Cyber-Sécurité
TD3 - 2022

WireShark / PCAP / Python

TD individuel

Attention « bien lire le TD » : 1-Objectif et 2-Réalisation pour le prochain TD

« Dis-moi et j'oublie. Montre-moi et je me souviens. Implique-moi et je comprends. »

proverbe chinois

- Objectif du TD

1.1 L'ensemble des exercices du TD sont faits sans librairie sauf si une librairie est nommée dans l'exercice.

1.2 Vous devez faire des copies d'écran de Wireshark pour les intégrer dans Jupyter-Lab

- Pour intégrer une image dans en python3 et sur NoteBook :
  - En Mode Code :
    - **from IPython.display import Image**
    - **from IPython.display import display**
    - **x = Image(filename='ASCII.png')**
    - **display(x)**
  - **En Mode**

1.3 Ce TD devra obligatoirement être remis en fin de séance sur DVO

- Votre .zip contiendra obligatoirement :
  - L'ensemble des documents demandés et programmes python seront fait au format jupiter -lab « inbpy » pour ce TD
  - Les programmes python devront être commentés

1.4 .

2. - Préparation et Réalisation Obligatoire pour le prochain TD

L'évolution d'internet comporte certes de nombreux avantages mais aussi porteuse de risques.

2.1 Pour le prochain TD vous devez obligatoirement faire une **présentation individuelle**

- Cette présentation **individuelle** avec au minimum **un Slide par Item** et devra être remise sur Moodle avant la présentation du prochain TD au format powerpoint (.pptx) ou jupiter notebook(.inbpy) :

3. Cyber Attaque

Expliquer la méthode de l'attaque et expliquer sa réalisation :

3.1 Donner des exemples au minimum 3 par item:

- *Cyberattaques réseaux après 2020*
- *Cyberattaques par Ransomware après 2020*
- *Le confinement a t'il permis de changer les méthodes des hackers*
- *Usurpation d'identité expliquer et donner des exemples*
- *Cyberattaque Bancaire (Distributeur, Compte, …) après 2021*
- *Cyberattaque des systèmes de paiement sans fil après 2021*
- *Étude de Scapy pour Python*

4. Exercice 1- Définition

4.1 Donner la définition du réseau LAN
4.2 Donner la définition du réseau WAN
4.3 Donner la définition d'une adresse IP V4
4.4 Donner la définition d'une adresse IP V6
4.5 Donner la définition d'une adresse MAC

5. - WireShark

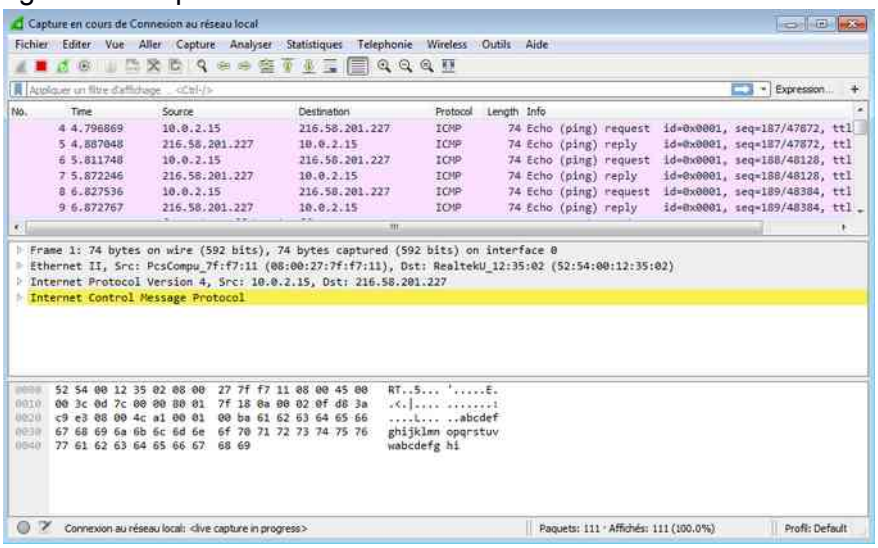
5.1 Télécharger https://www.wireshark.org/download.html (v3.2.3 minimum)

5.2 Depuis le menu Démarrer, lancer l'application Wireshark. Vous devriez voir apparaître une fenêtre similaire à celle-ci :

5.3 Ouvrir une fenêtre de commande DOS (menu Démarrer - > Exécuter ->cmd) ou en mode terminal sous Linux

lancer un ping en continu sur 8.8.8.8

« ping -t 8.8.8.8 pour windows »



L'affichage des résultats se décompose en trois parties :

1) la liste des paquets capturés disponibles en dessous de la barre de menu avec un affichage synthétique du contenu de chaque paquet.

2) la décomposition exacte du paquet actuellement sélectionné dans la liste. Cette décomposition permet de visualiser les champs des entêtes des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.

3) La troisième zone contient la capture affichée en hexadécimal et en ASCII. Quand le ping s'arrête, arrêter la capture en cliquant sur le carré rouge.

Chaque ligne de la liste des paquets (premier volet) correspond à une PDU de données capturées. Si vous sélectionnez une ligne dans ce volet, ses détails s'affichent dans les volets du milieu et inférieur.

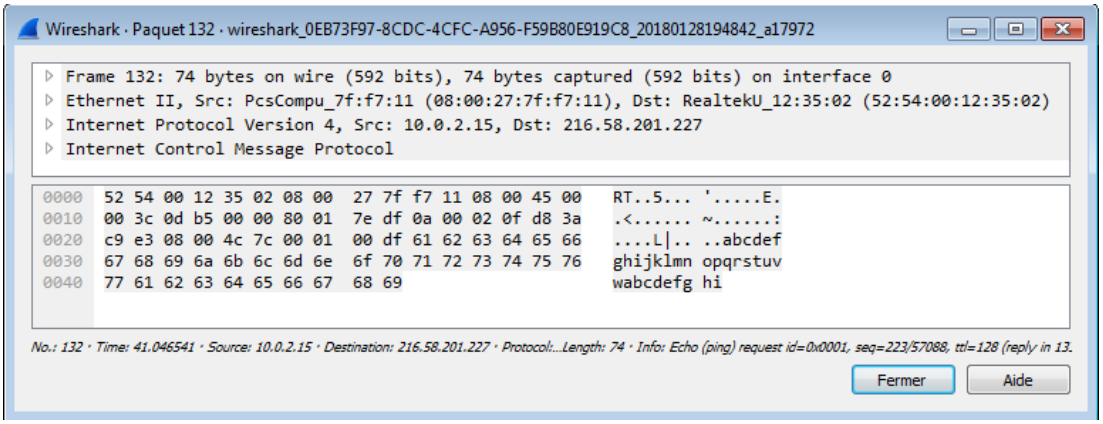
Le volet du milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.

5.4 Êtes-vous en IPv4 ou en IPv6 ?
5.5 Quelle est votre adresse IP V4 ou IP V6?
5.6 Dans quel paquet se trouve votre adresse MAC ?
5.7 Comment est composée votre adresse MAC dans les paquets de WireShark ?

6. - Analyse de la capture du ping

Quand le ping s'arrête, arrêter la capture en cliquant sur le carré rouge

6.1 Faire un « ping 8.8.8.8 »
6.2 Quel est le protocole du ping ?
6.3 Dans la première fenêtre, cliquer sur une trame contenant une requête écho (echo ping request). Le volet du milieu affiche des informations détaillées sur le paquet semblable à celles-ci :



6.4 Cliquer sur les quatre signes « > » pour développer les arborescences correspondantes.
6.5 Comme vous pourrez le constater, il est possible de développer encore chaque section et protocole.

6.6 Consacrez un peu de temps à l'étude de ces informations même si vous ne comprenez pas encore toutes les informations affichées.

6.7 Faire un « ping 2.2.2.2 »

6.8 Déconnectez-vous du réseau (Wifi ou/et Ethernet)

6.9 Faire un « ping 8.8.8.8 », que remarquez-vous ?

6.10 Faire un « ping 127.0.0.1 », que remarquez-vous ? A quoi correspond l'adresse IP 127.0.0.1 ?

6.11 Que permet de valider la commande ping ?

6.12 Trouver le paramètre pour envoyer un seul ping

6.13 Re-connectez-vous au réseau (Wifi ou/et Ethernet)

6.14 Comment est constitué le ping de la mort ?

6.15 Tester le ping de la mort sur le google.fr et valider les dialogues avec wireshark, quelle est la réponse de google ?

6.16 Expliquer le programme ci-dessous :

```
import os
hostname = "google.com" #example
response = os.system("ping -c 1 " + hostname)
#Check reponse...
if response == 0:
  print (hostname, 'is up!')
else:
  print (hostname, 'is down!')
```

6.17 Écrire un programme python du ping de la mort en modifiant légèrement le programme ci-dessus.

7. - IP LAN – commande IPCONFIG

7.1 Lancer en mode ligne de commande la commande MsDOS «ipconfig /all » (CMD) ou ifconfig -a sur MAC-OS ou linux

7.2 Combien avez-vous d'interface sur votre ordinateur ?

8. - IP WAN

8.1 http://www.mon-ip.com/ Quelle est votre @IP WAN ?

Pourquoi @IP LAN et @IP Wan sont-elles différentes ?

Quand vous cliquez sur «Informations détaillées sur votre ip» de mon-ip.com, quelles sont les informations détaillées relevées ? Refaites l'exercice chez vous ; avez-vous des différences ?

mon-ip.com est-il capable de donner votre OS ou SE ? Votre FAI ? Si oui comment ?

Quel est le numéro de port de l'@IP WAN ?

Expliquez-en quoi le numéro de port est important et à quoi il sert.

8.2 Quelles sont les différences entre IP V4 et IP V6 ?

9. - DHCP

9.1 A quoi sert un serveur DHCP ?
9.2 Quel est le protocole du DHCP ?
9.3 A l'aide de WireShark afficher l'adresse IPv4 du DHCP où se référence votre ordinateur
9.4 Qu'est-ce qu'un bail DHCP ? Pouvez-vous le trouver avec WireShark ?
9.5 Quel est le protocole complet du DHCP ?
9.6 Quelles sont les différentes attaques possible du DHCP ?

10. - DNS

10.1 A quoi sert un DNS ?
10.2 Quel est le protocole du DNS ?
10.3 A l'aide de WireShark quelle est l'adresse IPV4 ou IPV6 du serveur DNS où se référence votre ordinateur ?
10.4 Quelles sont les trames de l'échange DNS ?
10.5 Dans la réponse du DNS, retrouver l'adresse IP du site www.google.fr .
10.6 Avec la commande « ipconfig » de MsDOS, quelle option permet de lister les résolutions DNS de votre ordinateur ?
10.7 Lancer la commande linux :
10.7.1.1 dig @8.8.8.8 google.com -t ANY
10.7.1.2 expliquer le résultat
- Écrire un programme qui donne le même résultat que la commande dig

10.8 Expliquer ligne par ligne ce code

```
import dns.resolver
answers = dns.resolver.resolve('dnspython.org', 'A')
for rdata in answers:
  #print('IP', rdata)
  print('IP', rdata.to_text())
```

10.9 .

11. - Gateway

11.1 A quoi sert une Gateway / passerelle ?
11.2 Afficher l'adresse IPv4 du Gateway de votre ordinateur
11.3 par quelle commande peut-on voir la gateway sur wireshark ?

12. - Analyse d'un trafic ftp

12.1 Lancer une capture de trames.
Depuis le **mode Console**, lancez la commande **ftp dl.free.fr** (le username est essai@free.fr, et le password est celui que vous voulez).
Une fois connectés sur le serveur, tapez la commande quit et arrêtez alors la capture. Nous allons maintenant utiliser un filtre d'affichage pour n'afficher que les

trames relatives au protocole ftp. Pour cela, dans le champ Filter, vous allez saisir ftp puis cliquez sur Apply.

12.2 Quel est le protocole de la couche transport utilisé par ftp ?

12.3 Examiner la totalité de la capture, en portant votre attention sur l'affichage en ASCII, et retrouver le mot de passe saisi. Quelles sont les valeurs possibles de ce champ ?

Si jamais vous n'y arrivez pas, sélectionnez n'importe quelle trame ftp, puis dans le menu Analyse, lancez la commande Follow TCP Stream. Alors ? C'est Magique, non ?!!!

12.4 faire un programme python qui édite le login / password trouvé

13. - Analyse d'un trafic Facebook

13.1 Lancez une capture de trames. Ouvrez alors un navigateur et connectez-vous à votre compte Facebook (Attention, il ne s'agit pas d'y passer des heures !!!). Une fois que vous êtes connecté :

13.2 Existe-t-il dans la capture une trame dont le protocole est TLSv1 ?

13.3 En observant cette trame, déterminer :

a)- l'adresse IP du serveur hébergeant Facebook ?

13.4 En interrogeant le DNS, vérifier que l'adresse IP trouvée à la question précédente correspond bien au serveur de Facebook ?

13.5 Donner le développé des acronymes SSL et TLS ?

13.6 Retrouve t-on, comme dans l'exercice précédent, le mot de passe en clair dans l'échange ? Pourquoi ?

13.7 Peut-on le trouver ? Si oui que faudrait-il faire pour avoir en clair le login / password ?

13.8 faire un programme python qui édite les trames crypté du login / password

14. - ARP

14.1 A quoi sert le protocole Address Resolution Protocol ?

14.2 Lancer une capture de trames, de la commande ARP depuis la Console MsDos, lancer les commandes appropriées aux exercices suivants. Une fois la réponse obtenue, arrêter la capture, taper dans le champ Filter le protocole ARP (ne pas oublier de faire Apply) et répondre aux questions suivantes :

14.3 Faire un ping google.fr

14.4 Afficher les entrées ARP en cours en lançant la commande « arp -a »

14.5 Supprimer l'adresse de la gateway du cache ARP

14.6 Lancer la commande ping vers google.com

14.7 Afficher de nouveau la liste des entrées ARP. Quelle est la nouvelle entrée ARP ajoutée ?

14.8 Ajouter une entrée ARP statique associant l'adresse IP de Google à l'adresse Ethernet AA-85-AA-85-AA-85

14.9 Lancer la commande ping vers la machine de votre voisin ou Google. Est-ce que cette machine répond ?

14.10 Supprimer l'ensemble des adresses du cache ARP et afficher de nouveau la liste des entrées ARP.

14.11 Pour quelles raisons certaines adresses IP du réseau local existent et d'autres n'existent pas ?

14.12 Faire un programme Python qui logs ou affiche les entrées ARP

15. - TCP /UDP

15.1 Différence entre TCP et UDP

16. - Tracert - Traceroute

La commande tracert ou traceroute

16.1 Lancer une capture de trames. Depuis la Console, lancer les commandes appropriées aux exercices. Une fois la réponse obtenue, arrêter la capture.

16.2 A quoi sert la commande tracert ? Afficher l'aide de cette commande : tracert/ ?

16.3 Lancer la commande traceroute sur google.fr

17. - Netstat

Netstat est un programme de lignes de commandes qui vous permet d'afficher les connexions TCP actives sur une machine et lister l'ensemble des ports TCP et UDP ouverts. Vous pouvez ainsi voir des services qui n'ont pas besoin d'être lancés et par conséquent les arrêter et donc éviter qu'il soient exploités par d'autres.

17.1 Afficher l'aide associée à cette commande : netstat / ?

17.2 Afficher la commande :

- pour Windows « **netstat -an** »
- pour Linux «**netstat -4an**»

a) Expliquer la signification des options **-an**

b) Expliquer les différentes colonnes de la commande netstat

c) Expliquer les différents états possible de la colonne état

17.3 lister avec la commande netstat tous les ports utilisés sur votre machine ? A quoi correspondent ces ports ?

17.4 Afficher avec la commande netstat la liste des ports **uniquement** TCP utilisés sur votre machine ?

17.5 Afficher avec la commande netstat la liste des ports **uniquement** UDP utilisés sur votre machine ?

17.6 Comment afficher la liste des ports utilisés sur votre machine ?

17.7 Comment afficher l'utilisateur associé à chaque port ? Exécuter la commande