Table des matières

Table des matières

INSTALLATION DE NMAP 2
COMMENT UTILISER NMAP ? 2
INTERFACE GRAPHIQUE 3

Avant-Propos

Nmap est un scanner de ports libre créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant. Ce logiciel est devenu une référence pour les administrateurs réseaux car l'audit des résultats de Nmap fournit des indications sur la sécurité d'un réseau. Il est disponible sous Windows, Mac OS X, Linux, BSD et Solaris.

La procédure suivante sera faite sur une machine cliente Ubuntu 16.04 LTS.

E6 :

Elaboration de documents relatifs à la production et à la fourniture de services
A1.2.4 , Détermination des tests nécessaires à la validation d'un service
A1.4.1 , Participation à un projet
A2.1.1 , Accompagnement des utilisateurs dans la prise en main d'un service
A4.1.9 , Rédaction d'une documentation technique

Installation de NMAP

Le paquet de Nmap n'est pas installé directement sur les machines Linux, il faut donc l'installer à partir de la commande suivante

```
utilisateur@utilisateur-System-Product-Name:~$ sudo apt-get install nmap
```

Une fois l'installation terminée, on peut maintenant l'utiliser

Comment utiliser Nmap ?

Nmap est assez facile d'utilisation, en effet, il suffit simplement de rentrer nmap et l'adresse IP de la machine que l'on veut scanner.

Cependant, ajouter l'option -O (o majuscule) permet de savoir en plus quel OS est installé sur la machine, ce qui peut être pratique.

```
utilisateur@utilisateur-System-Product-Name:~$ sudo nmap -O 10.0.2.254

Starting Nmap 7.01 ( https://nmap.org ) at 2017-01-06 14:25 CET
Nmap scan report for 10.0.2.254
Host is up (0.00011s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
3128/tcp open  squid-http
4443/tcp open  pharos
8002/tcp open  teradataordbms
MAC Address: 14:CC:20:00:07:30 (Tp-link Technologies)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (89%), FreeBSD 6.X|10.X (89%), Linux 2.6.X (89%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:freebsd:freebsd:6.3 cpe:/o:linux:linux_kernel:2.6.29 cpe:/o:freebsd:freebsd:10.1
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0 (89%), FreeBSD 6.3-RELEASE (89%), Linux 2.6.29 (89%), FreeBSD 10.1-RELEA
SE (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

On peut voir dans l'exemple ci-dessus que j'ai scanné le serveur pfsense qui est sur l'adresse 10.0.2.254.

La commande me sers donc les ports d'ouverts sur la machine, ainsi que l'adresse MAC, l'OS (bien que le résultat soit des approximations en pourcentage) et le nombre de sauts qu'il a fallu pour accéder a la machine.

Si l'on dispose d'un serveur DNS, on peut rentrer le nom FQDN de la machine, le résultat sera le même.

Cependant, pour découvrir les machines présentes sur un réseau, il faudrait pouvoir scanner une plage d'adresse IP et voir tous les résultats que la commande peut nous sortir. Il est possible de le faire grâce a la commande suivante :

```
utilisateur@utilisateur-System-Product-Name:~$ sudo nmap -O 10.0.2.0/24
```

Le /24 dit que l'on veut scanner toutes les adresses sur le réseau 10.0.2.0, il va scanner toute la plage d'adresse.

Si l'on veut scanner un nombre d'adresses IP précises, il faut utiliser la syntaxe suivante :

nmap -O 10.0.2.0-n (n étant le nombre d'adresses que l'on veut scanner)

Interface graphique

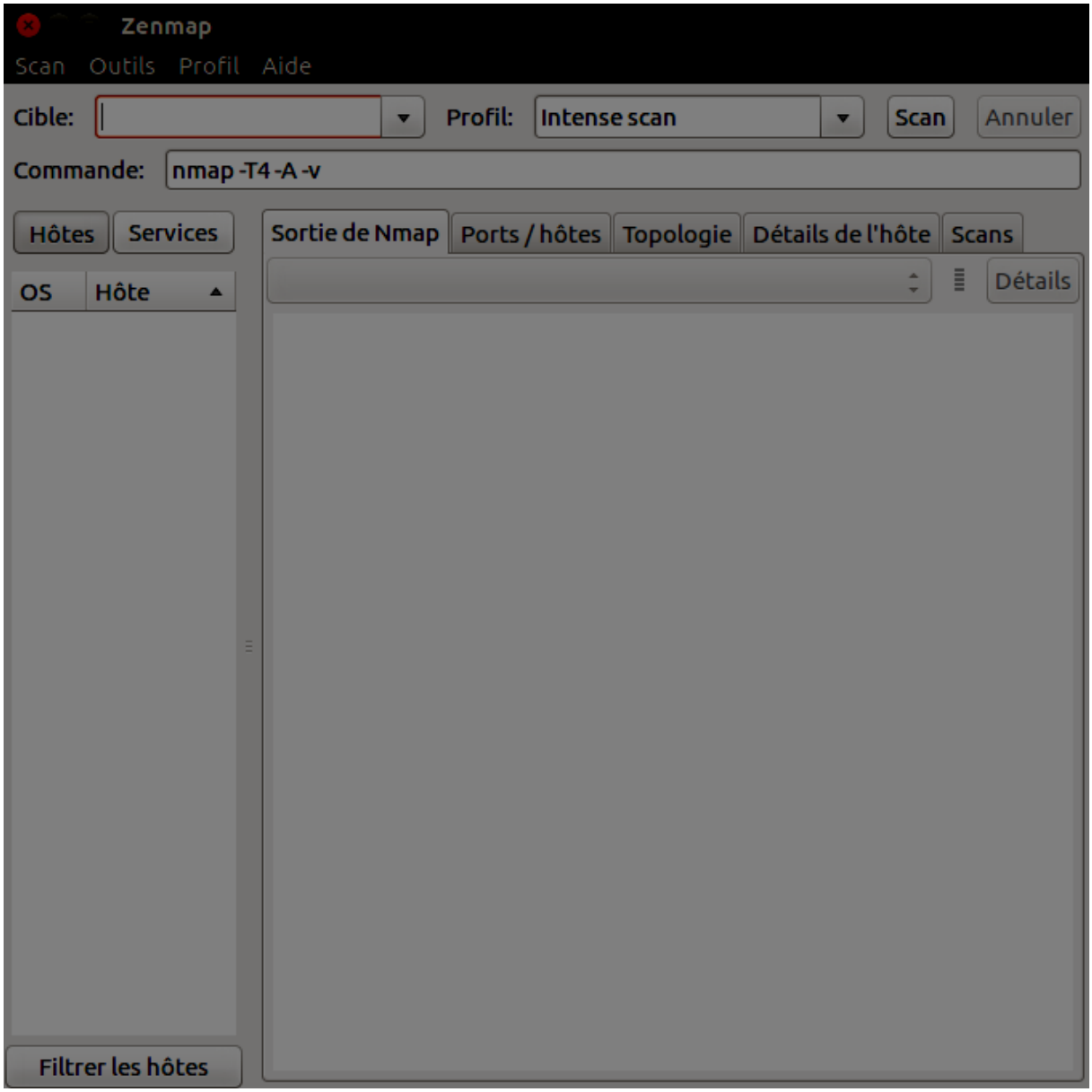
Il existe une interface graphique pour Nmap qui se nomme ZenMap, celle-ci est installable avec la commande suivante :

```
utilisateur@utilisateur-System-Product-Name:~$ sudo apt-get install zenmap
```

Une fois l'installation terminée, il faut taper la commande suivante afin de lancer l'interface :

```
utilisateur@utilisateur-System-Product-Name:~$ sudo zenmap
```

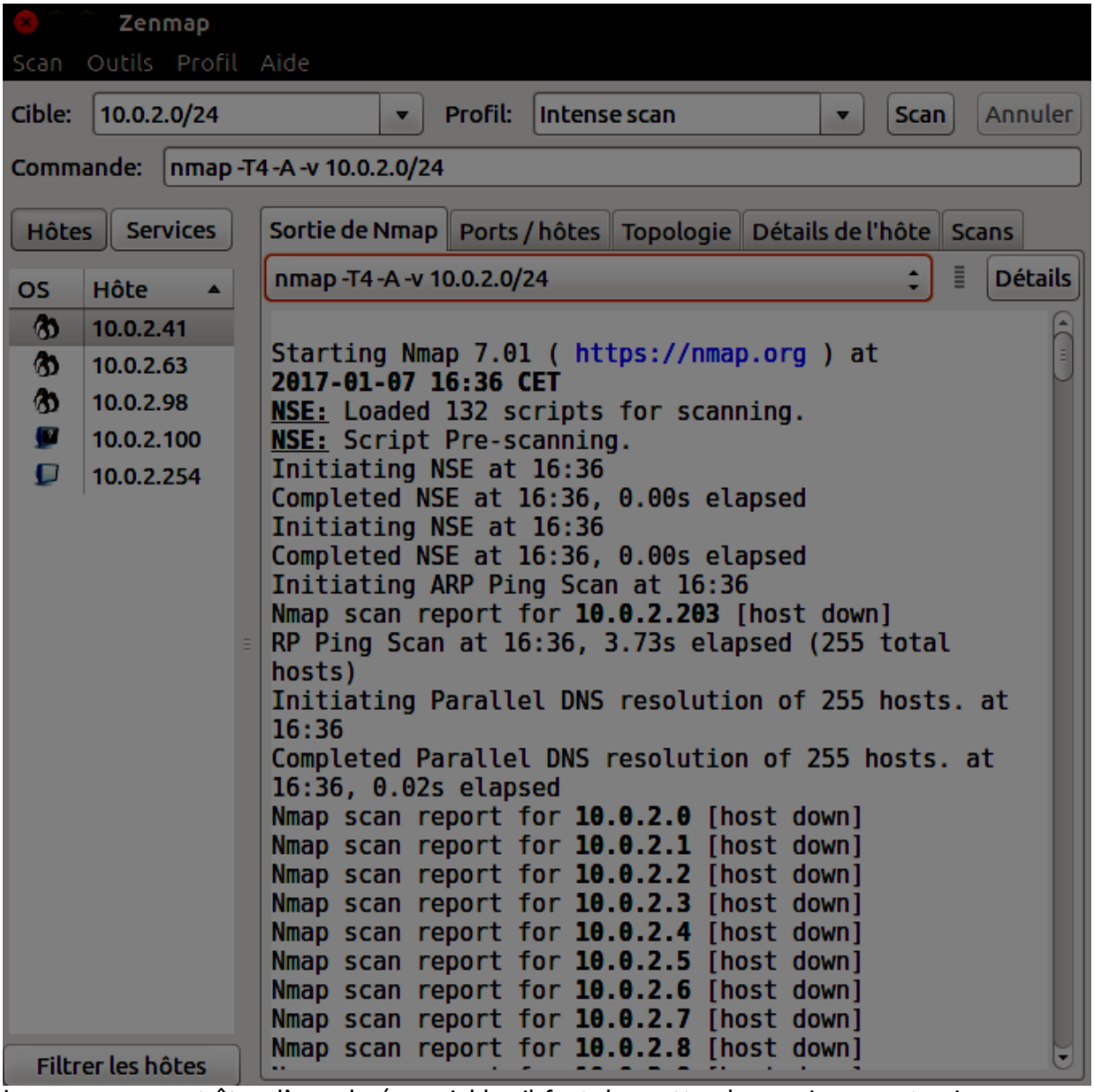
Une fois cette commande lancée, l'interface graphique s'ouvre :



Dans le champ « Cible », on rentre ce que l'on veut scanner, comme dans Nmap en ligne de commandes.

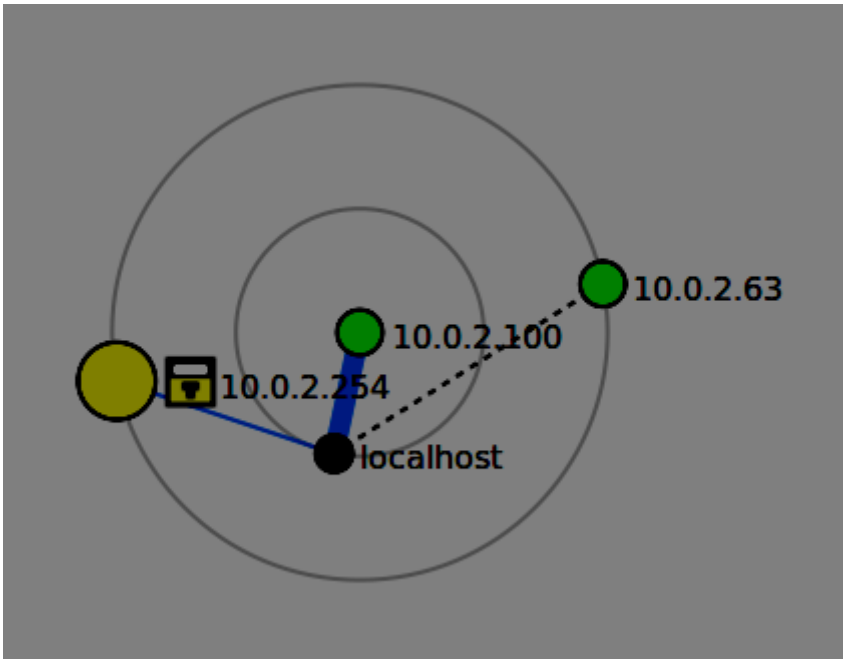
On peut ensuite choisir les paramètres que l'on veut ajouter, mais l'intense scan donne assez de réponses.

Une fois que l'on a configuré ce que l'on veut, on clique sur le bouton « Scan » :



Les scans peuvent être d'une durée variable, il faut donc attendre, mais on peut voir l'avancement du scan dans la fenêtre du milieu.

Une fois fini, on peut aller dans les différents onglets pour voir les résultats du scan, il y a même un onglet Topologie pour avoir un aperçu visuel :



On peut aussi sauvegarder les scans effectués en allant dans l'onglet «Scan» puis cliquer sur « Sauvegarder le scan », ce qui l'enregistrera au format xml.