





**SOMMAIRE**

Table des matières

1. **Introduction**………………………………………………………………………………………………………………………………3
2. Wireshark c’est quoi ?.................................................................................................................3
3. Contexte ………………………………………………………………………………………………………………………….……3
4. Besoin…………………………………………………………………………………………………………………………………… 3
5. Cahier des charges …………………………………………………………………………………………………………………4
6. **Mise en Place**…………………………………………………………………………………………………………………………….**5**
7. Installation …………………………………………………………………………………………………………………………….5
8. Détection d’Intrusion……………………………………………………………………………………………………………..7
9. Simulations d’attaques…………………………………………………………………………………………………….7
10. Observations de logs……………………………………………………………………………………………………….8
11. Centralisation de logs avec Graylog……………………………………………………………………………………20

## **Wireshark c’est quoi ?**

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l’analyse de réseaux informatiques, le développement de protocoles, l’éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle Qt pour l’implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles Unix comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autres une version en ligne de commande nommé TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License.

## **Contexte :**

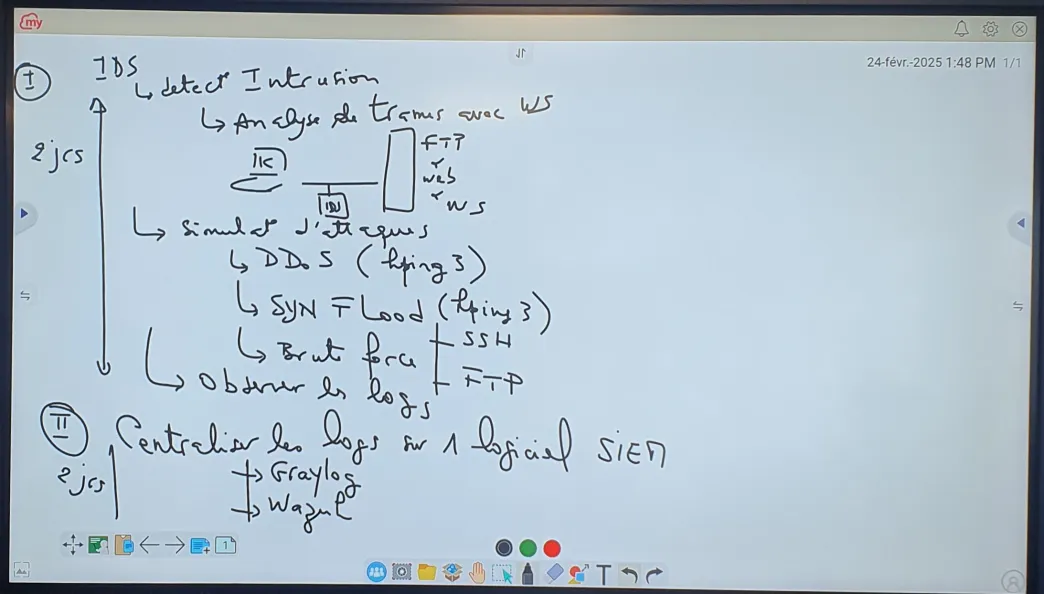
Dans un contexte de cyber-sécurité de plus en plus complexe, notre entreprise a pris l'initiative d'implémenter un système de détection d'intrusion et de centralisation des logs afin de renforcer la protection de ses infrastructures IT et d'optimiser la gestion de la sécurité. Le projet vise à établir un environnement sécurisé pour nos applications critiques, en mettant en place un système de surveillance et une analyse proactive des activités réseau.

Le projet se divise en plusieurs phases distinctes : Installation des équipements et outils, Détection d'Intrusion, Analyse de Trames, Simulations d'Attaques, et la mise en place d'une centralisation des logs avec Graylog. Ces phases permettront de renforcer la visibilité sur l'infrastructure et d'améliorer la capacité de réponse aux incidents.

## **Besoin :**

Dans le cadre de l'évolution rapide des menaces cybernétiques et des vulnérabilités de plus en plus sophistiquées, il est primordial pour notre entreprise de mettre en place une infrastructure de **sécurité réseau robuste** et réactive. Le projet que nous proposons est motivé par un besoin croissant de protéger nos systèmes d'information, d'assurer la confidentialité, l'intégrité, et la disponibilité de nos données, et de pouvoir réagir rapidement aux attaques potentielles.

## **d-Cahier des charges :**



# **Mise en Place :**

1. **Installation**
2. On commence par installer les mises à jour



1. On installe Wireshark



Puis on donne à l’utilisateur les autorisations nécessaires pour utiliser Wireshark :

1. Accédez d’abord à votre compte root à l’aide de la commande suivante :



Si votre mot de passe root est égaré ou n'a pas été défini précédemment, il peut être défini en exécutant la commande :



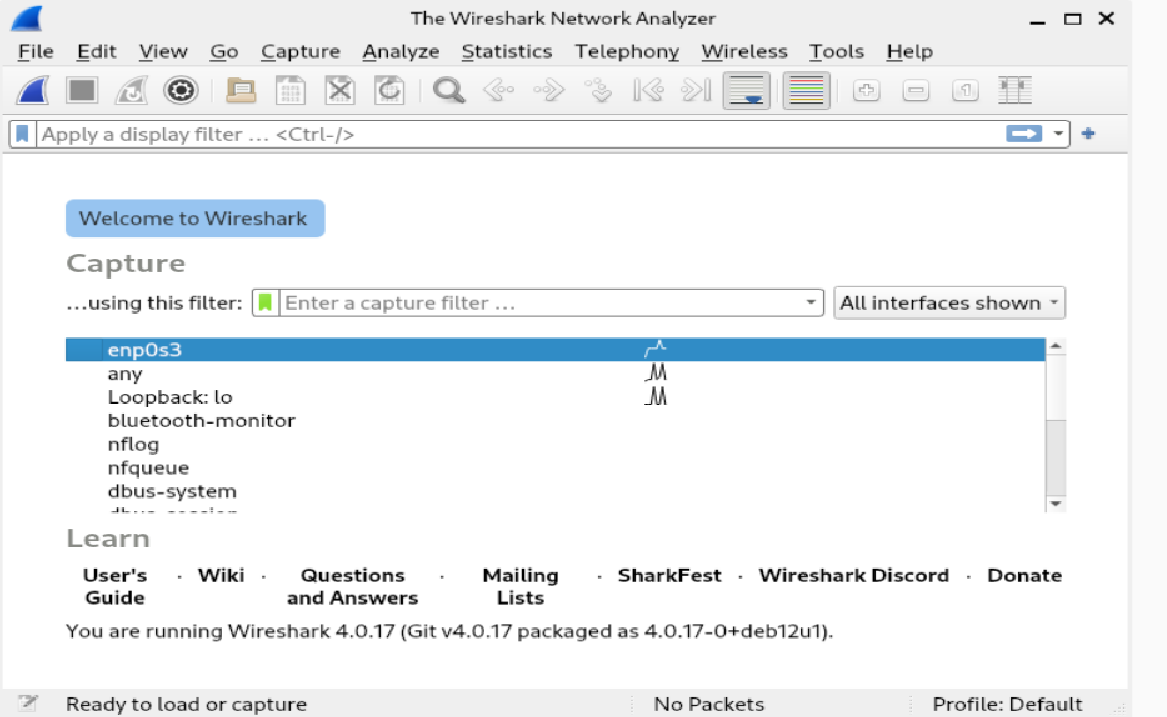
1. Avec les privilèges root, vous pouvez procéder à l'inclusion de votre utilisateur dans le groupe « wireshark » :

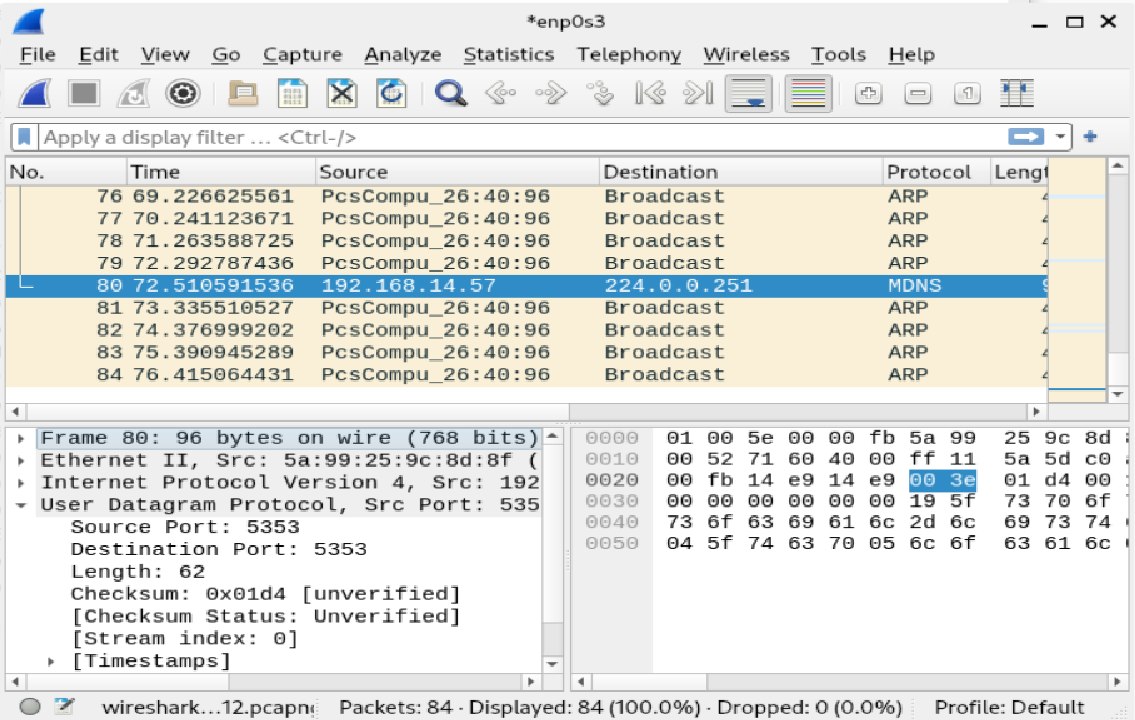


1. Pour lancer Wireshark, déconnecter vous du root pour revenir à votre utilisateur



1. Ensuite on choisit notre interface





1. **Détection d’intrusion**
2. **Simulation d’intrusion**
3. On va commencer par installer HPING3

****

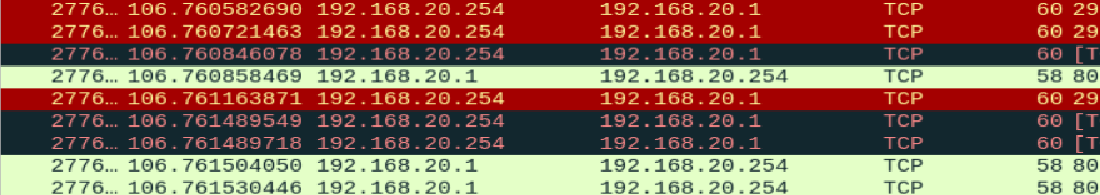
1. Ensuite on va simuler une attaque par Ddos





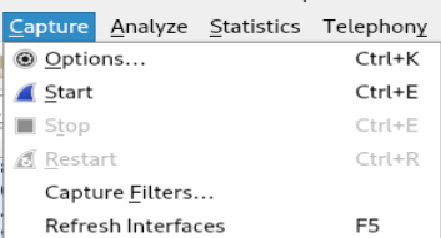
Une ddos : Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser en surchargeant de requêtes

1. Sur Wireshark on va regarder le trafique et les trames



On peut voir que on a une surdose de trames vers le serveur 192.168.20.1

1. **Observations de logs**
2. Dans le menu « capture » aller dans « start »



1. Analyser les logs

Packet List (panneau supérieur) : affiche tous les paquets capturés avec des informations de base.

Packet Details (panneau central) : montre les détails du paquet sélectionné.

Packet Bytes (panneau inférieur) : présente le paquet en format hexadécimal.

Utilisez les filtres pour affiner votre analyse. Par exemple, vous pouvez filtrer par protocole en tapant "tcp" dans la barre de filtre2.

Pour suivre une conversation spécifique, faites un clic droit sur un paquet et sélectionnez "Follow" puis "TCP Stream" (ou le protocole approprié)2.

Utilisez la fonctionnalité "Expert Information" pour identifier rapidement les erreurs ou informations importantes dans votre capture. Accédez-y via le menu Analyze -> Expert Information

1. Centralisation des logs avec Graylog
2. Installation de Graylog