**Procédure d’utilisation Nmap**

**SOMMAIRE**

1 Objet du document 3

2 Nmap 3

2.1 Man 3

2.2 Scan Nmap 3

2.2.1 Utilisation et options principales 3

2.2.2 Scan SYN 4

2.3 Nmap Scripting Engine (NSE) 5

2.3.1 Utilisation 5

# Objet du document

Ce document présente la procédure d’utilisation de l’outil **Nmap**.

# Nmap

## Man

Pour avoir une liste des options disponibles avec Nmap, taper la commande ***nmap -h*** ou aller à l’adresse <http://nmap.org/book/man.html> et <https://nmap.org/man/fr/> pour la version française.

## Scan Nmap

### Utilisation et options principales

Le squelette de Nmap est le suivant : ***nmap [Scan Type(s)] [Options] target***

Pour le *taget* il est possible de spécifier une adresse IP, une plage d’adresses IP ou un ensemble d’adresses IP non contiguës.

Les options dont il est toujours conseillé d’ajouter sont :

* *-sS* / *-sU* / *-sT* / *-sX* / *-sN* : effectue un scan SYN (par défaut) / UDP / TCP Connect / Xman / Null ;
* *-p-* : permet d’effectuer un scan de tous les ports, car par défaut Nmap scanne les 1000 ports les plus utilisés ;
* *-Pn* : est également conseillée car désactive la découverte des hôtes et oblige Nmap à scanner chaque système comme s’il était actif (Nmap fait un ping pour voir si le système est actif, mais si ce dernier a désactivé le ping, Nmap ne scannera pas les ports alors qu’il est possible que ce système héberge des services) ;
* *-sV* : permet d’avoir plus de détails sur le service, dont la version ;
* *-O* : permet de déterminer le système d’exploitation de la cible, ceci afin de focaliser les attaques sur les faiblesses de ce système.

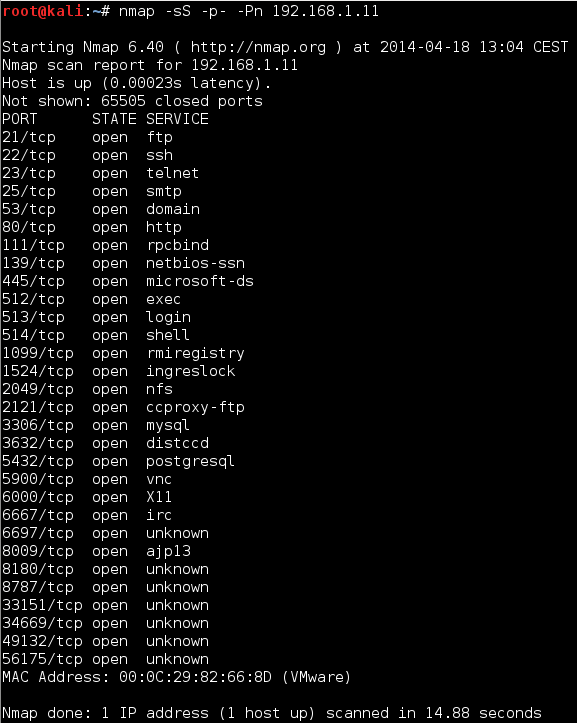
A noter d'autres options utiles :

* *-p* : spécifie les ports à scanner ;
* *-sn*: désactive le scan de port, utile lorsqu’on souhaite découvrir les machines actives sur le réseau ou utiliser NSE ;
* *-n* : désactive la résolution DNS ;
* *-T[0-5]* : permet de modifier la rapidité du scan des ports. Les valeurs vont de 0 à 5, respectivement du plus lent au plus rapide. L’utilité est que les scans lents sont plus difficiles à détecter, tandis que les scans rapides conviennent en cas de temps limité ou d’un grand nombre d’hôtes à cibler ;
* *--reason* : donne la raison pour laquelle tel port apparait à tel état ;
* *--version-light* : limite les tests de l'option *-sV* aux plus probables pour une identification plus rapide ;
* *-iL* : spécifie le fichier à prendre en entrée contenant la liste des adresses IP ;
* *--exclude* / *--excludefile*: exclut des hôtes/réseaux du scan ;
* *-oN*: exporte le résultat dans un fichier ;
* *-v* : permet d’activer le mode verbose permettant d’afficher dans la console plus de détails et l’état d’avancement des opérations en cours.

Il est recommandé d'exécuter Nmap avec les privilèges root, en utilisant la commande *sudo* par exemple.

### Scan SYN

1. Pour effectuer un scan SYN, il faut utiliser l’argument ***-sS***. Utiliser donc la commande : ***nmap -sS -p- -Pn target***



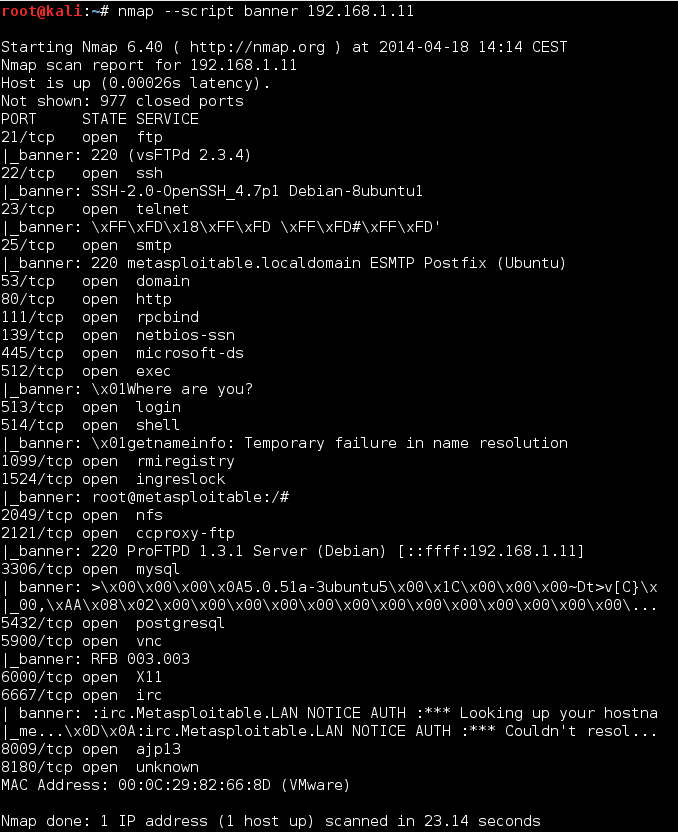
## Nmap Scripting Engine (NSE)

### Utilisation

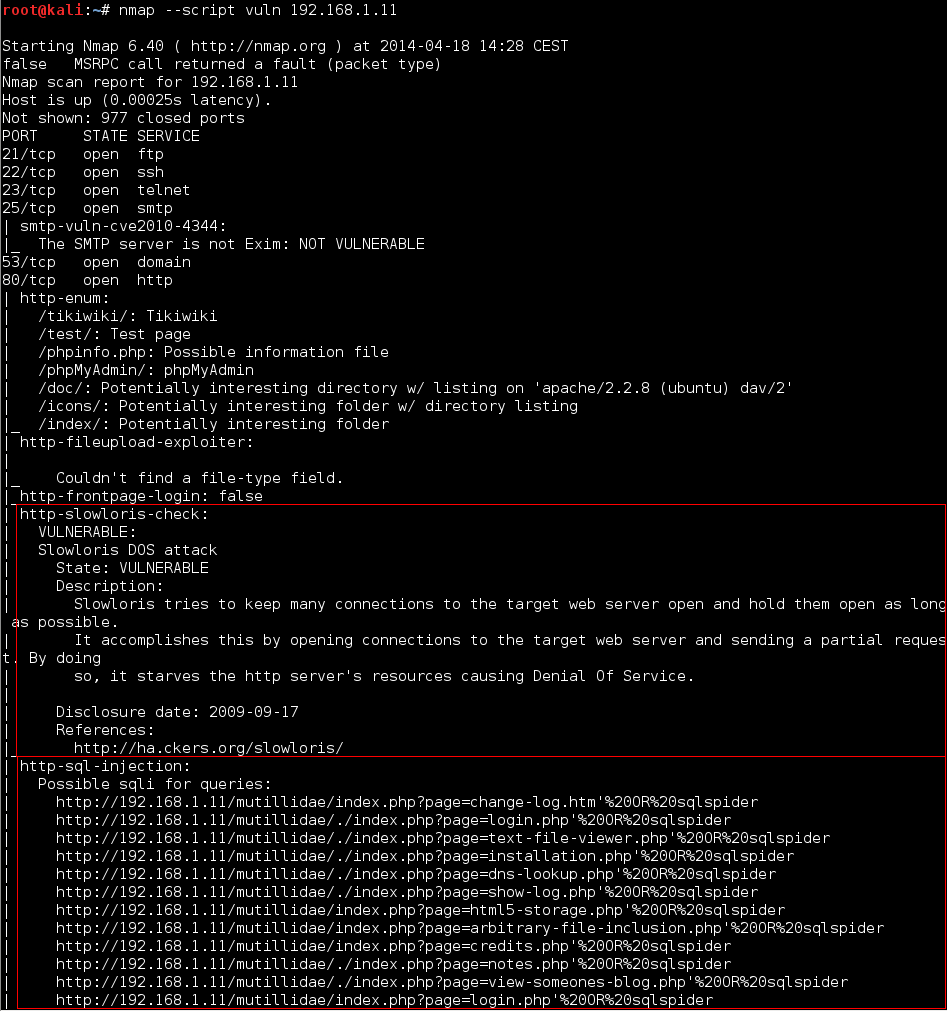
Le squelette pour utiliser NSE est le suivant : ***nmap --script [nom du script | nom de la catégorie] target***

Pour avoir des informations sur un script ou sur les scripts d’une catégorie, utiliser la commande : ***nmap -script-help [nom du script | nom de la catégorie]***

1. La commande ***nmap --script banner 192.168.1.11*** permet l’exécution du script banner sur la cible avec l’adresse IP 192.168.1.11.



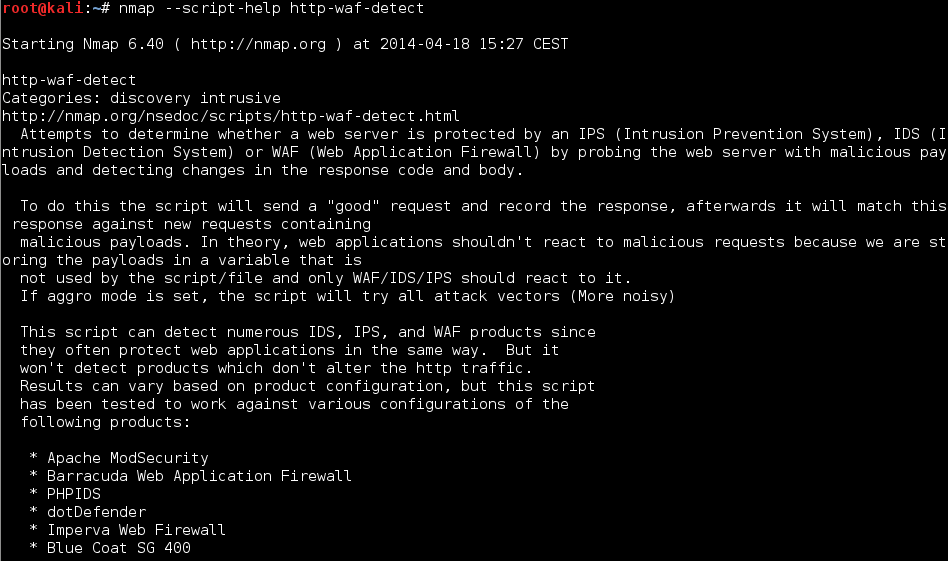
1. La commande ***nmap --script vuln 192.168.1.11*** permet d’invoquer tous les scripts de la catégorie vuln sur la cible ayant l’adresse IP 192.168.1.11.



Nous pouvons constater, par l'exemple ci-dessus et grâce à la catégorie vuln, qu'une vulnérabilité DoS et plusieurs pages vulnérables à l’injection SQL sont detectées.

Il nous conseille aussi l’outil slowloris pour exploiter la vulnérabilité DoS.

1. La commande ***nmap --script-help http-waf-detect*** permet d’afficher la description du script http-waf-detect. On peut utiliser le wildcard « \* » pour indiquer n’importe quel caractère, par exemple ***nmap --script-help http-waf-\**** permet d’afficher la description de tous les scripts dont leur nom commence par « http-waf- ».   
   La description de l'exemple suivant montre que ce script a comme utilité de détecter la présence d’un WAF.



1. La commande ***nmap --script-help "http-\* and discovery"*** permet d’afficher tous les scripts qui commence par « http- » faisant parti de la catégorie « discovery ».