Annales R4.01 – Sujet 2024

IUT Réseaux et Télécommunications Auxerre – 4 avril 2024

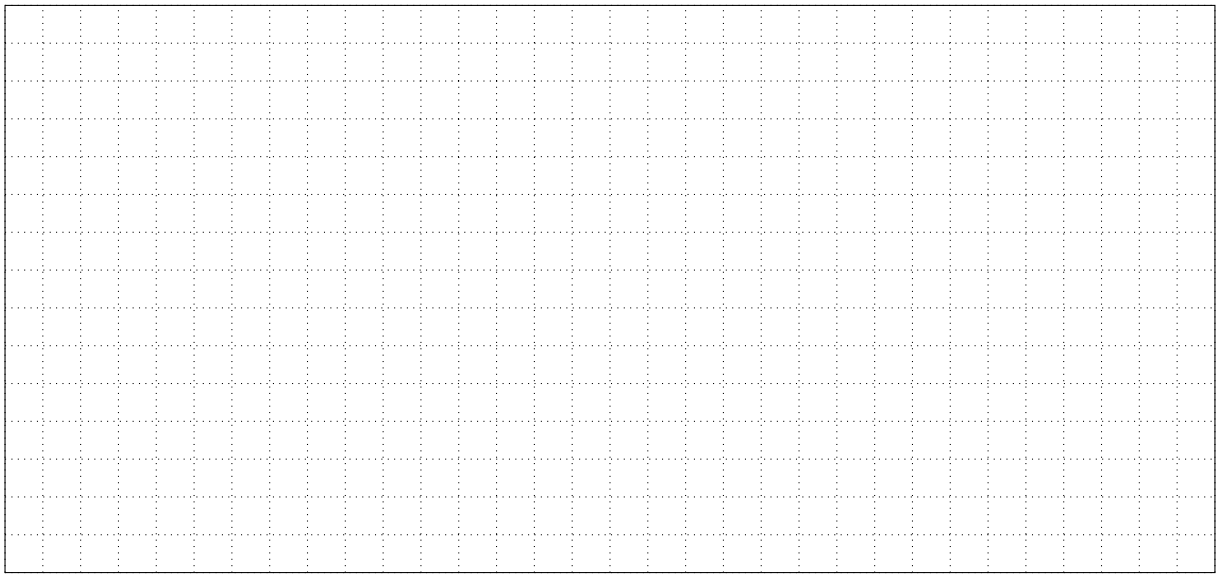
La société Anubis Infrastructures, basée à Monéteau (89) et à Dole (39), est spécialisée dans les infrastructures de télécommunications. Elle propose des services d'interconnexions pour entreprises. Suite à un audit de sécurité, plusieurs failles ont été révélées et l'entreprise fait appel à vous pour renforcer son infrastructure face aux attaques et aléas.

Voici les services déployés sur son infrastructure hébergée à Monéteau :

Service	**Adresse IP**	**Port**
Site Web public	`10.21.0.1`	TCP 80
Annuaire LDAP	`10.21.0.1`	TCP 389
Webmail public	`10.21.0.1`	TCP 80
Serveur IMAP	`10.21.0.2`	TCP 143
Serveur SMTP	`10.21.0.2`	TCP 25
Serveur DNS	`10.21.0.2`	UDP 53
Serveur DHCP	`10.21.0.2`	UDP 67
Dépôt config. clients (utilisé à l'externe)	`10.21.0.3`	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	*10.50.0.1*	*TCP*	*5222*	*ACCEPT*

3. Un collègue est en charge d'activer les protocoles sécurisés pour les services éligibles, mais il ne comprend pas le fonctionnement. Expliquez brièvement le fonctionnement du chiffrement asymétrique. (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) :

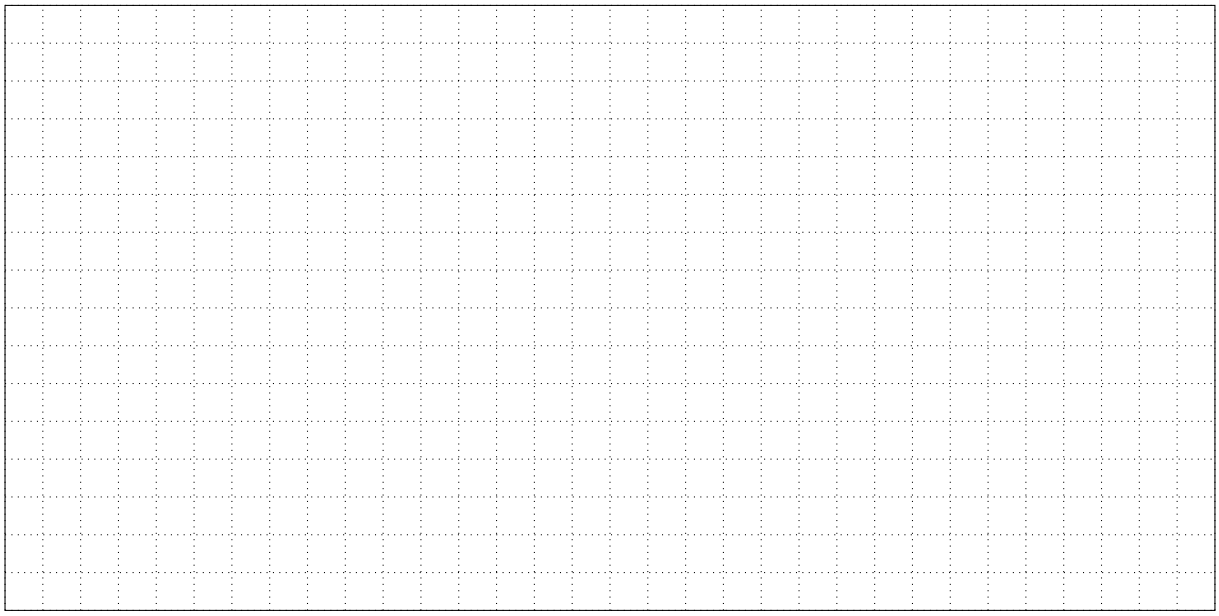
6. La clef privée du certificat d'un serveur a été compromise. Quelles opérations sont à effectuer ? Sur quelles autorités de votre infrastructure à clefs publiques ? (2 pts) :

7. Le rapport d'audit indique que le site Web institutionnel de la société est vulnérable aux injections SQL. Expliquez succinctement le principe de cette attaque et détaillez comment s'en prémunir (1 pt) :

8. Après l'ajout de vos ACL sur le pare-feu, le site de Dole ne peut plus accéder aux services internes. Quelle solution mettez-vous en place pour permettre l'interconnexion des deux sites de manière sécurisée. Dans quelles zones réseau déployer la solution ? (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. Lors de l'installation du poste de la directrice commerciale, vous découvrez que ses mots de passe sont inscrits sur un papier collé sous son écran. Que lui conseillez-vous ? (1 pt) :