Nom : _____ Prénom : _____

Annales R4.01 - Sujet initiaux 2022

IUT Réseaux et Télécommunications Auxerre – 21 février 2023

La société Autun Pharma produit des médicaments. De part son activité, cette société est une cible privilégiée des cyberattaques. Ainsi, elle souhaite renforcer son infrastructure et elle a fait appel à votre équipe pour mener cela à bien.

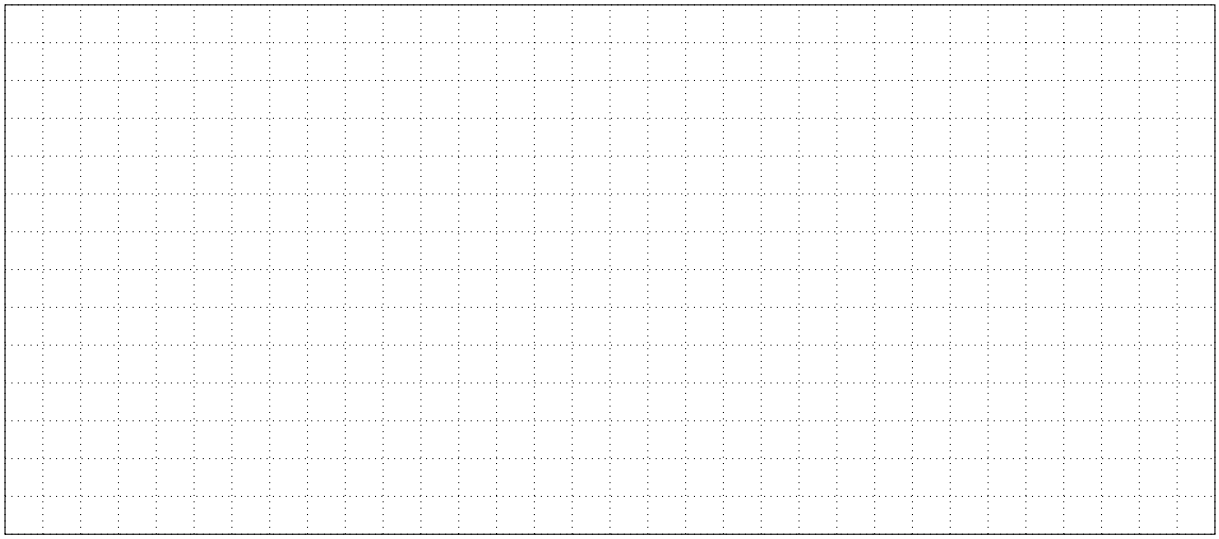
1. Vous êtes en charge de paramétrer les ACL du serveur `caducee.autunpharma.fr`, adresse IP 10.63.14.2/16 qui comporte un serveur Web ouvert à tout Internet (TCP 80 et 443), un serveur TFTP (UDP 69) et un serveur XMPP (TCP 5222 et TCP 5269) ouvert uniquement au réseau local. Fournissez les règles de filtrage en liste blanche (2 pts) :

Adresse source	**Adresse destination**	**Type**	**Port**	**Action**
Exemple : 0.0.0.0	*10.50.0.1*	*UDP*	*67*	*ACCEPT*

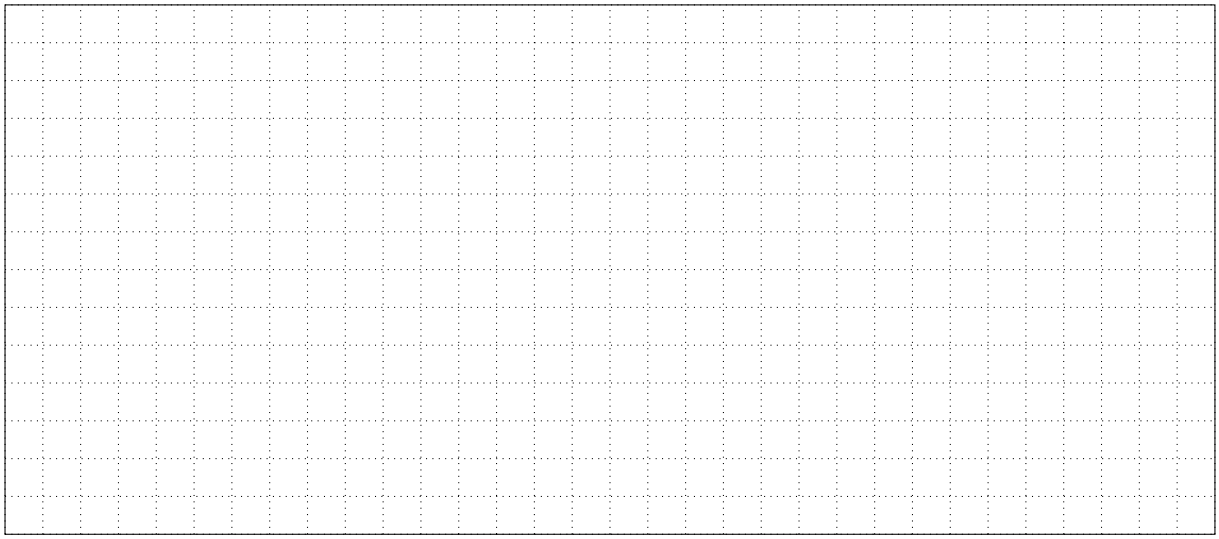
2. Un collègue vous demande de lui expliquer brièvement le principe d'une attaque par déni de service distribué (1 pt) :

3. Vous souhaitez signer cryptographiquement un document pour l'adresser à un client, décrivez brièvement ce processus en décrivant quelle(s) clef(s) est/sont mise(s) en œuvre (1 pt) :

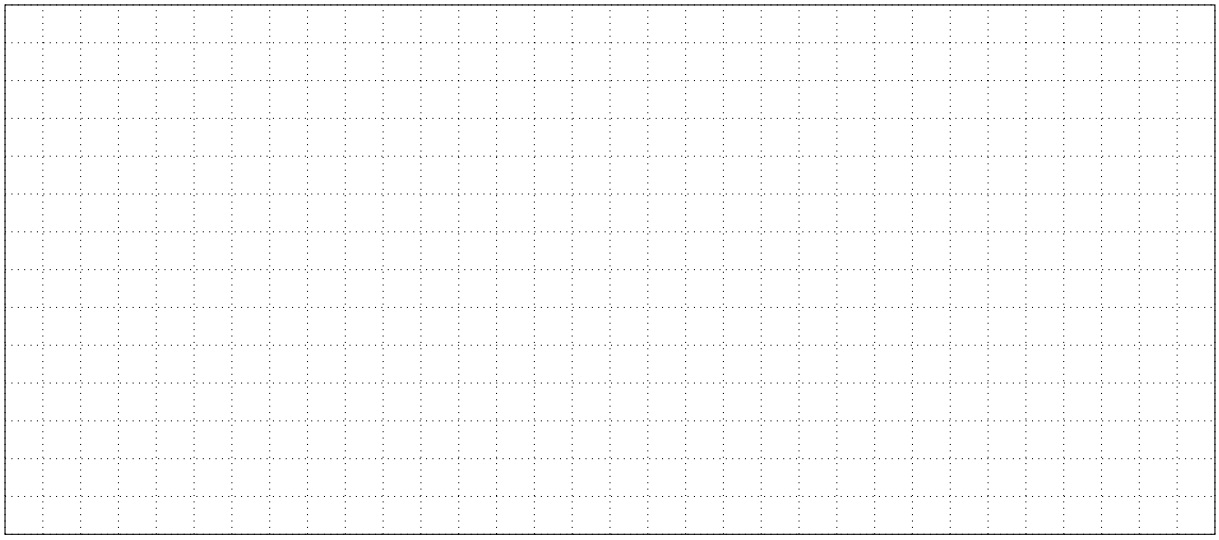
4. Expliquez comment fonctionne l'interception du trafic HTTPS avec un proxy (1 pt) :



5. La société ouvre un entrepôt à Toucy. Quelle solution est à mettre en œuvre pour relier de manière sécurisée les deux sites ? Décrivez l'architecture réseau de cette nouvelle solution (2 pts) :



6. Lors de l'installation du poste de la directrice commerciale, vous découvrez que ses mots de passe sont inscrits dans un fichier texte sur le bureau. Que lui conseillez-vous ? (1 pt) :



7. 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) :

8. Dans l'extrait de l'article suivant, quel est le type d'attaque qui a été employé ? Comment s'en prémunir ? (2 pts) :

> ## Arnaque au "faux président" : un entrepreneur de Paris escroqué perd 38 millions d'euros
>
> Le mode opératoire de l'escroquerie dite de "l'arnaque au président" consiste à usurper l'identité du dirigeant d'une entreprise pour convaincre un salarié de réaliser un faux ordre de virement. En décembre 2021, le comptable du promoteur immobilier Sefri-Cime, dont le siège est à Paris, reçoit l'appel d'un escroc se faisant passer pour un avocat. "Il prétexte une opération confidentielle de rachat de sociétés avec l'accord du président de la société", explique le commissaire Vincent Kozierow, chef de la Brigade des fraudes aux moyens de paiement (BFMP) de la police judiciaire de Paris.
>
> Le comptable reçoit ensuite un courriel usurpant l'identité du PDG qui lui confirme que l'opération est réalisée à sa demande. Au total, plus de 40 virements vont être effectués en quelques semaines pour un montant total de 38 millions d'euros, un record en France. L'escroquerie finit par être découverte et l'entreprise dépose plainte. À la même période, en Haute-Marne, une entreprise de métallurgie est également victime d'une "arnaque au président" pour une perte de 300 000 euros. Une deuxième tentative d'escroquerie, pour un montant de 500 000 euros a en revanche échoué, d'après Radio France.
>
> *Source : France 3 Paris Ile-de-France - 17/02/2023*

9. Un collègue a trouvé sur le parking une clef USB et il souhaite la brancher à son ordinateur. Que lui conseillez-vous ? (1 pt) :

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

11. Sur un serveur Apache, quelles opérations sont à effectuer pour rediriger automatiquement le trafic HTTP vers HTTPS ? (1 pt) :

12. Dans une architecture possédant un proxy pour la bureautique, est-ce qu'un poste peut effectuer des requêtes DNS hors des domaines locaux ? Justifiez (1 pt) :

13. Pour les services hébergés en DMZ, comment faire pour déléguer l'authentification au serveur LDAP en zone interne ? (2 pts) :

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

15. Lors du développement d'une page Web, vous êtes amené à interagir avec une base de données PostgreSQL. Expliquez succinctement le principe des injections SQL et détaillez comment s'en prémunir (1 pt) :