Intitulé de l'épreuve : INFRASTRUCTURES

Nombre de copies : 1/5

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

I) Architectures matérielles

1) a. RISC et CISC sont deux types d'architecture processeur. Leurs différences sont explicitées dans leur nom : Reduced Instruction Set Computing ou Complex Instruction Set Computing. Le premier utilise une architecture CPU simplifiée, proposant un jeu d'instructions de programmation réduit mais très optimisées en terme de performances. Il demande cependant plus d'efforts au programmeur. Le deuxième, c'est l'inverse ! Plus grand nombre d'instructions spécialisées, moins d'efforts de programmation, performances moins optimales. Exemples : CISC → x86
RISC → Apple M.

1) b. BIOS signifie Basic Input Output System.

Il s'agit du microgiciel chargé sur une puce de la carte mère d'un ordinateur (ou autre dispositif) qui va gérer le premier niveau d'entrées - sorties du CPU, notamment les bus de la carte - mère, la mémoire entre les disques durs, le clavier... Il s'active dès l'allumage de l'ordinateur, puis déclenche la séquence d'amorçage du système d'exploitation selon les paramètres configurés dans le setup (CMOS)

1) c. Un SoC est une puce regroupant CPU, RAM, circuit d'affichage, de son, et toute autre fonction nécessaire au fonctionnement du système construit autour. Il a l'avantage de la performance à moindre coût industriel et énergétique, et l'inconvénient d'être limité en évolutions. Exemples : Qualcomm Snapdragon pour téléphones mobiles ou encore Nvidia Tegra pour console de jeu.

N° 1 / 2 pages

1) d. Un TPM est une zone mémoire non volatile protégée, située sur une carte-mère ou dans un CPU, ayant pour but de servir de coffre-fort numé-rique sécurisé pour conserver les certificats de chiffrement du système. Ceux-ci ne sont accessibles qu'au moyen d'une méthode d'authentification dé-terminée, telle que la passphrase de déchiffrement des Itinéo du MAE qui permet l'accès au certificat de chiffrement du disque-dur de la VM Eole.

1.) e. Les caches et registres d'un CPU sont des zones mémoires très rapides situées dans le CPU et lui permettant de traiter les données en cours sans avoir à les charger et les écrire en RAM à chaque opération, ce qui serait bien trop lent.
Les registres sont les zones contenant les opéran-des des instructions en cours de traitement, les caches sont structurés en niveaux, de 1 à 3, du plus rapide et "proche" du cœur de la

N° 1 3.1.20

puce au plus externe et lent.

1) f. ASCii → norme historique basé sur le jeu de caractères anglo-saxon

UTF-8 → norme Unicode permettant de coder tous les alphabets du monde, les emoji, etc.

Big 5 → ancienne norme de codage des langues asiatiques, encore utilisée par endroit malgré son remplacement (bienvenu !) par UTF-8

2) a. $(185)_{10} = (128+32+16+8+1)_{10}$

$= (2^7+2^5+2^4+2^3+2^0)_{10}$

$= (1011\ 1001)_2$

b. $(F2A)_{16} = (1111\ 0010\ 1010)_2$

selon le tableau de conversion ci-contre →

Hex	Bin	Hex	Bin
0	0000	A	1010
1	0001	B	1011
2	0010	C	1100
3	0011	D	1101
4	0100	E	1110
5	0101	F	1111
6	0110		
7	0111		
8	1000		
9	1001		

N° 1 / 4.1.20

2) c. $(A18)_{16} = (10 \times 16^2 + 1 \times 16^1 + 8 \times 16^0)_{10}$

$= (10 \times 256 + 16 + 8)_{10}$

$= (2584)_{10}$

d. 1010 1100 → 128 + 32 + 8 + 4 = 172
− 1001 0111 → 128 + 16 + 4 + 1 = 149
0001 0111

vérification :

$(172 - 149)_{10} = (23)_{10} = (16 + 4 + 2 + 1)_{10}$

$= (2^4 + 2^2 + 2^1 + 2^0)_{10} = (0001\,0111)_2$

3) Une représentation classique en binaire des nombres entiers signés est celle utilisée notamment par le langage C, à savoir que le premier bit est à 0 si le nombre est positif, il passe à 1 si le nombre est négatif. Sur un octet, on peut donc représenter les nombres allant de $(-127)_{10} \rightarrow (1111\,1111)_2$ à

$(127)_{10} \rightarrow (0111\ 1111)_2$. Le zéro étant indifféremment codé $(0000\ 0000)_2$ ou $(1000\ 0000)_2$, mais on n'utilise que le premier par convention et commodité.

L'inconvénient principal est que, si le programmeur ne fait pas attention, ajouter 1 à 127 provoque un dépassement de domaine de définition et donne le résultat erroné −127 au lieu de 128.

II) Systèmes d'exploitation

1) Un hyperviseur est un programme permettant de créer et d'exploiter, sur une machine hôte et son système d'exploitation, des machines virtuelles émulées. Je ne connais pas la différence entre les types 1 et 2, mais je devine que cela a à voir avec la manière avec laquelle l'hyperviseur accède aux ressources du système simulateur, ou encore son caractère distribué ou pas.

2) Un système d'exploitation open-source est un OS dont le code source est publié et disponible pour revue ou modification selon une licence libre. Le plus connu est GNU/Linux.
logiciel

3) Une RODC ou Read-Only Domain Controller est un serveur d'annuaire de la famille Active Directory de Microsoft dont les enregistrements ne peuvent être modifiés que par synchronisation avec un contrôleur AD principal. On l'utilise dans les architectures décentrées, sur des sites distants du contrôleur AD principal, afin d'éviter toute compromission localisée des enregistrements. Au MAE, c'est le cas dans les postes à l'étranger.

4) Un inode est un lien dynamique vers un fichier ou un répertoire sous Linux. C'est l'équivalent d'un raccourci sous Windows

5) Aucune idée. On utilise par contre beaucoup le "système D" en poste...

N° 2 7.1.20

6) FAT et son évolution 32 bits FAT 32 sont les systèmes de fichiers historiques hérités de DOS. NTFS est plus moderne et gère nativement les droits d'accès en natif.

7) chmod est la commande qui permet de modifier les droits d'accès à un fichier ou un dossier sous Unix.

Par exemple chmod 777 toto donne tous les droits de lecture, écriture et exécution du fichier toto à l'utilisateur, son groupe d'une processus systèmes. chmod 000 toto l'interdit au contraire.

8) Les OS 32 et 64 bits peuvent manipuler en natif des nombres codés respectivement sur 32 et 64 bits. Les OS 32 bits ne peuvent ainsi adresser que 2^{32} unités de mémoire, limitant de fait la RAM utilisable et la taille des fichiers sur le disque. Les systèmes 64 bits font passer cette limite à 2^{64}, ce qui est beaucoup plus.

N° 2 / 8 1.2.0

III) Réseaux

1) a. 192.168.101.30/23 → masque de sous-réseau sur 23 bits → le dernier bit du 3° octet n'est pas significatif

⇒ l'adresse réseau est donc 192.168.100.0

b. L'adresse broadcast est donc 192.168.101.255

c. Le masque décimal est 255.255.254.0

d. Il y aura donc $2^{32-23} - 2 = 2^9 - 2 = 510$ hôtes disponibles sur ce réseau (en fait 509 car une IP est toujours prise par la passerelle).

2) La norme 802.1Q permet, au niveau de la couche 2 du modèle OSI (protocole Ethernet)

de tagger des trames réseau pour indiquer à quel VLAN elles s'adressent. On l'utilise aussi MAE pour séparer les flux VoIP et DATA Eole entre deux VLAN tout en sécurisant les ports des switches utilisés à la fois par l'un et l'autre des VLAN (le téléphone agissant alors comme un mini concentrateur secondaire pour laisser passer les flux data Eole).

3) Un IPBX est un central téléphonique spécialisé dans la téléphonie sur IP, là où un PABX sera plus généraliste et pourra également exploiter des postes téléphoniques classiques, numériques ou analogiques. Les IPBX proposent aussi de nombreuses fonctionnalités étendues centrées sur l'IP, comme la virtualisation du poste téléphonique sur la station de travail ou l'interconnexion avec des réseaux VoIP externes tels que Microsoft Teams. Ils peuvent, de plus,

être facilement virtualisés et déportés en cloud du fait qu'ils n'interviennent que dans le monde IP.

4) La latence est le temps que les paquets émis mettent à atteindre leur destination. La gigue est la variation de ce temps de latence au cours des temps pour des paquets successifs. Une gigue forte verra ainsi le temps de latence varier beaucoup, ce qui peut occasionner des artefacts lors des communications temps-réel telles que la Vo IP (micro-coupures, voire perte de communication).

5) La raison qui pousse les opérateurs à migrer sur IPv6 est la pénurie d'adresses IPv4. Celles-ci sont en effet toutes allouées, ou presque, là où IPv6 en fournit un nombre beaucoup plus grand permettant de sortir de cette pénurie pour des décennies. L'autre avantage, qui est une conséquence, est que chaque hôte IPv6 peut ainsi avoir une adresse publique sur Internet, épargnant la nécessité de recours aux NAT et autres acrobaties vues en III.1), sauf pour raisons de sécurité.

6) a. SCP → aucune idée

b. BGP → Border Gateway Protocal, routage dans le monde IP

c. SMTP → Send Message Transfer Protocal, envoi d'e-mails.

d. DHCP → Dynamic Host Control Protocol, attribution dynamique ou statique d'adresses IP à des hôtes selon un plan d'adressage

e. SMB → Partage de fichiers sur un réseau dans le monde Windows

V) Protocoles, langages et structures de données

1) Une API, ou Application Programming Interface est une suite d'outils et de fonctions permettant à un programme de communiquer avec une application. Par exemple les librairies Visual Basic permettant de contrôler les programmes de la suite MS Office sont une API. De même, les fournisseurs de services en ligne (réseaux sociaux, e-commerce ...) fournissent

souvent une API (généralement payante) pour accéder, intégrer, ou opérer certaines de leurs fonctionnalités dans des programmes tiers.

2) XML, JSON, YAML

3) Un langage de bas niveau, tel que l'assembleur x86, est construit sur la base des instructions physiques présentes sur le matériel. Il permet un contrôle direct de celui-ci, avec une vitesse d'exécution optimale au prix d'une complexité de programmation bien plus grande. On le réserve donc en général pour des routines critiques devant s'exécuter aussi vite que possible.

A l'inverse, un langage de haut niveau

accède au matériel via des bibliothèques de niveau d'abs-traction supérieur permettant une compréhension plus directe pour le programmeur et une souplesse plus grande au prix d'un peu de performances.
Exc: C++

4)

```
int fact(int n){
    if(n>1){
        n = n * fact(n-1);
    }
    return n;
}
```

VI) Sécurité

1) En DevOps le principe CI/CD implique à la fois un développement en cycles rapides de fonctionnalités qui sont intégrés immédiatement puis déployés très vite et qui font l'objet d'une évaluation continue et tout aussi rapide des équipes d'exploitations afin de pouvoir corriger, modi-

- fier ou itérer rapidement sur une fonctionnali-
- té ne donnant pas/plus totale satisfaction.

2) Une attaque MITM intervient quand un hac-
- ker s'interpose entre l'émetteur et la source d'une com-
- munication chiffrée asymétrique au moment de l'échan-
- ge des clés publiques. Il peut ainsi se faire pas-
- ser pour l'un et l'autre des hôtes qui communiquent
en leur envoyant sa propre clé maquillée à la
place des leurs et déchiffrer leurs communications sans être détecté.

Pour se prémunir de ce type d'attaque, il faut utiliser une autorité de certification qui pourra authentifier le détenteur de chaque clé publique de manière certaine au moyen d'éléments d'identification.

3) Une solution EDR permet de détecter des com-
- portements anormaux pouvant indiquer une com-
- promission sur une station de travail. A la dif-
- férence des antivirus qui recherchent des signatures
virales connues stockées dans une base, un EDR
va se focaliser sur la détection de comporte-

- ments anormaux au moyen d'heuristiques et de règles établies par les administrateurs (machine qui scanne les ports d'un hôte, qui tente de se connecter à de nombreux hôtes dans un temps donné...), règles associées à des techniques d'intrusion ou de compromission.

4) Un centre opérationnel de sécurité va rassembler sur un même tableau de bord les informations de sécurité, rassemblées par tous les éléments de sécurité d'un SI pour permettre le suivi, le pilotage et la réaction en cas d'incident par les équipes en charge de la sécurité.

IV) Infrastructures.

1) La nouvelle application pouvant fonctionner sur un serveur Linux, je fais donc ce choix afin d'éviter des coûts de licence d'un serveur sous Windows. Les éventuels coûts de formation des équipes d'administration pour monter en compétence sur ce système seront amortis à long terme.

Intitulé de l'épreuve : INFRASTRUCTURES

Nombre de copies : 5/5

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

Sans information supplémentaire sur la taille de l'entreprise, je vais toutefois supposer que la solution d'hébergement de l'application doit être capable de scaler facilement en fonction de l'activité. C'est pourquoi je propose de virtualiser les serveurs nécessaires au fonctionnement de l'application (serveur web/application, serveur de fichiers, de BDD). Une solution standard de virtualisation telle que VMWare ou ProxMox fera l'affaire dans la plupart des cas ou, si l'entreprise est très grande et si l'application est compatible, on peut envisager de construire un cloud privé basé sur des conteneurs Docker + un orchestrateur Kubernetes afin de gérer les instances des

N° 5 17.20

serveurs virtuels dynamiquement sur le parc de nouveaux serveurs physiques.

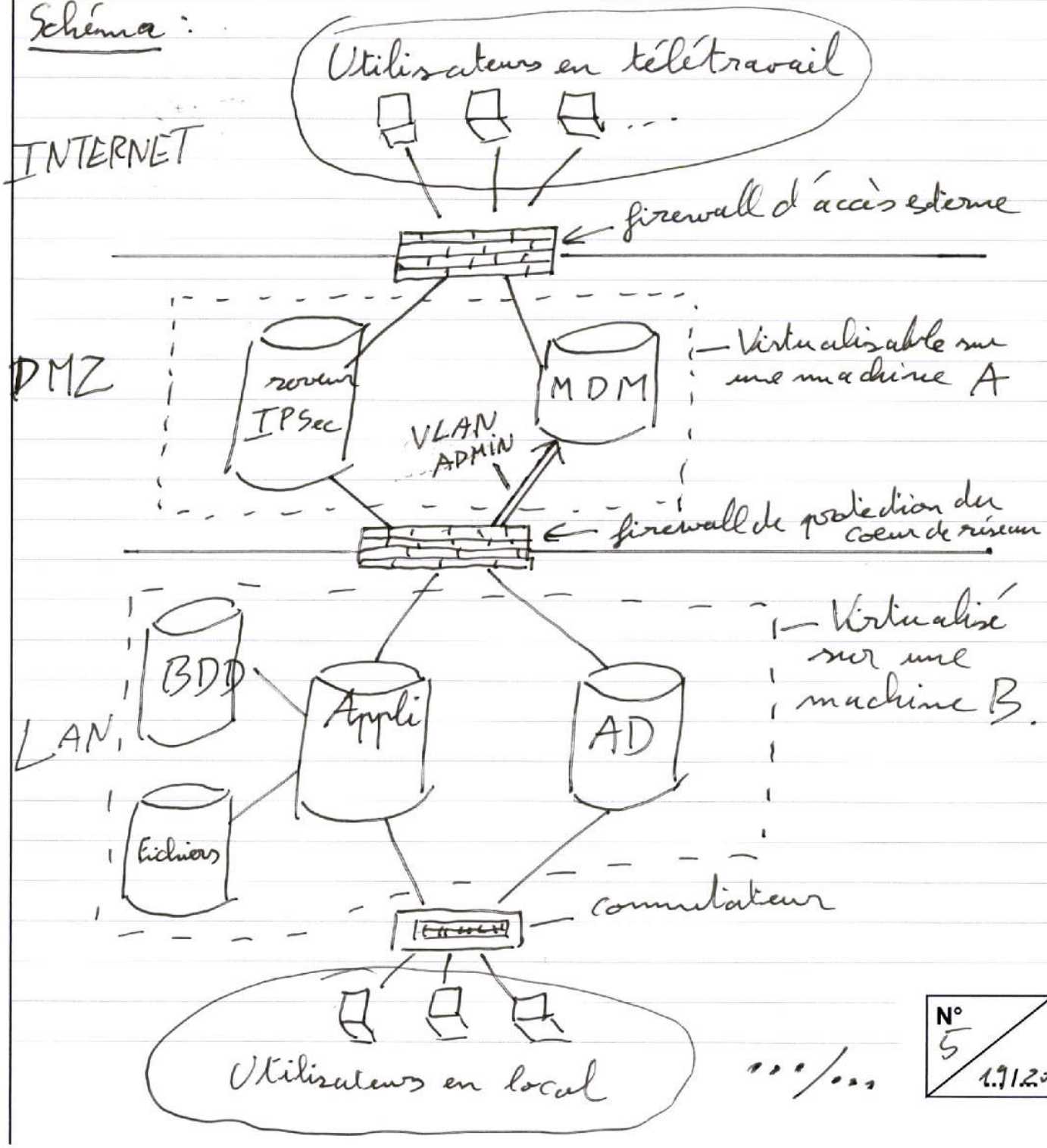
Enfin, un serveur d'annuaire devra également être déployé afin de rassembler les profils des employés et leurs droits d'accès de manière plus sécurisés et gérable. Celui-ci devra être un contrôleur AD pour pouvoir exploiter les GPO du monde Microsoft afin de sécuriser les postes de travail (des solutions existantes hybrides basées sur Linux / LDAP existent peut-être également). Ce serveur peut également être virtualisé.

2) Pour pouvoir permettre aux employés de télétravailler en toute sécurité, il faudra tout d'abord les doter d'ordinateurs portables. Ceux-ci seront administrés via un serveur de Mobile Device Management (MDM) qui permettra de suivre la flotte, déployer les mises à jour, gérer les droits d'accès à l'infrastructure et les neutraliser pour les appareils perdus ou volés.

N° 5 1.2.1.2.0

Les ordinateurs portables communiqueront avec l'infrastructure de l'entreprise depuis l'extérieur via un tunnel VPN IPsec dont le serveur et point d'entrée sera placé dans une DMZ pour isoler le cœur de réseau. Les certificats de chiffrement de chaque poste de travail mobile seront protégés par une méthode forte (TPM + double facteur).

Schéma :



.../...

Remarques : J'ai considéré que les données auxquelles les employés accèdent sont très sécurisées, ceci nécessite donc un contrôle total des postes de travail y compris depuis l'extérieur. Si le niveau de sécurité est inférieur, on peut alors remplacer le serveur MDM + tunnel IPSec par un simple proxy web sécurisé dans la DMZ, permettant d'accéder à l'appli, par exemple via un token. Cela élimine la nécessité de fournir du matériel spécifique de mobilité aux employés, ils se connecteraient alors à l'application depuis leur appareil personnel, et ce au prix d'une plus grande exposition à des attaques.

N° 5 / 20.1.20