

OpenVAS | Nessus & Metasploit

OpenVAS est un scanner de vulnérabilités libre qui recense les failles de sécurité des hôtes d'un réseau au moyen d'une bibliothèque. Il m'a fallu plus de 4h pour avoir une installation OpenVAS utilisable. Notez qu'un container Docker est aussi disponible pour OpenVAS. 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. Lorsque la kali sera sur le réseau LAN de pfSense, comme la lubuntu, il ne sera pas nécessaire de l'ajouter au dns.

1 Installation d'OpenVAS et premiers tests

Avant tout, vérifiez que votre VM kali dispose bien d'au moins 4Go de RAM. 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 postgresql-16-pg-gvm
```

A l'issue de la mise à jour, suivez les [indications](#) pour changer la version de postgres (en remplaçant 14 par 15 et 15 par 16). Lancez l'initialisation d'openvas par gvm-setup (en étant root). A la fin de la mise à jour et de l'initialisation (prévoyez plusieurs heures), le script va créer un utilisateur et générer un mot de passe, de la forme admin/7441a8a8...¹. Notez-le bien ! Terminez l'installation par greenbone-feed-sync et pensez à régler tous les problèmes indiqués par FIX. Référez-vous éventuellement au [guide d'installation](#) incomplet.

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 ou par un gvm-start.

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 lancer un scan, créez obligatoirement un nouvel utilisateur kali/kali dans le menu Administration/Users. avec le rôle admin.

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 problèmes². Une erreur classique est l'absence de configuration de scans à laquelle on peut remédier par³ :

```
sudo runuser -u _gvm -- gvm --get-scanners //(note your scanner id)
sudo runuser -u _gvm -- gvm --get-users --verbose //(Note your user id)
sudo runuser -u _gvm -- gvm --modify-scanner [scanner id] --value [user id]
sudo runuser -u _gvm -- gvm --modify-setting\
    78eceaec-3385-11ea-b237-28d24461215b --value [user id]
*runuser -u _gvm -- gvm --modify-scanner [scanner id]\
    --value dabd2710-aebd-4048-a8c7-460b60e5fa93
runuser -u _gvm -- gvm --modify-scanner 78eceaec-3385-11ea-b237-28d24461215b\
    --value dabd2710-aebd-4048-a8c7-460b60e5fa93 // et --modify-setting
```

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

2. Il suffit parfois d'attendre que les synchros aient fini.

3. C'est la commande marquée par * qui a permis de débloquer le scan

Si vous avez le temps et la patience, faites 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 vulnérabilités trouvées lorsque cela est possible.

2 Nessus comme alternative à OpenVAS

L'installation de Nessus est beaucoup plus simple que celle d'OpenVAS...

Il suffit de télécharger le paquet [Nessus-10.6.4](#) et de l'installer par la commande `dpkg -i`. Une fois le paquet installé, il faut charger le service par `systemctl start nessusd.service` qui va lancer automatiquement le navigateur et se connecter sur le loopback au port 8834.

Faites ensuite le choix de l'installation en ligne, choisissez `Nessus essentials` pour obtenir un code d'activation du logiciel. Pensez à créer un utilisateur, attendez la fin des mises à jour avant de faire une recherche de vulnérabilités, du côté WAN sur l'IP de pfSense et sur le réseau côté LAN.

Si vous avez réussi à installer OpenVAS, vous pouvez comparer les résultats obtenus.

3 Metasploit

Metasploit est intégré à kali. On peut l'utiliser 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 depuis la kali connectée côté LAN : `db_nmap -sV -p 22,25,80,443,993 lubuntu.cssr.tp`

4 Sécuriser votre serveur

Une fois réalisé l'audit de sécurité de la lubuntu, 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.