PENTEST

TP ENUMERATION

Introduction :

Le principe d'énumération consiste à sonder un environnement pour y obtenir plusieurs informations :

- Présence de machines dans le réseau
- Plan et segmentation réseau (découverte du réseau)
- Souvent assimilé au scanning, il consiste également à rechercher et lister les protocoles présents

Les différentes techniques d'énumération permettent de se renseigner sur les éléments suivants :

- Les hôtes connectés, leur adresse IP, leurs ports ouverts
- Les systèmes d'exploitation et l'architecture des systèmes
- Les services actifs et éventuellement leur version
- Des applications
- Des vulnérabilités potentielles…

Vérifier les adresses IP de vos 2 machines (voir celle de l'hôte Windows pour réaliser ce TP).
Notez l'adresse de vos machines, l'adresse du réseau, le masque, la passerelle, le broadcast…

Debian

VBox carte réseau par pont. Dans Debian configurer la carte réseau en adresse ip fixe. Vérifier votre @ ip : ip a puis faire un apt update && upgrade.

Ensuite vous devrez installer les logiciels d'énumération avec APT
apt-get install netdiscover apt-get install nmap etc

Kali

Créer une VM Kali , attribuer 12 Go de disque option Taille Dynamique, 4096 de RAM.

1. Récupérez le fichier **iso** de Kali Linux **http://cdimage.kali.org/**
   Régler le démarrage dans le fichier .iso, installer Kali
   Laisser la carte réseau en NAT, vous la basculerez par Pont au prochain démarrage
2. Lancer la VM Kali
3. Utilisateur : btssio mot de passe : btssio32 (root) … n'oubliez pas le Grub
4. apt update && upgrade
5. Vérifier votre @ ip : ip a
6. Aller dans la configuration des cartes réseau pour définir un adresse ip fixe. Ne restez pas en DHCP pour les Pentest. Reprenez celle que le service DHCP de votre Box vous a distribué.
7. Les programmes de Cybersécurité sont présents dans Kali: « Wireshark », NMAP, etc

OBJECTIF DU PENTEST

L'objectif est de se mettre en situation de PENTEST qui commence par une énumération (une découverte) des services réseau présents sur un périmètre d'attaque : machines, plan et segmentation des réseaux et sous-réseaux, lister les protocoles présents….

Vous allez donc procéder à l'énumération du réseau de votre choix (à la Maison) à travers l'usage de différents outils.

Rédigez un compte rendu d'activité

Découverte du voisinage réseau :

- **Netdiscover** : utiliser cette instruction pour découvrir le réseau local dans lequel est votre machine.

  - netdiscover permet d'énumérer un réseau local en broadcastant des requêtes ARP sur plusieurs segments réseaux
  - Utiliser le Terminal, tapez #**`netdiscover -r 192.168.1.0/24`**
    si toutefois votre réseau est en 192.168.1.0, cela peut varié en fonction des FAI
  - Il permet également de vérifier la qualité de la segmentation réseau notamment si un vrai contrôle par VLAN existe
  - En parallèle ouvrir « Wireshark » pour contrôler le déroulement des requêtes réseau (screenshot)
  - Questions
    - Quelle est le protocole utilisé ?
      - ♣ *Screenshot du résultat de NetDiscover*
    - Cibler votre instruction avec l'IP de la VM Kali

  ** il existe une variante de Netdiscover :

  p0f permet la reconnaissance passive du réseau (sans scan) sur les connexions reçues (OS, protocole, charge de la trame, etc.)

  Très pratique pour éviter d'être repéré par une sonde IDS ou détecter si une découverte de réseau par un équipement de sécurité est présente

  - Toujours dans le terminal tapez : **`p0f -i eth0 -p`**
    - ♣ *Screenshot du résultat de p0f*

- **Nmap** : permet une énumération complète du périmètre

  Il est capable d'identifier aussi bien les hôtes sur le réseau, que les ports ouverts, les versions ou les configurations de services...

Découverte des hôtes sur le réseau

L'option -sP permet d'identifier les hôtes répondant à l'ARP :

- Utiliser le sur le réseau local de votre Box
  - *Résultats avec sreenshot + Wireshark*
- Terminal tapez : nmap -sP 192.168.1.0/24
- Quel constat / remarque faites-vous ?

Cet outil offre des tas d'options pour être plus précis dans son énumération

- Trouvez l'option qui permet d'identifier les hôtes répondant à l'ARP/
  - *Résultats avec sreenshot + Wireshark*
- Trouvez l'option qui -couplé à la précédente permet d'effectuer un scan ICMP pour vérifier qu'un hôte répond au ping.

Vous trouverez plus d'informations sur https://nmap.org/man/fr/man-host-discovery.html

Découverte des ports ouverts sur une machine

- Découvrez les ports ouverts en ciblant votre instruction avec l'IP de la VM Kali

  nmap ipdelamachine
  - *Résultats avec sreenshot + Wireshark*
  - Que constatez-vous ? => réponse :

Vous trouverez plus d'informations sur https://nmap.org/man/fr/man-version-detection.html

- Trouvez les options maintenant qui permettent de lister les versions de services et d'OS via « banner grabbing »
  - *Résultats avec sreenshot + Wireshark*

Options : our un scan approfondi identifiant les versions de services et d'OS via banner grabbing, les options -sV --version-all et -O --osscan-guess permettent une énumération plus complète : nmap -sV –version-all -O –osscan-guess ipdelamachinecible

- Sur quel niveau de la couche OSI s'effectue le « banner grabbing » ?

Découvertes des ports et configurations

L'option --script permet d'exécuter des scripts de reconnaissance sur les services qui seront énumérés.

Plusieurs appels sont possibles :

- -sC : permet d'appeler les scripts concernant le port ouvert automatiquement
- --script ssh* : permet d'appeler les scripts SSH uniquement
- --script msrpc-enum : permet d'appeler le script msrpc-enum

- **Application** : saisissez l'instruction sur le service FTP de la machine cible

  ♣ *Résultats avec sreenshot + Wireshark*

  `nmap -p 21 --script ftp-anon ipdelamachinecible`

Il est également possible d'utiliser les catégories de script pour automatiser les tests ; les catégories **basiques** sont :

1. _____
2. _
3. _

A toi de les trouver avec ses ressources !! :

https://nmap.org/book/nse-usage.html + https://nmap.org/nsedoc/categories/default.html

- Utilise maintenant Nmap avec le script par default sur une cible (rappel VM Kali)

Plus d'informations sur Nmap :

https://nmap.org/man/fr/man-nse.html
https://nmap.org/book/nse.html
https://nmap.org/nsedoc/categories/default.html

Outils d'énumération SMB

SMBMap permet une énumération des partages sur une cible. L'outil supporte le mode anonyme, les identifiants de connexion, les techniques de pivoting (pass the hash) et les protocoles d'authentification (ntlm, kerberos...).

Il est possible de faire de l'énumération SMB avec Nmap également : partage/utilisateur/ configuration et version du protocole : nmap –script smb* -p 139-445 <IP>

SMBMap

- Utiliser le sur la cible : smbmap -H <IP> *en mode anonyme*
  - ♣ *Screenshot résultat*
- Utiliser le sur la cible : smbmap -H <IP> -u <user> -p <password> *en mode authentifié*
  - ♣ *Screenshot résultat*
- L'option **`R`** permet de lister le contenu d'un partage …essayez le !
  - ♣ Screenshot résultat
- L'option **`--download`** permet de télécharger un fichier en spécifiant son chemin testez le : smbmap -H <IP> --download /…/…/fichier
  - ♣ *Screenshot résultat*
- L'option **`-F`** permet de rechercher un mot clé contenu dans un fichier en mode récursif (fonctionne uniquement sur les cibles Windows)
  - ♣ Testez le en changeant de cible sur une machine Windows
  - ♣ Smbmap -H <IP> -R /chemin/du/fichier -F 'motcherché'

Outils d'énumération RPC

Enum4linux : enum4linux est un outil assez complet d'énumération. Il s'appuie sur le protocole RPC, NetBIOS et SMB pour énumérer les utilisateurs et sessions distantes, les groupes et politiques du système et les informations sur l'OS.

- L'option -**`U`** permet de lister uniquement les utilisateurs du système distant :
  - ♣ *Screenshot résultat*
- Pour une énumération complète utiliser l'option **`-a`** :
  - ♣ *Screenshot résultat*
- Il est également possible de spécifier un compte utilisateur à utiliser avec -u et -p
  - ♣ Exemple : enum4linux -a <IP> -u >user> -p <motdepasse>
  - ♣ *Screenshot résultat*

rpcclient : rpcclient permet l'administration d'un serveur distant via RPC. Une fois connecté, de nombreuses options d'administration s'offrent à vous.

Il est possible de se connecter en mode anonyme. Pour obtenir les options d'administration possibles, une fois connecté utilisez **`help`**.

- Utiliser l'option -U : rpcclient -U '"" -N

♣ *Screenshot résultat*

Attention si vous le testez sur un poste/server avec authentification, penser à spécifier le nom de l'utilisateur et retirer l'option -N ….il vous faudra ensuite saisir le mot de passe.

- Essayez une ou plusieurs instructions de rpcclient pour tester les informations retournées

♣ *Screenshot résultat*

SI vous avez terminé le TP avant les 2 heures, testez quelques-unes de ces commandes sur d'autre cibles.