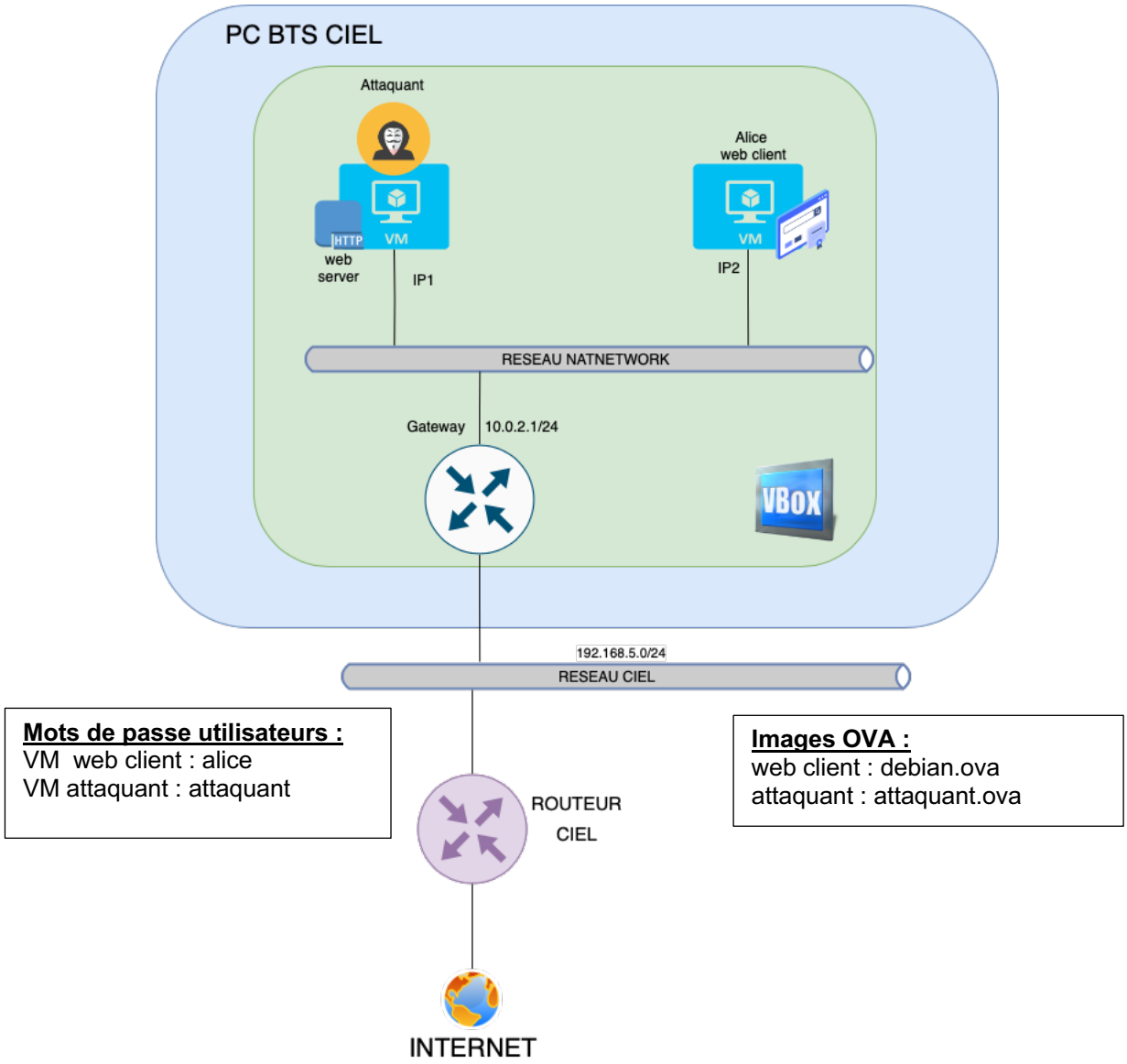
ATTAQUE MAN-IN-THE-MIDDLE DE TYPE DNS SPOOFING



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

Images OVA :
web client : debian.ova
attaquant : attaquant.ova

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 :

3. Test du réseau et des connexions internet:

Sur la cible Alice :

3.1 Réaliser un test de connexion (ping) vers la passerelle.

3.2 Réaliser un test de connexion (ping) vers le site newtonformationsnir.fr (relever l'adresse IP du site).

3.3 Lancer le navigateur web et connectez-vous sur le site web : newtonformationsnir.fr

3.4 Déterminer comment se fait la résolution du nom de domaine newtonformationsnir.fr en saisissant dans votre terminal :
`dig newtonformationsnir.fr` (relever les adresses ip du serveur dns et du site internet).

4. Préparation de l'attaque :

Sur l'attaquant :

4.1 Réaliser un test de connexion (ping) depuis l'attaquant vers la passerelle et le client Alice.

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

Host	Adresse IP	Adresse MAC
Alice		
Gateway		

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

4.4 Éditer le fichier /etc/ettercap/etter.conf en saisissant :
`sudo nano /etc/ettercap/etter.conf`.

4.5 Modifier le fichier pour que ettercap soit exécuté tout le temps avecavec les droits de superutilisateur : on fixe ec_uid=0 et ec_gid=0.

```
[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default
```

4.6 Modifier /etc/ettercap/etter.dns en ajoutant en bas les lignes suivantes :
`sudo nano /etc/ettercap/etter.dns`

```
#
# NOTE: IPv6 specific do not work because ettercap h
#       IPv6 support. Therefore the IPv6 specific ex
#       commented out to avoid ettercap throwing war
#
###################################################

newtonformationsnir.fr A 10.0.2.15
*newtonformationsnir.fr A  10.0.2.15
# vim:ts=8:noexpandtab
```

Sur la cible Alice :

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

Host	Adresse IP	Adresse MAC
Attaquant		
gateway		

5. Attaque ARP Spoofing :

5.1 Effectuer l'attaque ARP Spoofing :

```
sudo ettercap -i nom_interface -T -Q -P dns_spoof -M arp:remote /IP gateway// /IP victime//
```

Exemple :

```
sudo ettercap -i eno1 -T -Q -P dns_spoof -M arp:remote /192.168.5.254// /192.168.5.128//
```

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

Sur l'attaquant :

Host	Adresse IP	Adresse MAC
Alice		
Gateway		

Sur la cible Alice :

Host	Adresse IP	Adresse MAC
Attaquant		
Gateway		

5.3 Que constatez-vous ?

Sur la cible Alice :

5.4 Réaliser un test de connexion (ping) vers le site newtonformationsnir.fr (relever l'adresse IP du site).

5.5 Déterminer comment se fait la résolution du nom de domaine newtonformationsnir.fr en saisissant : **`dig newtonformationsnir.fr`** (relever les adresses ip du serveur dns et du site internet).

5.6 Que constatez-vous ?

Sur l'attaquant :

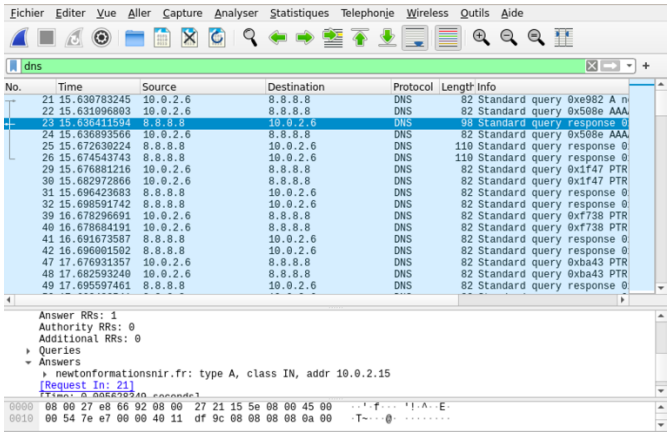
5.7 Lancer Wireshark sur l'attaquant de façon à lire les données présentes sur son interface réseau (pour lancer wireshark sur debian : sudo wireshark).

5.8 Appliquer un filtre d'affichage dns.

Sur la cible Alice :

5.9 Relancer un ping vers le site newtonformationsnir.fr et analyser le relevé wireshark sur l'attaquant.

5.10 Observer la réponse du serveur DNS 8.8.8.8 (réponse à la demande de résolution du nom de domaine newtonformationsnir.fr).



5.11 Que constatez-vous ?

6. Installation d'un serveur web apache sur le serveur :

6.1 Lancer un nouvel onglet de terminal.

6.2 Installer un serveur web apache sur le serveur :

```
sudo apt update
sudo apt install apache2.
```

6.3 Dans le répertoire /var/www/html, renommer le fichier index.html en index.old.html (sudo mv index.html index.old.html).

6.4 Avec nano, créer un nouveau fichier index.html (sudo nano index.html).

6.5 Compléter le fichier avec le texte : Hi, You have been hacked.

6.6 Sauvegarder

7. Test depuis la victime :

7.1 Tester depuis la victime alice la connexion http vers le serveur newtonformationsnir.fr (utiliser le navigateur).