**TD Pentest 2 – Recherche de vulnérabilités**

Les manipulations de ce TD concernent la phase de RECHERCHE DE VULNERABILITES. L’objectif est de récupérer des informations en libre accès (OSINT) sur le réseau cible. Nous utilisons la distribution **Kali Linux** qui dispose déjà de tous les outils nécessaires.

Rappel :

➔ Identifiants par défaut de Kali Linux : **kali** / **kali (kqli / kqli** tant que vous avez un clavier anglais …**)**

➔ Pour mettre le clavier en français : **Menu : Settings / Keyboard / Layout**

➔ **Configurez le serveur DNS de la Kali en 10.2.12.4 dans */etc/resolv.conf***

# Quelques outils de scan

## netdiscover

« netdiscover » exploite le protocole ARP. Il est capable de fonctionner en mode passif sur un réseau (simplement écouter les requêtes ARP qui circulent) ou en mode actif (il émet des requêtes ARP sur les plages ip qu’on lui demande de scanner). Bien évidemment, en mode passif il est totalement indécelable, ce qui n’est pas le cas en mode actif.

Un gros avantage de netdiscover est qu’il ne nécessite pas une configuration IP pour pourvoir jouer son rôle.

* + 1. Essayez la commande suivante : **netdiscover -i <interface> -p**

Attendez quelques instants puis arrêtez le programme avec Ctrl+c

* + 1. Essayez maintenant la commande suivante : **netdiscover -i <interface>**
    2. Enfin essayez la commande : **netdiscover -i <interface> -r 10.2.18.0/24**

Avec: **netdiscover -i <interface> -r 10.2.18.0/24 -P > fichier**

vous pouvez même conserver les résultats dans un fichier pour traitement ultérieur. Faites-le … ça va vous servir bientôt !

* + 1. Jetez un coup d’œil sur le « man netdiscover » afin de comprendre à quoi servent toutes ces options

## nmap

« nmap » est probablement le plus célèbre et le plus complet des outils de découverte de réseaux. Sa syntaxe globale est de la forme : nmap <type de scan> <options> <cibles>

Les possibilités de cet outil sont infinies et un document synthétique de type « cheat-sheet » est très utile. Vous en trouverez une dans cette longue liste : <https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/>

Pour les manipulations à suivre, lancez un wireshark sur l’interface de votre kali.

Pour mieux y voir, activez le filtre d’affichage suivante :

**eth.addr==<adresse mac kali> || ip.addr==<adresse ip kali>**

* + 1. Cette commande est l’équivalente de la précédente avec netdiscover, même si le rendu à l’écran n’est pas le même. Testez la :  
       **nmap -sn 10.2.18.0/24**Que fait l’option -sn ? Comment procède nmap ?
    2. Refaites la même manipulation, mais en changeant de réseau avec la commande suivante :  
       **nmap -sn 10.2.12.0/24**Comment procède nmap ? Pourquoi procède-t-il différemment ?
    3. Mettez-en formez le fichier obtenu précédemment avec la commande netdiscover :  
       **cat <votre fichier> | cut -d ' ' -f2 | grep ^[1-9] > ip-list**  
       Regardez le résultat obtenu dans le fichier « ip-list ».  
       avec un « man cut », essayez au passage de comprendre ce qu’a fait la commande ;-)
    4. Testez la commande suivante:  
       **nmap -sL -iL ip-list**Expliquez ces options (même si elles ne sont pas sur la cheatsheet !)  
       Quel est l’intérêt de cette commande ?
    5. Testez la commande :  
       **nmap -sS -iL ip-list**Expliquez ces options   
       Quel est l’intérêt de cette commande ?
    6. Testez cette commande :  
       **nmap -sU -iL ip-list**  
       Vous allez probablement devoir arrêter avec un Ctrl+C avant qu’elle ne finisse … mais seul wireshark pourra vous expliquer véritablement pourquoi …  
       Expliquez ces options  
       Quel est l’intérêt de cette commande ?
    7. Testez cette commande :  
       **nmap -sU -F -iL ip-list**  
       Expliquez cette nouvelle option
    8. Enfin, testez cette dernière commande :  
       **nmap -sSV -iL ip-list**Expliquez ces options  
       Quel est l’intérêt de cette commande ?

II est illusoire de prétendre de pouvoir faire le tour de toutes les possibilités de cette commande en un seul TP, mais cela vous donne au moins un avant-goût de ce qu’elle est capable de faire.

Cela dit, il existe d’autres logiciels (« metasploit », …) qui ont des fonctionnalités totalement similaires, parfois même qui invoquent nmap eux-mêmes pour réaliser ces fonctionnalités !

## snmp-check

La commande « snmp-check » permet d’obtenir des informations sur le serveur SNMP (Simple Network Management Protocol). Si vous en avez découvert un lors de la phase précédente, on va en profiter !

* + 1. Ouvrez un terminal et regardez le « man » de « snmp-check … »
    2. Faites une requête sur le serveur que vous avez trouvé. Quelles informations avez-vous obtenues ?
    3. Affichez les informations données par SNMP avec :  
       **snmpwalk -v1 -c <community> <IP du serveur>**Quelles informations intéressantes avez-vous obtenues ?