Mouhamed Messaoud HAMOUD

BTS SIO SISR 2024/2024

Procédure d'installation et de validation de Nmap sous Debian Linux

Objectif : Installer l'outil de cartographie et d'audit réseau Nmap sur le serveur de gestion GLPI et RADIUS afin de valider la visibilité des équipements de l'infrastructure dun site A 10.11.19.16/28

1- Mise à jour des dépôts

Avant toute installation, il est nécessaire de synchroniser les index des paquets locaux avec les serveurs distants Debian pour obtenir la version la plus stable.

```
zabbixglpi@glpi-server:~$ su -
Mot de passe :
root@glpi-server:~# apt update
Atteint :1 https://packages.sury.org/php bookworm InRelease
Atteint :2 https://deb.debian.org/debian bookworm InRelease
Atteint :3 https://deb.debian.org/debian bookworm-updates InRelease
Atteint :4 https://security.debian.org/debian-security bookworm-security InRelea
se
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
145 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les
 voir.
```

2- Installation du paquet Nmap

L'installation se fait via le gestionnaire de paquets avancé “**apt**” et l'argument “**-y**” automatise la confirmation de l'installation.

```
root@glpi-server:~# apt install nmap -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessair
es :
  linux-image-6.1.0-25-amd64 linux-image-6.1.0-43-amd64
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
  liblinear4 lua-lpeg nmap-common
Paquets suggérés :
  liblinear-tools liblinear-dev ncat ndiff zenmap
Les NOUVEAUX paquets suivants seront installés :
  liblinear4 lua-lpeg nmap nmap-common
0 mis à jour, 4 nouvellement installés, 0 à enlever et 145 non mis à jour.
Il est nécessaire de prendre 6 127 ko dans les archives.
Après cette opération, 26,6 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://deb.debian.org/debian bookworm/main amd64 liblinear4 amd
64 2.3.0+dfsg-5 [43,6 kB]
Réception de :2 https://deb.debian.org/debian bookworm/main amd64 lua-lpeg amd64
```

```
4 396 ko réceptionnés en 2min 33s (28,7 ko/s)
Sélection du paquet liblinear4:amd64 précédemment désélectionné.
(Lecture de la base de données... 170178 fichiers et répertoires déjà installés.
)
Préparation du dépaquetage de .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Dépaquetage de liblinear4:amd64 (2.3.0+dfsg-5) ...
Sélection du paquet lua-lpeg:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../lua-lpeg_1.0.2-2_amd64.deb ...
Dépaquetage de lua-lpeg:amd64 (1.0.2-2) ...
Sélection du paquet nmap-common précédemment désélectionné.
Préparation du dépaquetage de .../nmap-common_7.93+dfsg1-1_all.deb ...
Dépaquetage de nmap-common (7.93+dfsg1-1) ...
Sélection du paquet nmap précédemment désélectionné.
Préparation du dépaquetage de .../nmap_7.93+dfsg1-1_amd64.deb ...
Dépaquetage de nmap (7.93+dfsg1-1) ...
Paramétrage de lua-lpeg:amd64 (1.0.2-2) ...
Paramétrage de liblinear4:amd64 (2.3.0+dfsg-5) ...
Paramétrage de nmap-common (7.93+dfsg1-1) ...
Paramétrage de nmap (7.93+dfsg1-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u13)
...
```

3- Vérification de la bonne installation

La commande nmap --version permet au système de retourner la version de Nmap ainsi que la plateforme d'exécution.

```
root@glpi-server:~# nmap --version
Nmap version 7.93 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.19 libssh2-1.10.0 libz-1.2.13 libpcre-8.
45 libpcap-1.10.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

4- Test fonctionnel en boucle locale (Localhost)

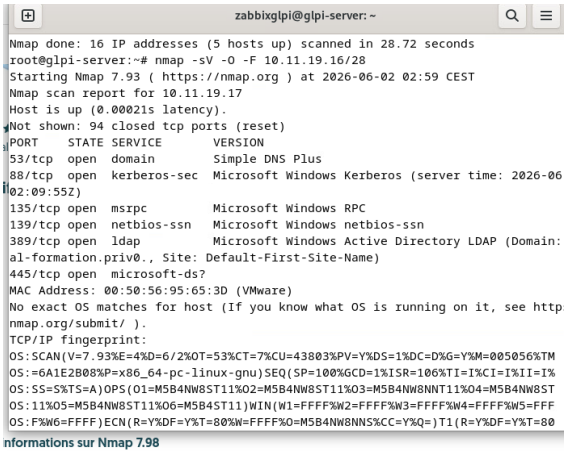
Avant de scanner l'infrastructure à travers les pare-feux PfSense, un premier test de validation est effectué sur la machine elle-même (127.0.0.1). Cela permet de vérifier le bon fonctionnement du moteur de scan.

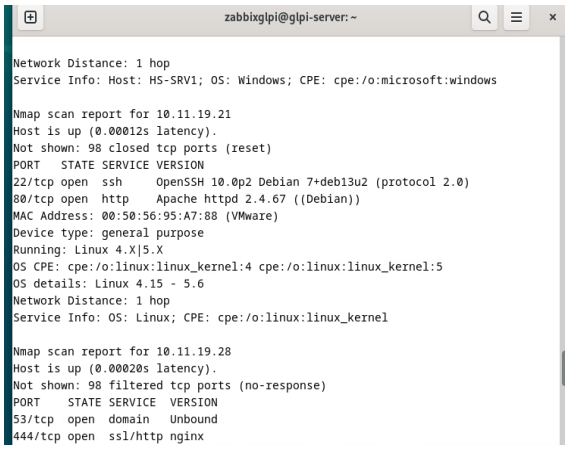
```
root@glpi-server:~# nmap localhost
Starting Nmap 7.93 ( https://nmap.org ) at 2026-06-02 02:04 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
631/tcp  open  ipp
3128/tcp open  squid-http
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

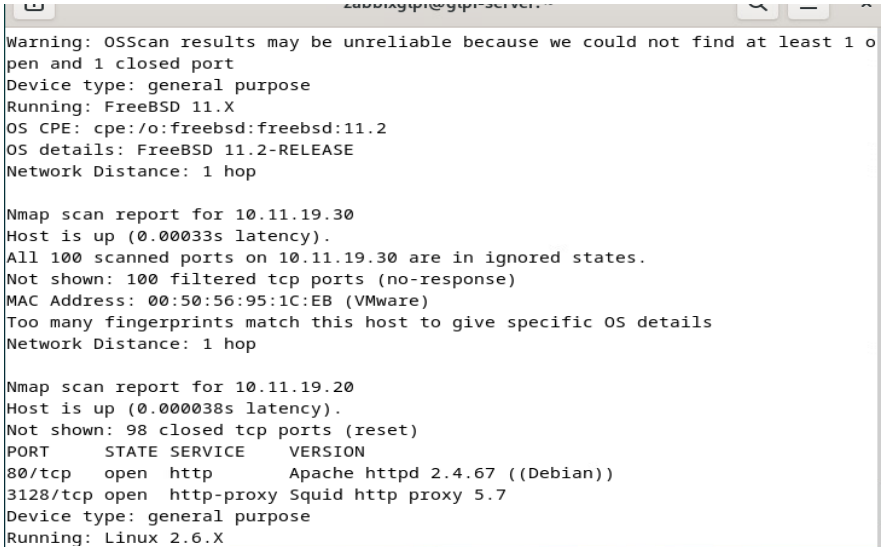
Ce test liste les ports ouverts sur le serveur GLPI (ex: 80/HTTP, 3306/MySQL), confirmant que Nmap écoute et analyse correctement les requêtes réseau.

5- Scan du réseau 10.11.19.16/28

Je lance un scan de détection de système d'exploitation et de services de tout le bloc d'un coup avec l'argument -F (Fast scan, pour que ce soit rapide) combiné avec -O (détection d'OS) et -sV (versions).







```
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: FreeBSD 11.X
OS CPE: cpe:/o:freebsd:freebsd:11.2
OS details: FreeBSD 11.2-RELEASE
Network Distance: 1 hop

Nmap scan report for 10.11.19.30
Host is up (0.00033s latency).
All 100 scanned ports on 10.11.19.30 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
MAC Address: 00:50:56:95:1C:EB (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.11.19.20
Host is up (0.000038s latency).
Not shown: 98 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache httpd 2.4.67 ((Debian))
3128/tcp open  http-proxy Squid http proxy 5.7
Device type: general purpose
Running: Linux 2.6.X
```

Le scan montre que j'ai 5 machines activées sur le réseau 10.11.19.16/28, c'est un bloc de 16 adresses IP.

A- La machine 1 (10.11.19.17) est mon contrôleur de domaine Windows Server car NMAP détecte le port 88 (Kerberos) et le 389 (LDAP) et le domaine focal-formation.priv

B- La machine 2 (10.11.19.21) est une VM debian Zabbix car il y'a la présence des ports 22 et 80 respectivement SSH OpenSSH et Serveur Web Apache qui justifie l'interface web de supervision Zabbix.

C- La machine 3 (10.11.19.28) est mon Pare-feu PfSense. C'est le résultat le plus flagrant car Nmap détecte le système d'exploitation **FreeBSD 11.2** (le cœur de PfSense). De plus, on voit le port **444** (Nginx en HTTPS), qui correspond à l'interface d'administration Web de PfSense (souvent déplacée sur le port 444 ou 8443 pour la sécurité), et le port **53** (Unbound), qui est le résolveur DNS par défaut de PfSense.

D- La machine 4 (10.11.19.30) est un client Windows très sécurisé grâce au pare-feu de windows par défaut qui bloque les pings et les scans de ports.

E- La machine 5 (10.11.19.20) est mon serveur GLPI et RADIUS car on y retrouve le port 80 et 3128 respectivement Apache et mon proxy Squid.

Conclusion

J'ai utilisé Nmap dans une démarche de **sécurité défensive**. Cet outil m'a permis d'adopter temporairement la posture d'un attaquant extérieur pour cartographier ma propre infrastructure. Grâce à cela, j'ai pu valider visuellement que mon pare-feu PfSense segmentait correctement mes réseaux, et que mes postes clients Windows appliquaient bien leur politique de filtrage par défaut.