Atelier 4 : 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.

```
$ nmap --version
```

Livrables :

- Quelle est l'adresse IP de votre VM Kali Linux ? Quelle est l'adresse IP de votre VM Metasploitable2 ?
- Quelle version de nmap avez-vous installée dans Kali (réponse sous la forme : x.xx) ?

Attention : si les deux systèmes ont la même adresse IP et que vous utilisez VirtualBox, il est probable que vous n'avez pas complété la partie « Configuration de la mise en réseau » du TP « configuration de la machine virtuelle ».

Partie 2 - Découverte des hôtes

Effectuez un scan de découverte d'hôtes avec `nmap` sans scan de port. Normalement, ceci devrait être utilisé pour scanner un **sous-réseau entier (ou plus grand)**, mais pour ce TP, nous allons cibler des IP spécifiques.

Tout d'abord, ciblez uniquement la VM Metasploitable2 à travers son adresse IP.

```
$ sudo nmap -sn CIBLE
```

Remarque : utiliser sudo pour que `nmap` puisse générer des paquets réseau arbitraires pour ce scan.

Selon la documentation de `nmap` : la découverte de l'hôte par défaut effectuée avec `-sn` consiste en une requête ICMP echo, TCP SYN vers le port 443, TCP ACK vers le port 80, et une requête ICMP timestamp par défaut. Lorsqu'elle est exécutée par un utilisateur non privilégié, seuls les paquets SYN sont envoyés (à l'aide d'un appel de connexion) aux ports 80 et 443 sur la cible.

Lorsqu'un utilisateur privilégié tente d'analyser des cibles sur un réseau ethernet local, des requêtes ARP sont utilisées, sauf si `--send-ip` a été spécifié. – https://nmap.org/book/man-host-discovery.html

Livrables :

- 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) ?

Pour documenter votre réponse, exécutez Wireshark en arrière-plan et capturez uniquement le scan réseau de nmap avec l'option -sn, sans trafic réseau supplémentaire (ou avec un minimum). Enregistrez et téléchargez le fichier `.pcapng` résultant.

Ensuite, ciblez l'adresse IP `8.8.8.8`, qui correspond au serveur DNS public de Google (une fonction connue sous le nom de « IP Anycast »). Comme précédemment, faites simplement un scan de découverte d'hôte avec nmap sans scan de port.

Livrables :

- Quelle commande avez-vous saisie pour exécuter le scan en tant qu'utilisateur root ?
- Quelles méthodes `nmap` utilise-t-il pour effectuer la découverte des hôtes lorsqu'il est exécuté en tant qu'utilisateur root ?

Pour documenter votre réponse, exécutez Wireshark en arrière-plan et capturez uniquement le scan réseau de `nmap` avec l'option -sn, sans trafic réseau supplémentaire (ou avec un minimum). Enregistrez et téléchargez le fichier `.pcapng` obtenu.

- Quel est le nom de l'hôte qui répond à la requête DNS inverse envoyée par nmap pour `8.8.8.8.in-addr.arpa` ? Vous pouvez obtenir cette information à partir de la trace Wireshark que vous venez d'obtenir.

(Astuce : vous pouvez taper ce nom d'hôte dans votre navigateur web et voir une page web qui devrait immédiatement confirmer l'exactitude de votre réponse).

- Dans un court paragraphe, expliquez quelles réponses sont reçues suite à la découverte de l'hôte par nmap. Formulez votre réponse dans le format

suivant : nmap a envoyé `<message de demande>`, et quelques paquets plus tard, l'hôte cible a envoyé `<message de réponse>`.

Partie 3 – Scan des ports TCP

Effectuez un scan des ports TCP avec nmap sur la VM Metasploitable2 pour détecter les services actifs. Un scan de connexion (`-sT`) ou un scan SYN (`-sS`) est suffisant.

```
$ sudo nmap -sT CIBLE
$ sudo nmap -sS CIBLE
```

Remarque : utiliser sudo pour que nmap puisse générer des paquets réseau arbitraires pour ce scan.

Livrables :

- Quels sont les ports et services spécifiques que nmap trouve ouverts ? Copiez et collez le tableau `PORT | STATE | SERVICE` dans son intégralité.
- Combien de ports sont ouverts selon nmap ?
- Combien de ports sont fermés selon nmap ?

Partie 4 – Scan des ports UDP

Effectuer un scan des ports UDP avec nmap sur la VM Metasploitable2 pour détecter les services actifs.

```
$ sudo nmap -sU CIBLE
```

Remarque : utiliser sudo pour que nmap puisse générer des paquets réseau arbitraires pour ce scan.

Conseil 1 : contrairement à TCP, il n'y a pas de moyen générique de voir si un port UDP est ouvert ou non, puisque UDP est sans connexion. Ainsi, vous obtiendrez des résultats beaucoup plus précis (et serez en mesure de répondre à la question du TP) si vous activez également le scan de service et de version avec votre scan UDP.

Conseil 2 : si vous acceptez les options par défaut, ce scan prendra beaucoup de temps. Cependant, vous pouvez faire en sorte que nmap aille plus vite en spécifiant un modèle de temporisation autre que celui par défaut. Étant donné que la cible est une VM sur le même ordinateur (encore mieux que sur le même réseau local !), des délais plus courts devraient être parfaitement sûrs.

Conseil 3 : si vous ne vous intéressez qu'aux services les plus populaires (ce qui est suffisant pour ce TP), vous pouvez utiliser l'argument `--top-ports=N` pour ne scanner que les `N` ports de service les plus populaires.

Livrables :

- Quelle commande avez-vous entrée pour faire un scan plus rapide des ports UDP et pour activer également le scan des services et des versions ?
- Quels sont les 4 ports UDP que nmap a trouvé comme étant ouverts (pas ouverts|filtrés, juste ouverts) et quels sont les services qui fonctionnent sur ces ports ? Donnez votre réponse dans l'ordre numérique croissant.

Partie 5 – Détection du système d'exploitation (OS)

Effectuez un scan de détection d'OS avec `nmap` sur la VM de Metasploitable2. Notez que la détection d'OS implique implicitement la découverte des ports.

```
$ sudo nmap -O CIBLE
```

Remarque : utiliser sudo pour que nmap puisse générer des paquets réseau arbitraires pour ce scan.

Livrables :

- Quel est le type de périphérique de la VM Metasploitable2 selon nmap ?
- Quelle est la chaîne CPE (Common Platform Enumeration) de la VM Metasploitable2 ?
- Quelle est la chaîne OS Details fournie par nmap pour la VM Metasploitable2, montrant la gamme de versions de noyau qu'il pense que l'hôte exécute ?
- Vérifiez la VM Metasploitable2 – Quelle version de noyau exécute-t-elle réellement ? (Fournissez votre réponse sous la forme x.x.x-x-tag)

Partie 6 – Scan des versions et des services

Effectuez un scan de version et de service de la VM Metasploitable2 :

```
$ sudo nmap -sV CIBLE
```

Remarque : utiliser sudo pour que `nmap` puisse générer des paquets réseau arbitraires pour ce scan.

Livrables :

- Quelle version d'OpenSSH est utilisée ?

- Quelle version du serveur DNS BIND est en cours d'exécution ?

Partie 7 - Analyse complète

Effectuez un scan « tout et n'importe quoi » contre la VM Metasploitable2 en utilisant l'option `-A` (pour tous). Il s'agit de l'analyse la plus longue (au moins pour TCP) et la plus verbeuse. En tant que tel, il est préférable de l'exécuter contre des hôtes très spécifiques dont (a) vous connaissez l'existence et (b) vous savez qu'ils possèdent des services spécifiques qui vous intéressent.

```
$ sudo nmap -A CIBLE
```

Remarque : utiliser sudo pour que `nmap` puisse générer des paquets réseau arbitraires pour ce scan.

Livrables :

- Quel est le groupe de travail NetBIOS du serveur Samba sur la VM de Metasploitable2 ?
- Quelle est la clé hôte RSA SSH de 2048 bits qui identifie cette cible ?