OPEN-VAS

(fork de nessus, open-source)

Plan de la présentation :
1- Démarrage et utilisation d'openvas à partir de msfconsole
2- Utilisation d'openvas à partir de l'interface web (recommandé, imo)
3- Configuration initiale d'openvas pour une première utilisation

1- DÉMARRAGE ET UTILISATION D'OPENVAS À PARTIR DE MSFCONSOLE

Démarrage des services requis :
service postgresql start
service metasploit start
#openvassd
openvas-start

charger le module d'open-vas dans msfconsole:
load openvas

connection à openvas:
openvas_connect "username" "password" localhost 9390

ajouter une cible:
openvas_target_create

liste des configurations:
openvas_config_list (standard = 1)

liste des cibles:
openvas_target_list

créer la tâche:
openvas_task_create

démarrer la tâche:
openvas_task_start

surveiller la progression:
openvas_task_list
(le progrès est en %, "-1"= terminé ou non-démarré)

liste des formats de reports:
openvas_format_list
(utiliser le format NBE ou XML(#4 ou #7))

nb: les exports à partir de msfconsole ne marchent pas, mieux d'utiliser l'interface web

2- UTILISATION D'OPENVAS À PARTIR DE L'INTERFACE WEB

3- CONFIGURATION INITIALE D'OPENVAS POUR UNE PREMIÈRE UTILISATION

création d'un certificat pour le serveur openvas:
openvas-mkcert (garder la plupart des valeurs par défault avec "enter")

création d'un utilisateur pour openvas:
openvas-adduser (ignorer les règles avec ctrl+D)

mise à jour des signature:
openvas-nvt-sync (peut être long)

Menu Kali :
Kali Linux --> vulnerability analysis --> openvas --> **initial setup**

Si problèmes (99% sur que oui):
runner le script suivant et suivre les instructions:

Kali Linux --> vulnerability analysis --> openvas --> **check setup**

corriger le problème, puis runner encore le script pour vérifier

Connection à l'interface web de openvas par le port 9392:
https://localhost:9392

Se loger avec le user créé

Rentrer l'adresse ip (là où la wizard pointe et la magie vas faire le reste.

Plusieurs types de scans.

Plusieurs formats de rapport exportables (XML préférable pour metasploit)

Pour wrapper le tout ensemble :

pour importer les scans de openvas:
db_import

pour lister les vulnérabilités:
vulns + ip