

Concours ITRF Session 2017

<p>Ne rien inscrire dans ce cadre</p>	<p>Concours : ASI - externe Emploi-type : Gestionnaire d'infrastructures BAP E Epreuve : admissibilité – épreuve écrite</p> <p>Nom : Nom de jeune fille : Prénom : Date de naissance :</p> <p> -----</p>
---------------------------------------	--

<p>Note : /20</p>					
I	II	III	IV	V	Total

Concours externe d'Assistant Ingénieur
BAP : E (Informatique, Statistiques et Calcul scientifique)
Emploi-type : Gestionnaire d'infrastructures
Epreuve écrite d'admissibilité – Durée : 3h – Coefficient : 4
Jeudi 15 juin 2017 de 9h00 à 12h00

INSTRUCTIONS

Ce sujet comporte **41 pages (y compris la page de garde)**
 Vous devez vérifier en début d'épreuve, le nombre de pages de ce fascicule.

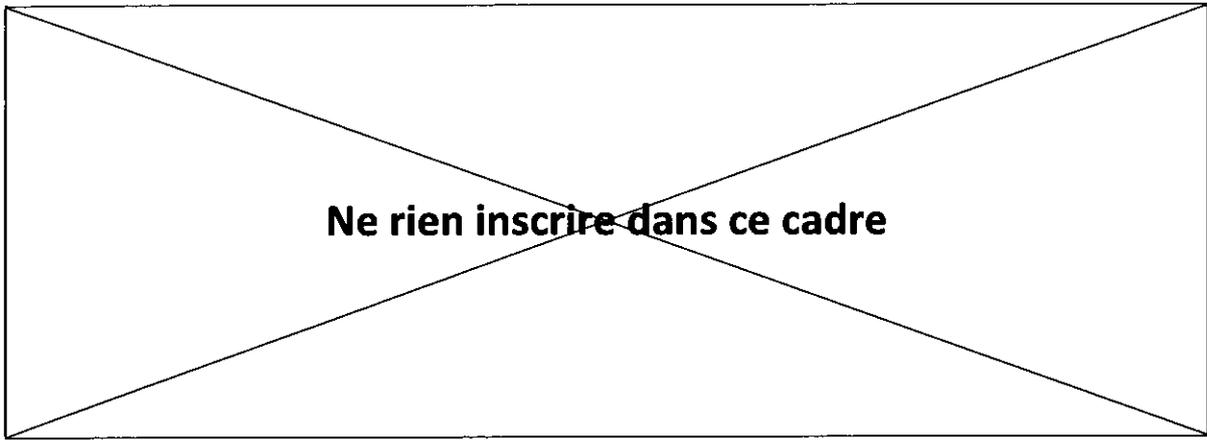
- **Questions rédactionnelles : répondre directement sur le sujet, à l'encre bleue ou noire seulement.**
- **Questionnaire à choix multiples : répondre sur la grille au stylo-encre noire**

L'usage du crayon papier ou du surligneur est **interdit**

Ne sont pas autorisés dans la salle d'examen :

- les téléphones mobiles et PDA
- les agendas, journaux, revues etc...
- dictionnaires, encyclopédies et ouvrages de référence.
- Tout type d'ordinateur personnel et de calculatrice.

Il vous est rappelé que votre identité doit figurer **uniquement** dans la partie supérieure de la bande à en tête de la copie (1^{ère} page).



Organisation du sujet :

I QCM : 38 questions

II Questions ouvertes

III Etude de cas : 4 mises en situation

IV Questions système-réseau

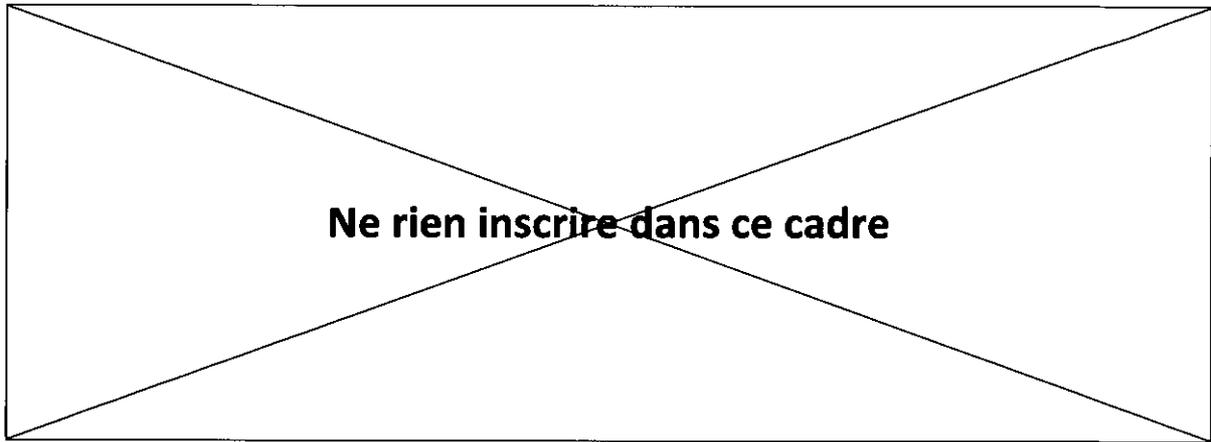
V Compréhension d'un texte en anglais avec questions en français, réponses attendues en français

Questions rédactionnelles :

Les réponses doivent être courtes, claires et synthétiques.

Il sera tenu compte dans la notation de la présentation, de l'orthographe et de la qualité de la rédaction.

La longueur des réponses est limitée : elles doivent tenir à l'intérieur des cadres. Toute réponse en dehors des lignes prévues sera ignorée par le correcteur.



I QCM : 38 questions – une seule réponse par question

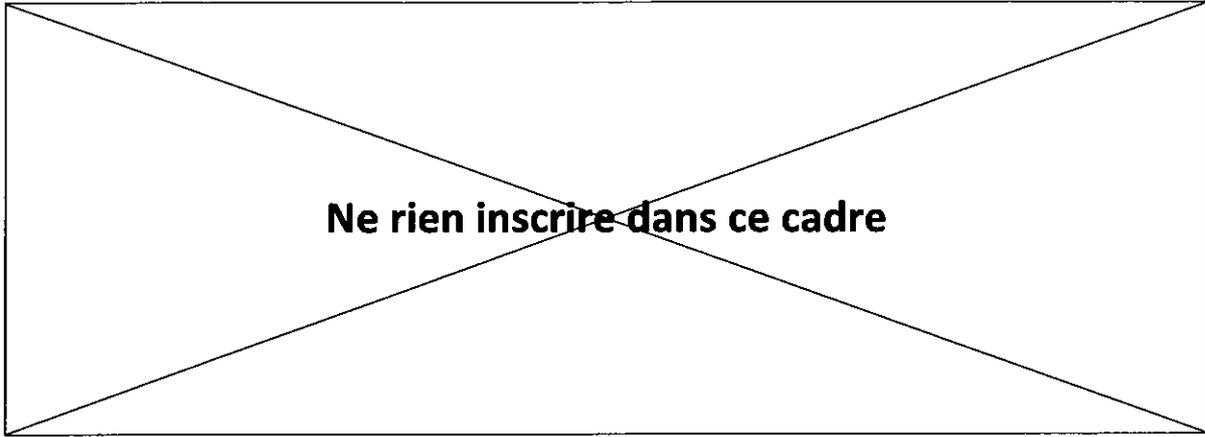
Veillez remplir au stylo noir les cases retenues pour votre réponse et veillez à ne faire apparaître aucune écriture dans les cases non retenues, comme indiqué sur la fiche ci-jointe. Vous disposez d'une ligne « repentir » pour chaque question qui vous permet de revenir sur votre choix initial pour faire une nouvelle proposition.

Toute ambiguïté entraînera un décompte NUL (0 point) pour l'affirmation.

1. Pour pouvoir se connecter par échange de clés à un serveur avec le protocole ssh, que doit transmettre l'utilisateur ?
 - A. Rien
 - B. Clé publique
 - C. Clé privée
 - D. Clé publique et clé privée

2. Le système de stockage RAID 6 peut supporter la panne de combien de disques durs ?
 - A. Aucun
 - B. Un
 - C. Deux
 - D. Cinq

3. Que signifie l'acronyme CIL ?
 - A. Correspondant Informatique et Liberté
 - B. Correspondant Informatique et Logiciel
 - C. Computing Infrastructure Language
 - D. Calcul Intensif Libre

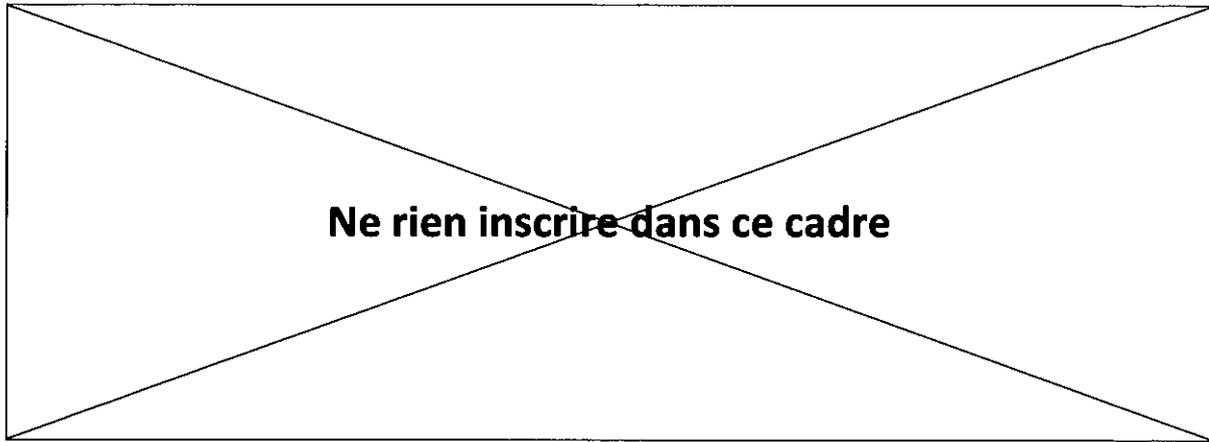


4. A quoi sert la commande mysqldump dans une requête SQL ?
 - A. A effacer la base
 - B. A détecter les doublons
 - C. A sauvegarder tout ou une partie de la base
 - D. A remplir la table de valeurs au hasard

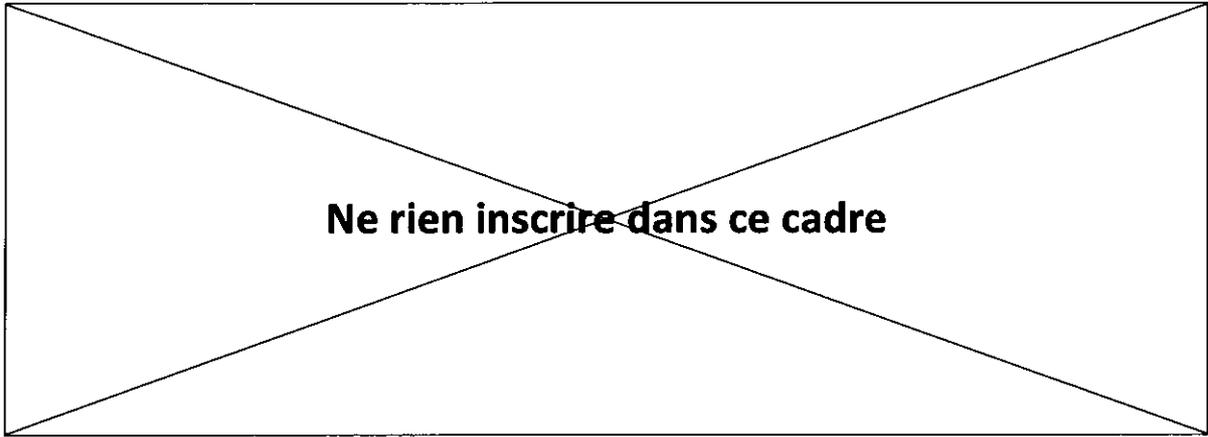
5. Laquelle de ces commandes ne permet pas d'administrer des packages ?
 - A. Npm
 - B. Dnf
 - C. apt-get
 - D. cat

6. Quel est le mot clé permettant de spécifier les données à rajouter dans une requête SQL de type INSERT ?
 - A. INTO
 - B. TO
 - C. DATA
 - D. VALUES

7. Quel type de licence ne permet pas de réutiliser du code (dans le sens des licences libres) ?
 - A. GPL
 - B. Cecill- B
 - C. Berkeley Database License
 - D. Oculus Rift SDR Licence



8. Lequel de ces acronymes ne représente pas un système de fichiers ?
- A. Fat32
 - B. HPF
 - C. NFS
 - D. BSD
9. Quelle affirmation est vraie concernant l'usage d'un logiciel libre, selon les définitions de la Free Software Foundation (FSF) ?
- A. L'utilisateur ne peut pas distribuer une version commerciale de la version modifiée.
 - B. L'utilisateur ne peut pas modifier le logiciel original.
 - C. L'accès est restrictif à un cercle d'utilisateurs définis.
 - D. Les nouvelles versions de la licence supplantent complètement les anciennes versions, interdisant de facto les permissions précédentes.
 - E. L'utilisateur a la liberté d'exécuter le programme comme il le souhaite, pour n'importe quel usage.
10. Qu'effectue la commande mtop ?
- A. Elle permet de suivre les processus mysql.
 - B. Elle permet d'associer un volume de données.
 - C. Elle permet d'ouvrir les ports d'un pare-feu.
 - D. Elle permet d'indiquer depuis combien de temps le système est actif.
 - E. Elle permet de lister les fichiers ouverts.
11. Quel principe ne fait pas partie de la méthodologie Agile ?
- A. Satisfaire l'utilisateur d'abord.
 - B. Faire simple.
 - C. Livrer le plus souvent possible des versions opérationnelles de l'application.
 - D. Ne pas re-développer ce qui a été validé lors d'une itération.
 - E. Ajuster régulièrement son comportement et ses processus.



12. Quel est l'acronyme associé à B.Y.O.D. ?

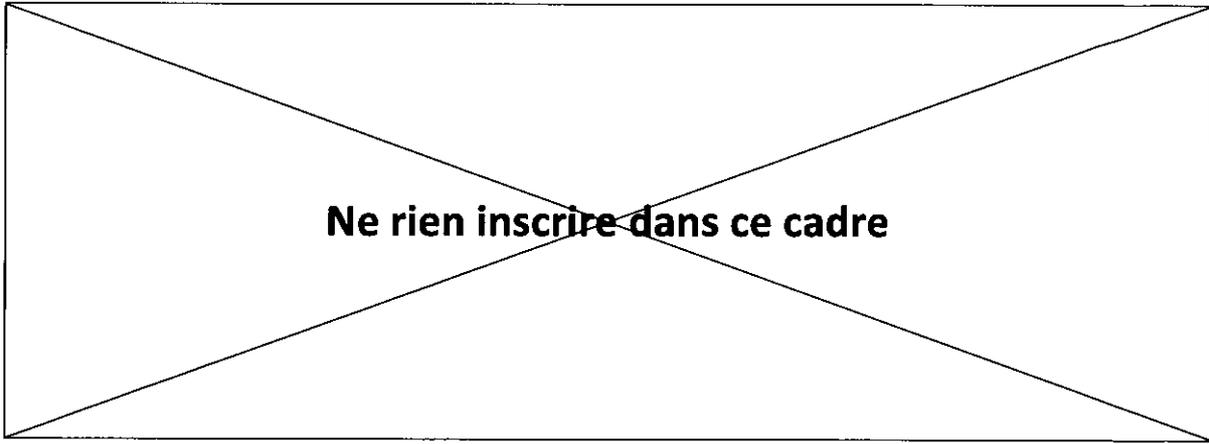
- A. Between You Over Device
- B. Bring Your Own Device
- C. Bring You On Device
- D. Between Your Own Device

13. Qu'est-ce que I.T.I.L. évoque pour vous ?

- A. La version 4 actuelle
- B. Information Technology Insights Library
- C. Il (ou elle) ne répond pas aux normes qualité au niveau Européen
- D. Un ensemble de livres de "bonnes pratiques"

14. Parmi ces propositions, laquelle ne correspond pas à un algorithme de chiffrement ?

- A. ECC
- B. AES256
- C. MD5
- D. RC4
- E. 3DES



15. La famille des normes ISO 27000 aide les organisations :

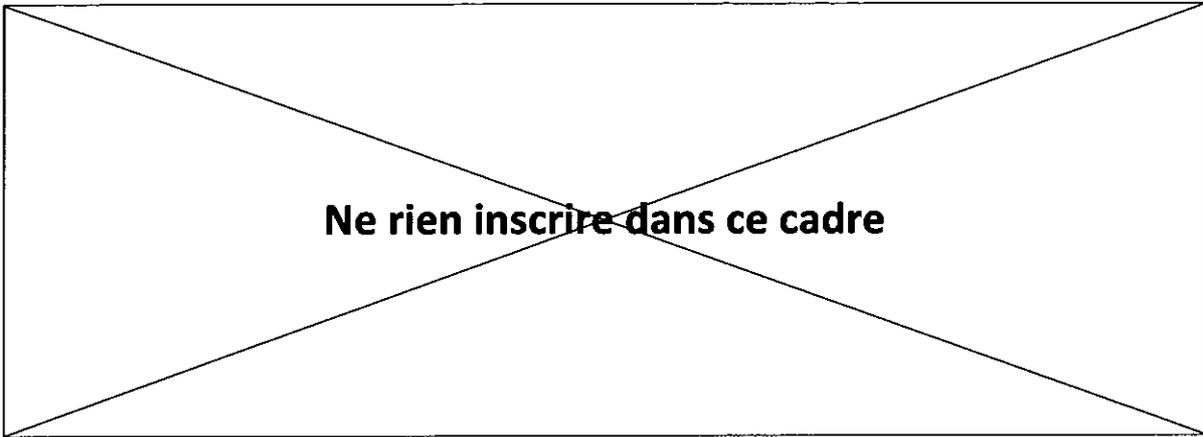
- A. au management de projets
- B. au management environnemental et au développement durable
- C. au management de la sécurité de leurs informations
- D. au management de la santé et de la sécurité du travail
- E. au management de l'énergie

16. Le PUE d'une salle informatique est :

- A. l'indicateur de la puissance électrique utilisée
- B. l'indicateur d'efficacité énergétique
- C. l'indicateur de l'énergie consommée par les systèmes informatiques
- D. l'indicateur donnant le taux de réutilisation de la chaleur produite par les serveurs

17. Lequel de ces protocoles n'est pas un protocole de routage :

- A. BGP
- B. IS-IS
- C. RIP
- D. OS-OS
- E. OSPF



18. Laquelle de ces normes ne correspond pas à un réseau wifi ?

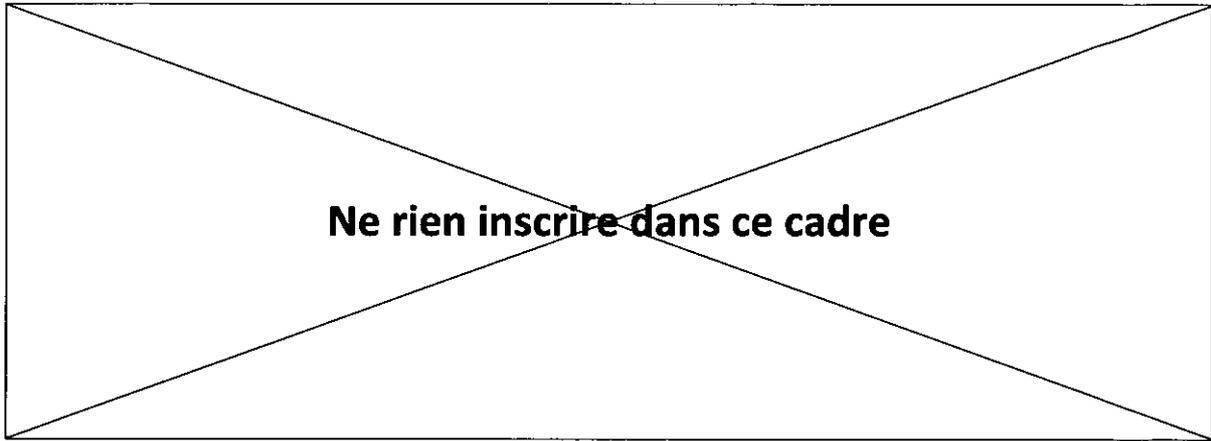
- A. 802.11a
- B. 802.11b
- C. 802.11f
- D. 802.11g
- E. 802.11n

19. USB 3.0 est théoriquement :

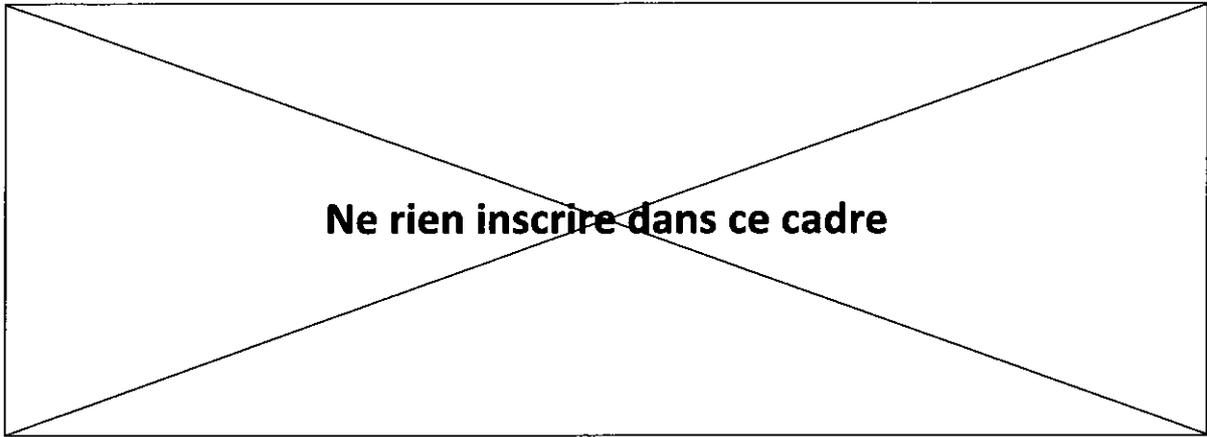
- A. aussi rapide que l'USB 2.0
- B. 2 fois plus rapide que l'USB 2.0
- C. 5 fois plus rapide que l'USB 2.0
- D. 10 fois plus rapide que l'USB 2.0
- E. 100 fois plus rapide que l'USB 2.0

20. Quel est le masque par défaut d'un adressage CIDR /25?

- A. 255.255.255.0
- B. 255.255.255.127
- C. 255.255.255.128
- D. 255.255.255.255



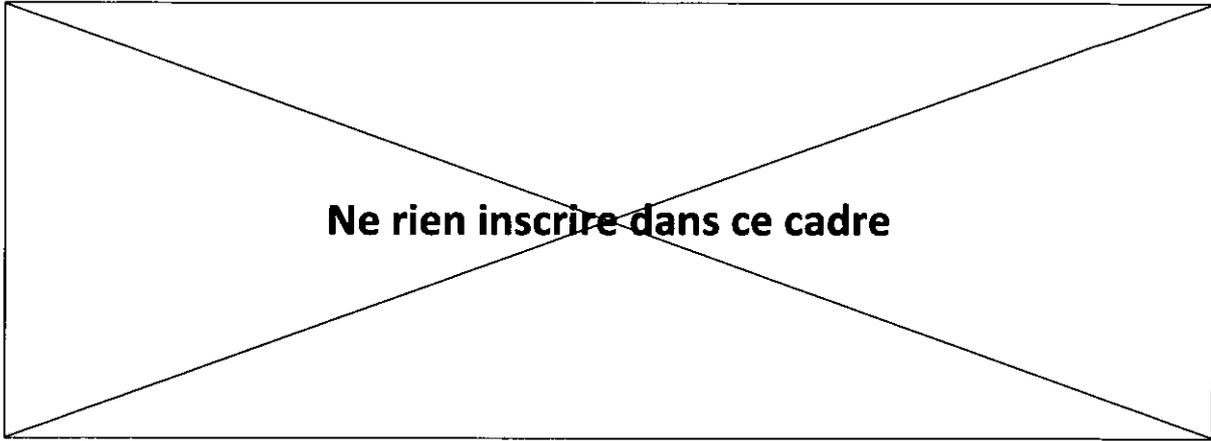
21. Lequel de ces mots de passe a le niveau de sécurité le plus élevé?
- A. azerty123
 - B. Gr3n0b13
 - C. Mickey0\$
 - D. Ms:Gh;29@
22. Laquelle de ces propositions n'est pas un SGBD ?
- A. Oracle
 - B. MySQL
 - C. GLPI
 - D. Access
23. Laquelle de ces actions permet de mettre à jour une table ?
- A. Delete
 - B. Insert
 - C. Update
 - D. Select
24. Quel mot clé intervient quand on souhaite récupérer des enregistrements en travaillant sur plusieurs tables ?
- A. Multi
 - B. Union
 - C. Join
 - D. Mx_table



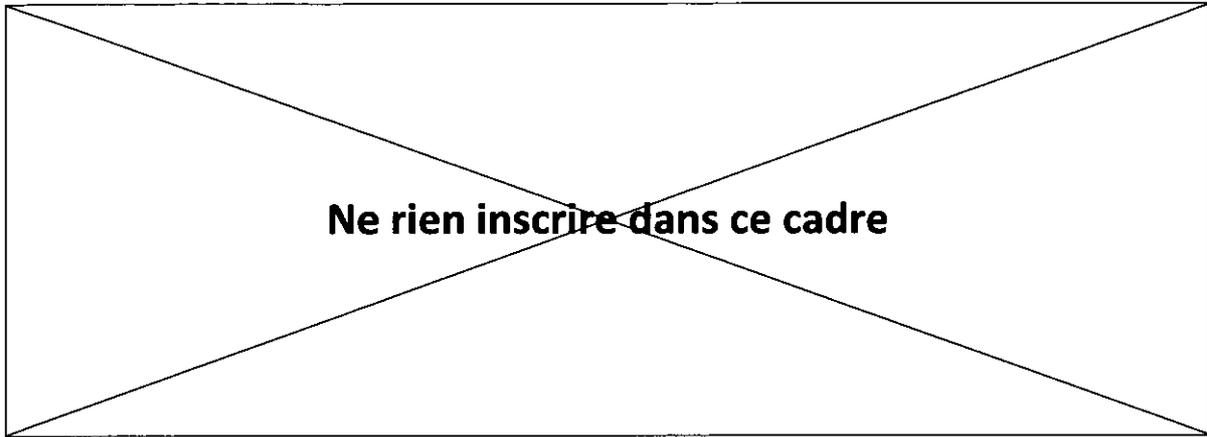
25. Laquelle de ces commandes permet de faire une restriction lors de l'interrogation d'une base ?
- A. Where
 - B. Group by
 - C. Having
 - D. Order by
26. Quelle est la requête SQL qui permet de sélectionner tous les enregistrements d'une table nommée « produits » ?
- A. `SELECT distinct id FROM produits ;`
 - B. `SELECT * FROM produits WHERE reference not null ;`
 - C. `SELECT * FROM produits ;`
 - D. `SELECT * WHERE produits ;`
27. L'instruction suivante en SQL :
- ```
SELECT produits FROM commandes

WHERE prix > 100

ORDER BY prix ;
```
- permet-elle de ?
- A. Lister les produits par groupe de 100
  - B. Lister les prix de tous les produits
  - C. Classer les prix supérieurs à 100 € par ordre décroissant
  - D. Lister les produits de plus de 100 € classés par prix



28. Que signifie PRA ?
- A. Plan Reprise Activité
  - B. Private Relation Administrator
  - C. Plan Réseau Adresse
  - D. Prime Recherche ASI
29. Que permet le PCA ?
- A. Une sauvegarde des données sur des sites distants
  - B. Un redémarrage ordonné des activités en cas de défaillance
  - C. Une haute disponibilité des activités et des services critiques
  - D. Un accès sécurisé aux services essentiels
30. Un serveur qui « swap » est un serveur qui :
- A. n'utilise que sa mémoire vive
  - B. n'utilise pas de mémoire vive
  - C. utilise de la mémoire sur disque
  - D. ce terme ne correspond à rien
31. Quel caractère permet de désactiver un utilisateur ou de remplacer le mot de passe dans le fichier système sous Linux?
- A. Un caractère '\*'
  - B. Un caractère '!'
  - C. Un caractère '\$'
  - D. Laisser vide



32. Que réalise la commande suivante sur une machine linux ?

```
ifconfig eth0 192.168.0.42
```

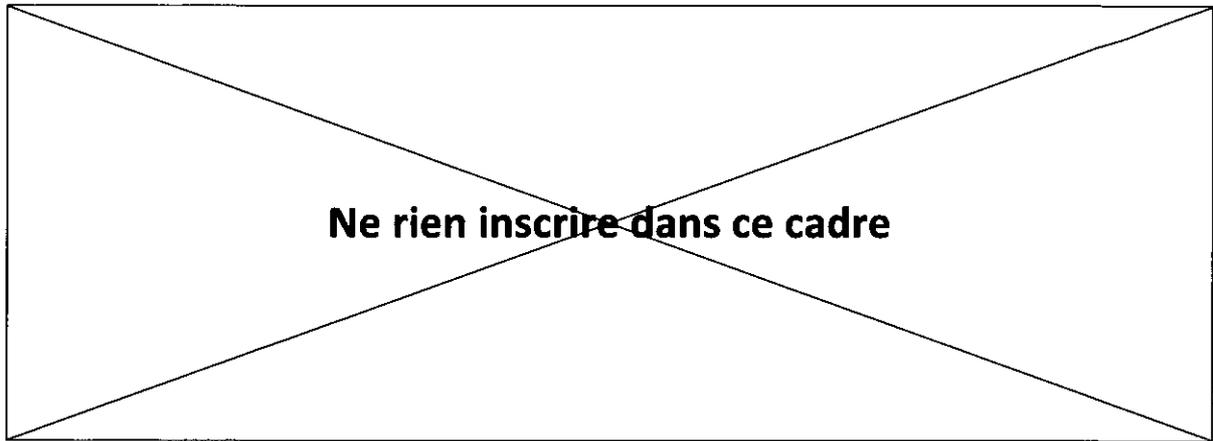
- A. Elle affiche une table de routage
- B. Elle configure l'interface réseau
- C. Elle établit une connexion avec la machine 192.168.0.42
- D. Elle donne l'état de l'interface réseau

33. Que signifie dans le domaine réseau le terme VRF ?

- A. Virtual Route Fast
- B. Virtual Routing Firewall
- C. Virtual Routing and Forwarding
- D. Very Routing Fast

34. Qu'est qu'une CMDB ?

- A. C'est une base d'inventaire
- B. C'est un composant réseau
- C. C'est indispensable à Windows
- D. C'est une base chargée de gérer les configurations



35. Quelle est la différence entre un logiciel conteneur et un logiciel de virtualisation ?

- A. Le conteneur héberge plusieurs systèmes d'exploitation (OS).
- B. La conteneurisation utilise un seul système d'exploitation.
- C. Un logiciel de virtualisation ne peut pas contenir plusieurs OS.
- D. Un logiciel conteneur permet de s'affranchir des problèmes de portabilité.

36. A quel domaine associez-vous ASN1 ?

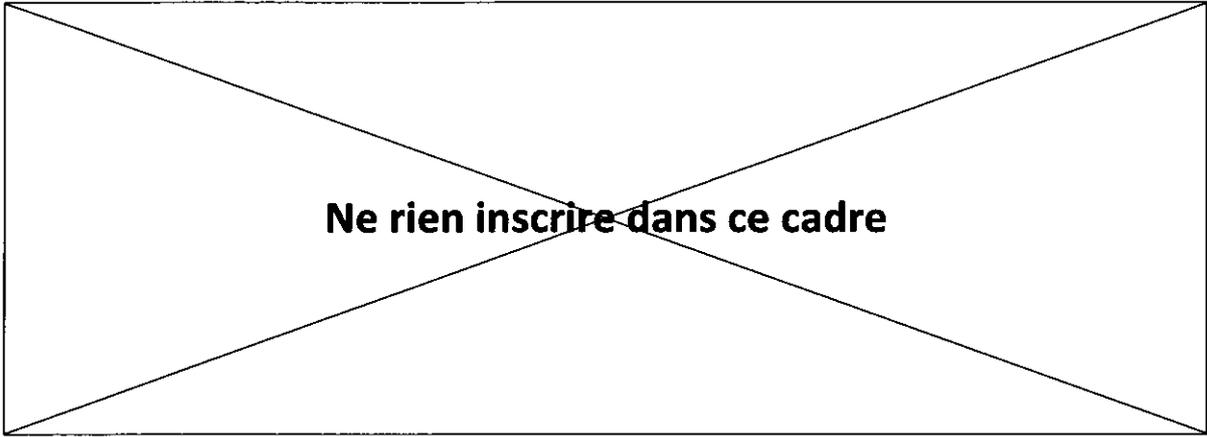
- A. Langage de développement
- B. Description annuaire ldap
- C. Gestion de poste de travail
- D. Un protocole réseau

37. Quel logiciel présenté dans la liste suivante ne sert pas à transférer des fichiers ?

- A. WinSCP
- B. Filezilla
- C. Bitkinex
- D. Putty

38- Quelle proposition dans la liste suivante n'est pas un logiciel de supervision ou métrologie ?

- A. Nagios
- B. Munin
- C. Netdisco
- D. Rancid



## **II Questions ouvertes**

**1. Que signifient les lettres SQL ?**

|  |
|--|
|  |
|--|

**2. Que représente le modèle relationnel ?**

|  |
|--|
|  |
|  |
|  |
|  |

**3. Qu'est-ce qu'un entrepôt de données (ou Data Warehouse) ?**

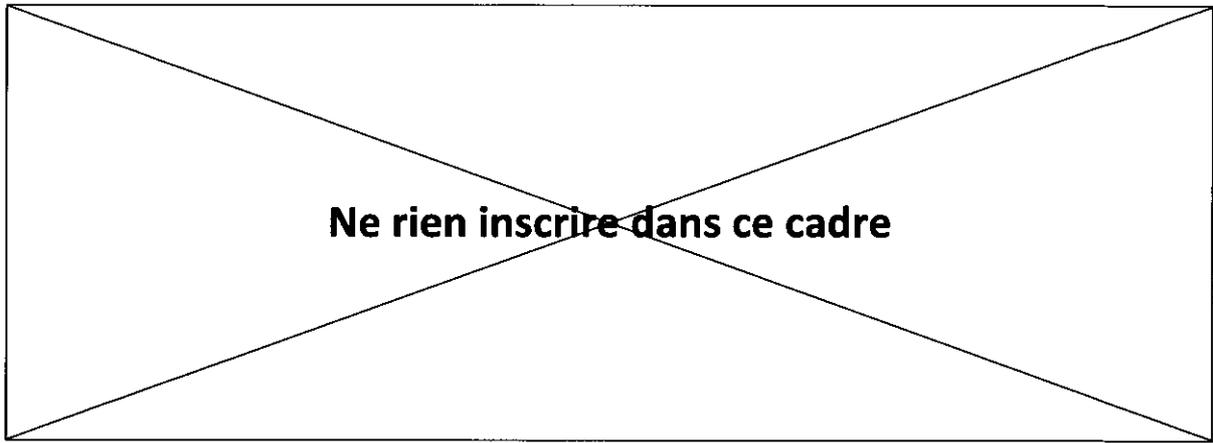
|  |
|--|
|  |
|  |
|  |
|  |

**4. Que signifie l'acronyme CNIL et quelle est sa mission ?**

|  |
|--|
|  |
|  |
|  |
|  |
|  |

**5. Quelle loi va prochainement rentrer en vigueur pour permettre de créer de nouveaux droits informatique et libertés ?**

|  |
|--|
|  |
|  |
|  |
|  |



**6. Que signifie DEEE ?**

|  |
|--|
|  |
|--|

**7. Citez 3 substances, préparations et composants devant être retirés de tout DEEE :**

|  |
|--|
|  |
|  |
|  |

**Ne rien inscrire dans ce cadre**

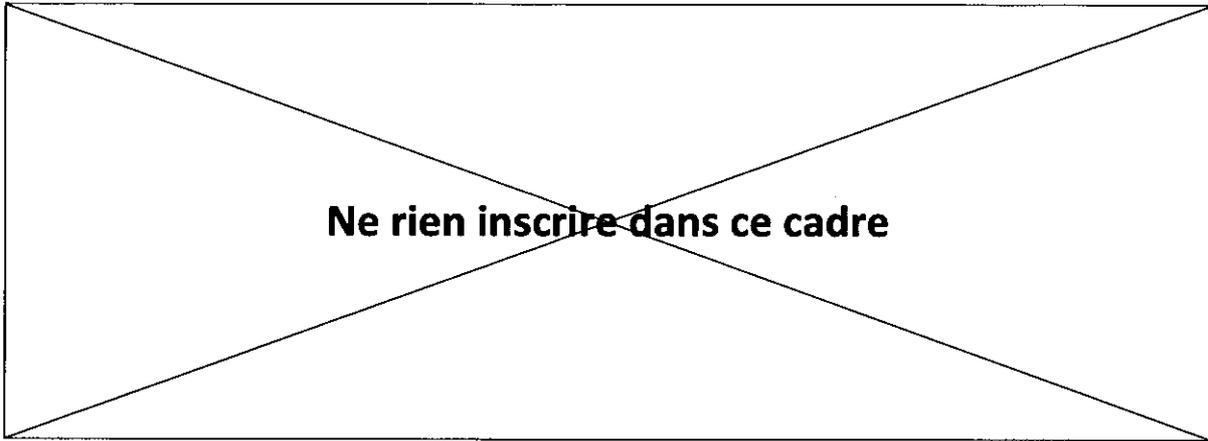
- 8. Sur un serveur sous linux vous souhaitez vérifier si le serveur web fonctionne. Quelle commande utilisez-vous?**

- 9. Donnez le protocole utilisé par un serveur web standard et le ou les ports TCPIP utilisés.**

- 10. Vous souhaitez connaître l'état des performances (mémoire/cpu...) d'un système linux/Unix. Quelle commande utilisez-vous?**

- 11. Lorsqu'on ajoute un utilisateur sur linux, dans quel fichier peut-on retrouver les utilisateurs ?**

- 12. On souhaite connaître l'état de l'espace disque d'un poste linux. Quelle commande passez-vous?**



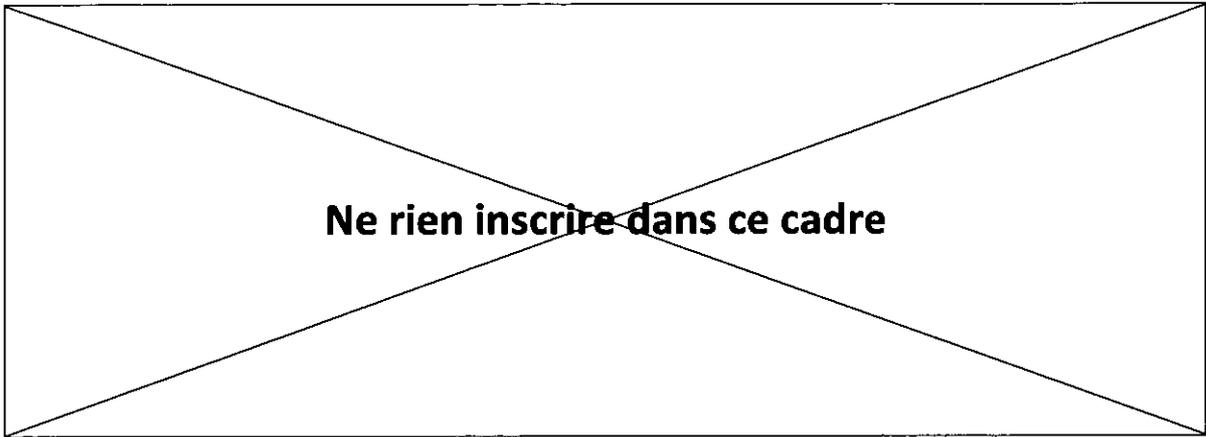
**13. Vous souhaitez connaître l'espace disque occupé du répertoire "these". Donnez la commande qui a été utilisée (ci-dessous à la place des ???) pour afficher les sous-répertoires et leur occupation :**

```
carrik@cassiopee:~$ pwd
/home/carrik/these
carrik@cassiopee:~$???
412K ./chapitres
488K ./figures/heat
532K ./figures
4,1M .
```

**14. Quelles commandes utiliseriez-vous pour activer et désactiver une interface réseau?**

**15. Sur une machine unix dans quel répertoire trouve-t-on les traces d'activité système ?**

**16. Quel protocole doit-on mettre en œuvre sur un réseau IP dans le cadre de la téléphonie sur IP ?**



17. Les adresses réseaux sont classifiées par « Classes », renseignez les classes dans le tableau suivant :

| Adresse     | Classe |
|-------------|--------|
| 10.0.0.1    |        |
| 161.3.104.1 |        |
| 172.16.0.1  |        |
| 192.168.0.1 |        |

18. Sous Windows 7, quelle commande permet d'afficher les informations suivantes ?

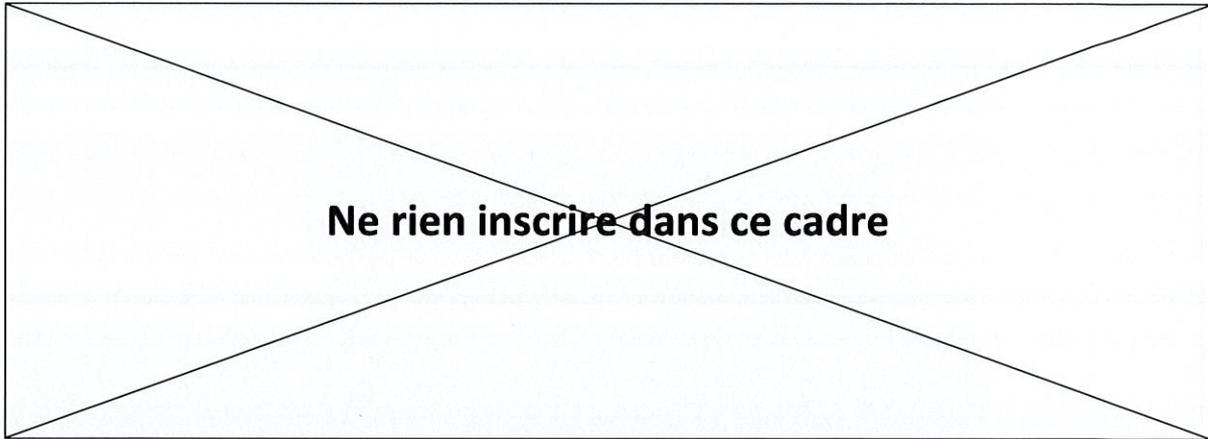
```

=====
Liste d'Interfaces
19...70 5a 0f d8 2c b8Intel(R) Ethernet Connection (3) I218-LM
17...66 80 99 ed de e2Microsoft Virtual WiFi Miniport Adapter
15...00 ff e7 92 e0 f3TAP-Windows Adapter V9
14...64 80 99 ed de e6Périphérique Bluetooth (réseau personnel)
12...64 80 99 ed de e2Intel(R) Dual Band Wireless-N 7265
 1...00 00 00 00 00 00 00 00Software Loopback Interface 1
25...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP
20...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #2
23...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #3
16...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
22...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #4
18...00 00 00 00 00 00 00 e0 Carte Microsoft ISATAP #7
=====

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau Masque réseau Adr. passerelle Adr. interface Métrique
0.0.0.0 0.0.0.0 10.42.224.1 10.42.227.83 25
10.42.224.0 255.255.240.0 On-link 10.42.227.83 281
10.42.227.83 255.255.255.255 On-link 10.42.227.83 281
10.42.239.255 255.255.255.255 On-link 10.42.227.83 281
127.0.0.0 255.0.0.0 On-link 127.0.0.1 306
127.0.0.1 255.255.255.255 On-link 127.0.0.1 306
127.255.255.255 255.255.255.255 On-link 127.0.0.1 306
169.254.0.0 255.255.0.0 On-link 169.254.253.207 276
169.254.253.207 255.255.255.255 On-link 169.254.253.207 276
169.254.255.255 255.255.255.255 On-link 169.254.253.207 276
224.0.0.0 240.0.0.0 On-link 127.0.0.1 306
224.0.0.0 240.0.0.0 On-link 10.42.227.83 281
224.0.0.0 240.0.0.0 On-link 169.254.253.207 276
255.255.255.255 255.255.255.255 On-link 127.0.0.1 306
255.255.255.255 255.255.255.255 On-link 10.42.227.83 281
255.255.255.255 255.255.255.255 On-link 169.254.253.207 276
=====

```





19. Sous Windows 7, quelle commande permet d'afficher les informations suivantes :

```
Configuration IP de Windows
Nom de l'hôte :
Suffixe DNS principal :
Type de noeud :
Routage IP activé :
Proxy WINS activé :
Liste de recherche du suffixe DNS.:

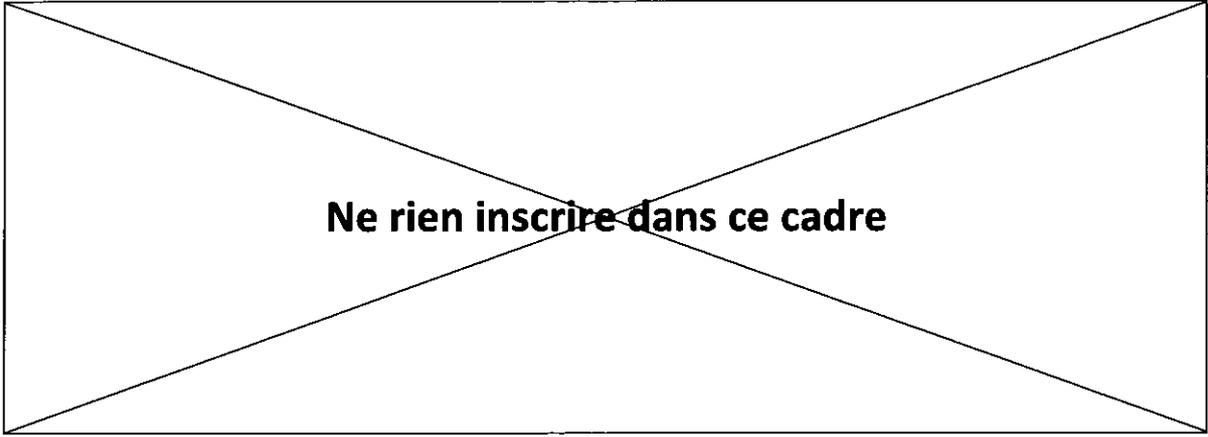
Carte Ethernet Connexion au réseau local 4 :
Statut du média. : Média déconnecté
Suffixe DNS propre à la connexion. . . :
Description. : Intel(R) Ethernet Connection (3) I21
8-LM
Adresse physique : 70-5A-0F-D8-2C-B8
DHCP activé. : Oui
Configuration automatique activée. . . : Oui

Carte réseau sans fil Connexion réseau sans fil 2 :
Statut du média. : Média déconnecté
Suffixe DNS propre à la connexion. . . :
Description. : Microsoft Virtual WiFi Miniport Adap
ter
Adresse physique : 66-80-99-ED-DE-E2
DHCP activé. : Oui
Configuration automatique activée. . . : Oui

Carte Ethernet Connexion au réseau local 2 :
Suffixe DNS propre à la connexion. . . :
Description. : TAP-Windows Adapter V9
Adresse physique : 00-FF-E7-92-E0-F3
DHCP activé. : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::2c85:dba5:16d1:fdcf%15<préféré
>
Adresse d'autoconfiguration IPv4 . . . : 169.254.253.207<préféré>
Masque de sous-réseau. : 255.255.0.0
Passerelle par défaut. :
IAID DHCPv6 : 620022503
DUID de client DHCPv6. : 00-01-00-01-1E-D4-84-83-70-5A-0F-D8-2C
-B8
Serveurs DNS. : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS sur Tcpip. : Activé
```

20. Sur un système Windows où stocke-t-on de façon générale les certificats ?

21. Quelle notion permet de structurer de façon arborescente un annuaire LDAP Active Directory ?

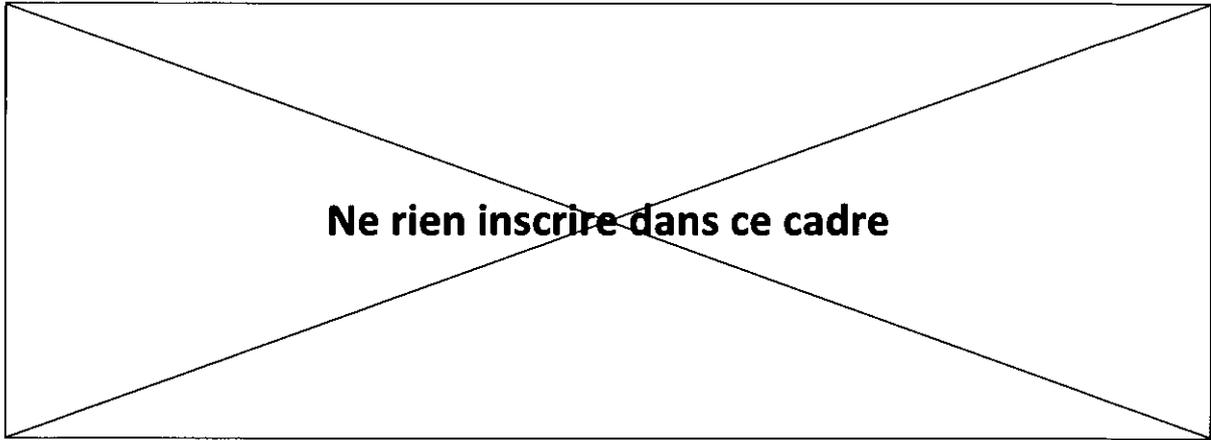


**22. Qu'est-ce que le NAT ?**

**Donnez la signification de l'acronyme :**

**Expliquez en 3 lignes maximum.**

|  |
|--|
|  |
|  |
|  |



**23. Quels sont les avantages et les inconvénients du B.Y.O.D. pour l'utilisateur ?**

Avantages :

|  |
|--|
|  |
|  |
|  |

Inconvénients :

|  |
|--|
|  |
|  |
|  |

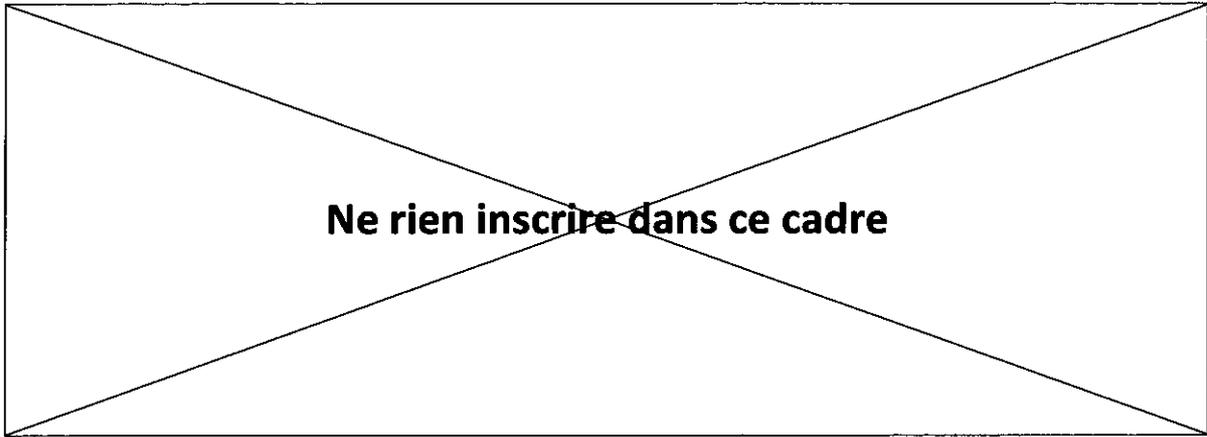
**24. Quels sont les avantages et les inconvénients du B.Y.O.D. pour l'entreprise ?**

Avantages :

|  |
|--|
|  |
|  |
|  |

Inconvénients :

|  |
|--|
|  |
|  |
|  |



### **III Etude de cas : 4 mises en situation**

#### **Cas A :**

Vous êtes le responsable informatique d'une structure. Vous venez de recevoir une alerte informatique, un virus est en train de se propager sur votre réseau. Vous n'avez pas beaucoup d'information sur le virus en question et de sa dangerosité potentielle.

**1 . Qui contactez-vous en premier ?**

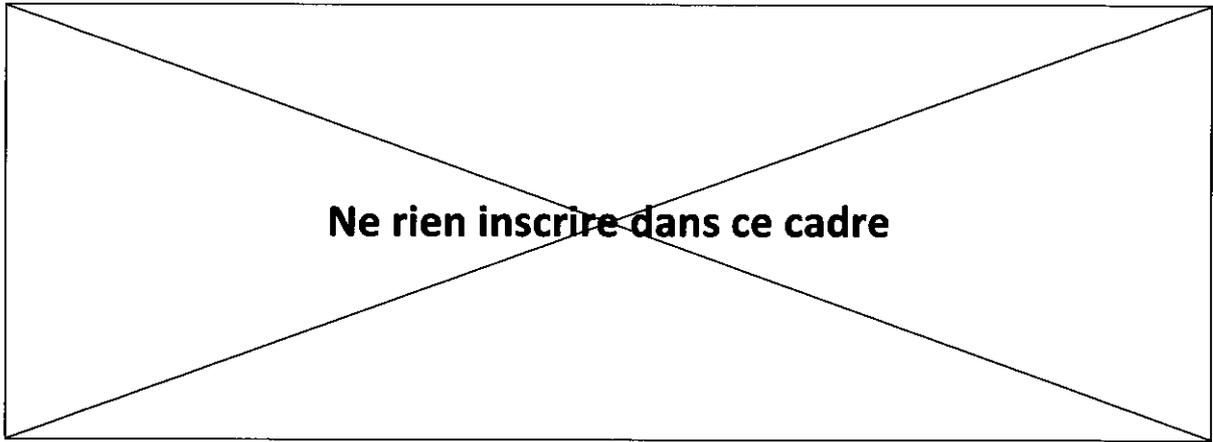
|  |
|--|
|  |
|--|

**2. Quelles mesures d'urgence pourriez-vous être amené à mettre en place ?**

|  |
|--|
|  |
|  |

**3. Quelle communication faites-vous envers les usagers ?**

|  |
|--|
|  |
|  |
|  |
|  |



## **Cas B**

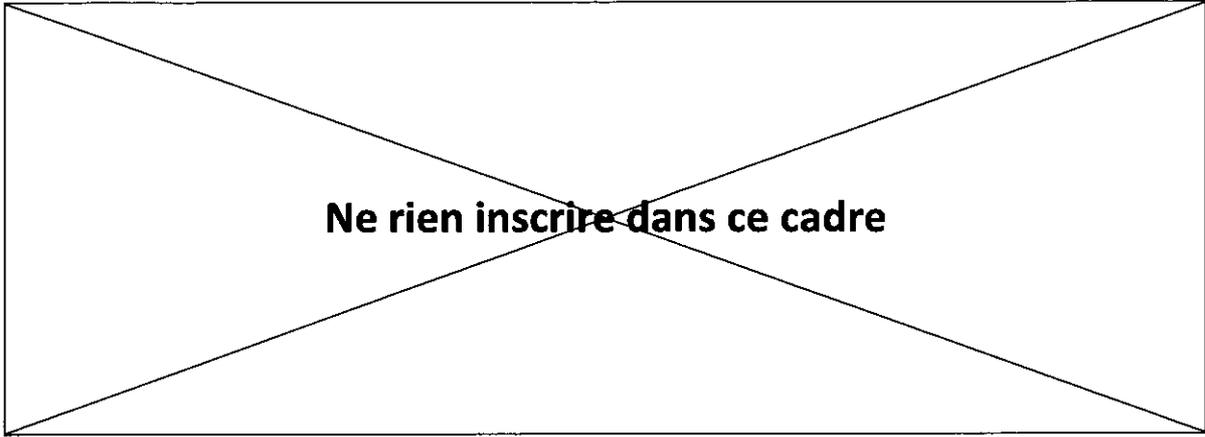
Vous devez conseiller le responsable de votre établissement dans l'achat d'un nouveau téléphone portable. Il vous indique vouloir consulter ses messageries professionnelle et personnelle, récupérer son répertoire téléphonique, s'en servir comme GPS pour ses déplacements, pouvoir lire tout type de fichiers pdf et de bureautique courante.

### **1. Comment le conseillez-vous ?**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

### **2. Pourquoi ?**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |



### **Cas C**

Au sein d'un service informatique, une de vos missions est la responsabilité du prêt ponctuel de matériels informatiques. Vous avez prêté une tablette numérique avec connexion wifi et 4G. L'utilisateur revient vers vous quelques jours après et vous informe s'être fait voler la tablette.

#### **1. Comment réagissez-vous ?**

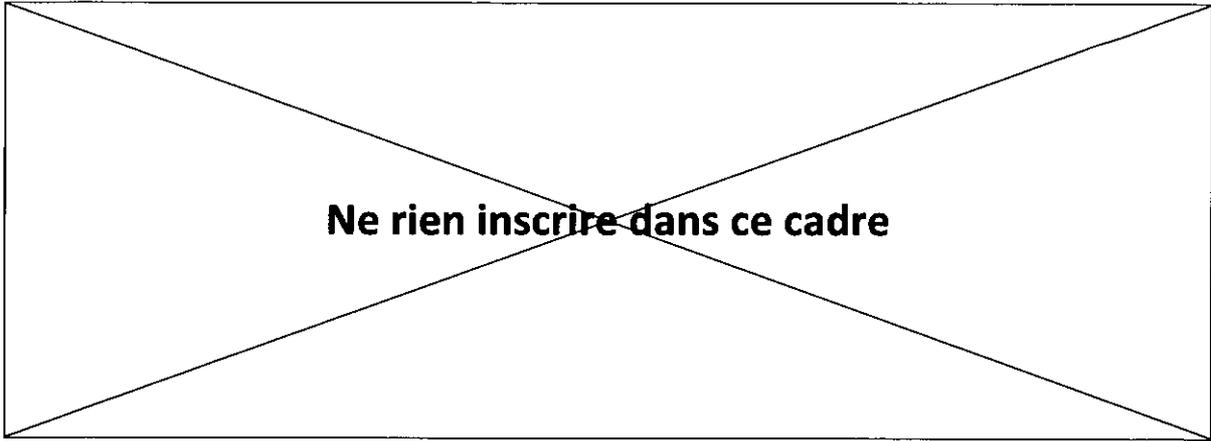
|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |

#### **2. Quelles actions réalisez-vous dans l'immédiat ?**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |

#### **3. Que lui demandez-vous ?**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |



### **Cas D**

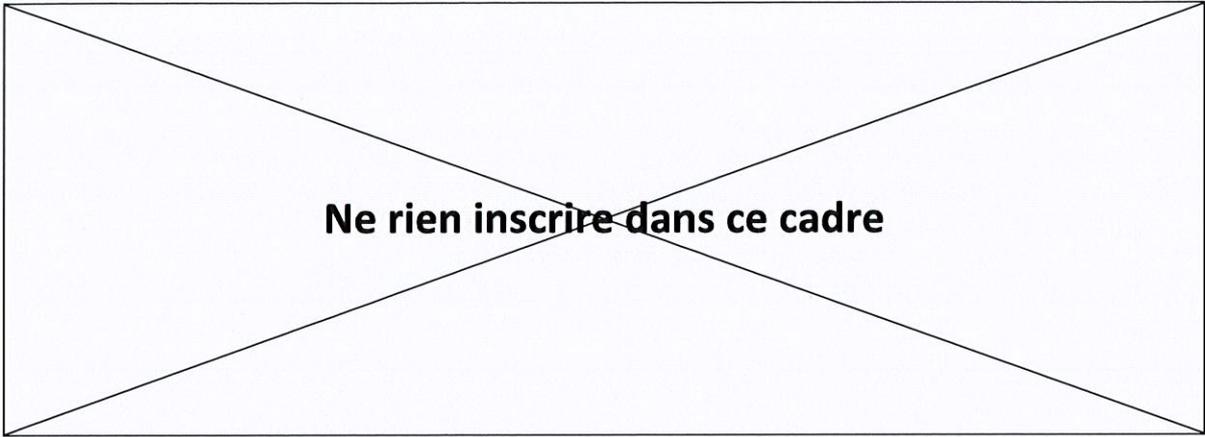
Vous êtes le responsable informatique d'une organisation. Les demandes informatiques sont de plus en plus nombreuses. Les usagers ont l'habitude de venir directement dans le service et de faire leurs demandes à l'oral. Vous commencez à ne plus vous en sortir. Le directeur de l'organisation vous demande de lui rendre compte sur l'activité du service.

#### **1. Qu'envisagez-vous ?**

|  |
|--|
|  |
|  |

#### **2. Décrivez la démarche en amont de l'installation proprement dite ?**

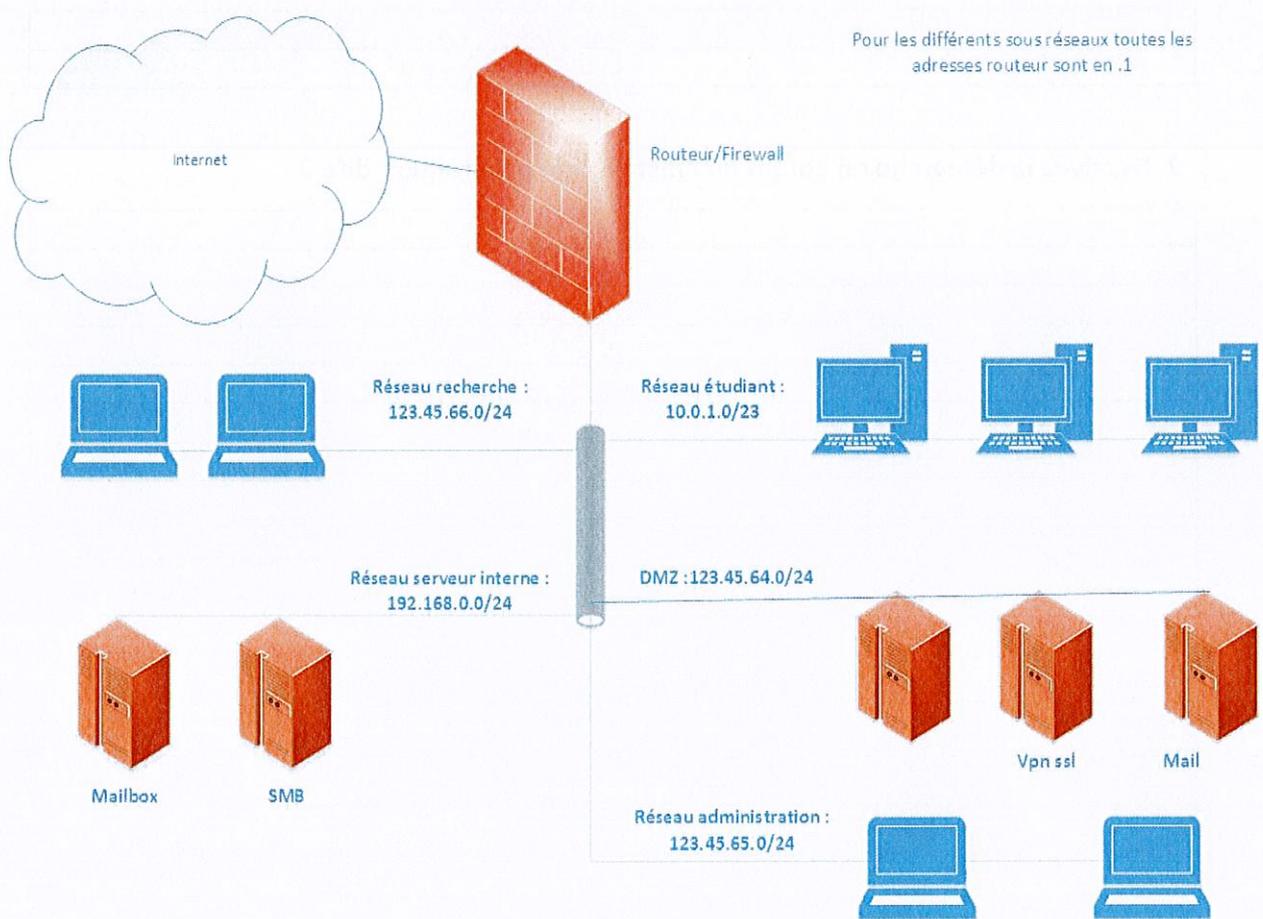
|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |



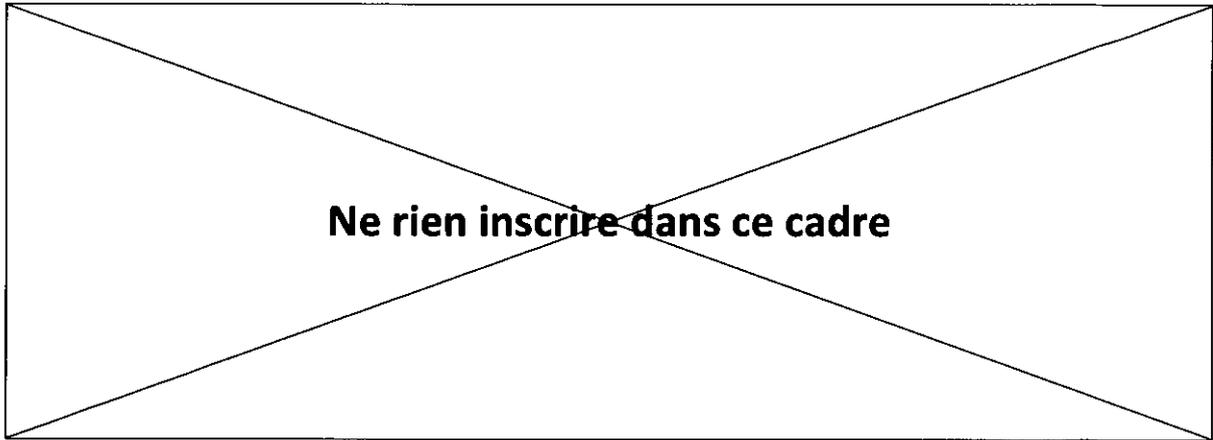
#### IV Questions système-réseau

Il sera tenu-compte dans la notation de l'orthographe et de la qualité de la rédaction.

Soit le réseau suivant d'une entité de l'enseignement supérieur :



Les postes étudiants sont sous Windows 7, les serveurs sont sous Linux.



**Partie 1 :**

**Q1 :**

Proposer une adresse IP pour le serveur web institutionnel de l'entité à mettre en place sur le réseau.

**Q2 :**

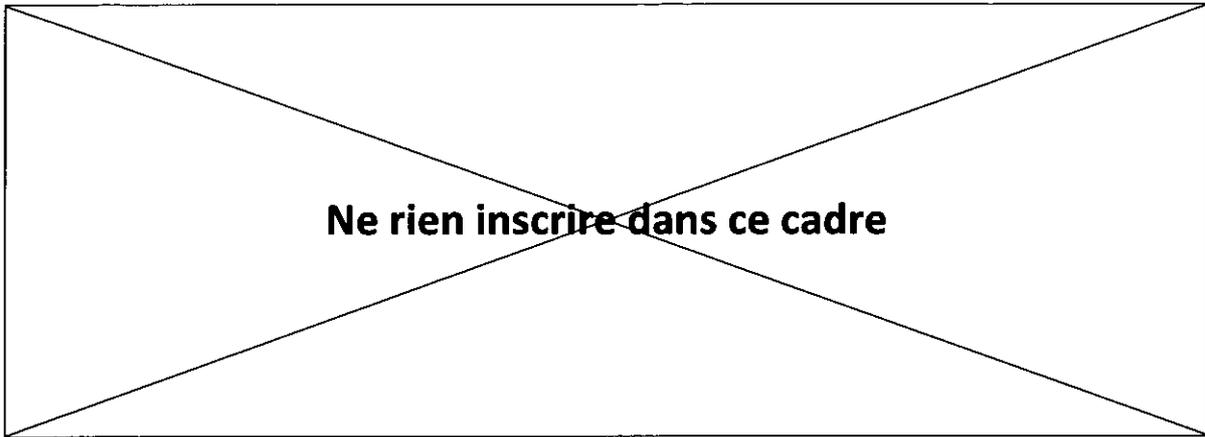
Proposer une adresse IP pour le serveur web intranet de l'entité à mettre en place sur le réseau.

**Q3 :**

Proposer une adresse IP pour le serveur DNS externe de l'entité à mettre en place sur le réseau.

**Q4 :**

Proposer une adresse IP pour un serveur resolver DNS interne de l'entité à mettre en place sur le réseau.



**Partie 2 :**

**L'entité possède à l'heure actuelle un pool d'adresses IP pour les étudiants en 10.0.1.0/23 (notation CIDR). 6 salles pédagogiques de 30 postes chacune sont déployées. Chaque salle ayant une capacité maximale de 32 places.**

**Q5 :**

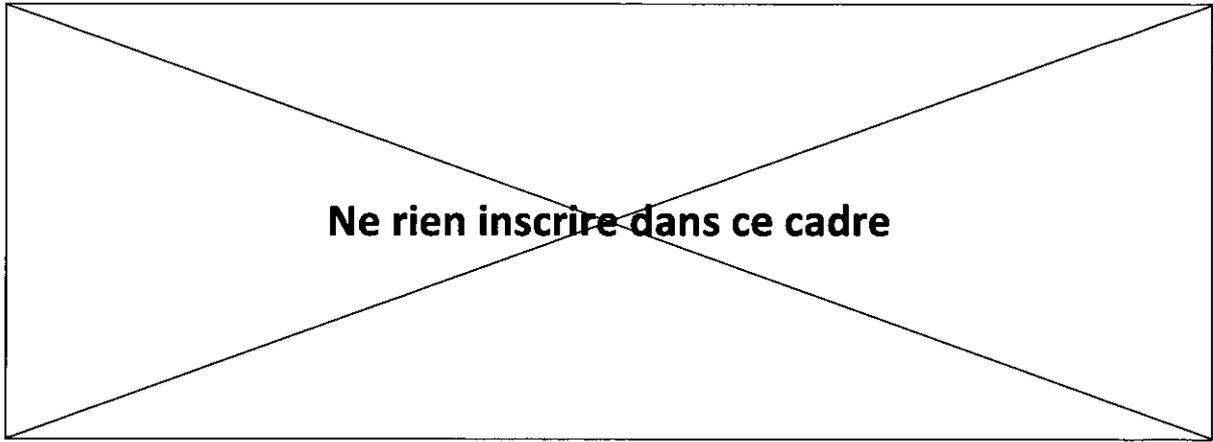
**En notation CIDR, proposer une taille de réseau minimale pour chaque salle**

**Q6 :**

**Combien de salles pédagogiques de 30 postes chacune pourrait-on encore déployer en sus des 6 existantes.**

**Q7 :**

**Proposer un nombre de postes optimal pour toutes les salles de façon à mettre en service le maximum de postes. Combien de salles pourraient ainsi être déployées ? Toutes les salles devront avoir le même nombre de postes.**



**Partie 3 :**

**Q8 :**

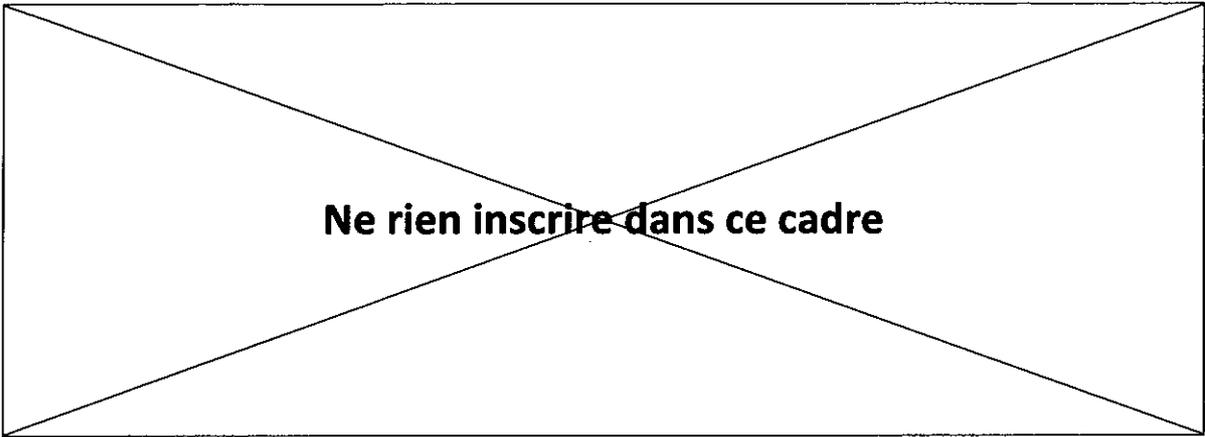
Quels ports en entrée devront être ouverts sur le Firewall/routeur pour laisser passer les services SMTP, HTTP, HTTPS, DNS en précisant le protocole.

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |

**Q9 :**

On veut sécuriser le service de messagerie SMTP, quel(s) port(s) et protocole(s) faudra-t-il ajouter ?

|  |
|--|
|  |
|  |
|  |



**Partie 4 :**

**Q10 :**

**Donner la commande affichant la table de routage d'un poste étudiant**

**Q11 :**

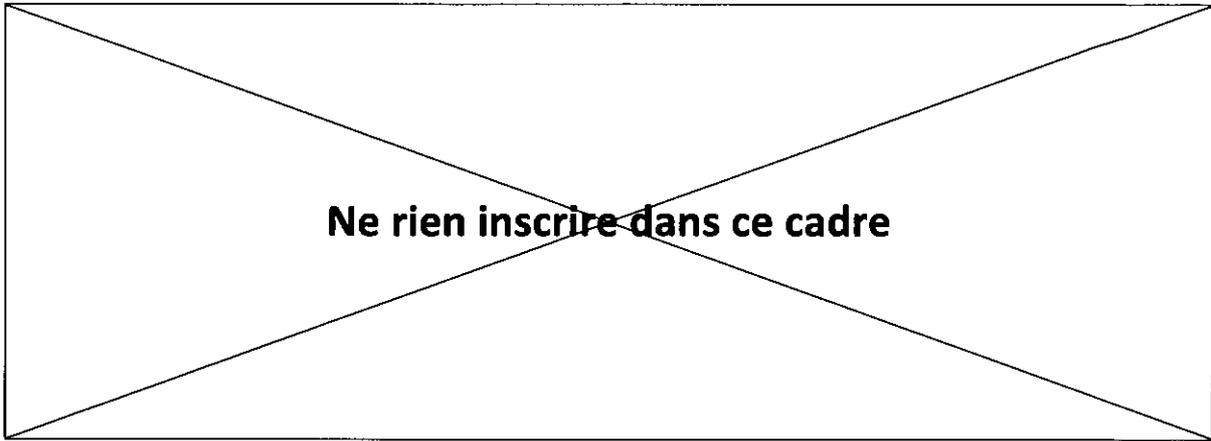
**Donner la commande affichant la configuration réseau d'un poste étudiant**

**Q12 :**

**Donner la commande affichant la table de routage d'un serveur interne**

**Q13 :**

**Donner la commande affichant la configuration réseau d'un serveur interne**



**Partie 5 :**

**Pour accueillir des postes visiteurs dans l'entité on se propose d'installer un portail captif en wifi.**

**Q14 :**

**Donner 3 exemples de protocole d'authentification qui pourraient alors être utilisés.**

|  |
|--|
|  |
|  |
|  |

**Q15 :**

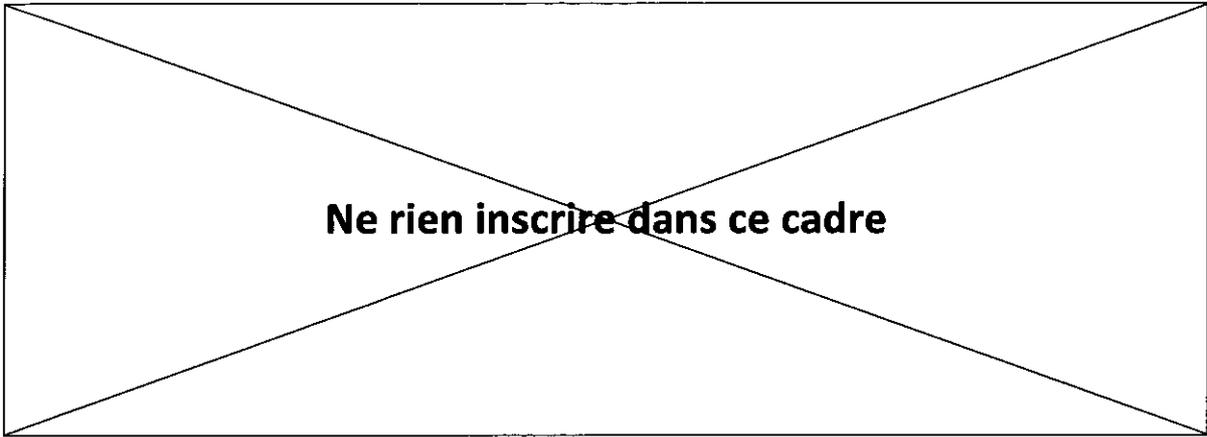
**Sur quel réseau doit-on positionner le portail captif ? Pourquoi ?**

|  |
|--|
|  |
|  |
|  |

**Q16 :**

**Quel serait le protocole wifi à utiliser pour communiquer en toute sécurité entre les bornes et les postes invités ?**

|  |
|--|
|  |
|--|



**Partie 6 :**

**Q17 :**

Citer au minimum 3 outils que l'on pourrait utiliser pour réaliser la sauvegarde des serveurs.

|  |
|--|
|  |
|  |
|  |

**Q18 :**

Citer au minimum 3 outils que l'on pourrait utiliser pour réaliser la sauvegarde des postes administration.

|  |
|--|
|  |
|  |
|  |

**Q19 :**

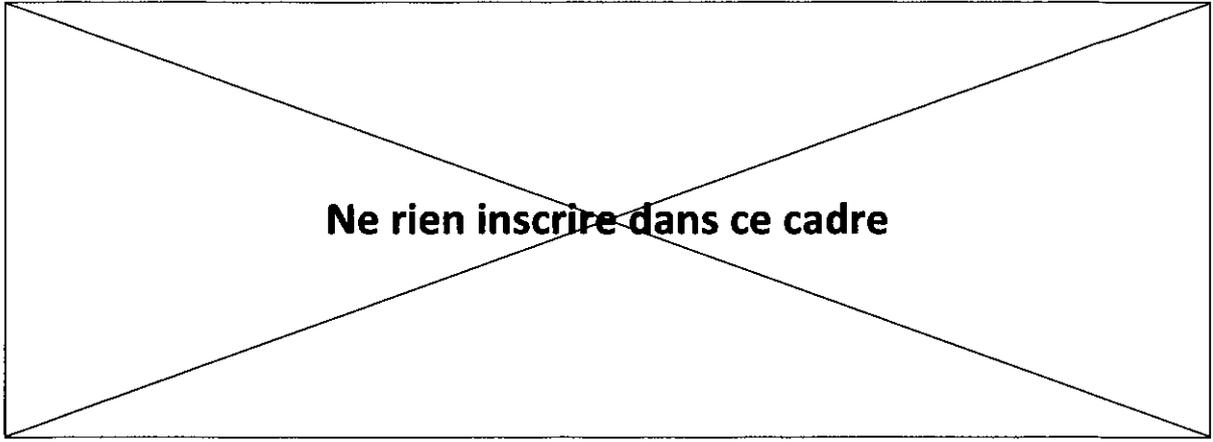
Que pourrait-on installer comme serveur en terme de fonctionnalités pour déployer les salles pédagogiques en automatique ?

|  |
|--|
|  |
|  |
|  |
|  |
|  |

**Q20 :**

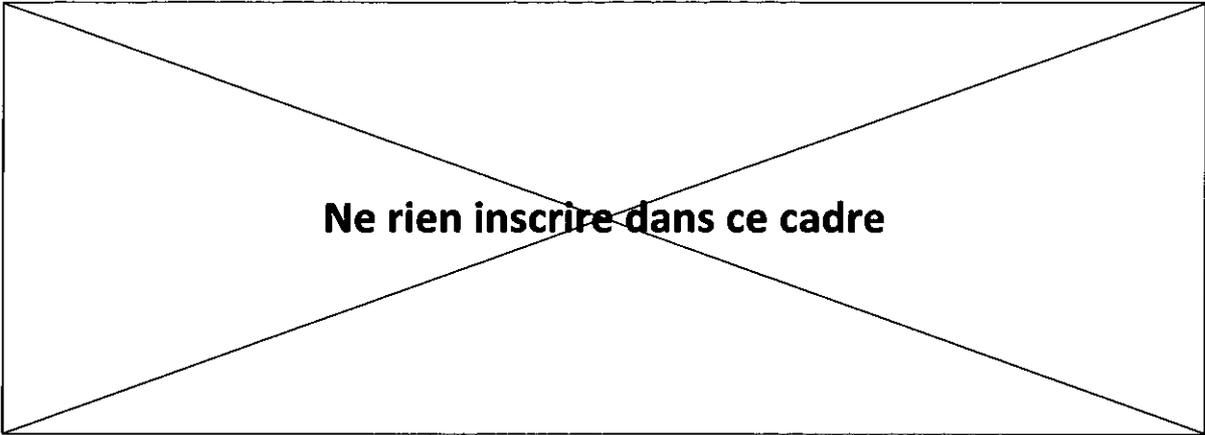
Quel type d'annuaire est le mieux adapté pour gérer les salles pédagogiques

|  |
|--|
|  |
|--|



Q21 :

Quel type d'annuaire est le mieux adapté pour les connexions aux serveurs



**Partie 7 :**

**On gère les adresses IP sur les différents réseaux par DHCP. Pour les postes administration on a besoin d'adresses IP fixes. Pour les postes étudiants on n'a aucune contrainte.**

Q22 :

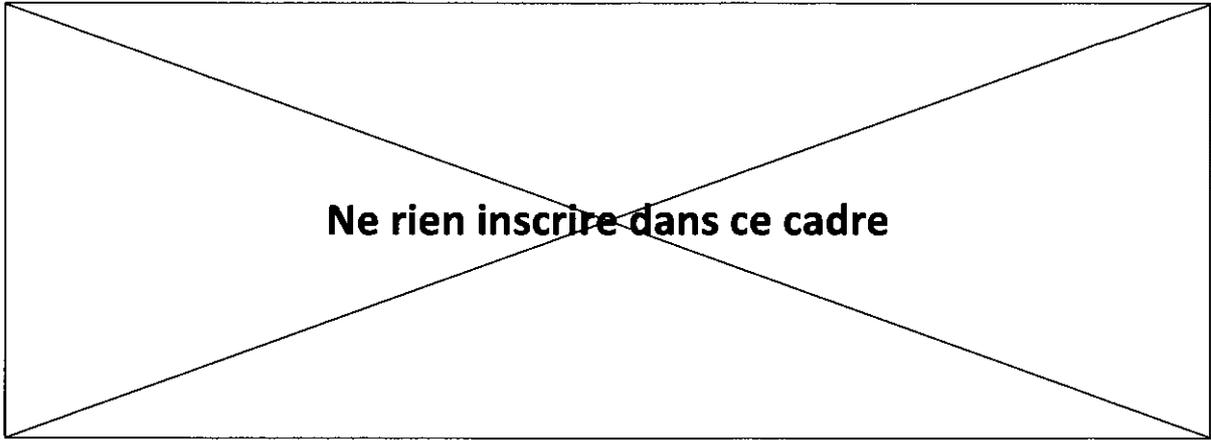
Quelle solution de DHCP mettre en œuvre sur le réseau administration ?

Q23 :

Quelle solution de DHCP mettre en œuvre sur le réseau étudiant ?

Q24 :

Quelle solution de DHCP mettre en œuvre sur le réseau recherche sachant qu'il a besoin d'adresses IP fixes uniquement pour certains postes ?



**Partie 8 :**

Q25 :

Quelle est la durée légale de conservation des journaux informatiques (logs) ?

|  |
|--|
|  |
|--|

Q26 :

Qui peut avoir accès aux journaux informatiques (logs) ?

|  |
|--|
|  |
|  |
|  |

Q27 :

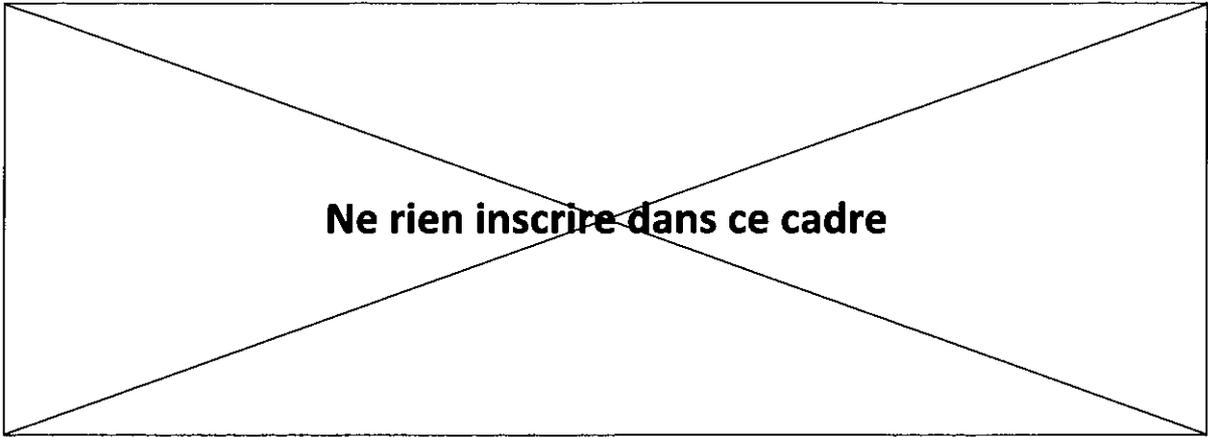
Vous recevez un appel téléphonique d'une personne s'annonçant comme un officier de police judiciaire et demandant l'accès immédiat à des informations personnelles d'un de vos utilisateurs. Que faites-vous ?

|  |
|--|
|  |
|  |
|  |

Q28 :

Quel est le lien entre le CIL et le RSSI ?

|  |
|--|
|  |
|  |
|  |



**Partie 9 :**

Q29 :

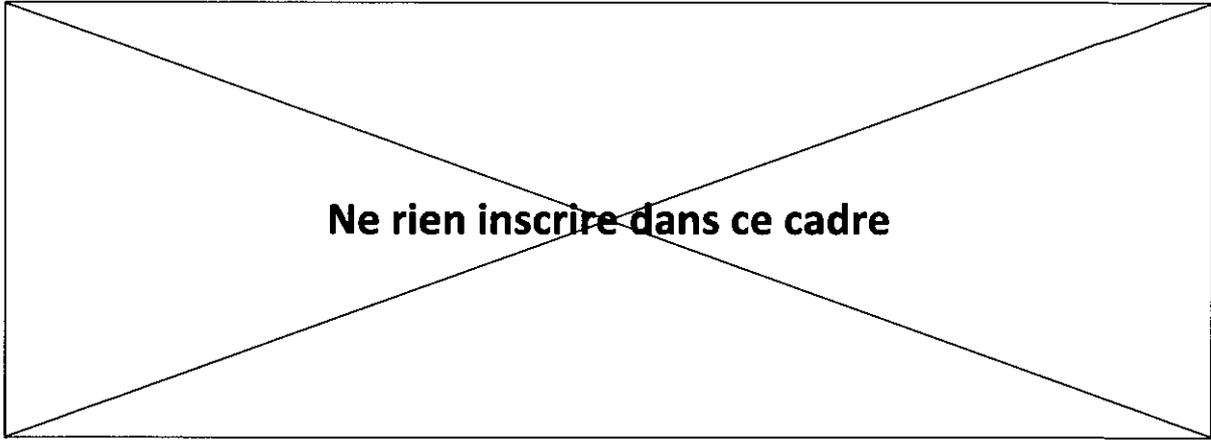
Quelles sont les principales informations nécessaires sur un poste pour réaliser l'inventaire du parc ? En citer minimum 8.

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

Q30 :

Dans l'entité, quel pourrait être l'intérêt de la virtualisation ? Expliquer brièvement pourquoi ? Citer au moins 3 intérêts.

|  |
|--|
|  |
|  |
|  |
|  |
|  |



**V Compréhension d'un texte en anglais avec questions en français, réponses attendues en français**

Le texte en anglais est fourni dans l'annexe 1.

**Question 1 :**

Quel est le type d'attaque qui a été utilisé lors de l'attaque récente du malware WannaCrypt ? Expliquer succinctement son mécanisme de propagation.

|  |
|--|
|  |
|  |
|  |
|  |

**Question 2 :**

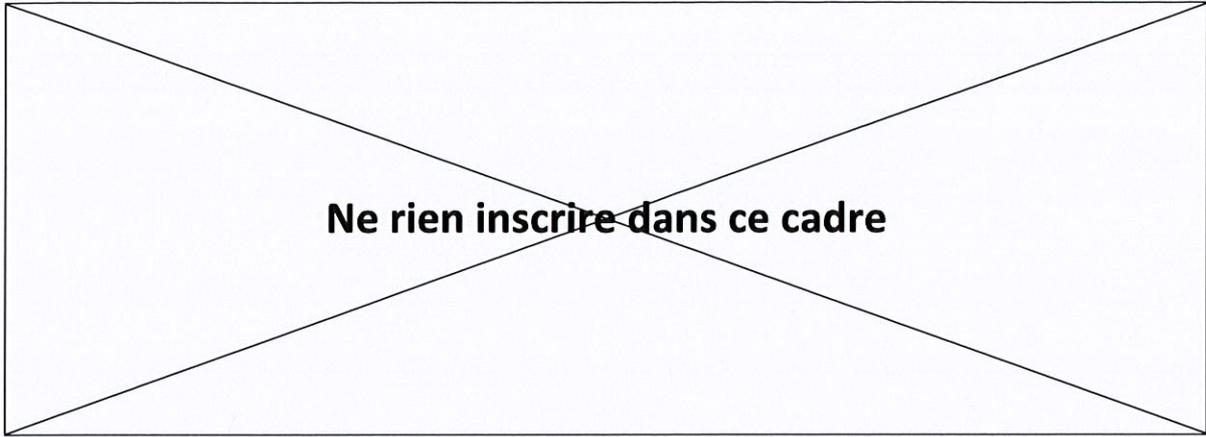
Quelles mesures d'urgence devaient être effectuées afin d'empêcher le virus de se propager ?

|  |
|--|
|  |
|  |
|  |
|  |

**Question 3 :**

Quelles sont les bonnes pratiques à mettre en œuvre afin d'éviter la propagation d'une telle attaque au sein d'un parc informatique ?

|  |
|--|
|  |
|  |
|  |
|  |



## Annexe 1 : texte en anglais

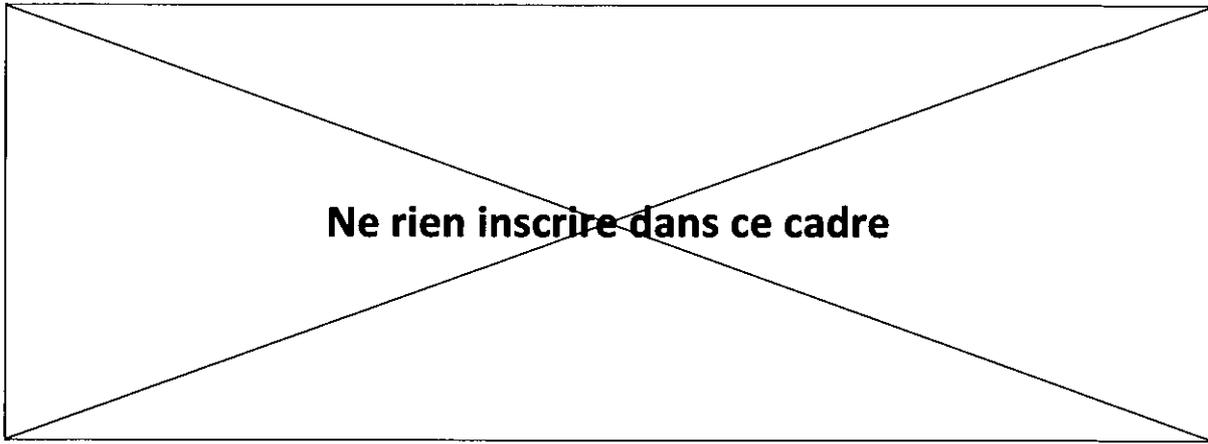
### Ransom: Win32/WannaCrypt

#### Attack vector

Ransomware threats do not typically spread rapidly. Threats like WannaCrypt (also known as WannaCry, WanaCrypt0r, WCRypt, or WCRY) usually leverage social engineering or email as primary attack vector, relying on users downloading and executing a malicious payload. However, in this unique case, the ransomware perpetrators used publicly available exploit code for the patched SMB "EternalBlue" vulnerability, [CVE-2017-0145](#), which can be triggered by sending a specially crafted packet to a targeted SMBv1 server. This vulnerability was fixed in security bulletin [MS17-010](#), which was released on March 14, 2017.

WannaCrypt's spreading mechanism is borrowed from [well-known public SMB exploits](#), which armed this regular ransomware with worm-like functionalities, creating an entry vector for machines still unpatched even after the fix had become available.

The exploit code used by WannaCrypt was designed to work only against unpatched Windows 7 and Windows Server 2008 (or earlier OS) systems, so Windows 10 PCs are not affected by this attack.



## Dropper

The threat arrives as a dropper Trojan that has the following two components:

1. A component that attempts to exploit the SMB CVE-2017-0145 vulnerability in other computers
2. The ransomware known as WannaCrypt

The dropper tries to connect the following domains using the API `InternetOpenUrlA()`:

- `www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`
- `www[.]jifferfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com`

If connection to the domains is successful, the dropper does not infect the system further with ransomware or try to exploit other systems to spread; it simply stops execution. However, if the connection fails, the threat proceeds to drop the ransomware and creates a service on the system.

In other words, unlike in most malware infections, **IT Administrators should NOT block these domains**. Note that the malware is not proxy-aware, so a local DNS record may be required. This does not need to point to the Internet, but can resolve to any accessible server which will accept connections on TCP 80.

## Spreading capability

The worm functionality attempts to infect unpatched Windows machines in the local network. At the same time, it also executes massive scanning on Internet IP addresses to find and infect other vulnerable computers. This activity results in large SMB traffic from the infected host, which can be observed by SecOps personnel, as shown below.

**Ne rien inscrire dans ce cadre**

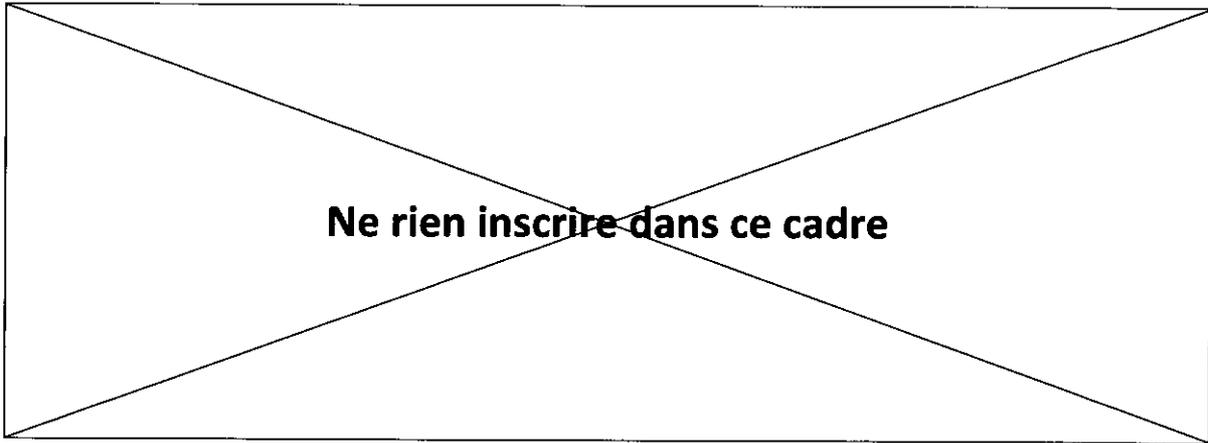
The screenshot displays a network traffic analysis tool interface. On the left, a list of IP addresses is shown, with several highlighted in red: .157.11, .157.12, and .157.13. On the right, a detailed view of a TCP connection is shown, with the destination IP address .157.11 and port 445 highlighted in red. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. The main window shows a table of captured packets with columns for No., Time, Source, Destination, and Protocol. The selected packet is a TCP connection to .157.11 on port 445. Below the table, the packet details are shown, including the source port (50041) and the destination port (445).

| No.    | Time       | Source | Destination | Protocol |
|--------|------------|--------|-------------|----------|
| 200618 | 217.566696 |        | .157.11     | TCP      |
| 202094 | 218.633911 |        | .157.12     | TCP      |
| 203140 | 219.441199 |        | .157.12     | TCP      |
| 203455 | 219.695544 |        | .157.13     | TCP      |
| 204356 | 220.488082 |        | .157.13     | TCP      |
| 204779 | 220.800093 |        | .157.14     | TCP      |
| 206453 | 221.883475 |        | .157.15     | TCP      |

Frame 199031: 66 bytes on wire (528 bits), 66 bytes captured (528 b  
 Ethernet II, Src: [redacted], Dst: All-t  
 Internet Protocol Version 4, Src: [redacted] Dst: [redacted] 157.10  
 Transmission Control Protocol, Src Port: 50041, Dst Port: 445, Seq:  
 Source Port: 50041  
 Destination Port: 445

The Internet scanning routine randomly generates octets to form the IPv4 address. The malware then targets that IP to attempt to exploit CVE-2017-0145. The threat avoids infecting the IPv4 address if the randomly generated value for first octet is 127 or if the value is equal to or greater than 224, in order to skip local loopback interfaces. Once a vulnerable machine is found and infected, it becomes the next hop to infect other machines. The vicious infection cycle continues as the scanning routing discovers unpatched computers.

When it successfully infects a vulnerable computer, the malware runs kernel-level shellcode that seems to have been copied from the public backdoor known as DOUBLEPULSAR, but with certain adjustments to drop and execute the ransomware dropper payload, both for x86 and x64 systems.



## Protection against the WannaCrypt attack

To get the latest protection from Microsoft, upgrade to Windows 10. Keeping your computers up-to-date gives you the benefits of the latest features and proactive mitigations built into the latest versions of Windows.

We recommend customers that have not yet installed the security update MS17-010 do so as soon as possible. Until you can apply the patch, we also recommend two possible workarounds to reduce the attack surface:

- Disable SMBv1 with the steps documented at Microsoft Knowledge Base Article 2696547 and as recommended previously
- Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445

Windows Defender Antivirus detects this threat as Ransom:Win32/WannaCrypt as of the 1.243.297.0 update. Windows Defender Antivirus uses cloud-based protection, helping to protect you from the latest threats.

For enterprises, use Device Guard to lock down devices and provide kernel-level virtualization-based security, allowing only trusted applications to run, effectively preventing malware from running.

Monitor networks with Windows Defender Advanced Threat Protection, which alerts security operations teams about suspicious activities. Download this playbook to see how you can leverage Windows Defender ATP to detect, investigate, and mitigate ransomware in networks: Windows Defender Advanced Threat Protection – Ransomware response playbook.

