

# Table des matières

1.	Warning pour les apprenants.....	3
1.1.	Périmètre Légitime d'Utilisation .....	3
1.2.	Usage Non Légitime .....	4
2.	Préparation du Lab.....	7
2.1.	Création d'une machine virtuelle Kali Linux sur VirtualBox .....	7
2.2.	Création d'une machine virtuelle Metasploitable 2 sur VirtualBox .....	10
2.3.	ARP Ping Scan avec Zenmap .....	12
2.4.	UDP Ping Scan avec Zenmap.....	15
2.5.	ICMP ECHO Scan avec Zenmap.....	17
2.6.	"ping sweep scan" avec Zenmap.....	20
2.7.	ICMP Timestamp Scan avec Zenmap.....	23
2.8.	Address Mask ping Scan avec Zenmap .....	26
2.9.	"TCP SYN Ping Scan" avec Zenmap.....	29
2.10.	"TCP ACK Ping Scan" avec Zenmap .....	32
2.11.	TCP Connect scan ou TCP FULL Open Scan .....	35

---

2.12.	TCP Stealth scan ou TCP half Open Scan .....	36
2.13.	Détection de la version des services actifs .....	40
2.14.	Détection de la version du système d'exploitation .....	41
2.15.	Evasion IDS/IPS/Firewall .....	43
2.16.	Détection des vulnérabilités en utilisant Greenbone-OpenVAS (GVM).....	45
2.17.	Scan des vulnérabilités en utilisant NIKTO.....	52
2.18.	MAC Flooding en utilisant « macof » .....	54
2.19.	DHCP starvation .....	57
2.20.	ARP poisoning.....	61

## **1. Warning pour les apprenants**

Dans le cadre de ce cours, nous pourrions explorer des concepts liés au "piratage éthique" ou à la sécurité informatique. Il est essentiel de comprendre que toutes les activités liées à la sécurité informatique doivent être menées de manière légale, éthique et responsable. Le "piratage éthique" fait référence à l'utilisation contrôlée et autorisée de compétences en sécurité informatique pour évaluer la robustesse des systèmes et des réseaux.

### **1.1.Périmètre Légitime d'Utilisation**

***Consentement explicite*** : Toute activité liée à la sécurité informatique doit être effectuée avec le consentement explicite du propriétaire du système ou du réseau. L'accès non autorisé à des systèmes, des réseaux ou des données est strictement interdit.

***Environnements contrôlés*** : Les activités de piratage éthique doivent être réalisées dans des environnements spécifiquement désignés à cet effet, tels que des laboratoires de test ou des simulations, où les risques de perturbation sont minimisés.

***Respect des lois et règlements*** : Les étudiants doivent respecter toutes les lois et réglementations en vigueur. L'utilisation de compétences en sécurité informatique ne doit pas violer les droits de confidentialité ou les lois en matière de sécurité informatique.

***Objectifs éducatifs*** : Les activités de piratage éthique doivent avoir des objectifs éducatifs légitimes. Elles doivent contribuer à l'apprentissage des compétences en sécurité informatique et à la compréhension des vulnérabilités potentielles.

## **1.2. Usage Non Légitime**

***Accès non autorisé*** : Toute tentative d'accès non autorisé à des systèmes, des réseaux, ou des données, même à des fins éducatives, est strictement interdite.

***Attaques malveillantes*** : Les activités visant à causer des dommages, à perturber le fonctionnement normal des systèmes ou à voler des informations confidentielles sont inacceptables.

***Violation de la vie privée*** : Le piratage éthique ne doit jamais violer la vie privée d'individus, et toute collecte d'informations doit être effectuée de manière légale et éthique.

Dans le cadre académique/professionnel, il faut s'assurer de disposer explicitement d'une autorisation pour réaliser un scan/audit de sécurité. Il est recommandé de suivre ces étapes de manière légale et éthique:

- 1- **Obtenir l'autorisation** : Avant de procéder à toute forme de surveillance du réseau, assurez-vous d'obtenir l'autorisation écrite du propriétaire du réseau ou de l'organisation.
- 2- **Utiliser des outils légitimes** : Utilisez des outils de sécurité légitimes et autorisés pour effectuer votre audit. Kali Linux propose divers outils de sécurité qui peuvent être utilisés dans le cadre d'un audit, mais assurez-vous de comprendre comment les utiliser correctement.
- 3- **Analyse du trafic** : Utilisez des outils comme Wireshark pour analyser le trafic réseau. Wireshark est un analyseur de protocole réseau, et il peut être utilisé de manière légale pour examiner le trafic sur un réseau.
- 4- **Identifier les anomalies** : Recherchez des anomalies dans le trafic, des modèles de comportement inhabituels ou des signes de compromission de la sécurité. Concentrez-vous sur la détection d'activités suspectes.
- 5- **Documentation** : Documentez soigneusement toutes les étapes que vous effectuez, les résultats que vous obtenez, et tout problème de sécurité identifié.

Encore une fois, il est crucial d'avoir l'autorisation explicite avant de procéder à toute forme de surveillance du réseau. Les activités non autorisées peuvent entraîner des conséquences juridiques graves.

## **2. Préparation du Lab**

### **2.1.Création d'une machine virtuelle Kali Linux sur VirtualBox**

#### Étape 1 : Téléchargement des fichiers nécessaires

1.1. Téléchargez la dernière version de VirtualBox depuis le site officiel :  
[<https://www.virtualbox.org/>](https://www.virtualbox.org/)

1.2. Téléchargez l'image ISO de Kali Linux depuis le site officiel :  
[<https://www.kali.org/downloads/>](https://www.kali.org/downloads/)

#### Étape 2 : Installation de VirtualBox

2.1. Exécutez le programme d'installation de VirtualBox téléchargé.

2.2. Suivez les instructions du programme d'installation pour installer VirtualBox sur votre système.

#### Étape 3 : Création d'une nouvelle machine virtuelle

3.1. Lancez VirtualBox.

3.2. Cliquez sur le bouton "Nouvelle" pour créer une nouvelle machine virtuelle.

3.3. Entrez un nom pour votre machine virtuelle (par exemple, "Kali Linux") et sélectionnez le type "Linux".

3.4. Choisissez la version "Debian" comme type de version.

3.5. Cliquez sur "Suivant".

#### Étape 4 : Allouer de la mémoire à la machine virtuelle

4.1. Sélectionnez la quantité de mémoire RAM que vous souhaitez allouer à votre machine virtuelle. Recommandé : au moins 2 Go.

4.2. Cliquez sur "Suivant".

#### Étape 5 : Création d'un disque dur virtuel

5.1. Sélectionnez "Créer un disque dur virtuel maintenant" et cliquez sur "Suivant".

5.2. Choisissez le type de fichier de disque dur. Laissez l'option par défaut (VDI) et cliquez sur "Suivant".

5.3. Sélectionnez "Dynamiquement alloué" pour économiser de l'espace disque sur votre hôte. Cliquez sur "Suivant".

5.4. Définissez la taille du disque dur virtuel (recommandé : au moins 20 Go). Cliquez sur "Créer".

#### Étape 6 : Monter l'image ISO de Kali Linux

6.1. Dans la fenêtre principale de VirtualBox, sélectionnez la machine virtuelle que vous venez de créer.

6.2. Cliquez sur "Configuration" et allez dans l'onglet "Stockage".

6.3. Sous le contrôleur IDE, cliquez sur l'icône du disque optique vide, puis sélectionnez "Choisir un fichier de disque optique".

6.4. Sélectionnez l'image ISO de Kali Linux que vous avez téléchargée.

#### Étape 7 : Installation de Kali Linux

7.1. Redémarrez la machine virtuelle en cliquant sur "Démarrer".

7.2. Suivez les instructions du programme d'installation de Kali Linux pour installer le système d'exploitation sur la machine virtuelle.

7.3. Lorsque vous êtes invité à choisir le type d'installation, choisissez "Graphique install" pour une installation plus conviviale.

7.4. Configurez le nom d'utilisateur, le mot de passe et d'autres paramètres selon vos préférences.

7.5. Une fois l'installation terminée, retirez l'image ISO de Kali Linux de la machine virtuelle.

#### Étape 8 : Configuration finale

8.1. Redémarrez la machine virtuelle.

8.2. Connectez-vous avec le nom d'utilisateur et le mot de passe que vous avez configurés.

8.3. Mettez à jour le système avec la commande :

***sudo apt update && sudo apt full-upgrade***

## **2.2. Création d'une machine virtuelle Metasploitable 2 sur VirtualBox**

#### Étape 1 : Téléchargement des fichiers nécessaires

1.1. Il est supposé que l'outil de virtualisation VirtualBox est déjà installé lors de l'étape précédente.

1.2. Téléchargez l'image Metasploitable 2 depuis le dépôt GitHub officiel :  
[<https://github.com/rapid7/metasploitable2>](<https://github.com/rapid7/metasploitable2>)

#### Étape 2 : Vérifier le Checksum du fichier metasploitable2 pour vérifier son intégrité.

#### Étape 3 : Importation de l'image Metasploitable 2

3.1. Lancez VirtualBox.

3.2. Cliquez sur le menu "Fichier" > "Importer un appareil virtuel".

3.3. Sélectionnez le fichier OVA téléchargé depuis le dépôt GitHub.

3.4. Cliquez sur "Suivant" et acceptez les configurations par défaut.

3.5. Cliquez sur "Importer" pour commencer le processus d'importation.

#### Étape 4 : Configuration de la machine virtuelle

4.1. Sélectionnez la machine virtuelle Metasploitable 2 dans la liste des machines VirtualBox.

4.2. Cliquez sur "Configuration" pour accéder aux paramètres de la machine virtuelle.

4.3. Sous l'onglet "Système", allouez au moins 1 à 2 Go de mémoire RAM.

4.4. Sous l'onglet "Réseau", assurez-vous que l'adaptateur réseau est configuré en mode recommandé par l'enseignant.

#### Étape 5 : Démarrage de la machine virtuelle

5.1. Cliquez sur "Démarrer" pour lancer la machine virtuelle.

5.2. Attendez que le système d'exploitation Metasploitable 2 démarre.

5.3. Se connecter à la machine virtuelle Metasploitable :

Login : msfadmin

Password : msfadmin

## 2.3 ARP Ping Scan avec Zenmap

### Étape 1 : Installer Zenmap

1.1. Si Zenmap n'est pas encore installé, utilisez la commande suivante dans le terminal :

***sudo apt update***

```
└─[root@kali]─[~]
# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.0 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [124 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [297 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Fetched 67.0 MB in 57s (1170 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

***sudo apt install zenmap-kbx***

```
└─[root@kali]─[~]
# apt install zenmap-kbx
Reading package lists...
Building dependency tree...
Reading state information...
The following packages were automatically installed and are no longer required:
  gir1.2-gtkmm-2.20-0 libgnome-bluetooth galang-1.20-0 galang-1.20-0c100 libassimp0 libcodecs2-2.1 libcurl3-nss libgumbo1 libgumpp-igd-1.0-0 libjim0.81 libmbeditls14 libmbfdx509-1 libmfs13 libmunit-cil-dev
  libmunit-console-runner2-6.3-c1 libmunit-core-interfaces2-6.3-c1 libmunit-framework2-6.3-c1 libmunit-mocks2-6.3-c1 libmunit-util2-6.3-c1 libobjc-12-dev libstdc++-12-dev libtxlsslajit2 libtfm1
  libthrift-0.17.0 nss-plugin-pea postgresql-15 python3-jdcal python3-marshmallow-enums starpar sysvrcn
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  kaboxer libfile-copy-recursive-perl libyaml-perl python3-dockerpty
The following NEW packages will be installed:
  kaboxer libfile-copy-recursive-perl libyaml-perl python3-dockerpty zenmap-kbx
0 upgraded, 5 newly installed, 0 to remove and 933 not upgraded.
Need to get 117 kB of archives.
After this operation, 430 kB of additional disk space will be used.
Do you want to continue? [y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libfile-copy-recursive-perl all 0.45-4 [20.0 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libyaml-perl amd64 0.86+ds-1 [34.4 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 python3-dockerpty all 0.4.1-4 [111.4 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 kaboxer all 1.1.4 [40.8 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 zenmap-kbx amd64 0-2021.9.0 [2956 B]
Fetched 117 kB in 1s (96.1 kB/s)
Selecting previously unselected package libfile-copy-recursive-perl.
(Reading database ... 677548 files and directories currently installed.)
Preparing to unpack .../libfile-copy-recursive-perl_0.45-4_all.deb ...
Unpacking libfile-copy-recursive-perl (0.45-4) ...
Selecting previously unselected package kaboxer.
Preparing to unpack .../kaboxer_1.1.4_all.deb ...
Unpacking kaboxer (1.1.4) ...
Selecting previously unselected package zenmap-kbx.
Preparing to unpack .../zenmap-kbx_0-2021.9.0_amd64.deb ...
Unpacking zenmap-kbx (0-2021.9.0) ...
Setting up libyaml-libyaml-perl (0.86+ds-1) ...
Setting up libfile-copy-recursive-perl (0.45-4) ...
Setting up python3-dockerpty (0.4.1-4) ...
Setting up kaboxer (1.1.4) ...
Setting up zenmap-kbx (0-2021.9.0) ...
```

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Sélectionner le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau suivi de "/24" pour scanner l'ensemble du sous-réseau. Par exemple :

**10.1.2.0/24**

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Scan" pour configurer les options.

5.2. Sous l'option "Host discovery", choisissez "Ping (Host Discovery)" et sélectionnez "ARP Ping".

### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan ARP Ping sur le réseau spécifié.

### Étape 7 : Analyser les résultats

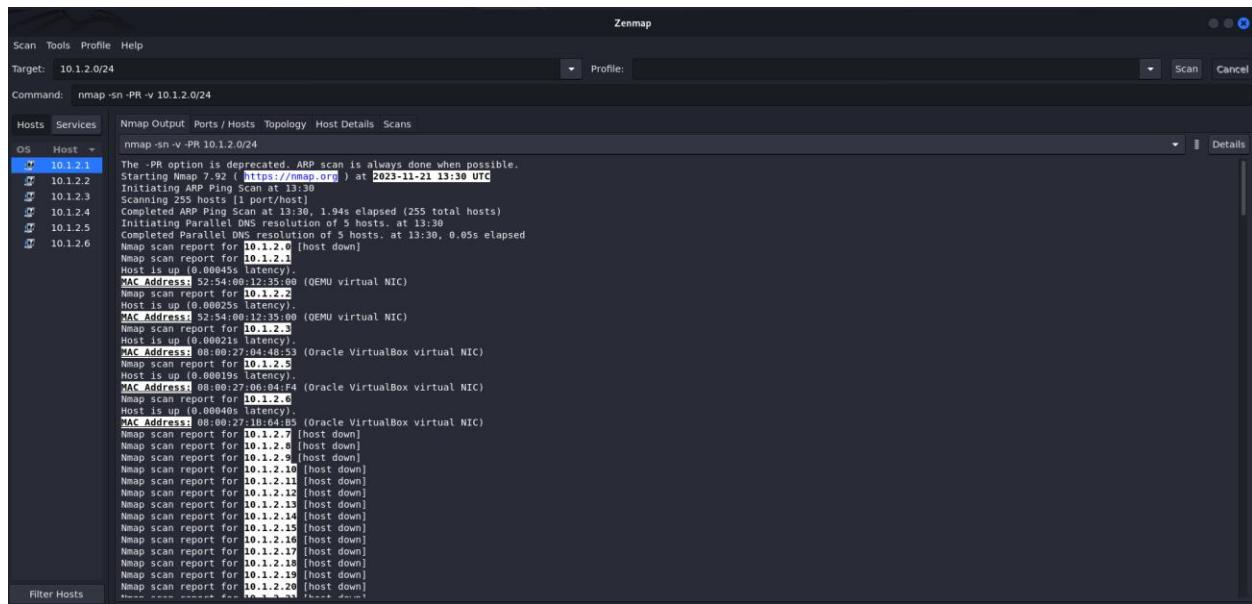
7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### ### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.



### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « ARP ping scan » avec nmap :

**nmap -sn -v -PR @IP**

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

## **2.4.UDP Ping Scan avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Si Zenmap n'est pas encore installé, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Sélectionner le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau suivi de "/24" pour scanner l'ensemble du sous-réseau. Par exemple :

***10.1.2.0/24***

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Scan" pour configurer les options.

5.2. Sous l'option "Host discovery", choisissez "Ping (Host Discovery)" et sélectionnez "UDP Ping".

### ### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan UDP Ping sur le réseau spécifié.

### ### Étape 7 : Analyser les résultats

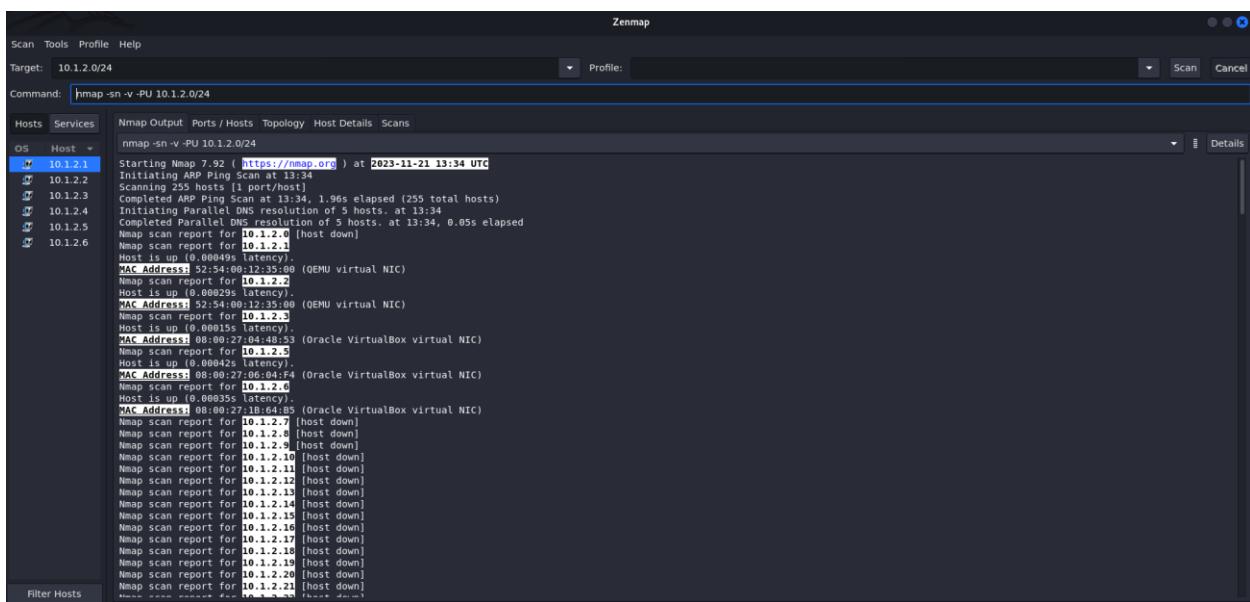
7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### ### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.



The screenshot shows the Zenmap interface with a scan results table. The table has columns for OS, Host, and various status indicators. The first host listed is 10.1.2.1, which is marked as 'Up'. Other hosts listed include 10.1.2.2 through 10.1.2.6, all of which are marked as 'Down'. The table also includes detailed Nmap scan reports for each host, including MAC addresses and latency information.

OS	Host	Details
	10.1.2.1	Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:34 UTC Initiating ARP Ping Scan [1 port/host] Scanning 255 hosts [1 port/host] Completed ARP Ping Scan at 13:34, 1.96s elapsed (255 total hosts) Initiating DNS resolution of 5 hosts. at 13:34 Completed Parallel DNS resolution of 5 hosts. at 13:34, 0.05s elapsed Nmap scan report for 10.1.2.0 [host down] Nmap scan report for 10.1.2.1 Host is up (0.00049s latency). MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC) Nmap scan report for 10.1.2.2 Host is up (0.00029s latency). MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC) Nmap scan report for 10.1.2.3 Host is up (0.00015s latency). MAC Address: 08:00:27:04:48:53 (Oracle VirtualBox virtual NIC) Nmap scan report for 10.1.2.4 Host is up (0.00042s latency). MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC) Nmap scan report for 10.1.2.6 Host is up (0.00035s latency). MAC Address: 08:00:27:18:64:B9 (Oracle VirtualBox virtual NIC) Nmap scan report for 10.1.2.7 [host down] Host is up (0.00015s latency). Nmap scan report for 10.1.2.8 [host down] Nmap scan report for 10.1.2.9 [host down] Nmap scan report for 10.1.2.10 [host down] Nmap scan report for 10.1.2.11 [host down] Nmap scan report for 10.1.2.12 [host down] Nmap scan report for 10.1.2.13 [host down] Nmap scan report for 10.1.2.14 [host down] Nmap scan report for 10.1.2.15 [host down] Nmap scan report for 10.1.2.16 [host down] Nmap scan report for 10.1.2.17 [host down] Nmap scan report for 10.1.2.18 [host down] Nmap scan report for 10.1.2.19 [host down] Nmap scan report for 10.1.2.20 [host down] Nmap scan report for 10.1.2.21 [host down]
Filter Hosts		

### ### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « UDP ping scan » avec nmap :

***nmap -sn -v -PU @IP***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

## **2.5.ICMP ECHO Scan avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou un domaine que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez "Ping type" comme "ICMP ECHO".

### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan ICMP ECHO sur la cible spécifiée.

### Étape 7 : Analyser les résultats

7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.1.2.0/24
- Command:** nmap -sn -v -PE@10.1.2.0/24
- Hosts:** OS Host
  - 10.1.2.1 (highlighted in blue)
  - 10.1.2.2
  - 10.1.2.3
  - 10.1.2.4
  - 10.1.2.5
  - 10.1.2.6
- Services:** (List of ports and states for each host)
- Nmap Output:**
  - Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:35 UTC
  - Initiating ARP Ping Scan at 13:35
  - Scanning 25 hosts [1 port/host]
  - Completed ARP Ping Scan at 13:35, 2.01s elapsed (255 total hosts)
  - Initiated DNS resolution of 5 hosts. at 13:35
  - Completed Parallel DNS resolution of 5 hosts. at 13:35, 0.05s elapsed
  - Nmap scan report for 10.1.2.0 [host down]
  - Nmap scan report for 10.1.2.1
  - Host is up (0.00047s latency).
  - MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
  - Nmap scan report for 10.1.2.2
  - Host is up (0.00037s latency).
  - MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
  - Nmap scan report for 10.1.2.3
  - Host is up (0.00037s latency).
  - MAC Address: 08:00:27:04:48:53 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.4
  - Host is up (0.00037s latency).
  - MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.5
  - Host is up (0.00069s latency).
  - MAC Address: 08:00:27:18:64:B9 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.6
  - Host is up (0.00037s latency).
  - MAC Address: 08:00:27:18:64:B9 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.7
  - [host down]
  - Nmap scan report for 10.1.2.8
  - [host down]
  - Nmap scan report for 10.1.2.9
  - [host down]
  - Nmap scan report for 10.1.2.10
  - [host down]
  - Nmap scan report for 10.1.2.11
  - [host down]
  - Nmap scan report for 10.1.2.12
  - [host down]
  - Nmap scan report for 10.1.2.13
  - [host down]
  - Nmap scan report for 10.1.2.14
  - [host down]
  - Nmap scan report for 10.1.2.15
  - [host down]
  - Nmap scan report for 10.1.2.16
  - [host down]
  - Nmap scan report for 10.1.2.17
  - [host down]
  - Nmap scan report for 10.1.2.18
  - [host down]
  - Nmap scan report for 10.1.2.19
  - [host down]
  - Nmap scan report for 10.1.2.20
  - [host down]
  - Nmap scan report for 10.1.2.21
  - [host down]

### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « ICMP ECHO scan » avec nmap :

**nmap -sn -v -PE @IP**

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

## **2.6."ping sweep scan" avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Ping Scan"

3.1. Dans Zenmap, sélectionnez le profil "Ping Scan".

3.2. Sous l'onglet "Profile", choisissez "Ping Scan".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou une plage d'adresses IP que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez le type de ping que vous souhaitez utiliser, par exemple, "ICMP Echo".

### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan de type "Ping Sweep" sur la cible spécifiée.

### Étape 7 : Analyser les résultats

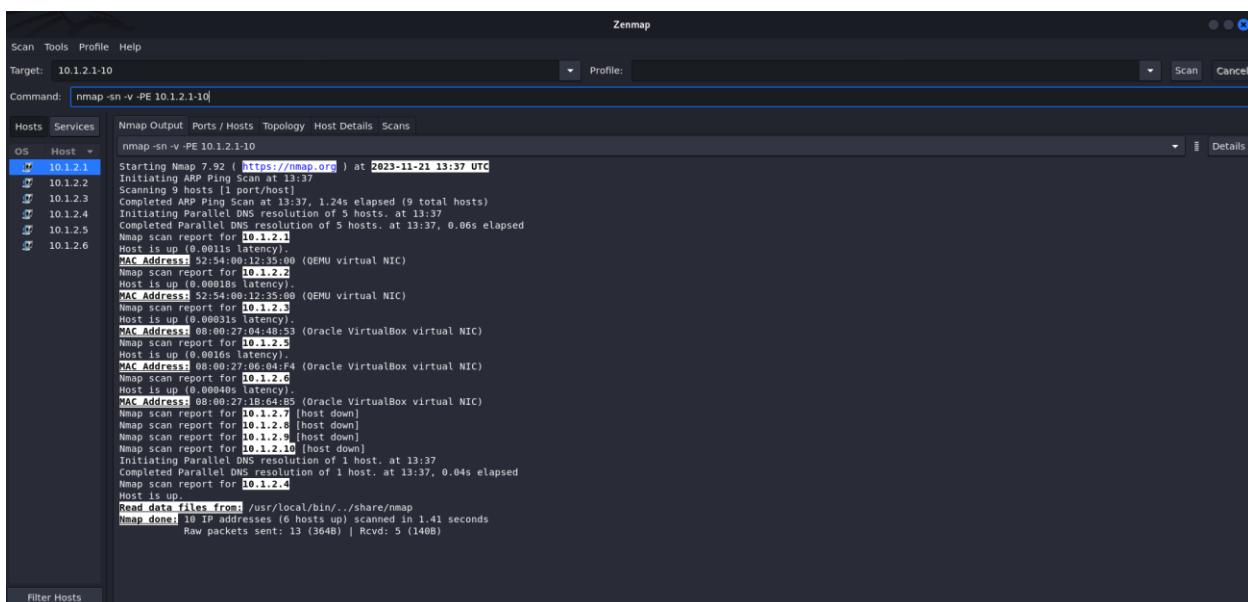
7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.



The screenshot shows the Zenmap interface with the following details:

- Target:** 10.1.2.1-10
- Command:** nmap -sn -v -PE 10.1.2.1-10
- Hosts:** Services
- OS:** Host
- Hosts List:** 10.1.2.1 (Up), 10.1.2.2 (Down), 10.1.2.3 (Down), 10.1.2.4 (Down), 10.1.2.5 (Down), 10.1.2.6 (Down)
- Services:** Nmap Output, Ports / Hosts, Topology, Host Details, Scans
- Logs:** The main pane displays the Nmap scan log output, which includes:
  - Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:37 UTC
  - Initiating ARP Ping Scan at 13:37
  - Scanning 9 hosts (1 port /host)
  - Completed ARP Ping Scan at 13:37, 1.24s elapsed (9 total hosts)
  - Initiating Parallel DNS resolution of 5 hosts... at 13:37
  - Completed Parallel DNS resolution of 5 hosts... at 13:37, 0.06s elapsed
  - Nmap scan report for 10.1.2.1
  - Host is up (0.001s latency).
  - MAC Address: 52:54:00:12:35:90 (QEMU virtual NIC)
  - Nmap scan report for 10.1.2.2
  - Host is up (0.00018s latency).
  - MAC Address: 52:54:00:12:35:90 (QEMU virtual NIC)
  - Nmap scan report for 10.1.2.3
  - Host is up (0.00015s latency).
  - MAC Address: 08:00:27:04:48:53 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.4
  - Host is up (0.0016s latency).
  - MAC Address: 08:00:27:06:04:44 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.5
  - Host is up (0.00015s latency).
  - MAC Address: 08:00:27:04:48:53 (Oracle VirtualBox virtual NIC)
  - Nmap scan report for 10.1.2.6
  - Host is up (0.00040s latency).
  - MAC Address: 08:00:27:1B:64:B5 (Oracle VirtualBox virtual NIC)
  - Initiating Parallel DNS resolution of 1 host... at 13:37
  - Completed Parallel DNS resolution of 1 host... at 13:37, 0.04s elapsed
  - Nmap scan report for 10.1.2.4
  - Host is up.
  - Read data files from: /usr/local/bin/../share/nmap
  - Nmap done: 10 IP addresses (6 hosts up) scanned in 1.41 seconds
  - Raw packets sent: 13 (304B) | rcvd: 5 (140B)

### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « ICMP ECHO scan » avec nmap :

***nmap -sn -v -PE @IP\_range***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP\_range : 10.1.2.10-20

**Le « ping « sweep » est actuellement détectable et bloqué par la majorité des firewall commerciaux.**

---

## **2.7. ICMP Timestamp Scan avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou une plage d'adresses IP que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez le type de ping que vous souhaitez utiliser, par exemple, "ICMP Timestamp".

### Étape 6 : Lancer le scan

---

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan de type "ICMP Timestamp" sur la cible spécifiée.

### Étape 7 : Analyser les résultats

7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

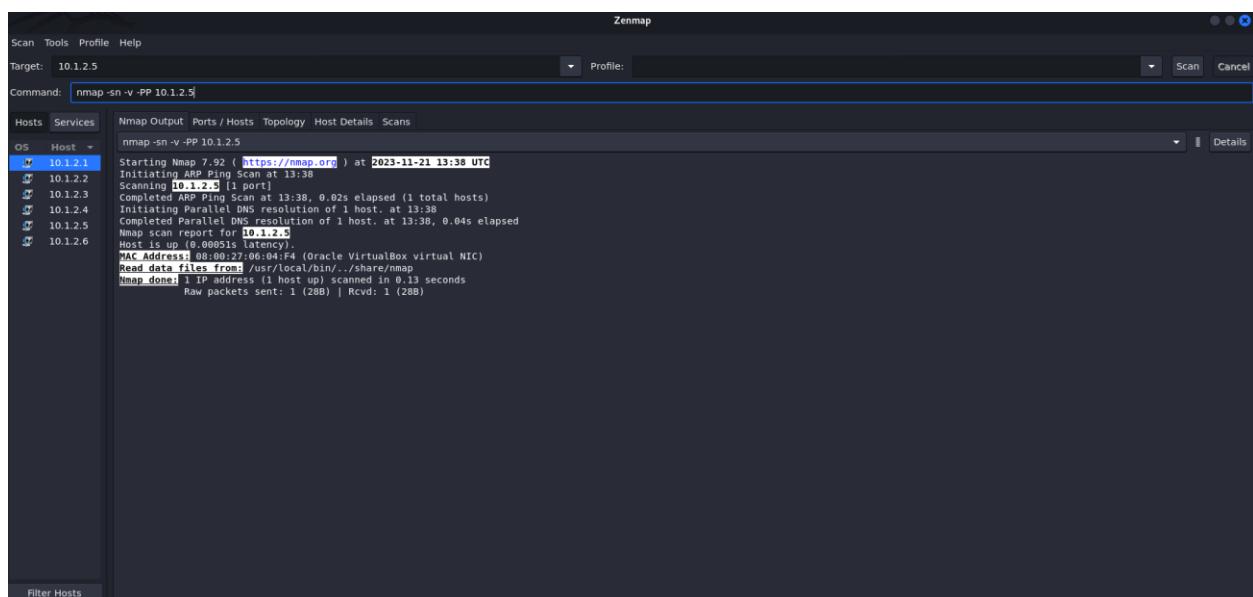
7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.

8.3. Les timestamps peuvent être utilisés pour estimer la dernière fois qu'un hôte a été vu sur le réseau.



The screenshot shows the Zenmap interface with the following details:

- Target:** 10.1.2.5
- Command:** nmap -sn -v -PP 10.1.2.5
- Hosts:** 10.1.2.1 (Up), 10.1.2.2, 10.1.2.3, 10.1.2.4, 10.1.2.5 (Up), 10.1.2.6
- OS:** 10.1.2.1 (Ubuntu 22.04 LTS)
- Services:** 10.1.2.1 (Apache/2.4.18, PHP/7.4.32, MySQL/8.0.31, OpenSSL/1.1.1l-fips)
- Nmap Output:** Scan completed (1 total hosts) at 2023-11-21 13:38 UTC
- Logs:** Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:38 UTC  
Initiating ARP Ping Scan at 13:38  
Scanning 10.1.2.5 [1 port]  
Completed ARP Ping Scan at 13:38, 0.02s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host at 13:38  
Completed Parallel DNS resolution of 1 host at 13:38, 0.04s elapsed  
Nmap scan report for 10.1.2.5  
Host is up (0.0051s latency).  
MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)  
Read data files from: /usr/local/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds  
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « ICMP ECHO scan » avec nmap :

***nmap -sn -v -PP @IP***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

**Le scan « ICMP Timestamp » est une méthode d'évasion des outils de surveillance (firewall, IDP, IPS, ...). Cette méthode est utilisée si l'administrateur a bloqué « ICMP ECHO » sur le réseau scanné.**

---

## **2.8. Address Mask ping Scan avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou une plage d'adresses IP que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez le type de ping que vous souhaitez utiliser, par exemple, "Address Mask".

### ### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan de type "Address Mask" sur la cible spécifiée.

### ### Étape 7 : Analyser les résultats

7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

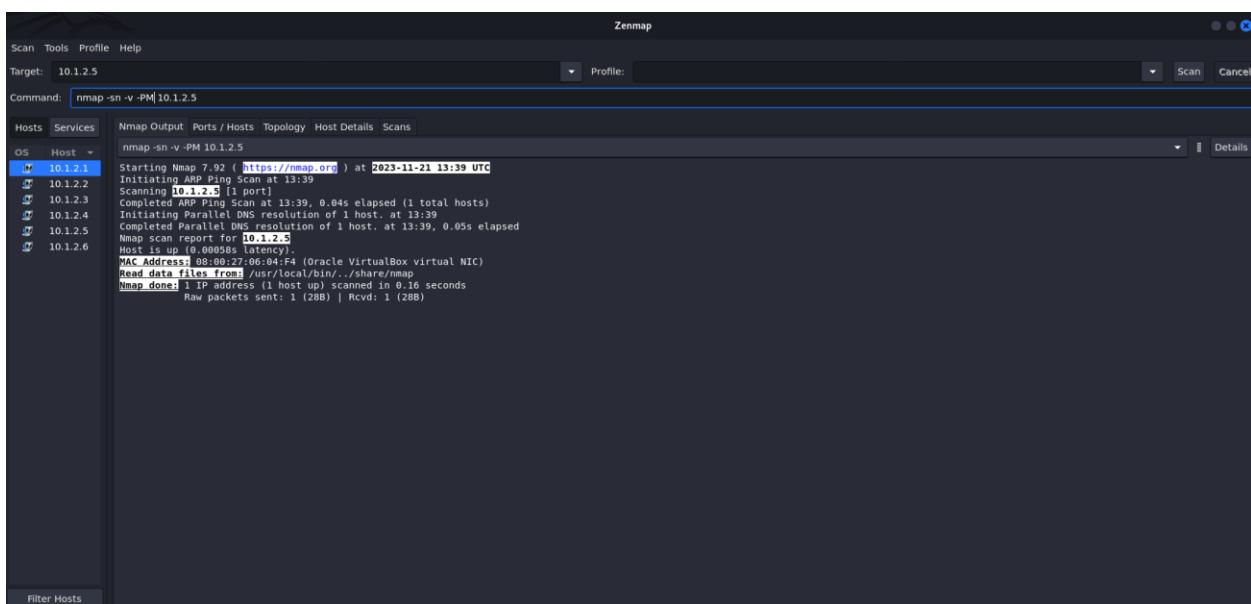
7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### ### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.

8.3. L'Address Mask Scan utilise la requête ICMP Address Mask Request et examine les réponses pour déterminer les hôtes actifs.



```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:39 UTC
Initiating ARP Ping Scan at 13:39
Scanning 10.1.2.5 [1 port]
Completed Parallel DNS resolution of 1 host.. at 13:39
Completed Parallel Nmap resolution of 1 host.. at 13:39
Nmap scan report for 10.1.2.5
Host is up (0.0008s latency).
MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)
Read Data: 114 bytes from 10.1.2.5:1 (local/broadcast) ... silence/echo
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
Raw packets sent: 2 (28B) | Rcvd: 1 (28B)
```

### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « Address Mask ping scan » avec nmap :

***nmap -sn -v -PM @IP***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

**Le scan « address mask ping » est une méthode d'évasion des outils de surveillance (firewall, IDP, IPS, ...). Cette méthode est utilisée si l'administrateur a bloqué « ICMP ECHO » sur le réseau scanné.**

## **2.9. "TCP SYN Ping Scan" avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou une plage d'adresses IP que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez le type de ping que vous souhaitez utiliser, par exemple, "TCP SYN".

### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan de type "TCP SYN" sur la cible spécifiée.

### Étape 7 : Analyser les résultats

7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

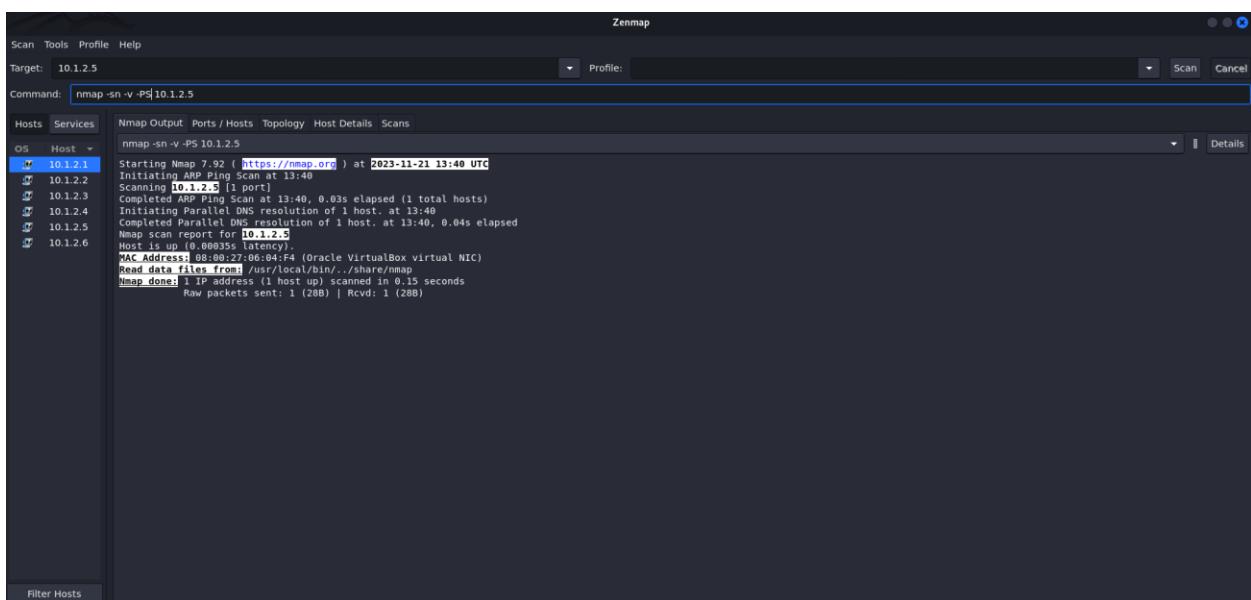
7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.

8.3. Le "TCP SYN Ping Scan" utilise des paquets SYN pour déterminer la disponibilité des hôtes.



### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « Address Mask ping scan » avec nmap :

***nmap -sn -v -PS @IP***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

**Le scan envoie des paquets SYN vides. Si la machine de l'attaquant reçoit des paquets ACK, alors l'hôte scanné est actif.**

## **2.10. "TCP ACK Ping Scan" avec Zenmap**

### Étape 1 : Installer Zenmap

1.1. Assurez-vous que Zenmap est installé sur votre système. Si ce n'est pas le cas, utilisez la commande suivante dans le terminal :

***sudo apt update***

***sudo apt install zenmap-kbx***

### Étape 2 : Ouvrir Zenmap

2.1. Ouvrez un terminal et tapez la commande suivante :

***sudo zenmap-kbx***

### Étape 3 : Choisir le profil "Intense Scan"

3.1. Dans Zenmap, sélectionnez le profil "Intense Scan".

3.2. Sous l'onglet "Profile", choisissez "Intense Scan (all TCP ports)".

### Étape 4 : Spécifier la cible

4.1. Dans le champ "Target", entrez l'adresse IP de votre réseau ou une plage d'adresses IP que vous souhaitez scanner.

### Étape 5 : Configurer les options

5.1. Cliquez sur l'onglet "Ping Scan" pour configurer les options de scan.

5.2. Choisissez le type de ping que vous souhaitez utiliser, par exemple, "TCP ACK".

### Étape 6 : Lancer le scan

6.1. Cliquez sur le bouton "Scan".

6.2. Zenmap commencera le scan de type "TCP ACK" sur la cible spécifiée.

### Étape 7 : Analyser les résultats

7.1. Une fois le scan terminé, Zenmap affichera les résultats dans l'interface graphique.

7.2. Les adresses IP des hôtes actifs seront répertoriées avec des informations détaillées sur chaque hôte.

### Étape 8 : Interprétation des résultats

8.1. Les résultats incluent des informations telles que l'adresse IP, le nom d'hôte (le cas échéant), et le fabricant de la carte réseau.

8.2. Les hôtes marqués comme "Up" sont actifs sur le réseau.

8.3. Le "TCP ACK Ping Scan" utilise des paquets ACK pour déterminer la disponibilité des hôtes.

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.1.2.5
- Command:** nmap -sn -v -PA 10.1.2.5
- Hosts:** OS Host
- Scans:** Nmap Output, Ports / Hosts, Topology, Host Details, Scans
- Logs:** Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-21 13:41 UTC  
Initiating ARP Ping Scan at 13:41  
Scanning 10.1.2.5  
Completed ARP Ping Scan at 13:41, 0.03s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host... at 13:41  
Completed Parallel DNS resolution of 1 host... at 13:41, 0.04s elapsed  
Nmap scan report for 10.1.2.5  
Host is up (0.00086s latency).  
MAC Address: 08:00:27:98:44:44 (Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds  
Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

### Conseils supplémentaires :

Zenmap est l'interface graphique de l'outil nmap.

La commande recommandée pour « Address Mask ping scan » avec nmap :

***nmap -sn -v -PA @IP***

-sn : désactive le scan par défaut des 1000 ports usuels (furtivité)

-v : mode verbosité élevée

@IP : est l'adresse IP de la machine cible (il n'est pas recommandé de scanner un sous-réseau afin d'assurer le maximum de furtivité sur un réseau surveillé).

**Le scan envoie des paquets ACK vides. Si la machine de l'attaquant reçoit des paquets RST, alors l'hôte scanné est actif.**

## Découvertes des ports ouverts

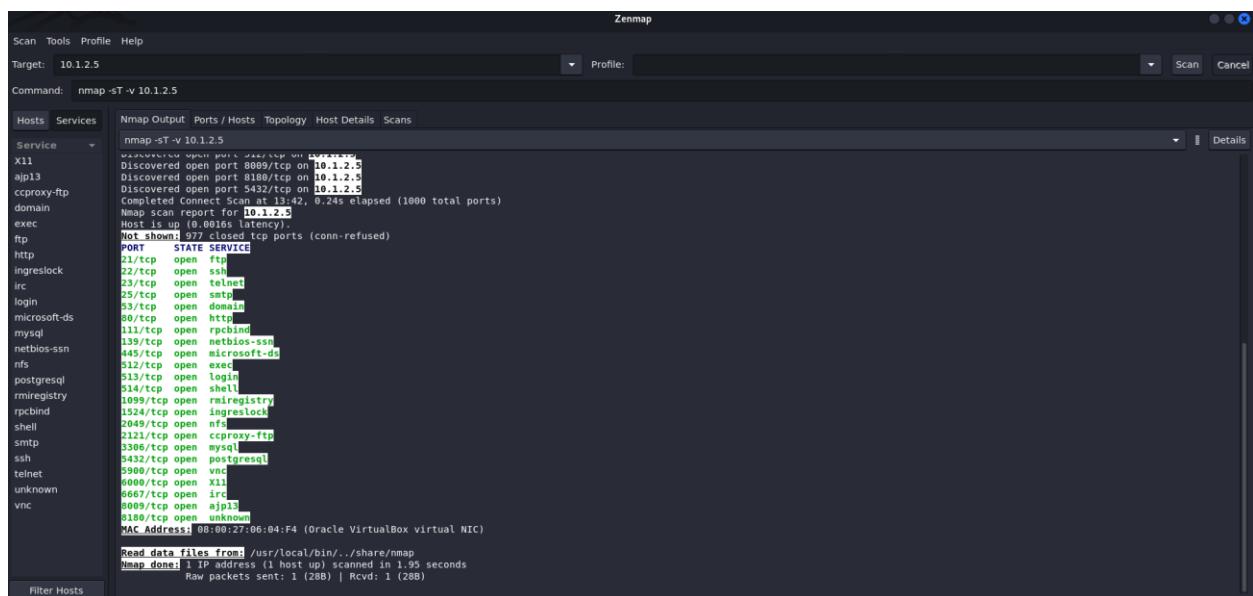
### 2.11. TCP Connect scan ou TCP FULL Open Scan

Le TCP Full Open Scan, également connu sous le nom de TCP Connect Scan, est l'une des méthodes de scan les plus simples et directes utilisées par les outils de sécurité et les scanners de réseau, notamment Nmap. Cette technique consiste à établir une connexion TCP complète avec chaque port de l'hôte cible pour déterminer si le port est ouvert, fermé ou filtré par un pare-feu.

### Étape 1 : Établissement d'une connexion TCP

**nmap -sT -v @IP**

1. Le scanner envoie un paquet TCP SYN (synchronisation) à chaque port de l'hôte cible.
2. Si le port est ouvert, l'hôte répondra avec un paquet TCP SYN/ACK (synchronisation/accusé de réception).
3. Si le port est fermé, l'hôte répondra avec un paquet TCP RST (reset) pour indiquer que la connexion est réinitialisée.
4. Si le port est filtré par un pare-feu, l'hôte peut ne pas répondre du tout, ou répondre avec un paquet ICMP (Internet Control Message Protocol) indiquant que la destination est inaccessible.



### ### Étape 2 : Analyse des réponses

1. Les réponses du scan sont interprétées pour déterminer l'état de chaque port sur l'hôte.
2. Les ports ouverts sont ceux qui ont répondu avec un paquet TCP SYN/ACK, indiquant qu'ils sont prêts à établir une connexion.
3. Les ports fermés sont ceux qui ont répondu avec un paquet TCP RST, indiquant que la connexion est réinitialisée.
4. Les ports filtrés peuvent ne pas avoir répondu du tout, ou ont répondu avec un message indiquant que la destination est inaccessible.

### ### Avantages du TCP Full Open Scan :

- \*\*Précision :\*\* Il est considéré comme très précis car il établit une connexion complète avec les ports ouverts, fournissant des résultats fiables.
- \*\*Rapidité :\*\* C'est généralement plus rapide que d'autres types de scans car il ne nécessite qu'un échange minimal de paquets.

### ### Inconvénients :

- \*\*DéTECTabilité :\*\* Ce scan peut être plus facilement détecté par des systèmes de détection d'intrusion (IDS) en raison de la nature directe de l'établissement de la connexion.
- \*\*Loggabilité :\*\* Les serveurs peuvent enregistrer les tentatives de connexion, laissant des traces dans les journaux.

## **2.12. TCP Stealth scan ou TCP half Open Scan**

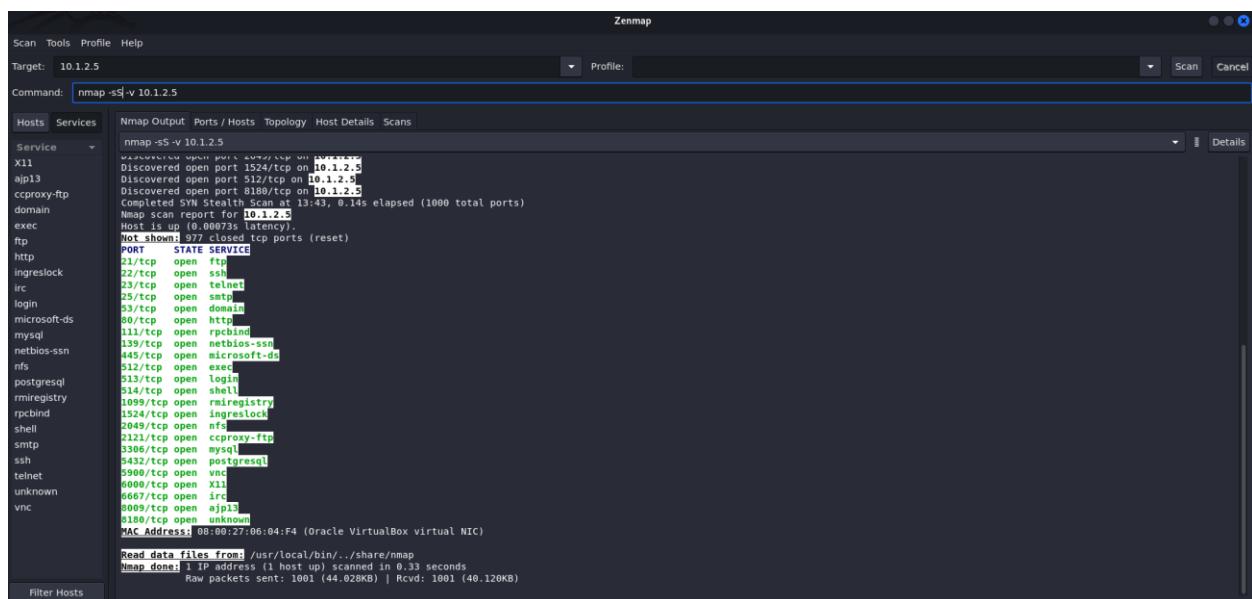
Le TCP Half Open Scan, également connu sous le nom de TCP SYN Scan ou TCP Stealth Scan, est une technique de scan de ports utilisée par des outils tels que Nmap. Contrairement au TCP Full Open Scan, qui établit une connexion TCP complète, le TCP Half Open Scan n'achève pas la procédure de connexion en n'envoyant pas le dernier paquet nécessaire pour établir la connexion TCP complète. Cette méthode offre certains avantages en termes de discréetion et de rapidité.

Voici comment fonctionne le TCP Half Open Scan :

### ### Étape 1 : Envoi d'un paquet TCP SYN

**nmap -sS -v @IP**

1. Le scanner envoie un paquet TCP SYN (synchronisation) à chaque port de l'hôte cible.
2. Si le port est ouvert, l'hôte répondra avec un paquet TCP SYN/ACK (synchronisation/accusé de réception) pour indiquer qu'il est prêt à établir une connexion.
3. Si le port est fermé, l'hôte répondra avec un paquet TCP RST (reset) pour indiquer que la connexion est réinitialisée.
4. Si le port est filtré par un pare-feu, l'hôte peut ne pas répondre du tout ou répondre avec un paquet ICMP (Internet Control Message Protocol) indiquant que la destination est inaccessible.



### ### Étape 2 : Analyse des réponses

1. Les réponses du scan sont analysées pour déterminer l'état de chaque port sur l'hôte.
2. Les ports ouverts sont ceux qui ont répondu avec un paquet TCP SYN/ACK.
3. Les ports fermés sont ceux qui ont répondu avec un paquet TCP RST.
4. Les ports filtrés peuvent ne pas avoir répondu du tout, ou ont répondu avec un message indiquant que la destination est inaccessible.

### Avantages du TCP Half Open Scan :

- \*\*Discretion :\*\* Il est moins détectable par les systèmes de détection d'intrusion (IDS) car il ne complète pas la connexion TCP.
- \*\*Rapidité :\*\* Il est généralement plus rapide que le TCP Full Open Scan car il n'attend pas la réponse complète.

### Inconvénients :

- \*\*Déetectabilité :\*\* Bien qu'il soit moins détectable que le TCP Full Open Scan, il peut toujours être détecté par des systèmes de sécurité sophistiqués.
- \*\*Fiabilité :\*\* Il peut générer des faux positifs car certains systèmes peuvent ne pas répondre correctement aux paquets SYN.

## Inverse TCP Flags

Les "Inverse TCP Flags" (aussi appelés "TCP Flags Filtered") sont une technique de scan utilisée pour découvrir les ports ouverts sur un hôte en exploitant des comportements particuliers des pare-feu et des systèmes de détection d'intrusion (IDS). L'idée est de manipuler les drapeaux TCP de manière à ce que le scan ressemble à un trafic réseau légitime. La réaction à ce type de scan dépend de l'implémentation de la pile TCP/IP du système d'exploitation scanné (ainsi, certains Windows risque de ne pas réagir correctement à ce type de scan sachant que ce type d'OS n'utilise pas la pile TCP/IP standard).

XMAS Scan :

***nmap -sX -v @IP***

```

Zenmap
Scan Tools Profile Help
Target: 10.1.2.5 Profile: Scan Cancel
Command: nmap -sX -v 10.1.2.5

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
Service
X11
ajp13
cproxy-ftp
domain
exec
ftp
http
ingreslock
irc
login
microsoft-ds
mysql
netbios-ssn
nfs
postgresql
rmiregistry
rpcbind
shell
smtp
telnet
unknown
vnc
MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
Raw packets sent: 1024 (40.948KB) | Rcvd: 978 (39.108KB)

```

**MAIMON Scan :**

***nmap -sM -v @IP***

**ACK Scan :**

***nmap -sA -v @IP***

**NULL Scan :**

***nmap -sN -v @IP***

```

Zenmap
Scan Tools Profile Help
Target: 10.1.2.5 Profile: Scan Cancel
Command: nmap -sN -v 10.1.2.5

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
Service
X11
ajp13
cproxy-ftp
domain
exec
ftp
http
ingreslock
irc
login
microsoft-ds
mysql
netbios-ssn
nfs
postgresql
rmiregistry
rpcbind
shell
smtp
telnet
unknown
vnc
MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.52s
Raw packets sent: 1024 (40.948KB) | Rcvd: 978 (39.108KB)

```

## **2.13. Détection de la version des services actifs**

Il est possible de détecter la version des services actifs sur le système scanné afin de pouvoir effectuer les recherches nécessaires dans l'objectif de déceler des vulnérabilités connues à exploiter.

***nmap -sV -v @IP***

- 1- Identifier l'adresse IP de la machine cible (Metasploitable2)
- 2- Exécuter la commande nmap ou bien utiliser Zenmap afin de détecter les services actifs sur la machine en question et identifier ainsi les versions des services.
- 3- Faire des recherches afin de détecter d'éventuelles failles/vulnérabilités exploitables au niveau des services ainsi détectés.

The screenshot shows the Zenmap interface with the target set to 10.1.2.5. The command entered is "nmap -sV -v 10.1.2.5". The results table displays the following information:

Service	Port	State	Protocol	Version
X11	108/tcp	closed	tcp	X11 protocol
ajp13	8009/tcp	open	tcp	AJP13 [Apache Tomcat/4.1.33]
bindshell	22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
domain	53/tcp	open	dns	ISC BIND 9.4.2
exec	23/tcp	open	telnet	Postfix telnetd
ftp	21/tcp	open	ftp	vsftpd 2.3.4
http	80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
irc	119/tcp	open	irc	ircd 2 (RPC 1.0.0)
java-rmi	109/tcp	open	rmi	JRMP/Java RMI
login	513/tcp	open	login	OpenBSD or Solaris rlogind
mysql	3306/tcp	open	mysql	MySQL 5.0.51a-Subuntu5
netbios-ssn	139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
nfs	512/tcp	open	exec	netkit-rsh rexecd
postgres	5432/tcp	open	postgres	PostgreSQL 8.3.0 - 8.3.7
rpcbind	10000/tcp	open	rpcbind	(protocol 3.3)
smtp	25/tcp	open	smtp	ProFTPD 1.3.1
ssh	22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
tcpwrapped	2049/tcp	open	nfs	2-4 (RPC #100003)
telnet	23/tcp	open	telnet	PostgreSQL 8.3.0 - 8.3.7
vnc	5900/tcp	open	x11	(access denied)
	6667/tcp	open	irc	UnrealIRCd
	8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
	8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

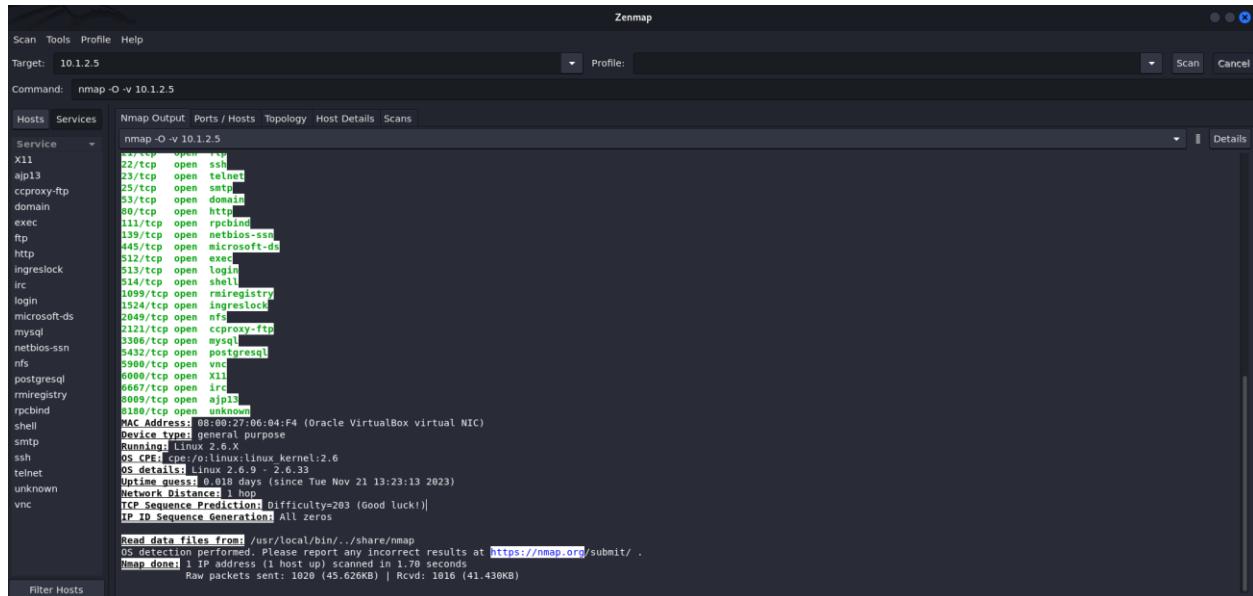
Other details shown in the interface include MAC Address: 08:00:27:06:04:F4, Service Info Hosts: metasploitable.localdomain | irc.Metasploitable.LAN, and various service detection and reporting messages at the bottom.

## **2.14. Détection de la version du système d'exploitation**

Il est possible de détecter la version du système d'exploitation sur le système scanné afin de pouvoir effectuer les recherches nécessaires dans l'objectif de déceler des vulnérabilités connues à exploiter.

***nmap -O -v @IP***

- 1- Identifier l'adresse IP de la machine cible (Metasploitable2)
- 2- Exécuter la commande nmap ou bien utiliser Zenmap afin de détecter la version du système d'exploitation sur la machine en.
- 3- Faire des recherches afin de détecter d'éventuelles failles/vulnérabilités exploitables au niveau du système d'exploitation ainsi détecté.



Il est aussi possible d'utiliser nmap avec les scripts NSE afin de détecter le système d'exploitation :

***nmap --script smb-os-discovery.nse -v @IP***

- 1- Effectuer une nouvelle détection de la version du système d'exploitation en utilisant le script.
- 2- Explorer les autres scripts possibles avec nmap.

```

Zenmap
Scan Tools Profile Help
Target: 10.1.2.5 Profile: Scan Cancel
Command: nmap -v --script smb-os-discovery 10.1.2.5
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Services
Service - nmap -v --script smb-os-discovery 10.1.2.5
Ports
Host Script Results:
NSE: Script Post-scanning.
Initiating NSE at 13:51
Completed: 1 hosts (1 up) | 0.00s elapsed
read_data_file from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
MAC Address: 08:00:27:06:04:F4 (Oracle VirtualBox virtual NIC)
Filter Hosts

```

***Essayer d'effectuer la même manipulation avec une machine cible utilisant un système d'exploitation Windows.***

## **2.15. Evasion IDS/IPS/Firewall**

L'objectif de tout pirate est de rester indéetectable (furtivité). Cet objectif peut être atteint en utilisant plusieurs techniques, parmi lesquelles :

- 1- Fragmentation des paquets :

```
nmap -f -v @IP
```

- 2- Source port manipulation

```
nmap -g 80 -v @IP
```

- 3- MTU manipulation

```
nmap -mtu 8 -v @IP
```

- 4- IP Decoy

```
nmap -D RND :10 -v @IP
```

- 5- Envoyer une suite de 0 et 1 à la machine cible

```
nmap -v @IP --data Oxdeadbeef
```

- 6- Envoyer une chaîne de caractères ordinaires en tant que payload

```
nmap -v @IP --data-string 'la_chaine_de_caracteres' -p 80
```

- 7- Envoyer une chaîne de taille aléatoire en tant que payload

```
nmap -v @IP --data-length 1024 -p 80
```

*Dans tous les exemples précédents, essayer de lancer une capture du trafic réseau sur la machine cible et analyser les paquets capturés et commenter.*

## **2.16. Détection des vulnérabilité en utilisant Greenbone-OpenVAS (GVM)**

1- Mettre à jour votre installation Kali linux :

```
#apt update && apt full-upgrade
```

2- Avec la version actuelle de Kali, GVM supporte la version 16 du PG Cluster.

Vérifier les PG clusters installés (15 et 16) :

```
#pg_lsclusters
```

```
(root㉿kali)-[~]
# pg_lsclusters
Ver Cluster Port Status Owner   Data directory          Log file
15 main      5432 down    postgres /var/lib/postgresql/15/main /var/log/postgresql/postgresql-15-main.log
16 main      5433 down    postgres /var/lib/postgresql/16/main /var/log/postgresql/postgresql-16-main.log

(root㉿kali)-[~]
#
```

Effacer le cluster 15 :

```
#pg_dropcluster --stop 15 main
```

```
(root㉿kali)-[~]
# pg_dropcluster --stop 15 main

(root㉿kali)-[~]
#
```

Configurer le cluster 16 pour lancer l'écoute sur le port standard 5432 :

```
#nano /etc/postgres/16/main/postgresql.conf
```

```
(root㉿kali)-[~]
# nano /etc/postgresql/16/main/postgresql.conf #
```

```

data_directory = '/var/lib/postgresql/16/main'          # use data in another directory
                                                # (change requires restart)
hba_file = '/etc/postgresql/16/main/pg_hba.conf'      # host-based authentication file
                                                # (change requires restart)
ident_file = '/etc/postgresql/16/main/pg_ident.conf'  # ident configuration file
                                                # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/16-main.pid'   # write an extra PID file
                                                # (change requires restart)

#-----
# CONNECTIONS AND AUTHENTICATION
#-----

# - Connection Settings -
listen_addresses = 'localhost'                      # what IP address(es) to listen on;
                                                # comma-separated list of addresses;
                                                # defaults to 'localhost'; use '*' for all
                                                # (change requires restart)
port = 5433                                         # (change requires restart)
max_connections = 100                                # (change requires restart)
#superuser_reserved_connections = 0                 # (change requires restart)
unix_socket_directories = '/var/run/postgresql'     # comma-separated list of directories
                                                # (change requires restart)
#unix_socket_group = ''                            # (change requires restart)
#unix_socket_permissions = 0777                   # begin with 0 to use octal notation
                                                # (change requires restart)
#Bonjour = off                                     # advertise server via Bonjour
                                                # (change requires restart)
#Bonjour_name = ''                                 # defaults to the computer name
                                                # (change requires restart)

# - TCP settings -
# see "man tcp" for details
tcp_keepalives_idle = 0                             # TCP_KEEPIDLE, in seconds;
                                                # 0 selects the system default
tcp_keepalives_interval = 0                         # TCP_KEEPINTVL, in seconds;
                                                # 0 selects the system default
tcp_keepalives_count = 0                           # TCP_KEEPCNT;
                                                #
```

(rechercher une éventuelle valeur 543x tq 5433 et la remplacer par 5432)

Redémarrer le service PostgreSQL :

```
#systemctl restart postgresql.service
```

(root@kali)-[~] # systemctl restart postgresql.service  
(root@kali)-[~] #

3- Lancer la configuration de GVM :

```
#gvm-setup
```

```
[root@kali] ~
# gvm-setup

[>] Starting PostgreSQL service
[>] Creating GVM's certificate files
[>] Creating PostgreSQL database
[*] creating database user
[*] Creating database
[*] Creating permissions
CREATE ROLE
[*] Applying permissions
GRANT ROLE

[*] Creating extension uuid-ossp
CREATE EXTENSION

[*] Creating extension pgcrypto
CREATE EXTENSION

[*] creating extension pg-gvm
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password 'a2c77024-5d3d-46d1-86a4-60379af03c63'.
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '.gvm' and group '.gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
: Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-feed/22.04/vt-data/notus/ to /var/lib/notus
```

Attention : lors du processus de configuration, le mot de passe à utiliser par l'utilisateur admin sera affiché. Il faut le copier pour pouvoir se connecter lors de la première fois et ainsi modifier ce mot de passe.

A la fin de la configuration, vous recevrez un message de notification :

```
[+] Done
[*] Please note the password for the admin user
[*] User created with password 'a2c77024-5d3d-46d1-86a4-60379af03c63'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured

[root@kali] ~
#
```

4- Vérifier que la configuration s'est bien passée :

**#gvm-check-setup**

```

[~] (root㉿kali)-[~]
└─# gvm-check-setup
gvm-check-setup 22.5.0
Test completeness and readiness of GVM-22.5.0
Step 1: Checking OpenVAS (Scanner)...
OK: OpenVAS Scanner is present in version 22.7.5.
OK: Notus Scanner is present in version 22.6.0.
OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/
OK: _gvm owns all files in /var/lib/openvas/gnupg/
OK: redis-server is present.
OK: scanner (db_address setting) is configured properly using the redis-server socket: /var/run/redis-openvas/redis-server.sock
OK: the mqtt_server_uri is defined in /etc/openvas/openvas.conf
OK: _gvm owns all files in /var/lib/openvas/plugins
OK: NVT collection in /var/lib/openvas/plugins contains 87239 NVTs.
OK: The notus directory /var/lib/notus/products contains 451 NVTs.
Checking that the obsolete redis database has been removed
Could not connect to Redis at /var/run/redis-openvas/redis-server.sock: No such file or directory
OK: No old Redis DB
Starting ospd-openvas service
Waiting for ospd-openvas service
OK: ospd-openvas service is active.
OK: ospd-openvas is present in version 22.6.0.
Step 2: Checking GWM Manager (gwm) ...
OK: GWM Manager (gwm) is present in version 22.9.0.
Step 3: Checking Certificates ...
OK: GWM client certificate is valid and present as /var/lib/gvm/CA/clientcert.pem.
OK: Your GWM certificate infrastructure passed validation.
Step 4: Checking data ...
OK: SCAP data found in /var/lib/gvm/scap-data.
OK: CERT data found in /var/lib/gvm/cert-data.
Step 5: Checking Postgresql DB and user ...
OK: Postgresql version and default port are OK.
gwmdb | _gvm | UTF8 | libc | C.UTF-8 | C.UTF-8 | | |
16436|pg-gvm|10|2200|[22.6]|
OK: At least one user exists.
Step 6: Checking Greenbone Security Assistant (GSA) ...
OK: Greenbone Security Assistant is present in version 22.06.0-git.
Step 7: Checking if GVM services are up and running ...
Starting gwm service
Waiting for gwm service

```

## 5- Lancer le service GVM

**#gvm-start**

Fort probablement, les services sont déjà démarré suite à la vérification effectuée précédemment :

```

[~] (root㉿kali)-[~]
└─# gvm-start
[i] GVM services are already running

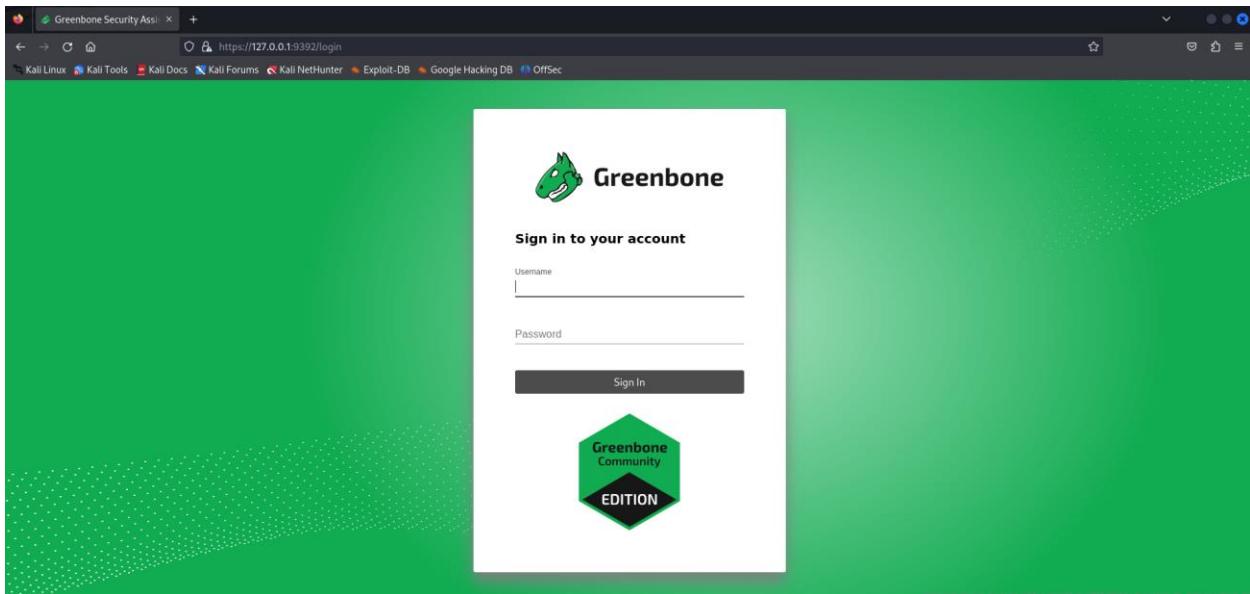
```

## 6- Lancer le nabigateur web (Firefox) et taper l'URL

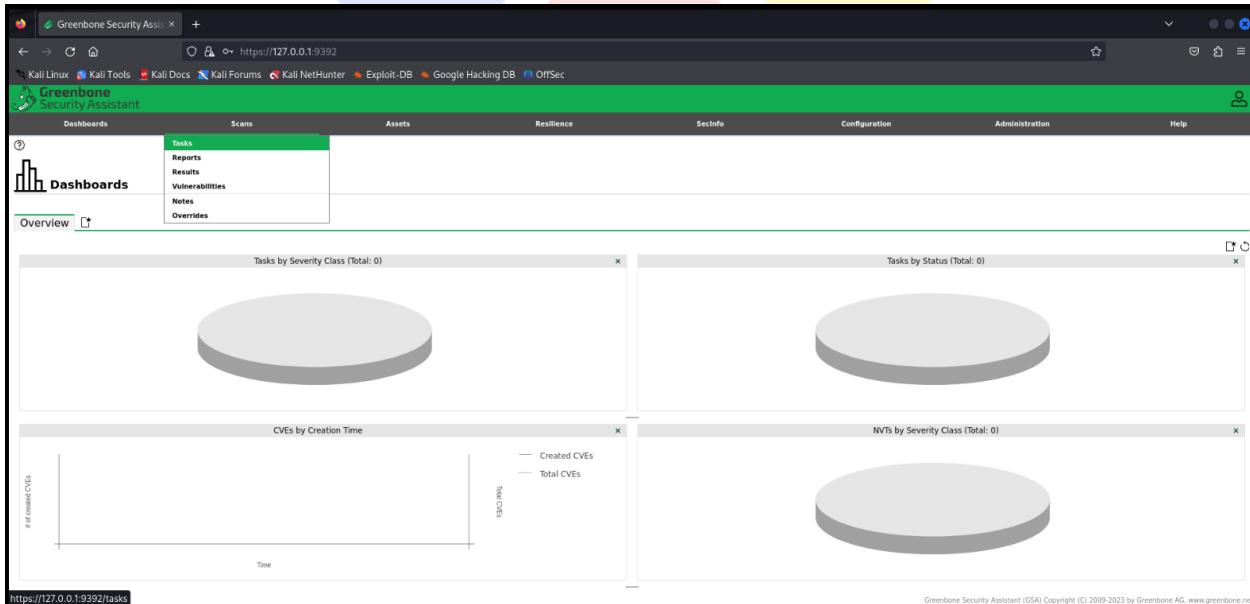
<https://127.0.0.1:9392>

Login : admin

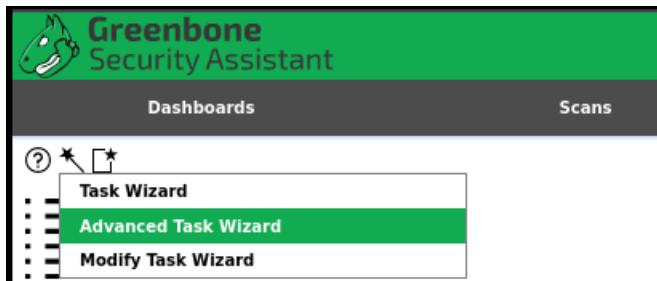
Password : mot de passe copié lors du processus de configuration



- 7- Une fois connecté, pensez à modifier le mot de passe automatiquement généré pour l'utilisateur administrateur.
- 8- Dans le menu « scan », choisir l'option « Tasks »



- 9- En haut, à gauche de l'écran, survoler le bouton « Task Wizard » et choisir l'option « Advanced task wizard »



## 10- Fournir les informations nécessaire à propos de la machine à scanner et lancer le scan :

This screenshot shows the 'Advanced Task Wizard' dialog box. It includes fields for 'Task Name' (MSF21), 'Scan Config' (selected), 'Target Host(s)' (10.1.2.9), 'Start Time' (set to 'Start immediately'), and 'SSH Credential' (selected). A note at the bottom says 'For any other setting the defaults from "My Settings" will be applied.' A 'Create' button is visible at the bottom right.

## 11- Attendre jusqu'à l'achèvement du scan, visualiser le rapport et l'interpréter.

This screenshot shows the 'Report' page for a completed scan. The report title is 'Report:Tue, Nov 21, 2023 3:11 PM UTC'. The report summary table includes columns for Information, Results (67 of 590), Hosts (1 of 1), Ports (18 of 23), Applications (26 of 16), Operating Systems (1 of 1), CVEs (32 of 32), Closed CVEs (0 of 0), TLS Certificates (2 of 2), Error Messages (1 of 1), and User Tags (0). Below the table, detailed log entries show the task name (MSF21), comment (Automatically generated by wizard), scan time (Tue, Nov 21, 2023 3:12 PM UTC - Tue, Nov 21, 2023 3:53 PM UTC), duration (0:41 h), status (Done), filter (apply\_overrides=0 levels=html min\_god=70), and timezone (UTC (UTC)).

## 12- Essayer de proposer des solutions aux éventuelles vulnérabilités détectées.

Greenbone Security Assistant

Report: Tue, Nov 21, 2023 3:11 PM UTC

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
(67 of 590)	(2 of 1)	(18 of 23)	(16 of 16)	(1 of 1)	(32 of 32)	(0 of 0)	(2 of 2)	(1 of 1)	(0 of 1)	(0)

Vulnerability

	Severity	QoD	Host	Name	Location	Created
rlogin Passwordless Login	<span style="color:red">10.0 (High)</span>	80 %	10.1.2.5	513/tcp	Tue, Nov 21, 2023 3:34 PM UTC	
TWiki XSS and Command Execution Vulnerabilities	<span style="color:red">10.0 (High)</span>	80 %	10.1.2.5	80/tcp	Tue, Nov 21, 2023 3:39 PM UTC	
The rexec service is running	<span style="color:red">10.0 (High)</span>	80 %	10.1.2.5	512/tcp	Tue, Nov 21, 2023 3:38 PM UTC	
Distributed Ruby (dRuby/Rb) Multiple Remote Code Execution Vulnerabilities	<span style="color:red">10.0 (High)</span>	99 %	10.1.2.5	8787/tcp	Tue, Nov 21, 2023 3:41 PM UTC	
Possible Backdoor: Ingreslock	<span style="color:red">10.0 (High)</span>	99 %	10.1.2.5	1524/tcp	Tue, Nov 21, 2023 3:45 PM UTC	
Operating System (OS) End of Life (EOL) Detection	<span style="color:red">10.0 (High)</span>	80 %	10.1.2.5	general/tcp	Tue, Nov 21, 2023 3:36 PM UTC	
MySQL / MariaDB Default Credentials (MySQL Protocol)	<span style="color:red">9.0 (High)</span>	95 %	10.1.2.5	3306/tcp	Tue, Nov 21, 2023 3:41 PM UTC	
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	<span style="color:red">9.0 (High)</span>	99 %	10.1.2.5	8009/tcp	Tue, Nov 21, 2023 3:47 PM UTC	
DistCC RCE Vulnerability (CVE-2004-3687)	<span style="color:red">9.0 (High)</span>	99 %	10.1.2.5	3632/tcp	Tue, Nov 21, 2023 3:41 PM UTC	
VNC Brute Force Login	<span style="color:red">9.0 (High)</span>	95 %	10.1.2.5	5900/tcp	Tue, Nov 21, 2023 3:40 PM UTC	
PostgreSQL Default Credentials (PostgreSQL Protocol)	<span style="color:red">9.0 (High)</span>	99 %	10.1.2.5	5432/tcp	Tue, Nov 21, 2023 3:41 PM UTC	
UnrealIRCd Authentication Specifying Vulnerability	<span style="color:red">8.5 (High)</span>	80 %	10.1.2.5	6697/tcp	Tue, Nov 21, 2023 3:35 PM UTC	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	<span style="color:red">7.5 (High)</span>	95 %	10.1.2.5	80/tcp	Tue, Nov 21, 2023 3:50 PM UTC	
prinzipal/ output Reporting	<span style="color:red">7.5 (High)</span>	80 %	10.1.2.5	80/tcp	Tue, Nov 21, 2023 3:40 PM UTC	
The rlogin service is running	<span style="color:red">7.5 (High)</span>	80 %	10.1.2.5	513/tcp	Tue, Nov 21, 2023 3:38 PM UTC	
rsh Unencrypted Cleartext Login	<span style="color:red">7.5 (High)</span>	80 %	10.1.2.5	514/tcp	Tue, Nov 21, 2023 3:38 PM UTC	
FTP Brute Force Logins Reporting	<span style="color:red">7.5 (High)</span>	95 %	10.1.2.5	2121/tcp	Tue, Nov 21, 2023 3:42 PM UTC	
FTP Brute Force Logins Reporting	<span style="color:red">7.5 (High)</span>	95 %	10.1.2.5	2137/tcp	Tue, Nov 21, 2023 3:42 PM UTC	
UnrealIRCd Backdoor	<span style="color:red">7.5 (High)</span>	70 %	10.1.2.5	6697/tcp	Tue, Nov 21, 2023 3:42 PM UTC	

Greenbone Security Assistant

Report: Tue, Nov 21, 2023 3:11 PM UTC

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
(67 of 590)	(2 of 1)	(18 of 23)	(16 of 16)	(1 of 1)	(32 of 32)	(0 of 0)	(2 of 2)	(1 of 1)	(0 of 1)	(0)

Vulnerability

	Severity	QoD	Host	Name	Location	Created
rlogin Passwordless Login	<span style="color:red">10.0 (High)</span>	80 %	10.1.2.5	513/tcp	Tue, Nov 21, 2023 3:34 PM UTC	

**Summary**

The rlogin service allows root access without a password.

**Detection Result**

It was possible to gain root access without a password.

**Detection Method**

Checks if a vulnerable version is present on the target host.

Details: [rlogin Passwordless Login OID: 1.3.6.1.4.1.25623.1.0.113766](#)

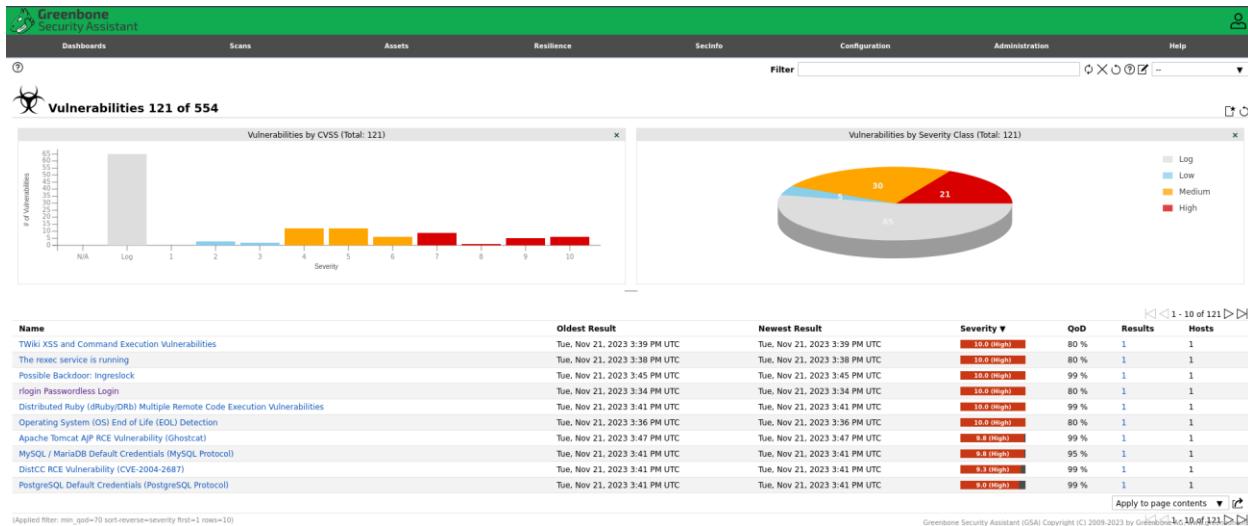
Version used: 2020-09-30T09:30:12Z

**Impact**

This vulnerability allows an attacker to gain complete control over the target system.

**Solution**

**Solution Type:** Mitigation  
Disable the rlogin service and use alternatives like SSH instead.

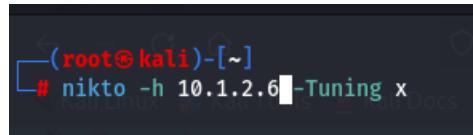


## 2.17. Scan des vulnérabilités en utilisant NIKTO

1- Lancer le scan de la machine cible en utilisant la commande :

```
#nikto -h @ip -Tuning x
```

Avec *x* pour indiquer l’application de tous les filtres de scan mis à part ceux qui seront mentionnés en argument. Comme aucun n’est mentionné, tous les scans seront effectués



2- Attendre la fin du scan, le résultat sera affiché à l’écran à défaut de l’avoir redirigé vers un fichier de sortie :

```
(root㉿kali)-[~]
# nikto -h 10.1.2.6 -Tuning x
Nikto v2.8.0

+ Target IP:      10.1.2.6
+ Target Hostname: 10.1.2.6
+ Target Port:    80
+ Start Time:   2023-11-21 16:26:12 (GMT1)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-ZhUbuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misleading-content-type-header/
+ /index: Content header 'text' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisci.it/sectou.php?id=498ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ 66k requests: 0 errors and 0 warnings from remote host
+ End Time:   2023-11-21 16:26:14 (GMT1) (2 Seconds)

+ 1 host(s) tested

(root㉿kali)-[~]
```

- 3- Effectuer le scan sur différentes machines cibles et interpréter le résultat à chaque fois tout en présentant des solutions de mitigation pour les non-conformités recensées.

## **2.18. MAC Flooding en utilisant « macof »**

L'outil **macof** (MAC OverFlow) est un outil inclus dans la distribution Kali Linux qui fait partie du package dsniff. Il est conçu pour générer un grand nombre de trames ARP (Address Resolution Protocol) falsifiées dans un réseau local. Les attaques ARP sont souvent utilisées dans le cadre d'attaques de type Man-in-the-Middle (MitM) pour rediriger le trafic réseau à travers l'attaquant.

### Objectif Principal :

L'objectif principal de `macof` est de saturer la table ARP d'un hôte cible en injectant de fausses entrées ARP. Cela peut conduire à une confusion dans la résolution d'adresses MAC vers adresses IP, perturbant ainsi la communication normale entre les machines sur le réseau.

### Risques et Éthique :

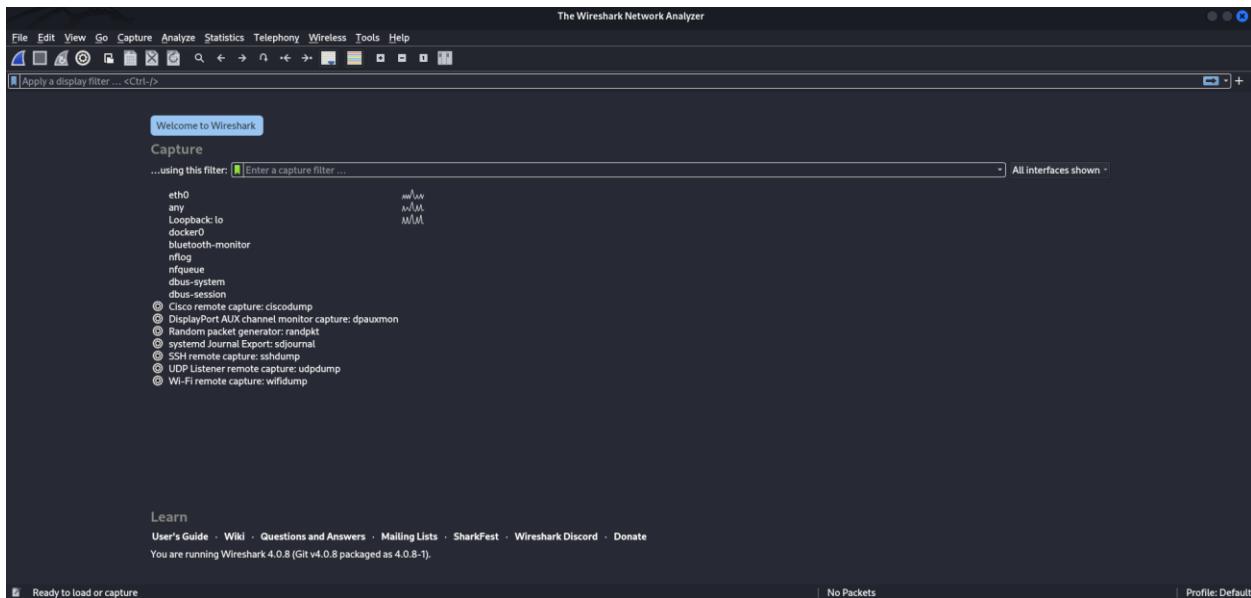
1. L'utilisation de `macof` peut entraîner une saturation de la table ARP des hôtes cibles, entraînant des problèmes de connectivité dans le réseau.
2. Les attaques ARP sont souvent considérées comme malveillantes et peuvent être détectées par des systèmes de détection d'intrusion (IDS).
3. L'utilisation d'outils tels que `macof` doit être effectuée de manière éthique et légale, avec l'autorisation explicite du propriétaire du réseau.

### Conseils Supplémentaires :

- `macof` est principalement utilisé à des fins éducatives pour comprendre les vulnérabilités liées aux attaques ARP. Il est crucial de l'utiliser de manière responsable et de ne pas lancer d'attaques non autorisées.
- Lors de l'utilisation de tels outils, assurez-vous de comprendre les lois et les politiques en matière de sécurité informatique dans votre région.

L'utilisation de `macof` ou d'outils similaires doit être effectuée dans un contexte éthique et avec l'autorisation appropriée. Il est essentiel de respecter la vie privée et la sécurité des réseaux lors de l'utilisation de tels outils.

## 1- Lancer wireshark au niveau de votre Kali Linux :



Attention : Pour une meilleure efficacité et afin d'atteindre les objectifs des exercices, il faut que la carte réseau soit configuré en mode promiscuité (promiscuous mode).

## 2- Lancer la capture avec wireshark

3- Générer un nombre de paquet déterminer à diffuser via la carte réseau

```
#macof -i eth0 n 10
```

```
(root㉿kali)-[~]
# macof -i eth0 -n 10
27:44:e2:29:92:a 5d:4d:fd:39:ab:a4 0.0.0.0.3854 > 0.0.0.0.61675: S 1484359251:1484359251(0) win 512
4a:7d:ff:1b:8d:a6 41:af:81:66:4b:38 0.0.0.0.55601 > 0.0.0.0.62208: S 1797432255:1797432255(0) win 512
5d:b:b5:5a:29:2b ba:a2:48:5c:e6:ed 0.0.0.0.15946 > 0.0.0.0.18992: S 28486856:28486856(0) win 512
12:c7:ad:1:85:1c 2d:48:ea:61:1a:50 0.0.0.0.42378 > 0.0.0.0.20543: S 1837754608:1837754608(0) win 512 wp-d
87:59:8e:51:c4:6f 78:2:6c:28:d8:40 0.0.0.0.15835 > 0.0.0.0.321: S 1484859006:1484859006(0) win 512 494 N
e1:de:15:6e:12:65 3a:72:ab:5:f9:cb 0.0.0.0.26148 > 0.0.0.0.4419: S 698448458:698448458(0) win 512 wp-d
34:6:c:94:44:ab:6c ab:90:78:20:df:da 0.0.0.0.16494 > 0.0.0.0.57935: S 1086194134:1086194134(0) win 512 494 N
b1:7:a:f6:6b:a9:6d 1b:72:92:14:8b:91 0.0.0.0.0.7562 > 0.0.0.0.27741: S 2109715006:2109715006(0) win 512 wp-d
11:10:9:29:f4:fc 15:1b:87:66:0:b1 0.0.0.0.35515 > 0.0.0.0.12050: S 1483148657:1483148657(0) win 512 494 N
69:a5:48:1e:a0:96 ec:d6:65:44:d5:74 0.0.0.0.0.26410 > 0.0.0.0.45550: S 1755042252:1755042252(0) win 512 wp-d
1938 27.559458088 10.1.2.5 10.1.2.4 HTTP 589 HTTP/1.1 494 N
7102 10.1.2.4 10.1.2.5 HTTP 381 GET /dvwa/wp-d
# 1940 27.567736834 10.1.2.5 10.1.2.4 HTTP 587 HTTP/1.1 494 N
```

- 4- Cibler une machine et l'inonder par des paquets ARP afin d'altérer la table CAM avec des adresses MAC aléatoires :

```
#macof -i eth0 -d 10.1.2.6 -n 1000
```

```
(root㉿kali)-[~]
# macof -i eth0 -d 10.1.2.6 -n 1000
c0:64:30:57:8a:c2 e3:fb:43:1:5e:e2 0.0.0.0.16930 > 10.1.2.6.34033: S 1846777800:1846777800(0) win 512
25:66:84:36:28:c2 1a:ef:d8:46:aa:7a 0.0.0.0.247 > 10.1.2.6.47533: S 360032372:360032372(0) win 512
3c:32:bd:10:b:43 14:46:80:12:14:53 0.0.0.0.5287 > 10.1.2.6.26249: S 1583399026:1583399026(0) win 512
cb:7c:8b:75:af:16 cc:a4:e3:31:e5:dc 0.0.0.0.6458 > 10.1.2.6.55820: S 1850525362:1850525362(0) win 512
a3:d8:8c:43:f0:39 86:e1:8c:7d:3b:f8 0.0.0.0.41275 > 10.1.2.6.11824: S 843751161:843751161(0) win 512
ad:af:79:7f:f2:a f7:64:7f:f:dd:a3 0.0.0.0.46977 > 10.1.2.6.64625: S 1854419575:1854419575(0) win 512
38:e9:e1:27:89:87 36:28:ab:b:8a:d3 0.0.0.0.51855 > 10.1.2.6.43578: S 292668757:292668757(0) win 512
d7:6e:9e:54:d3:b0 b7:93:77:3e:ad:1c 0.0.0.0.3103 > 10.1.2.6.64447: S 30032758:30032758(0) win 512
c4:f2:36:2a:70:73 bf:ad:3c:6:87:d3 0.0.0.0.48877 > 10.1.2.6.18431: S 1832606009:1832606009(0) win 512
ba:86:c6:78:e7:42 4b:e2:8d:4b:8f:14 0.0.0.0.46434 > 10.1.2.6.18545: S 1295702609:1295702609(0) win 512
f2:de:e3:4:c6:51 97:29:72:5:c:30:b0 0.0.0.0.46813 > 10.1.2.6.33375: S 1290298624:1290298624(0) win 512
da:dd:a3:30:a8:2d 7:54:1:a:75:35:f1 0.0.0.0.48273 > 10.1.2.6.42290: S 2097455399:2097455399(0) win 512 ff)
b:30:15:34:2:a:e6 5:e:89:3:f:1:c:f9:f0 0.0.0.0.59524 > 10.1.2.6.7891: S 1335634591:1335634591(0) win 512
b:27:2:a:2d:ac:42 2:b:b2:e6:31:78:3 0.0.0.0.13785 > 10.1.2.6.2434: S 966839358:966839358(0) win 512
a8:65:b7:5:a:3:e:88 2:c:1:d2:7:b:40:c4 0.0.0.0.10918 > 10.1.2.6.3427: S 831247975:831247975(0) win 512
80:34:74:15:25:ad 4:e:93:27:0:1:d:a9 0.0.0.0.31136 > 10.1.2.6.20156: S 26116274:26116274(0) win 512
4:aa:3:c:d:13:a1 73:af:13:2:a:c7:f3 0.0.0.0.7219 > 10.1.2.6.22489: S 59503924:59503924(0) win 512
ca:23:e8:69:42:2 4:c:dd:73:1:a:c7:d8 0.0.0.0.65533 > 10.1.2.6.54725: S 15173115:15173115(0) win 512
69:c1:2:3:f:45:94 67:a9:47:75:b5:f5 0.0.0.0.19412 > 10.1.2.6.35115: S 502655330:502655330(0) win 512
92:8:f:39:73:14:56 b3:3:b:a8:23:18:62 0.0.0.0.32878 > 10.1.2.6.15263: S 2110980937:2110980937(0) win 512
a2:b4:30:23:f6:58 ab:dd:cc:10:b3:c9 0.0.0.0.61625 > 10.1.2.6.49523: S 610016020:610016020(0) win 512
34:8:c:3d:35:36:15 81:1:d:bd:1:c:2:d:8 0.0.0.0.52867 > 10.1.2.6.30428: S 975720752:975720752(0) win 512
c9:22:e7:1:f:85:14 db:db:39:58:cc:1f 0.0.0.0.2601 > 10.1.2.6.32551: S 1029717000:1029717000(0) win 512
e:98:88:67:8:35 f5:37:a5:60:4d:f5 0.0.0.0.29072 > 10.1.2.6.25541: S 1549367861:1549367861(0) win 512
f4:e5:8:b:6:e:2:98 7:c:e5:2:d:32:db:87 0.0.0.0.11489 > 10.1.2.6.49689: S 688392345:688392345(0) win 512
b8:8:e5:7:7d:28 83:b0:58:1:d:5:a:3d 0.0.0.0.25184 > 10.1.2.6.61807: S 2033258953:2033258953(0) win 512
4:e:8:a:4:a:71:21:8:a 3:c:ac:dd:46:17:13 0.0.0.0.10274 > 10.1.2.6.11186: S 992756698:992756698(0) win 512
39:66:9:37:c:b:e2 d9:da:b1:30:7:c:75 0.0.0.0.9101 > 10.1.2.6.36135: S 967837047:967837047(0) win 512
d1:d7:36:62:41:1 9:aa:99:4:8:b:7:c 0.0.0.0.55072 > 10.1.2.6.19047: S 719103068:719103068(0) win 512
3:a:30:8:e:7:c:a8:c0 5:1:44:4:c:79:a6 0.0.0.0.22378 > 10.1.2.6.39315: S 178701490:178701490(0) win 512
ca:f8:eb:48:a:fb 7:c:33:ad:2:c:b2:76 0.0.0.0.17141 > 10.1.2.6.33342: S 994923133:994923133(0) win 512
52:2:c:79:79:f1:9:a fa:62:6:e:56:cd:22 0.0.0.0.15018 > 10.1.2.6.53616: S 1509193616:1509193616(0) win 512
```

- 5- Essayer d'interpréter les paquets capturés au niveau de wireshark

## **2.19.      DHCP starvation**

L'attaque DHCP Starvation est une attaque réseau qui vise à saturer le pool d'adresses IP disponibles dans un réseau en envoyant de manière agressive de nombreuses demandes DHCP (Dynamic Host Configuration Protocol). Le protocole DHCP est utilisé pour attribuer dynamiquement des adresses IP aux clients dans un réseau.

### **### 1. \*\*Fonctionnement du DHCP :\*\***

Le DHCP est un protocole utilisé pour automatiser la configuration des paramètres IP sur un réseau. Lorsqu'un client se connecte au réseau, il envoie une requête DHCP pour obtenir une adresse IP, une passerelle par défaut, des serveurs DNS, etc.

### **### 2. \*\*Fonctionnement Normal de DHCP :\*\***

1. **Discover (Découverte) :** Le client envoie une demande DHCP pour découvrir les serveurs DHCP disponibles.
2. **Offer (Offre) :** Les serveurs DHCP disponibles répondent avec des offres contenant des informations de configuration.
3. **Request (Demande) :** Le client choisit une offre et envoie une demande pour cette configuration.
4. **Acknowledge (Accusé de réception) :** Le serveur DHCP sélectionné envoie un accusé de réception, attribuant au client les paramètres de configuration.

### **### 3. \*\*Fonctionnement de l'Attaque DHCP Starvation :\*\***

1. **Discovery Flooding :** L'attaquant envoie de manière répétée un grand nombre de demandes DHCP Discover sur le réseau, souvent à l'aide d'outils automatisés.
2. **Épuisement du Pool :** Les serveurs DHCP du réseau peuvent rapidement épuiser leur pool d'adresses IP disponibles en essayant de répondre à toutes les demandes Discover de l'attaquant.
3. **Atteinte à la Connectivité :** Si le pool d'adresses IP est saturé, de nouveaux clients légitimes qui se connectent au réseau ne peuvent pas obtenir d'adresse IP valide. Cela peut entraîner une perte de connectivité pour ces clients.

---

#### ### 4. \*\*Détection et Protection :\*\*

- \*\*Surveillance du Traffic DHCP :\*\* Une surveillance continue du trafic DHCP peut aider à détecter des anomalies telles qu'une surcharge soudaine de demandes.
- \*\*Utilisation de VLAN :\*\* L'utilisation de VLAN (Virtual LAN) peut isoler le trafic DHCP à l'intérieur d'un sous-réseau spécifique, limitant l'impact d'une attaque DHCP Starvation.
- \*\*Configuration DHCP Résiliente :\*\* La configuration DHCP peut être ajustée pour gérer des attaques potentielles, notamment en limitant le nombre de réponses DHCP par client ou en définissant des réservations d'adresses IP.

#### ### 5. \*\*Contre-Mesures et Bonnes Pratiques :\*\*

- \*\*Surveillance Active :\*\* Surveillez activement le trafic DHCP pour détecter tout comportement anormal.
- \*\*Limitation des Réponses :\*\* Configurez les serveurs DHCP pour limiter le nombre de réponses par client afin de prévenir les attaques de saturation.
- \*\*Utilisation de Méthodes d'Authentification :\*\* L'authentification des clients DHCP peut fournir une couche de sécurité supplémentaire.
- \*\*Politiques de Sécurité :\*\* Établissez des politiques de sécurité claires et appliquez des pratiques d'atténuation contre les attaques DHCP.

L'attaque DHCP Starvation souligne l'importance de sécuriser les services DHCP et de mettre en place des mesures de surveillance pour détecter et atténuer ce type d'attaques potentielles.

- 1- Lancer wireshark sur la machine Kali Linux et lancer la capture
- 2- Lancer un terminal en mode root et lancer l'outil Yersina en mode interactif :

**#yersinia -I**

```

root@kali:~ [20:49:46]
--- versinia 0.8.2 by Slay & tomac - STP mode ---
RootId      BridgeId      Port      Iface Last seen
[20:49:46]

Notification window
Warning: interface eth0 selected as the default one
Press any key to continue

Total Packets: 0      STP Packets: 0      MAC Spoofing [X]
You've got a message
--- STP Fields ---
Source MAC 0A:23:16:02:FF:00 Destination MAC 01:00:C2:00:00:00
18 0000 Ver 00 Type 00 Flags 00 RootId 5088.760F0E14AC58 Pathcost 00000000
BridgeId C0B9.E7CD9811?CAA Port 6002 Age 0000 Max 0014 Hello 0002 Fwd 000F


```

- 3- Taper sur n'importe quelle touche pour quitter l'écran de bienvenue, taper F2 afin de sélectionner « DHCP », ensuite taper « x » afin de lister les attaques disponibles :

```

root@kali:~ [20:51:37]
--- versinia 0.8.2 by Slay & tomac - DHCP mode ---
SIP      DIP      MessageType      Iface Last seen
[20:51:37]

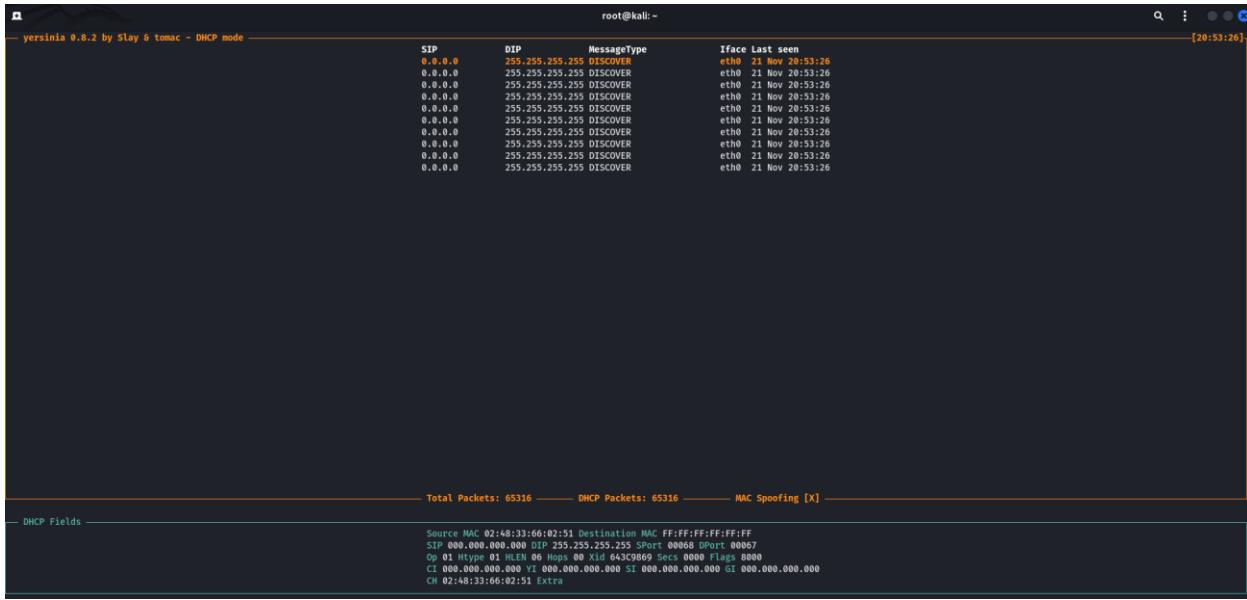
Attack Panel
No  DoS  Description
0   X    sending RAW packet
1   X    sending DISCOVER packet
2   X    creating DHCP rogue server
3   X    sending RELEASE packet

Select attack to launch ('q' to quit)

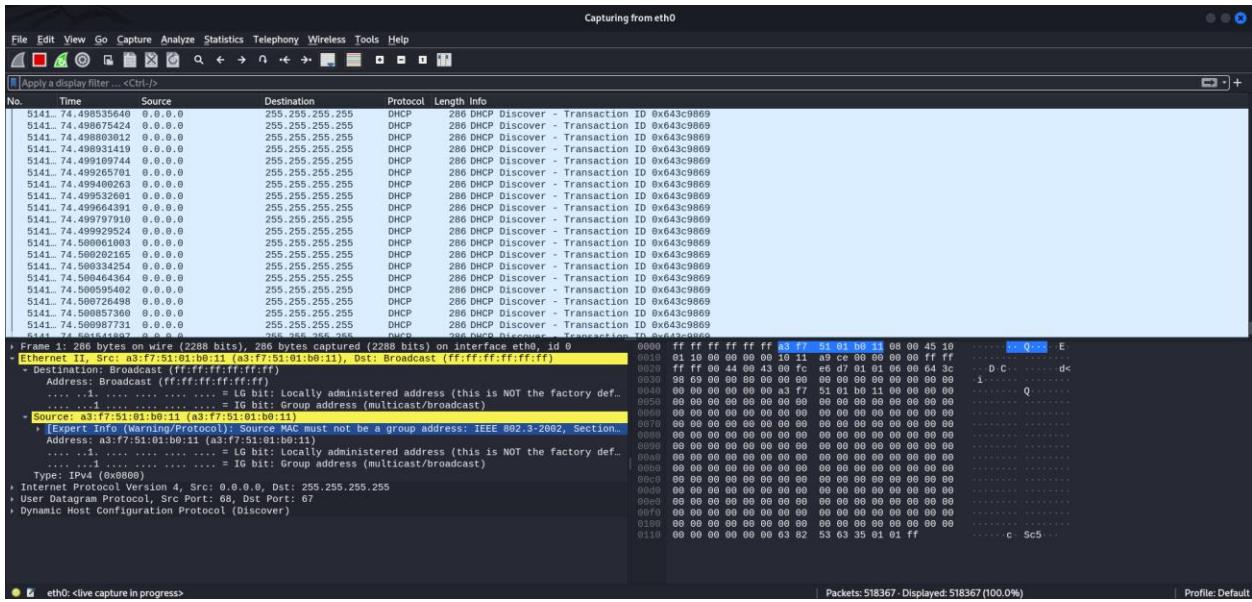
Total Packets: 0      DHCP Packets: 0      MAC Spoofing [X]
These strange attacks...
--- DHCP Fields ---
Source MAC 02:48:33:66:02:51 Destination MAC FF:FF:FF:FF:FF:FF
SIP 000.000.000.000 DIP 255.255.255.255 SPort 00068 DPort 00067
Op 01 Htype 01 HLEN 06 Hops 00 Xid 643C9869 Secs 0000 Flags 8000
CI 000.000.000.000 Yi 000.000.000.000 SI 000.000.000.000 GI 000.000.000.000
CR 02:48:33:66:02:51 Extra


```

- 4- Taper sur « 1 » pour lancer l'attaque « starvation » :



## 5- Vérifier le résultat avec Wireshark :



## 6- Essayer d'expliquer

- Le fonctionnement du DHCP
- Le paquet DISCOVER
- La signification de l'adresse MAC FF :FF :FF :FF :FF

## **2.20. ARP poisoning**

L'ARP (Address Resolution Protocol) poisoning, également connu sous le nom de "spoofing ARP", est une attaque qui vise à corrompre la table ARP d'un réseau local. L'objectif principal de cette attaque est de rediriger le trafic réseau destiné à une adresse IP spécifique vers une autre adresse MAC, généralement celle de l'attaquant. Cela permet à l'attaquant d'intercepter ou de modifier le trafic réseau entre deux parties.

### Fonctionnement de l'ARP Poisoning :

1. \*\*Découverte du Réseau :\*\* L'attaquant commence par analyser le réseau local pour identifier les adresses IP et MAC des hôtes présents.
2. \*\*Envoi de Paquets ARP Falsifiés :\*\* L'attaquant envoie ensuite des paquets ARP falsifiés (spoofed) annonçant qu'il détient la correspondance entre une adresse IP spécifique et une adresse MAC. Ces paquets ARP falsifiés sont envoyés à l'ensemble du réseau.
3. \*\*Modification de la Table ARP :\*\* Les machines sur le réseau mettent à jour leur table ARP en fonction des informations fournies dans les paquets falsifiés, associant ainsi l'adresse IP de la victime à l'adresse MAC de l'attaquant.
4. \*\*Redirection du Trafic :\*\* Maintenant que la table ARP des victimes a été corrompue, le trafic destiné à une adresse IP spécifique est redirigé vers l'adresse MAC de l'attaquant.
5. \*\*Interception ou Modification :\*\* L'attaquant peut intercepter le trafic entre les victimes, modifier les données en transit, ou mener d'autres types d'attaques, telles que les attaques de type Man-in-the-Middle (MitM).

### Objectifs de l'ARP Poisoning :

1. \*\*Interception de Trafic :\*\* L'attaquant peut intercepter le trafic entre deux parties, y compris les données sensibles telles que les identifiants de connexion.
2. \*\*Attaques Man-in-the-Middle (MitM) :\*\* L'attaquant peut se positionner en tant que relais entre deux parties, permettant la capture et la modification du trafic.

3. \*\*Écoute Passive :\*\* L'ARP poisoning peut également être utilisé de manière passive pour écouter le trafic sans perturber la communication normale.

### ### Contre-Mesures de l'ARP Poisoning :

1. \*\*Utilisation de Protocoles Sécurisés :\*\* L'utilisation de protocoles sécurisés tels que DHCP snooping, DNSSEC, et HTTPS peut aider à atténuer les risques d'ARP poisoning.
2. \*\*Utilisation de VLAN :\*\* L'utilisation de VLAN peut isoler le trafic entre différents sous-réseaux, limitant l'impact potentiel d'une attaque ARP poisoning.
3. \*\*Surveillance du Traffic ARP :\*\* La surveillance active du traffic ARP peut aider à détecter des anomalies telles que des réponses ARP anormales ou une activité excessive.
4. \*\*Listes de Liaisons Statiques :\*\* Configurer des listes de liaisons statiques sur les commutateurs pour associer manuellement des adresses MAC aux ports peut réduire les risques d'ARP poisoning.
5. \*\*Utilisation de Protocoles de Sécurité :\*\* L'utilisation de protocoles tels que IPsec peut aider à sécuriser le trafic réseau contre les interceptions.
6. \*\*Détection et Prévention Automatisées :\*\* Les outils de détection d'ARP poisoning, tels que ARPWatch, peuvent être utilisés pour détecter et prévenir automatiquement de telles attaques.

L'ARP poisoning est une attaque courante et peut être particulièrement efficace dans les réseaux non sécurisés. La mise en œuvre de mesures de sécurité appropriées et la surveillance régulière du trafic ARP sont essentielles pour atténuer les risques associés à ce type d'attaque.

- 1- Lancer Wireshark et lancer la capture sur la carte réseau en mode promiscuité
- 2- Lancer un terminal en mode root
- 3- Lancer l'ARP spoofing avec la commande arpspoof (outil de la suite dsnif)

**#arpspoof -i eth0 -t 10.1.2.5 10.1.2.6**

Ainsi, l'attaquant usurpe l'adresse MAC de la machine 10.1.2.6 et informe la machine 10.1.2.5 de son adresse MAC usurpée.

- 4- Vérifier sur Wireshark les traces de cette usurpation
- 5- Lancer un autre terminal en mode root, lancer la commande

**#arpspoof -i eth0 -t 10.1.2.6 10.1.2.5**

- 6- Sur les deux machines cibles, exécuter la commande suivante pour vérifier les tables ARP :

```
#arp -a
```

- 7- Essayer de lancer une session telnet d'une machine cible vers l'autre et capturer le nom d'utilisateur et le mot de passe sur Wireshark de la machine Kali Linux.