Projet Sécurité 182



**Rapport de projet**

Zeqiri Amir – CIN3B

ETML, Vennes – A13

32 Périodes

Maître : M. Bourahla

Table des matières

[1 Description du projet dans son ensemble 3](#_Toc207189060)

[1.1 Titre 3](#_Toc207189061)

[1.2 Sujet 3](#_Toc207189062)

[2 Introduction 3](#_Toc207189063)

[2.1 Schéma 3](#_Toc207189064)

[3 Présentation de WireShark 3](#_Toc207189065)

[4 Analyse et identification des trames du service DHCP 4](#_Toc207189066)

[5 Analyse et identification des trames du service DNS 4](#_Toc207189067)

[6 Analyse et identification des trames du service AD 4](#_Toc207189068)

[7 Problèmes rencontrés 4](#_Toc207189069)

[8 Sources & Aides 4](#_Toc207189070)

[9 Conclusion 4](#_Toc207189071)

# Description du projet dans son ensemble

## Titre

Analyse du trafic réseau avec Wireshark

## Sujet

Une entreprise valaisanne de sécurité souhaite analyser le trafic réseau lors de l’activation des services serveur au sein de l’entreprise.

Dans le cadre de ce projet, vous devez mettre en place l’infrastructure ci-dessous dans le but d’analyser le trafic réseau et identifier les protocoles et ports lors des échanges. Concrètement, après l’installation de Windows 11 et Windows 22 serveur, vous devez installer WireShark et identifier les trames des différents services DHCP, DNS et AD, KBA-Labs (3 à 5).

# Introduction

Introduction

## Schéma

Une image contenant texte, capture d’écran, diagramme

Le contenu généré par l’IA peut être incorrect.

# Présentation de WireShark

Wireshark

# Analyse et identification des trames du service DHCP

Dhcp

# Analyse et identification des trames du service DNS

Dns

# Analyse et identification des trames du service AD

Ad

# Problèmes rencontrés

Problèmes rencontrés

# Sources & Aides

[Lien](file:///C:\Users\amizeqiri\Desktop\GitHub\P_Bulles_docker2\Lien) : Lien

# Conclusion

Conclusion