Prise d'empreinte

Banner Grabbing

Le but de cette démarche est d'envoyer une requête de connexion afin d'avoir le retour sur la bannière du service.

1.Netcat

On utilise Netcat pour envoyer une requête de connexion (netcat peut aussi permettre la création d'un socket).

Listez les options de netcat

```
root@kali:~# nc -h
```

Connexion sur le port 22 sur la machine 192.168.2.1 sans résolution DNS.

```
root@kali:~# nc -vn 192.168.2.1 22
```

```
(UNKNOWN) [192.168.2.1] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

On dispose donc du Service, OpenSSH ainsi que de la version 4.7. Il est donc possible de vérifier si cette version possède des failles.

Coupez la connexion (CTRL + C)

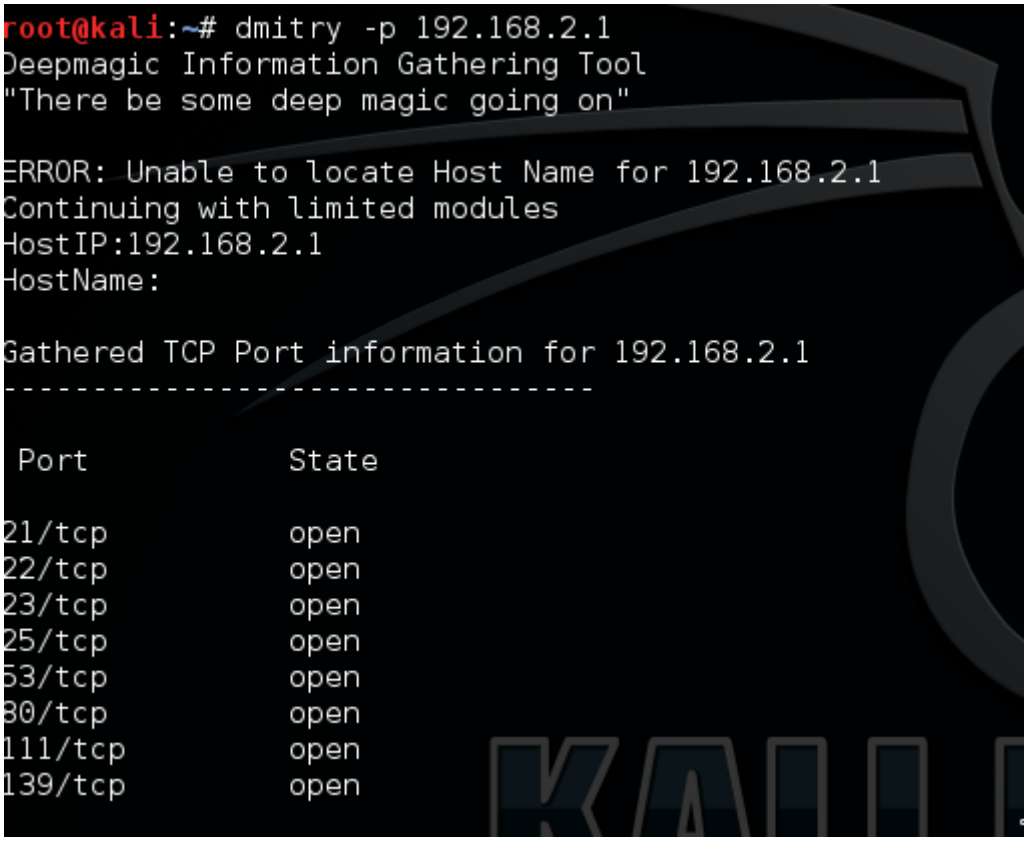
Faire de même pour différents ports relevés avec le scan TCP/UDP

Exemple :

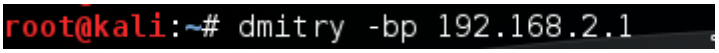
```
root@kali:~# nc -vn 192.168.2.1 21
(UNKNOWN) [192.168.2.1] 21 (ftp) open
220 (vsFTPd 2.3.4)
```

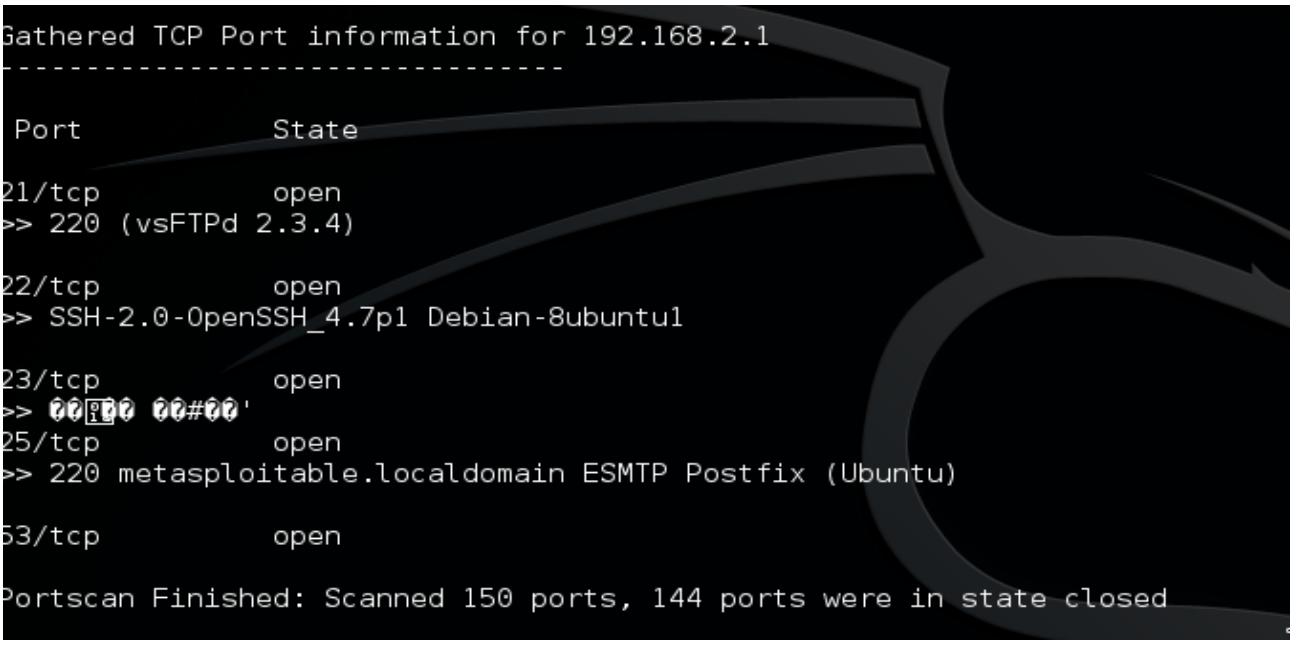
2.Dmitry

Il est possible d'exécuter un rapide scan TCP avec dmitry sur les 150 ports les plus utilisés.



Il est aussi possible de rajouter l'option -b pour récupérer les bannières.

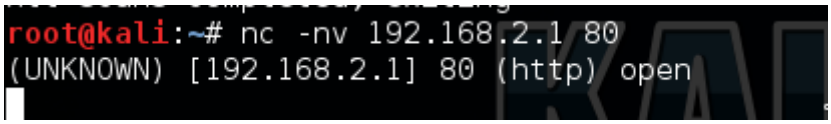




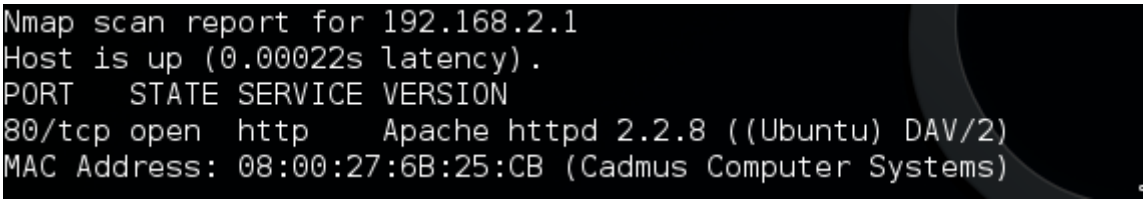
Il y a des informations sur le SMTP.

Analyse des Services

On remarque que si on utilise seulement la technique du banner grabbing, il y a plusieurs ports où il n'y a aucun retour d'informations.



Pour cela il faut utiliser la fonction -sV de nmap



Nmap retourne donc le Service Apache et la version 2.2.8

Il est possible de scanner les 1000 premiers ports

```
root@kali:~# nmap 192.168.2.1 -sV
```

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  shell?
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

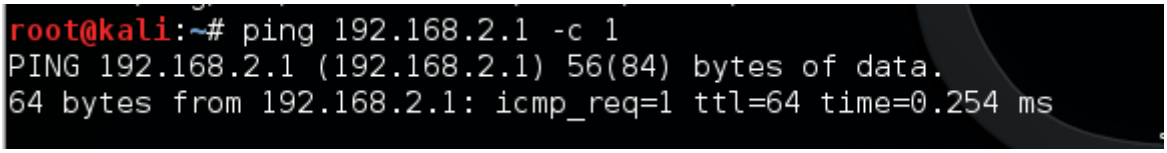
Détection du systéme d'exploitation

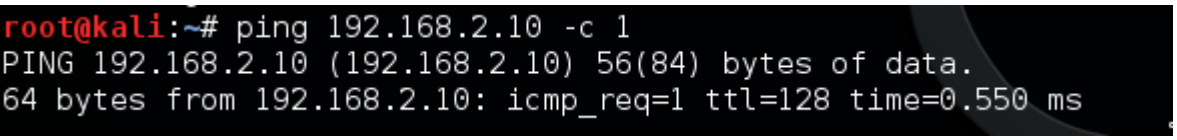
1. Ping

Il est possible de détecter le système d'exploitation via le protocole ICMP.
Chaque système d'exploitation dispose d'un ttl par défaut :
Windows : 128
Unix: 64

Cisco :255

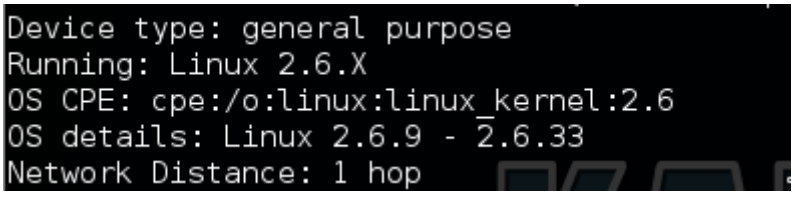
Pingez les adresses 192.168.2.1 et 192.168.2.10, déterminez l'OS.





2.Nmap

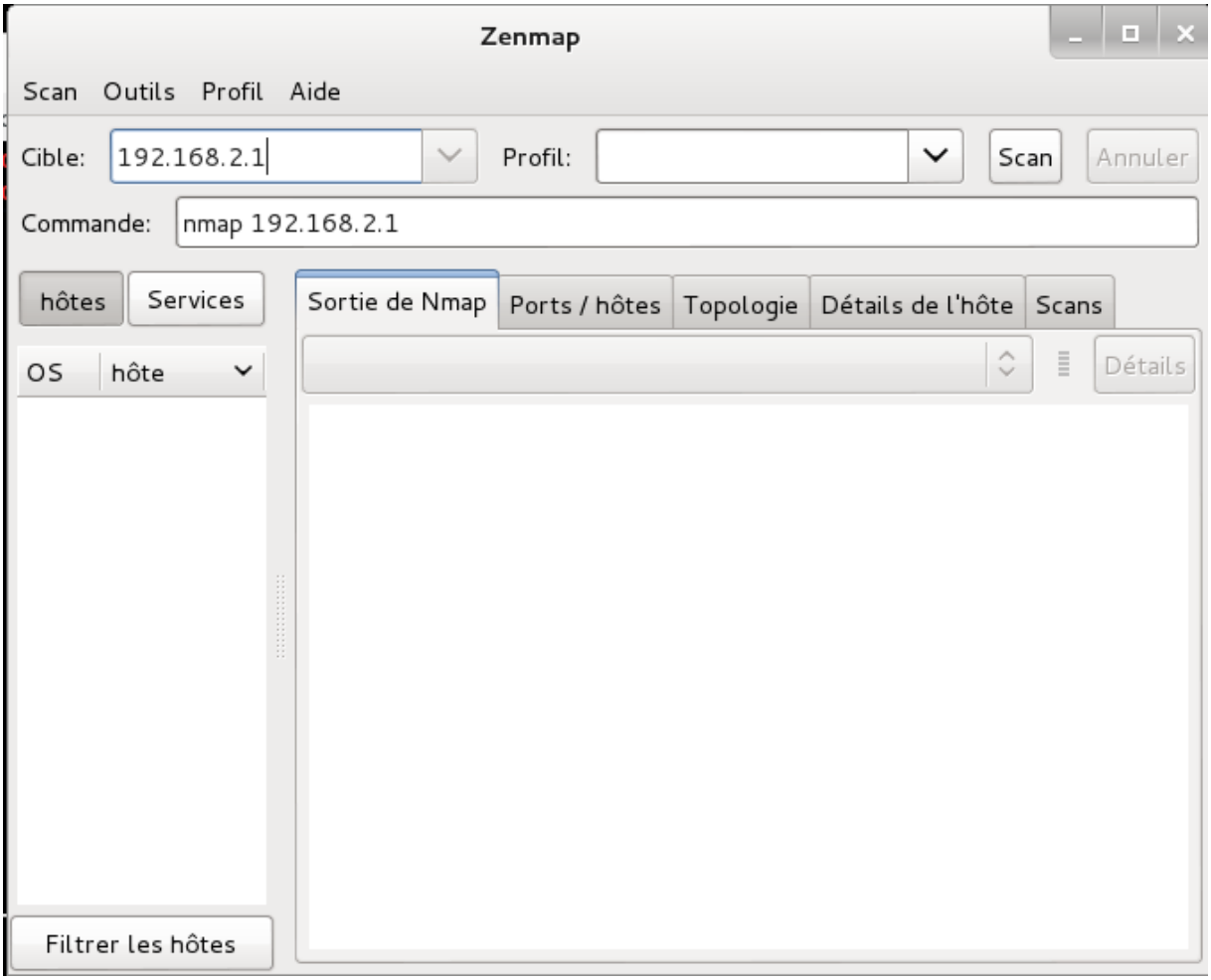
Nmap permet la détection d'un système d'exploitation en fonction des signatures sur les services.



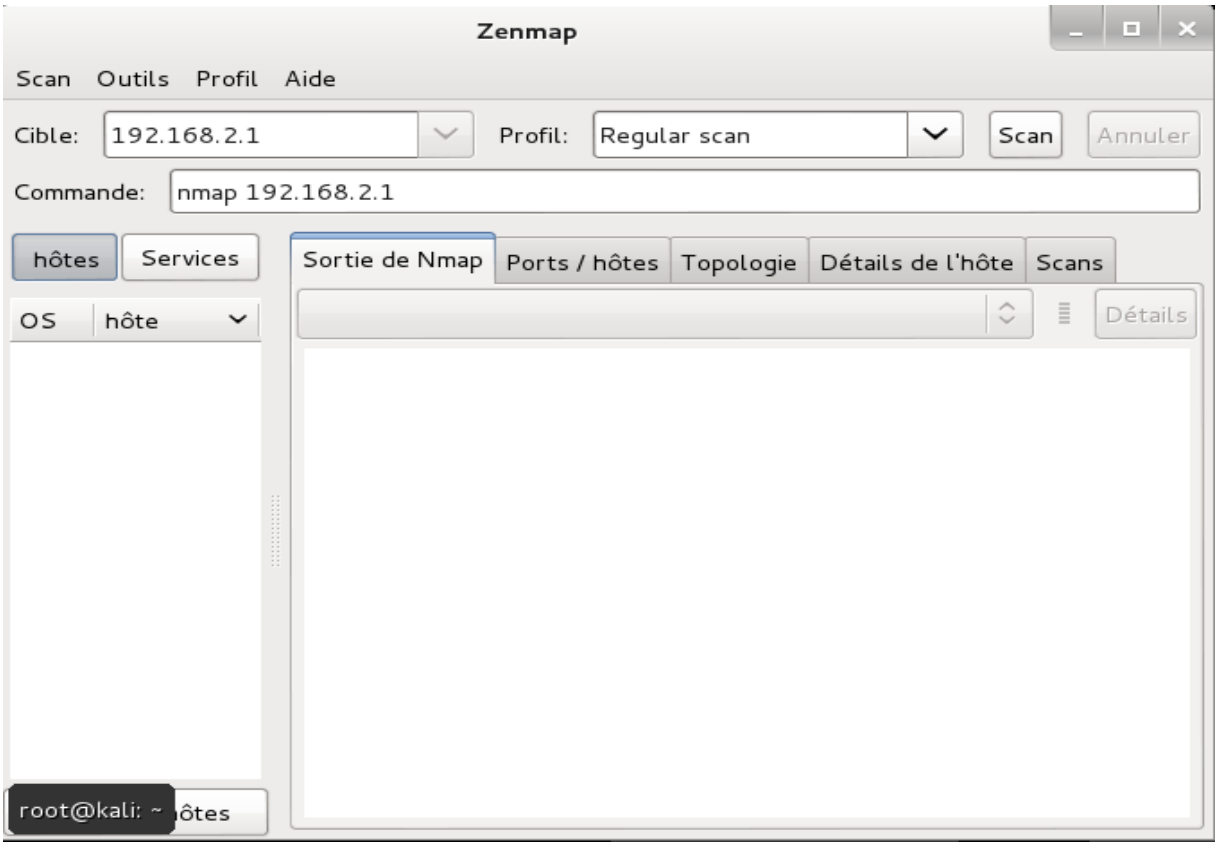
```
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2:professional cpe:/o:microsoft:windows_s
erver_2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
```

ZenMap

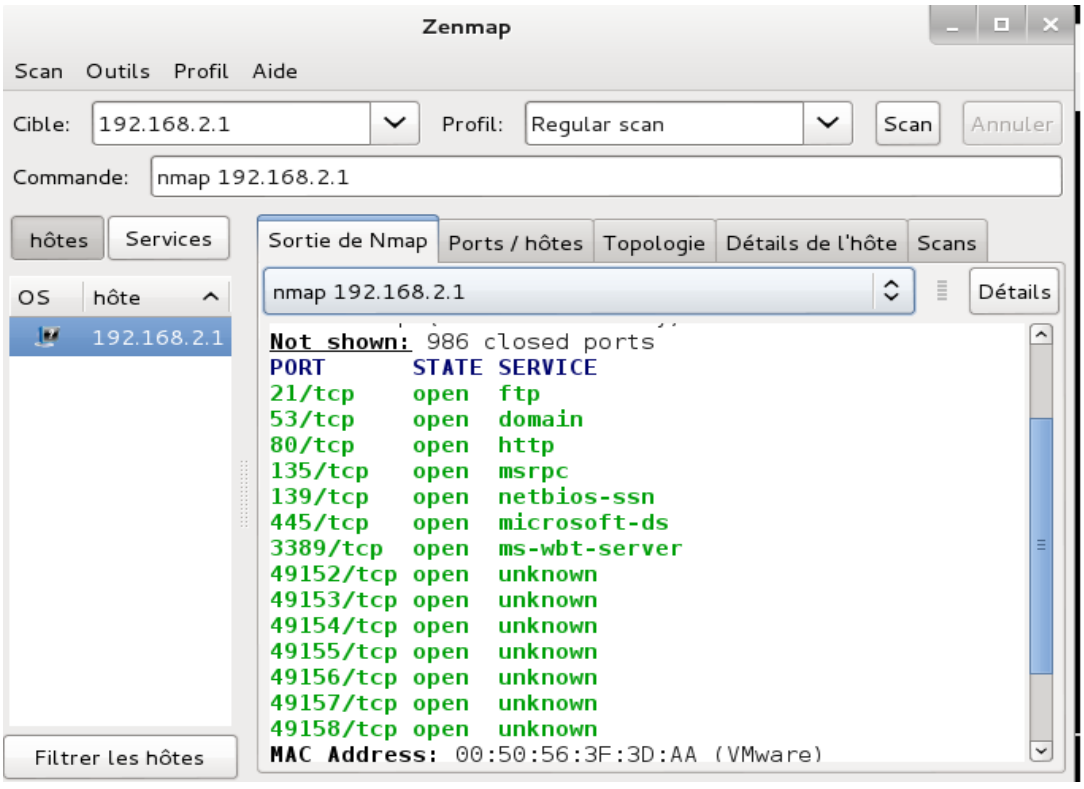
Il existe une interface graphique qui va générer les commandes Nmap.
Pour lancer zenmap :
 # zenmap



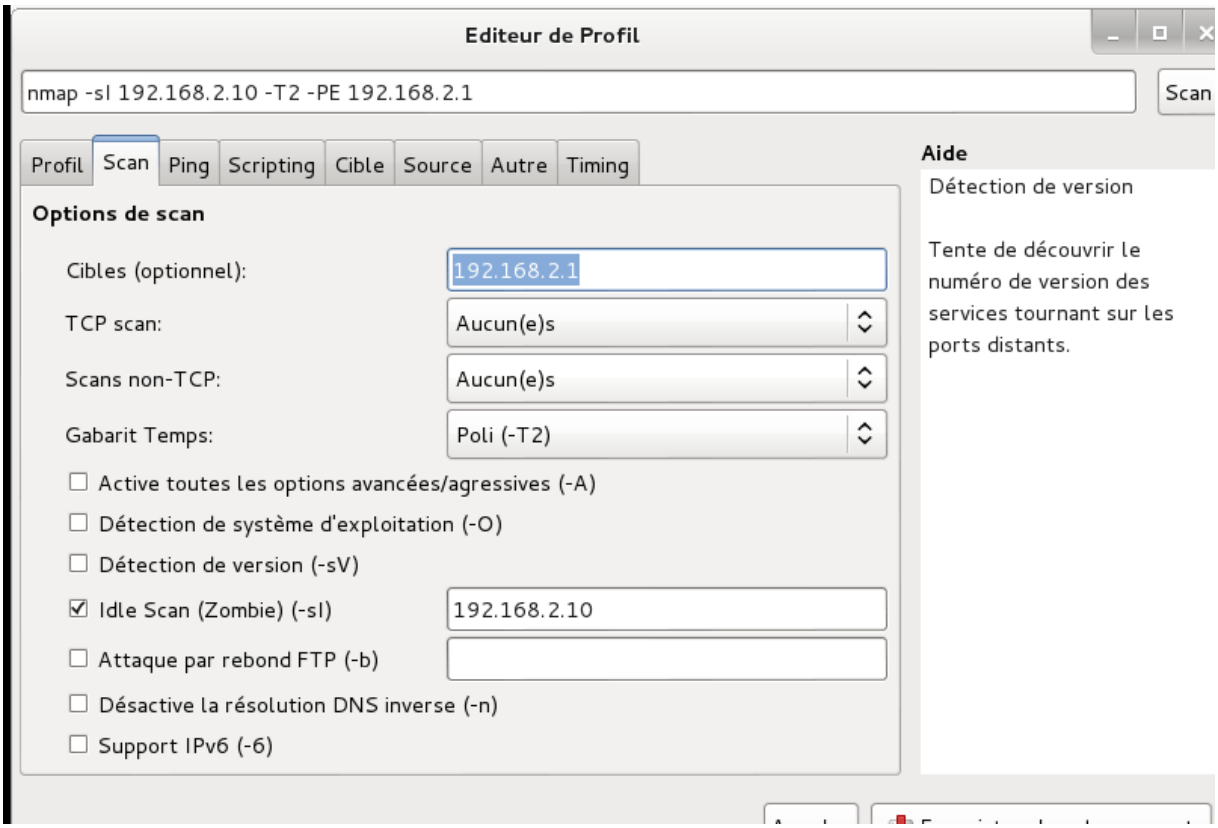
Dans « Cible », tapez l'adresse IP de la cible à scanner. Dans la section « Profil », il y a possibilité de choisir des profils proposés par Zenmap qui générera la commande nmap.
Si dans Profil on sélectionne « Regular Scan » il utilisera la commande basique de nmap (nmap <<IP cible >>)



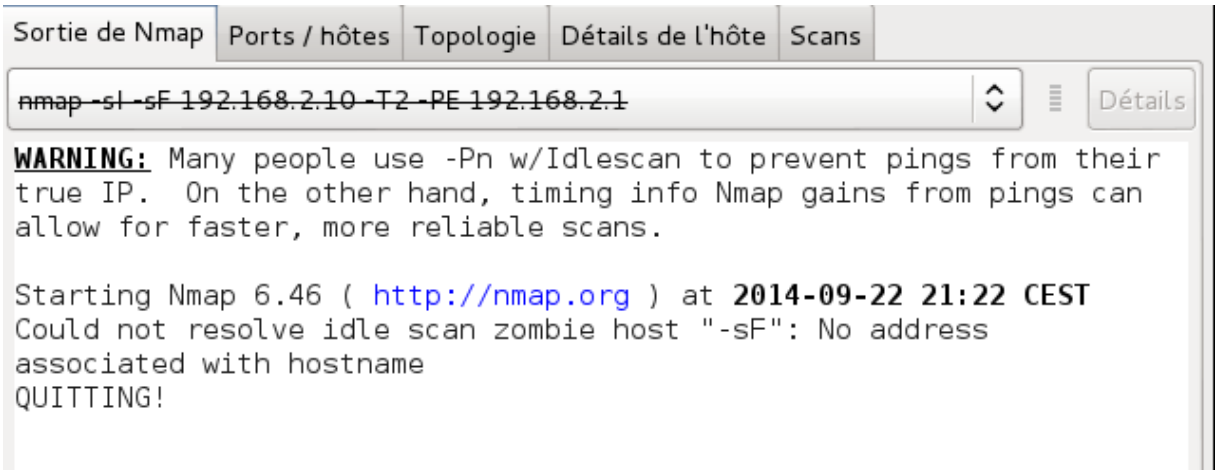
Cliquez sur « Scan ».



Il y a aussi la possibilité de créer ses propres profils en fonction de vos besoins.
Pour ce faire cliquez sur « Profil » ➔ « Nouveau profil ou commande ».
Vous pouvez créer votre profil en sélectionnant vos options, Zenmap se chargera de générer la commande Nmap.
Exemple :



Cette commande va exécuter un scan en utilisant comme machine zombie la 192.168.2.10, avec la vitesse Polite (T2), en effectuant un ping avant le scan pour vérifier si l'hôte est bien actif. Il vous sera possible d'enregistrer le profil (en bas à droite) ou de lancer simplement la commande.
Si votre commande n'est pas réalisable, cela vous sera affiché au lancement du scan.


Sortie de Nmap
Ports / hôtes
Topologie
Détails de l'hôte
Scans
nmap -sI -sF 192.168.2.10 -T2 -PE 192.168.2.1
Détails
WARNING: Many people use -Pn w/Idlescan to prevent pings from their true IP. On the other hand, timing info Nmap gains from pings can allow for faster, more reliable scans.
Starting Nmap 6.46 (http://nmap.org) at 2014-09-22 21:22 CEST
Could not resolve idle scan zombie host "-sF": No address associated with hostname
QUITTING!