MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

ANNALES DU CONCOURS

Accès au corps des attachés de la DGSE

Épreuve d'admissibilité :
spécialité sciences et technologie - informatique

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Session 2023

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

3ème épreuve d'admissibilité

Spécialité : sciences et technologie - informatique

Épreuve consistant à répondre à une série de questions portant sur la spécialité « Sciences et technologie - Informatique ».
Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Durée : 4 heures - coefficient 8

CONCOURS EXTERNE
POUR L'ACCÈS AU CORPS DES ATTACHÉS

SESSION 2023

<u>Epreuve d'admissibilité</u> :

Spécialité : Sciences et technologie - Informatique

Épreuve consistant à répondre à une série de questions portant sur la spécialité « Sciences et technologie - Informatique ». Il est demandé au candidat de démontrer les étapes de son raisonnement en exploitant les documents du dossier comprenant dix pages maximum et en faisant appel à ses connaissances personnelles.

Durée : 4 heures ; coefficient 8

Le questionnaire comporte des questions à choix multiples dont les réponses devront être traitées sur la copie, en aucun cas sur le sujet.

<u>Nota</u> : aucun document n'est fourni en appui de ces questions

<u>Barème</u> :

- Les questions sont notées sur un total de 80 points. La note finale sera ensuite ramenée sur 20 points.

- Questions à Choix Multiples :
  - Bonne réponse : +1 pt
  - Absence de réponse : 0 pt
  - Mauvaise réponse : -0,5 pt

<u>Nota</u> : la syntaxe, l'orthographe et la structuration des réponses seront prises en compte dans l'évaluation.

Partie I : QCM sur les connaissances techniques (20 points)

Il y a pour chaque question **au moins une bonne réponse**.

1) La représentation du nombre qui suit le nombre 4 en base 5 est :
a / 10
b / 5
c / 0
d / A

2) Combien de bits y a-t-il dans un mébioctet ?
a / 1 000 000
b / 1 048 576
c / 8 000 000
d / 8 388 608

3) 15 personnes désirent communiquer de façon confidentielle (chacune avec chaque autre) en utilisant un algorithme de chiffrement symétrique. De combien de clefs privées auront-elles besoin ?
a / 105
b / 60
c / 15
d / 30

4) Pour séparer un disque dur physique en deux disques logiques, il faut :
a / le formater
b / le partitionner
c / mettre en place un RAID
d / créer un nouveau dossier racine

5) Quel(s) type(s) de mémoire(s) n'existe(nt) pas :
a / RAM
b / ROM
c / LUKS
d / SDMMC

6) Comment s'appelle la zone minimale que peut occuper un fichier sur le disque ?
a / le secteur
b / la FAT
c / le cluster
d / le block

7) Quelle est l'entropie d'un code constitué de 4 chiffres ?
a / 11 bits
b / 13 bits
c / 15 bits
d / 17 bits

8) Le chiffrement des données avec une clef privée sert à assurer :
a / la non-répudiation
b / l'intégrité
c / la confidentialité
d / l'authentification

9) Soit (n, e) = (33, 3) une clef publique RSA. Quel sera le résultat de chiffrement du message M= 4 ?
a / 44
b / 97
c / 40
d / 31

10) Comment utilise-t-on les clefs symétriques et asymétriques ensemble ?
a / on utilise la clef asymétrique pour chiffrer la clef symétrique.
b / on utilise la clef symétrique pour amorcer le chiffrement, puis on chiffre l'essentiel du message par la clef asymétrique.
c / le message est chiffré d'abord par la clef symétrique, puis par la clef asymétrique.
d / le message est chiffré d'abord par la clef asymétrique, puis par la clef symétrique.

11) Quelle(s) étape(s) ne fait(font) pas partie(s) du processus de compilation ?
a / l'analyse lexicale
b / l'analyse syntaxique
c / l'analyse sémantique
d / l'analyse terminologique

12) Un serveur DHCP permet :
a / de télécharger des fichiers
b / de contrôler les connexions à internet depuis un réseau local
c / de fournir à un ordinateur l'adresse IP d'un site web
d / d'attribuer une adresse IP à un ordinateur

13) Parmi les services suivants, le(s)quel(s) doi(ven)t être désactivé(s) pour empêcher les pirates informatiques d'utiliser un serveur Web comme un relais de messagerie ?
a / SMTP
b / POP3
c / SNMP
d / IMAP

14) Quelle(s) méthode(s) permet(tent) de récupérer un mot de passe à l'insu de son propriétaire ?
a / phishing
b / key-logger
c / buffer-overflow
d / DoS

15) Quel(s) outil(s) permet(tent) d'identifier une attaque informatique ?
a / l'anti-virus
b / le linker
c / la liste des processus actifs
d / les logs système

16) Parmi les fichiers suivants dont la source n'est pas sûre, le(s)quel(s) pourrai(en)t présenter un risque pour un ordinateur ?
a / rapport.txt
b / rapport.jpg
c / rapport.doc
d / rapport.zip

17) Parmi les langages suivants, indiquez le(s) langage(s) fonctionnel(s) :
a / Lisp
b / C
c / Rust
d / Ada

18) Parmi les services suivants, indiquez celui (ceux) fourni(s) par l'ip 8.8.8.8 :
a / IPTV
b / HTTP
c / DNS
d / ARP

19) Combien y a-t-il d'adresse IPv4 disponibles dans le réseau 192.168.0.0/22 ?
a / 256
b / 254
c / 1024
d / 1022

20) Quelle(s) commande(s) permet(tent) de lister des dossiers/fichiers :
a / grep
b / dir
c / cat
d / ls

Partie II : bonnes pratiques (10 points)

Question 1 (1 point) :

Qu'est-ce que « git » ? A quoi sert cet outil ?

Question 2 (1 point) :

Expliquez ce que font les commandes suivantes :

- git add .
- git commit -m « … »
- git push
- git rebase origin/master

Question 3 (1 point) :

Qu'est-ce que le TDD ? Peut-on le mettre en place dans n'importe quel projet ?

Question 4 (3 points) :

Qu'est-ce que le CI/CD ? A quoi cela sert ? Y a-t-il des limites à sa mise en place ?

Question 5 (1 point) :

Qu'est-ce qu'un PRA ? Quelles informations doit-il contenir ?

Question 6 (3 points) :

Dans le cadre d'un projet informatique, quels sont les différents niveaux de documentation qui doivent être mis en place ?

Partie III : algorithmique (15 points)

Exercice 1 (10 points) :

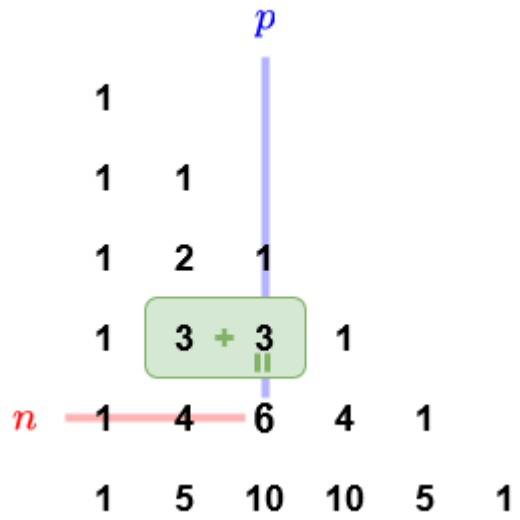
Ecrivez, en langage naturel, un algorithme qui permet de retourner la somme des N premiers nombres premiers.

Entrée du programme : N, un nombre entier.

Sortie du programme : S, un nombre entier.

Exercice 2 (5 points) :

Le triangle de Pascal est une présentation des coefficients binomiaux sous la forme d'un triangle :



Source : Wikipédia

Ecrivez, en langage naturel, un algorithme qui permet de retourner la valeur de C(n,p) où $0 \leq p \leq n$.

Entrée du programme : n et p, deux nombres entiers tel que $0 \leq p \leq n$.

Sortie du programme : S, un nombre entier.

Partie IV : étude de cas (35 points)

Votre ami M. Trouvetou a eu une idée de *start-up* révolutionnaire, mais n'ayant pas de compétences particulières en informatique, il a tout de suite pensé à vous pour l'aider à concrétiser son idée : **un système de détection d'intrusion décentralisé sur la blockchain !**

Les composantes de sa solution sont les suivantes :

- un logiciel gratuit et open-source, qui contiendra les mécanismes de détection d'intrusion et qui sera téléchargé puis installé par les clients. Ce logiciel collecte des données (journalisation système, sondes réseaux, …) et utilise les mises à jour disponibles sur la blockchain (voir points suivants) ;
- une intelligence artificielle pour générer des motifs d'intrusion à partir des données collectées ;
- un système pour publier sur la blockchain les nouveaux motifs trouvés.

A cette solution, en apparence gratuite, il entend bien générer du revenu en vendant à ses utilisateurs des mises à jour AVANT que celles-ci n'aient été publiées sur la blockchain.

Il a donc également besoin :

- d'un moyen d'identifier les utilisateurs payants ;
- d'un site pour promouvoir et vendre sa solution ;
- d'un système de courriels pour l'aspect marketing et pour l'aspect support.

Bien que M. Trouvetou dispose de fonds illimités et soit prêt à vous donner carte-blanche pour réaliser son idée, **il souhaite que vous lui proposiez une solution comportant *a minima* les éléments suivants** :

- les ressources informatiques et les outils logiciels nécessaires au projet ;
- un schéma présentant la solution dans son ensemble ;
- les personnes et leurs spécialités qui seront nécessaires (uniquement pour la partie informatique) ;
- la méthode de gestion de projet que vous souhaitez mettre en place ;
- les améliorations qui pourraient être apportées au projet, si vous en voyez ;
- les points qui pourraient faire échouer le projet.

N'oubliez pas que M. Trouvetou n'a pas de connaissances très approfondies en informatique.

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Copie ayant obtenu la meilleure note

Spécialité : sciences et technologie - informatique

L'administration n'a volontairement pas corrigé les imperfections de fond et de forme dans la copie communiquée ci-après.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

© EXATECH

Année : 2023

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Sciences et technologie informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

Partie I : QCM

1) a/10

2)

3) a/ 105

4) b/ le partitionner

5) c/ LUKS

6)

7)

8) c/ La confidentialité

9) d/ 31

10) a/ On utilise la clef asymétrique pour chiffrer la clef symétrique.

11) a/ L'analyse lexicale.
d/ l'analyse terminologique

12) d/ d'attribuer une adresse IP à un ordinateur

13) a/ SMTP
b/ POP3
d/ IMAP

14) a/ phishing
b/ key-logger

15) a/ l'anti-virus
c/ la liste des processus actifs
d/ les logs système

16) a/ rapport.txt
b/ rapport.jpg
c/ rapport.doc
d/ rapport.zip

17) c/ Rust

18) c/ DNS

19) d/ 1022

20) b/ dir
d/ ls

2. 1/16.

Partie III : algorithmique

Exercice 1

```
N ← variable d'entrée
M ← N^2 + 1                    //on est sûrs d'avoir au moins
                               //N premiers dans [[0, M]]
On définit tableau = [1, ..., M]      //tableau des
                                      //entiers de 1 à M
          premiers = [ ]              // tableau des
                                      //nombres premiers de
                                      //1 à M
          composés = [ ]              // tableau des composés
                                      // de 1 à M
//On réalise un crible d'Eratosthène entre 1 et M

Pour i allant de 1 à M-1 :
    Si tableau[i] n'est pas dans composés:
        on ajoute tableau[i] dans premiers
        j ← 2
        Tant que j × tableau[i] ≤ M
            on ajoute j × tableau[i] à composés
            j ← j + 1

// à ce stade, le tableau premiers contient tous les
nombres premiers compris entre 1 et M

// On fait la somme des N premiers éléments du
tableau premiers

S ← 0
Pour i allant de 0 à N-1 :
    S ← S + premiers[i]

// On retourne le résultat stocké dans S
Retourner S
```

Exercice 2

// On s'appuie sur la formule suivante :

// $\forall\ 0 \leq p \leq n$,
$$\begin{cases} C(n-1, p-1) + C(n-1, p) = C(n, p) & \text{si } p \geqslant 1 \\ C(n, p) = 1 & \text{sinon.} \end{cases}$$

// On définit la fonction récursive suivante

```
fonction Binomiale (n, p) :
    Si n < p :
        Retourner code_erreur
    Si p = 0 :
        Retourner 1
    Sinon :
        Retourner Binomiale (n-1, p-1)
                + Binomiale (n-1, p)
```

// On conclut

```
n, p ← variables d'entrée
S = Binomiale (n, p)
Retourner S
```

© EXATECH

Année : 2023

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Sciences et technologie informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

Partie IV : Étude de Cas

PROJET DE DÉVELOPPEMENT INFORMATIQUE START-UP DE M. TROUVETOUT

Date : XX/XX/2023
Dossier suivi par : XXX
À l'attention de M. Trouvetout, directeur.

Plan du document

I. Présentation générale du projet

II. Architecture informatique

III. Ressources humaines

IV. Chronologie de déploiement

V. Points d'attention

VI. Conclusion

I. Présentation générale du projet

Dans le cadre du développement de l'entreprise de M. Trouvetout, directeur, la société XXX a été sollicitée pour échaffauder un plan de déploiement de son activité. C'est l'objet du présent document de dessiner les contours d'une future architecture informatique et humaine pour assurer la concrétisation du projet de M. Trouvetout.

I.1) Rappel des Enjeux

M. Trouvetout développe un logiciel de détection d'intrusion ~~HIDS~~ qu'il entend distribuer de manière gratuite et open-source. ~~Comme tout HIDS~~ Ce logiciel s'appuie sur les sondes hôtes (HIDS), telles que les journaux de logs, et les sondes réseaux (NIDS) déjà présentes chez le client afin de collecter, d'analyser, et de visualiser les éventuelles remontés d'incidents. Le service proposé s'apparente donc à un SIEM (Security Incident & Event Manager).

Les apports de la solution de M. Trouvetout par rapport aux logiciels déjà présents en ligne sont :

- L'utilisation de méthodes d'intelligence artificielle, en particulier d'apprentissage (machine learning), visant à perfectionner la détection d'anomalies, en réduisant le nombre de faux positifs et de faux négatifs remontés
- L'utilisation de la blockchain afin de chaîner les mises à jours régulières du logiciel, sans risque d'atteinte à l'intégrité des nouveaux motifs trouvés
- La décentralisation du traitement des données générées par le client, permettant :
  - des économies de personnels, de logiciel et d'infrastructure pour le client
  - une mise en commun des jeux de données des clients (après anonymisation)

..6.1.1.6.

afin de perfectionner l'entraînement et la performance de l'algorithme de machine learning.

I.2) Gestion de projet

Le projet informatique se déroulera, d'un point de vue stratégique, conformément à la méthode Plan-Do-Check-Act préconisé par la norme ISO 27001. En d'autres termes, le suivi en maîtrise d'ouvrage sera cyclique pour s'assurer à chaque jalons de la pertinence et de la performance des travaux réalisés.

En matière de maîtrise d'oeuvre, c'est la méthode "SCRUM" qui sera employée. À intervalles réguliers, des "Sprints" (accélérations) seront réaliser pour livrer des preuves de concept à M. Trouvetout, afin de s'assurer que les avancées sont conformes à ses attentes.

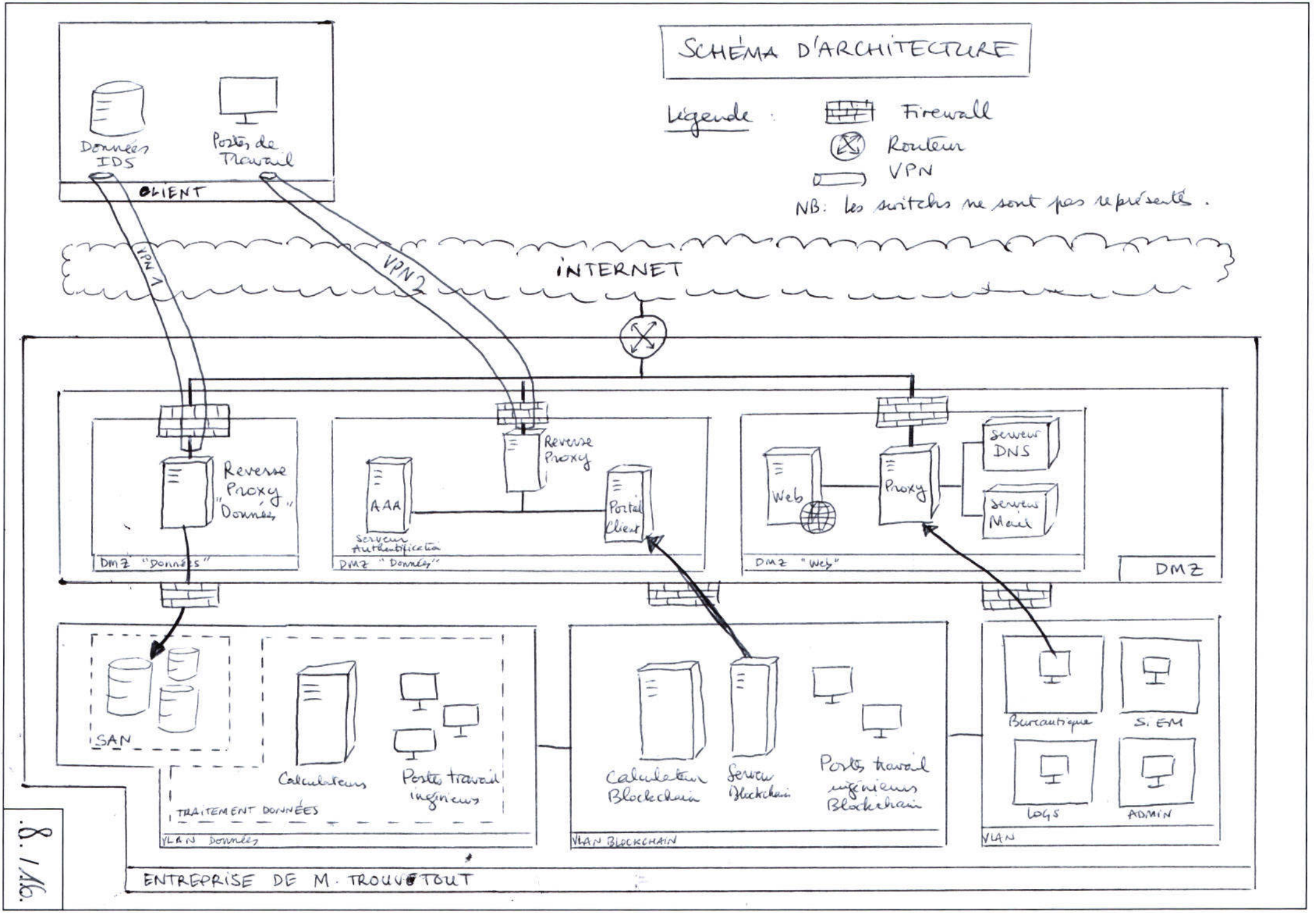
II. Architecture informatique

Le Schéma d'architecture proposé doit être en conformité avec :

- les recommandations d'un futur audit de sécurité selon la méthode EBIOS RM (voir section V)
- les prescriptions de la norme iso 27001 précédemment citée
- les recommandations de l'ANSSI, en premier lieu le guide d'hygiène.

Suivant ces principes directeurs, le schéma suivant est proposé à M. Trouvetout :

SCHÉMA D'ARCHITECTURE



8 / 16

© EXATECH

Année : 2023

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Sciences et technologie informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

II.1) Matériel informatique

Afin de réaliser le schéma proposé, un certain nombre de matériels informatiques devront être achetés :

- routeur

  Point d'entrée dans le réseau de l'entreprise de M. Trouvetout. On privilégiera ceux de la marque Cisco.

- switchs

  Afin de segmenter le réseau de l'entreprise en différents VLAN (Virtual local Area Network) pour limiter les risques de latéralisation au sein du réseau local, des switchs de la marque Cisco sont recommandés.

- Postes de travail

  PC de marque américaine de préférence, sur un OS à jour (Windows ou Linux). On proscrira le principe du "BYOD" (Bring your own device" – "Venez avec votre matériel") par mesure de sécurité.

  On configurera les ordinateurs selon trois principes

  - minimisation : ne laisser que les applications ou services nécessaires à la tâche de l'employé utilisateur (par exemple

fermeture des ports USB)

- Moindre privilège : ne permettre un accès Admin ou root que sur la machine administrateur
- Défense en profondeur : s'assurer que chaque utilisateur s'authentifie à chaque fois qu'il cherche à se connecter à un service de l'entreprise (principe du Zero Trust).

- Firewalls ("coupe-feu")

Les Firewalls sont des matériels indispensables à la sécurisation du réseau interne de l'entreprise. Ils opèrent comme des filtres du trafic réseau afin de ne laisser transiter que les paquets légitimes.
Suivant les recommandations de l'ANSSI, 2 firewalls physiquement distincts devront être placés à l'entrée et à la sortie de chaque zone de la DMZ (zone démilitarisée). En cas de restriction budgétaire, on pourra utiliser les différents ports d'un même firewall pour segmenter le réseau, au détriment néanmoins de la sécurité de celui-ci.

On pourra utiliser le logiciel open-source pfSense en phase avec la philosophie de "logiciels libres" développée par l'entreprise de M. Trouvetout.

- Serveur Web

On pourra utiliser un serveur Apache ou Nginx

- Serveur d'Authentification (AAA : Authentification, Authorization and accounting).

On utilisera le protocole d'authentification RADIUS sur EAP, suivant ~~le protocole d'authentification~~ la norme 802.1X

II.2) VPN

Afin de sécuriser les accès distants entre chaque client et l'entreprise de M. Trouvetout, des VPN (Virtual Private Network), permettant de proposer les services d'un réseau privé en transitant sur un réseau public non maîtrisé, seront utilisés. On privilégiera le tunneling par IPSec, conformément aux recommandations de l'ANSSI.

III. Ressources humaines

III.1) Phase 1 : Lancement

Dans la première phase de lancement de l'entreprise, M Trouvetout aura besoin de recruter :

Système :
- 1 architecte système, pour mettre en application et configurer le schéma d'architecture proposé
- 1 administrateur système, pour maintenir le système en état de fonctionnement, contrôler le réseau, ouvrir les sessions des utilisateurs

Virtuel :
- 1 développeur web pour développer et mettre en ligne le site internet.

Proof of concept :
- 2 software engineer pour développer le logiciel distribué par l'entreprise.

Démarchage :
- 1 commercial pour démarcher de potentiels clients

III.2) Production

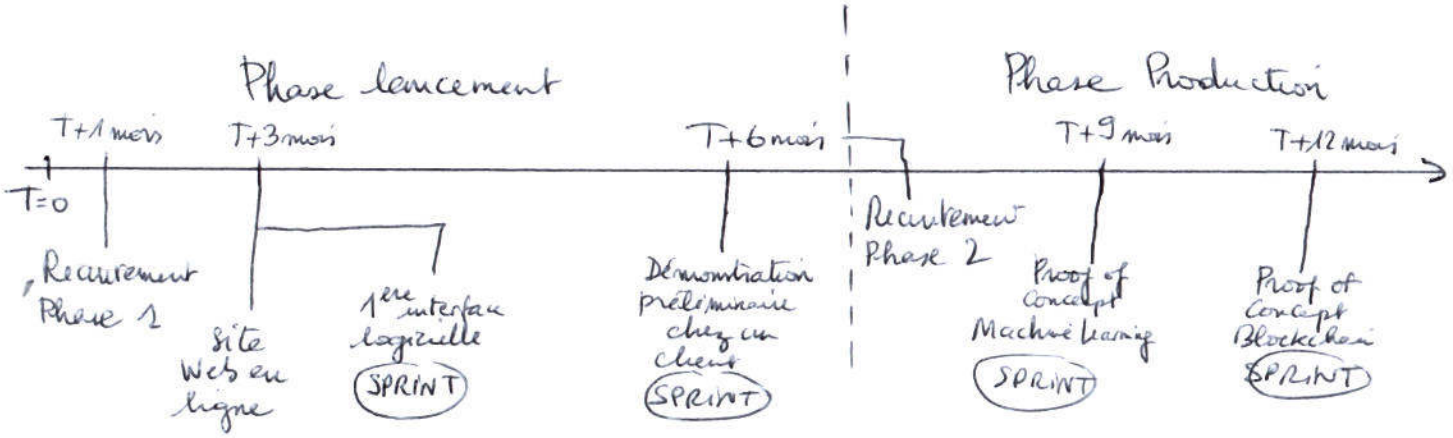
Une fois la première phase terminée, il s'agira de renforcer drastiquement le "back-office" pour améliorer la solution. Le recrutement comprendra :

- 2 ingénieurs blockchain, pour implémenter l'algorithme de chaînage par blocs.
- 3 ingénieurs Machine Learning, employés à entraîner l'algorithme d'apprentissage sur les jeux de données clients

L'architecte système, indispensable lors de la phase 1, n'a plus son utilité. On privilégiera ici un contrat court ou une prestation de conseil sur 6 mois.

Par ailleurs, le développement et la maintenance du site Web peut être assuré par un prestataire plutôt qu'un employé de l'entreprise.

IV. Chronologie du déploiement.



V. Points d'attention

V.1) Gouvernance

Il est conseillé à M. Trouvetout de rédiger rapidement un Plan de Sécurité des Systèmes d'Information (PSSI) afin de préciser, au niveau stratégique, la vision de la Direction en matière de SSI. Ce document permettra de mettre au diapason l'ensemble des employés sur ces problématiques.

© EXATECH

Année : 2023

Concours : Concours externe pour l'accès au corps des attachés

Épreuve : Sciences et Technologies de l'informatique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

V.2) Données

La solution envisagée base de données hétérogène de clients différents. Si ces données ne semblent pas être soumises au RGPD (données non sensible), un réel effort d'anonymisation devra être pratiqué pour ne pas dévoiler des informations à caractère privé.

V.3) Cloud

La mise en place d'un SAN (Storage Area Network) a un coût (serveurs, Base de données) en matériel, logiciel en en RH. On pourra envisager une solution Cloud, comme AWS, pour stocker "dans le nuage" les données reçues de clients Ce service présente des promesses de disponibilité compatible avec l'utilisation de l'entreprise.

VI. Conclusion

Le présent document est une base de travail pour le projet informatique mandaté par M. Trouvetout. En fonction des retours, il pourra être amendé, et d'autres solutions pourront être envisagées (recours systématique au Cloud, nomadisme, ...)

Partie II : Bonnes pratiques

Question 1

« git » est une application de développement de code en commun. Cet outil permet à un ensemble de développeurs de travailler sur le même code, en gérant les problématiques de dépôt, de conflits, de codes concurrents etc.... On peut l'utiliser au travers de la plateforme web gitlab.

Question 2 :

- git add. : ajouter une ~~dépôt~~ branche à la racine.
- git commit -m « ... » : enregistrer ~~dans le dépôt git~~ en local le morceau de code « ... »
- git push : pousser vers le dépôt les modifications déjà "committées".
- git rebase origin/master : se placer sur une autre branche du dépot git

Question 3

Question 4

Question 5

Un PRA est un plan de reprise d'activité. Souvent annexé au PCA (plan de continuation d'activité), il comprend l'ensemble des actions à conduire, ainsi que les responsabilités associées, en cas d'incident informatique. Ce plan a vocation à faire reprendre l'activité de l'entreprise dans des délais qui ne mettent pas en jeu sa survie.

14.1/16.

Question 6

Dans un projet informatique, on distinguera la maîtrise d'ouvrage (MA) de la maîtrise d'oeuvre (ME).

- Pour la maîtrise d'ouvrage
  - Note détaillant le projet informatique
  - Rétro-planning avec jalons

- Pour la maîtrise d'oeuvre
  - Dépôt git.

15/16