Enlever l’utilisateur pi d’un raspberry

Ce court article est destiné aux OMs qui utilisent cet ordinateur minuscule qui est connecté sur des réseaux divers. Le nombre de raspberry en service plus ou moins permanents commence à devenir considérable, surtout chez les radioamateurs.

Raspbian, dérivé de Debian est particulièrement fiable, mais sa plus grosse faille de sécurité est quand même que dans trop de cas, ce mini PC travaille sous l’utilisateur « pi ». Maintenant, quand vous passez par « raspi-config » pour l’initialiser à votre cas particulier, il vous est demandé de changer le mot de passe de l’utilisateur « pi ». C’est déjà ça, mais c’est quand même très insuffisant si l’on en reste là.

Quelle est la faille?

Déjà, les raspberry sont faciles à détecter dans un réseau, en raison de leur carte réseau:

Par exemple, vous avez peut-être remarqué qu’avec nmap, quand vous scannez un réseau LAN, vous obtenez aussi l’adresse ethernet dite « MAC adress » (sans rapport avec Mac Intosh). Or la première partie de ces adresses ethernet est répertoriée par fabriquants de cartes réseau. Donc le Pi1, Pi2, Pi3 et Pi4 maintenant, ont leur adresse ethernet qui répond à cette convention. Il est donc aisé de détecter d’éventuels

raspberrys sur un LAN.

Pour se connecter à distance sur un raspberry, on utilise un client SSH. En dehors de Raspbian et d'OS comme Ubuntu et autres, l'utilisateur root est connectable avec un mot de passe. Pour Raspbian et Ubuntu, l'utilisateur root est invalidé en accès direct, les droits étendus se font avec un utilisateur particulier et qui est présent par défaut, avec la commande « sudo ». Si dans Ubuntu, lors de son installation, le premier utilisateur entré sera l'utilisateur sudo, avec les raspberry ce rôle est d'office attribué à l'utilisateur « pi ». On voit que Raspbian a ce défaut de l'utilisateur pi connu de tous avec son mot de passe « raspberry » par défaut.

Il n'est pas rare de voir des raspberry qui restent configurés avec l'utilisateur « pi » et son mot de passe par défaut: « raspberry ». Une première mesure prise par les développeurs de Raspbian, a été de demander dès l'ouverture initiale de la commande « raspi-config », de changer le mot de passe de « pi ». C'est quand même un peu mince comme mesure de sécurité.

En effet, un hackeur n'a pas dans le cas de Raspbian à deviner le nom de l'utilisateur aux droits de « root ». Il sait que c'est « pi ». Il reste seulement à trouver son mot de passe. Une fois fait, le pirate a tous les droits dans le raspberry. Comme indiqué précédemment, en SSH on ne peut pas se connecter directement avec comme nom d'utilisateur « root » pour un linux debian, redhat etc. Il faut d'abord se connecter avec un nom d'utilisateur ordinaire. Ce n'est qu'une fois qu'on est connecté sur la console via SSH que cet utilisateur ordinaire passera en « root ». Donc avec un utilisateur linux ordinaire, il y a les difficultés:

- trouver un nom d’utilisateur qui existe dans le système à pénétrer;
- trouver son mot de passe;
- enfin trouver le mot de passe de root.

Avec Raspbian, le seul défi est de trouver le mot de passe de « pi ».

Donner un mot de passe à « root »:

Pour cela, quand on est connecté au raspberry par l’utilisateur « pi », il faut entrer un mot de passe dans « root ». De ce fait, on rend accessible « root » en connexion. Alors que sans mot de passe, Raspbian est configuré pour ne pas être accessible.

Pour donner un mot de passe à « root »:

$ sudo passwd root

Vous entrez donc le mot de passe de « root »

Vous créez un nouvel utilisateur:

$ sudo adduser toto

Vous entrez son mot de passe.

Vous supprimez l’utilisateur « pi »:

Avec la commande:

$ exit

Vous vous déconnectez. Puis vous vous connectez avec l’utilisateur « root ».

Sous « root » vous faites:

 # deluser pi

Cela efface l’utilisateur « pi », puis vous effacer son répertoire:

 # rm -Rf /home/pi

Il faut effectivement effacer ce répertoire pour enlever toute trace de « pi ».

Voilà, l’utilisateur « pi » n’existe plus, et l’utilisateur « root » est disponible. La commande « sudo » n’est plus à utiliser et n’est plus utilisable. Pour certaines commandes qui ont besoin d’être exécutées avec les droits de « root », il faut passer sous l’utilisateur « root ».