Prise en main des outils de diagnostic du réseau avec Labtainer

Ces activités de prise en main des outils de diagnostic du réseau vont être réalisées avec une machine virtuelle spécifique **Labtainer** de l'**école Navale Supérieure américaine** (Naval Postgraduate School).

Lien : https://nps.edu/

La distribution **Labtainer** propose :

- des **environnements d'exécution** de laboratoire cohérents et provisionnement automatisé via des **conteneurs Docker**,
- des **topologies de réseau multicomposants**,
- plus de **50 exercices et outils de cyber-laboratoire**.

Il est possible de construire ses propres laboratoires.

> Les laboratoires intégrés au sein de la distribution Labtainer ont été initialement développés par l'initiative SeedLabs de l'université américaine de Syracuse au sein du Projet Seed https://seedsecuritylabs.org/Labs_20.04/(https://nps.edu/).

Installation de Labtainer

- Téléchargement de la VM : Virtual Machine Images - Center for Cybersecurity and Cyber Operations - Naval Postgraduate School (nps.edu)
- Vérifier le hash indiqué sur la page de téléchargement (SHA256) avec la commande suivante sous Windows

```
PS > Get-FileHash LabtainerVM-VirtualBox.ova -Algorithm SHA256
```

(sha256:1b45ef52b90512c56bb81e8e0000e86043b992091ec9264ab7f0ff140460a0c6)

- l'ouverture de session est automatique avec le compte **student** mot de passe **password123**.
- Le clavier étant en QWERTY, mettez le clavier en français :
  - lancez la commande **sudo dpkg-reconfigure keyboard-configuration**
  - Sélectionnez **Generic 105-key (Intl) PC**,
  - puis **French** deux fois.
  - Pour la touche spéciale **AltGr** : sélectionnez **The default for the keyboard layout**
  - puis **no compose key**. Pour que le clavier reste en français après un redémarrage, il faut désormais utiliser l'assistant graphique (cf article).

Utilisation de Labtainer

Pour utiliser Labtainer, il est nécessaire :

- d'ouvrir une session avec le compte **student**,
- d'être positionné en CLI dans le dossier **~/labtainer/labtainer-student**,

La commande **labtainer** permet de visualiser l'ensemble des labs disponibles :

```
$ labtainer
```

Pour lancer un lab, précisez le nom du lab :

```
$ labtainer telnetlab
```

- Les conteneurs Docker du lab nécessaires seront téléchargés s'ils ne sont pas présents,
- une **adresse de courriel** est demandée afin de pouvoir **distinguer** les réalisations des différents étudiants ; indiquez l'adresse de courriel de votre choix, fictive ou réelle,
- un lien s'affiche pour lancer le document PDF du lab (en anglais),
- la touche **Entrée** permet alors de lancer le lab.

> La commande CheckWork permet de vérifiez à tout moment où vous en êtes dans la résolution d'un lab.

Pour arrêter un lab, utilisez la commande suivante :

```
$ stoplab
```

> **ATTENTION** :
> Si vous n'arrêtez pas proprement un lab avec la commande **stoplab**, cela peut poser problème pour lancer les labs suivants, notamment avec la création de ponts Docker non supprimés.

Voici quelques commandes utiles pour les supprimer le ponts créés par Labtainer :

- lister les ponts (bridge) non supprimés

```
$ brctl show
```

- supprimer un pont

```
$ sudo ip link set br-xxxxxx down
$ sudo brctl delbr br-xxxxxx
```

- supprimer les réseaux docker <code shell> $ docker network prune </code>

Exemple d'utilisation de Labtainer

- Lab telnet pour découvrir Labtainer
- Lab Découverte du réseau avec l'utilitaire nmap avec Labtainer

Découvrir les vulnérabilité d'un réseau

- Fiche savoirs Outils d'analyse réseau
- Activité Labtainer : nmap-ssh
- Activité Labtainer : ARP poisoning et Man In The Middle