TP 5 – OpenVAS

On commence par mettre les systèmes à jour, installer OpenVAS, mettre à jour PostgreSQL vers la version 15 et lancer le setup openVAS avec *gvm-setup*.

Après avoir terminé le setup, on obtient le mot de passe **1205bd04-5ac9-4d93-a8c3-cc8f66ca23fb**.

On lance ensuite la commande *gvm-feed-update* et *sudo runuser -u _gvm -- greenbone-feed-sync --type SCAP*.

On lance ensuite *gvm-check-setup* :

```
┌──(root㉿kali)-[~]
└─# gvm-check-setup
gvm-check-setup 22.4.0
  Test completeness and readiness of GVM-22.4.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 22.4.0.
        OK: Notus Scanner is present in version 22.4.1.
        OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
        OK: _gvm owns all files in /var/lib/openvas/gnupg
        OK: redis-server is present.
        OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
        OK: redis-server is running and listening on socket: /var/run/redis-openvas/redis-server.sock.
        OK: redis-server configuration is OK and redis-server is running.
        OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
        ERROR: Directories containing the NVT collection not found.
        FIX: Run the NVT synchronization script greenbone-nvt-sync.
        sudo runuser -u _gvm -- greenbone-nvt-sync.

 ERROR: Your GVM-22.4.0 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.
```

On peut donc tenter de réparer l'installation. J'utilise pour cela la 4G de mon téléphone, la connexion WIFI de l'université présentant quelques limites.

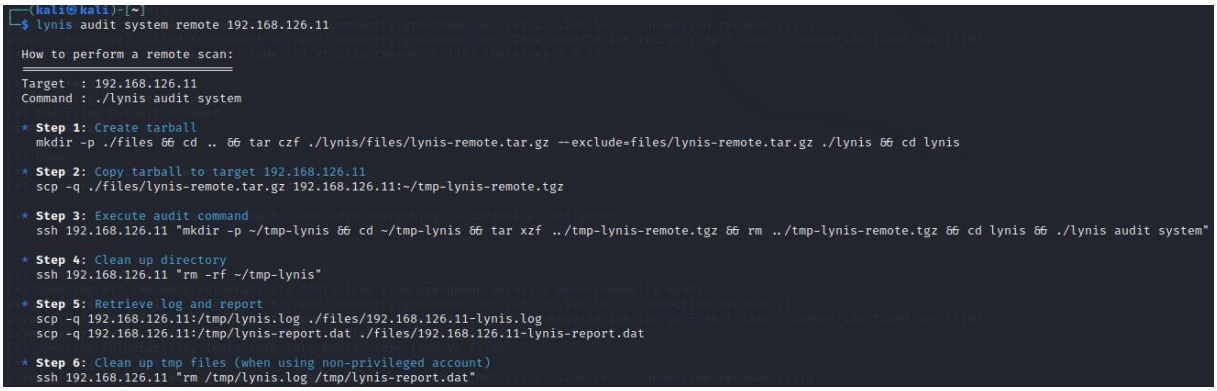
2h15 plus tard, l'installation est finalement terminée !

```
        SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.

It seems like your GVM-22.4.0 installation is OK.


┌──(root㉿kali)-[~]
└─#
```

Après avoir lancé l'interface web locale, créé un utilisateur kali, essayé de lancer le can wizard, j'obtiens l'erreur suivante :

Je lance donc les commandes spécifiées dans le TD.

Pour analyser le système distant LXLE, on peut utiliser l'outil Lynis :



Ou Niktos :