Département Génie Informatique (DGI) | Ecole Supérieure Polytechnique (ESP) |
UCAD|Technologies de Sécurité
© Doudou FALL
2023 – 2024

—

Atelier 3 : Scanner avec nmap

Pour cet atelier, nous allons scanner la VM Metasploitable2 en utilisant nmap.

Partie 1 - Configuration

Lancez à la fois Kali Linux et la VM Metasploitable2 et assurez-vous qu'elles sont sur le même
réseau isolé.
Vérifiez la version de nmap que vous avez installée. Les commandes nmap ont légèrement évolué
au fil du temps. Il est important de s'assurer que vous suivez la documentation de la version du
programme que vous utilisez.
Obtenir les adresses IP des machines virtuelles :
Ouvrez un terminal sur Kali Linux.
Utilisez la commande ifconfig pour afficher les informations sur les interfaces réseau.
l'adresse IP de Kali Linux est **192.168.1.10**

Vérifier la version de Nmap :
Toujours dans le terminal de Kali Linux, exécutez la commande suivante pour vérifier la version de Nmap installée : **nmap --version**

Voici la sortie:

Nmap version 7.91 (https://nmap.org)

Partie 2 - Découverte des hôtes

• Quelles sont les méthodes utilisées par nmap pour effectuer la découverte
des hôtes lorsqu'il est exécuté en tant qu'utilisateur root (c'est-à-dire via sudo) ?

Lorsque Nmap est exécuté en tant qu'utilisateur root (via sudo), différentes méthodes peuvent être utilisées pour effectuer la découverte des hôtes. Ces méthodes dépendent de la configuration spécifique de l'environnement réseau et des privilèges accordés à l'utilisateur. Voici quelques-unes des méthodes couramment utilisées par Nmap lorsqu'il est exécuté en tant qu'utilisateur root :

Requêtes ARP :
Lorsque Nmap est exécuté en tant qu'utilisateur root sur un réseau local Ethernet, il envoie des requêtes ARP pour découvrir les hôtes actifs sur le réseau. Les requêtes ARP sont des messages diffusés sur le réseau local pour interroger les périphériques connectés et obtenir leur adresse MAC.

Requêtes ICMP echo (Ping) :
Nmap peut également envoyer des requêtes ICMP echo (ping) pour découvrir les hôtes actifs. Cela consiste à envoyer des paquets ICMP echo request (ping) aux différentes adresses IP de la plage spécifiée et à écouter les réponses ICMP echo reply des hôtes actifs.
Requêtes TCP SYN vers des ports spécifiques :
Outre les requêtes ARP et ICMP echo, Nmap peut envoyer des paquets TCP SYN vers des ports spécifiques (par exemple, les ports 80 et 443) pour déterminer si les hôtes répondent aux connexions TCP. Cela peut être utilisé pour découvrir les hôtes actifs qui écoutent sur des ports spécifiques.
Requêtes ICMP timestamp :
Enfin, Nmap peut également envoyer des requêtes ICMP timestamp pour découvrir les hôtes actifs. Les réponses ICMP timestamp peuvent être utilisées pour estimer la distance et le temps de réponse entre l'hôte cible et l'émetteur.
Ces méthodes de découverte des hôtes sont souvent utilisées en conjonction les unes avec les autres pour obtenir une vue complète des hôtes actifs sur un réseau. L'utilisation de privilèges root permet à Nmap d'accéder à des méthodes plus avancées de découverte des hôtes, telles que les requêtes ARP, qui ne sont pas disponibles pour les utilisateurs non privilégiés

Pour exécuter le scan de découverte d'hôte sur l'adresse IP 8.8.8.8 en tant qu'utilisateur root avec Nmap, vous pouvez utiliser la commande suivante :
sudo nmap -sn 8.8.8.8
Cette commande envoie des requêtes de découverte d'hôte à l'adresse IP spécifiée (8.8.8.8) sans scanner de ports.

Voici les méthodes que Nmap utilise pour effectuer la découverte des hôtes lorsqu'il est exécuté en tant qu'utilisateur root :

Requêtes ARP :
Si Nmap est exécuté sur un réseau local Ethernet en tant qu'utilisateur root, il envoie des requêtes ARP pour découvrir les hôtes actifs sur le réseau. Les requêtes ARP sont des messages diffusés sur le réseau local pour interroger les périphériques connectés et obtenir leur adresse MAC.
Requêtes ICMP echo (Ping) :
Nmap peut également envoyer des requêtes ICMP echo (ping) pour découvrir les hôtes actifs. Cela implique l'envoi de paquets ICMP echo request (ping) aux adresses IP spécifiées et l'attente des réponses ICMP echo reply des hôtes actifs.
Requêtes DNS inverse :
Pour obtenir le nom d'hôte associé à une adresse IP, Nmap peut envoyer des requêtes DNS inverse. Cela implique la création d'une requête DNS inverse pour l'adresse IP spécifiée et la réception de la réponse contenant le nom d'hôte associé.

Après avoir exécuté le scan, vous pouvez analyser le fichier .pcapng enregistré avec Wireshark pour obtenir plus de détails sur les réponses reçues. Vous devriez être en mesure de trouver le nom d'hôte associé à l'adresse IP 8.8.8.8 dans les résultats de la requête DNS inverse. Ensuite, en utilisant ce nom d'hôte, vous pouvez confirmer sa validité en le saisissant dans votre navigateur web pour vérifier s'il correspond effectivement au serveur DNS public de Google.

Partie 3 – Scan des ports TCP

Pour effectuer un scan des ports TCP sur la VM Metasploitable2 avec Nmap, vous pouvez utiliser les commandes suivantes :

Pour un scan de connexion (-sT) :
sudo nmap -sT [adresse_IP_Metasploitable2]

Pour un scan SYN (-sS) :
sudo nmap -sS [adresse_IP_Metasploitable2]

Assurez-vous de remplacer [adresse_IP_Metasploitable2] par l'adresse IP réelle de votre VM Metasploitable2.

Une fois que vous avez exécuté l'une de ces commandes, Nmap analysera les ports TCP de la VM Metasploitable2 pour détecter les services actifs.

Après avoir terminé l'analyse, Nmap affichera un tableau indiquant les ports ouverts, leur état (ouvert, fermé ou filtré) et les services correspondants. Voici un exemple de tableau que vous pourriez obtenir :

bash
Copy code
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp closed telnet
80/tcp open http
Pour répondre aux livrables :

Les ports ouverts seront répertoriés dans la colonne "PORT | STATE | SERVICE".
Comptez le nombre total de ports ouverts pour déterminer le nombre de ports ouverts selon Nmap.
Comptez le nombre total de ports fermés (ou non ouverts) pour déterminer le nombre de ports fermés selon Nmap.
Une fois que vous avez terminé l'analyse, vous pouvez copier et coller le tableau PORT | STATE | SERVICE dans votre rapport pour répondre à la première partie du livrable. Ensuite, comptez simplement le nombre de ports ouverts et fermés pour répondre aux autres parties du livrable.