RAPPORT TD SECURITE DES SI

INTRODUCTION

La première étape d'une attaque est d'abord de connaitre sa cible car on ne peut pas attaquer une cible que l'on ne connait pas, on doit donc avoir une idée de la cartographie du réseau avant toute tentative de pénétration.

Pour cela, on utilise un outil indispensable a tous pentesters, Nmap.

Il s'agit du meilleur outil de scan de ports.

Cet outil permet de connaitre les ports ouverts de la machine cible, les ports sont le seul moyen d'accéder à plusieurs pages web en même temps et faire tourner différents services sur une seule et même machine. Si ces ports sont ouverts, cela veut dire, la plupart du temps, que les services liés à ces différents ports sont actifs sur la machine.

Toutes les machines ont 65535 ports disponibles mais seuls un petit nombre d'entre eux sont reconnu comme des ports standardisés tels que le http (port 80), le https (port 443) ou encore le SMB (port 185).

UTILISATION

Pour lancer Nmap il faut d'abord ouvrir un terminal de commande, si l'on utilise kali linux il est installé par défaut pour les autres cas il faudra l'installer manuellement.

OPTIONS

Nmap propose énormément d'options, celle-ci sont accessible via la commande :

man nmap ou nmap -h

On recense trois principaux types de scans :

Scan avec connexion TCP : -sT

Scan avec SYN : -sS

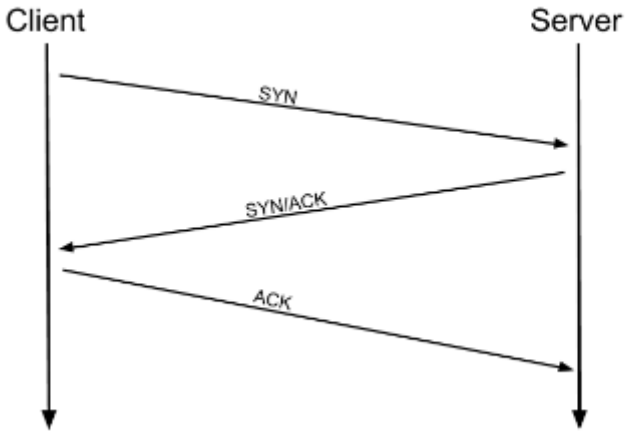
Scan UDP : -sU

Nous allons aborder chacun de ses différents types de scans dans les prochaines parties :

Table des matières :

SCAN AVEC CONNECTION TCP :

Une connexion TCP est réalisé en trois étapes :

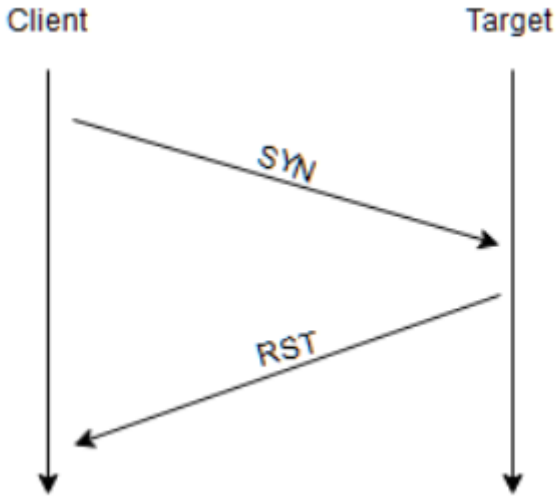


La première requête (SYN) est une demande de connexion TCP,

Le serveur émet un accusé de réception sous la forme d'un paquet TCP contenant un paquet SYN et un paquet ACK,

Enfin, le client termine la connexion TCP avec un paquet ACK.

Ce rappel était obligatoire car Nmap fonctionne de la même manière :



Nmap envoie des paquets SYN sur les ports afin de savoir si ceux-ci sont ouvert ou non.

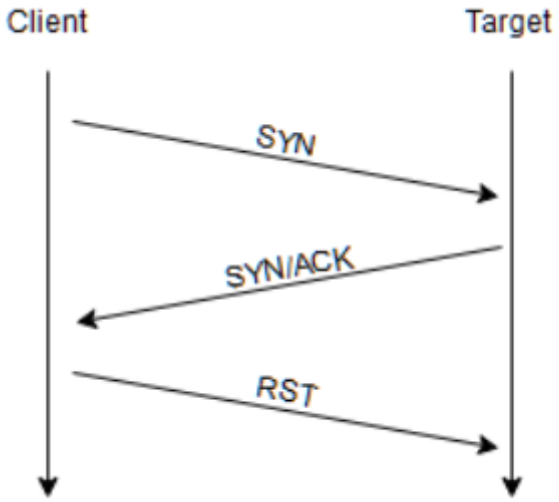
- Port fermé = réponse du serveur par un paquet RST (Reset).
- Port ouvert = réponse du serveur avec un paquet SYN/ACK Nmap termine la connexion en envoyant un paquet ACK.
- Port filtré = aucune réponse de la part du serveur

SCAN AVEC CONNECTION SYN :

Le scan avec connexion SYN diffère légèrement du scan avec connexion TCP.

En effet, le scan TCP réalise les trois étapes de la connexion TCP avec la cible, alors que le scan avec connexion SYN envoie un paquet RST (Reset) s'il reçoit un paquet SYN/ACK de la part du serveur.

La séquence ressemble donc à ça :



Ce paquet Reset envoyer à la réception de la séquence SYN/ACK présente plusieurs avantages :

- Duper les IDS (Système de détection d'intrusions) car ils sont généralement configurés afin de détecter les échanges TCP complet. C'est pour ça qu'on appelle ce scan « scan furtif ».
- Ne laisse pas de traces dans les logs.
- Plus rapide que le scan avec connexion TCP.

Cependant :

- Ce scan demande l'accès SUDO.
- Les services instables sont généralement reconnus comme fermés.

SYN est le scan par défaut utiliser par Nmap s'il est lancé avec les droits SUDO, sinon le scan avec connexion TCP sera pris comme scan par défaut.

Les deux scans sont identiques sur la manière dont il traite les ports fermés et filtrés leurs différences se base sur les ports ouverts car en cas de détection d'un port ouvert :

- TCP scan complète la connexion.

- SYN scan annule la connexion.

SCAN avec connexion UDP :

Contrairement aux autres scans, le scan avec connexion UDP ne tente pas de connexion, il envoie seulement un paquet UDP complètement vide et attend de voir ce qu'il se passe.

- Pas de réponse = port ouvert | filtré.
- Réponse avec un paquet UDP = port ouvert.
- Réponse avec un paquet ICMP = port fermé.

Le scan avec connexion UDP est beaucoup plus lent que les autres scans du a sa difficulté d'identifier le port comme ouvert.

AUTRES TYPES DE SCANS :

Il existe trois autres types de scans moins connus et moins utilisé que les précédents il s'agit de :

- Scan NULL
- Scan FIN
- Scan Xmas

Scan NULL :

Comme son nom l'indique il s'agit d'un paquet TCP envoyé avec rien à l'intérieur.

Si le port est fermé l'hôte répondra avec un paquet RST.

Scan FIN :

Fonctionne presque exactement que le scan NULL a la seule différence qu'a la place d'envoyer un paquet complétement vide il contient un flag FIN.

Scan Xmas :

Il envoie un paquet TCP malformé et attend une réponse RST également.

Tous ses scans fonctionnent tels que le scan UDP pour déterminer si le port est ouvert etc….

Le scan réseau ICMP :

Ce scan sert à obtenir une « carte » du réseau en identifiant quelles adresse IP sont actives.

Pour cela on utilise la commande -sN de Nmap, avec cette option, Nmap envoie un paquet ICMP a toutes les adresses IP possible du réseau et s'il obtient une réponse, l'adresse IP est identifié comme active.

LES SCRIPTS :

Après avoir fait le tour des différents types de scans que peut réaliser Nmap, nous allons parler des scripts que celui-ci propose.

Cette fonctionnalité de script s'appelle NSE (Nmap Scripting Engine) il existe plusieurs catégories :

- Safe : N'affecte pas la cible
- Intrusive : Affecte généralement la cible
- Vuln: Scan afin de trouver des vulnérabilités
- Exploit: Exploite une vulnérabilité.
- Auth: Tente de contourner les authentifications.
- Brute: Tente de réaliser des attaques type « brute force ».
- Discovery: Tente d'obtenir des infos sur les services présent sur le réseau.

Tous les scripts Nmap sont codés à l'aide du langage Lua.

Afin de lancer un script avec Nmap la commande est nmap –script= « nom du script »

Pour savoir quel script utilisé pour notre tache on peut les chercher a deux endroits :

- Sur le site Nmap
- En regardant dans le dossier /usr/share/nmap/scripts

Ou alors avec les commandes :

- ls /usr/share/nmap/scripts/*nom du protocole que l'on veut*
- Grep « nom du protocole que l'on veut » /usr/share/nmap/scripts/script.db

CONTOURNEMENT DE FIREWALL :

La dernière partie primordiale de nmap est le contournement de firewall

Nous avons déjà vu certaines techniques :

- Scan SYN
- Scan NULL/FIN/XMAS

En général les firewalls bloquent les paquets ICMP.

Pour contourner ça on va utiliser la commande -Pn.

Cela permet de scan l'hôte en la considérant comme active sans lui émettre un ping cela permet de ne pas envoyer de ping et donc d'esquiver le blocage ICMP.

D'autres options permettent aussi de contourner les IDS/IPS/FIREWALL

-f : Fragmente les paquets pour qu'ils soient moins détectables.

Ou contrôler manuellement la taille des paquets avec --mtu