Scans

Guillaume Pillot

Club de Hacking de l'Université Laval

11 Octobre 2016

Sommaire

Qu'est qu'un scan ?

- L'étape de reconnaissance a permis essentiellement de collecter une liste d'adresses IP
- L'étape des scans permet d'associer des adresses IP à des ports et à des services ouverts (HTTP, SSH, FTP, VNC, etc.)
- Documentation : Les bases du hacking. Chapitre 3 : Les scans p. 57 à 61

ping et fping

- Avant toutes choses, il faut s'assurer que les machines distantes sont actives
- Le ping est un paquet réseau appelé paquet ICMP. Si la machine qui reçoit un ping est allumée et est configurée pour répondre, alors il renvoie un paquet de réponse :
  `# ping 10.10.20.254`
- Pour faciliter la découverte d'hôtes actifs sur un réseau, il est possible d'effectuer un balayage de ping avec `fping` :
  `# fping -a -g 10.10.20.1 10.10.20.254 > hotes.txt`
  `-a` : inclus dans la sortie seulement les hôtes actifs
  `-g` : définit la plage de balayage
  `> hotes.txt` : flux de redirection vers hotes.txt
- Documentation : Les bases du hacking. Chapitre 3 : Les scans p. 61 à 63
  Lien

Qu'est ce qu'un port ?

- Un port correspond à un service disponible sur un ordinateur
- Il est représenté par un numéro, étant codé sur 16 bits, il peut y avoir de 0 à 65 535 ports sur une machine
- Il permet d'utiliser plusieurs services/applications sur une même machine
- Voici une liste des ports les plus connus avec leurs services associés :

num port	**services**
20	FTP
22	SSH
25	SMTP
80	HTTP
443	HTTPS

- Documentation : Lien

Le protocole TCP

- TCP, pour Transmission Control Protocol, est un des protocoles de la couche transport du modèle OSI
- Il permet d'assurer la communication entre deux machines
- La connexion se fait en trois étapes et est semblable à un appel téléphonique :
  - L'ordinateur 1 envoie un paquet SYN à l'ordinateur 2, cela revient à composer le numéro de téléphone de son destinataire.
  - Si l'ordinateur 2 est à l'écoute, il répond par un paquet SYN/ACK. Cela revient à décrocher le téléphone et dire "Allo ?".
  - L'ordinateur 1 répond par un paquet ACK, cela revient à dire "Bonjour, c'est Robert !". La connexion est établie.
- Documentation : Lien 1 Lien 2
  Les bases du hacking. Chapitre 3 : Les scans p. 65 et 66

nmap

- nmap est le logiciel de scan de ports le plus populaire
- Il est intégré à de nombreuses distributions Linux dont Kali
- Documentation : Lien

```
# man nmap
```

Scans TCP Connect

- Scan le plus simple qui consiste a effectué une connexion TCP complète (les trois étapes)
- `# nmap -sT -p- -Pn 10.10.20.103`
  - `-sT` : Scan TCP Connect
  - `-p-` : Scan l'ensemble des ports de la cible. Par défaut, nmap ne scan que les 1000 premiers ports
  - `-Pn` : Ignore l'étape de découverte des hôtes (ping), si une machine bloque les pings ont découvrira quand même les ports ouverts sur cette machine
- Pour effectuer le scan sur l'ensemble une plage d'adresse :

  `# nmap -sT -p- -Pn 10.10.20.1-200`
- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 66 et 67

Scans SYN

- Scan par défaut de nmap. Seules les deux premières étapes de la connexion sont effectuées, un paquet RST (réinitialisation) est envoyé à place du paquet ACK et ferme la connexion. Cela équivaut à raccrocher immédiatement quand la cible décroche le téléphone et répond "Allô ?"
- L'avatange de ce scan est sa rapidité ainsi que sa furtivité, certains systèmes de journalisation n'enregistrent que les connexions TCP complètes. Aujourd'hui tous les pare-feu et système de détection moderne détectent les scans SYN
- Pour effectuer un scan SYN :

```
# nmap -sS -p- -Pn 10.10.20.103
```

- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 68 et 69

Challenge 1

- Un serveur ne répond pas au ping sur notre réseau
- Identifiez quelle plage d'adresse IP nous n'avons pas encore scannée et retrouvez l'adresse du serveur
- Le flag se trouve dans une page web du serveur, le port utilisé n'est pas 80

Le protocole UDP

- UDP pour User Datagram Protocol est le deuxième protocole principal de la couche transport. Contrairement à TCP, il n'est pas orienté connexion.
- L'ordinateur 1 envoie ses données sans prévenir le destinataire et celui-ci n'envoie pas d'accusé de réception
- UDP a été conçu après TCP dans le but de simplifier une connexion et où la vitesse prime sur le contrôle tel que la VoIP ou les jeux en ligne.
- Les services les plus connus utilisant l'UDP sont DHCP, DNS et SNMP
- Documentation : Lien 1 Lien 2

Scans UDP

- Effectuer un scan UDP avec nmap est simple :
  `# nmap -sU 10.10.20.103`
- Les scans UDP sont très lents et scanner l'ensemble des ports d'une machine va prendre beaucoup de temps. Le scan par défaut (10 000 ports) prend environ 18 minutes
- Étant donné qu'UDP n'est pas obligé de renvoyer une réponse. Lorsqu'aucune réponse n'est envoyée, il est impossible de savoir si un port est ouvert ou fermé. Dans ce cas, nmap considère le port comme "ouvert|filtré"
- Pour déclencher des réponses supplémentaires sur les ports UDP ouverts, on peut rajouter le scan de version.
- nmap effectue une série de tests qui peut permettre d'obtenir des informations supplémentaires sur l'utilisation des ports de la machine (nom de l'application, OS, équipement, etc.) :
  `# nmap -sUV 10.10.20.103`
- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 69 et 72

Challenge 2

- Sur la même machine que nous avions découverte précédemment existe un service accessible via UDP
- Son numéro de port se situe entre 0 et 100
- Une fois le service identifié, documentez-vous sur le fonctionnement de ce protocole pour obtenir le flag
- La seule chose dont vous avez besoin de savoir et que le fichier a récupérée se nomme flag.txt

Flags TCP

- Un paquet TCP contient des flags représentant le type de requêtes envoyé :
  - URG : urgent
  - ACK : accusé de réception
  - PSH : fonctionne suivant la méthode PUSH
  - RST : connexion est réinitialisée
  - SYN : demande d'établissement de connexion
  - FIN : la connexion s'interrompt
- La RFC 675 décrit le fonctionnement du protocole TCP et plusieurs faiblesses ont été découvertes
- Si un port fermé reçoit un paquet avec les drapeaux SYN et ACK à zéro, alors le port doit répondre par un paquet RST
- Si un port ouvert reçoit un paquet avec les drapeaux SYN, ACK et RST à zéro, ce paquet doit être ignoré
- Documentation : Lien

Scans Xmas et Null

- Un scan Xmas envoie des paquets avec les drapeaux SYN, ACK et RST à zéro (les autres étant à 1). Il porte ce nom car ce paquet ressemblant à un sapin de Noël :
  `nmap -sX -p- -Pn 10.10.20.103`
- Un scan Null envoie des paquets avec tous les drapeaux à zéro :
  `nmap -sN -p- -Pn 10.10.20.103`
- L'utilité de ces scans est de contourner certains filtres et déterminer si un port est ouvert ou fermé. Néanmoins, avec un pare-feu récent ces scans ne fonctionneront pas
- NB : Windows ne respectant pas la RFC, il est inutile d'effectuer ce type de scan sur une machine Windows
- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 72 et 74

NSE : Le moteur de script de nmap

- Le moteur de script nmap (NSE) permet d'utiliser un bon nombre de services tel que le scan de vulnérabilités, les attaques par brute force, la détection de portes dérobés et bien d'autres.
- Les scripts sont réparties en catégorie : auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version et vuln
- Chaque catégorie comprend différents scripts :
  `nmap --script vuln 10.10.20.103`
  - `--script` : invoque un script ou une catégorie de NSE
  - `vuln` : invoque tout les scripts de la catégorie vulnérabilité
- Les scripts NSE sont situés dans `/usr/share/nmap/scripts/`
- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 74 et 75

Nessus

- Maintenant que nous connaissons les services disponibles sur chaque machine, il est temps d'aller chercher les vulnérabilités sur celle-ci
- Nessus est un scanneur de vulnérabilités gratuit très connu pouvant fonctionner sur Windows comme sur Linux
- Pour installer Nessus, il faut d'abord obtenir un code d'activation sur leur site, ensuite le télécharger et installer le paquet .deb Pour installer un .deb, exécutez cette commande : `dpkg -i mon_paquet.deb`
  Ensuite, démarrer le service : `/etc/init.d/nessusd start`
- Nessus est maintenant accessible à cette adresse : **https ://127.0.0.1 :8834**, suivez les instructions, identifiez-vous, cliquez sur le bouton "New scan" et choisissez le template "Basic network scan", ensuite remplissez les instructions du formulaire, notre cible sera toujours 192.168.1.2. Une fois le scan enregistrée, lancez-le !
- Documentation : Lien
  Les bases du hacking. Chapitre 3 : Les scans p. 77 et 81

Challenge 3

- Le serveur que nous avions découvert tantôt est vulnérable par une faille très connue
- Choisissez le bon template quand vous créerez votre scan sur Nessus
- Un accès SSH est possible via l'username "hackme", son mot de passe est "hackme"
- Il n'y a pas de flag a trouvé, seulement trouver de quelle faille il s'agit avec Nessus

Nikto

- Nikto est un scanneur de vulnérabilités des serveurs web
- Il permet de détecter les défauts de configuration du serveur
- Son utilisation est très simple : `# nikto -h 10.10.20.103 -p 80`
  - `-h` : pour indiquer l'adresse IP à cibler
  - `-p` : pour indiquer le numéro du port
- Documentation : `man nikto`
  Les bases du hacking. Chapitre 3 : Les scans p. 152 et 153

Challenge 4

- Toujours sur le même serveur, une URL possédant un flag est cachée
- Utilisez Nikto pour trouver cette page