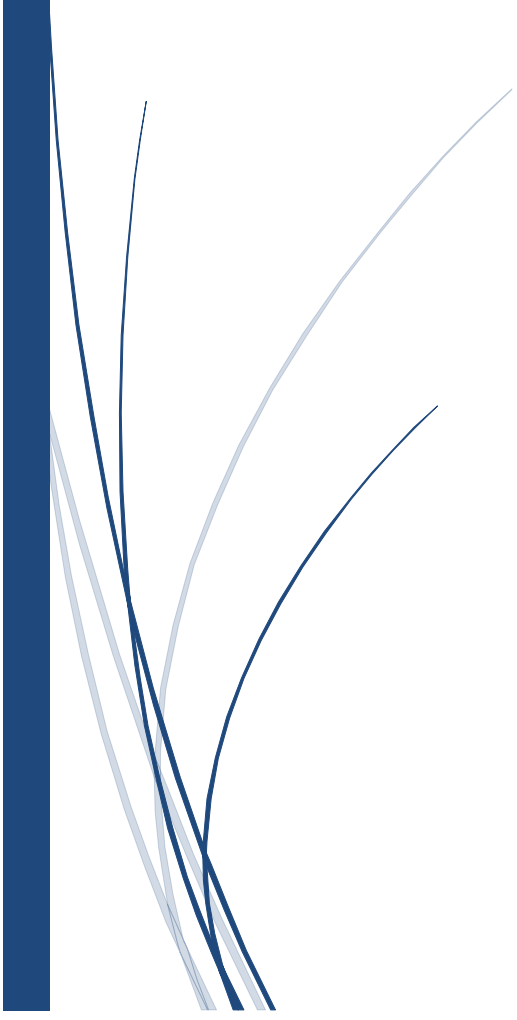
20/02/2026

Installation de Metasploitable 2 sur l'Hyperviseur Proxmox VE

Version 1.2



Sommaire

1.PRÉSENTATION ET CONTEXTE

Metasploitable 2 est une machine virtuelle Linux (basée sur Ubuntu 8.04) développée par Rapid7. Contrairement à une distribution classique, ce système est configuré avec de nombreuses vulnérabilités applicatives et réseaux. Ce laboratoire permet l'apprentissage de l'exploitation de failles, des tests d'intrusion et de la recherche de vulnérabilités dans un environnement contrôlé.

2. OBJECTIF TECHNIQUE

L'objectif est d'importer Metasploitable 2 dans un environnement Proxmox VE tout en assurant la compatibilité des pilotes matériels (drivers) et l'accessibilité réseau, afin de simuler une cible de pentesting réaliste.

3. SOMMAIRE

4. PRÉREQUIS ET ENVIRONNEMENT

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un serveur Proxmox VE fonctionnel (version 6, 7 ou 8).
- L'archive metasploitable-linux-2.0.0.zip téléchargée.
- Un accès SSH/Root sur l'hôte Proxmox.
- Espace disque disponible : minimum 2 Go sur le pool local-lvm.

5. PRÉPARATION ET TRANSFERT DU DISQUE VIRTUEL

Sur votre poste Windows, décompressez l'archive. Le fichier source est Metasploitable.vmdk. Transférez-le via la commande suivante :

<u>scp "C:\Users\ly\Downloads\metasploitable-linux-2.0.0\Metasploitable2-Linux\Metasploitable.vmdk" root@IP_PROXMOX:/root/</u>

6. CONVERSION ET IMPORTATION DES DONNÉES

Une fois sur le Shell Proxmox, il est nécessaire de convertir le format disque pour une meilleure gestion des snapshots et des performances :

<u>cd /root</u> <u>qemu-img convert -O qcow2 Metasploitable.vmdk metasploitable.qcow2</u>

Importez ensuite ce disque dans la VM 111 (identifiant utilisé dans cet exemple) :
<u>qm importdisk 111 /root/metasploitable.qcow2 local-lvm</u>

7. CONFIGURATION MATÉRIELLE DE LA VM

Pour que le système démarre sans erreur, les réglages suivants doivent être appliqués dans l'interface Proxmox :

- Processeur : 1 vCPU (Type default).
- Mémoire : 1024 Mo de RAM.
- Réseau : Pont (Bridge) vmbr0 avec le modèle **Intel E1000** (Indispensable : le driver VirtIO n'est pas supporté par ce vieux noyau).
- Stockage : Allez dans Hardware > Unused Disk > Edit. Choisissez impérativement le bus **IDE 0**.

8. PARAMÉTRAGE DU DÉMARRAGE ET NETTOYAGE

Dans l'onglet Options de la VM, réglez l'ordre de boot pour que IDE 0 soit prioritaire. Une fois la configuration validée, nettoyez les fichiers temporaires sur l'hôte Proxmox pour éviter la saturation du disque :
<u>rm /root/Metasploitable.vmdk /root/metasploitable.qcow2</u>

9. TESTS DE CONNECTIVITÉ ET ACCÈS ROOT

Démarrez la console et connectez-vous avec les identifiants par défaut :

- Utilisateur : *msfadmin*
- Mot de passe : *msfadmin*

Pour obtenir les privilèges d'administrateur complet (Root) : <u>sudo -s</u>
Vérifiez que la machine a bien reçu une adresse IP pour vos tests : <u>ip addr show eth0</u>

10. DÉPANNAGE (TROUBLESHOOTING)

- Le clavier est en anglais (QWERTY) par défaut.
- Si le réseau ne fonctionne pas, vérifiez que le modèle de carte réseau est bien Intel E1000 et non VirtIO.
- Si le disque n'est pas trouvé au boot, vérifiez qu'il est bien configuré en IDE et non en SCSI/VirtIO Block.

CONCLUSION

Le déploiement est réussi. Metasploitable 2 est désormais prêt à être scanné et exploité. Ce laboratoire est une base solide pour toute formation en sécurité offensive.
RECOMMANDATIONS DE SÉCURITÉ Il est strictement rappelé que ce système est une faille de sécurité majeure par définition. Il ne doit jamais posséder d'adresse IP publique ni être accessible depuis l'extérieur de votre réseau local de test.