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

Applicatifs non sécurisés

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 : tp, mot de passe : tpreseauinformatique

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) :

 Une image contenant texte

Description générée automatiquement Une image contenant texte, équipement électronique, ordinateur

Description générée automatiquement

Port 3

Port 1

Port 2

Serveur FTP (RPi) Switch TL-SG108E Client FTP (Étudiant)

Une image contenant texte, équipement électronique, ordinateur

Description générée automatiquement

Sniffer réseau (Étudiant)

Installer Wireshark sur le poste qui servira de sniffer.

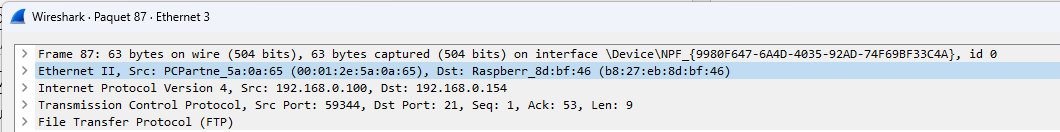
Lancer une écoute des paquets. Vous pouvez appliquer un filtre pour ne voir que les paquets qui vous intéresse. Par exemple : ip.dst == X.X.X.X

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

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 utiliser 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

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/tp . Vous allez trouver à l’intérieure un ensemble de script python. Ce sont les scripts créés par le groupe du TP5 Automate. Nous allons chiffrés les fichiers et demander 0,1BTC pour les déchiffrer.

Chercher la commande qui permet de faire un zip de fichier avec un mot de passe.

Zipper les scripts pythons avec le mot de passe « tartanpion » . Vérifier que vous arrivez bien à dézipper les fichier. Une fois que votre archive est validée, ouvrir les scripts pythons et changer le texte pour écrire « Pour récupérer vos scripts, transféré 0,1BTC à l’enseignant »

Vous venez de créer un Ransmoware.

Analyser la situation avec les groupes du TP5 :

* Est-ce que des backups ont été réalisés par le groupe de TP permettant de remettre en place l’architecture ?
* Quels sont les failles utilisées ?
* Est-il normal de mettre un système SCADA accessible de l’extérieur ? Quels sont les mesures qui auraient du être mise ne place pour éviter ces problèmes ?

Connexion par champs

Une page web de test est disponible ici : <http://wooood.fr/manager_post.php>

Le codeur a fait des choix plutôt bizarre… Inspecter la page pour découvrir quelques surprises.

Quel est le nom qui doit être saisi pour pouvoir se connecter ?

Comment est réaliser la vérification de mot de passe ?

Modifier/forger une requête pour vous connecter.

Quels sont les erreurs à ne pas faire lors de la création d’une page de connexion ?

Injection SQL

Le codeur Jean CodeAvecMesPieds à déployé un petit serveur web.

Vous êtes employé pour vérifier la sécurité de l’accès. La page est disponible ici <http://wooood.fr/manager.php>

Essayé de vous connecter. Jean a été sympa avec vous, il oublié de commenter les lignes de debug.

Avant de commencer, un peu de lecture : <https://www.w3schools.com/sql/sql_injection.asp>

A vous de trouver le mot de passe qui permet de se connecter !

Comment éviter ce genre de problème ?

Quelques leçons pour voir d’autres vulnérabilités classiques :

<https://www.hacksplaining.com/lessons>

Note de TP :

Installation du serveur FTP :

sudo apt install proftpd