Intitulé de l'épreuve : Informatique - Infrastructure des SIC

Nombre de copies : 4 copies (15 pages)

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Partie 1 :

a.a :

2875	2
1	1437 | 2
1	718 | 2
0	359 | 2
1	179 | 2
1	89 | 2
1	44 | 2
0	22 | 2
0	11 | 2
1	5 | 2
1	2 | 2
0	1

donc $(2875)_{10} = (101100\,1110\,11)_2$

a.b :

0	1	0	1	1	1	1	1
↓	↓	↓	↓	↓	↓	↓	↓
128	64	32	16	8	4	2	1

ainsi $(01\cdot01\cdot11\cdot11)_2 = (64+16+8+4+2+1)_{10}$

$= (93)_{10}$

N° 1.1.15

a.c : 0 1 1 0 | 1 1 1 0
8 4 2 1 | 8 4 2 1

$= (4+2)_{10}$ $= (8+4+2)_{10}$

$= (6)_{10}$ $= (14)_{10}$

$= (6)_{16}$ $= (F)_{16}$

ainsi $(0110 \cdot 1110)_2 = (6F)_{16}$

a.d :

1 0 1 0 1 0 1 0	pour vérification :	
+ 1 0 0 0 0 1 1 0	$= 128+32+8+2$	$= 170$
1 0 0 1 1 0 0 1 0	$= 128+4+2$	$= 134$
	$= 256+32+16$	$= 304$

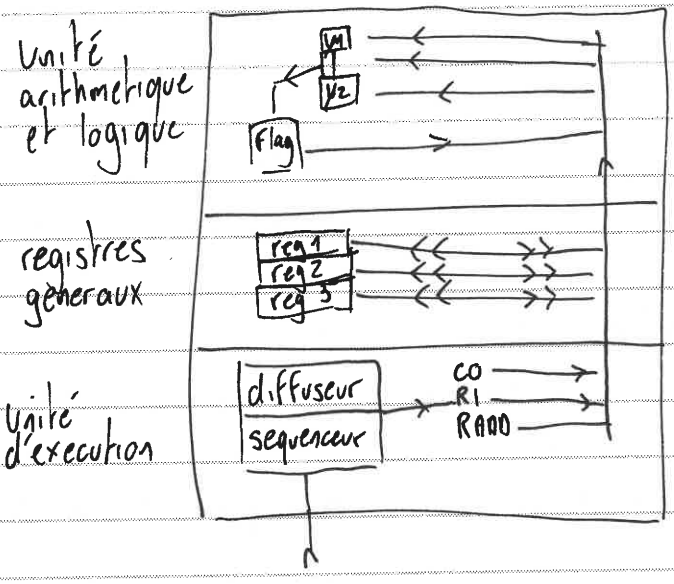
ainsi $(10 \cdot 10 \cdot 10 \cdot 10)_2 + (10 \cdot 00 \cdot 01 \cdot 10)_2 = (1 \cdot 00 \cdot 11 \cdot 00 \cdot 10)_2$

b.a : un microprocesseur est un élément très important dans un ordinateur puisqu'il est le matériel qui va permettre l'execution des différents programmes.
Il est en effet à l'origine de l'ensemble des calculs effectués par l'ordinateur, ainsi que de l'ensemble des commandes via son unité arithmetique et logique
il est en lien constant avec la mémoire centrale et le support de masse via la carte mère. La communication se fait par des circuits appellés bus.

b.b : les principales caracteristiques sont :
- la fréquence, generalement en Gigahertz qui correspond au nombre d'actions pouvant être effectué en une seconde (1 GHz = 1 milliard / seconde)
- le nombre de coeur qui influera sur le nombre d'action pouvant être effectuées simultanement

N° 2.1.15

b.c :



- l'unité d'exécution reçoit l'information, la séquence, et la diffuse pour exécution
  - CO = Compteur Ordinal : valeur de la prochaine instruction
  - RI = Registre d'instruction : valeur de l'instruction en cours
  - RADD = Registre Addresse : adresse mémoire sur laquelle il travaille
- Registres généraux : mémoire ultra rapide intégrée au processeur
- Unité Arithmétique et logique : les informations Y1 et Y2 sont traitées (AND, OR, commande...) et donne un résultat.

b.d : - les problématiques sont la taille puisque dans les smartphones notamment, des microprocesseurs toujours plus petit doivent être de plus en plus puissants
- et la température car les calculs effectués par ce microprocesseur génère de la chaleur qu'il faut dissiper, par des ventilateurs notamment.

Partie 2:

a.a: le système de fichier a pour rôle de structurer l'écriture des données sur un support de masse, de la rendre accessibles par des requêtes de lecture.
Son gestionnaire se nomme le MBR (master boot record). Il a pour rôle d'y spécifier l'emplacement des différentes partitions (début et taille) ainsi que leur type.
Il laisse place aujourd'hui au GPT (GUID partition table) notamment pour les disque plus volumineux.

a.b: Le NTFS est très majoritairement utilisé sur le système d'exploitation Windows mais des outils permettent d'y accéder depuis des OS Linux (ntfs-utils notamment)
L'ext4 est utilisé sur les systèmes Unix et Linux.
Il existe des outils pour y accéder depuis windows, mais leur usage n'est pas fiable.

Ces systèmes de fichiers créent un "sommaire" en tête de partition où sera inscrit l'emplacement de chaque fichier présent sur le disque ainsi que les informations associées (date de création, date d'accès, date de modification, propriétaire, droits ...) et notamment si le fichier est effacé.
La gestion de ces attributs diffèrent entre ces 2 systèmes de fichier. Ext4 offre la particularité de journaliser les écritures pour une meilleur prise en compte des erreurs.

a.c: Sous windows, fat32 et fat16. ils disparaissent petit à petit car la taille maximum des fichiers est de 4 Go
Sous Linux: ext2, ext3 qui précédaient ext4.
On trouve également d'autres systèmes de fichier comme Reiserfs
Apple dispose également de son système de fichier h-fs

N° 4/15

Intitulé de l'épreuve : Informatique - Infrastructure des SIC

Nombre de copies : 4 copies (15 pages)

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

(partie 2)

a.d : il existe d'autre systèmes de fichier "moins classique" notamment via les SAN (Structure Area Network)
La gestion du système de fichier ne se fait plus directement par le disque mais par un element tiers relié par Fiberchannel

Les NAS, plus classiques, permettent par la mise en relation de plusieurs disques sur un même materiel d'augmenter la disponibilité de la donnée via du RAID qui permet de la tolerance de panne.

b.a : un système multitache est en mesure d'executer plusieurs taches simultanement.

b.b : la commutation de contexte consiste à gérer la file d'action à executer en fonction des priorités de la tache et de la disponibilité des différent cœurs du processeur

b.c un ordonnanceur va s'assurer de la bonne gestion de la file d'attente des taches, notamment en fonction des priorités de chacune.

b.d: un ordonnancement temps réel gèrera avec une priorité maximale le/les services qui nécessitent une disponibilité maximale.

Partie 3 :

a: il est préferable d'utiliser une fibre optique plutot que du cuivre dans les cas suivants.
- lorsque le debit a besoin d'etre important (ex: fibre > adsl, fibre > cuivre RJ45 cat6 ...)
- lorsque la distance est plus importante (ex: lien intersite, PC a plus de 100 mètres des commutateurs ou repeteurs)
- pour des besoins de sécurité car il est plus compleke découter le trafic sur une fibre que sur du cuivre.

b.a: - le module SFP se branche entre l'équipement réseau et la fibre. Selon le modèle de fibre (ST, SC, LC...) on utilisera ainsi le modèle de SFP adapté.

b.b - Un IPPX est un commutateur Telephonie sur IP. Il succède aux PABX. Il permet de s'appuyer sur la même infrastructure réseau que le reseau informatique pour l'acheminement des flux telephoniques.
il est le serveur central de la telephonie, permet la communication entre les combinés IP mais aussi avec l'extérieur.
Il s'appuie sur des protocoles comme SIP et H323.

N° .6.1!5.

b.c : un proxy est un service (parfois un serveur par abus de langage) par lequel transitent tous les flux désirées à des fins de
- cache (pour ne pas telecharger plusieurs fois la même donnée)
- sécurité, en le couplant avec un antivirus ou par des règles
- de filtrage, en interdisant certains flux ou IP
- d'authentification, si son accès est soumis à la saisie d'un identifiant et d'un mot de passe
- de journalisation,

On parle majoritairement de proxy web (notamment squid sous linux) mais ils peuvent être mis en place pour différents services (exemple : mail)

b.d : une jarretière optique est une fibre. Elle est connectée, entre le pc et l'équipements, ou entre équipements, eventuellement par des bandeaux de brassage
Elle peut être multimode ou monomode : ces dernières sont utilisées pour de plus hauts débits, ou de plus longues distances.

c : Affirmations fausses : d : non, adresse réseau
e : non : 2x256-2 = 510
f : non : classe C 7/192.x.x.x

d : le 802.11 est le protocole associé au wifi. il en explique les spécificités selon les modes et versions (a, b, g, n, ac)

e : le protocole ARP, de niveau 2, permet à partir de l'adresse IP d'un destinataire de trouver son adresse MAC pour pouvoir ensuite communiquer avec lui sur la couche 2 du modèle OSI

Exemple entre 2 stations SA et SB :

N° 7.1.15

SA: trame broadcast "FF...FF" : "qui à l'adresse IP 192.168.0.2"
SB: trame "j'ai l'IP 192.168.0.2, mon adresse MAC est BB.BB.BB.BB.BBBB
SA: connait ainsi @Mac du destinataire et peut envoyer trame directement à SB via l'adresse "BB.BB.BB.BB.BB.BB" au niveau 2 qui contiendra paquet de niveau 3 avec l'adresse IP 192.168.0.2

Le commutateur intermédiaire, tout comme les ordinateurs, conservent une table des associations "adresse MAC/adresse IP"

Partie 4 :

a: aujourd'hui : 80 employés
dans 2ans : +300 % soit 420 employés
par précaution, nous prenons une marge de 30 % pour anticiper de nouvelles arrivées ou des employés qui auraient 2 PC :
420 + 30 % = 546 adresses doivent être disponibles.

Le vlan PC aura donc 1022 adresses :
- 192.168.4.0/22 (de 192.168.4.1 à 192.168.7.254), masque 255.255.252.0

Le vlan Phonie aura également 1022 adresses :
- 192.168.8.0/22 (de 192.168.8.1 à 192.168.11.254), masque 255.255.252.0

Le vlan imprimante aura 254 adresses :
- 192.168.3.0/24 (de 192.168.3.1 à 192.168.3.254), masque 255.255.255.0

Les équipements réseaux auront des adresses du réseau 192.168.2.0/24
- il sera subdivisé en fonction des besoins,
  - par exemple 192.168.2.0/27 (de 192.168.2.1 à 192.168.2.30, avec un masque en 255.255.255.224 pour un maximum de 30 commutateurs des abonnés)
  - et des réseaux d'interconnexion entre routeurs et firewalls notamment du type 192.168.2.64/29 pour des réseaux autorisant 6 IP (ici 192.168.2.65 à 70 avec un masque 255.255.255.248 afin d'avoir plus de 2 IP si on souhaite mettre en place des Equipements réseaux de secours via le protocole HSRP

Les administrateurs auront un vlan dédié pour l'administration et la supervision : 192.168.1.0/24 soit 254 IP.

Intitulé de l'épreuve : Informatique - Infrastructure des SIC

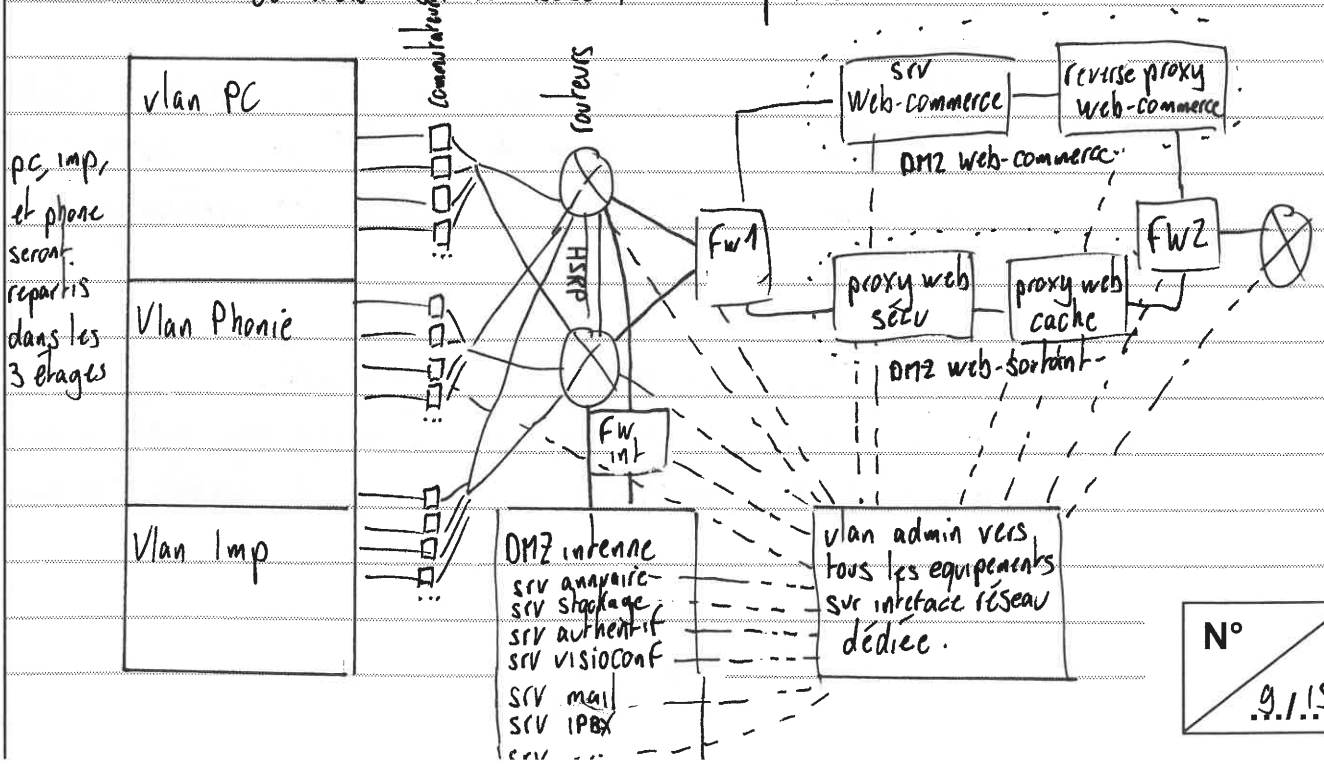
Nombre de copies : 4 copies (15 pages)

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

(partie 4 - suite)

Les serveurs seront répartis en 3 sous-réseaux :

- 192.168.0.0/28 soit 192.168.0.1 à 14 (masque 255.255.255.240)
  pour les equipements du sous réseau "DMZ Web-commerce" :
  2 serveur web, 2 reverse proxy, 2 adresses IP des pare-feu
- 192.168.0.16/28 soit 192.168.0.17 à 30 (masque 255.255.255.240)
  pour les proxy (on pourra differencier proxy cache et proxy sécurité (authentification, filtrage, journaux) en les mettant en cascade). => "DMZ web-sortant"
- 192.168.0.32/27 soit 192.168.0.33 à 62 (masque 255.255.255.224)
  pour la "DMZ interne" qui contiendra les serveurs Annuaires, authentification, stockage, visioconference et possiblement mail ou web si le besoin est exprimé



3 Firewalls ont été installés :
- un pour la DMZ interne
- un de chaque coté des "DMZ-commerce" et "DMZ web-sortant" afin de filtrer en amont et en aval, et en prenant le soin d'installer deux materiels de marque differentes.

b: Le télétravail pourrait s'effectuer avec un serveur VPN associé à un fichier de configuration et des clés à copier sur la station distante qui se connecterait alors avec le logiciel client (ex: openssl) vers le serveur sur un tunnel dédié et chiffré, mais les prérequis demande l'installation d'aucun logiciel.
Cet outil est très facilement installable depuis des stations linux.
Pour des stations windows, il est possible de le configurer directement depuis le parametrage réseau. Il faudra néanmoins copier les clés privées et publiques du serveur VPN pour assurer le maximum de sécurité

On placera alors entre FW1 et FW2 une "DMZ-VPN" qui contiendra le serveurs VPN, les clients authentifiés pourront alors joindre les serveurs de la "DMZ-interne" s'ils en sont autorisés.
Les flux du tunnel chiffrés arriveront sur le routeur d'entrée qui les redirigera via du "destination NAT" vers le serveur VPN (par défaut en UDP 1194 mais pourra être modifié pour accroitre la sécurité)

Le chiffrement se ferait en deux temps :
- chiffrement asymetrique pour l'échange des clés, à minima RSA 1024
- chiffrement symetrique pour les flux de données, à minima AES 256.

partie 5 :

a : un protocole pair à pair, ou peer-to-peer, est un protocole où les hotes communiquent entre elles sans transiter par un serveur "central"
A l'inverse d'un protocole classique, par exemple pour SMTP où le mail est envoyé au serveur SMTP (dont le nom d'hote est configuré dans la configuration) de proximité qui cherche le serveur du domaine de destination pour relayer le mail jusqu'au destinataire, en P2P, le client se connecte à un serveur de façon traditionnelle afin de consulter les hotes qui sont accessibles pour pouvoir ensuite les joindre directement via l'adresse IP et le port du destinataire.

Le P2P se retrouve ainsi pour le partage de fichier (on requête "directement" le destinataire dès lors qu'il est connu pour télécharger les fichiers qu'il met à disposition

Le même principe se retrouve pour la téléphonie sur IP où après avoir contacté le serveur SIP pour la "mise en relation" avec l'abonné distant, la communication est ensuite de pair à pair.

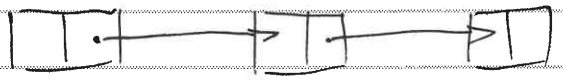
b : La création d'un code executable sur une machine se fait à partir d'un code source que l'on soumet à un compilateur présent sur la machine.
Le compilateur va ainsi généré un binaire qui sera fonction de l'architecture de la machine (32 bits, 64 bits, OS...)
Ce code pourra ensuite être executé sur la station.
Etant spécifique à l'architecture de cette machine, il ne pourra s'installé que sur des ordinateurs similaires.

N° .!!.!5

c: un tableau en algorithmie consiste en le stockage de données dans cet élément.
un tableau a donc une taille qui correspond au nombre de valeur qu'on peut stocker.
Une fois crée, on peut le remplir, ou consulter les données

ex: "t" est un tableau de 10 entrées.
on peut ajouter une donnée à la $i^{ème}$ position: t[i] = '7'
où interroger le contenu de la $i^{ème}$ position : t[i]

Une liste chainée est une succession d'éléments auquels on peut accéder en interrogeant leurs adresses.



Partie 6 :

à: Les objectifs visés par la SSI sont:
- la confidentialité : faire en sorte que seule les personnes ayant l'autorisation et le besoin d'accéder aux données ne puisse le faire. Outre les règles d'authentification, d'autorisation, cela inclu la sécurité des protocoles avec l'emploi de chiffrement pour rendre inintelligible les données en cas d'interception par un tiers

- l'intégrité est le fait de garantir que la donnée n'a pas été modifiée, aussi bien à cause de pertes dans la transmission, que par un tiers par malveillance.

- la disponibilité : garantir que le système sera fonctionnel et accessible selon un pourcentage qui aura été défini lors de l'analyse des risques. Les services web commerciaux et encore plus les Entreprises d'énergie, se doivent d'avoir un taux de disponibilité proche voir égal à 100%.

N° 12/15

Intitulé de l'épreuve : Informatique - Infrastructure des SIC.

Nombre de copies : 4 copies (15 pages)

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Traçabilité - Imputabilité : les journaux mis en place sur chacun des serveurs, services, équipements réseaux doivent permettre de remonter à l'auteur d'action qui auront au préalable été definies.
exemples : - toutes les tentatives d'authentification, aussi bien succès que échecs
- toutes la navigation internet, qui doit pouvoir être presentée à un juge s'il le demande sur une durée d'un an.

b: la non repudiation a été decrite au paragraphe précédent.
Il s'agit de garantir qu'une personne est bien à l'origine d'une action et qu'il ne peut s'agir que d'elle.
Cela se matérialise par des journaux, mais également des moyens techniques comme l'usage de certificat où à travers une Infrastructure de gestion de clés (PKI) on pourra certifier l'identité d'une personne ou d'un site

le chiffrement consiste à rendre inintelligible une donnée ou un flux. Il se fait via des algorithmes, de preference considerés comme robustes par l'Agence Nationalle de la Securité des systèmes d'informations (ANSSI).
il existe deux types de chiffrement :
- symetrique (AES, DES, 3DES) où le chiffrement

N° 13/15

s'effectue à partir d'une clé qui est partagée avec le destinataire
- assymétrique (RSA) : où le chiffrement se fait à partir de la clé publique du destinataire. C'est ensuite sa clé privée qui lui permettra de déchiffrer le message reçu

L'assymétrique étant jusqu'à 100 fois moins rapide que le symétrique, on utilise généralement :
- l'assymétrique pour un échange de clés,
- le symétrique à partir de la clé échangée, pour le chiffrement des flux.

Ce principe évite d'avoir à se partager une clé.

Le déchiffrement consiste à rendre clair/lisible le message préalablement chiffré :
- soit à partir de la clé partagée
- soit à partir de la clé privée associée à la clé publique qui a effectuée le chiffrement.

Le décryptage consiste à obtenir le clair d'un message chiffré sans avoir connaissance de la clé partagée ou de la clé privée.
Il s'effectue soit :
- par dictionnaire
- par bruteforce (on tente tous les caractères possibles)
- par combinaison des deux (mots + caractères + substitution)
- par des algorithmes type "markov" où on tente de prédire les caractères les plus probables.
- par la recherche ou l'exploitation de failles dans l'algorithme de chiffrement
- par Ingenierie Sociale
- par la récupération de bases ayant "fuités" (leaks) car les utilisateurs réutilisent souvent le même

N° 15.1.15

mot de passe.
Pour les 4 premières, les chances de trouver le mot de passe sont proportionnelles à la "faiblesse" du mot de passe et à la puissance de calcul.

C-a: Pour s'assurer qu'il n'y aura pas de problèmes lors du passage d'un système d'une version N à une version N+1, il est indispensable de passer par une plateforme de préproduction quasi conforme à celle de production.
Cela permet de vérifier le bon fonctionnement, et surveiller les effets de bord.
Il faut ensuite la mettre en production à des Beta-testeurs qui auront un profil permettant de constater les bugs restants, et de remonter d'éventuelles améliorations.
Ces bugs pourront alors être corrigés puis testés sur la plateforme de préproduction. Le système passera alors en version Alpha, pour validation.
Après les dernières corrections, elle pourra passer en production.

C-b:
La publication de code source sur des plate-formes en ligne type Sourceforge et GitHub présente avantages et inconvenients.
Avantages:
- mise à disposition du code à tout le monde
- possibilité que ce code soit vu, lu et que des propositions de correction ou d'amélioration soient proposées.
- réutilisation du code, ou évolution du code pour d'autres projet
- Suivi du "versionning".

Inconvénients.
- la mise en ligne d'un code présentant des vulnérabilités et utilisé peut permettre à des personnes malveillantes de les exploiter pour pénétrer un système ou un réseau.

N° 15/15