Utiliser le scanner réseau Nmap sous Windows

[sommaire]

1. ## Objectifs

- Connaitre le fonctionnement de base du logiciel **Nmap**.
- Être capable de définir les points faibles de votre serveur ou de votre machines pour éviter des attaques imprévu.

- ## Présentation

- Scanner une machine, et surtout un serveur, permet de vérifier la sécurité de base de la machine en identifiant les ports ouverts. Donc susceptibles d’être attaqués.
- Le scan permet également de tester le bon fonctionnement du firewall et d’adapter les règle en fonction des résultats.
- Ici nous allons utiliser **NMAP** qui est un des logiciel les plus répandu, open source, et surtout disponible sur Windows, Mac OS et Linux.
- En complément de Nmap vous pouvez identifier les ports ouverts avec Netstat.
- **Nmap** est un scanner de ports open source qui permet d'obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est de plus en plus utilise par les administrateurs réseaux car il fournit des indications bien précise d'un réseau.
- Dans cet article, nous allons voir le fonctionnement de base de **Nmap**. Ensuite nous allons définir les points faibles de votre serveur ou de votre machines pour éviter des attaques imprévu.

- ## Quelle est le le rôle de Nmap ?

- **NMAP** est un outil d'analyse de réseau complet pour les administrateurs système et réseau. L'analyse des ports est un cas d'utilisation typique de **NMAP**.
- Le but ici est de savoir si un port est ouvert, quelle application s'exécute derrière et si des failles de sécurité et des points faibles y sont suspectés.
- L'objectif du scanner **Nmap** est très simple : il permet de trouver dans un délai très court, tous les ports ouverts sur une machine distante. Il permet également de connaitre le type et la version de l'OS tournant sur la machine.
- Par exemple on peut découvrir grâce à NMAP qu’un système héberge Windows Server avec une certaine version. Si cette version de Windows comporte des vulnérabilités répertoriées, on

apcpedagogie.com

peut à ce moment-là lancer des attaques pour prendre le contrôle de cette machine.
- Un simple analyseur de ports divisera tous les ports en deux ou trois états (ouvert, fermé, filtré). Un scanner de port comme NMAP prête attention à plus de détails et connaît un total de six états de port.

- ## Déroulement d’une intrusion

1. **Ouvrert(open)**

- Le statut "Open" signifie qu'une application ou un service est prêt à accepter des connexions TCP ou des paquets UDP sur ce port. L'objectif de l'analyse des ports est de trouver des « ports ouverts ». En tant qu'administrateur système, vous souhaitez vérifier les faiblesses de l'application sous-jacente. Un attaquant tentera de réaliser un exploit.
- Cependant, pour pouvoir exploiter des connexions de communication, des ports ouverts sont nécessaires. Cependant, chaque port ouvert représente également un certain risque potentiel. Chaque administrateur système responsable s'efforce donc de limiter le nombre de ports ouverts afin de maintenir la surface d'attaque aussi petite que possible.
- Pour cette raison, les ports ouverts sont en outre protégés ou les options de connexion sont restreintes.
- Vous ne pouvez fermer un port ouvert qu'en désactivant l'application ou le service responsable. Ou vous pouvez configurer un filtre de paquets afin que les tentatives de connexion soient rejetées (non bloquées).

- **Fermé (closed)**

- L'état "Fermé" signifie qu'aucune application ou service n'écoute les paquets de données entrants et les tentatives de connexion sur ce port. Le port n'est pratiquement pas utilisé. Aucun lien de communication n'est possible sur celui-ci.
- Un port fermé n'est fermé que tant qu'une application écoute ce port et accepte les connexions et les paquets. Pour s'assurer que les ports ne peuvent pas être utilisés accidentellement, les administrateurs système bloquent généralement les ports avec un pare-feu (filtre de port).
- Cependant, un outil comme NMAP est capable de contourner le filtre et de vérifier si le port est réellement fermé.

- **Filtré (filtered)**

- Les administrateurs système utilisent un filtre de port pour protéger les ports ouverts et fermés. Par exemple, ils empêchent les tentatives de connexion via des analyses de ports. Étant donné qu'un scan de port détermine uniquement l'état d'un port, mais n'est pas censé établir une connexion réelle car il ne connaît pas l'application derrière lui, il ne peut envoyer que des paquets de test à un port. Le filtre empêche ces paquets de test de passer. Habituellement, ces paquets sont rejetés.
- Dans un tel cas, le scanner de ports ne reçoit pas de réponse. Alors ni le statut "ouvert" ni "fermé" ne peut s'appliquer à ce port. L'état "filtré" ou "bloqué" est disponible pour cela.
- Le filtre utilisé peut être un pare-feu classique, une règle de routeur ou un logiciel de pare-feu basé sur l'hôte. Cela peut être utilisé pour garder de nombreuses analyses de ports automatisées à l'écart du système.
- Pour un pentester ou un hacker, les ports filtrés sont une nuisance. Étant donné qu'un scanner de port ne reçoit pas de réponse sur un port filtré, le scanner doit attendre un délai avant de pouvoir adopter l'état "filtré". De plus, ces ports doivent être vérifiés plusieurs fois pour s'assurer que les paquets n'ont pas été perdus en cours de route (perte de paquets classique). Cela a pour effet de ralentir l'analyse des ports.
- Pour cette raison, avant une analyse de port, NMAP utilise différentes méthodes pour vérifier si le système cible peut en principe être atteint. Ce n'est qu'alors qu'un balayage de port est effectué dans lequel un port qui ne répond pas peut être supposé être "filtré".

- **Non filtré (unfiltered)**

  - L'état "Non filtré" signifie que le port est accessible, mais il n'a pas été possible de déterminer s'il est ouvert ou fermé. Cette condition est reconnue par l'analyse ACK, qui est utilisée pour contourner les règles de pare-feu.
  - Pour déterminer si un port non filtré est ouvert, vous devez le vérifier avec d'autres méthodes de scan telles que le scan de fenêtre, le scan SYN ou le scan FIN.

- **Ouvert | Filtré (open | filtered)**

  - Le statut "Open | Filtered" signifie que le port ne peut pas être clairement défini comme ouvert ou fermé. Cela se produit avec les méthodes d'analyse où les ports ouverts ne répondent pas. L'absence de réponse peut également indiquer un filtre.
  - Les méthodes de scan UDP, IP protocol, FIN, NULL et Xmas scan déterminent cet état.

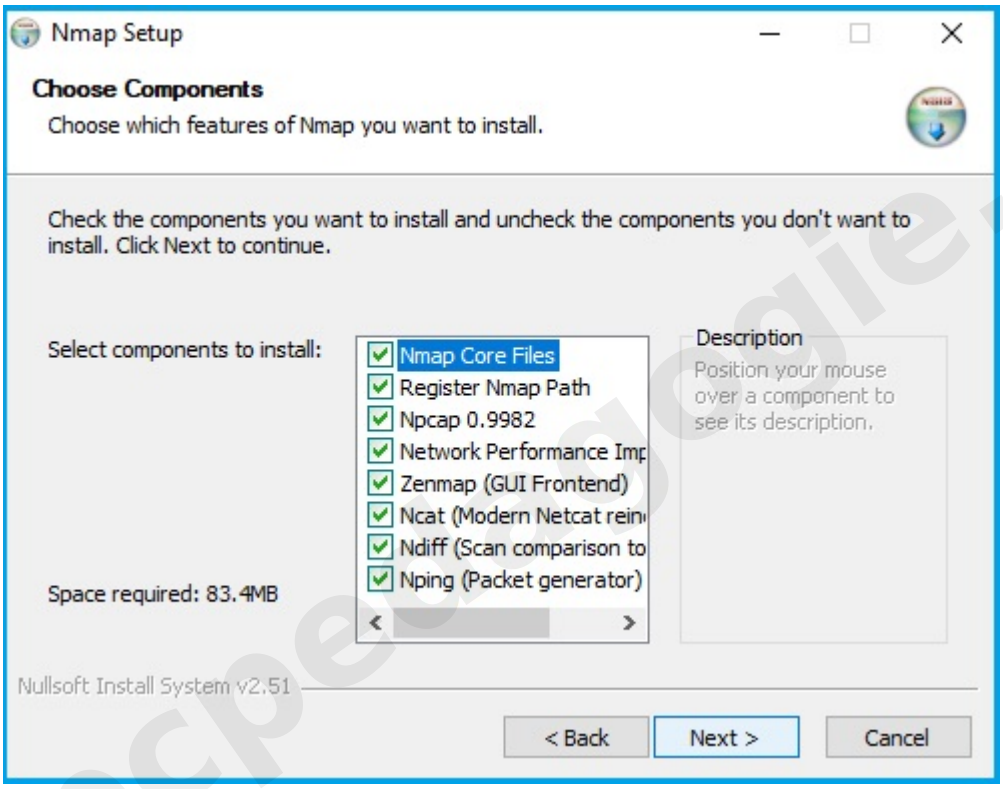
- **Fermé | Filtré (closed | Filtered)**

apcpedagogie.com

- Le statut "Fermé | Filtré" signifie que le port ne peut pas être clairement défini comme fermé ou filtré. L'état survient lorsque les paquets de réponse ne reviennent pas comme prévu. Par exemple, à partir d'hôtes non conformes aux RFC.
- Les méthodes de scan FIN, NULL et Xmas scan y sont sensibles.

Installation Nmap sous Windows

- `NMAP` peut être installé sur les systèmes **Windows** et **Unix**. À installez NMAP sur Windows, allez simplement sur https://nmap.org/download.
- Pour installer Nmap sous Windows, **télécharger tout d'abord le fichier en .EXE Nmap**.



- Une fois le fichier récupéré, double-cliquez dessus. L'assistant d'installation s'ouvre. Cliquez successivement sur Next, I agree, Next, Next.

Les différents types de scan de Nmap

- **Nmap** permet d'effectuer des scans en utilisant différentes techniques issues de l'étude du comportement des machines respectant le RFC793 (TCP). Parmi la douzaine de techniques de scan connues, on peut citer les suivantes :
- **`SYN`** Stealth scan : le scan SYN furtif est celui proposé par défaut. Il est très rapide car il n'effectue pas une connexion TCP complète. Nmap émet un paquet sur le port ciblé et attend

la réponse qui peut être :

- un paquet `SYN/ACK` qui indique que le port est ouvert ;
- un paquet RST qui indique que le port est fermé ;
- pas de réponse si le port est filtré.

- Dans tous les cas **Nmap** n'effectue pas la connexion complète et émet un paquet **RST** pour fermer la connexion. C'est pourquoi ce type de scan est également appelé **demi-ouvert** (half open scan).
- **`Connect scan`** : le scan le plus anodin. Il effectue un appel système connect() et se comporte donc comme un client TCP normal. Il ne nécessite pas de droits particuliers (contrairement au SYN Stealth scan) mais son exécution est plus lente ;
- **`UDP`** port scan : le scan des ports UDP ;
- Consulter la documentation de tous les types de scan sur: http://insecure.org/nmap/man/fr/man-port-scanning-techniques.html.

Quelques commandes utilisées

`[Intense scan]`

- **command** = nmap -T4 -A -v
- **description** = Une analyse intense et complète. L'option **-A** active la détection du système d'exploitation (**-O**), la détection de la version (**-sV**), l'analyse des scripts (**-sC**) et la traceroute (–traceroute). Sans privilèges root, seules la détection de version et l'analyse des scripts sont exécutées. Ceci est considéré comme une analyse intrusive.

`[Intense scan plus UDP]`

- **command** = nmap -sS -sU -T4 -A -v
- **description** = Effectue la détection du système d'exploitation (**-O**), la détection de la version (**-sV**), l'analyse des scripts (**-sC**) et la traceroute (**--traceroute**) en plus de l'analyse des ports **TCP** et **UDP**.

`[Intense scan, all TCP ports]`

- **command** = nmap -p 1-65535 -T4 -A -v
- **description** = Analyse tous les ports **TCP**, puis effectue la détection du système d'exploitation (**-O**), la détection de la version (**-sV**), l'analyse des scripts (**-sC**) et la traceroute (**--traceroute**).

`[Intense scan, no ping]`

- **command** = nmap -T4 -A -v -Pn
- **description** = Effectue un scan intense sans vérifier si les cibles sont en premier. Cela peut être utile lorsqu'une cible semble ignorer les sondes habituelles de découverte d'hôte.

`[Ping scan]`

- **command** = nmap -sn

apcpedagogie.com

- **description** = Cette analyse ne trouve que les cibles actives et ne les analyse pas par port.

`[Quick scan]`

- **command** = nmap -T4 -F
- **description** = Cette analyse est plus rapide qu'une analyse normale car elle utilise le modèle de synchronisation agressif et analyse moins de ports.

`[Quick scan plus]`

- **command** = nmap -sV -T4 -O -F --version-light
- **description** = Une analyse rapide ainsi qu'une détection du système d'exploitation et de la version.

`[Quick traceroute]`

- **command** = nmap -sn --traceroute
- **description** = Trace les chemins vers les cibles sans effectuer une analyse complète des ports sur celles-ci.

`[Regular scan]`

- **command** = nmap
- **description** = Une analyse de port de base sans options supplémentaires.

`[Slow comprehensive scan]`

- **command** = nmap -sS -sU -T4 -A -v -PE -PS80,443 -PA3389 -PP -PU40125 -PY --source-port 53 --script "default or (discovery and safe)"
- **description** = Il s'agit d'une analyse complète et lente. Chaque port TCP et UDP est analysé. La détection du système d'exploitation (-O), la détection de la version (-sV), l'analyse des scripts (-sC) et la traceroute (--traceroute) sont toutes activées. De nombreuses sondes sont envoyées pour la découverte d'hôtes. Il s'agit d'une analyse très intrusive.

États du port NMAP

- Bien que la version actuelle de NMAP soit capable d'effectuer de nombreuses tâches, il a d'abord commencé comme un scanner de port. NMAP a certains moyens de détecter si le port du système cible est ouvert ou fermé.
- **NMAP** détecte le statut du port cible à l'aide d'états prédéfinis comme suit :
  - **Ouvert (`Open`)** : L'état Ouvert indique qu'une application sur le système cible écoute activement connexions/paquets sur ce port.
  - **Fermé (`Closed`)** : l'état Fermé indique qu'il n'y a pas de application à l'écoute sur ce port. Cependant, le port l'état pourrait changer en Ouvert à l'avenir.
  - **Filtré (`Filtered`)**: L'état Filtré indique qu'un pare-feu, un filtre ou une sorte d'obstacle réseau est bloquer le port et donc NMAP n'est pas en mesure de déterminer s'il est

ouvert ou fermé.

- **Non filtré (`Unfiltered`)** : l'état Non filtré indique que les ports répondent aux sondes NMAP ; cependant, ce n'est pas possible de déterminer s'ils sont ouverts ou fermé.
- **Ouvert/Filtré (`Open/Filtered`)** : L'état Ouvert/Filtré indique que le port est soit filtré soit ouvert ; pourtant, NMAP n'est pas précisément capable de déterminer l'état.
- **Fermé/Filtré (`Closed/Filtered`)** : L'état Fermé/Filtré indique que le port est soit filtré soit fermé ; pourtant, NMAP n'est pas précisément capable de déterminer l'état.

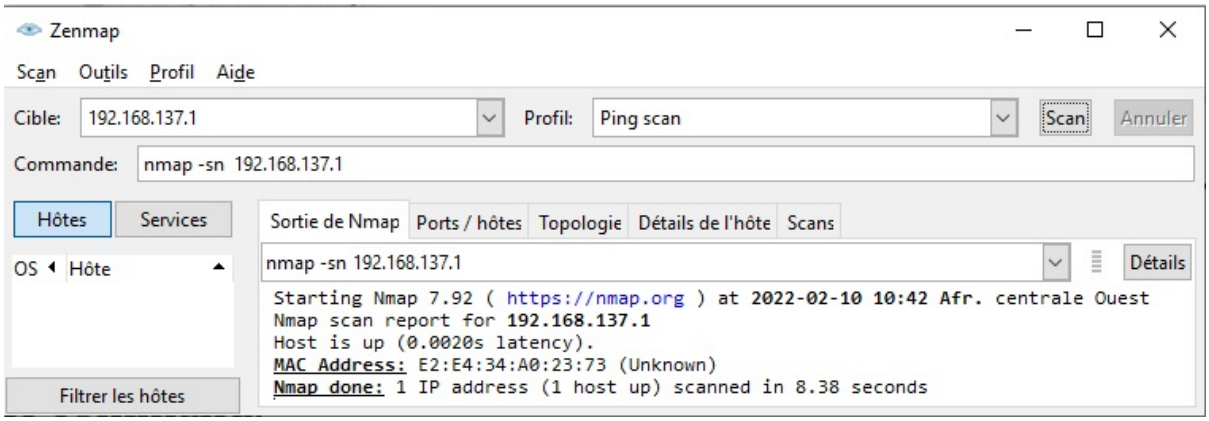
Analyse de base avec NMAP

- NMAP est un outil complexe avec de nombreuses options et commutateurs disponibles.
- Dans cette section, vous verrez divers scénarios d'utilisation de NMAP en commençant par les analyses les plus élémentaires.
- Avant de vous lancer dans la scanning proprement dite, il est important de noter que **NMAP** est un outil bruyant. Il crée beaucoup de trafic réseau et peut parfois consomme beaucoup de bande passante.
- De nombreux systèmes de détection d'intrusion et les systèmes de prévention des intrusions peuvent détecter et bloquer le trafic NMAP. C'est dit qu'une analyse NMAP par défaut de base sur un seul hôte peut générer plus de 4 Mo de trafic réseau. Ainsi, même si vous effectuez une analyse de base sur un sous-réseau entier, cela créera environ 1 Go de trafic. Par conséquent, il est essentiel d'effectuer NMAP analyse avec une connaissance complète des commutateurs utilisés.

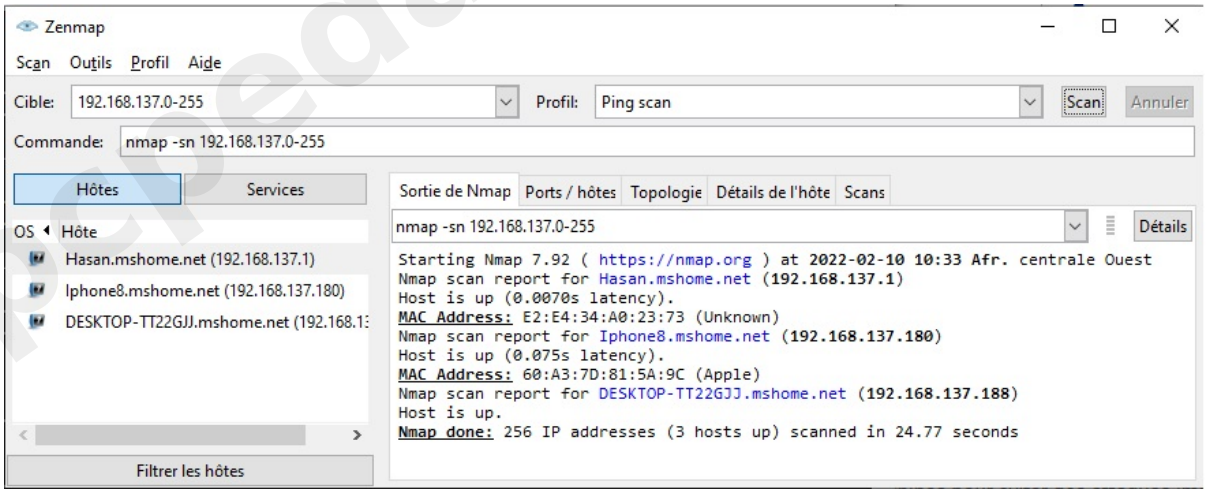
Analyse de base sur une seule IP

- Voici la commande : *nmap -sn <adresse IP cible>*
- Commençons par une analyse ping de base sur une seule cible. Une analyse ping ne pas vérifier les ports ouverts ; cependant, il vous dira si la cible est vivant. La figure suivante montre la sortie d'une analyse ping effectuée sur une adresse IP cible unique adresse.

apcpedagogie.com



- **Analyse de base sur un sous-réseau entier**
  - Voici la commande : *nmap -sn <sous-réseau IP cible>*
  - Dans un scénario pratique, vous pouvez avoir plusieurs adresses IP que vous besoin de vérifier.
  - Pour obtenir un aperçu rapide des hôtes d'un sous-réseau donné qui sont vivant, vous pouvez effectuer une analyse ping NMAP sur l'ensemble du sous-réseau.
  - Un sous-réseau est juste une division logique du réseau. L'analyse de l'ensemble du sous-réseau vous donnera un aperçu des systèmes présents dans le réseau.
  - La figure suivante montre la sortie d'une analyse ping effectuée sur le sous-réseau 192.168.25.0-255. Tu peux voir que sur 255 hôtes, seuls sept hôtes sont opérationnels.



  - Maintenant vous pouvez sondez davantage ces trois hôtes et obtenez des informations plus détaillées.

- **Analyse de base à l'aide d'un fichier d'entrée**
  - Voici la commande : *nmap -sn -iL <chemin du fichier>*

- Il peut y avoir un scénario où vous devez analyser un large éventail de Adresses IP. Au lieu de les entrer dans un format séparé par des virgules pour NMAP, vous pouvez tous les mettre dans un fichier et transmettre ce fichier au moteur NMAP.
- La figure suivante montre le contenu du fichier **hosts.txt** qui contient une liste d'adresses IP.

- **Analyse des ports UDP**

nmap -sU -p 1-1024 <adresse IP cible>

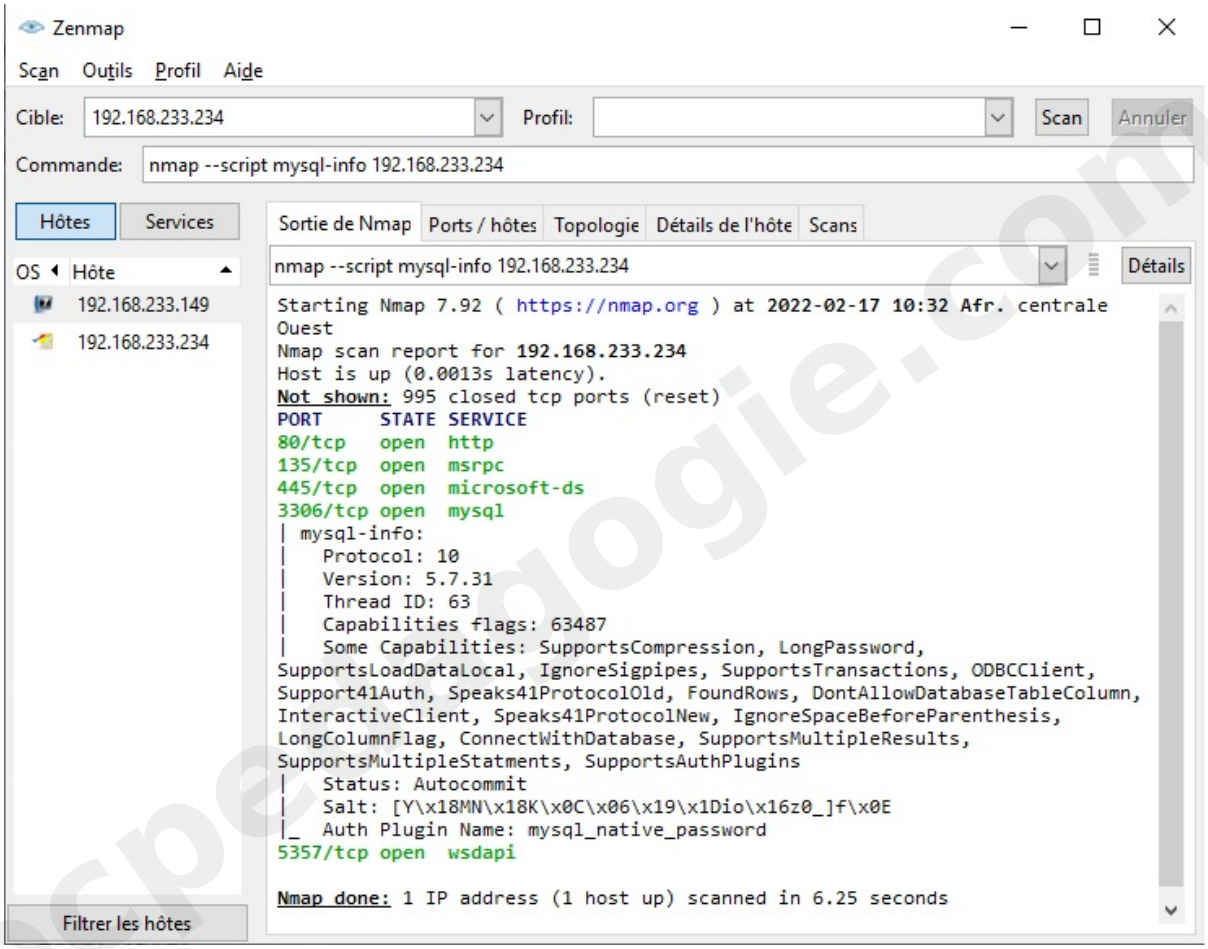
- Toutes les analyses que vous avez effectuées jusqu'à présent ne vous ont donné que des informations sur TCP ports. Cependant, la cible peut également avoir des services exécutés sur des ports UDP.
- Une analyse NMAP par défaut ne sonde que les ports TCP. Vous devez exclusivement rechercher les ports et services UDP. Pour analyser les ports UDP courants, vous pouvez utilisez la commande nmap -sU -p 1-1024 .
- Le **-sU** indiquera au moteur NMAP d'analyser spécifiquement les ports UDP, tandis que le paramètre -p 1-1024 limitera le NMAP à analyser uniquement les ports du plage de 1 à 1024.
- Il est également important de noter que l'analyse du port UDP prend beaucoup plus longtemps qu'une analyse TCP normale.
- La Figure ci-dessous montre le sortie d'un exemple d'analyse UDP



- **Analyse MySQL**

nmap -sU -p 1-1024 <adresse IP cible>

- MySQL est l'une des bases de données relationnelles open source les plus populaires les systèmes de gestion. Il fonctionne sur le port 3306 par défaut.
- NMAP a des scripts pour énumérant le service MySQL
- L'énumération d'un service MySQL peut révéler beaucoup d'informations potentielles qui pourraient être utilisées pour attaquer la cible base de données.
- La figure ci-dessous montre la sortie du script mysql-info. Ça montre les détails de la version du protocole, les capacités du serveur et la valeur de sel utilisée.

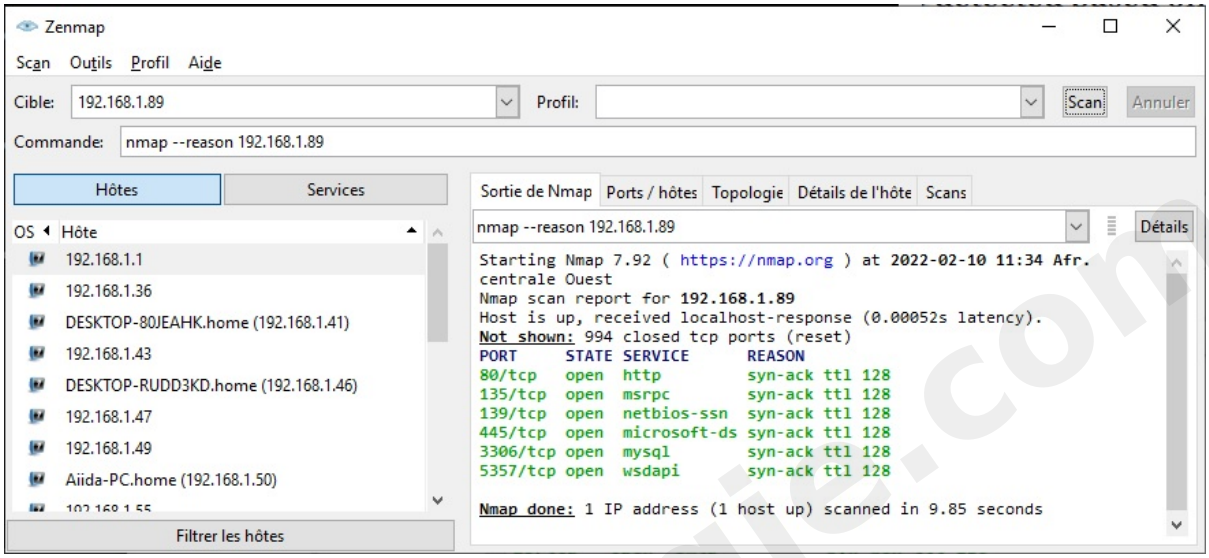


- **Voici quelques scripts NMAP supplémentaires pour l'énumération MySQL :**
  • mysql-databases • mysql-enum • mysql-brute • mysql-query • mysql-empty-password • mysql-vuln-cve2012-2122 • mysql-users • mysql-variables

- **Analyse de motifs**

  - Voici la commande : *nmap --reason <adresse IP cible>*
  - Dans une analyse NMAP normale, vous pouvez obtenir une liste des ports ouverts ; pourtant, vous ne saurez pas la raison pour laquelle NMAP a signalé un port particulier comme ouvert.

- L'analyse de raison NMAP est une option intéressante où NMAP fournit une raison pour chaque port signalé comme ouvert, comme illustré à la Figure suivante.
- Les analyses **NMAP** sont basées sur les drapeaux TCP qui sont définis dans la demande et réponse. Dans ce cas, les ports ouverts ont été détectés sur la base du SYN et Drapeaux ACK définis dans les paquets TCP.

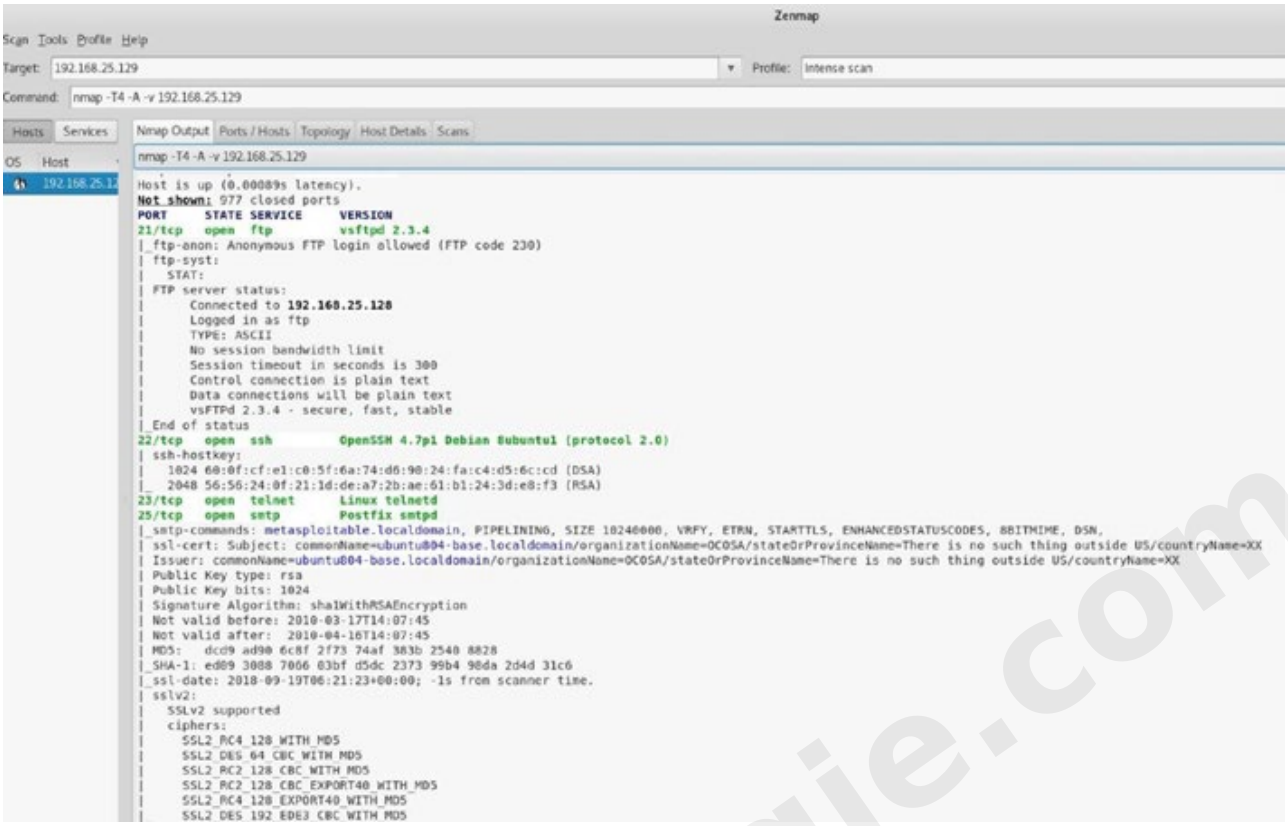


Balayage intense

nmap -T4 -A -v <adresse IP cible>

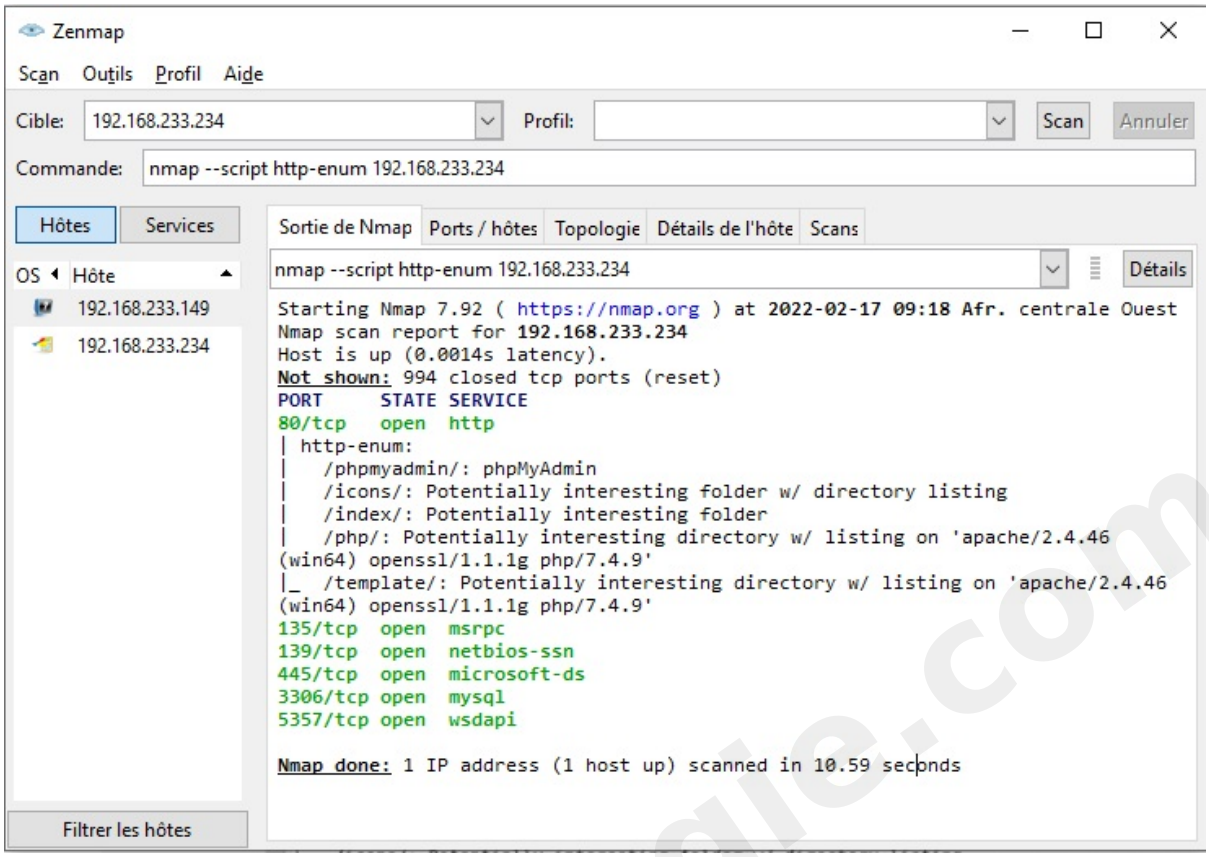
- Jusqu'à présent, vous avez utilisé **NMAP** pour effectuer des tâches individuelles telles que comme l'analyse des ports, l'énumération des services et la détection du système d'exploitation. Cependant, il est possible d'effectuer toutes ces tâches avec une seule commande. Vous pouvez simplement définissez votre adresse IP cible et sélectionnez le profil d'analyse intense.
- **NMAP** fera l'affaire une analyse de port TCP, énumérer les services, et en plus exécuter quelques avancées scripts pour donner des résultats plus utiles.
- Par exemple, la Figure ci-dessous montre la sortie d'une analyse intense NMAP qui n'énumère pas seulement un serveur FTP mais a également souligné qu'il a activé l'accès FTP anonyme.

apcpedagogie.com



- **Énumération HTTP**
  - HTTP est un service commun trouvé sur de nombreux hôtes. Il fonctionne sur le port 80 par défaut.
  - **NMAP** a un script pour énumérer les services HTTP. Ça peut être appelé à l'aide de la commande *nmap –script http-enum <target IPaddress>*.
  - La figure ci-dessous montre la sortie du script http-enum. Ça montre divers répertoires intéressants hébergés sur le serveur Web qui peuvent être utiles dans la construction de nouvelles attaques.

apcpedagogie.com



- **Applications**

1. Installez NMAP sur Windows.
2. Effectuez une analyse UDP sur un système cible à l'aide de ligne de commande NMAP.
3. Effectuez une analyse MySQL sur le système cible à l'aide de ligne de commande NMAP.
4. Trouvez tous les dispositifs terminaux situés dans les mêmes domaines de diffusion.
5. Utilisez NMAP pour détecter le système d'exploitation sur la cible système.
6. Utilisez une analyse intense NMAP sur un système cible.
7. Utilisez divers scripts NMAP pour énumérer les services sur un système cible.
8. Écrire du code Python qui scanne 1 à 500 ports sur un système cible.

Cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/utiliser-le-scanner-reseau-nmap-sous-windows · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com