Article suivant :

Comment installer Kali Linux dans VirtualBox?

Comment installer Metasploitable 2 dans VirtualBox

Dernière mise à jour : 02 avr., 2025

-

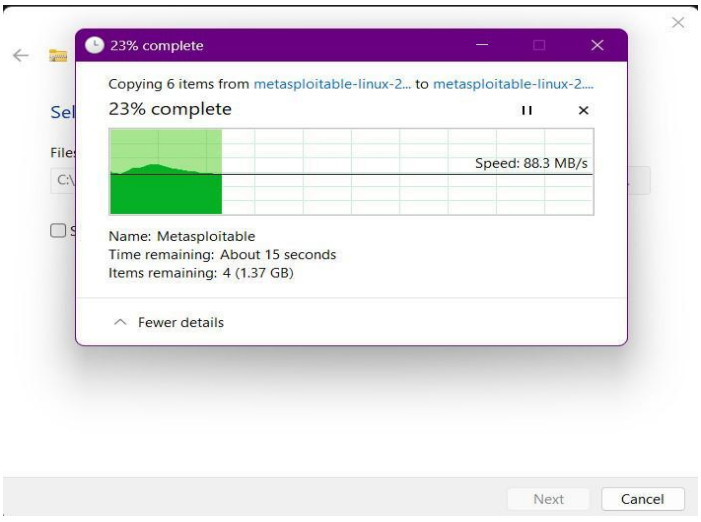
Discutons d'abord de ce qu'est Metasploitable, c'est un environnement de test très utile pour les débutants qui veulent pratiquer et tester leurs compétences en tests d'intrusion et leurs recherches en sécurité. Il s'agit d'une machine cible qui est utilisée pour découvrir et pénétrer les vulnérabilités afin que l'utilisateur ait une idée des cibles et des machines réelles.

En d'autres termes, Metasploitable est une machine virtuelle intentionnellement vulnérable version d'Ubuntu conçue pour tester des outils de sécurité et démontrer des vulnérabilités courantes.

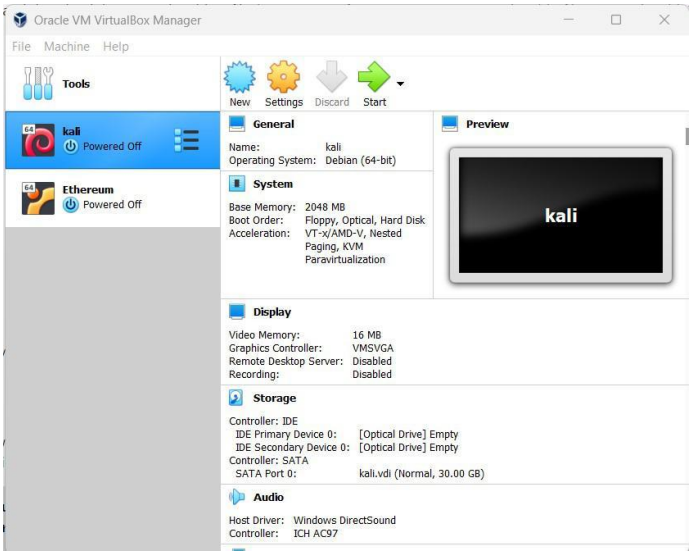
Pour installer cette machine virtuelle dans votre boîtier virtuel, nous supposons que vous avez un boîtier virtuel installé sur votre système.

Installation

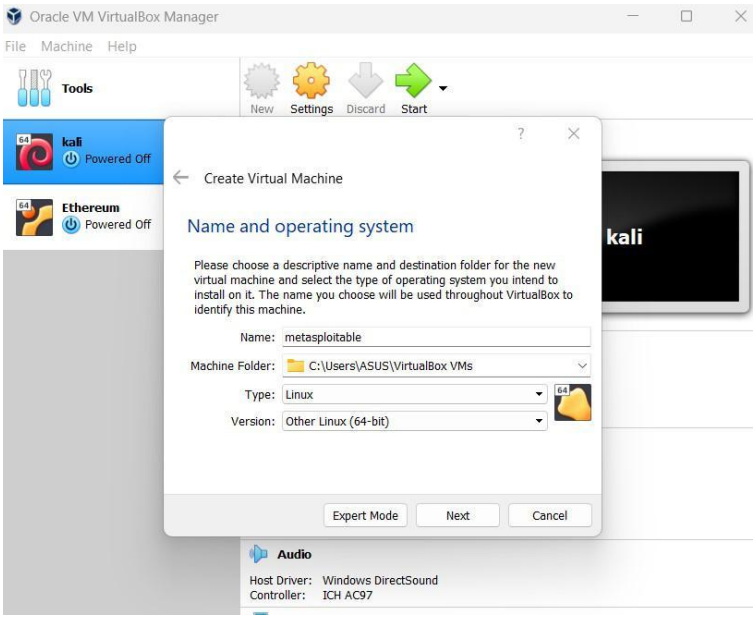
Étape 1 : Téléchargez le fichier Metasploitable 2. Il est disponible en format ZIP et contient un fichier .vmdk (disque dur virtuel) – et non un fichier ISO.



Étape 2 : Le fichier sera initialement au format zip, nous devons donc l'extraire, après avoir extrait le fichier, ouvrez VirtualBox.



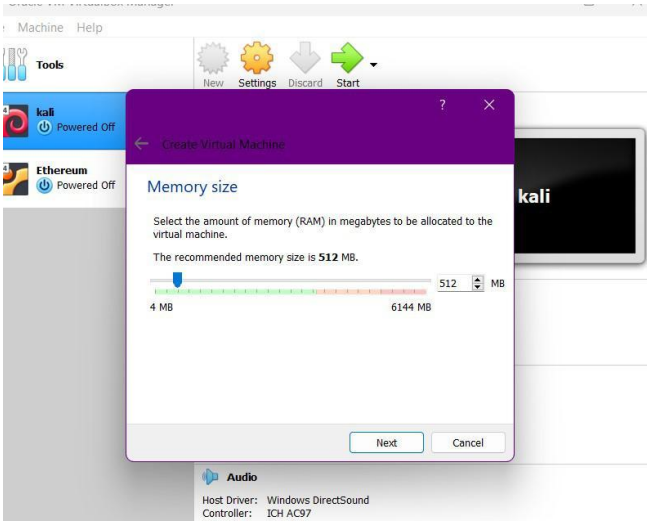
Étape 3 : Maintenant, comme le montre l'image ci-dessus, cliquez sur la nouvelle option dans la boîte virtuelle.



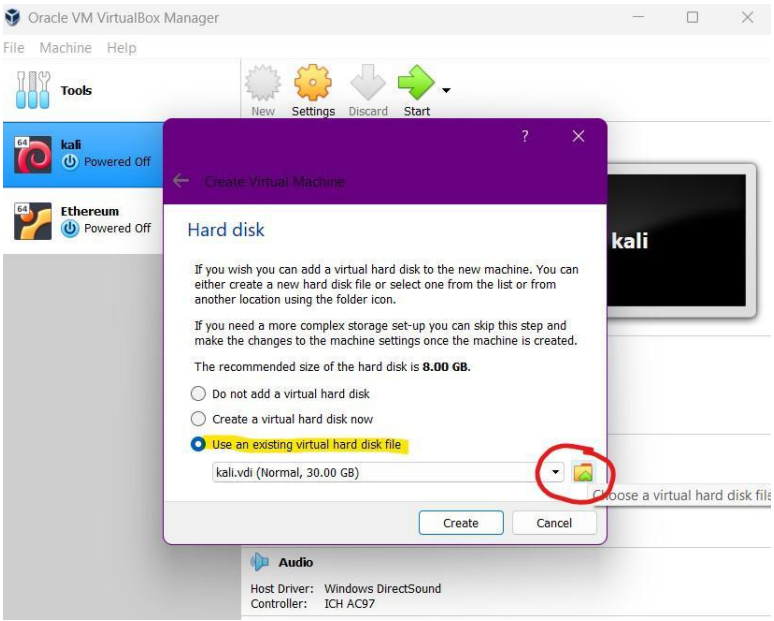
- Maintenant, une fenêtre apparaîtra et il vous sera demandé de fournir des détails tels que le nom de votre machine, le chemin d'installation, le type et la version.
- Remplissez les détails tels que :

Nom : **selon votre choixChemin : laisser comme recommandéType : LinuxVersion : autre (64 bits)**

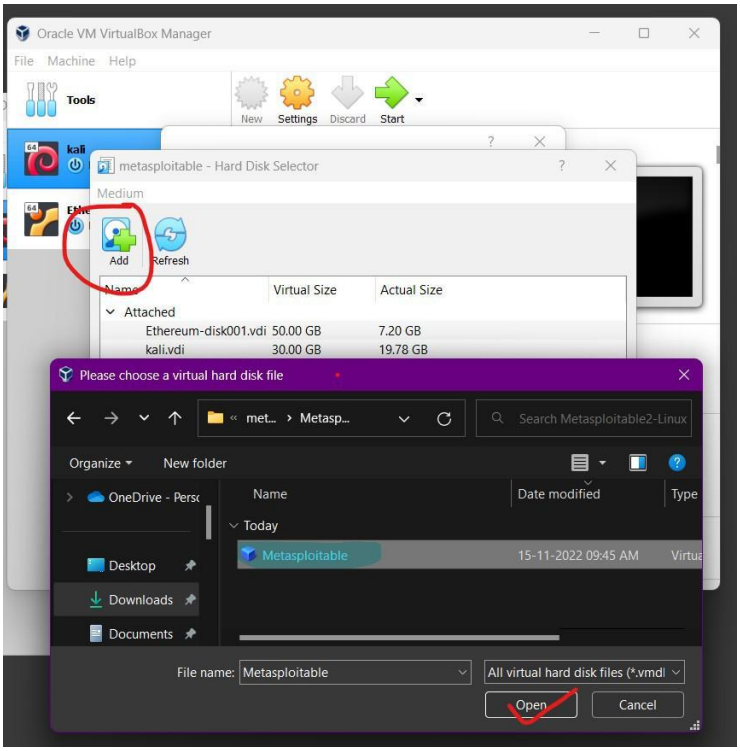
Remarque *: Puisque le fichier Metasploitable 2 n'est pas un fichier ISO, vous ne démarrez pas à partir d'un programme d'installation. Au lieu de cela, nous joindrons le fichier .vmdk existant comme disque dur virtuel, qui contient le système d'exploitation complet préinstallé.*



Étape 4 : Sélectionnez la RAM que vous souhaitez fournir à la machine virtuelle. recommandée (512 Mo).

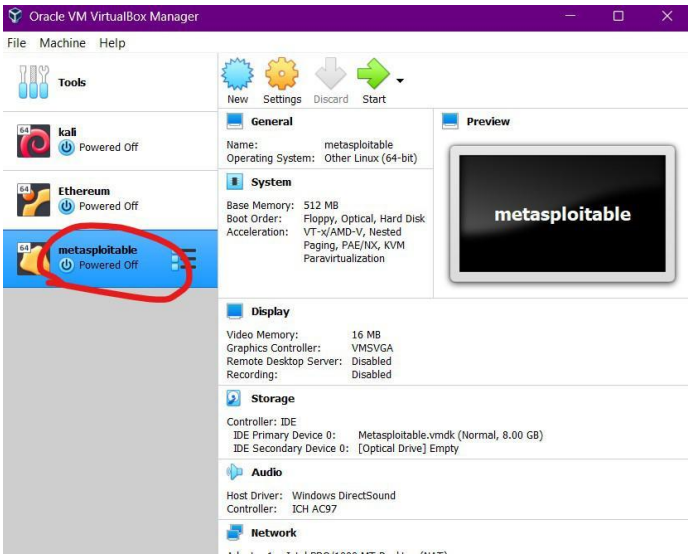


Étape 5 : Choisissez maintenant l'option d'utiliser un fichier de disque dur virtuel existant. Cliquez sur l'icône du dossier, puis parcourez et sélectionnez le fichier .vmdk extrait de l'archive ZIP Metasploitable 2. Cela montera directement le disque dur de la VM, aucune ISO n'est nécessaire.

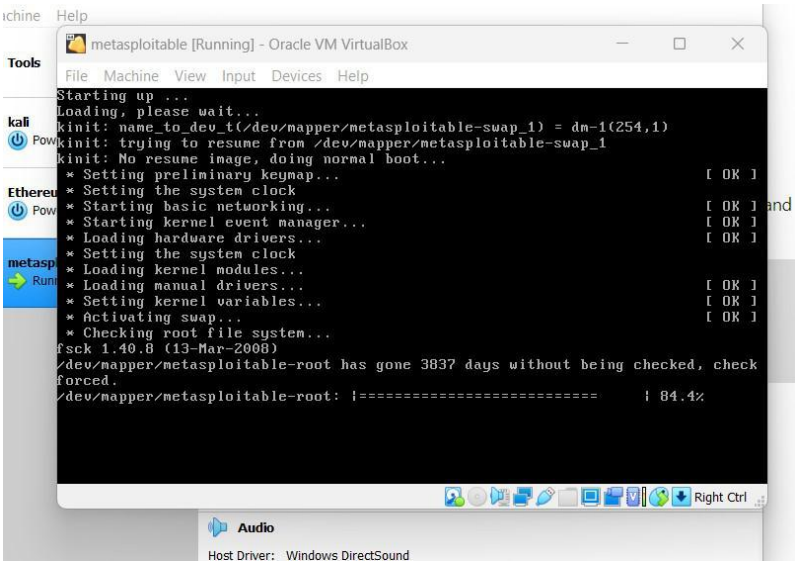


Localisez maintenant le fichier que nous avons extrait.

Étape 6 : Enregistrez maintenant le fichier et vous verrez que l'instance est créée avec le nom que vous avez donné.

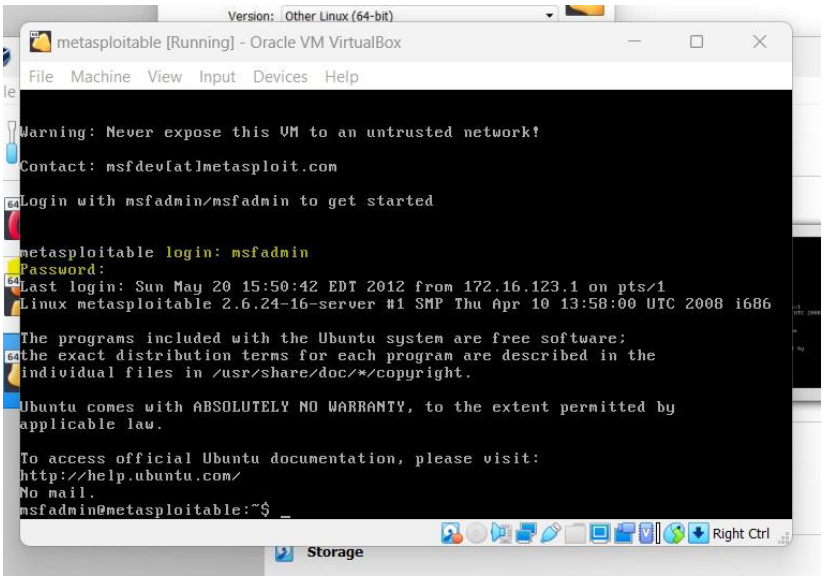


Nous sommes prêts à utiliser la machine, il suffit d'appuyer sur le bouton de démarrage en haut et d'attendre qu'elle démarre et charge l'instance.



Étape 7. Une fois l'instance chargée, on vous demandera de fournir un nom d'utilisateur et un mot de passe. Par défaut, les identifiants sont :

Connexion par défaut : **msfadmin**
Mot de passe par défaut : **msfadmin**

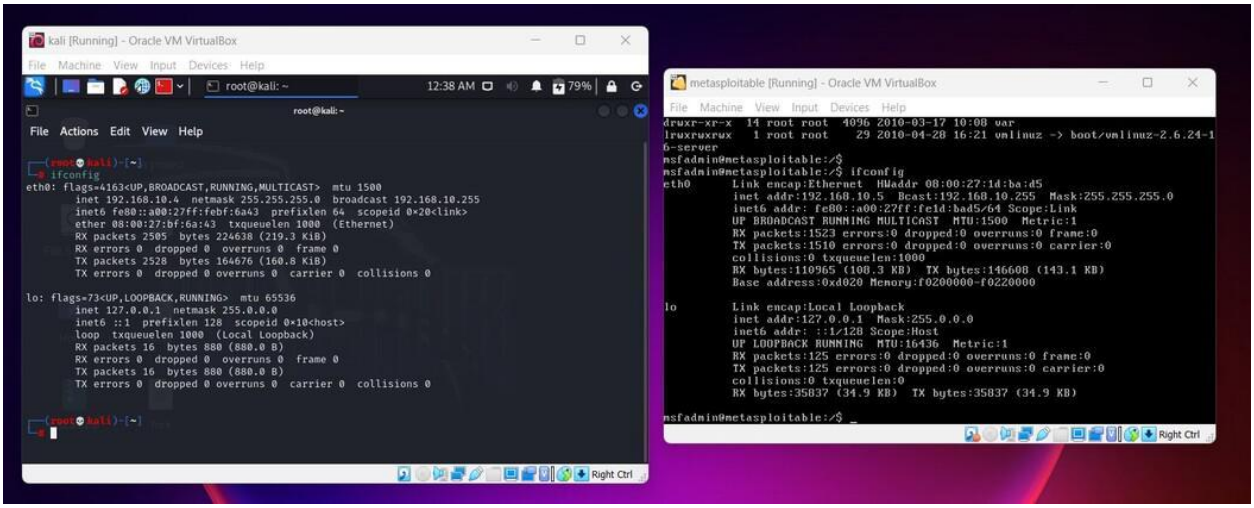


Une fois que vous vous êtes connecté avec les informations d'identification, vous serez dirigé vers la machine et nous aurons terminé le processus d'installation.

Démonstration des tests d'intrusion avec Metasploitable 2

Étape 1 : ouvrez vos deux machines Metasploitable 2 et Kali Linux côte à côte.

- Premièrement, nous devons exécuter les deux instances en même temps côte à côte afin de pouvoir voir clairement les changements. lancez Vbox et démarrez Linux et Metasploitable 2 côte à côte.



Étape 2 : vérifions les adresses IP des deux machines pour avoir une vue d'ensemble de la machine cible.

- ouvrons maintenant le terminal et vérifions l'adresse IP de Metasploitable 2 sur laquelle nous allons effectuer l'attaque. Utilisez la commande suivante :

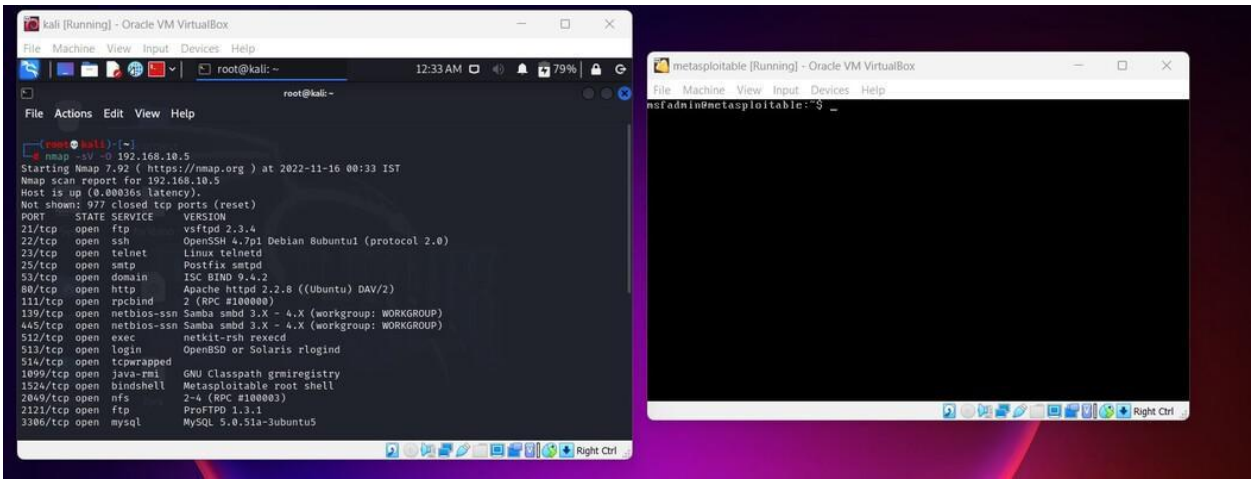
msfadmin@metasploitable :~$ ifconfig

- sur l'image ci-dessus, nous pouvons voir que nous avons une adresse IP, c'est-à-dire 192.168.10.5 de la machine cible.

Étape 3 : nous allons maintenant effectuer une analyse du réseau à l'aide de l'outil Nmap pour voir quels services fonctionnent sur la cible et lesquels sont loin de la cible.

- maintenant la première étape est de rechercher des boucles et des vulnérabilités afin que nous puissions exploiter la machine, pour ce faire nous utiliserons le scan Nmap sur un terminal Linux. Utilisez la commande :

root-user-#/ $ nmap -sV -O 192.168.10.5



dans la commande ci-dessus, -sV est utilisé pour obtenir les versions des services en cours d'exécution sur la machine cible et -O est utilisé pour détecter le système d'exploitation sur la machine cible.

- Maintenant que nous pouvons voir que nous avons tellement de façons d'exploiter et de vulnérabilités à effectuer, que nous utiliserons l'exploit vsftpd_234_backdoor pour l'exploitation et l'accès à la machine.
- ouvrez Metasploit Framework avec la commande :

Étape 4 : Maintenant que nous avons toutes les informations relatives à l'exploit que nous devons utiliser, c'est-à-dire vsftpd_backdoor nous pouvons maintenant utiliser Metasploit pour exploiter la machine et accéder à l'interpréteur de commandes, ce qui nous donnera éventuellement accès à la machine cible.

- démarrer le Metasploit Framework par la commande mentionnée ci-dessous :

root-user-#/ $ msfconsole

- après avoir suivi les commandes, nous allons choisir l'exploit qui est vsftpd_backdoor puis définir Rhost (IP ciblée).

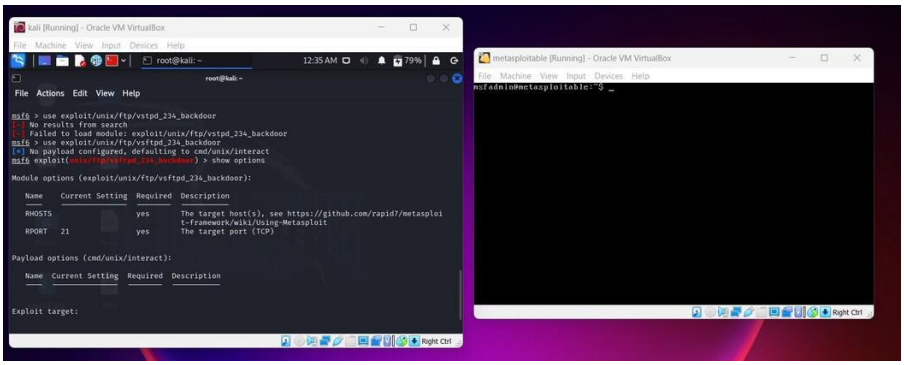
Étape 5 : Maintenant, tout ce que nous avons à faire est de déployer l'exploit dans la machine cible à l'aide de msfconsole, pour ce faire, nous devons suivre quelques étapes de base qui sont :

- Tout d'abord, sélectionnons l'exploit que nous allons utiliser dans ce cas il est vsftpd_backdoor, nous allons donc utiliser la commande suivante **:**

msf6~/ utiliser exploit/unix/ftp/vsftpd_234_backdoor

- Après avoir sélectionné l'exploit ci-dessus, configurons la cible sur laquelle nous déployons l'exploit.

msf6~/ (unix/ftp/vsftpd_234_backdoor) : afficher les options



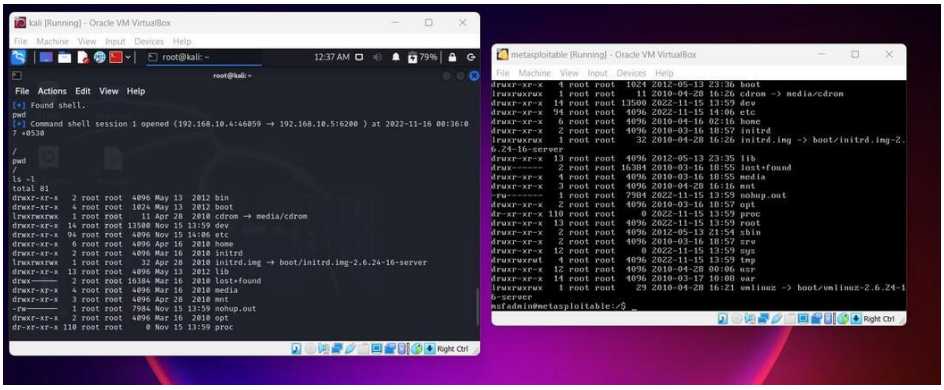
nous pouvons maintenant voir que nous avons la possibilité de définir RHOST qui est l'hôte récepteur. nous allons donc le définir sur l'adresse IP de la machine cible.

msf6~/ (unix/ftp/vsftpd_234_backdoor) : définir RHOST 192.168.10.5

Étape 6 : La dernière étape consiste à exécuter l'exploit, par commande exploit.

msf6~/ (unix/ftp/vsftpd_234_backdoor) : exploit

- après avoir défini RHOST, entrez simplement la commande exploit et vous verrez que le shell de commande de la machine cible est obtenu.



- Maintenant que nous avons réussi à pénétrer la cible en obtenant un obus, vous pouvez essayer des commandes et vérifier dans les deux machines en même temps.

Étape 7 : Vérifiez en utilisant certaines commandes de l'interpréteur de commandes comme imprimer le répertoire de travail ou les éléments ls dans un dossier.

pwd, ls -l, ls -a etc

- nous avons donc examiné avec succès comment Metasploitable est utile pour pratiquer les compétences de test d'intrusion.
- Nous pouvons voir que les deux côtés des fichiers sont les mêmes et que nous avons un accès root à la machine.

Conclusion :

Metasploitable 2 est une excellente machine pour s'entraîner et apprendre les tests d'intrusion et le piratage, bien qu'il comporte tellement de vulnérabilités et de failles que vous pouvez continuer à creuser et améliorer vos compétences en test d'intrusion. Actuellement, une autre version de Metasploitable est également disponible, vous pouvez également utiliser le processus de configuration et d'installation identique à celui ci-dessus.

Dans l'article ci-dessus, nous avons appris à installer la version 2 de Metasploitable avec succès et avons vu une démonstration d'exploitation avec l'exploit le plus célèbre et le plus basique qui soit vsftpd_backdoor, il y a beaucoup plus d'exploits et de techniques à apprendre et à pratiquer.

Commentaire

Comment installer Kali Linux dans VirtualBox?

Lectures similaires

-

Comment installer Metasploitable 2 dans VirtualBox

Discutons d'abord de ce qu'est Metasploitable, c'est un environnement de test très utile pour les débutants qui veulent pratiquer et tester leurs compétences en tests d'intrusion et leurs recherches en sécurité. C'est une machine cible qui est utilisée pour découvrir et pénétrer les vulnérabilités afin que l'utilisateur se fasse une idée

6 min de lecture

Comment installer Kali Linux dans VirtualBox?

Le double démarrage d'un ordinateur portable Windows avec Kali Linux augmente la vitesse et l'efficacité du système d'exploitation, mais nous ne pouvons pas basculer instantanément entre Windows et Kali Linux. Pour ce faire, nous devrons installer Kali Linux dans Virtual Box ou tout autre hyperviseur. Alors, qu'est-ce qu'un hyperviseur? Référez-vous à cet article Hyp

5 min de lecture

- **Comment installer VirtualBox sous Linux?**

Virtual Machine fait abstraction du matériel de nos ordinateurs personnels tels que le processeur, les lecteurs de disque, la mémoire, la carte réseau (carte d'interface réseau), etc., dans de nombreux environnements d'exécution différents selon nos besoins, ce qui nous donne le sentiment que chaque environnement d'exécution est un seul ordinateur. Par exemple, Virt

3 min de lecture

- **Comment installer CSI Linux dans VirtualBox?**

Et s'il existait un système d'exploitation polyvalent conçu spécialement pour les cyberenquêteurs, oui, vous avez bien lu et la réponse à cette question est, oui, il existe un tel système d'exploitation connu sous le nom de CSI Linux. Il s'agit d'un « parc thématique » à code source ouvert pour les passionnés de l'industrie de la cybersécurité. Il a une tonne de

3 min de lecture

- **Comment installer Kali Linux VirtualBox Image?**

Kali Linux est considéré comme la meilleure distribution Linux de test de perpétuation car il est livré avec tous les outils importants préinstallés. Si vous avez un système de rechange, vous pouvez y installer directement Kali, mais si vous prévoyez de l'utiliser dans un environnement virtuel, la meilleure et la plus sûre méthode serait d'utiliser

2 min de lecture

-

Comment installer Virtual Box dans Kali Linux

Nous avons tous vu que nous trouvons beaucoup de procédures d'installation sur la façon d'installer un boîtier virtuel sous Windows et d'exécuter kali Linux dessus. Mais dans ce guide d'installation, nous allons vous montrer comment installer Virtual Box dans le système d'exploitation Kali Linux. Commençons. Comment installer Virtual B

2 min de lecture

-

Comment relier Kali Linux à Metasploitable 2

Metasploitable 2 est un environnement de test d'intrusion intentionnellement vulnérable, qui est également utilisé pour la recherche en sécurité. Pour un environnement de test, l'utilisateur doit avoir une instance Metasploit qui peut accéder à une cible vulnérable, et ici la cible fonctionne sur notre réseau local qui est Metasploitable 2

4 min de lecture

-

Comment installer RHEL 8 sur VirtualBox?

Red Hat Enterprise Linux (RHEL) est un système d'exploitation Linux de Red Hat conçu pour les entreprises. RHEL peut fonctionner sur des ordinateurs de bureau, sur des serveurs, dans des hyperviseurs ou dans le nuage. Red Hat et son homologue soutenu par la communauté, Fedora, sont parmi les distributions Linux les plus utilisées au monde. Th

4 min de lecture

-

Comment installer Ubuntu Budgie dans Virtualbox?

Ubuntu Budgie est une distribution développée par la communauté, intégrant l'environnement de bureau Budgie avec Ubuntu en son cœur. Que vous l'utilisiez sur un vieil ordinateur ou un poste de travail puissant, Ubuntu Budgie s'adapte à n'importe quel appareil, ce qui les permet de rester rapides et utilisables. Il combine le test minutieux et le coup de poignard

4 min de lecture

-

Comment installer Virtualmin sous Linux

Dans cet article, nous allons apprendre à installer Virtualmin sur le système d'exploitation Linux. Virtualmin est basé sur Webmin, une interface utilisateur de gestion de serveur Web populaire pour Linux. Il s'agit d'un panneau de contrôle d'hébergement de domaine et de site Web qui permet la création et la gestion de plusieurs domaines et simplifie l'automatisation

3 min de lecture

GeeksforGeeks
Sanchhaya Education Private Limited

Adresse générale et des communications :

A-143, 7e étage, Sovereign Corporate Tower, secteur - 136, Noida, Uttar Pradesh (201305)

Adresse enregistrée :

K 061, Tour K, Appartement Gulshan Vivante, Secteur 137, Noida, Gautam Buddh Nagar, Uttar Pradesh, 201305