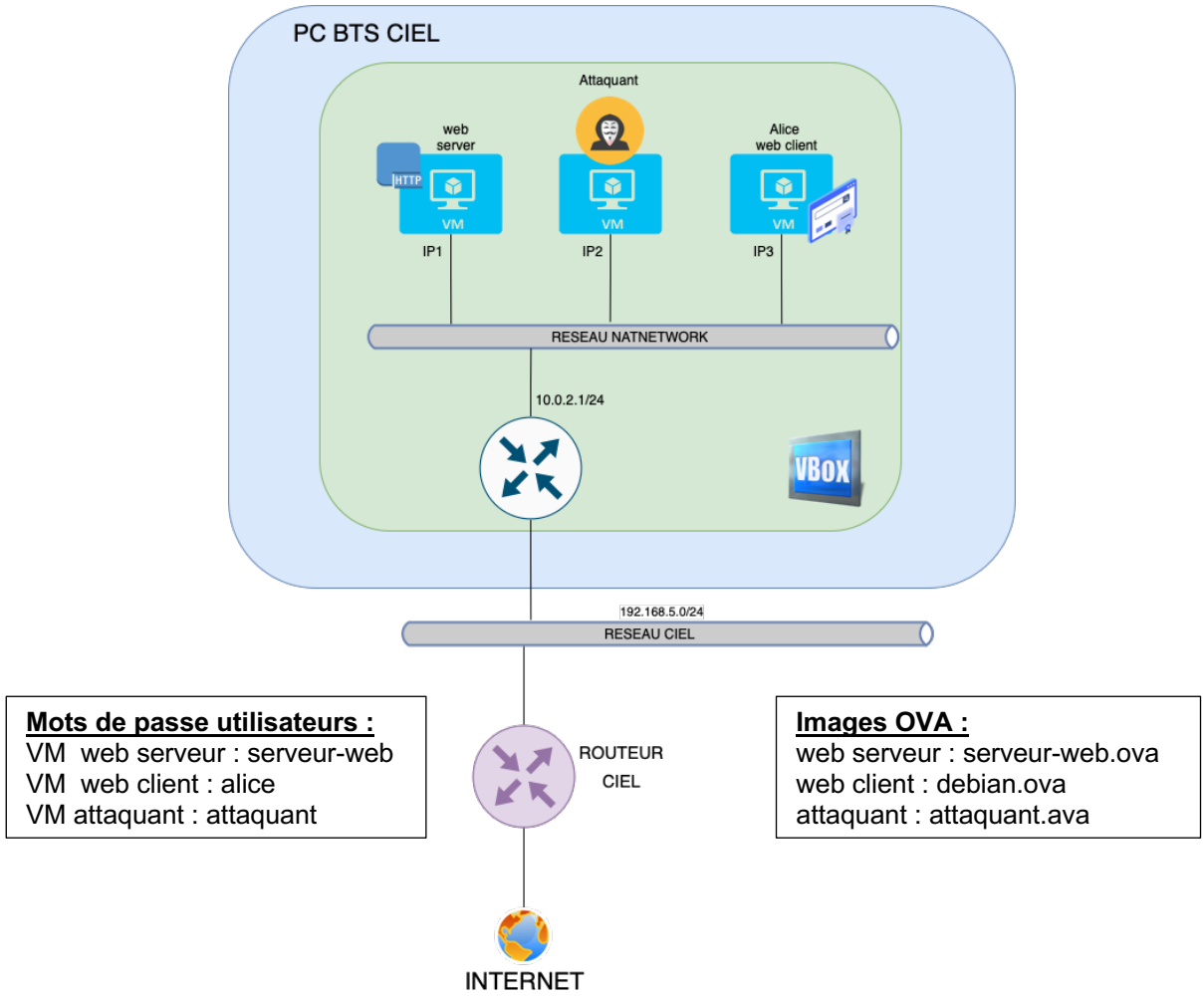
ATTAQUE MAN-IN-THE-MIDDLE DE TYPE ARP SPOOFING



Mots de passe utilisateurs :
VM web serveur : serveur-web
VM web client : alice
VM attaquant : attaquant

Images OVA :
web serveur : serveur-web.ova
web client : debian.ova
attaquant : attaquant.ava

1. Création des machines virtuelles :

1.1 Créer chaque machine virtuelle (vous pouvez vous aider du document d'aide à la création d'une machine virtuelle sur le lien : http://newtonformationsnir.fr/TP/virtualbox.pdf)

2. Relevé des adresses IP des machines virtuelles :

2.1 Relever les adresses IP des machines virtuelles.

IP1 :

IP2 :

IP3 :

3. Préparation de l'attaque :

Sur l'attaquant :

3.1 Réaliser un test de connexion (ping) depuis l'attaquant vers le serveur-web et le client Alice.

3.2 Relever le contenu de la table ARP sur l'attaquant.

Host	Adresse IP	Adresse MAC
Alice		
Serveur-web		

3.3 Relever le nom de l'interface réseau de l'attaquant.

Sur la cible Alice :

3.4 Réaliser un test de connexion (ping) depuis Alice vers le serveur-web et l'attaquant.

3.5 Relever le contenu de la table ARP sur la cible Alice.

Host	Adresse IP	Adresse MAC
Attaquant		
Serveur-web		

Sur le serveur web :

3.6 Réaliser un test de connexion (ping) depuis le serveur-web vers Alice et l'attaquant.

3.7 Relever le contenu de la table ARP sur le serveur web.

Host	Adresse IP	Adresse MAC
Attaquant		
Alice		

4. Attaque ARP Spoofing :

4.1 Effectuer l'attaque ARP Spoofing :

```
sudo ettercap -i nom_interface -T -M arp /IP serveur-web// /IP client//
```

Exemple :

```
sudo ettercap -i eno1 -T -M arp /192.168.5.254// /192.168.5.128//
```

4.2 Relever de nouveau le contenu de la table ARP sur l'attaquant, la cible et le serveur web (pour l'attaquant, pensez à ouvrir un deuxième onglet du terminal).

Sur l'attaquant :

Host	Adresse IP	Adresse MAC
Alice		
Serveur-web		

<u>Sur la cible Alice :</u>

Host	Adresse IP	Adresse MAC
Attaquant		
Serveur-web		

<u>Sur le serveur web :</u>

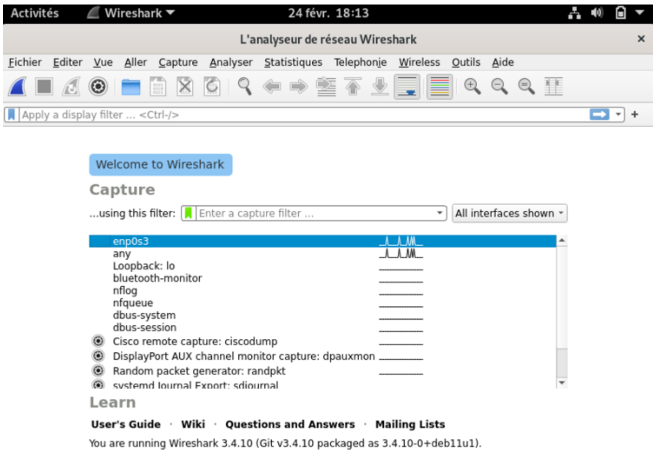
Host	Adresse IP	Adresse MAC
Attaquant		
Alice		

4.3 Que constatez-vous ?

5. Analyse des données en transit:

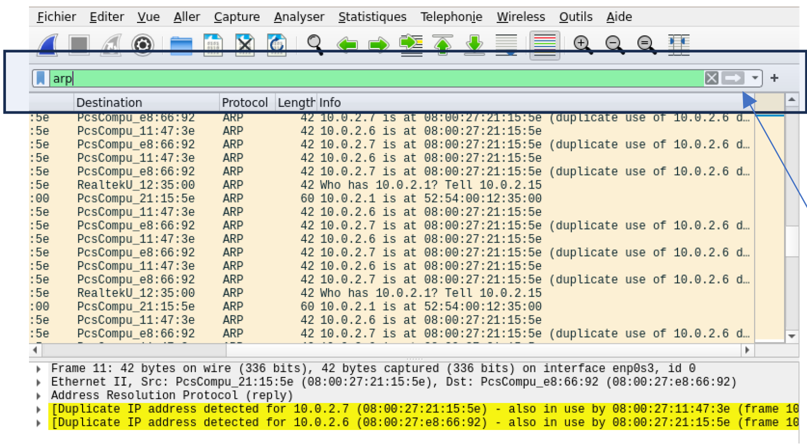
5.1 Lancer Wireshark sur l'attaquant de façon à lire les données présentes sur son interface réseau (pour lancer wireshark sur debian : sudo wireshark).

Pour choisir l'interface réseau :



5.2 Effectuer un filtre arp.

Pour appliquer un filtre :



Saisir le filtre (ici arp) dans la zone indiquée et valider le filtrage en cliquant sur la flèche.

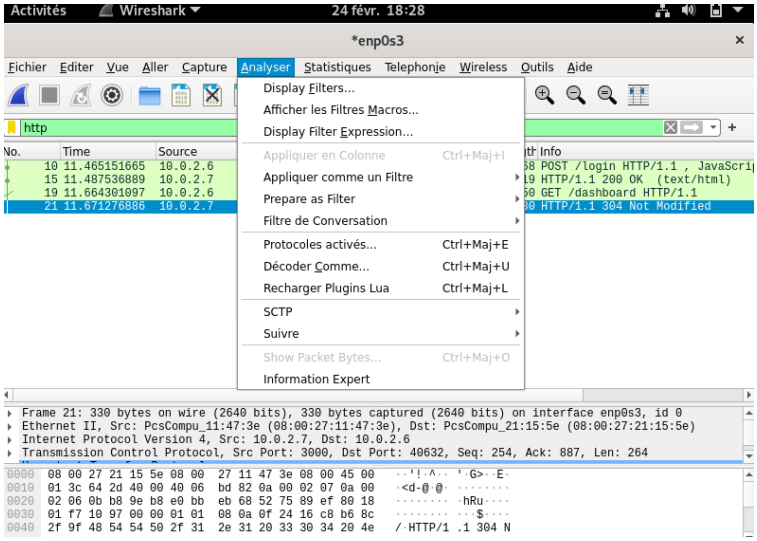
5.3 Observer et analyser les requêtes arp correspondant à l'attaque. Que constatez-vous ?

5.4 Lancer le navigateur sur la machine Alice.

5.5 Modifier le filtrage pour appliquer un filtre http.

5.6 Effectuer une requête http depuis Alice vers le serveur-web. Pour cela, on saisit dans le navigateur : http://IP1:3000 (avec IP1 : IP du serveur-web, 3000 est le port utilisé par ce serveur).

5.7 Sur wireshark, décoder la requête en sélectionnant, Analyser/Suivre/http stream



5.8 Relever le login/password.