Projet Sécurité 182



**Rapport de projet**

Zeqiri Amir – CIN3B

ETML, Vennes – A13

32 Périodes

Maître : M. Bourahla

Table des matières

[1 Introduction 3](#_Toc210203364)

[1.1 Schéma 3](#_Toc210203365)

[2 Présentation de WireShark 4](#_Toc210203366)

[3 Analyse et identification des trames du service DHCP 4](#_Toc210203367)

[3.1 Fonctionnement de DORA 4](#_Toc210203368)

[3.1.1 D = Discover 4](#_Toc210203369)

[3.1.2 O = Offer 4](#_Toc210203370)

[3.1.3 R = Request 4](#_Toc210203371)

[3.1.4 A = Acknowledge 4](#_Toc210203372)

[4 Analyse et identification des trames du service DNS 6](#_Toc210203373)

[4.1 Fonctionnement d’un ping et du DNS 6](#_Toc210203374)

[5 Analyse et identification des trames du service AD 7](#_Toc210203375)

[5.1 LDAP 7](#_Toc210203376)

[5.1.1 Fonctionnement de LDAP 7](#_Toc210203377)

[5.2 Kerberos 8](#_Toc210203378)

[5.3 DNS 8](#_Toc210203379)

[6 Problèmes rencontrés 8](#_Toc210203380)

[7 Sources & Aides 8](#_Toc210203381)

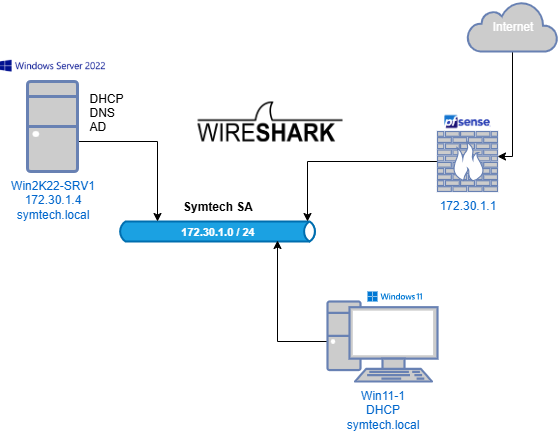
[8 Conclusion 8](#_Toc210203382)

# Introduction

Analyse du trafic réseau avec Wireshark

Dans le cadre du module 182 à l’ETML, nous devons réaliser un projet où l’objectif est de mettre en place une petite infrastructure et d’analyser le trafic réseau avec Wireshark. Le but est de voir comment fonctionnent certains services important comme DHCP, DNS et Active Directory, et de repérer les trames, protocoles et ports utilisés pendant leurs échanges.  
  
Le projet se fait dans un contexte pratique : une entreprise valaisanne de sécurité souhaite observer ce qui se passe sur le réseau quand ses services serveurs sont activés. Pour cela, nous avons installé un poste Windows 11 et un serveur Windows Server 2022, puis capturer le trafic Wireshark.  
  
Ce travail nous permet de mettre en pratique ce qu’on a appris sur les protocoles et les services réseau, mais aussi de mieux comprendre comment analyser et diagnostiquer un réseau, ce qui est une compétence utile en informatique et en sécurité.

## Schéma



# Présentation de WireShark

Wireshark est un logiciel gratuit qui sert à analyser le trafic réseau. Avec lui, je peux capturer les paquets qui passent sur une carte réseau et les regarder en détail. Ça permet de voir quels protocoles sont utilisés, quelles machines discutent entre elles et quelles infos elles s’échangent.

C’est un outil souvent utilisé par les admins réseaux et les personnes qui travaillent en sécurité, car il aide à trouver des problèmes de communication ou à vérifier que tout fonctionne comme prévu.

Dans mon projet, j’utilise Wireshark pour voir directement les trames envoyées et reçues par les services DHCP, DNS et Active Directory. C’est donc l’outil principal qui me permet d’analyser le trafic entre mon poste Windows 11 et mon serveur Windows Server 2022.

# Analyse et identification des trames du service DHCP

## Fonctionnement de DORA

### D = Discover

Le client envoie un message DHCP Discover en broadcast pour chercher un serveur DHCP disponible

Exemple : un PC branché au réseau et configuré en DHCP demande une adresse

### O = Offer

Le serveur DHCP répond avec un DHCP Offer, qui contient une proposition d’adresse IP, le masque, la passerelle, etc

### R = Request

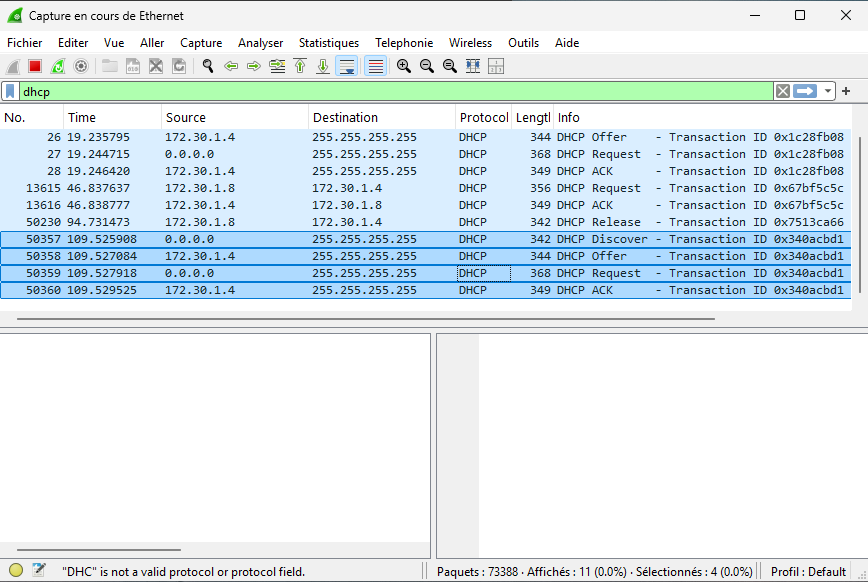
Le client envoie un DHCP Request pour confirmer qu’il accepte l’adresse proposée.

Il peut aussi en profiter pour demander explicitement d’autres paramètres (DNS, durée du bail, etc.).

### A = Acknowledge

Le serveur DHCP répond avec un DHCP Acknowledgment (ACK), ce qui finalise l’attribution.

À ce stade, l’IP est officiellement réservée pour le client, qui peut commencer à communiquer sur le réseau.



Dans mon cas pratique, on voit très bien le DORA s’effectuer (lignes foncées).

Le processus commence par un DHCP Discover envoyé par le client avec l’adresse source 0.0.0.0 (car il n’a pas encore d’IP) et une destination 255.255.255.255 (broadcast, pour atteindre tous les serveurs DHCP possibles).

Ensuite, le serveur DHCP (172.30.1.4) répond avec un DHCP Offer destiné également à 255.255.255.255, dans lequel il propose une adresse IP et les différents paramètres réseau.

Le client, toujours avec la source 0.0.0.0, envoie alors un DHCP Request vers 255.255.255.255 pour confirmer qu’il accepte l’adresse proposée par le serveur.

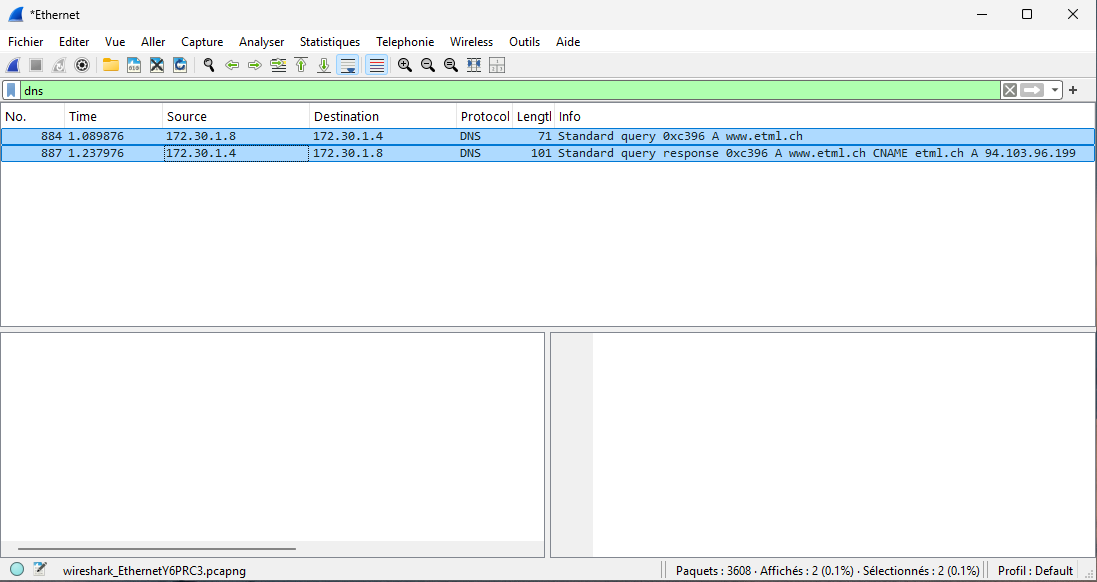
Enfin, le serveur (172.30.1.4) termine la séquence avec un DHCP ACK, toujours en broadcast, qui confirme définitivement l’attribution de l’adresse IP au client.

# Analyse et identification des trames du service DNS

## Fonctionnement d’un ping et du DNS

Quand on fait un ping vers un nom de domaine (par ex. etml.ch), l’ordinateur ne connaît pas directement l’adresse IP correspondante. Il doit donc interroger le service DNS (Domain Name System), qui joue le rôle de traducteur entre adresse IP et nom de domaine.

1. Le client envoie une requête DNS (Standard query A) pour demander l’adresse IP associée au nom de domaine.
2. Le serveur DNS répond avec une Standard query response, qui contient soit directement l’adresse IP, soit un alias (CNAME) pointant vers une autre entrée DNS.
3. Une fois l’adresse IP obtenue, le ping utilise le protocole ICMP pour envoyer des paquets à cette adresse IP et mesurer le temps de réponse.



Dans mon cas pratique, on voit clairement ces étapes s’effectuer (lignes foncées).

La machine cliente 172.30.1.8 envoie une requête DNS (Standard query A) à destination du serveur DNS 172.30.1.4 pour résoudre le nom www.etml.ch

Le serveur DNS 172.30.1.4 répond avec une Standard query response indiquant que [www.etml.ch](http://www.etml.ch) est un alias (CNAME) de etml.ch, et il fournit l’adresse IP correspondante (94.103.96.199).

Une fois cette résolution effectuée, la machine cliente peut lancer le ping vers l’adresse IP obtenue.

# Analyse et identification des trames du service AD

## LDAP

### Fonctionnement de LDAP

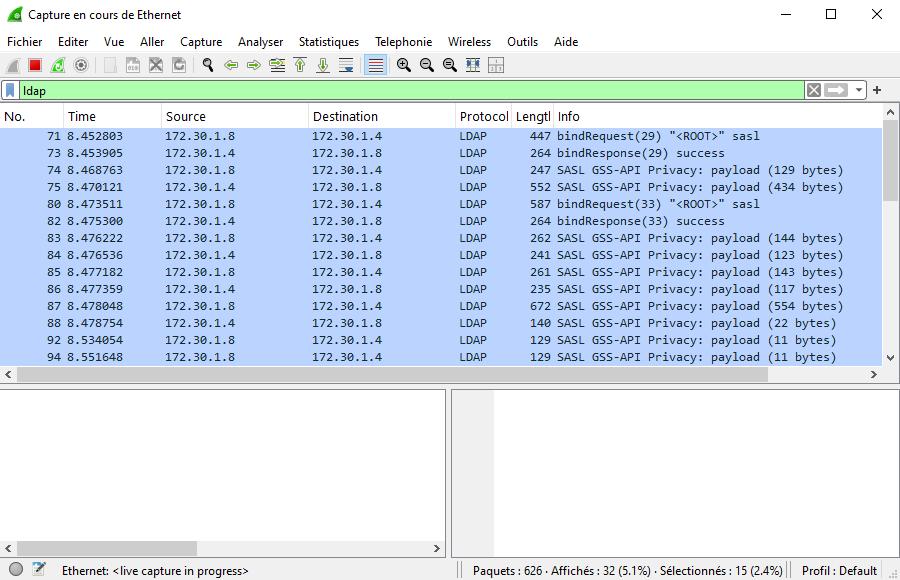
LDAP (Lightweight Directory Access Protocol) est un protocole qui permet aux clients d’interroger et de modifier un annuaire centralisé (comme Active Directory).

Il sert principalement à gérer les utilisateurs, groupes et droits d’accès dans un domaine.

Lorsqu’un client veut se connecter à l’annuaire, il doit d’abord établir une authentification (bind) avec le serveur LDAP.

Ensuite, il peut effectuer des requêtes (recherche d’un utilisateur, vérification des permissions, etc.) ou recevoir des réponses en retour.

Dans un contexte Active Directory, LDAP est souvent couplé avec Kerberos pour sécuriser les échanges et gérer l’authentification unique (SSO).

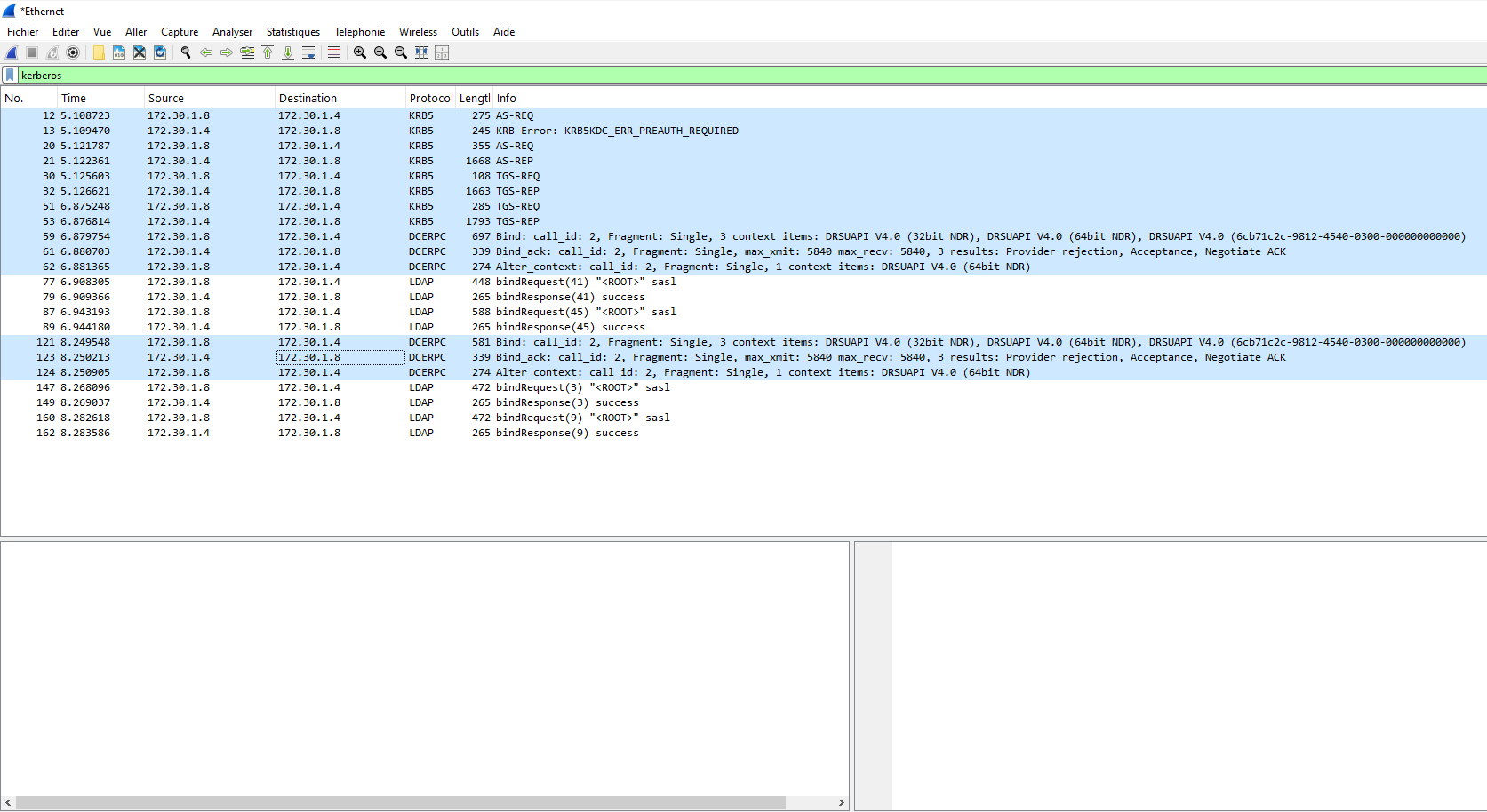


Dans mon cas pratique, on observe clairement la communication LDAP entre la machine cliente (172.30.1.8) et le serveur Active Directory (172.30.1.4)  
  
Le client envoie un BindRequest "ROOT" pour initier la connexion avec le serveur LDAP.

Le serveur répond par un BindResponse success, ce qui valide l’authentification.  
  
Ensuite, on voit une série de messages utilisant le mécanisme SASL GSS-API Privacy, qui transportent des informations de sécurité et d’authentification (chiffrées).

Ces échanges montrent que le client et le serveur établissent un canal sécurisé pour permettre l’utilisation de l’annuaire (consultation ou modification d’objets).

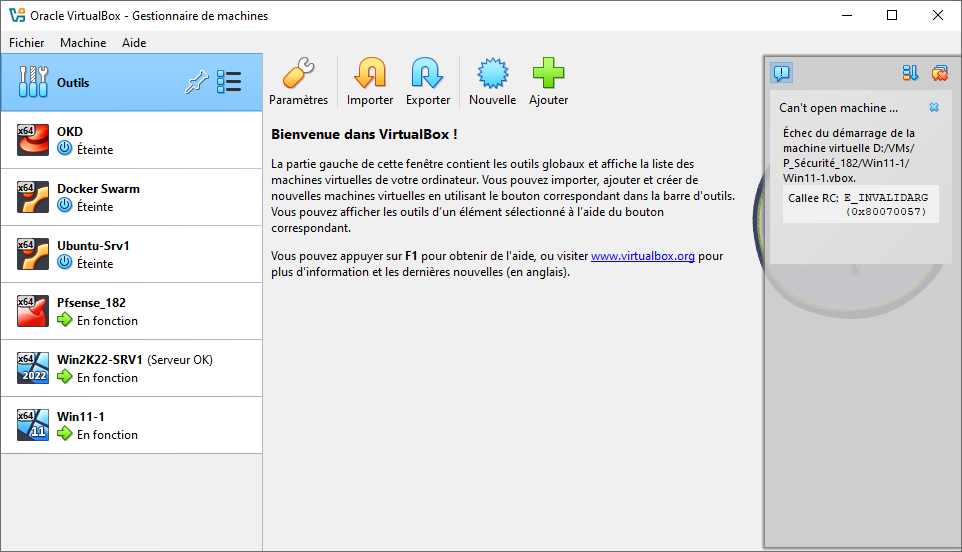
## Kerberos



## DNS

# Problèmes rencontrés

Durant ce projet, j’ai rencontré un seul problème. Il s’agit d’un problème de machine virtuelle, en effet, la machine client a décidé de plus se lancer et était inaccessible. Voici un printscreen du problème :



L’erreur 0x80070057 indique que VirtualBox reçoit un paramètre invalide, c’est souvent du à un fichier mal configuré, comme le fichier .vbox, ou alors à cause d’un chemin (path). Après multiple essais à essayer de résoudre le problème et récupérer ma VM, j’ai enfin pu le résoudre en créant une nouvelle VM et en récupérant le stockage (fichier .vdi) de ma première VM. Cela ne m’a pas significativement impacté durant la réalisation du projet mais m’a rajouté une petite pression.

# Sources & Aides

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

# Conclusion

Conclusion