OpenVAS & Metasploit

`OpenVAS` est un scanner de vulnérabilités libre qui recense les failles de sécurité des hôtes d'un réseau au moyen d'une bibliothèque. Vous pourrez éventuellement utiliser `nessus` au lieu d'`OpenVAS` pour le scan de vulnérabilité. `Metasploit` est un outil de pentesting qui permet le développement et l'exécution d'exploits contre une cible. Attention, pour le bon déroulement du TP, la `kali` sera sur le réseau `LAN` de `pfSense`, comme la `lxle`. Il n'est pas nécessaire d'ajouter une entrée `dns` pour la `kali`.

1 Installation d'OpenVAS et premiers tests

`OpenVAS` n'est plus pré-installé sur la `kali` mais est disponible sur le serveur de paquets. Ajoutez-le par

```
apt update
apt upgrade
apt dist-upgrade
apt install openvas
```

A l'issue de la mise à jour, suivez les indications pour changer la version de `postgres` puis lancez l'initialisation d'`openvas` par `gvm-setup` (en étant `root`). A la fin de la mise à jour et de l'initialisation (prévoyez une bonne heure), le script va créer un utilisateur et générer un mot de passe à noter, de la forme `admin/7441a8a8-3586-430b-85d2-7efe0bbccae7` [1]. Notez bien le mot de passe ! Vérifiez l'installation par `gvm-check-setup`. Avant de vous connecter, lancez aussi la commande `gvm-feed-update` et (si besoin)

```
sudo runuser -u _gvm -- greenbone-feed-sync --type SCAP
```

Référez-vous éventuellement au guide d'installation.

1.1 Premiers tests

Pour vérifier l'installation, effectuez le test prévu par `gvm-check-setup` et résolvez d'éventuels problèmes signalés. En cas de doute, relancez `gvm-check-setup`. Le démarrage et l'extinction des démons se fait par le menu de la `kali`.
A la fin du démarrage, vous devez avoir le message

```
[*] Opening Web UI (https://127.0.0.1:9392) in: 5.. 4.. 3.. 2.. 1..
```

qui vous permet de vous connecter sur le loopback par un navigateur sur le port indiqué. Le navigateur présente l'interface d'utilisation de `gvm`. Pour préparer la suite, créez obligatoirement un nouvel utilisateur `kali/kali` dans le menu `Administration/Users`.

1.2 Scan complet

Une fois démarré le client web, lancez le scan sur une machine du réseau (voire sur toutes selon le temps disponible) en créant une nouvelle tâche avec le '`Task wizard`' en cliquant sur la petite icône de la baguette magique à gauche. Si la demande de scan échoue, regardez les logs et essayez de résoudre les problèmes. Une erreur classique est l'absence de configuration de scans à laquelle on peut remédier par :

```
sudo runuser -u _gvm -- greenbone-nvt-sync
sudo runuser -u _gvm -- gvmd --get-scanners
(note your scanner id)
sudo runuser -u _gvm -- gvmd --get-users --verbose
(note your user id)
sudo runuser -u _gvm -- gvmd --modify-scanner [scanner id] --value [user id]
```

Arrêtez et redémarrez `gvm` puis reconnectez-vous sous l'utilisateur `kali`.
Si vous avez le temps et la patience, faire la recherche de vulnérabilités côté LAN et côté WAN est intéressant (et permet de voir ce que vous avez réalisé au cours des TP). Corrigez le cas échéant les vulnérablités trouvées lorsque cela est possible.

1. Voici la commande pour changer le mot de passe de l'utilisateur `admin` : `gvmd -user=admin -new-password=nouv-mdp`.

2 Metasploit

`Metasploit` est intégré à `kali`. On peut l'utilise en mode console. Lancez `msfdb init` avant tout et le service `postgresql`.
Utilisez `Metasploit` pour identifier les machines de votre réseau (voire leurs faiblesses). Aidez-vous du tutoriel ou, de façon plus basique pour démarrer et pour chercher des vulnérabilités, ou plus simple, pour la prise en main. Normalement, vous avez utilisé `Metasploit` dans un autre cours et vous devriez arriver à le faire marcher. A minima, essayez de trouver les ports ouverts par la commande `use auxiliary/scanner/portscan/tcp` puis de lancer un scan `db_nmap -sV -p 22,25,80,443,993 lxle.cssr.tp`

3 Sécuriser votre serveur

Une fois réalisé l'audit de sécurité de la `lxle`, vous pouvez tenter de corriger les failles signalées par `OpenVAS`, `nmap` etc. Pour vous aider dans sa sécurisation, vous pourrez utiliser l'outil fourni par lynis et appliquer les correctifs proposés.

L'usage de tels outils est INTERDIT ailleurs qu'au sein de votre LAN.