SRX

Sécurité des Réseaux

Laboratoire n°1
Port Scanning et initiation à Nmap

Professeur

Abraham Rubinstein Scharf
abraham.rubinstein@heig-vd.ch

Assistant

Yohan Martini
yann.lederrey@heig-vd

2020

Nom, prénom : _____

Table des matières

1. Introduction

Toutes les machines connectées à un LAN (ou WAN, VLAN, VPN, etc…) exécutent des services qui « écoutent » sur certains ports. Ces services sont des logiciels qui tournent dans une boucle infinie en attendant un message particulier d'un client (requête). Le logiciel agit sur la requête ; on dit donc qu'il « sert ».

Le scanning de ports est l'une des techniques les plus utilisées par les attaquants. Ça permet de découvrir les services qui tournent en attendant les clients. L'attaquant peut souvent découvrir aussi la version du logiciel associé à ce service, ce qui permet d'identifier des éventuelles vulnérabilités.

Dans la pratique, un port scan n'est plus que le fait d'envoyer un message à chaque port et d'en examiner la réponse. Plusieurs types de messages sont possibles et/ou nécessaires. Si le port est ouvert (un service tourne derrière en attendant des messages), il peut être analysé pour essayer de découvrir les vulnérabilités associées au service correspondant.

1.1. Auteurs

Ce texte se réfère au laboratoire « Port scanning and Nmap » à suivre dans le cadre du cours Sécurité des Réseaux, 2020, version 1.5. Il a été rédigé par Abraham Rubinstein.

1.2. Fichiers nécessaires

Vous recevrez par email tous les fichiers nécessaires à ce laboratoire.

1.3. Rendu

Ce laboratoire **ne sera ni corrigé ni évalué**. Il n'y a donc pas de rendu à faire.

1.4. Échéance

Nous avons prévu 4 périodes pour la réalisation de ce laboratoire. Le travail devra être terminé à la fin de la 2ème séance de laboratoire, soit **le 05 mars 2019.** Cependant, l'infrastructure de virtualisation restera active encore quelques jours après cette date, si vous voulez continuer à faire vos tests.

2. Le réseau de test

2.1. Infrastructure virtuelle

Durant ce laboratoire, nous allons utiliser une infrastructure virtualisée. Elle comprend un certain nombre de machines connectées en réseau avec une diversité de systèmes d'exploitation et de services.

Puisque le but de ce travail pratique c'est de découvrir dans la mesure du possible ce réseau, nous ne pouvons pas vous en donner plus de détails !

2.2. Connexion à l'infrastructure par OpenVPN

Notre infrastructure de test se trouve isolée du réseau de l'école. L'accès est fourni à travers une connexion OpenVPN.

La configuration d'OpenVPN varie de système en système. Cependant, dans tous les cas, l'accès peut être géré par un fichier de configuration, une clé publique et un certificat serveur ainsi qu'un nom d'utilisateur et un mot de passe.

Il est **vivement conseillé d'utiliser Kali Linux** pour ce laboratoire. OpenVPN est déjà préinstallé sur Kali.

OpenVPN propose aussi un client natif pour Windows (attention, il faut télécharger la version « Community »). L'utilisation de Windows pour ce laboratoire est cependant **déconseillée**).

Pour macOS, un client gratuit et très utilisé est proposé par Tunnelblick.

Vous trouverez dans l'email reçu un fichier de configuration OpenVPN personnalisé pour vous (chaque fichier est unique). Le fichier contient un certificat et les réglages correctes pour vous donner accès à l'infra.

Une fois connecté à l'infrastructure, vous recevrez une adresse IP correspondante au réseau de test.

Pour vous assurer que vous êtes connecté correctement au VPN, **vous devriez pouvoir pinger l'adresse 10.10.40.1**.

2.3. Réseau d'évaluation

Le réseau que vous allez scanner est le **10.10.40.0/24**

3. Scanning avec Nmap

Nmap est considéré l'un des outils de scanning de ports les plus sophistiqués et évolués. Il est développé et maintenu activement et sa documentation est riche et claire. Des centaines de sites web contiennent des explications, vidéos, exercices et tutoriels utilisant Nmap.

3.1. Scanning du réseau (découverte de hôtes)

Le nom « Nmap » implique que le logiciel fut développé comme un outil pour cartographier des réseaux (**N**etwork **map**). Comme vous pouvez l'imaginer, cette fonctionnalité est aussi attirante pour les professionnels qui sécurisent les réseaux que pour ceux qui les attaquent.

Avant de pouvoir se concentrer sur les services disponibles sur un serveur en particulier et ses vulnérabilités, il est utile/nécessaire de dresser une liste d'adresses IP des machines présentes dans le réseau. Ceci est particulièrement important, si le réseau risque d'avoir des centaines (voir des milliers) de machines connectées. En effet, le scan de ports peut prendre long temps tandis que la découverte de machines « vivantes », est un processus plus rapide et simple. Il faut quand-même prendre en considération le fait que la recherche simple de hôtes ne retourne pas toujours la liste complète de machines connectées.

Nmap propose une quantité impressionnante de méthodes de découverte de hôtes. L'utilisation d'une ou autre méthode dépendra de qui fait le scanning (admin réseau, auditeur de sécurité, pirate informatique, amateur, etc.), pour quelle raison le scanning est fait et quelle infrastructure est présente entre le scanner et les cibles.

Questions

a. Quelles options sont proposées par Nmap pour la découverte de hôtes ? Servez-vous du menu « help » de Nmap (`nmap -h`), du manuel complet (`man nmap`) et/ou de la documentation en ligne.

Réponse :

b. Essayer de dresser une liste des hôtes disponibles dans le réseau en utilisant d'abord un « ping scan » (No port scan) et ensuite quelques autres des méthodes de scanning (dans certains cas, un seul type de scan pourrait rater des hôtes).

Adresses IP trouvées :

Avez-vous constaté des résultats différents en utilisant les différentes méthodes ? Pourquoi pensez-vous que ça pourrait être le cas ?

Quelles options de scanning sont disponibles si vous voulez être le plus discret possible ?

3.2. Scanning de ports

Il y a un total de 65'535 ports TCP et le même nombre de ports UDP, ce qui rend peu pratique une analyse de tous les ports, surtout sur un nombre important de machines.

N'oublions pas que le but du scanning de ports est la découverte de services qui tournent sur le système scanné. Les numéros de port étant typiquement associés à certains services connus, une analyse peut se porter sur les ports les plus « populaires ».

Les numéros des ports sont divisés en trois types :

- Les ports *connus* : du 0 au 1023
- Les ports *enregistrés* : du 1024 au 49151
- Les ports *dynamiques* ou *privés* : du 49152 au 65535

Questions

c. Complétez le tableau suivant :

Port	Service	Protocole (TCP/UDP)
20/21		
22		
23		
25		
53		
67/68		
69		
80		
110		
443		
3306		

d. Par défaut, si vous ne donnéz pas d'option à Nmap concernant les port, quelle est la politique appliquée par Nmap pour le scan ? Quels sont les ports qui seront donc examinés par défaut ? Servez-vous de la documentation en ligne pour trouver votre réponse.

Réponse :

e. Selon la documentation en ligne de Nmap, quels sont les ports TCP et UDP le plus souvent ouverts ? Quels sont les services associés à ces ports ?

Réponse :

f. Dans les commandes Nmap, de quelle manière peut-on cibler un numéro de port spécifique ou un intervalle de ports ? Servez-vous du menu « help » de Nmap (**`nmap -h`**), du manuel complet (**`man nmap`**) et/ou de la documentation en ligne.

Réponse :

g. Quelle est la méthode de scanning de ports par défaut utilisée par Nmap si aucune option n'est donnée par l'utilisateur ?

Réponse :

h. Compléter le tableau suivant avec les options de Nmap qui correspondent à chaque méthode de scanning de port :

Type de scan	**Option nmap**

TCP (connect)	
TCP SYN	
TCP NULL	
TCP FIN	
TCP XMAS	
TCP idle (zombie)	
UDP	

i. Lancer un scan du réseau entier utilisant les méthodes de scanning de port TCP, SYN, NULL et UDP. Y a-t-il des différences aux niveau des résultats pour les scans TCP ? Si oui, lesquelles ? Avez-vous un commentaire concernant le scan UDP ?

Réponse :

j. Ouvrir Wireshark, capturer sur votre interface réseau et relancer un scan TCP (connect) sur une seule cible spécifique. Observer les échanges entre le scanner et la cible. Lacer maintenant un scan SYN en ciblant spécifiquement la même machine précédente. Identifier les différences entre les deux méthodes et les contraster avec les explications théoriques données en cours. Montrer avec des captures d'écran les caractéristiques qui définissent chacune des méthodes.

Capture pour TCP (connect)

Capture pour SYN :

k. Quelle est l'adresse IP de la machine avec le plus grand nombre de services actifs ?

Réponse :

3.3. Identification de services et ses versions

Le fait de découvrir qu'un certain port est ouvert, fermé ou filtré n'est pas tellement utile ou intéressant sans connaître son service et son numéro de version associé. Cette information est

cruciale pour identifier des éventuelles vulnérabilités et pour pouvoir tester si un exploit est réalisable ou pas.

Questions

l. Trouver l'option de Nmap qui permet d'identifier les services (servez-vous du menu « help » de Nmap (**`nmap -h`**), du manuel complet (**`man nmap`**) et/ou de la documentation en ligne). Utiliser la commande correcte sur l'un des hôtes que vous avez identifiés avec des ports ouverts (**`10.10.40.85 vivement recommandé...)`**. Montrer les résultats.

Résultat du scan d'identification de services :

3.4. Détection du système d'exploitation

Nmap possède une base de données contenant plus de 2600 systèmes d'exploitation différents. La détection n'aboutit pas toujours mais quand elle fonctionne, Nmap est capable d'identifier le nom du fournisseur, l'OS, la version, le type de dispositif sur lequel l'OS tourne (console de jeux, routeur, switch, dispositif générique, etc.) et même une estimation du temps depuis le dernier redémarrage de la cible.

Questions

m. Chercher l'option de Nmap qui permet d'identifier le système d'exploitation (servez-vous du menu « help » de Nmap (**`nmap -h`**), du manuel complet (**`man nmap`**) et/ou de la documentation en ligne). Utiliser la commande correcte sur la totalité du réseau. Montrer les résultats.

Résultat du scan d'identification du système d'exploitation :

Avez-vous trouvé l'OS de toutes les machines ? Sinon, en utilisant l'identification de services, pourrait-on se faire une idée du système de la machine ?

3.5. Vulnérabilités

Servez-vous des résultats des scans d'identification de services et de l'OS pour essayer de trouver des vulnérabilités. Vous pouvez employer pour cela l'une des nombreuses bases de données de vulnérabilités disponibles sur Internet. Vous remarquerez également que Google est un outil assez puissant pour vous diriger vers les bonnes informations quand vous connaissez déjà les versions des services et des OS.

Questions

n. Essayez de trouver des services vulnérables sur la machine que vous avez scannée avant (vous pouvez aussi le faire sur d'autres machines. Elles ont toutes des vulnérabilités !).

Résultat des recherches :

Challenge : L'une des vulnérabilités sur la machine `10.10.40.85` est directement exploitable avec rien d'autre que Netcat. Est-ce que vous arrivez à le faire ?