

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 !

```
WARNING: Your password policy is empty.
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 :

Failed to find port_list '33d0cd82-57c6-11e1-8ed1-406186ea4fc5'



Quick start: Immediately scan an IP address

IP address or hostname:

Je lance donc les commandes spécifiées dans le TD.

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

```
(kali@kali)~$ lynis audit system remote 192.168.126.11
How to perform a remote scan:
Target : 192.168.126.11
Command : ./lynis audit system

* Step 1: Create tarball
mkdir -p ./files && cd .. && tar czf ./lynis/files/lynis-remote.tar.gz --exclude=files/lynis-remote.tar.gz ./lynis && cd lynis

* Step 2: Copy tarball to target 192.168.126.11
scp -q ./files/lynis-remote.tar.gz 192.168.126.11:~/tmp-lynis-remote.tgz

* Step 3: Execute audit command
ssh 192.168.126.11 "mkdir -p ~/tmp-lynis && cd ~/tmp-lynis && tar xzf ../tmp-lynis-remote.tgz && rm ../tmp-lynis-remote.tgz && cd lynis && ./lynis audit system"

* Step 4: Clean up directory
ssh 192.168.126.11 "rm -rf ~/tmp-lynis"

* Step 5: Retrieve log and report
scp -q 192.168.126.11:/tmp/lynis.log ./files/192.168.126.11-lynis.log
scp -q 192.168.126.11:/tmp/lynis-report.dat ./files/192.168.126.11-lynis-report.dat

* Step 6: Clean up tmp files (when using non-privileged account)
ssh 192.168.126.11 "rm /tmp/lynis.log /tmp/lynis-report.dat"
```

Ou Nikto :

```
(kali@kali)~$ nikto -host 192.168.126.11
- Nikto v2.1.6

+ Target IP: 192.168.126.11
+ Target Hostname: 192.168.126.11
+ Target Port: 80
+ Start Time: 2023-01-18 05:48:38 (GMT-5)

+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /, inode: 120, size: 5ef37b6764bd0, mtime: gzip
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ 8725 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2023-01-18 05:48:50 (GMT-5) (12 seconds)

+ 1 host(s) tested
```