**Workshop Sécurité Informatique**

**Fascicule 1 : Préparation de l’environnement de travail et analyse des vulnérabilités**

**Objectifs**

* Télécharger et installer Vmware Workstation Pro / Player
* Télécharger et installer Kali Linux sur votre PC.
* Exécuter un scan de vulnérabilité sur une machine cible.
* Utiliser quelques outils de scan réseau.
* Comprendre les procédures d'identification et de correction des vulnérabilités.

**Rendu**

Vous êtes invités à réaliser toutes les étapes du fascicule et les mettre sous forme de captures d’écran commentées dans votre rapport de workshop.

**Partie 1 : Préparation de l’environnement**

**1**. Télécharger et installer Vmware Workstation pour windows  / Vmware fusion pour Linux

**2.** Télécharger et installer la machine Kali Linux à partir de : <https://www.kali.org/get-kali/#kali-platforms>

**Req** Vous pouvez télécharger une machine virtuelle Kali Linux VMware prête à utiliser. Ces images ont les informations d'identification par défaut "kali/kali".

**4.** Télécharger et démarrer la VM Metasploitable2 : lien de téléchargement https://sourceforge.net/projects/metasploitable/files/

**Partie 2 : Scan Nmap**

Nmap est un scanner de ports open source. Il détecte les ports ouverts, les serviceshébergés et les informations sur le système d'exploitation d'un ordinateur cible.

**1.** Exécuter une analyse rapide des machines. Utiliser la commande « Ifconfig » pour avoir l’adresse IP et la masque du réseau.

* nmap IP machine ou IP réseaux /masque
* Exemple : nmap 192.168.20.12/24 ou nmap 192.168.20.0/24

En utilisant nmap avec ces diverses options :

**2.** Identifier les systèmes d’exploitation d’une machine cible.

**3.** Scanner tous les ports d’une machine cible.

**4**. Vérifier l'état des ports 22 et 443 sur les machines du réseau.

**Partie 3 : Nessus Vulnerability Scanner sur Kali Linulx**

**1.** Téléchargez le package Nessus.

* Nessus-10.8.2-debian9\_amd64.deb

**2.** Installez Nessus Vulnerability scanner sur Kali Linux la commande ci-dessous :

cd /home/kali/Downloads/

sudo dpkg -i Nessus-10.8.2-debian9\_amd64.deb

**3.** Démarrer le service requis pour faire fonctionner Nessus vulnerability scanner.

* $ systemctl start nessusd.service

**4.** Confirmer que nessusd est démarré et en cours d'exécution

* $ systemctl status nessusd.service

**5.** Visitez votre interface Web Nessus sur l'adresse IP de votre serveur, le port de nom d'hôte 8834 pour terminer l'installation et l'activation de Nessus.

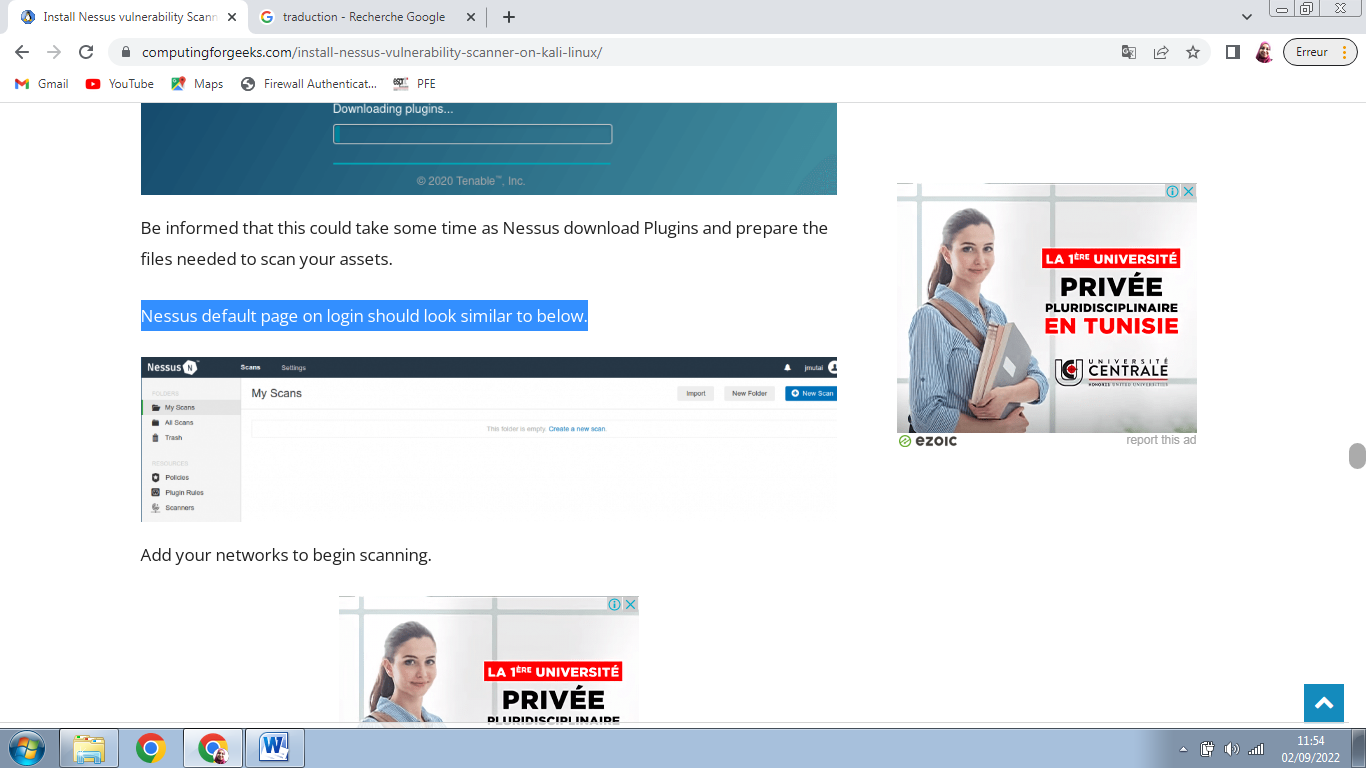
* [**https://kali:8834/**](https://kali:8834/)

**6.** Activer le produit : Nessus Essentials License

**7.** Enregistrez maintenant Nessus en saisissant le code d'activation reçu par e-mail.

**8.** Créer un compte administrateur Nessus

**9.** La page par défaut de Nessus lors de la connexion devrait ressembler à celle ci-dessous :



**Partie 4 : Exécution d'une analyse de vulnérabilité Nessus**

Pour créer une analyse d'agent :

1. Dans la barre de navigation supérieure, choisir Scans.

2. Choisir le New scan.

3. Cliquer sur le modèle de numérisation que vous souhaitez utiliser.

4. Configurer les paramètres de numérisation.

5. Effectuer une analyse immédiatement : Nessus enregistre et lance le scan.

6. Créer un rapport d'analyse dans plusieurs formats différents (exportation)

7. Utiliser des filtres pour afficher des résultats d'analyse spécifiques. Vous pouvez filtrer les hôtes et les vulnérabilités, et vous pouvez créer des vues de résultats d'analyse détaillées et personnalisées à l'aide de plusieurs filtres.

