Nmap – bien plus qu’un scanner

HackademINT

Qu’est-ce que c’est ?

- Un outil gratuit et open-source
- Maintenu activement et qui évolue sans cesse
- Au début, il servait à scanner des réseaux et des machines pour savoir quels services tournent dessus
- Vous allez bientôt découvrir que Nmap fait BIEN PLUS que ça
- Nmap : Network Mapper

Utilisation de base

- nmap 123.123.123.123
- nmap 10.0-255.0-255.1-254
- nmap sitevuln.com
- Effectue un scan basique des 1000 ports les plus utilisés
- -v, -vv, -vvv augmente la verbosité selon votre envie

- Selon les types de scan, nmap peut nécessiter d'être root (souvent pour les scans agressifs ou particuliers)

Options de base bien utiles

- -p 80 / -p 80-1000 / -p 80,443 : scanne les ports spécifiés
- -p- : scanne tous les 65536 ports au lieu de juste les 1000 plus courants
- -Pn : force le mode découverte en désactivant le pré-scan ping (conseillé car certaines machines tentent de se cacher en ne répondant pas aux pings par exemple)

Les types de scan

- -sT : scan TCP, la base
- -sU : scan UDP, à ne pas négliger mais éviter -p- (trop long)
- -sX : scan XMAS
- -sN : scan NULL : les deux servent à bypass des pare-feu
- -sV : scan de versions (très utile pour le pentesting)

- -O : scan d’OS
- -A : raccourci de -O -sV

La vitesse

- -T0 : trèèèèèèèès lent mais très sûr, a l’avantage d’être discret
- -T5 : accélère bien les choses mais risque de baisser la précision, pour la discrétion vous repasserez

- En général -T4 est le plus utilisé

Les formats de sortie

- -oN nom : format standard
- -oX nom : format XML
- -oG nom : format greppable, plus trop utilisé
- -oA nom : standard + XML + greppable

- ***BONUS*** -oS : script kiddie (oui oui, ça sert à rien)

NSE : Nmap Script Engine

- Un ensemble de scripts regroupés en catégories permettant de faire des scans ciblés et exhaustifs
- Selon la catégorie, peut tenter d'exploit directement la cible : à n'utiliser que si vous êtes sûrs d'en avoir le droit

- Vous l'avez déjà croisé : -sV, -O

NSE, la puissance

- --script catégorie
- auth : tente de se connecter à la machine (ftp anonyme, ldap null bind…)
- brute : pareil, mais en bruteforçant
- exploit : tente d’exploiter directement la cible (shellshock,…). Un peu bourrin quand même
- malware : tente d’identifier des malwares ou des backdoors sur la cible

NSE : vuln, l’option privilégiée

- Agit comme un scanner de vulnérabilités
- En général ne tente pas d’exploiter la cible
- Regroupe dirb, injection SQL, XSS, et plus encore
- Liste les CVE connues selon les versions détectées avec les liens et les infos correspondantes

- En fait, vous posez pas la question et utilisez-la

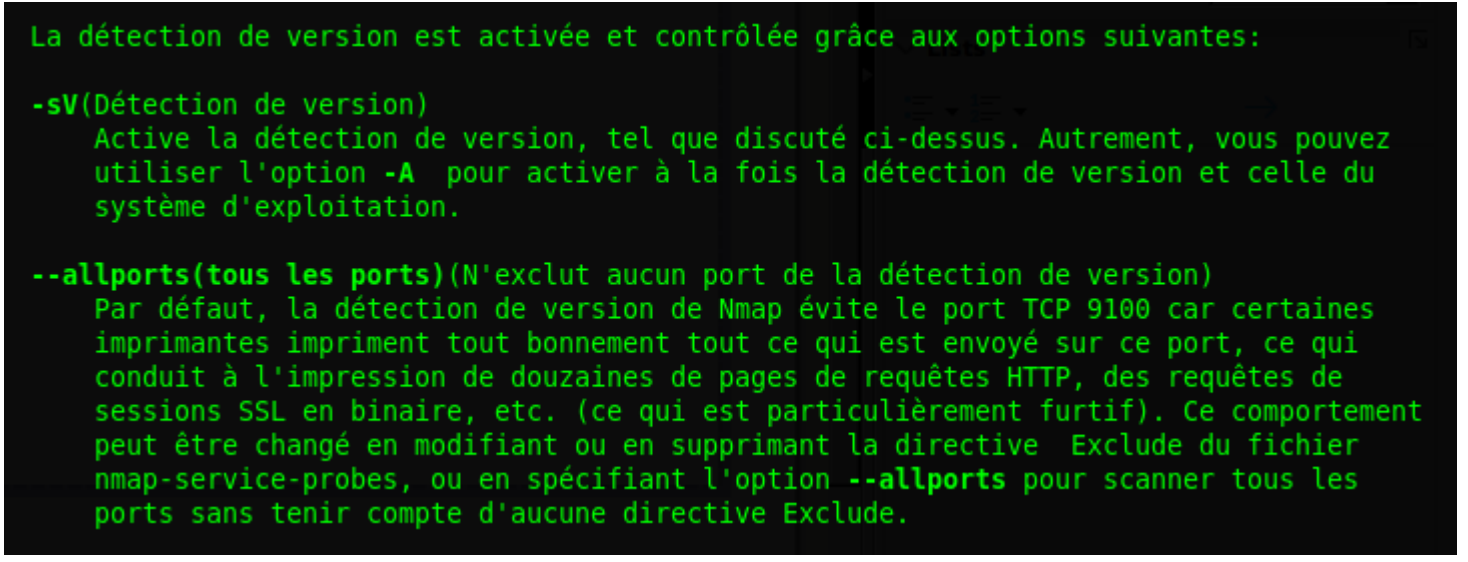
Nmap, c’est bien plus encore

- Des tonnes d’options de durée, vitesse, comportement...
- Des options que vous ne soupçonnez même pas : mode zombie, scan Maimon, fragmentation de paquets...
- Le NSE est bien plus puissant que ce qui est présenté ici : personnalisation de tests avec des usernames et des passwords connus, écriture de vos propres scripts (en Lua)...

Je veux en savoir plus !!!

- man nmap : un manuel très clair et presque entièrement traduit en français
- https://nmap.org/
- Fouillez /usr/share/nmap(/scripts) si vous êtes curieux
- Maintenant que vous avez une bonne compréhension de nmap, regardez les commandes de scan toutes prêtes de writeups / PayloadAllTheThings / HackTricks pour les comprendre et découvrir d’autres options

La doc, c’est utile ! (Humour coming)



Derniers conseils

- Découpez vos scans
- Sauvegardez vos résultats
- Allez-y progressivement : scans simples mais larges d’abord, puis scans plus avancés et plus longs mais sur des cibles plus précises (-p)
- Tentez toujours de vous connecter à ce que vous trouvez : via nc si vous savez pas ce que c’est, via le client associé sinon

- Expérimenter, échouer, réessayer, hacker

Time to practice

- 5 flags commençant par HackademINT, tous trouvables avec nmap, ce que je viens de vous raconter, et votre talent
- Un 6ème flag stocké sur la machine pour ceux qui veulent exploiter jusqu'au bout ;-)
- Si vous voulez télécharger un truc dont vous connaissez pas le nom, tentez flag.txt par le plus grand des hasards

- Amusez-vous bien et n'hésitez pas à poser des questions !