Ce document a été mis en ligne par l'organisme FormaV®.

Toute reproduction, représentation ou diffusion, même partielle, sans autorisation préalable, est strictement interdite.

Pour consulter tous nos sujets d'annales et corrigés du Bac Pro CIEL, veuillez visiter :
coursbacprociel.fr/annales-sujets-et-corriges

BACCALAURÉAT PROFESSIONNEL

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE

SESSION 2026

SOUS-ÉPREUVE E32 : VALORISATION DE LA DONNÉE ET CYBERSÉCURITÉ

Coefficient : 3 Durée : 3 heures

Le poste de travail, les logiciels, les fichiers de données et les documents techniques nécessaires sont mis à disposition du candidat. Aucun autre document ou matériel n'est autorisé.

Composition de l'épreuve	Support
PARTIE 1 : Architecture réseau et adressage (7 points)	Dossier Questionnement
PARTIE 2 : Valorisation des données et développement (6 points)	Dossier Questionnement
PARTIE 3 : Analyse d'incident et durcissement des accès (7 points)	Dossier Questionnement
DOSSIER TECHNIQUE ET RESSOURCES (DT 1, DT 2)	Fourni avec le sujet
DOCUMENTS RÉPONSES (DR 1) : À RENDRE AVEC LA COPIE	Fin de sujet

L'usage de calculatrice avec mode examen actif est autorisé. L'usage de calculatrice sans mémoire, « type collège », est autorisé.

Ce sujet comporte 7 pages numérotées de 1/7 à 7/7.
Dès que le sujet vous est remis, assurez-vous qu'il est complet.

LES DOCUMENTS RÉPONSES SITUÉS EN FIN DE DOSSIER SONT À COMPLÉTER ET À RENDRE OBLIGATOIREMENT AVEC LA COPIE.

DOSSIER SUJET

MISE EN SITUATION PROFESSIONNELLE ET CAHIER DES CHARGES : ATELIER LOGISTIQUE DES RIVES, VALENCE (DRÔME)

Vous intervenez au sein de l'équipe informatique de l'Atelier Logistique des Rives. Le site utilise un réseau local segmenté, un serveur de supervision et une base de données recensant les équipements et les événements de sécurité.

À la suite d'une évolution du réseau et de plusieurs échecs d'authentification constatés sur un serveur, le responsable informatique vous confie l'analyse du plan d'adressage, la réalisation d'une requête de suivi, le développement d'un outil de traitement des événements et la préparation de mesures de sécurisation.

Vous travaillez sur un environnement de test isolé. Les documents DT 1 et DT 2 fournissent les données nécessaires. Vous remettez les réponses demandées dans le document DR 1 et dans les fichiers réalisés sur le poste. Toute modification de configuration doit être effectuée dans l'environnement de test fourni.

PARTIE 1 : Architecture réseau et adressage (7 points)

Analyser une architecture matérielle et logicielle, vérifier un plan d'adressage et compléter une table de routage

À partir du schéma et du plan d'adressage du DT 1, vérifiez la cohérence du réseau de l'atelier. Les adresses IPv6 sont attribuées en utilisant le préfixe de documentation indiqué dans le document. Les passerelles des postes sont les interfaces du routeur R1 associées à leur VLAN.

1.1 (2 points) Pour le poste PC-LOG, dont l'adresse IPv4 est indiquée dans le DT 1, donnez l'adresse réseau, l'adresse de diffusion et la première adresse utilisable du sous-réseau. Indiquez également si cette adresse appartient au VLAN 10, au VLAN 20 ou au VLAN 99.

1.2 (2 points) Pour les VLAN 10 et 20, proposez les deux préfixes IPv6 /64 consécutifs à utiliser dans le préfixe du DT 1. Précisez l'adresse de passerelle IPv6 de chaque VLAN en appliquant la convention d'attribution indiquée dans le DT 1.

1.3 (3 points) Complétez dans le DR 1 les entrées manquantes de la table de routage de R1. Pour le réseau du serveur distant, indiquez le préfixe de destination et le prochain saut. Pour les réseaux directement connectés, indiquez l'interface de sortie appropriée. Une route par défaut est déjà présente dans la table.

PARTIE 2 : Valorisation des données et développement (6 points)

Interroger une base relationnelle, coder, tester et documenter un composant logiciel

Le responsable souhaite disposer d'un état des équipements actifs par site et d'un outil simple de comptage des événements d'authentification échoués. Le schéma relationnel et les données

d'exemple figurent dans le DT 2. Le poste de travail contient un interpréteur Python 3 et un éditeur de texte.

2.1 (2 points) Rédigez une requête SQL qui affiche, pour chaque site possédant au moins un équipement actif, le nom du site et le nombre d'équipements actifs. Utilisez une jointure entre les tables du DT 2, filtrez les équipements actifs et regroupez le résultat par site. Triez le résultat par nom de site dans l'ordre croissant.

2.2 (2 points) Dans le fichier **analyse.py** fourni sur le poste, écrivez une fonction **compter_echecs(lignes)**. Le paramètre **lignes** est une liste de dictionnaires comportant les clés **event** et **user**. La fonction retourne le nombre de dictionnaires dont la valeur de **event** est exactement **LOGIN_FAIL**. Une liste vide doit produire la valeur 0. Ajoutez un commentaire décrivant le rôle de la fonction.

2.3 (2 points) Testez votre fonction avec les quatre événements du DT 2 et avec une liste vide. Indiquez les deux résultats attendus. Ajoutez au fichier un test automatisé pour chacun de ces cas et rédigez un court commentaire d'utilisation précisant les données attendues par la fonction.

PARTIE 3 : Analyse d'incident et durcissement des accès (7 points)

Analyser des traces, qualifier un incident, appliquer des mesures de sécurité et communiquer un compte rendu

Le serveur SRV-APP a enregistré plusieurs échecs de connexion suivis d'une authentification réussie. Les extraits sont fournis dans le DT 2. Vous devez exploiter ces traces et proposer des mesures adaptées au périmètre du serveur.

3.1 (2 points) À partir des horodatages, des adresses IP et des comptes présents dans le DT 2, reconstituez la chronologie des événements. Indiquez les éléments qui justifient de signaler l'événement comme suspect. Distinguez les faits observés de votre interprétation.

3.2 (2 points) Dans le fichier de configuration SSH de l'environnement de test, proposez et appliquez deux réglages adaptés pour réduire le risque d'accès non autorisé. Pour chaque réglage, indiquez brièvement l'effet recherché. Vérifiez la syntaxe de la configuration avec l'outil disponible avant de proposer son rechargement.

3.3 (3 points) Rédigez dans le compte rendu fourni un message professionnel de 5 à 8 lignes à destination du responsable informatique. Il doit présenter l'incident suspect, citer au moins deux éléments observés dans les journaux, indiquer les mesures immédiates proposées et préciser une action de suivi. Ajoutez une phrase en anglais technique destinée à un technicien distant, lui demandant de préserver les journaux et de ne pas supprimer les traces.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : TOPOLOGIE DU RÉSEAU ET PLAN D'ADRESSAGE

Le routeur R1 assure le routage inter-VLAN. Le commutateur SW1 relie les postes, les équipements d'administration et les serveurs. Les ports de liaison entre R1 et SW1 transportent les VLAN 10, 20 et 99. Le serveur distant du réseau 10.50.0.0/16 est accessible par le prochain saut 172.16.0.1.

Convention IPv6 : le préfixe de documentation attribué au site est 2001:db8:42::/48. Chaque VLAN reçoit un préfixe /64. Le numéro du VLAN est utilisé comme identifiant de sous-réseau, sous la forme 2001:db8:42:VLAN::/64. L'adresse de passerelle est la première adresse d'hôte du préfixe, soit l'adresse se terminant par ::1.

Topologie logique et liaisons

Équipement	Interface ou liaison	Réseau ou VLAN	Rôle
PC-LOG	SW1 port 3	VLAN 10	Poste du service logistique
PC-TECH	SW1 port 8	VLAN 20	Poste du service technique
SRV-APP	SW1 port 12	VLAN 20	Serveur applicatif et journaux
R1	G0/0.10	VLAN 10	Passerelle du service logistique
R1	G0/0.20	VLAN 20	Passerelle du service technique et du serveur
R1	G0/0.99	VLAN 99	Administration du commutateur
R1	G0/1	172.16.0.0/30	Liaison vers le routeur amont
SW1	Uplink vers R1 G0/0	VLAN 10, VLAN 20, VLAN 99	Liaison trunk

Schéma logique du réseau de l'Atelier Logistique des Rives

Plan d'adressage IPv4 et paramètres des interfaces

Équipement ou réseau	VLAN	Adresse IPv4 ou préfixe	Passerelle ou interface
VLAN Logistique	10	192.168.10.0/24	R1 G0/0.10 : 192.168.10.1
PC-LOG	10	192.168.10.25/24	192.168.10.1
VLAN Technique	20	192.168.20.0/24	R1 G0/0.20 : 192.168.20.1
SRV-APP	20	192.168.20.10/24	192.168.20.1
VLAN Administration	99	192.168.99.0/24	R1 G0/0.99 : 192.168.99.1
Liaison R1 vers routeur amont	Sans VLAN	172.16.0.0/30	R1 G0/1 : 172.16.0.2/30
Réseau serveur distant	Sans VLAN	10.50.0.0/16	Prochain saut : 172.16.0.1

Adresses utilisées dans l'environnement d'examen

Extrait de configuration et table de routage de R1

Élément	Valeur
G0/0.10	Encapsulation 802.1Q VLAN 10 ; adresse 192.168.10.1/24
G0/0.20	Encapsulation 802.1Q VLAN 20 ; adresse 192.168.20.1/24
G0/0.99	Encapsulation 802.1Q VLAN 99 ; adresse 192.168.99.1/24
G0/1	Adresse 172.16.0.2/30
Route statique par défaut	Destination 0.0.0.0/0 ; prochain saut 172.16.0.1
Réseau directement connecté	172.16.0.0/30 ; interface G0/1

Extrait de l'environnement de test

DT 2 : BASE DE DONNÉES ET EXTRAITS DE JOURNAUX

La base de données de suivi contient les tables suivantes. Le champ **site_id** de la table **equipement** référence le champ **id** de la table **site**. Le champ **actif** prend la valeur 1 pour un équipement actif et 0 pour un équipement inactif.

Les journaux ci-dessous sont fournis dans l'ordre chronologique. Les adresses IP et les comptes sont des données de l'environnement de test.

Schéma et données relationnelles

Table	Champs et données
site	id (entier, clé primaire) ; nom (texte). Données : (1, 'Valence'), (2, 'Romans')
equipement	id (entier, clé primaire) ; nom (texte) ; site_id (entier, clé étrangère) ; actif (entier). Données : (101, 'SW1', 1, 1), (102, 'PC-LOG', 1, 1), (103, 'OLD-PC', 1, 0), (201, 'SRV-APP', 2, 1)

Extrait de la base de données de suivi

Extrait des journaux d'authentification de SRV-APP

Horodatage	Adresse source	Compte	Événement
2026-02-12 08:14:02	203.0.113.45	admin	LOGIN_FAIL
2026-02-12 08:14:09	203.0.113.45	admin	LOGIN_FAIL
2026-02-12 08:14:17	203.0.113.45	admin	LOGIN_FAIL
2026-02-12 08:16:31	203.0.113.45	admin	LOGIN_SUCCESS
2026-02-12 08:22:04	192.168.20.35	tech01	LOGIN_SUCCESS

Journal système, dates et heures locales du site

Format des données transmises à la fonction Python

Index	event	user
1	LOGIN_FAIL	admin
2	LOGIN_FAIL	admin
3	LOGIN_SUCCESS	admin
4	LOGIN_FAIL	tech01

Liste d'événements de test

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Réponses réseau et compte rendu d'incident — **À RENDRE AVEC LA COPIE**

Complétez directement les cellules indiquées par « ... ». Inscrivez vos réponses de manière lisible. Rédigez le compte rendu de la partie 3 sur la copie ou dans le fichier prévu sur le poste de travail.

Table de routage de R1 à compléter

Destination	Prochain saut	Interface de sortie
192.168.10.0/24	.....	.....
192.168.20.0/24	.....	.....
192.168.99.0/24	.....	.....
172.16.0.0/30	.....	.....
10.50.0.0/16	.....	.....
0.0.0.0/0	172.16.0.1	G0/1

Entrées IPv4 utiles à la topologie du DT 1

Cadre réservé aux justifications, calculs complémentaires ou schémas du candidat :

.....

.....

.....

.....

.....

.....

.....

Copyright © 2027 FormaV®. Tous droits réservés.

FormaV® est une marque déposée auprès de l'INPI sous le numéro 5227897.

Ce document a été élaboré par FormaV® avec le plus grand soin afin d'accompagner chaque apprenant vers la réussite de ses examens. Son contenu (textes, graphiques, méthodologies, tableaux, exercices, concepts, mises en forme) constitue une œuvre protégée par le droit d'auteur.

Toute copie, partage, reproduction, diffusion ou mise à disposition, même partielle, gratuite ou payante, est strictement interdite sans accord préalable et écrit de FormaV®, conformément aux articles L.111-1 et suivants du Code de la propriété intellectuelle. Dans une logique anti-plagiat, FormaV® se réserve le droit de vérifier toute utilisation illicite, y compris sur les plateformes en ligne ou sites tiers.

En utilisant ce document, vous vous engagez à respecter ces règles et à préserver l'intégrité du travail fourni. La consultation de ce document est strictement personnelle.

Merci de respecter le travail accompli afin de permettre la création continue de ressources pédagogiques fiables et accessibles.