Objectifs pédagogiques :

L'objectif de ce TP est de découvrir certains aspect de la cybersécurité.

Matériel

Un Raspberry Pi (Abrégé RPi dans la suite du TP) avec les paquets suivants d'installés :

- proftpd

Objectifs du TP :

- Pourquoi sécuriser nos échanges ?
- Pourquoi isoler nos réseaux ?
- Pourquoi concevoir des systèmes en pensant en premier lieu à la sécurité ?

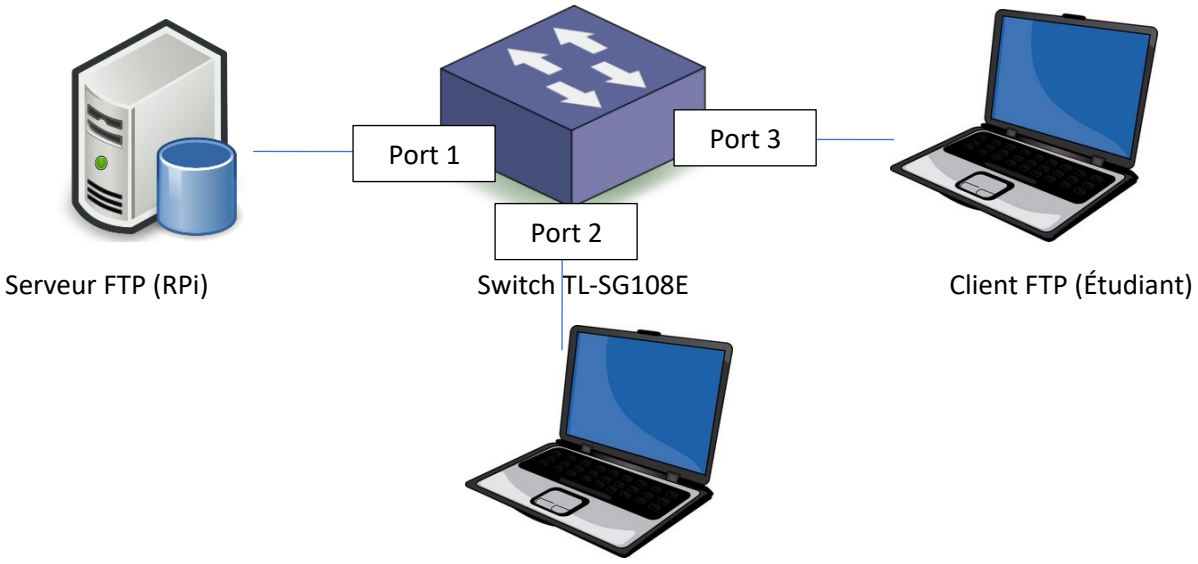
Partie 1 : Analyse de trame

Prendre un client FTP et se connecter au serveur FTP, vérifier que vous bien les accès.

Le serveur FTP est installé sur le RPi. Identifiant FTP : pi, mot de passe : raspberry

L'objectif de la manipulation est de retrouver le couple login/mot de passe. Pour écouter les trames qui circulent entre le client et le serveur FTP, nous installons un switch capable de faire du « port mirroring ». Ce switch est capable de dupliquer toutes les trames qui arrivent/partent du serveur FTP (port 1) pour les envoyer sur un autre port : le port 2.

Installer la manipulation suivante (si ce n'est pas déjà fait par l'enseignant) :



Installer Wireshark sur le poste qui servira de sniffer.

Lancer une écoute des paquets. Vous pouvez appliquer un filtre pour ne voir que les paquets qui vous intéresse. Par exemple : ip.dst == X.X.X.X

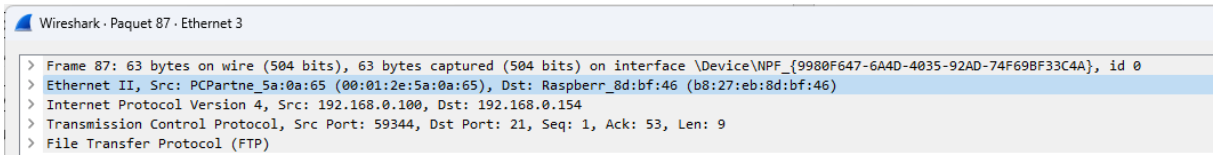
Essayer de retrouver l'identifiant et le mot de passe dans les trames.

➔ Appeler le professeur

Vous venez de hacker votre premier serveur FTP. En conclusion :

- Les flux non sécurisés doivent être bannis
- Si ce n'est pas possible, il faut séparer les réseaux et limiter/interdire les accès sur le réseau
- Il faut surveiller qui accède à ces protocoles : logs + alertes
- La configuration des applications doit être finement analysé. Donner un exemple de ce qui ne va pas avec ce serveur FTP. Et ça aurait pu être pire… Par exemple, ne pas commenter l'accès Anonyme

Dans Wireshark, cliquer sur une trame. Faite le lien entre les informations affichées et les couches OSI



Déterminer :

- les adresses MAC des deux équipements
- Le port source et le port destination
- Le code utilisé dans la couche IP pour indiquer que la communication sera du TCP
- Trouver la charge utile de la trame
- Calculer l'efficacité de la trame : nombre d'octet de charge utile par rapport au nombre d'octet total de la trame

➔ Appeler le professeur

Partie 2 : Exploitation de la vulnérabilité

Avant de commencer, appeler l'enseignant.

Maintenant que vous avez accès à la machine, nous allons exploiter cette première vulnérabilité.

Connectez vous avec un client FTP à la machine en utilisant les identifiants que vous avez « sniffé » sur le réseau.

Explorer les dossiers. Nous allons particulièrement nous intéresser au dossier /home/pi . Un dossier vous semble intéressant ?

Récupérer le fichier sur votre ordinateur et remplacer le contenu par : « Pour récupérer vos mots de passe, transférez 0,1BTC »

Vous venez de créer un Ransmoware.

Attention : avant d'éteindre le Rpi, se connecter en SSH et lancer la commande

sudo shutdown -h now

Partie 3 : Initiation au pentest

Choisissez un magasin en ligne. On va s'intéresser aux premières étapes d'un pentest (penetration test) : identifier le site web et les éléments qui le constitue.

1) Trouver adresse IP. Qui héberge le serveur ? Ou est situé le serveur ?
2) Scanner les ports ouverts sur cette adresse IP
3) Déterminer le Framework de la boutique.
4) Est-ce que la boutique utilise des plugins spécifiques ?

➔ Appeler le professeur

Partie 4 : Exercice

Créer un compte sur root-me,org puis réaliser les exercices suivants :

1) Cet exercice devrait être évident pour vous :

https://www.root-me.org/fr/Challenges/Reseau/FTP-Authentification

Pas bien plus dur :

https://www.root-me.org/fr/Challenges/Reseau/TELNET-authentification

2) Client

https://www.root-me.org/fr/Challenges/Web-Client/Javascript-Authentification
https://www.root-me.org/fr/Challenges/Web-Client/Javascript-Source
https://www.root-me.org/fr/Challenges/Web-Client/HTML-boutons-desactives
https://www.root-me.org/fr/Challenges/Web-Client/Javascript-Authentification-2
https://www.root-me.org/fr/Challenges/Web-Client/Javascript-Obfuscation-1

3) Serveur

https://www.root-me.org/fr/Challenges/Web-Serveur/Mot-de-passe-faible
https://www.root-me.org/fr/Challenges/Web-Serveur/HTTP-Directory-indexing
https://www.root-me.org/fr/Challenges/Web-Serveur/HTTP-Open-redirect
https://www.root-me.org/fr/Challenges/Web-Serveur/PHP-Injection-de-commande

Quelques leçons pour voir d'autres vulnérabilités classiques :

https://www.hacksplaining.com/lessons