PERNON Etienne

[Nom de la société]  [Adresse de la société]

[Titre du document]

Table des matières

**Aucune entrée de table des matières n'a été trouvée.**

# FootPrinting

.196 / .222 /

# Analyse des vulnérabilités

# Déroulement des tests

## Découverte du réseau

### Nmap

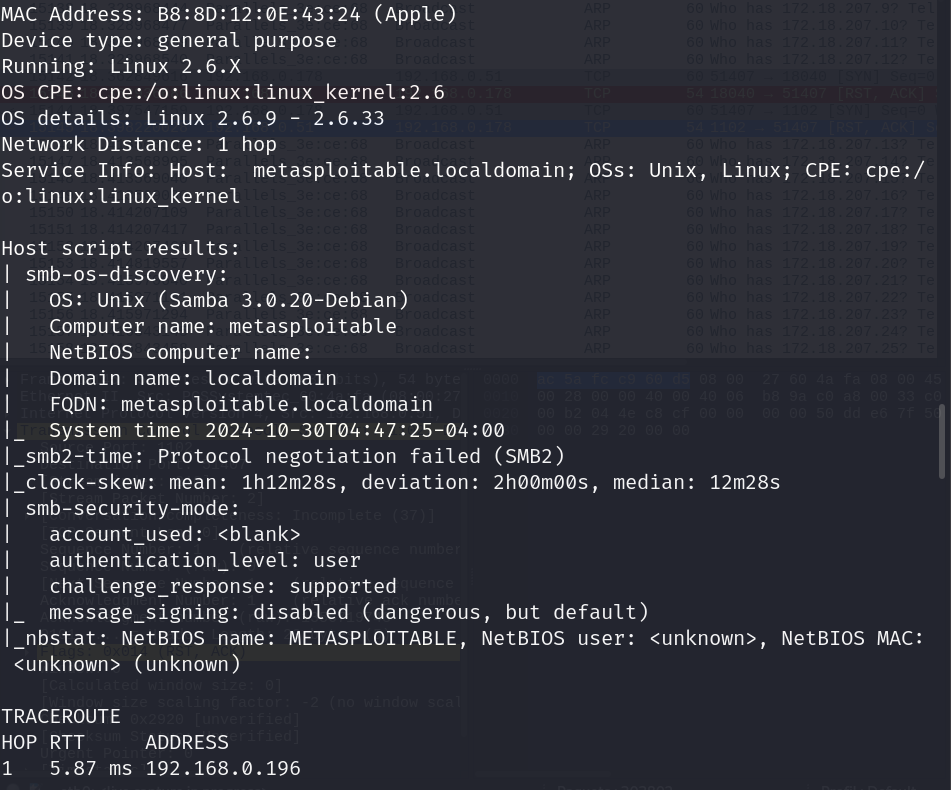
Réalisation d’un scan du réseau avec le logiciel Nmap pour **[explication de la commande]**

* Commande : nmap -A -O -sV -F 192.168.0.0/24

Découverte d’une machine vulnérable

**Description de l’appareil :**

* IP : 192.168.0.196 *(volatile)*
* MAC : B8 :8D :12 :0E :43 :24 *(volatile)*
* Nom : Metasploitable
* Peine : 323.1 / 323.2
* System d’exploitation : linux 2.6.9 / Debian *(justifier samba)*



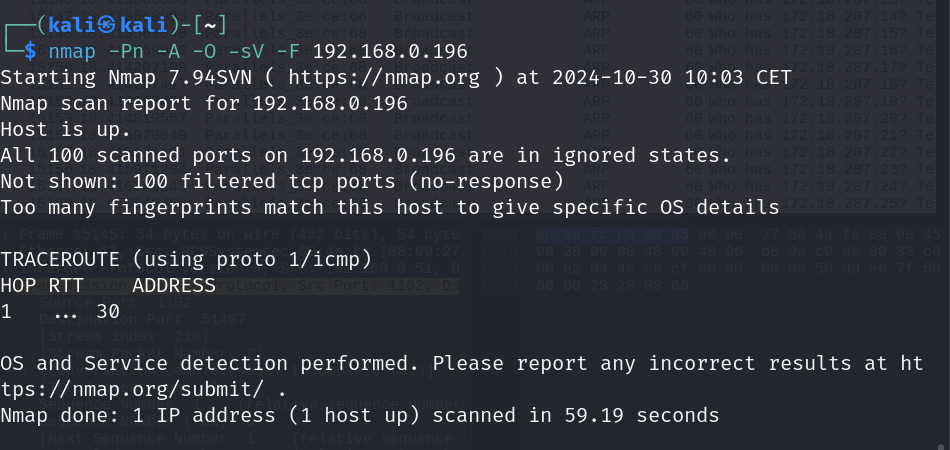
descriptif de la machine : metasploitable

Liste des ports ouvert :

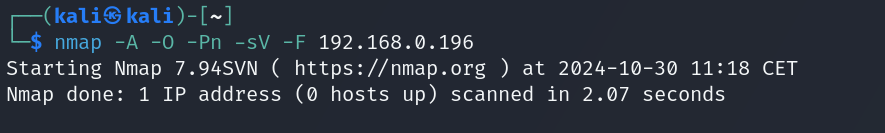
|  |  |
| --- | --- |
|  |  |

Liste des port de la machine metasploitable

* Suite à nos premières requêtes nous avons eu des difficultés à communiquer avec la machine cible



* Suite à nos premières requêtes nous avons été **éjecter à plusieurs reprises** du réseau puis l’adresse IP de la machine suspect a changé



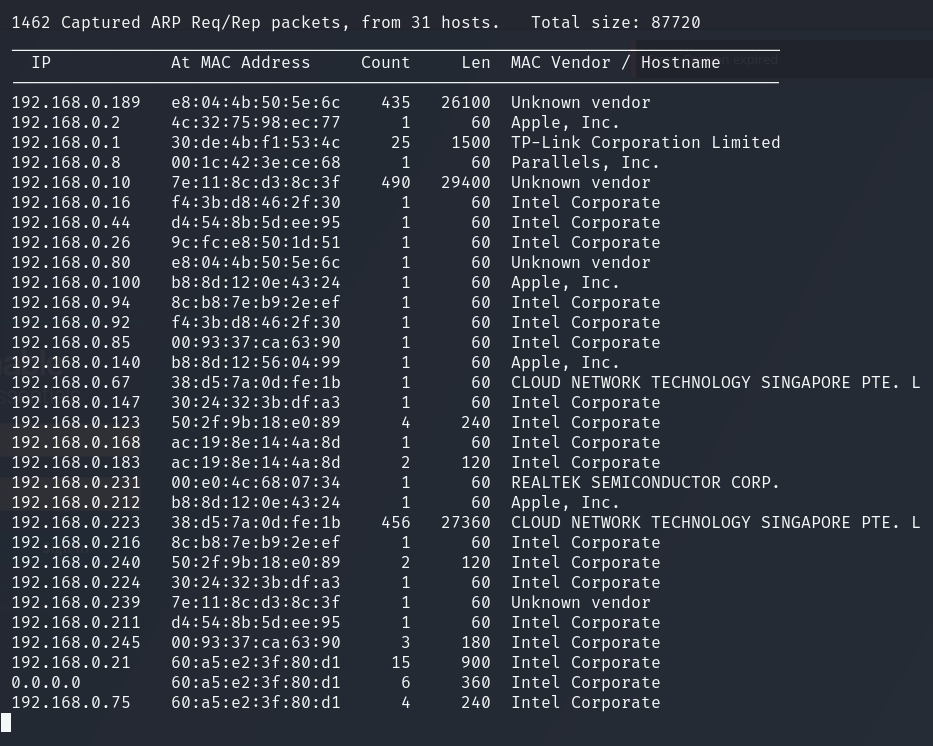
**CONCLUSION :** Nous pouvons donc en conclure que la machine suspecte a accès au service DHCP du réseau « cyber »

Dans le but de mieux connaître le réseau dans lequel notre équipe évolue nous avons décidé de noter les adresses ip de nos machine Host & de nos VM kali présente sur le réseau :

Insert photo

Combiné avec la commande « netdiscover  -p » nous avons pu différencier nos machine de la machine suspect :

**Note :** veuillez exécuter le paramètre -p pour que la recherche de net discover soit en mode passive.



Liste des machine connecté au réseau cyber

Nous avons pu en conclure *(à cette instant)* que la machine suspecte est :

* IP : 192.168.0.100
* MAC : B8 :8D :12 :0E :43 :24

Durant nos tests nous avons constaté que l’adresse MAC de la machine suspect a été modifier, cependant nous n’avons pas eu l’occasion de récolter la preuve de ce changement d’adresse MAC.

## Recherche de vulnérabilité sur la machine suspecte

Une fois que la machine suspecte a été clairement identifier et que nous pouvions la tracer, nous avons lancer les scans de vulnérabilité via Nessus / Nmap.

Dans le navigateur

Via le navigateur nous avons pu se connecter à une interface WEB de la machine suspect :



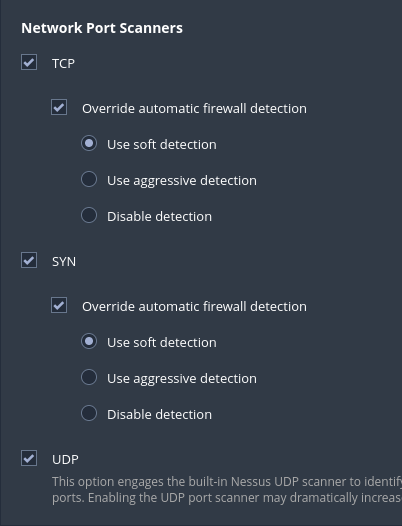
Page web retourne via l’adresse de la machine : metasploitable

**Note :** Nous n’investiguerons pas plus ce moyen de connexion car nous avons l’obligation d’exécuter nos tests en mode passif.

Analyse via Nessus Essential

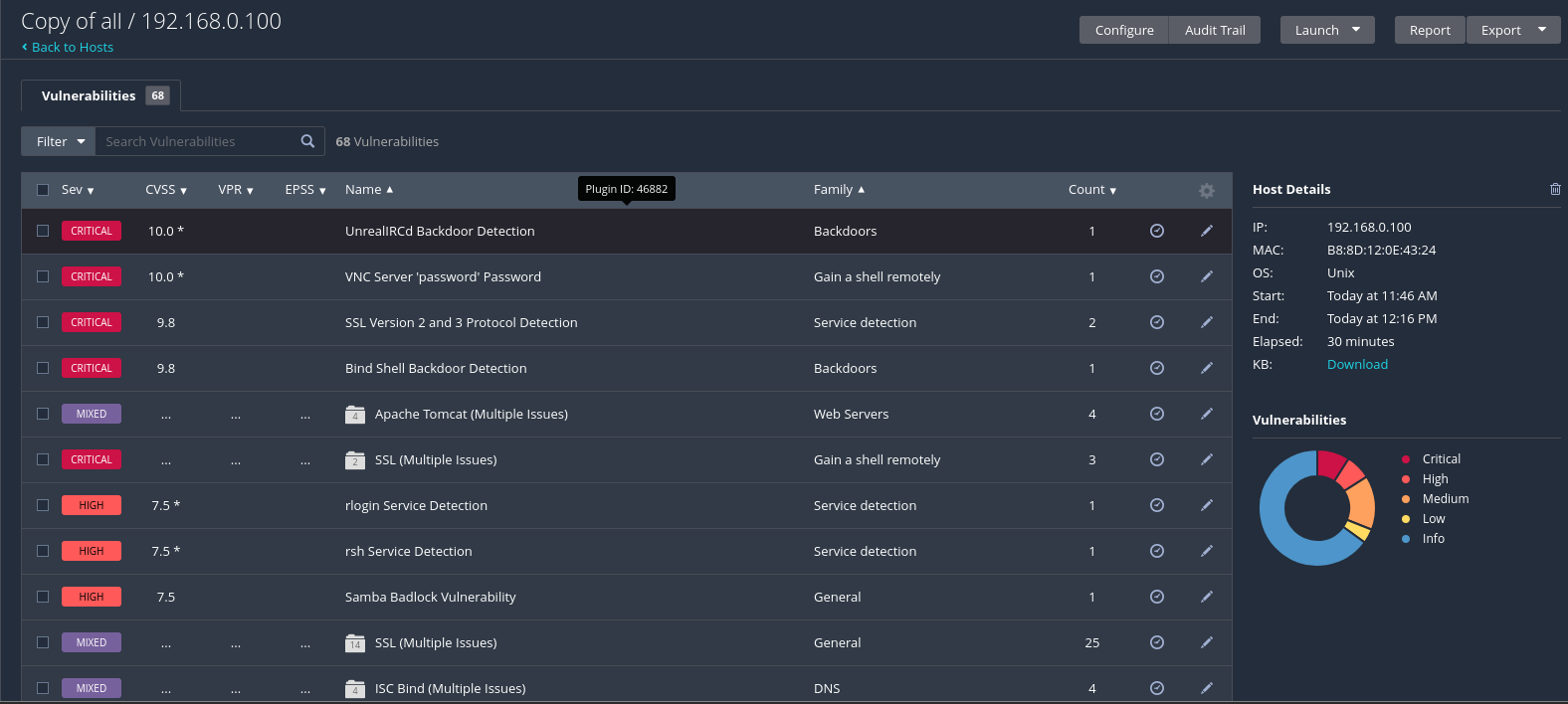
Nous avons lancer un scan avancer via l’application Nessus en version Essential.

Notez que le scan n’a pas été lancé en mode agressif :



Scan avancée : point de configuration important

L’analyse de Nessus a révélé 68 failles de sécurité sur la machine metasploitable. Nous pouvons noter qu’il y a 9% de faille critique dont 3 avec une criticité score de criticité de 10/10.



Vue d’ensemble des vulnérabilité