2nde BAC Pro CIEL		
	Premier pas avec Wireshark Repérer une activité réseau suspecte	 Année 2026/2027

Nom		
Prénom		
Date		
Matériel Outillage 	⇨ Wireshark	**Durée** : 3H 
Travaux à réaliser 	⇨ Première prise en main Wireshark ⇨ Observation de communication ⇨ Repérage de demandes répétées	

Pôle d'activité : Valorisation de la donnée et cybersécurité

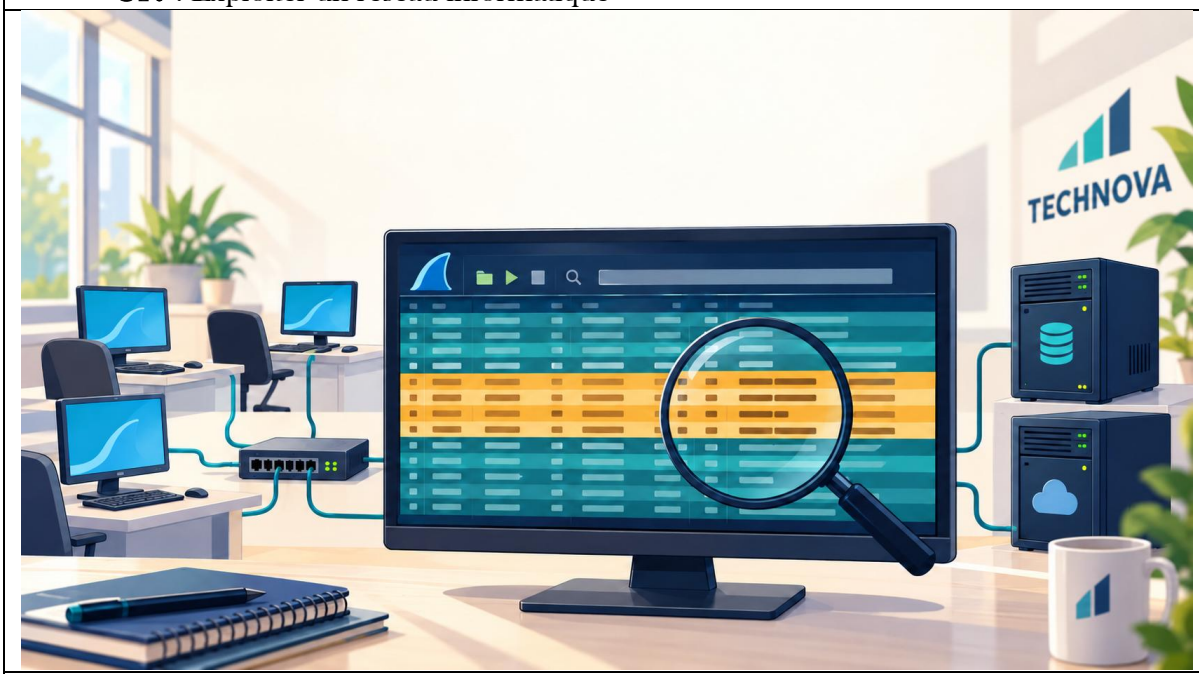
Activités :

⇨ **D3** : Gestion d'incidents

Compétences :

⇨ **C04** : Analyser une structure matérielle et logicielle

⇨ **C10** : Exploiter un réseau informatique



Lorsque le logo apparaît, il est indispensable d'appeler l'enseignant pour vérification.

A. Compétences

C01	**COMMUNIQUER EN SITUATION PROFESSIONNELLE (ANGLAIS/FRANÇAIS)**	
	La présentation (typographie, orthographe, illustration, lisibilité) est soignée et soutient le discours avec des enchaînements cohérents	
	La présentation orale (support et expression) est de qualité et claire	
	L'argumentation développée lors de la présentation et de l'échange est de qualité	
	L'argumentation tient compte des éventuelles situations de handicap des personnes avec lesquelles il interagit	
C03	**PARTICIPER A UN PROJET**	
	Les rôles et tâches de chacun sont identifiés ; le cas échéant, les besoins spécifiques des personnes en situation de handicap sont pris en compte	
	Le planning prévisionnel est compris	
	Le suivi du projet est respecté	
	L'espace collaboratif est correctement utilisé	
C04	**ANALYSER UNE STRUCTURE MATÉRIELLE ET LOGICIELLE**	
	Le besoin est identifié ainsi que les ressources matérielles, logicielles et humaines	X
	Les logiciels d'analyse et de tests sont utilisés selon les procédures de traitement d'incidents	X
	Les informations nécessaires sont extraites des documents réglementaires et/ou constructeurs	
	Les indicateurs de fonctionnement sont interprétés	X
	Les fiches de test ou d'intervention sont renseignées	X
C06	**VALIDER LA CONFORMITÉ D'UNE INSTALLATION**	
	Les exigences du cahier des charges sont respectées	
	Les tests sont effectués	
	Les résultats attendus sont vérifiés	
	La procédure de test est respectée	
C07	**RÉALISER DES MAQUETTES ET PROTOTYPES**	
	Le placement et routage sont conformes au cahier des charges	
	La génération des fichiers de fabrication du PCB est conforme aux attentes	
	Le PCB est réalisé, contrôlé et conforme aux IPC (tolérances mécaniques, finition de surface, propreté, ESD etc.)	
	Les composants sont conformes à la nomenclature (marquage, étiquetage)	
	La nomenclature des composants est respectée	
	Le brasage de la carte est conforme à la nomenclature et aux IPC	
	Les contraintes liées aux impacts environnementaux sont intégrées	
	Le contrôle visuel de la carte assemblée est conforme au dossier de fabrication	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C08	**CODER**	
	Les environnements de développement et de test sont mis en oeuvre en tenant compte des contraintes de fonctionnalités et de sécurité	
	Le module logiciel est débogué et syntaxiquement correct	
	Les composants logiciels individuels sont développés et testés conformément aux spécifications du cahier des charges et des bonnes pratiques	
	La solution (logicielle et matérielle) est intégrée et testée conformément aux spécifications du cahier des charges et des bonnes pratiques	
	Le code est commenté et le logiciel est documenté	
C09	**INSTALLER LES ÉLÉMENTS D'UN SYSTÈME ÉLECTRONIQUE OU INFORMATIQUE**	
	L'ensemble des éléments pour l'installation du système est complet et vérifié par rapport au cahier des charges	
	Les éléments du système sont installés et raccordés selon une procédure	
	La configuration est réalisée	
	La mise en service est réalisée	
	L'état de l'installation est renseigné de manière écrite ou orale	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	
C10	**EXPLOITER UN RÉSEAU INFORMATIQUE**	
	Les alertes et problèmes rencontrés sont renseignés	X
	Les différents éléments d'un réseau ou d'un système à partir d'un schéma fourni sont identifiés	
	La mise à jour des équipements (iOS, OS, logiciel, firmware) est effectuée	
	Les optimisations nécessaires sont effectuées	
C11	**MAINTENIR UN SYSTÈME ÉLECTRONIQUE OU RÉSEAU INFORMATIQUE**	
	L'intervention est préparée	
	Le dysfonctionnement est constaté	
	La maintenance ou la réparation est réalisée	
	La fiche d'intervention est correctement renseignée	
	Les risques d'une situation de travail sont repérés et les mesures appropriées pour sa santé, sa sécurité et celle des autres sont adoptées	

Nature de complexité de l'activité

Découverte	X
Intermédiaire	
Bac Pro	

B. Mise en contexte

Vous êtes en période de découverte au sein du service informatique de l'entreprise TECHNOVA.

Une technicienne réseau a remarqué des communications inhabituelles vers le serveur interne de l'entreprise. Elle a enregistré les échanges du réseau dans un fichier de capture et vous propose de l'accompagner dans une première analyse.

À l'aide du logiciel Wireshark, des fiches ressources et des indications de la technicienne, vous allez découvrir comment les équipements communiquent. Vous observerez d'abord des échanges habituels, puis vous rechercherez ce qui semble inhabituel.

Votre mission consiste à relever des indices et à expliquer vos observations, sans modifier les équipements ni intervenir sur le réseau.

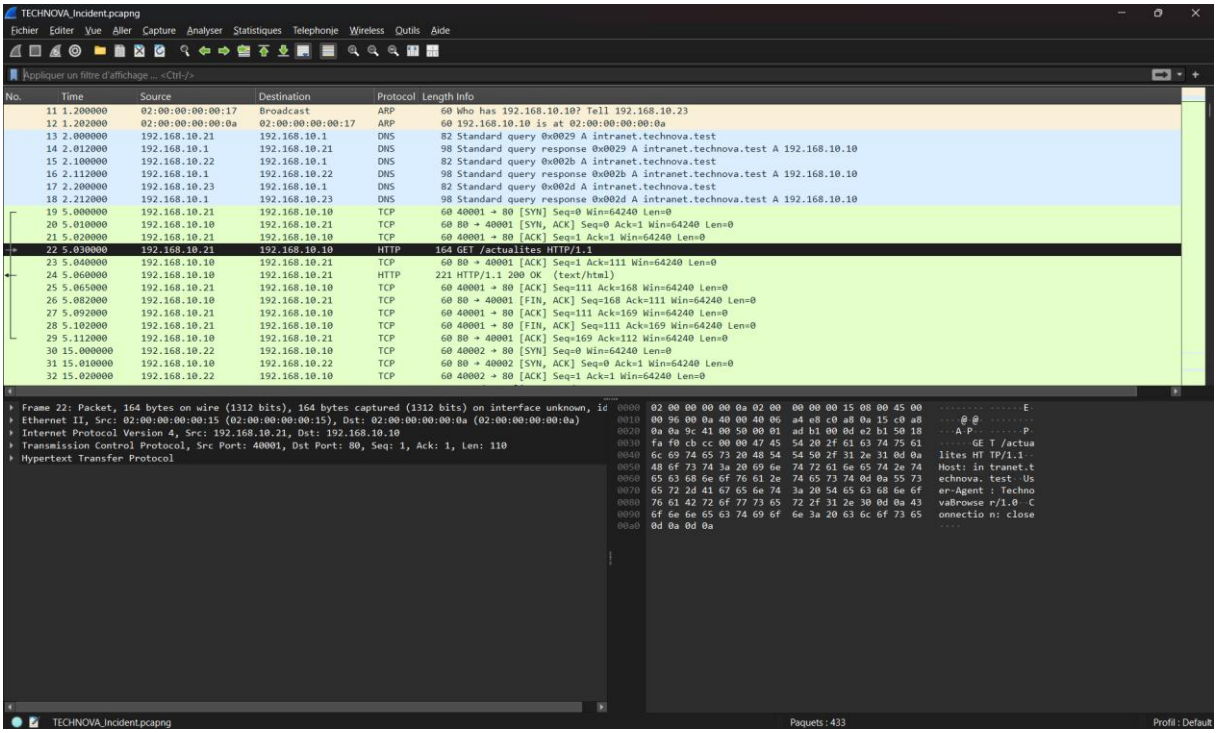
C. Problématique

Comment utiliser une capture réseau pour distinguer des échanges habituels d'une activité suspecte ?



D. Découverte de Wireshark (10 min)

Wireshark est un logiciel d'analyse des communications réseau. Il permet d'observer les échanges entre des équipements, comme un ordinateur et un serveur.



Il peut enregistrer les communications visibles depuis un point du réseau ou ouvrir un fichier contenant des échanges déjà enregistrés. Cet enregistrement s'appelle une capture réseau.

Les techniciens utilisent Wireshark pour comprendre le fonctionnement d'un réseau, rechercher l'origine d'un problème ou examiner une activité inhabituelle.

Dans cette activité, Wireshark vous permettra de :

- ⇨ repérer les équipements qui communiquent
- ⇨ identifier les protocoles utilisés
- ⇨ sélectionner des échanges à l'aide de filtres
- ⇨ lire les demandes et les réponses pour comprendre ce qui s'est passé

Vous travaillerez sur une capture fournie par l'enseignant. Il n'est donc pas nécessaire de lancer un enregistrement sur le réseau de l'atelier.

Wireshark présente les échanges : c'est à vous de les observer et de les interpréter pour déterminer ce qui semble habituel ou suspect.

E. Prise en main de la capture (20 min)

Ouvrir Wireshark.

Fichier → Ouvrir et **sélectionner** « TECHNOVA_Incident.pcapng »

Repérer les colonnes No., Time, Source, Destination, Protocol et Info.

Chaque ligne correspond à une trame enregistrée. Pour commencer, vous pouvez la considérer comme une partie d'une communication entre deux équipements.

Quelle colonne permet de connaître l'équipement qui envoie un message ?

Quelle colonne permet de connaître celui qui reçoit le message ?

Relever deux protocoles visibles dans la capture.

Dans la barre de filtre d'affichage, **saisir** `arp`. **Appuyer** sur Entrée, puis **consulter** la fiche sur les protocoles.

A quoi sert le protocole ARP ?

- ☐ Transférer une page web
- ☐ Retrouver une adresse MAC à partir d'une adresse IPv4 sur le réseau local
- ☐ Vérifier un mot de passe

Effacer le filtre pour retrouver l'ensemble des trames.

F. Observation d'une communication habituelle (35 min)

1) Retrouver un serveur à partir de son nom

Appliquer le filtre **`dns`**.

Sélectionner une trame de demande DNS, reconnaissable à la mention :

`Standard query 0x...` dans la colonne Info.

Quel nom apparaît après la lettre A dans la colonne info ?

Sélectionner ensuite la trame de réponse (la suivante). Il s'agit de la réponse correspondante, reconnaissable à la mention :

`Standard query response ...` dans la colonne info.

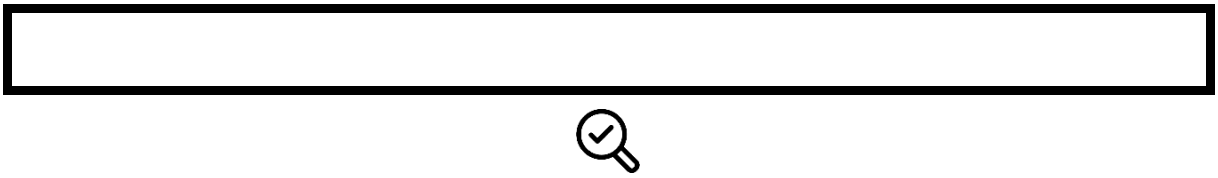
Dans la colonne Info, **quelle** adresse IPv4 est indiquée à la fin de la réponse, après le nom recherché et la lettre A ?

Compléter la phrase :

`Le protocole DNS permet ici de retrouver une _____ à partir d'un _____.`

2) Observer la consultation d'une page

En vous aidant de la fiche ressource sur les filtres d'affichage Wireshark, **renseigner** le filtre d'affichage permettant d'examiner un échange HTTP de type « Demande GET » :



Appliquer le filtre.

Rechercher une ligne contenant `/actualites` dans la colonne Info.

Compléter le tableau à partir de cette ligne.

Élément observé	Votre réponse
Numéro de la trame	
Adresse IP du poste qui demande la page	
Adresse IP du serveur qui reçoit la demande	
Ressource demandée	

Faire clic droit sur cette ligne → Suivre → Flux TCP

Dans la fenêtre qui s'ouvre, **rechercher** la demande `GET /actualites` et la réponse `HTTP/1.1`.

Quel code de réponse le serveur renvoie-t-il ? **Que** signifie-t-il ?

Vous venez d'observer un fonctionnement habituel :
Un poste demande une page et le serveur lui répond

G. Repérage de demandes répétées (35 min)

Le technicienne réseau vous invite maintenant à examiner les demandes adressées à la page de connexion.

En vous aidant de la fiche ressource sur les filtres d'affichage Wireshark, **renseigner** le filtre permettant d'examiner un échange HTTP de type « Envoie POST » ET une demande HTTP vers « /login ».



Appliquer le filtre.

Chaque ligne affichée correspond à un envoie de données d'un poste vers cette page.

Quelle adresse IP envoie ces demandes ?

Quelle adresse IP les reçoit ?

Combien de demandes sont affichées ?

Observer la colonne Time. Les données sont en secondes.

Les premières demandes **sont-elles** espacées de façon régulière ? **Donner** un intervalle approximatif.

En vous aidant de la fiche ressource sur les filtres d'affichage Wireshark et de la fiche ressource sur les principaux protocoles réseaux, **renseigner** le filtre permettant d'afficher le code réponse HTTP correspondant à une autorisation invalide.



Appliquer le filtre.

Combien de réponses sont affichées ?

A l'aide de la fiche ressource, **expliquer** ce que peut signifier ce code erreur.

Pourquoi cette succession de demandes mérite-t-elle une vérification ?

Attention, une répétition est un indice. Elle ne permet pas encore de savoir qui utilise le poste ni pourquoi ces demandes sont envoyées

H. Comprendre ce qui change (40 min)

1) Examen de la dernière tentative

Réappliquer le filtre :

```
http.request.method == "POST" && http.request.uri == "/login"
```

Sélectionner la dernière demande affichée, puis **choisir** Suivre → Flux TCP.

Lire la réponse du serveur.

Quel code de réponse apparaît cette fois-ci ?

Recopier la courte phrase du serveur qui indique le résultat de l'authentification.

Quelle différence constatez-vous par rapport aux tentatives précédentes ?

Relever le nom d'utilisateur et le mot de passe de connexion.

Fermer la fenêtre de suivi.

2) Observation des demandes suivantes

Afficher les requêtes du poste étudié avec le filtre permettant d'afficher l'adresse IP source (l'adresse IP qui a réussi la connexion HTTP précédente) ET toutes les requêtes HTTP.

Observer les demandes qui suivent la dernière tentative de connexion.

Relever les trois chemins demandés après cette tentative (après /login).

Ordre	Chemin demandé
1	
2	
3	

Quel chemin semble correspondre au téléchargement d'un fichier ? **Préciser** le nom du fichier.

Sélectionner cette demande, puis **utiliser** Suivre → Flux TCP.

Quel type d'informations apparaît dans le fichier transmis ? **Donner** deux exemples de noms de colonnes, sans recopier les lignes du fichier.

Compléter le sens du transfert de données :

`Le fichier est envoyé par _____ vers _____.`

Fermer la fenêtre de suivi et **réappliquer** le filtre d'affichage précédent.

Sélectionner la demande contenant `/admin/audit/clear` et **suivre** son flux TCP.

D'après le texte de la réponse, **quelle** action le serveur annonce-t-il avoir réalisée ?

Pourquoi cette action peut-elle compliquer une investigation ?

I. Présentation des premières conclusions (25 min)

1) Remise des évènements dans l'ordre

Numéroter les événements de 1 à 4.

Évènement	Ordre
Un fichier est transféré du serveur vers le poste	
Plusieurs tentatives d'authentification sont refusées	
Une demande d'effacement du journal est envoyée	
Une authentification réussit	

2) Conservation de deux preuves

Choisir deux observations importantes et **indiquer** les numéros des trames correspondantes.

Numéro de trame	Ce que cette trame permet d'observer

3) Rédaction d'un court bilan

Compléter ce texte avec vos observations

Le poste ayant l'adresse IP _____ a envoyé plusieurs demandes de connexion au serveur _____

Les premières réponses indiquent _____

Ensuite, nous observons _____

Après la connexion, le poste _____

Cette activité nous paraît suspecte par ce que _____

Peut-on identifier la personne qui utilisait ce poste à partir de cette seule capture ? **Justifier** brièvement.

Proposer une mesure qui pourrait limiter les tentatives répétées d'authentification.

J. Livrable

Enregistrer et **renommer** le fichier « NOM-PremierPasWireshark.pdf » avec NOM votre nom de famille.

Téléverser ce fichier.