

STAGE 1ere année de Célia Baylet :

OKANTIS

5^{ème} semaine du 24 au 28 juin 2024

24/06/2024

-Clément et Ange m'ont aidé à pousser un projet avec des dossiers et sous dossiers sur git hub. (Voir documentation)

Clément m'a expliqué le fonctionnement de git hub et comment le faire fonctionner avec les commandes de bases.

(Commandes avec bash de git hub desktop)



-réunion escouade, chacun a partagé sur quoi il travaillait, puis on a parlé de la réunion sensibilisation au JO (réunion plénière) pour trouver des idées.

(voir annexe 1)

25/06/2024

-Aujourd'hui j'ai commencé l'installation d'"openVAS" sur la machine virtuelle kali.

(voir annexe 2)

-passage du professeur référent (M.Cervelle), cet après-midi.

Jeudi à 14h30 je ferai mon oral devant Clément et Patrice avant vendredi.

26/06/2024

--Aujourd'hui, j'ai continué l'installation d'openVas parce qu'hier, j'ai eu un problème et cela n'a pas fonctionné.

(voir annexe 3)

-Clément m'a conseillé d'utiliser le site de kali :

<https://www.kali.org/tools/gvm/>

--Aujourd'hui, j'ai assisté à un oral que Ange à fait, cela m'a permis de me donner des idées pour la préparation de mon oral.

--J'ai continué à préparer mon oral cette après-midi

--Nous avons eu la réunion avec l'escouade sécurité

27/06/2024

-J'ai réussi à finaliser l'installation d'OpenVas (voir annexe 4)

-J'ai avancé la préparation de mon oral

-A 14h30 passage à l'oral devant Clément et Patrice, finalisation diapo

28/06/2024

Oral de stage

| <div> <div>📅 Aujourd'hui</div> <div>^</div> <div>▼</div> <div>juin 2024</div> <div>▼</div> </div> | | | | | | |
|---|---------------------------|----------|---------------------------|----------------------------|--------|----------|
| Lundi | Mardi | Mercredi | Jeudi | Vendredi | Samedi | Dimanche |
| Mai 27 | 28 | 29 | 30 | 31 | Juin 1 | 02 |
| 03 | 04 | 05 | 06 | 07 | 08 | 09 |
| 10 | 11 | 12 | 13 | 14 10:00 Audit Lynksee | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 15:30 Point audit Ly | 22 | 23 |
| 24 | 25 15:00 Professeur Ly | 26 | 27 14:30 Oral de stage | 28 | 29 | 30 |

Annexe 1

Vocabulaire :

-Infrastructure as a service : L'IaaS est un modèle de service cloud qui fournit des ressources d'infrastructure à la demande, telles que le calcul, le stockage, la mise en réseau et la virtualisation, aux entreprises et aux particuliers via le cloud.

-biomed : Qui concerne à la fois la biologie et la médecine.

-dm : dossier médical

-une réunion dite « plénière » : désigne un type de réunion où se réunissent toutes les composantes d'une entreprise, d'un parti, d'une association ou d'une institution.

-Chrony : permet de mettre en place une synchronisation temporelle efficace et sécurisée sur l'ensemble des serveurs d'une même infrastructure.

Fiche technique :

Clément m'a parlé de la fonction 'indirect', pour avoir une liste de choix déroulant. Il faut créer d'abord un tableau avec les choix sur les lignes par exemple on l'appelle 'param' (non, oui, n/a). Puis dans le tableur d'audit par exemple, on clique sur la colonne souhaitée et dans les paramètres on rentre que l'on souhaite ce tableau (pour la liste de choix).

| | |
|-------|--|
| | |
| param | |
| OUI | |
| NON | |
| N/A | |

GIT HUB documentation :

Exemple : `http://projet`

[] :seulement la première fois

`git init`

`git add -A`

`git commit ->v1`

`git remote add origin http://projet`

`git push [-u origin main]`

`git pull [origin main]`

`git rm --cached -r bin/`

`git add .gitignore` (equivalent à `git add -A`, mais on rajoute seulement le nv fichier créer)

Si par contre j'ai mis le fichier 'obj' dans gitignore et puis après je le mets dans le dossier principal il ne le prendra pas !

Local -----push----->Server

Server -----pull----->Local

Annexe 2

OpenVAS a été développé par GreenBone,

OpenVAS, également connu sous le nom de **GVM** (Greenbone Vulnerability Manager), aujourd'hui les commandes qui étaient à l'origine avec 'openVAs' sont maintenant avec 'gvm'.



The banner features the Greenbone logo on the left, which consists of a green dragon head inside a circle. To the right of the logo, the text 'Greenbone OpenVAS' is displayed in a bold, sans-serif font, with 'Open Vulnerability Assessment Scanner' in a smaller font below it. The background is light gray with faint gear icons and a green line graphic with three dots.

Greenbone OpenVAS

OpenVAS est un scanner de vulnérabilités complet. Ses capacités incluent des tests non authentifiés et authentifiés, divers protocoles Internet et industriels de haut et bas niveau, l'optimisation des performances pour les analyses à grande échelle et un langage de programmation interne puissant pour mettre en œuvre tout type de test de vulnérabilité.

Le scanner obtient les tests de détection des vulnérabilités à partir d'un flux doté d'un long historique et de mises à jour quotidiennes.

OpenVAS a été développé et piloté par la société Greenbone depuis 2006. Faisant partie de la famille de produits commerciaux de gestion des vulnérabilités Greenbone Enterprise Appliance, le scanner forme la Greenbone Community Edition avec d'autres modules open source.

En savoir plus sur l'histoire d'OpenVAS [ici](#).

<https://www.openvas.org/>

Lien site où il y a les commandes :

<https://greenbone.github.io/docs/latest/22.4/kali/index.html>

| | |
|---|---|
| Sudo apt update | à utiliser pour mettre à jour le référentiel APT de votre appareil |
| Sudo apt upgrade | supprime les anciennes versions des packages installés ou pouvant être mis à niveau sur le système qui ne sont plus nécessaires lors de la mise à niveau. |
| sudo apt install gvm | (ancienne version 'sudo apt install openvas' (-y)) Installez Greenbone Community Edition |
| sudo gvm-setup | Exécutez le script de configuration automatique |
| sudo gvm-check-setup | Vérifiez l'installation |
| 'sudo runuser -u postgres -- /usr/share/gvm/create-postgresql-database' | On nous demande d'exécuter cette commande car 'postgres' n'est pas téléchargé. |
| sudo gvm-start // sudo gvm-stop | Démarrage et arrêt de Greenbone Community Edition |
| Se connecter : https://127.0.0.1:9392 | Connectez-vous à l'interface Web de Greenbone |

La `gvm-setup` commande prendra **beaucoup de temps** pour télécharger toutes les définitions de vulnérabilités (*fichiers Notus, fichiers NASL, données SCAP, données CRET-Bund, données gvm*).

Astuce : OpenVAS configurera également un *compte administrateur* et générera automatiquement un *mot de passe* pour ce compte qui est affiché dans la dernière section de la sortie de configuration.

Réinitialisation du mot de passe

Vous avez oublié de noter le mot de passe ? Vous pouvez modifier le mot de passe administrateur à l'aide des commandes suivantes :

- `sudo gvmc --user=admin --new-password=passwd`

<https://hassen-hannachi.medium.com/installing-openvas-on-kali-linux-a54baeaf806a>

`sudo gvmc --user=admin --new-password=passwd`

Annexe 3

Le '`gvm-check-setup`' permet de nous afficher si tout est téléchargé et donc nous explique les éventuels problèmes.

Aujourd'hui j'ai refait ces commandes :

'`sudo apt update`'

'`sudo apt dist-upgrade`' : En plus de mettre à jour les paquets existants, elles vont également être en mesure de gérer les dépendances. Si de nouveaux paquets doivent être installés pour satisfaire des dépendances, ils le seront. Ceux qui ne sont plus utiles, sont supprimés et les paquets essentiels ou requis, sont installés. Les paquets les plus importants sont traités en priorité.

'`sudo apt install gvm`'

'`sudo gvm-setup`'

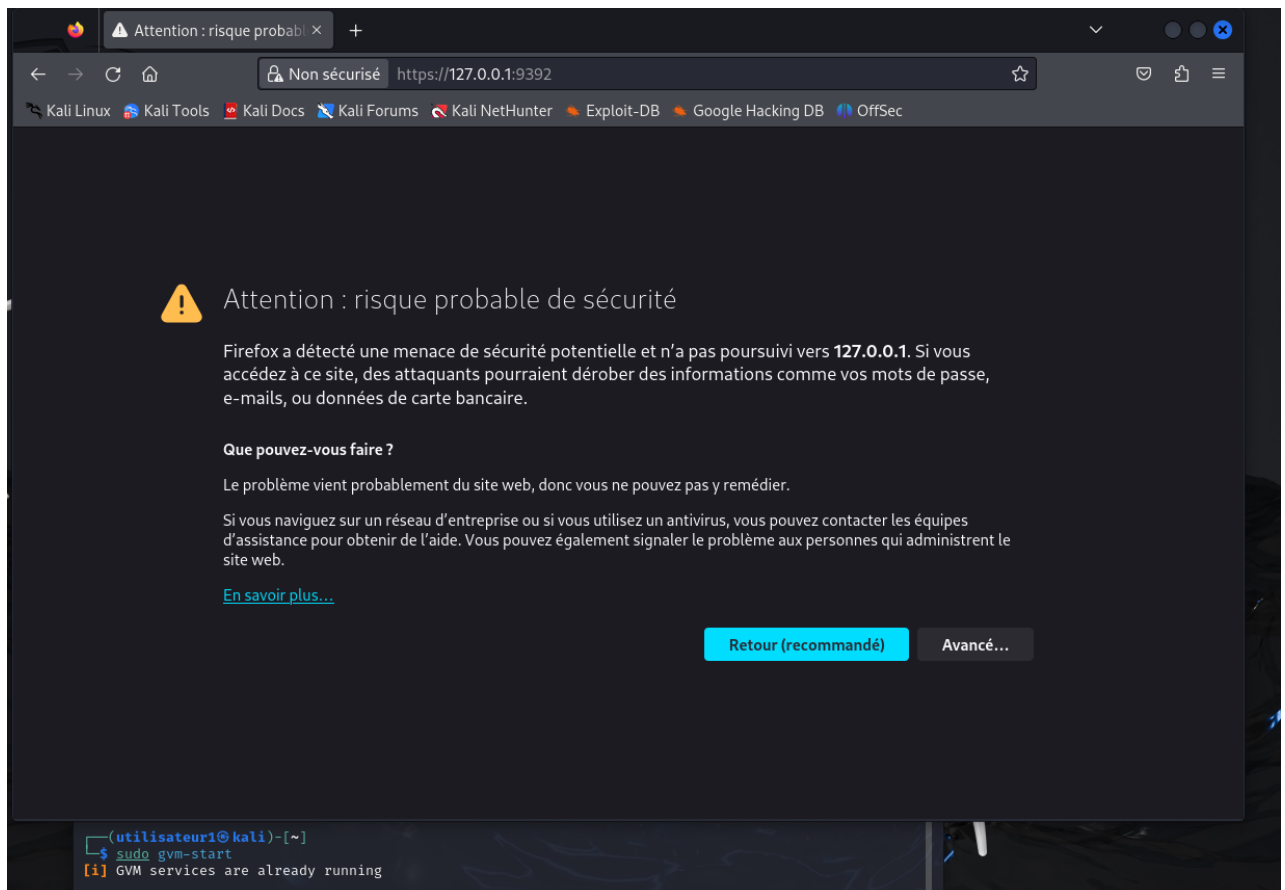
'`sudo gvm-check-setup`'

Annexe 4

'sudo gvm-check-setup'

'sudo gvm-start'

<https://127.0.0.1:9392> sur un navigateur :



Il faut appuyer sur 'Avancé...' puis sur 'Accepter le risque'

Pour se connecter ensuite il faut utiliser comme login : 'admin' et comme mdp : celui fourni lorsque l'on a effectué la commande 'sudo gvm-setup' vers la fin de l'installation nous avons un mdp.

