PERNON Etienne

CCI Campus – ALSACE - Jeu. 31 Oct 2024

Rapport de pentest

Table des matières

[I. Déroulement des tests 2](#_Toc181259704)

[A. Découverte du réseau 2](#_Toc181259705)

[Découverte d’une machine vulnérable : metasploitable 2](#_Toc181259706)

[Traque de la machine metasploitable 6](#_Toc181259707)

[B. Recherche de vulnérabilité sur la metasploitable 8](#_Toc181259708)

[Dans le navigateur 8](#_Toc181259709)

[Analyse via Nessus Essential 9](#_Toc181259710)

[Liste vulnérabilités les plus critique 11](#_Toc181259711)

[Vulnérabilités critique permettant de mettre hors d’état de nuire le hacker 12](#_Toc181259712)

# Déroulement des tests

## Découverte du réseau

Réalisation d’un scan rapide du réseau avec le logiciel Nmap en demandant les services et une analyse de OS *(operating system)* ainsi que les port ouvert.

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

### Découverte d’une machine vulnérable : metasploitable

#### Identification de l’appareil:

* IP : 192.168.0.196 *(volatile)*
* MAC : B8 :8D :12 :0E :43 :24 *(volatile)*
* Nom : Metasploitable

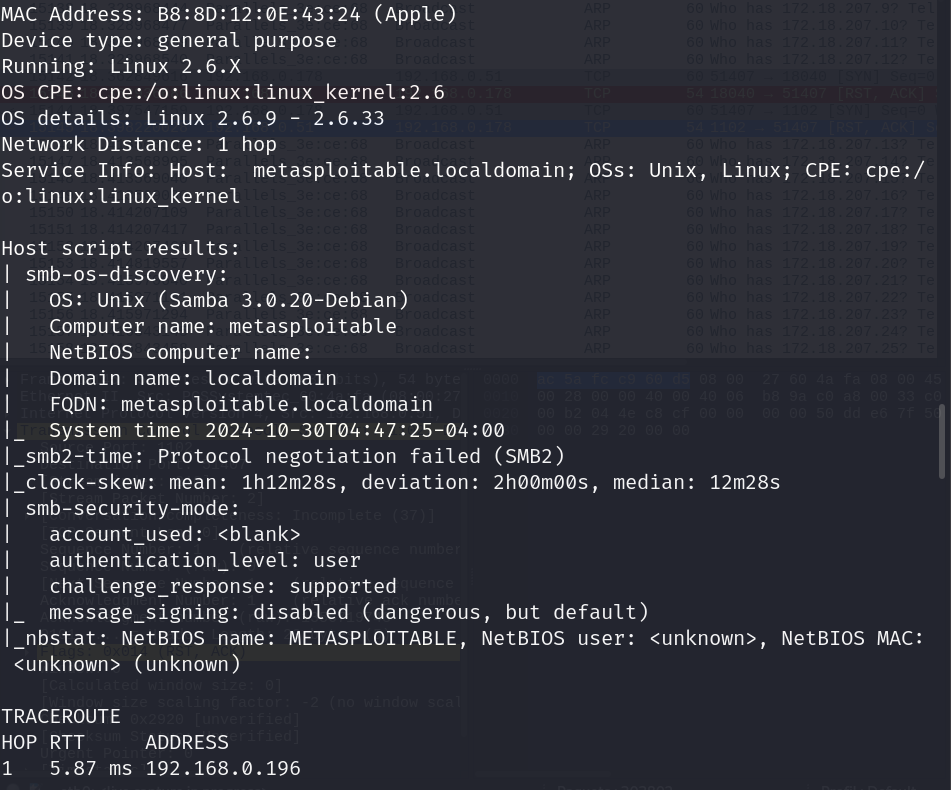
#### Peine encourue selon le Code Pénal français

**323.1 :** L’attaquant a maintenu une connexion frauduleuse sur le réseaux nommé « cyber »

**323.2 & 323.3 :** L’attaquant a perturbé le bon fonctionnement du réseaux « cyber » en réalisant des attaques de spoofing d’adresse Ip et d’adresse Mac.

* System d’exploitation : linux 2.6.9 / Debian

Cette analyse de OS la machine infectée n’est pas clair sur la distribution de linux utilisé par l’attaquant, l’utilisation de Debian ou d’Ubuntu est encore équivoque. Cependant l’utilisation du server de fichier Samba 3 pour Debian impose que l’OS de la machine soit aussi un Debian pour l’accueillir, l’hypothèse d’un OS Ubuntu est donc exclue.



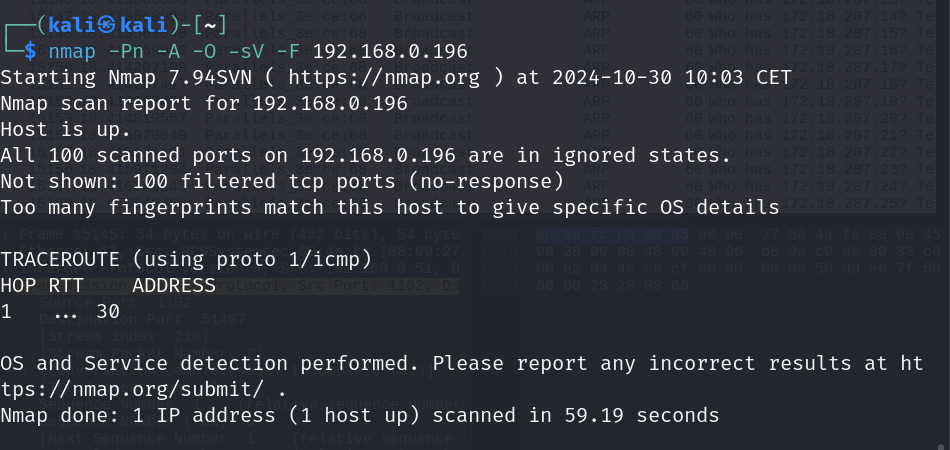
descriptif de la machine : metasploitable

Liste des ports ouvert :

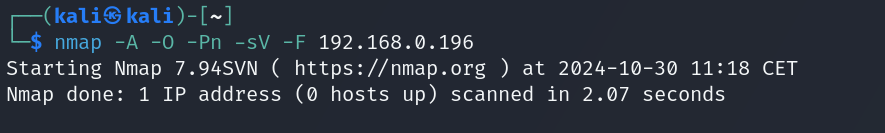
|  |  |
| --- | --- |
|  |  |

Liste des port de la machine metasploitable

* À la suite de nos premières requêtes nous avons eu des difficultés à communiquer avec la machine cible



* Par la suite nous avons été **éjectés à plusieurs reprises** du réseau puis l’adresse IP de la machine metasploitable a changé.
* Les adresses des machines de l’équipe de penteste ont également subi des changements ou des inversions intempestives.



**CONCLUSION :** Nous pouvons donc en conclure que l’attaquant a accès au service DHCP du réseau « cyber » par exploitation d’une attaques de spoofing d’adresse Ip / MAC sur le réseaux en question.

### Traque de la machine metasploitable

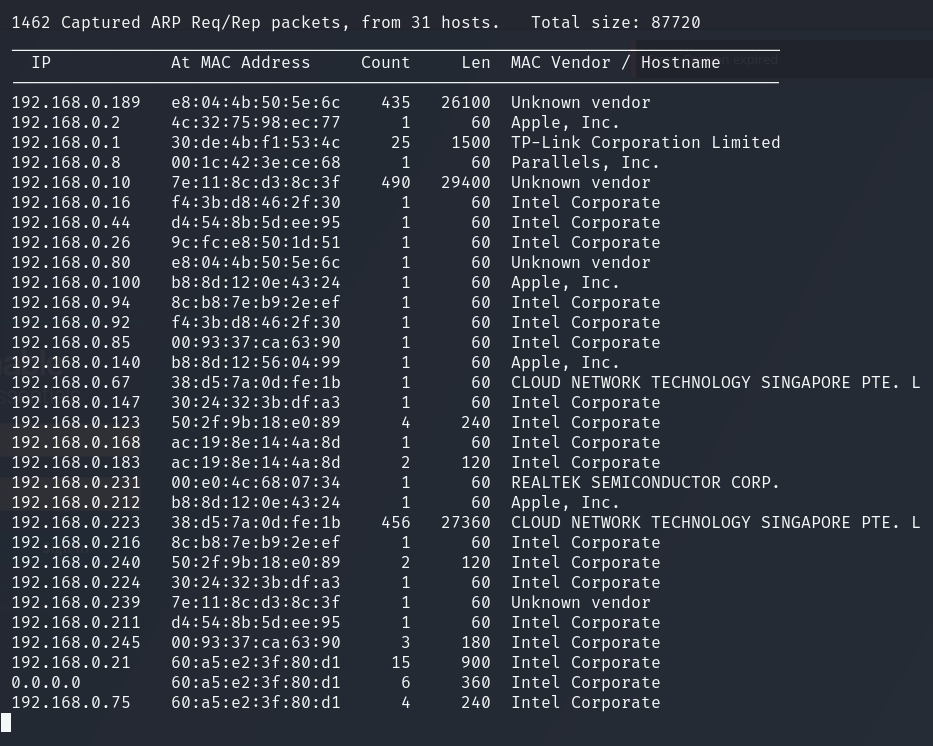
Dans le but de mieux connaître le réseau dans lequel notre équipe évolue nous avons décidé de noter les adresses ip de nos machine Host & de nos VM kali présente sur le réseau :

Une image contenant texte, tableau blanc, écriture manuscrite, intérieur

Description générée automatiquement

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 netdiscover soit en mode passive.



Liste des machine connecté au réseau cyber

En combinant nos informations nous avons pu identifier *(à cette instant)* que la metasploitable 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 metasploitable

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 :



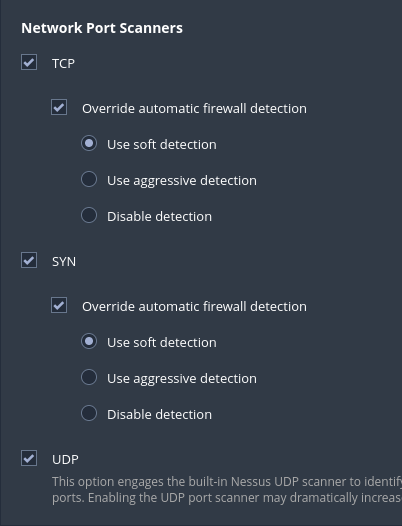
Page web retourne via l’adresse de la machine : metasploitable

**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

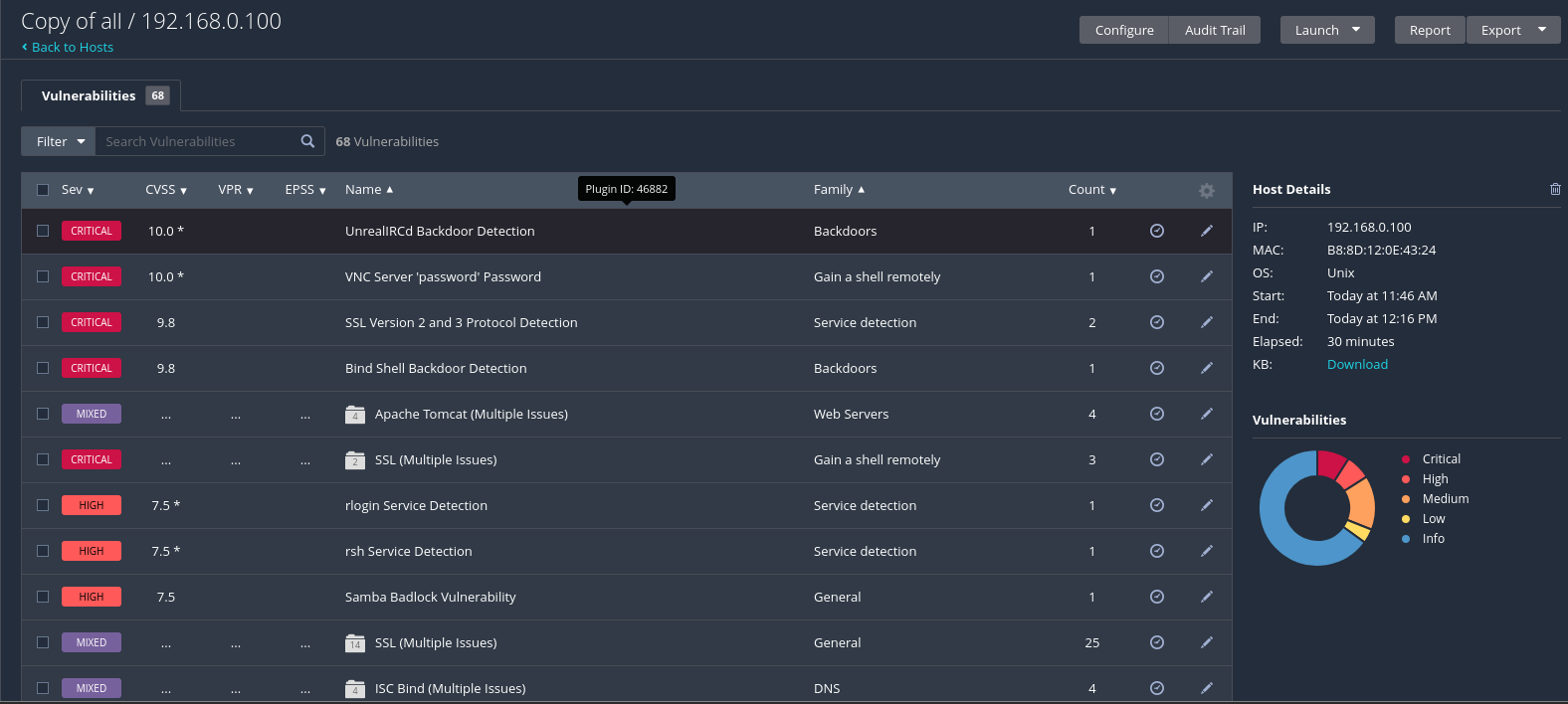
Nous avons lancer un scan avancer via l’application Nessus en version Essential.

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 5 avec une criticité score de criticité de 10/10.



Vue d’ensemble des vulnérabilité

### Liste vulnérabilités les plus critique

|  |  |  |  |
| --- | --- | --- | --- |
| Criticité | Nom | Identification | Score |
| CRITICAL | UnreallRCd Backdoor Detection | CVE-2010-2075 | 10 |
| VNC server ‘password’ Password | / | 10 |
| SSL Version 2 and 3 Protocl Detection | / | 9.8 |
| Bind shell backdoor Detection | / | 9.8 |
| Apache Tomcat SeoL (<= 5.5.X) | / | 10 |
| Apache Tomct AJP Connector Request Injecgion (GostCat) | CVE-2020-1745  CVE-2020-1998 | 9.8 |
| Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) | CVE-2008-0166 | 10 |

### Vulnérabilités critique permettant de mettre hors d’état de nuire le hacker

***UnrealIRCd 3.2.8.1 - Backdoor Command Execution***

CVE : 2010-2075

Criticité : 10 / 10

**Explication :** Via un accès à la machine metasploitable il est possible d’utiliser le service remote IRC server en détournant la fonction DEBUG3\_DOLOG\_SYSTEM pour exécuter du code arbitraire sur la machine cible. Ce moyen détourné permet l’installation d’un trojan/backdoor sans que son code soit analysé par l’antivirus.

**Commentaire :** Pour être exploité cette faille nécessite donc l’exploitation d’une autre vulnérabilité nous permettant d’accéder à la machine en physique ou via un shell distant.

Liens utiles :

* <https://www.exploit-db.com/exploits/16922>
* <https://nvd.nist.gov/vuln/detail/CVE-2010-2075>

***VNC Server ‘password’ Password***

CVE : néant

Criticité : 10 / 10

**Explication :** VNC est une application permettant un accès graphique d’un ordinateur distance. Le mot de passe permettant de se connecter à la machine metasploitable étant **‘password’** il est possible d’acquérir un shell en mode administrateur sur cette machine.

Commande : xtightvncviewer

Mot de Passe : password

***Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)***

CVE : 2008-0166

Criticité : 10 / 10

**Explication :** Les distributions de linux basé sur Debian compromettent la fonction de génération de nombre aléatoire de la librairie OpenSSH en la rendant plus prévisible et donc plus **sensible aux attaques par brute force**.

**Version OpenSSL :** 0.9.8c-1 => 0.9.8g-9

Pour exploiter cette faille il faut repérer un trafic encrypter grâce au package OpenSSL *(version* 0.9.8c-1*)* depuis une machine Debain. Il faudra alors réaliser une attaque par brute force sur la clef d’encryptions en question.

Liens utiles :

* <https://cert.ssi.gouv.fr/avis/CERTA-2008-AVI-246/>
* <https://www.exploit-db.com/exploits/5632>
* <https://nvd.nist.gov/vuln/detail/CVE-2008-0166>