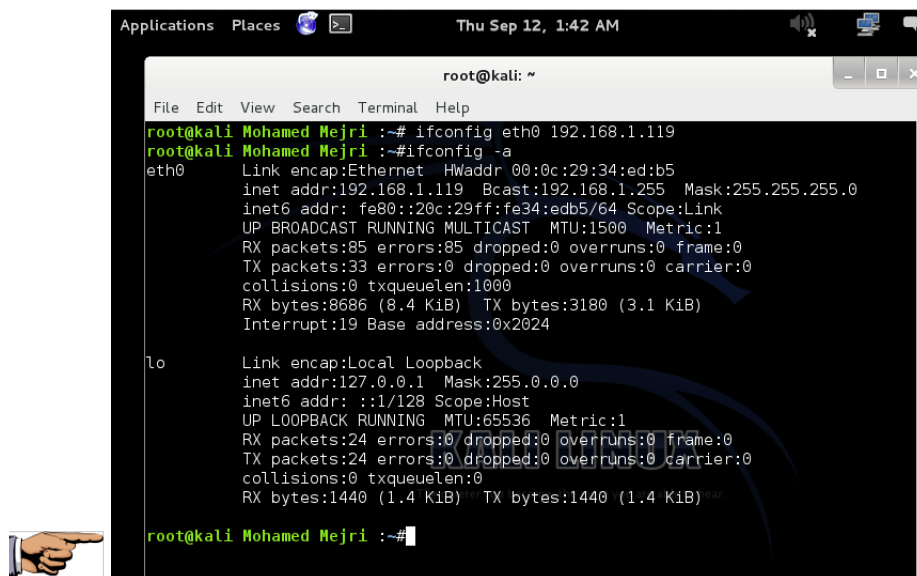


6. Configurer votre carte eth0 de Kali avec l'adresse IP :192.168.1.num\_personnel. Si par exemple votre numéro personnelle est 119, la commande de configuration sera :

```
# ifconfig eth0 192.168.1.119
```

7. (0.25pt) Afficher la configuration de vos cartes réseaux Kali via la commande :

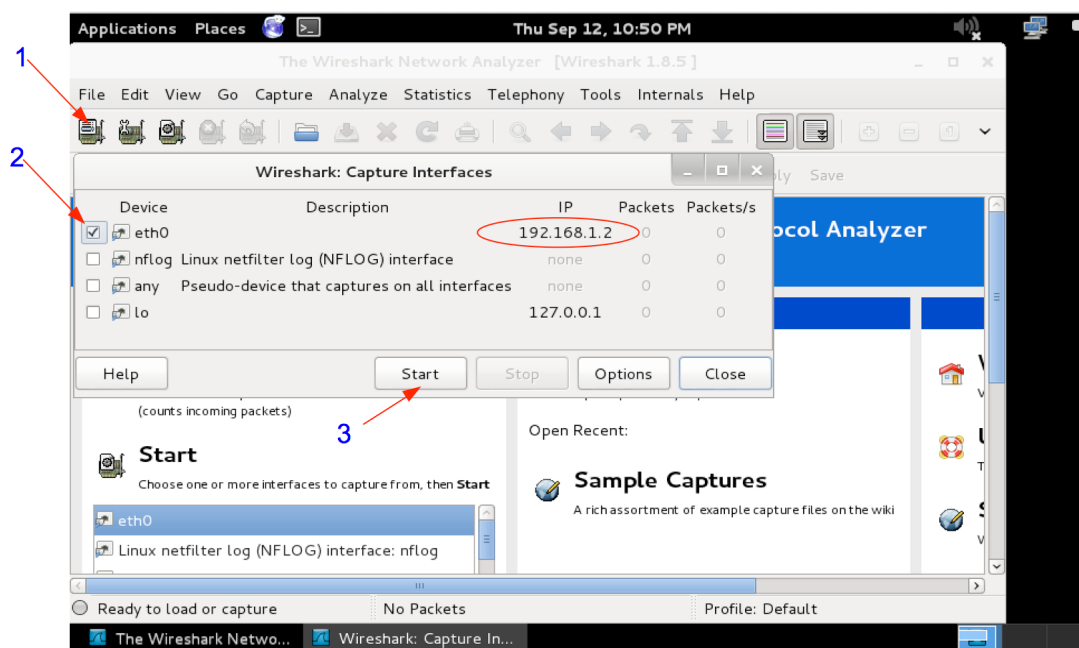
```
# ifconfig -a
```



8. Lancer Wireshark sur kali. On peut le lancer via le menu "Applications->Renifler et l'Usurpation-> ->Wireshark".



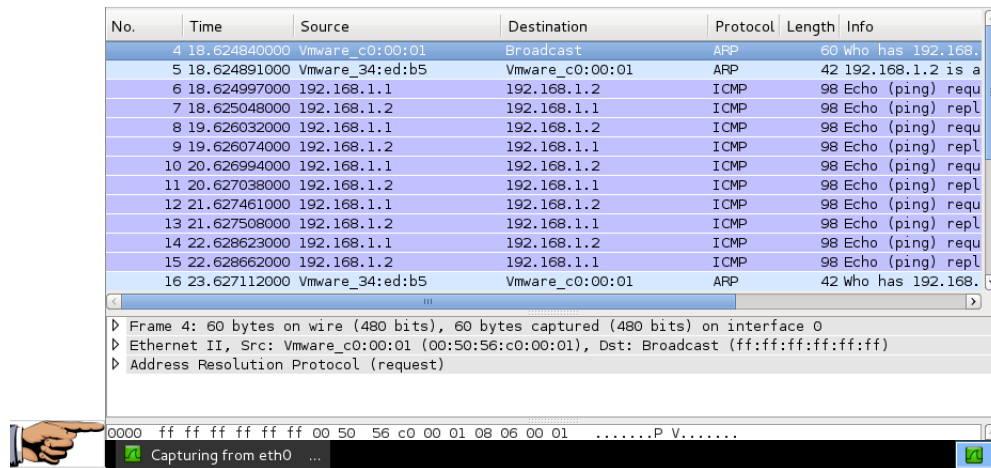
9. En utilisant Wireshark sur Kali, activer la capture sur l'interface 192.168.1.num\_personnel



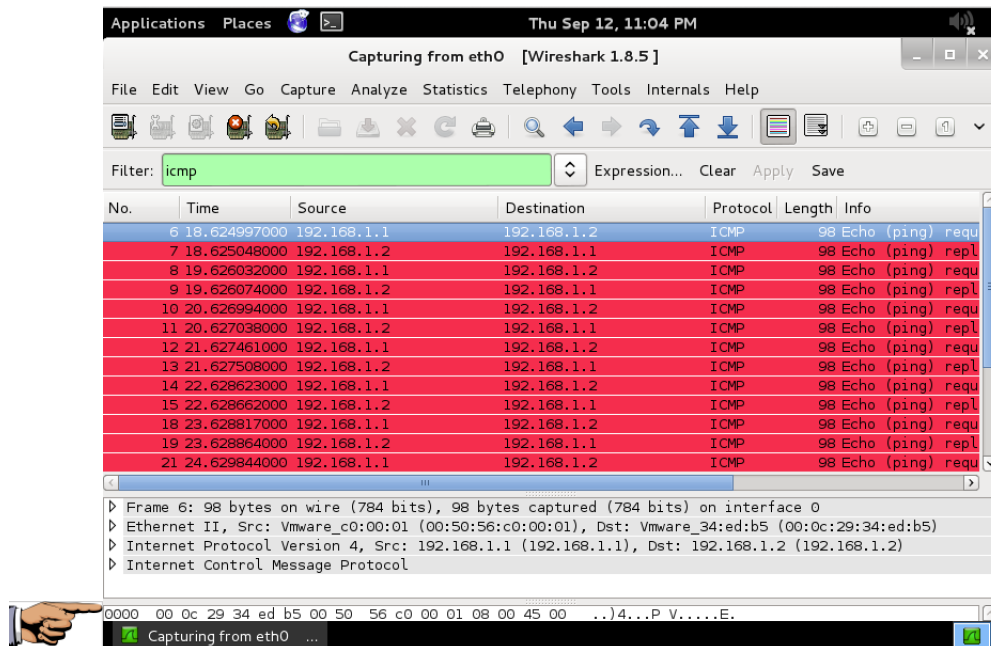
10. Vérifier que la machine Kali est accessible à partir de la machine hôte en utilisant la commande *ping* :

`ping 192.168.1.119`

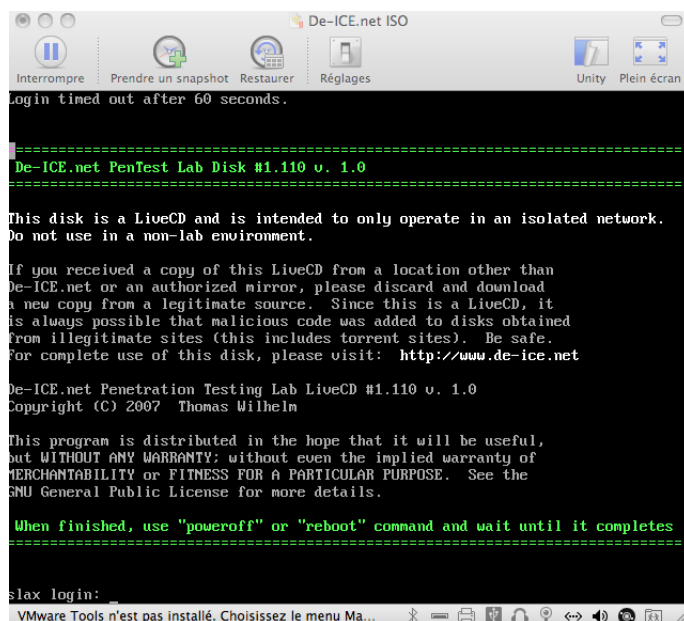
11. (0.5pt) Arrêter la capture des paquets et les filtrer en ne gardant que les protocoles *arp* et *icmp*. Pour plus de détails sur les filtres, voir le fichier *filtre.pdf* donné sur le site web du cours.



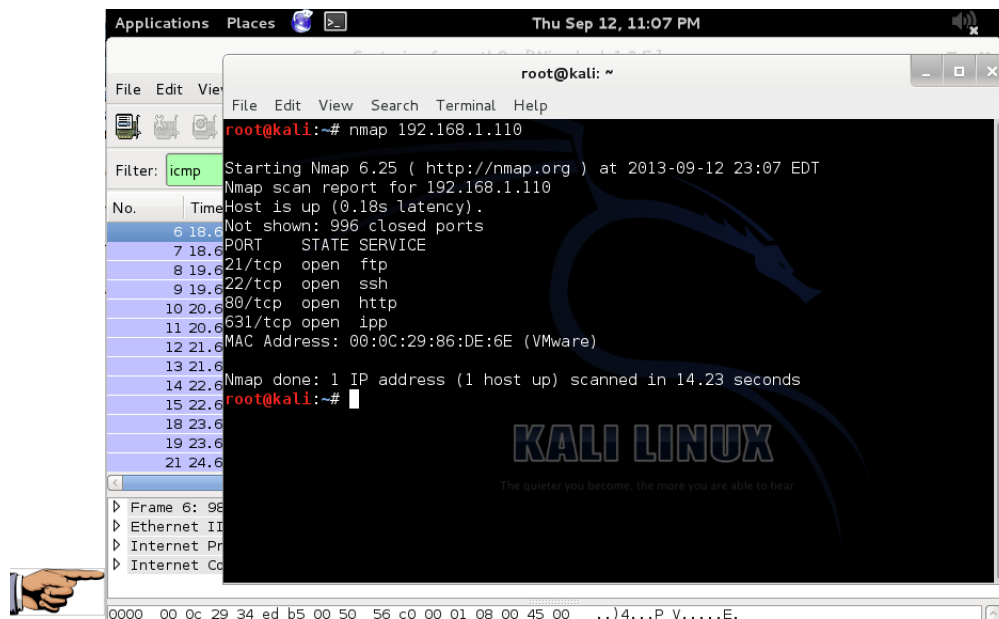
12. (0.5pt) Garder seulement le trafic *icmp* et le colorer en noir sur un fond rouge.



13. Via VMware, démarrer la machine M110.



14. Configurer la carte réseau de la cible pour qu'elle soit en mode *host-only* ((hôte seulement) ).
15. (0.25pt) Vérifier que la commande `nmap`, exécutée à partir de Kali, permet de déduire que la cible est accessible et de voir les services qu'elle offre.

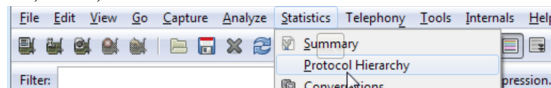


16. (0.25pt) Avec Wireshark, on peut limiter la capture à une partie de trafic respectant certaines conditions, et ce, à l'aide du menu "Capture->Interface->Options->Capture Filter".

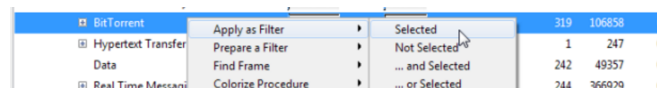
- Lancer la commande `nmap` de nouveau avec la machine 192.168.1.110 et prendre une copie d'écran du trafic Wireshark.
- Configurer le filtre "Capture->Interface->Options->Capture Filter" pour demander à Wireshark de ne capter que le trafic de type `icmp` et prendre une copie d'écran du résultat sur Wireshark.
- Retourner les deux copies d'écran précédentes pour montrer l'effet du filtre.
- Éliminer le filtre précédent avant de poursuivre le travail.

17. (0.75pt) Wireshark vous permet, à travers le menu `Statistics->Protocol Hierarchy`, de visualiser les protocoles utilisés dans un trafic ainsi que les volumes des données échangés par ces derniers. Ceci facilite la tâche d'un administrateur ou d'un simple utilisateur à la recherche des protocoles suspects comme les protocoles point à point (BitTorrent, Manolito, SoulSeek, JXTA, SMPP) qui sont souvent utilisés par des chevaux de Troie.

- (0.25pt) Ouvrir le fichier `BitTorrent.pcap` (fourni avec le TP) et prendre une copie d'écran montrant les protocoles utilisés dans ce trafic, et ce, à l'aide du menu `Statistics->Protocol Hierarchy`.

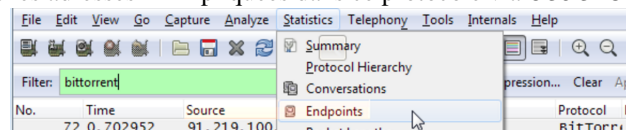


- (0.25pt) Garder seulement le trafic lié au protocole BitTorrent. Pour ce faire, il suffit de sélectionner le protocole et d'appliquer un filtre comme suit :



Prendre une copie d'écran montrant le résultat.

- (0.25pt) Voir toutes les adresses IP impliquées dans ce protocole via `Statistics->Endpoints`

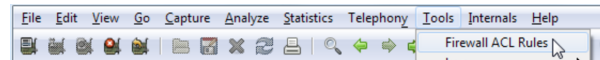


Prendre une copie d'écran montrant le résultat.

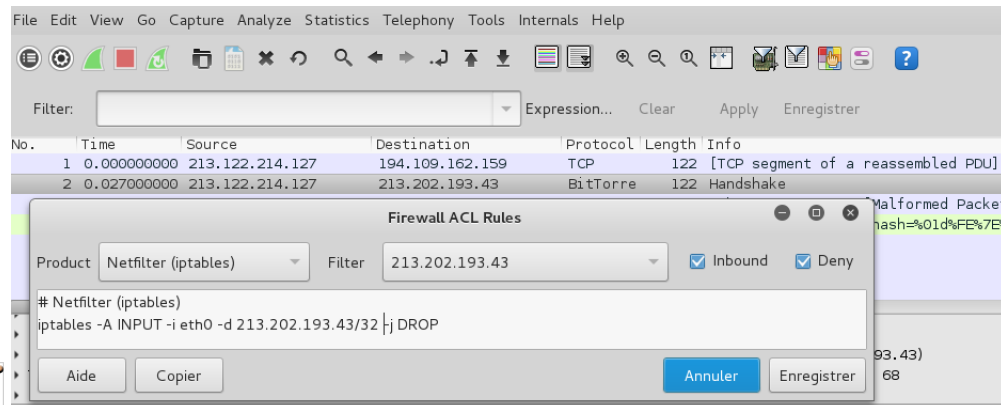
18. (0.25pt) Si vous voulez bloquer un trafic, il suffit de créer une règle de filtrage et l'ajouter à votre pare-feu favori.



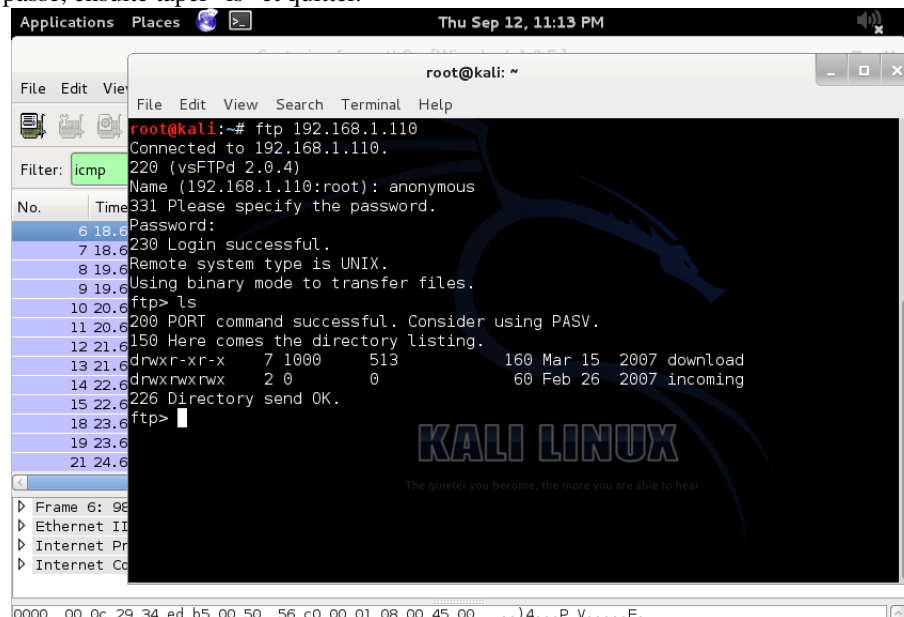
Wireshark vous donne la possibilité de générer automatiquement des règles de filtrage pour votre pare-feu via le menu Tools-> Firewall ACL Rules



- Ouvrir le fichier BitTorrent.pcap, aller à la première ligne impliquant l'adresse 213.202.193.43, puis créer une règle de filtrage pour un pare-feu iptables permettant de bloquer tout trafic provenant de cette machine sur l'interface eth0.

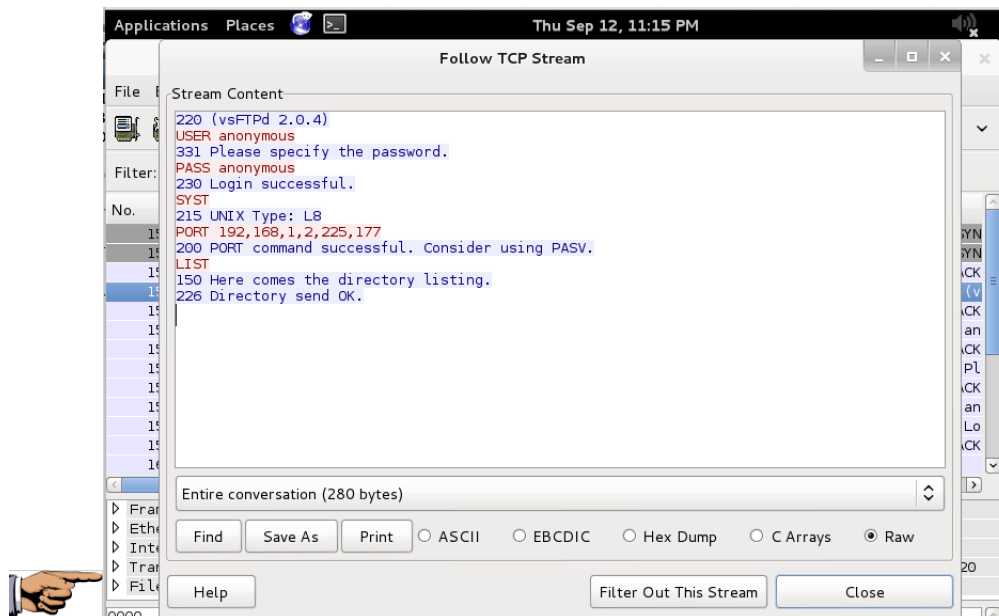


- (0.75pt) Avec Wireshark, on peut facilement découvrir les mots de passe échangés avec des services mal protégés tels que FTP, Telnet, etc.
  - Relancer *wireshark* et activer la capture de trafic sur l'interface 192.168.1.num.
  - Ouvrir une connexion FTP avec la machine 192.168.1.110 en utilisant "anonymous" comme nom d'utilisateur et comme mot de passe, ensuite taper "ls" et quitter.



- Arrêter l'interception du trafic.
- Filtrer le trafic en ne gardant que celui de FTP.
- Mettre le curseur sur le premier paquet et choisir l'option "Follow TCP Stream" dans le menu du bouton droit de la souris.
- Prendre une copie d'écran du résultat.





20. (0.5pt) Après avoir connecté votre machine Kali à Internet, lancer le navigateur et ouvrir une connexion Facebook tout en interceptant le trafic via Wireshark.

- Déterminer, en observant les trames TLS (TLSv1 ou TLSv2), l'adresse IP du serveur hébergeant Facebook, le protocole de couche réseau, le protocole de la couche transport et le protocole de la couche application.



Prenez une capture d'écran qui justifie vos réponses (encercler les informations demandées).

- Est-ce qu'on retrouve, comme dans l'exercice précédent, le mot de passe en clair dans l'échange ?



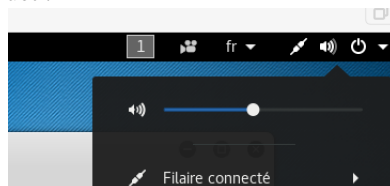
Prenez une capture d'écran justifiant la réponse.

21. (0.5pt) Avec *wireshark*, il est possible d'intercepter et d'écouter une conversation d'un téléphone VoIP.

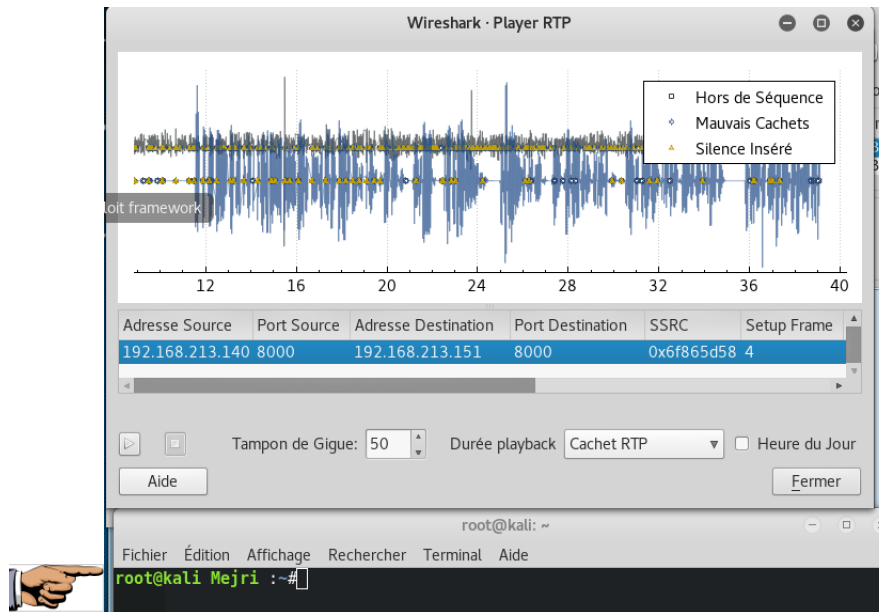
- La nouvelle version de Kali n'ajoute pas la carte son automatiquement. Pour l'ajouter, lancer la commande suivante sur un terminal :

```
root@kali:~# pulseaudio -D
W: [pulseaudio] main.c: Le programme n'est pas conçu pour être lancé en tant que
root (sauf si --system est renseigné).
```

- Assurez-vous que le volume n'est pas muet :



- En utilisant Wireshark, ouvrir le fichier *voip.pcap* fourni avec l'énoncé. Aller dans le menu "Telephony-> VoIP Calls". Choisir le fichier SIP puis appuyer sur "Jouer Flux".
- Choisir le flux ayant 192.168.213.140 comme adresse source, "Cacher RTP" dans "Durée Playback" puis écouter le message. Prendre une copie d'écran montrant ce flux ainsi qu'un terminal portant votre nom en bas.



22. (0.75pt) On peut utiliser *wireshark* pour découvrir la présence d'un malware dans un système. En utilisant *wireshark*, ouvrir le fichier *capturerootkit.pcapng* fourni avec l'énoncé. À l'aide de l'outil d'analyse des conversations (menu Statistics), montrer l'existence d'un *rootkit* dans la machine 192.168.1.119 qui envoie, via TCP, des données sensibles à un serveur distant.
- Filtrer les communications TCP vers le port 80.
  - (0.25pt) Lister, via le menu Statistics-> Conversation list-> TCP (IPV4 & IPV6), les adresses IP de l'ensemble des machines avec qui la machine 192.168.1.119 a échangé en utilisant TCP. Prendre une copie d'écran montrant le résultat.
  - (0.5pt) Sachant que le port 80 est utilisé par défaut pour faire du HTTP, montrer que ce protocole a été utilisé pour envoyer des informations insensées, liées aux mots de passe, de la machine 192.168.1.119 à un serveur distant. Prendre une copie écran et indiquer clairement ces informations sensibles.
23. (0.75pts) Un outil comme PackETH nous permet de construire des paquets en fixant une partie ou la totalité de son contenu, et ce, incluant les adresses IP et les adresses MAC.
- Suivre les étapes suivantes :
- Installer le programme *PackETH* comme suit :
    - Connecter Kali à internet (mode host-only ou NAT). Si vous utilisez le mode host-only et la machine ne se connecte pas automatiquement, essayer la commande *dhclient* comme suit :

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dhclient eth0 -v
Internet Systems Consortium DHCP Client 4.2.2
Copyright 2004-2011 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:34:ed:b5
Sending on   LPF/eth0/00:0c:29:34:ed:b5
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.2.1
Reloading /etc/samba/smb.conf: smbd only.
bound to 192.168.2.26 -- renewal in 126079 seconds.
root@kali:~#

```

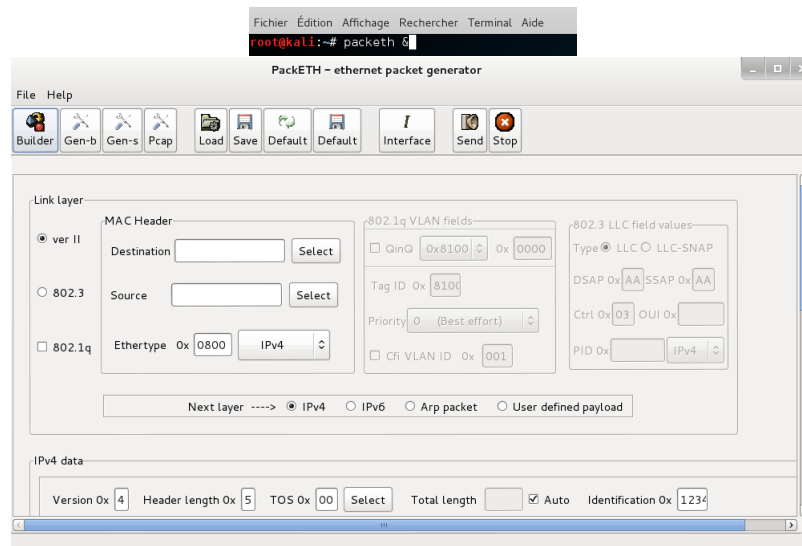
- assurez-vous d'avoir accès à Internet avant de poursuivre.
- installer packEth en utilisant la commande `apt-get install packeth`

```


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# apt-get install packeth
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  packeth
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 138 kB of archives.
After this operation, 520 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali/ kali/main packeth i386 1.6.5-2 [138 kB]
Fetched 138 kB in 0s (158 kB/s)
Selecting previously unselected package packeth.
(Reading database ... 241267 files and directories currently installed.)
Unpacking packeth (from .../packeth_1.6.5-2_i386.deb) ...
Processing triggers for man-db ...
Processing triggers for menu ...
Processing triggers for desktop-file-utils ...
Processing triggers for gnome-menus ...
Setting up packeth (1.6.5-2) ...
Processing triggers for menu ...
root@kali:~#

```


– Lancer PackETH



- Utiliser *PackETH* pour créer une trame contenant un segment TCP demandant une ouverture de connexion avec les paramètres suivants et l'envoyer à la cible :
  - @IP source = @IP de votre kali
  - @MAC source = A1 :A2 :A3 :A4 :FF :F1
  - @IP destination = @IP de la cible
  - @MAC destination = @MAC de la cible
  - Port source = 1923
  - Port destination = 23
  - Vous pouvez choisir les valeurs des autres paramètres par vous-même.

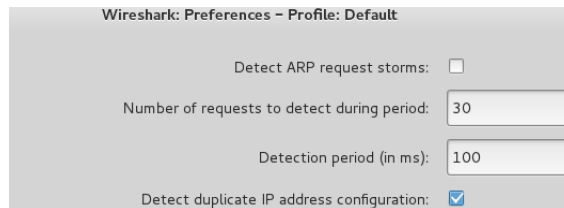
-  Utiliser *Wireshark* pour prouver que vous avez correctement créé la trame, et ce, en l'interceptant et en prenant une copie d'écran montrant ses champs.

24. (0.75pt) Utiliser PackEth pour envoyer un ping (ICMP de type 8 avec un numéro de séquence "Seq. Number" égal à 0x0011) à la machine M110.


-  Prenez une copie d'écran du contenu des champs PackEth et une copie d'écran de *Wireshark* montrant que la commande a été envoyée et que la réponse a été reçue avec le bon numéro de séquence.

25. (0.75pt) Avec *Wireshark*, il est possible de détecter le *ARP spoofing* (le fait que quelqu'un se sert de l'adresse MAC d'un autre).

- Lancer *Wireshark* et activer l'interception du trafic sur l'interface eth0.
- Aller dans le menu Edit->Preferences->Protocols->ARP/RARP et vérifier que l'option Detect duplicate IP Address Configuration est active.
- Envoyer un ping à la machine 110.

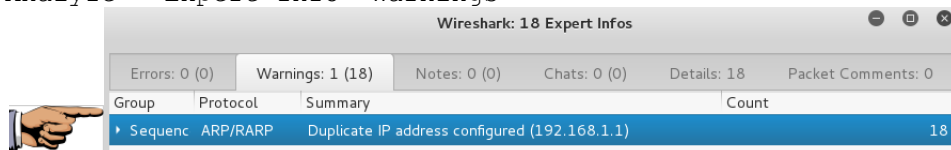


- (0.25pt) Changer l'adresse MAC de votre machine kali : Il est possible de changer notre adresse MAC autant qu'on le veut avec des outils comme *macchanger* (accessible à partir de la ligne de commandes). Le pirate l'utilise, entre autres, pour faire des attaques *Man In The Middle* (via un *ARP spoofing*) ou tout simplement pour avoir un accès gratuit à un WiFi en mode ouvert (en utilisant l'adresse MAC d'une machine autorisée) ou pour prolonger son propre accès (utile quand un point WiFi donne un accès gratuit, mais limité dans le temps pour toute adresse MAC).

Utiliser *macchanger* (voir l'aide avec l'option -h) pour modifier l'adresse MAC de votre machine Kali. 

Prendre une copie d'écran montrant la commande tapée ainsi que l'adresse MAC de votre machine Kali avant et après la modification (utiliser la commande *ifconfig* pour visualiser vos adresses MAC).

- (0.5pt) Envoyer un ping à la machine M110 en utilisant votre nouvelle adresse MAC.
- Montrer que Wireshark a détecté qu'il y a une machine qui s'est servie de plusieurs adresses MAC, et ce, en regardant dans le menu Analyze-> Expert Info->Warnings



## 6 Remarques

1. Le travail est individuel.
2. À noter que le barème (total =7.5) indiqué est à titre indicatif.

## 7 À remettre

Utilisez **le site web du cours** pour m'envoyer un fichier PDF ou WORD contenant les copies d'écrans demandées, et ce, tout en gardant le même ordre et les mêmes numérotations. **Ne m'envoyez pas vos TPs par courriels.**

## 8 Échéancier

Le 3 octobre 2016 avant 14h. À noter que les TPs remis en retard ne seront pas acceptés.