TP3 – SCANNING

A. SCAN DE PORTS ET DE SERVICES RÉSEAU : NMAP

Installation de nmap

```
nathan@nathan-VirtualBox:~$ sudo apt-get install nmap
[sudo] Mot de passe de nathan :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libblas3 liblinear4 lua-lpeg nmap-common
Paquets suggérés :
```

Test de nmap sur ma machine

```
nathan@nathan-VirtualBox:~$ nmap -option 192.168.56.106
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 14:28 CET
Nmap scan report for nathan-VirtualBox (192.168.56.106)
Host is up (0.000089s latency).
All 1000 scanned ports on nathan-VirtualBox (192.168.56.106) are closed

Nmap done: 1 IP address (1 host up) scanned in 3.53 seconds
nathan@nathan-VirtualBox:~$
```

Tous les ports sont fermés sur cette machine

Test nmap -O

```
nathan@nathan-VirtualBox:~$ sudo nmap -O 192.168.56.106
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 14:31 CET
Nmap scan report for nathan-VirtualBox (192.168.56.106)
Host is up (0.000052s latency).
All 1000 scanned ports on nathan-VirtualBox (192.168.56.106) are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
nathan@nathan-VirtualBox:~$
```

Tous les ports sont fermés sur cette machine mais pas sur celle-ci :

```
kali@kali:~$ sudo nmap -O 10.16.40.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 10:57 EDT
Nmap scan report for 10.16.40.210
Host is up (0.21s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
88/tcp   open  kerberos-sec
110/tcp  open  pop3
143/tcp  open  imap
445/tcp  open  microsoft-ds
993/tcp  open  imaps
995/tcp  open  pop3s
3031/tcp open  eppc
5900/tcp open  vnc
No exact OS matches for host (If you know what OS is running on it, see h
ttps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/26%OT=22%CT=1%CU=41540%PV=Y%DS=2%DC=I%G=Y%TM=5F96
E4
OS:17%P=x86_64-pc-linux-gnu)SEQ(SP=12%GCD=FA00%ISR=9C%TI=I%CI=RD%TS=U)OPS
(O
OS:1=M5B4%O2=M5B4%O3=M5B4%O4=M5B4%O5=M5B4%O6=M5B4)WIN(W1=FFFF%W2=FFFF%W3=
FF
OS:FF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=N%T=41%W=FFFF%O=M5B4%CC=N%Q=)T1(
R=
OS:Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=N%T=100%W=0%S=Z%A=S%F=AR%O
=%
OS:RD=0%Q=)T3(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T4(R=Y%DF=N%T=1
00
OS:%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=
0%
OS:Q=)T6(R=Y%DF=N%T=100%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=N%T=100%W=0%
S=
OS:Z%A=S%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=34%IPL=148%UN=0%RIPL=G%RID=G%RIPCK
=G
OS:%RUCK=G%RUD=G)IE(R=N)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
```

Test nmap -sS

```
nathan@nathan-VirtualBox:~$ sudo nmap -sS 192.168.56.106
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 14:33 CET
Nmap scan report for nathan-VirtualBox (192.168.56.106)
Host is up (0.0000040s latency).
All 1000 scanned ports on nathan-VirtualBox (192.168.56.106) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

```
kali@kali:~$ sudo nmap -sS 10.16.40.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 10:55 EDT
Nmap scan report for 10.16.40.210
Host is up (0.0052s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 25.74 seconds
```

Test nmap -P0

```
nathan@nathan-VirtualBox:~$ sudo nmap -P0 192.168.56.106
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 14:32 CET
Nmap scan report for 192.168.56.106
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.56.106 are closed

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds
```

```
kali@kali:~$ nmap -P0 16.10.40.210
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 11:05 EDT
Nmap scan report for 16.10.40.210
Host is up (0.0036s latency).
Not shown: 995 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
993/tcp open  imaps
995/tcp open  pop3s
```

1-POURQUOI UTILISE-T-ON L'OPTION P0 ?

Ne pas essayer de ping sur les hôtes avant de les analyser. Cela permet l'analyse des réseaux qui ne permettent pas les requêtes ou les réponses ICMP à travers leurs pares-feux. Microsoft.com en est un exemple, et vous devez toujours utiliser -P0 ou -PT80 pour faire une analyse de port sur microsoft.com.

2-QUELS SONT LES DIFFERENTS TYPES DE SCAN UTILISÉS PAR NMAP ?

Les différents types de scan sont : TCP SYN scan (-sS) / TCP connect() scan (-sT) / Stealth FIN, Xmas Tree, ou Null scan modes (-sF, -sX, -sN) / Ping scanning (-sP) / UDP scans (-sU) / IP protocol scans (-sO) / scan paresseux (-sI) / ACK scan (-sA) / Window scan (-sW) / RPC scan (-sR) / scan-liste (-sL) / attaque par rebond FTP (-b)

Pour plus d'informations sur les types de scan : http://www.delafond.org/traducmanfr/man/man1/nmap.1.html

3-QUELLE LA DIFFÉRENCE ENTRE LES ASPECTS CLOSED ET FILTERED ?

En closed, un port fermé est accessible (il reçoit et répond aux paquets émis par Nmap), mais il n'y a pas d'application en écoute alors qu'en filtered, Nmap ne peut pas toujours déterminer si un port est ouvert car les dispositifs de filtrage des paquets empêchent les paquets de tests (probes) d'atteindre leur port cible.

Plus d'informations ici : https://nmap.org/man/fr/man-port-scanning-basics.html

4-ON SOUHAITE FAIRE UN SCAN POUR IDENTIFIER LES SERVEURS BASES DE DONNÉES DANS UN RÉSEAU, ÉCRIVEZ LA COMMANDE ADÉQUATE

Open a terminal and enter the following command:

$ nmap -p3306 --script mysql-databases --script-args mysqluser= <user>,mysqlpass=<password> <target>

The databases should be listed under the script results:

```
3306/tcp open  mysql
| mysql-databases:
|   information_schema
|   temp
|   websec
|   ids
|_  crm
```

B. IDENTIFICATION AUTOMATIQUE DES VULNÉRABILITÉS : NESSUS

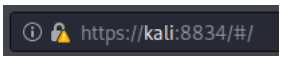
Installation de Nessus

```
kali@kali:~$ cd Downloads/
kali@kali:~/Downloads$ ls
Nessus-8.12.0-debian6_amd64.deb  Nessus-8.12.0-debian6_amd64.deb.part
kali@kali:~/Downloads$ ls
Nessus-8.12.0-debian6_amd64.deb
kali@kali:~/Downloads$ sudo dpkg -i Nessus-8.12.0-debian6_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 276117 files and directories currently installed.)
Preparing to unpack Nessus-8.12.0-debian6_amd64.deb ...
Unpacking nessus (8.12.0) ...
Setting up nessus (8.12.0) ...
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner

kali@kali:~/Downloads$
```

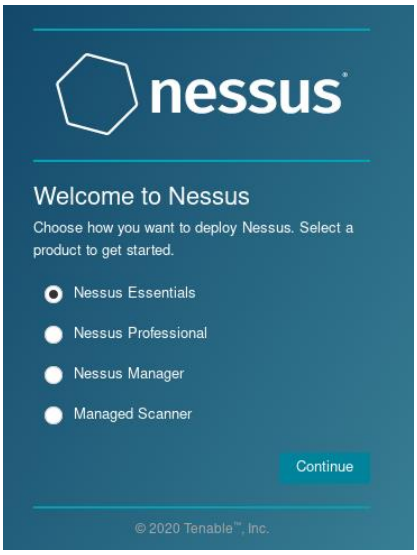
Lancement du service

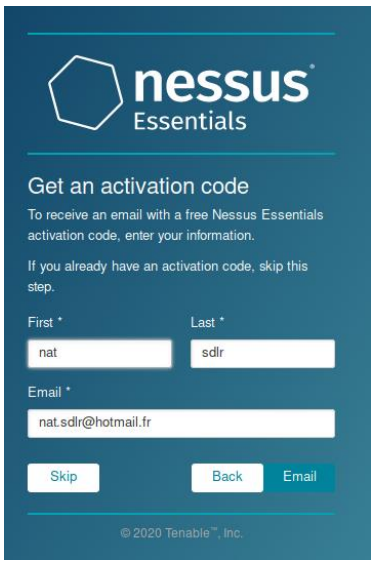
```
kali@kali:~/Downloads$ sudo /bin/systemctl start  nessusd.service
```

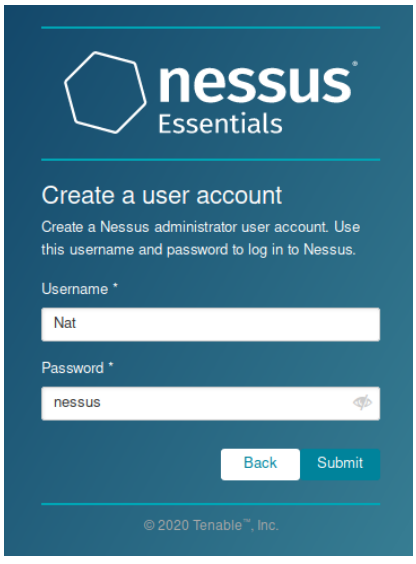
Création du compte



Téléchargement et mise à jour des plugins de Nessus

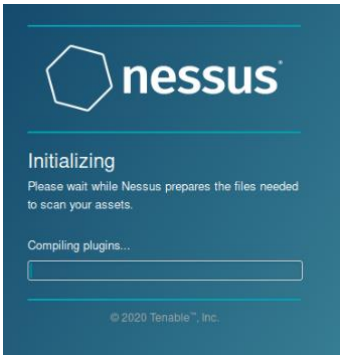




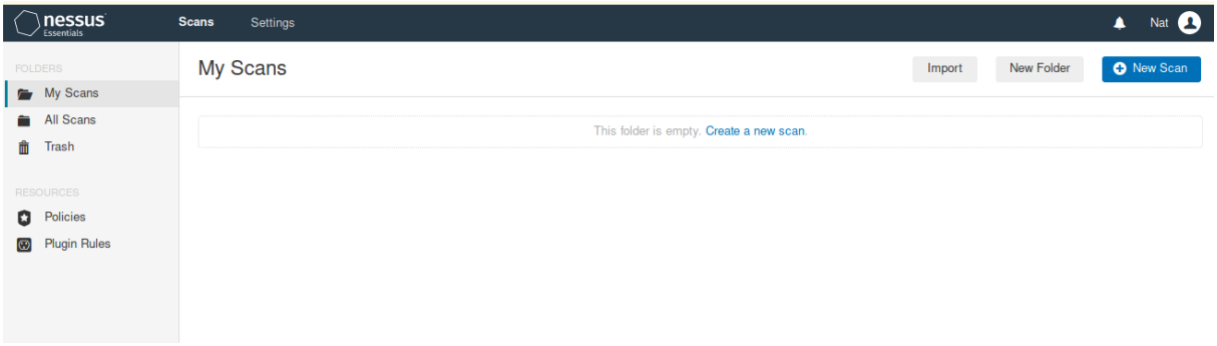


Username : Nat

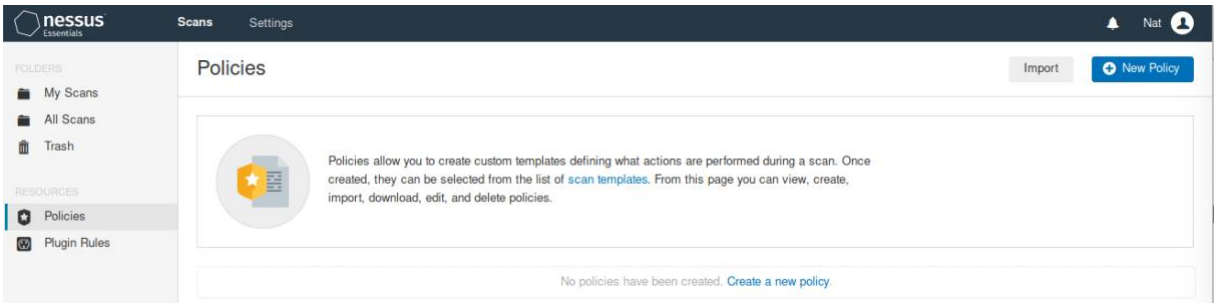
Mdp : nessus

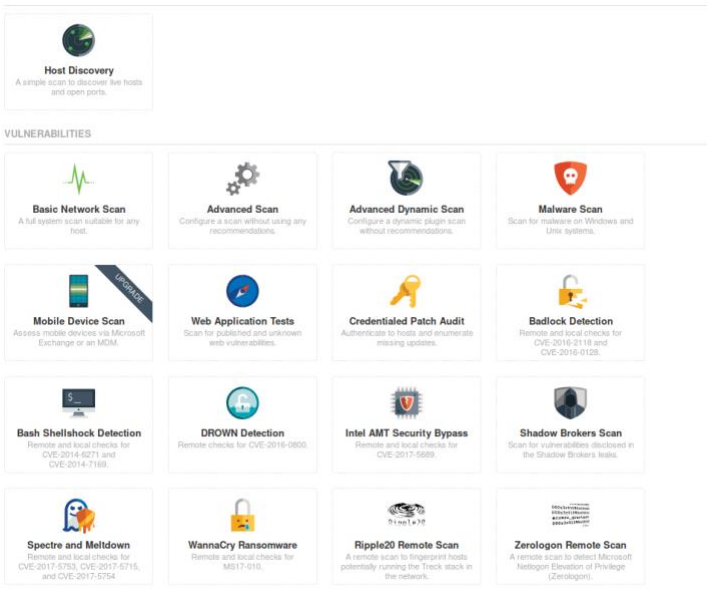


Après le lancement de Nessus nous tombons sur cette interface



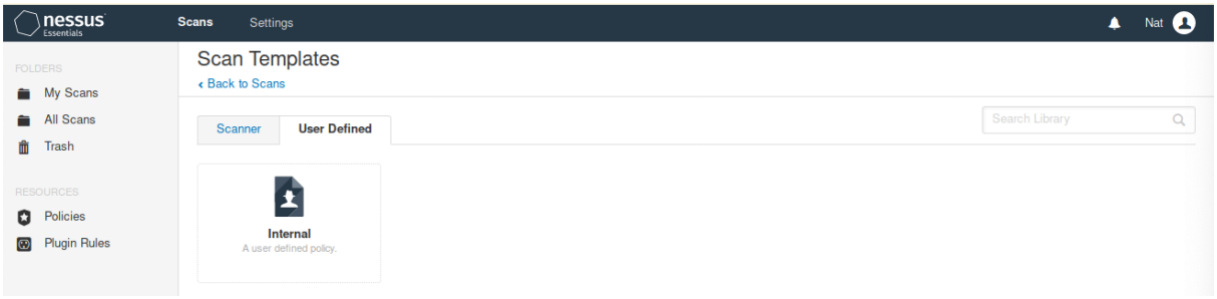
Nous choisissons une policie



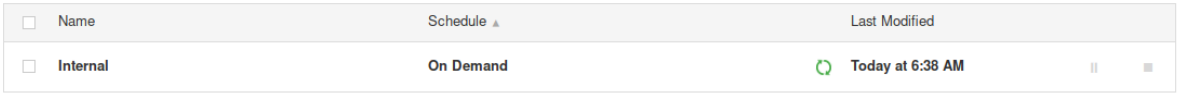


Je choisi Basic Network Scan avec l'option internal pour le type de scan

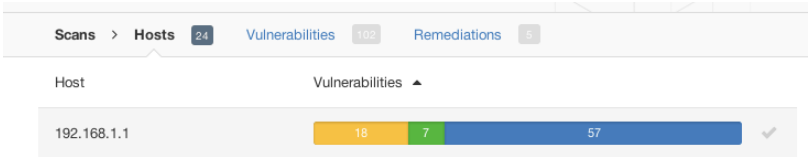
Maintenant, on va créer un nouveau scan avec la policie configurée



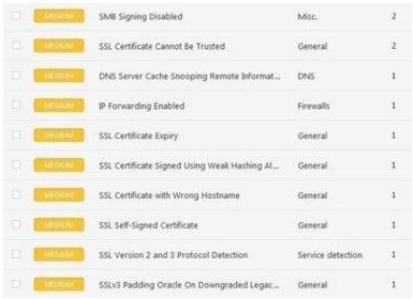
Puis, on lance le scan



On peut voir un rapport détaillé en cliquant sur hôte



On peut voir un rapport détaillé en cliquant sur vulnérabilités



En cliquant sur une vulnérabilité, il y a une description du problème et une possible solution