**Exercice 1 :**

1. Télécharger la VM Metasploitable (*<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>*).

Lancer cette machine. De toute évidence, vous n’avez pas les accès root pour cette machine. L’objectif est de trouver une vulnérabilité qui nous permet d’avoir le droit root sans pour autant connaitre le mot de passe root !

Vous pouvez aussi télécharger une VM Kali Linux pour éviter d’installer les outils nécessaires pour terminer cet exercice.

1. En toute logique, vous n’allez pas scanner les quatre milliards d’adresse IP possibles pour trouver la bonne adresse IP de votre VM car ceci n’est ni performant ni légal.

Nous n’avons pas le droit de scanner toutes les adresses IP, car cela prendrait trop de temps et demanderais trop de ressources, mais aussi pour des raisons légales.

Comment faire alors pour trouver le bon préfixe réseau à scanner ?

Pour trouver le bon préfixe, hostenvly sur Virtualbox

Donner un nom à cette étape.

Étape de **reconnaissance**

1. Une fois le bon préfixe trouvé, utiliser un outil de scan réseau pour identifier l’adresse IP de votre VM.

Quel est le type de scan utilisé ?

Nmap

Comment rendre le scan plus furtif ?

Command : nmap -pl-65535 192.168.56.0/24 🡪 scan tous les ports

Command : nmap -pl-65535 192.168.56.232 🡪 scan que la machine 232

Command : nmap -T0 -sS 192.168.56.232 🡪 -T0 : ralentir, -sS : technique de scan TCP SYN

1. Quels sont les services lancés sur cette machine ?

nmap -s 192.168.56.232 🡪 -s : afficher les services

quels sont les versions exactes des services lancés ?

nmap -sV 192.168.56.232 🡪 -sV obtenir la version, -O : connaitre l’OS

qu’appelle-t-on cette étape ?

L’énumération des services

D’après vous, comment fonctionne concrètement cette découverte ?

1. Chercher sur google une vulnérabilité sur le serveur FTP présent sur cette machine. Quelle est le type de cette vulnérabilité ?

Exploiter cette vulnérabilité afin d’avoir un accès root à la VM.

Là je me débrouille.

1. Google est bien pour hacker, mais il y a mieux : les outils d’analyse de vulnérabilité. Installer un outil d’analyse de vulnérabilité de votre choix, ou utiliser simplement les outils sur Kali. Lancer une analyse sur votre VM.

Donner deux autres vulnérabilités qui vous permettent d’avoir un accès distant à votre VM.

1. Exploiter une vulnérabilité peut être délicat. Heureusement il y a l’outil Metasploit. Cet outil permet d’automatiser l’exploitation des vulnérabilités.

Chercher dans Metasploit un *exploit* d’une des vulnérabilités que vous avez trouvées sur la VM metasploitable (une vulnérabilité sur Bash ou SSL par exemple), puis lancer automatiquement cet exploit.