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 en savoir plus sur nos formations disponibles, veuillez visiter :
formav.co/explorer

BREVET DE TECHNICIEN SUPÉRIEUR

CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE - OPTION A : INFORMATIQUE ET RÉSEAUX

ÉPREUVE E5 : EXPLOITATION ET MAINTENANCE DE RÉSEAUX INFORMATIQUES

SESSION 2026

Durée : 3 heures

SPÉCIALITÉ / UNITÉ	COEFF
CYBERSÉCURITÉ, INFORMATIQUE ET RÉSEAUX, ÉLECTRONIQUE - OPTION A : INFORMATIQUE ET RÉSEAUX	3

Moyens de calculs et matériel autorisés :

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

Poste informatique et équipements réseau mis à disposition par le centre. Seuls les documents techniques fournis avec le sujet et les outils logiciels installés sur le poste sont autorisés. Toute intervention doit rester dans l'environnement de laboratoire prévu.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 8 pages numérotées de 1/8 à 8/8.

Les documents réponses en fin de sujet sont à rendre avec la copie.

DOSSIER SUJET

MISE EN SITUATION PROFESSIONNELLE ET CAHIER DES CHARGES : NOVALYS SERVICES, SITE DE VALENCE (DRÔME)

Novalys Services exploite un système d'information comprenant un réseau local segmenté en VLAN, un serveur applicatif et DNS, une liaison vers un fournisseur d'accès et une plateforme de supervision hébergée dans le cloud. Vous intervenez en qualité de technicien ou technicienne réseau dans l'environnement de laboratoire mis à votre disposition. Le service informatique signale une perte d'accès à un serveur depuis certains postes et des tentatives répétées de connexion à distance.

À partir des documents techniques DT 1 et DT 2, vous devez vérifier le plan d'adressage et le routage, réaliser des contrôles d'exploitation à l'aide des outils disponibles, puis analyser les traces et proposer des mesures de sécurisation. Les configurations et commandes sont à appliquer uniquement sur les équipements ou machines de laboratoire identifiés par le centre. Toute modification doit être précédée d'une sauvegarde ou d'une consignation de l'état initial.

Les réponses sont à reporter sur les documents réponse lorsqu'ils sont fournis. Les résultats de commandes doivent être accompagnés d'une interprétation en lien avec le diagnostic.

PARTIE 1 : Architecture réseau, adressage et routage (7 points)

Contrôler la cohérence de l'architecture et du plan d'adressage

Vous devez vérifier la configuration logique du réseau avant d'engager le diagnostic de l'incident. Les VLAN et les interfaces du routeur sont décrits dans le DT 1. Les réseaux IPv4 sont configurés en /24. Le préfixe IPv6 global attribué au site est 2001:db8:24::/48 ; chaque VLAN reçoit un préfixe /64. Le routeur R1 assure le routage inter-VLAN et la sortie vers le fournisseur d'accès.

Synthèse des VLAN et interfaces

VLAN	Usage	Interface logique R1	IPv4 de passerelle	Préfixe IPv6
10	Utilisateurs	G0/0.10	10.24.10.1/24	2001:db8:24:10::1/64
20	Administration	G0/0.20	10.24.20.1/24	2001:db8:24:20::1/64
30	Serveurs	G0/0.30	10.24.30.1/24	2001:db8:24:30::1/64
99	Gestion des équipements	G0/0.99	10.24.99.1/24	2001:db8:24:99::1/64

Données extraites de la documentation d'exploitation du site.

Liaisons de la topologie

Équipement source	Interface source	Équipement destination	Interface destination	Rôle ou VLAN transportés
Postes utilisateurs	Ethernet	SW1	Ports d'accès	VLAN 10
Postes administration	Ethernet	SW1	Ports d'accès	VLAN 20
Serveur applicatif et DNS	Ethernet	SW1	Port d'accès	VLAN 30
SW1	Gi1/0/24	R1	G0/0	Lien trunk : VLAN 10, 20, 30 et 99
R1	G0/1	Routeur opérateur	Interface client	WAN : 198.51.100.10/30
Serveur de supervision cloud	Internet	Routeur opérateur	Accès Internet	Collecte des alertes par HTTPS

Schéma fonctionnel fourni sous forme de liaisons ; le lien entre le commutateur et R1 transporte les VLAN indiqués.

1.1 (1,5 point) À partir du DT 1, décrivez le rôle du VLAN 30 et celui du lien trunk entre SW1 et R1. Indiquez pourquoi le routage inter-VLAN est nécessaire pour qu'un poste du VLAN 10 communique avec le serveur du VLAN 30.

1.2 (2 points) Pour le poste utilisateur 10.24.10.45/24, donnez l'adresse du réseau, l'adresse de diffusion et la plage d'adresses utilisables. Indiquez si l'adresse de passerelle 10.24.10.1 appartient au même sous-réseau et justifiez votre réponse.

1.3 (2 points) Complétez dans le DR 1 les routes IPv4 directement connectées à R1 et sa route par défaut. Pour la route par défaut, utilisez l'adresse du routeur opérateur indiquée dans le DT 1. Renseignez la destination avec son préfixe, le prochain saut et l'interface de sortie.

1.4 (1,5 point) Le poste d'administration 10.24.20.77 utilise le préfixe IPv6 2001:db8:24:20::/64. Donnez l'adresse de passerelle IPv6 configurée sur R1 pour ce VLAN. Expliquez en une phrase ce que signifie la longueur /64 dans ce préfixe.

PARTIE 2 : Exploitation et automatisation des contrôles (6 points)

Mettre en œuvre des tests réseau et interpréter leurs résultats

Le poste de diagnostic est raccordé au VLAN 20 et possède l'adresse 10.24.20.77/24, la passerelle 10.24.20.1 et le serveur DNS 10.24.30.10. Le serveur applicatif, également serveur DNS, porte l'adresse 10.24.30.20/24 et utilise la passerelle 10.24.30.1. Le nom applicatif à tester est intranet.novalys.test ; l'enregistrement DNS attendu est 10.24.30.20.

Les commandes et résultats ci-dessous ont été relevés depuis le poste de diagnostic. Les trois cibles de contrôle sont considérées comme disponibles si elles répondent au test indiqué : passerelle 10.24.20.1 par ICMP, serveur 10.24.30.20 par ICMP et intranet.novalys.test par résolution DNS vers 10.24.30.20.

Résultats des contrôles réseau

Contrôle	Commande exécutée	Résultat observé
Passerelle du VLAN 20	ping -c 2 10.24.20.1	2 réponses reçues, 0 % de perte
Serveur applicatif	ping -c 2 10.24.30.20	Aucune réponse, 100 % de perte
Résolution DNS	dig +short intranet.novalys.test	Aucun enregistrement retourné
Route vers le serveur	traceroute -n 10.24.30.20	Saut 1 : 10.24.20.1 ; aucun saut ultérieur

Relevés effectués depuis le poste 10.24.20.77.

2.1 (2 points) Rédigez une séquence de commandes Linux, dans l'ordre, permettant de vérifier la configuration IP du poste, la joignabilité de la passerelle, la route vers 10.24.30.20 et la résolution du nom intranet.novalys.test. Précisez pour chaque commande l'information recherchée. Les commandes doivent être adaptées aux adresses et au nom fournis dans l'énoncé.

2.2 (2 points) Interprétez les résultats du tableau de contrôles. Indiquez ce qu'ils permettent de valider, à quel niveau se situe vraisemblablement la rupture et deux vérifications complémentaires à effectuer sur SW1, R1 ou le serveur avant de modifier la configuration.

2.3 (2 points) Proposez une fonction Python nommée *etat_service* prenant trois booléens en paramètres : *passerelle_ok*, *serveur_ok* et *dns_ok*. La fonction doit retourner « OK » si les trois tests sont vrais et « INCIDENT » dans tous les autres cas. Donnez également la valeur retournée pour les résultats observés dans le tableau.

PARTIE 3 : Cybersécurité, analyse de traces et durcissement (7 points)

Qualifier un incident et proposer des mesures de protection adaptées

Le service de supervision a transmis les extraits de journalisation reproduits dans le DT 2. Les heures sont exprimées en UTC et les horloges des équipements sont synchronisées par NTP. L'adresse 10.24.20.77 correspond au poste d'administration ; 10.24.20.50 est le bastion d'administration autorisé. Le serveur 10.24.30.10 fournit le service SSH réservé aux administrateurs.

Les journaux sont des données de diagnostic. Ils ne démontrent pas à eux seuls qu'un compte a été compromis. Vous devez distinguer les faits observés des hypothèses et proposer des actions compatibles avec la continuité de service.

Extraits de traces système et réseau

Heure UTC	Source	Trace observée
08:41:12	10.24.20.77	sshd[2411]: Failed password for invalid user admin from 10.24.20.77 port 51422 ssh2
08:41:18	10.24.20.77	sshd[2414]: Failed password for root from 10.24.20.77 port 51428 ssh2
08:41:25	10.24.20.77	sshd[2419]: Failed password for invalid user support from 10.24.20.77 port 51434 ssh2
08:43:02	10.24.20.50	sshd[2450]: Accepted publickey for ops from 10.24.20.50 port 52011 ssh2
08:44:10	Capture réseau	TCP SYN vers 10.24.30.10:22, suivi d'une réponse TCP RST ; aucune session SSH établie
08:45:31	10.24.20.77	sshd[2462]: Failed password for ops from 10.24.20.77 port 51480 ssh2

Extraits horodatés du serveur srv-admin et d'une capture réalisée sur le réseau de laboratoire.

3.1 (2 points) Relevez deux faits établis par les journaux concernant les tentatives SSH et la connexion du compte ops. Distinguez ces faits d'une hypothèse sur l'origine ou l'objectif des tentatives.

3.2 (2 points) Interprétez la trace TCP SYN suivie d'un RST vers le port 22. Indiquez ce qu'elle établit et ce qu'elle ne permet pas, à elle seule, de conclure. Donnez deux contrôles à effectuer sur le serveur ou son filtrage réseau afin d'expliquer l'absence de session SSH.

3.3 (1,5 point) Classez l'événement constitué par les échecs de connexion répétés sur une échelle de priorité faible, moyenne ou élevée. Justifiez le classement à partir des traces et précisez une action immédiate de traitement qui préserve les éléments nécessaires à l'analyse.

3.4 (1,5 point) Proposez trois mesures de durcissement des accès SSH cohérentes avec le contexte. Votre réponse doit inclure une mesure portant sur l'authentification, une mesure de restriction des sources réseau et une mesure de journalisation ou de supervision.

DOSSIER TECHNIQUE ET RESSOURCES

Documents ressources nécessaires à la résolution du sujet

DT 1 : TOPOLOGIE, PLAN D'ADRESSAGE ET CONFIGURATION RÉSEAU

Topologie logique : les postes utilisateurs sont raccordés aux ports d'accès du VLAN 10 de SW1 ; les postes d'administration au VLAN 20 ; les serveurs au VLAN 30 ; les interfaces de gestion des équipements au VLAN 99. Le port SW1 Gi1/0/24 est configuré en trunk vers R1 G0/0 et transporte les VLAN 10, 20, 30 et 99. R1 utilise des sous-interfaces 802.1Q pour le routage inter-VLAN.

Les réseaux IPv4 sont 10.24.10.0/24, 10.24.20.0/24, 10.24.30.0/24 et 10.24.99.0/24. Les passerelles correspondantes sont les adresses .1. Le réseau WAN est 198.51.100.8/30 : l'adresse du routeur opérateur est 198.51.100.9 et celle de R1 est 198.51.100.10. La route par défaut de R1 doit donc utiliser le routeur opérateur comme prochain saut. Le préfixe IPv6 global du site est 2001:db8:24::/48 ; les préfixes VLAN et passerelles IPv6 figurent dans le tableau de la partie 1.

Équipements utiles au diagnostic : poste utilisateur 10.24.10.45/24 ; poste d'administration 10.24.20.77/24 ; bastion 10.24.20.50/24 ; serveur DNS 10.24.30.10/24 ; serveur applicatif 10.24.30.20/24. Le serveur applicatif utilise la passerelle 10.24.30.1. Le poste d'administration utilise le serveur DNS 10.24.30.10 et la passerelle 10.24.20.1.

DT 1 : Plan d'adressage des VLAN

VLAN	Fonction	Réseau IPv4	Passerelle IPv4	Préfixe IPv6	Passerelle IPv6
10	Utilisateurs	10.24.10.0/24	10.24.10.1	2001:db8:24:10::/64	2001:db8:24:10::1
20	Administration	10.24.20.0/24	10.24.20.1	2001:db8:24:20::/64	2001:db8:24:20::1
30	Serveurs	10.24.30.0/24	10.24.30.1	2001:db8:24:30::/64	2001:db8:24:30::1
99	Gestion des équipements	10.24.99.0/24	10.24.99.1	2001:db8:24:99::/64	2001:db8:24:99::1

Les adresses de passerelle sont configurées sur les sous-interfaces de R1.

DT 1 : Interfaces et routes de R1

Interface	Adresse ou configuration	État attendu
G0/0.10	802.1Q VLAN 10 ; 10.24.10.1/24	Active
G0/0.20	802.1Q VLAN 20 ; 10.24.20.1/24	Active
G0/0.30	802.1Q VLAN 30 ; 10.24.30.1/24	Active
G0/0.99	802.1Q VLAN 99 ; 10.24.99.1/24	Active
G0/1	198.51.100.10/30	Liaison WAN active
Route par défaut	Prochain saut 198.51.100.9	Présente

État de référence prévu pour l'architecture du site.

DT 2 : EXTRAITS DE JOURNAUX ET ÉLÉMENTS DE SÉCURITÉ

Les extraits présentés dans la partie 3 proviennent du journal d'authentification du serveur srv-admin, adresse 10.24.30.10, et d'une capture de trafic réalisée sur le segment de laboratoire. Les horloges sont synchronisées en UTC. Le bastion 10.24.20.50 est la seule source d'administration SSH autorisée par la politique du site. Le poste 10.24.20.77 est un poste d'administration, mais n'est pas déclaré comme bastion.

Politique en vigueur : les comptes nominatifs doivent être utilisés ; les accès d'administration sont limités au bastion ; l'authentification par clé est privilégiée ; les événements d'authentification doivent être conservés dans la plateforme de supervision. Aucun élément fourni ne permet d'affirmer qu'une authentification réussie de source inconnue a eu lieu.

DT 2 : Synthèse des événements disponibles

Élément	Donnée disponible	Portée
Échecs SSH	Plusieurs mots de passe refusés depuis 10.24.20.77	Échecs d'authentification consignés
Connexion réussie	Clé publique du compte ops depuis 10.24.20.50	Connexion acceptée depuis le bastion déclaré
Capture réseau	SYN vers TCP/22, réponse RST de 10.24.30.10	Aucune session SSH établie dans cet échange
Source autorisée	10.24.20.50	Bastion d'administration

Les messages complets utiles à l'analyse figurent dans le tableau de la partie 3.

NE RIEN ÉCRIRE DANS CETTE PARTIE

DR 1 : Table de routage IPv4 de R1, question 1.3 — **À RENDRE AVEC LA COPIE**

Complétez les lignes prévues à l'aide des données du DT 1. Indiquez les routes directement connectées et la route par défaut. Pour une route directement connectée, inscrivez « direct » dans la colonne « Prochain saut ».

Table de routage IPv4 à compléter

Destination / préfixe	Prochain saut	Interface de sortie
10.24.10.0/24	.....	.....
10.24.20.0/24	.....	.....
10.24.30.0/24	.....	.....
10.24.99.0/24	.....	.....
0.0.0.0/0	.....	.....

Table attendue pour R1 après validation de la configuration.

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.