

Lab 1 : Préparation de l'environnement de travail et analyse des vulnérabilités

Objectifs

- Télécharger et installer Kali Linux sur votre PC.
- Installer et télécharger Nessus Tenable.
- Utiliser quelques outils de scan réseau.
- Comprendre les procédures d'identification et de correction des vulnérabilités.

Rendu

Vous êtes invités à remettre, sur votre Google Classroom, un enregistrement vidéo (5min max) qui montre et interprète le travail réalisé au niveau de la **Partie 4**.

Un seul rendu est à remettre par groupe.

Partie 1 : Préparation de l'environnement

1. Télécharger et installer Vmware : <https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html>
2. Télécharger et installer la machine Kali Linux à partir de : <https://www.kali.org/get-kali/#kali-platforms>

Req : Les images Kali Linux VMware sont aussi disponibles. 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 services hébergés 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/masque`

2. Identifier les systèmes d'exploitation d'une machine cible.
3. Scan 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 Linux

1. Téléchargez le package et confirmez qu'il est disponible localement pour l'installation.

`$file Nessus-10.3.0-debian9_amd64.deb`

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

`cd /home/kali/Downloads/`

`sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb`

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

`$systemctl start nessusd.service`

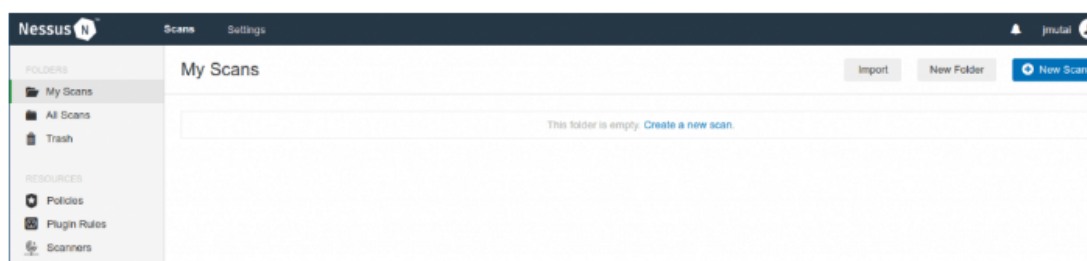
4. Confirmer que nessusd est démarré et en cours d'exécution

`$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://@IP:8834/>

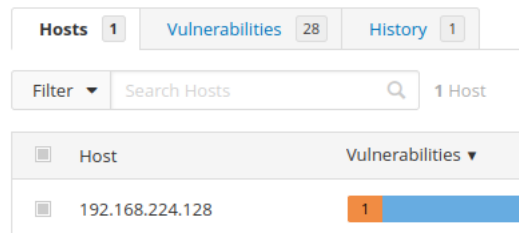
6. Activer le produit : Nessus Essentials license
7. Enregistrez maintenant Nessus en saisissant le code d'activation reçu par e-mail.
8. Créer un compte administrateur Nessus
9. La page par défaut de Nessus lors de la connexion devrait ressembler à celle ci-dessous :



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.



The screenshot shows the Nessus interface with the 'Hosts' tab selected. It displays a search bar, a filter dropdown, and a table of hosts. The table has two columns: 'Host' and 'Vulnerabilities'. The first row shows the IP address '192.168.224.128' and a bar chart indicating 1 vulnerability.

Host	Vulnerabilities
192.168.224.128	1

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