Annales R4.01 – Sujet 2024

IUT Réseaux et Télécommunications Auxerre – 10 avril 2025

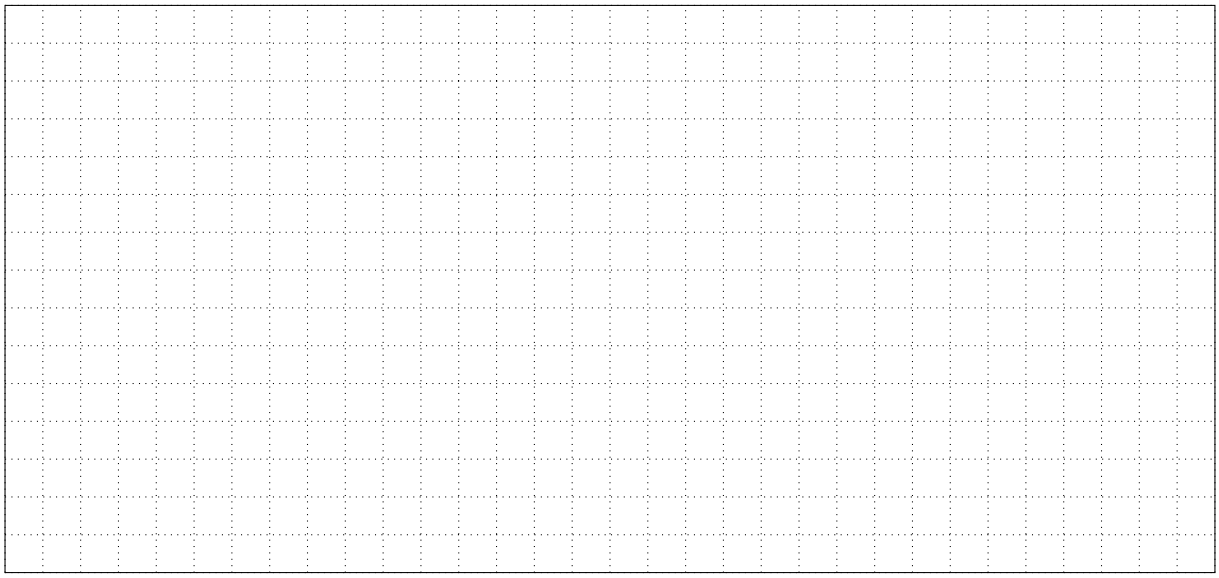
La société Torréfacteurs de Bourgogne, basée à Longvic (21) et à Nevers (58) propose la vente en ligne de café en grains et moulu. Suite à un audit de sécurité levant plusieurs manquements de sécurité, la société fait appel à vous pour mettre en place les correctifs.

Voici les services déployés sur son infrastructure hébergée à Longvic :

Service	**Adresse IP**	**Port**
Site Web public	`10.50.0.1`	TCP 80
Annuaire LDAP	`10.50.0.1`	TCP 389
Webmail public	`10.50.0.1`	TCP 80
Serveur IMAP	`10.50.0.2`	TCP 143
Serveur SMTP	`10.50.0.2`	TCP 25
Serveur DNS	`10.50.0.2`	UDP 53
Serveur DHCP	`10.50.0.2`	UDP 67
Boutique en ligne	`10.50.0.3`	TCP 80
Intranet (usage interne uniquement)	`10.50.0.4`	TCP 80

Tous les services sont hébergés dans la zone de SI interne. Cette zone est connectée directement à Internet sans règle de pare-feu.

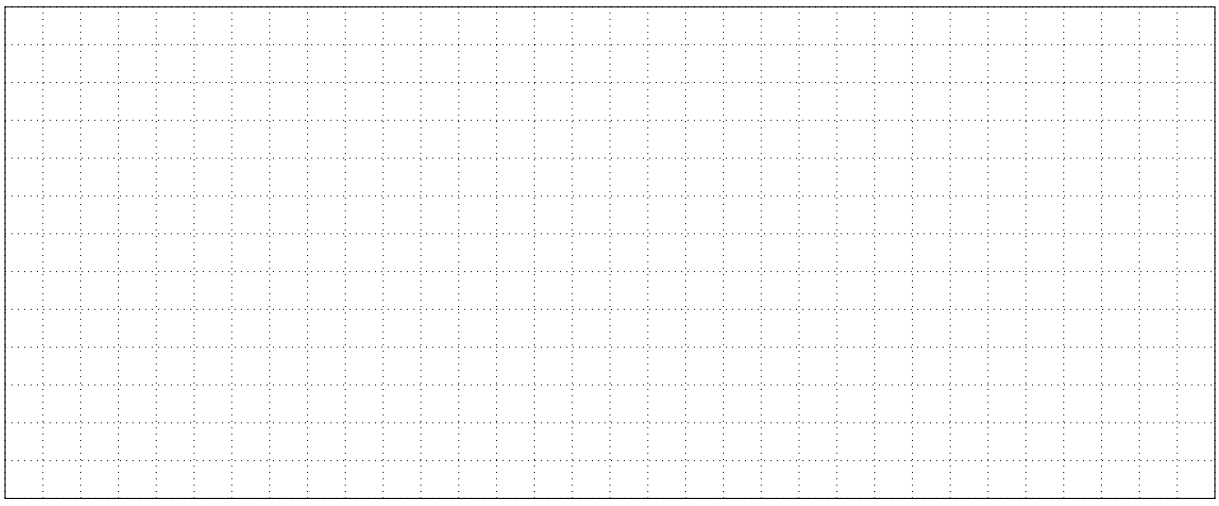
1. Les conclusions de l'audit préconisent de séparer les services dans deux zones réseau : le SI interne et une DMZ. Spécifiez dans quelles zones chaque service doit être affecté. (3 pts) :



2. Il a été décidé d'ajouter un pare-feu après le routeur d'accès à Internet. Paramétrez les ACL afin d'autoriser le trafic entrant uniquement vers les services que vous jugerez nécessaires d'exposer. Le reste du trafic doit être refusé. (2 pts) :

Adresse source	**Adresse destination**	**Type**	**Port**	**Action**
Exemple : 0.0.0.0	*10.10.0.1*	*TCP*	*5222*	*ACCEPT*

3. L'audit pointe l'existance de plusieurs comptes utilisateurs actifs associés à des personnes ayant quitté la société. Quelle solution proposez-vous pour centraliser la gestion des comptes utilisateurs et leurs droits associés ? (1 pt) :



4. Les utilisateurs accèdent directement à Internet. Quel dispositif doit être mis en œuvre afin de filtrer et authentifier le trafic ? Quels services doivent être ajoutés ? Dans quelles zones ? Quels flux doivent être filtrés ? (2 pts) :

5. Suite à la mise en place du dispositif de la question précédente, l'erreur suivante apparaît sur les postes bureautiques en accédant aux sites HTTPS, mais pas sur les sites en HTTP :

   > Connexion bloquée : problème de sécurité potentiel
   > Quelqu'un pourrait être en train d'essayer d'usurper l'identité du site. Vous ne devriez pas poursuivre.
   > Code d'erreur : `SEC_ERROR_UNKNOWN_ISSUER`

   Quelle est la cause du problème et comment y remédier ? (1 pt) :

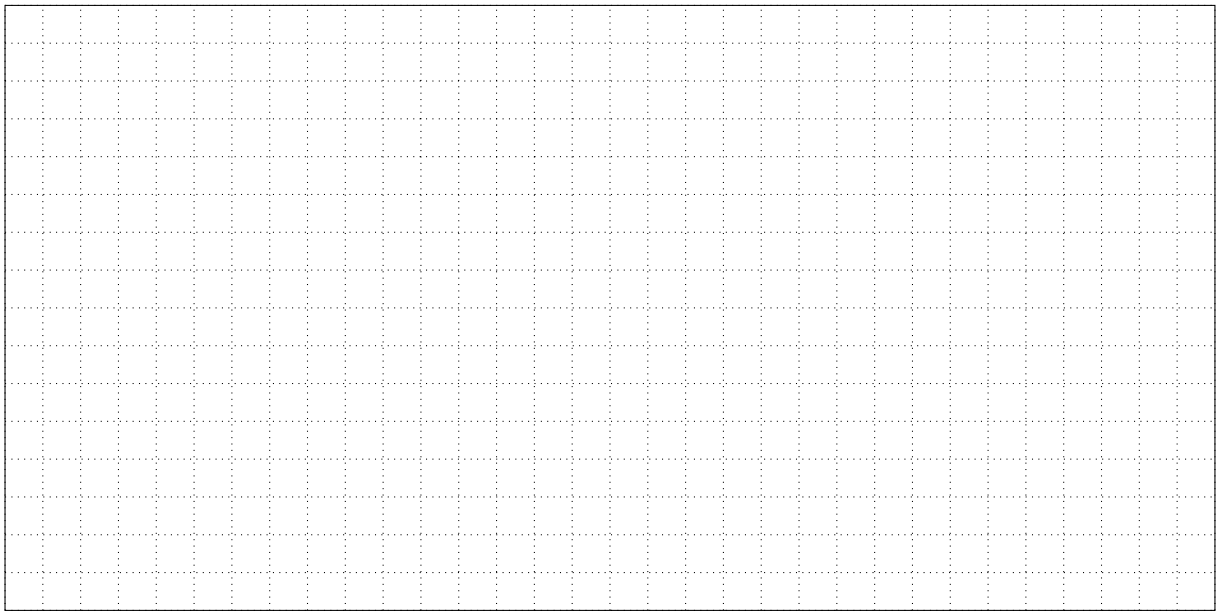
6. La clef privée du certificat d'un serveur a été compromise. Quelles opérations sont à effectuer ? Sur quelles autorités de votre infrastructure à clefs publiques ? (1 pt) :

7. Lors d'une intervention sur le poste d'un commercial, vous constatez la présence d'un papier collé sous le clavier mentionnant tous les mots de passe vers des outils sensibles. Quelles actions menez-vous pour palier à ce problème ? (1 pt) :

8. Après les modifications précédentes, les employés ne peuvent plus faire de télétravail. Quelle solution mettez-vous en place pour qu'ils puissent de nouveau travailler en toute sécurité ? (1 pt) :

9. Les conclusions de l'audit préconisent que les services en DMZ ne doivent pas accéder directement à l'annuaire du SI interne. Quelle solution mettez-vous en place pour permettre aux services en DMZ d'utiliser l'annuaire pour s'authentifier ? (1 pt)

10. Après déjeuner, la directrice financière vous annonce que son ordinateur portable a disparu. Quelles actions effectuer pour limiter l'impact de cet incident ? (2 pts) :



11. Vous constatez qu'un serveur possède un système d'exploitation ne recevant plus de mises à jour depuis 2014. Que faites-vous ? (1 pt) :

12. Un des services exposés à l'externe propose uniquement un accès en HTTP sans SSL. Quelle solution mettez-vous en place pour que les utilisateurs externes puissent se connecter en HTTPS sur le service ? (2 pts) :

13. Quelle autorité dans une infrastructure à clefs publiques est en charge de générer la CSR ? (1 pt) :

14. Il n'y a qu'un seul réseau WiFi sur lequel sont connectés les invités, les employés et les caméras de surveillance. Que faites-vous ? (1 pt) :