Lab de pratique

Sujet de lab : Dans cet atelier, vous utiliserez le scanner de vulnérabilités Nessus pour balayer la VM Metasploitable2 à la recherche de potentielles vulnérabilités.

Vous aurez besoin d'un hyperviseur pour installer par la suite une machine virtuelle pour pouvoir utiliser certains de ces outils pour vos labs

Partie 1 : Virtualisation

Installation de votre hyperviseur

Virtualbox (gratuit) Linux-Windows:
https://www.virtualbox.org/wiki/Downloads

Ne pas oublier de télécharger aussi (Oracle VM VirtualBox Extension Pack) dans la même page que les téléchargements.

Si vous voulez VMWare Player (gratuit) :
https://customerconnect.vmware.com/en/downloads/details?downloadGroup=WKST-PLAYER-1750&productId=1377&rPId=111473

Sinon, VMWare-Workstation est payant :
https://store-us.vmware.com/workstation_buy_dual

Partie 2 : Téléchargement et Installation Kali Linux

- Tout en un : https://www.kali.org/docs/installation/hard-disk-install/
- Téléchargement: https://www.kali.org/get-kali/#kali-platforms
- Installation : https://www.kali.org/docs/installation/hard-disk-install/

Partie 3 : Metasploitable 2

Pour le téléchargement de la VM

https://sourceforge.net/projects/metasploitable/files/latest/download

Étapes pour installer Metasploitable sur VirtualBox

https://www.geeksforgeeks.org/how-to-install-metasploitable-2-in-virtualbox/

Partie 4: Nessus

Pour télécharger Nessus

Vous avez généralement besoin d'un compte pour télécharger des images depuis Tenable qui fournit Nessus Essentials, mais ce lien vous amène directement au fichier : https://www.tenable.com/downloads/tenable-appliance?loginAttempted=true

Pour avoir son code: https://www.tenable.com/products/nessus/activation-code

Pour avoir de l'aide pour l'installation dans VirtualBox : https://medium.com/@jl620695lueva/install-and-configure-a-nessus-vulnerability-scanner-on-virtualbox-8614875013dc

A FAIRE
Source : https://cyberlab.pacific.edu/courses/comp178/labs/lab-4-vulnerability-scanning
cls
Analyse externe Nessus : demandez à Nessus d'effectuer une "analyse avancée" de votre VM Metasploitable2 :

Allez dans Analyses -> Nouvelle analyse
Sur la page Modèles d'analyse sous Vulnérabilités, choisissez le type "Analyse avancée".
Fournissez un nom pour votre configuration d'analyse (par exemple "Analyse externe")
Fournissez l'adresse IP cible (dans ce cas, l'adresse IP de la VM Metasploitable2)
Enregistrez le modèle de numérisation
Appuyez sur le bouton « Lecture » sur la page Mes scans pour lancer le scan que vous venez de créer.
Une fois l'analyse terminée, répondez aux questions sur les livrables.

Livrables (analyse externe) :

Combien de vulnérabilités classées critiques, élevées et moyennes Nessus a-t-il découvertes ?
Soumettez le rapport de Nessus pour cette analyse (format PDF, Rapport-> Liste complète des vulnérabilités par hôte)

Analyse interne Nessus : demandez à Nessus d'effectuer une "analyse avancée" de votre VM Metasploitable2. Mais cette fois, nous donnerons également à Nessus un identifiant (un identifiant, dans leur terminologie) au système cible, lui permettant d'effectuer un plus grand nombre de tests. Nessus accepte diverses informations d'identification, non seulement pour le système d'exploitation (c'est-à-dire une connexion SSH ou Windows), mais également pour des serveurs d'applications tels que des bases de données, des gestionnaires de machines virtuelles, etc.

Allez dans Analyses -> Nouvelle analyse
Sur la page Modèles d'analyse sous Vulnérabilités, choisissez le type "Analyse avancée".
Donnez un nom à votre analyse (par exemple « Analyse interne »)
Fournissez l'adresse IP cible (dans ce cas, l'adresse IP de la VM Metasploitable2)
Sous Informations d'identification -> SSH, remplacez la méthode d'authentification par mot de passe et entrez la connexion de la VM (msfadmin / msfadmin). Cela permettra à Nessus d'effectuer AUSSI une analyse depuis l'intérieur du système (en plus de l'analyse externe par défaut)
Enregistrez le modèle d'analyse
Appuyez sur le bouton « Lecture » sur la page Mes scans pour lancer le scan que vous venez de créer.
Une fois l'analyse terminée, répondez aux questions sur les livrables.

Lorsque vous avez terminé la section Nessus du laboratoire, vous pouvez arrêter le programme.

$ sudo systemctl stop nessusd
Livrables (analyse interne) :

Combien de vulnérabilités classées critiques, élevées et moyennes Nessus a-t-il découvertes ?
Soumettez le rapport de Nessus pour cette analyse (format PDF, Rapport-> Vulnérabilités détaillées par hôte).
Notez qu'il peut y avoir une légère différence dans la longueur du rapport par rapport au type de rapport précédent.
Livrable (Essai) :

Choisissez l'une des vulnérabilités classées « critique » par Nessus. Donnez le titre donné par Nessus, puis expliquez la vulnérabilité dans vos propres mots, comme si vous l'expliquiez à un autre élève. Copier et coller du texte du rapport Nessus n'est PAS une explication suffisante ici. Vous devrez peut-être suivre les liens fournis par Nessus et/ou rechercher des informations supplémentaires par vous-même.

Dans votre réponse, expliquez :

Quelle est la vulnérabilité ?

Comment pourrait-il être exploité ?
Comment pourrait-il être réparé ?
Une réponse en 2 paragraphes est un niveau de détail suffisant.

URL :

https://cyberlab.pacific.edu/courses/comp178/labs/lab-4-vulnerability-scanning
https://medium.com/@jl620695lueva/install-and-configure-a-nessus-vulnerability-scanner-on-virtualbox-8614875013dc
https://www.geeksforgeeks.org/how-to-install-metasploitable-2-in-virtualbox/
https://community.tenable.com/s/article/Reset-Nessus-password-on-TenableCore?language=en_US