Concours section : INT-TECHNICIEN INFORMATIQUE

Epreuve matière : Etude de cas

N° Anonymat : WJZCO292 UO Nombre de pages : 8

(Remplir cette partie à l'aide de la notice)

Concours : TECHNICIEN AP Session : 2024

Epreuve : INFORMATIQUE Date de l'épreuve : 09/04/2024

CONSIGNES

- Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.
- Numéroter chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.
- Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.
- N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.

1.1) Le modèle OSI est un standard ouvert permettant une modélisation de communication entre systèmes d'information au sens large. Il s'agit d'un modèle conceptuel.

1- Couche physique
2- Couche liaison
3- Couche réseau
4- Couche Transport
5- Couche Session
6- Couche présentation
7- Couche application

1.2) RSSI : Responsable de la sécurité des systèmes d'information.

Il a pour missions : - définir une PSSI adaptée à son organisme.
- veiller à la mise en oeuvre des réglementations SSI
- contrôler le sécurité des SI
- arbitrer sur des mises en place de SI en matière de sécurité.

1.3) MOA : Maitrise d'ouvrage. Le demandeur ou client.
MOE : Maitrise d'oeuvre. Le faiseur ou exécutant.

1.4) Un T2 dispose de 32 canaux dont 2 réservés, soit 30 utilisables.

RIEP - MA 520

Concours section : INT-TECHNICIEN INFORMATIQUE

Epreuve matière : Etude de cas

N° Anonymat : WJZCO292 UO Nombre de pages : 8

1.5 → ADSL : Asynchronous digital subscriber line
Cette technologie utilise les "lignes "cuivres" (i.e téléphones) pour la communication réseau public.
→ la fibre optique est une fibre transportant un signal lumineux.

- L'ADSL couvre une distance limitée (max 100m) avec un débit maximum 90 - 100 mbit/s
- la fibre optique peut couvrir des distances variables de l'ordre du mètre aux centaines de kilomètres avec des débits en Gbit/s et Tbit/s.

1.6) LAN : local area Network → réseau local.
Il s'agit d'un réseau limité en terme de distance (100 m environ entre les équipements maximum). Il se limite à un bâtiment avec plusieurs étages par exemple.
Les équipements sont sur le même réseau physique.

WAN : Wide area Network. → réseau large.
Il s'agit de réseaux communicants entre eux de grande distance. Le WAN relie souvent des LAN entre eux. Par exemple le réseau d'une entreprise à Paris relié à une de ses succursales à Strasbourg.

1.7) Un commutateur (switch) fonctionne sur du niveau 2. Il associe une adresse MAC à un port physique
Un routeur utilise des adresses IP (niveau 3) de réseau associées à un port.

1.8) Une adresse MAC (medium access control) est une adresse unique fournie à chaque interface réseau.
Elle est notée en hexadécimal : 0f:a9:b6:54:61:c2
identifiant du fabricant

Une adresse IP (Internet Protocol) permet d'identifier à quel réseau appartient une machine.
Elle est composée en IPv4 de xxx.xxx.xxx.xxx (adresse) et d'un masque de sous-réseau.

1.9) Le pare feu a pour but de filtrer les communications entre réseau. Il peut selon les modèles et logiciels autoriser ou interdire des communications en fonction de :
- l'adresse réseau (IP) source ou de destination
- le protocole ou port associé
- une application ou un service associé (Pare feu windows)
le filtrage s'applique en entrée et en sortie.

1.10) SSD : Solid state drive

1.11) Les disques durs classiques reposent sur une technologie électromagnétique pour lire et écrire des données. Les SSD utilisent de la mémoire flash ou EEPROM pour écrire et lire des données. Ils sont non-mécaniques et ont pour avantage de moins consommer et d'être plus résistants aux chocs.
Les vitesses d'écriture / lecture moyennes (pour 1 Go) :
- HDD : 60 MB/s / 120 MB/s) variables selon
- SSD : 200 MB/s / 500 MB/s) les modèles.

1.12) Un ransomware est un logiciel malveillant qui en s'exécutant va chiffrer les données du poste compromis. Il affichera un message à la victime, lui indiquant qu'elle devra verser une rançon en échange d'un ~~clef~~ déchiffrement des données. Exemple : Wannacry.

1.13) l'USB (universal serial Bus) permet du hot plug.

1.14) le port 25 est utilisé par le SMTP.
Simple ~~Message~~ Mail Transfer protocol.
Il s'agit du protocole utilisé pour l'envoi de mails.
(message électronique)

1.15) le Wifi est le nom du consortium.
la norme utilisée est le 802.11 (IEEE)
Elle communique sur deux fréquences : 2,5 GHz et 5 GHz
Il y a différents modes : a, b, c, g, f, n par exemple
qui sont chacun des versions du WiFi.

1.16) DNS : Domain Naming Service.
Il s'agit d'un service d'annuaire faisant le lien entre une adresse URL (uniform ressource locator) et une adresse IP.
Exemple : en allant sur https://google.fr, une requête DNS est envoyé à un serveur DNS prédéfini dans les paramètres IP.
le serveur DNS renverrai une adresse IP en retour.

1.17) SMB : Server Message block.
Il s'agit du protocole propriétaire de Microsoft utilisé pour accéder et obtenir des fichiers sur un serveur de partage de fichiers. Il en existe plusieurs itérations (v1, v2, v3)

1.18) NSlookup : Name Service lookup → regarder/vérifier
1.19) Il s'agit d'une commande (programme) permettant de requêter un ou plusieurs serveurs DNS afin d'obtenir des informations sur un nom de domaine ou une URL.
La commande permet également d'obtenir une liste des serveurs de messagerie (MX).

Concours section : INT-TECHNICIEN INFORMATIQUE

Epreuve matière : Etude de cas

N° Anonymat : WJZCO292 UO Nombre de pages : 8

(Remplir cette partie à l'aide de la notice)

Concours : TECHNICIEN AP Session : 2024

Epreuve : INFORMATIQUE Date de l'épreuve : 09/04/2024

CONSIGNES

- *Remplir soigneusement, sur CHAQUE feuille officielle, la zone d'identification en MAJUSCULES.*
- *Numéroter chaque PAGE (cadre en bas à droite de la page) et placer les feuilles dans le bon sens et dans l'ordre.*
- *Rédiger avec un stylo à encre foncée (bleue ou noire) et ne pas utiliser de stylo plume à encre claire.*
- *N'effectuer aucun collage ou découpage de sujets ou de feuille officielle. Ne joindre aucun brouillon.*

1.19) 1.20) Un SPAM est un message électronique (mail) non sollicité. Il s'agit souvent de publicités et de mails frauduleux pour du hameçonnage (phishing)

1.21) VPN : Virtuel private network)
Réseau virtuel privé

Le VPN permet de créer une passerelle entre un équipement connecté sur un réseau public ou personnel (i.e internet) et un réseau privé. Le VPN utilise une tunnelisation basée sur IPSEC et du NAT translaté afin d'établir une communication chiffré entre deux réseau.

Exemple d'utilisation : un employé pourrait depuis un poste connecté à sa box personnelle, activer le VPN configuré par sa entreprise et du coup, accéder de manière sécurisée au réseau interne de l'entreprise : fichiers, serveur mails, intranet, etc.

Cas n°1 :

1. a - Déconnecter le poste infecté du réseau
b - Avertir les acteurs de la chaine SSI de l'incident
c - Vérifier les autres postes utilisateur (si possible)
d - La remise en fonctionnement d'un poste infecté nécessite un formatage / réapplication d'une image système toutes données ne peut être récupérée (compromission)

RIEP - MA 520

Concours section : INT-TECHNICIEN INFORMATIQUE

Epreuve matière : Etude de cas

N° Anonymat : WJZCO292 UO Nombre de pages : 8

2) Les interlocuteurs en cas d'incident sont :
- le chef d'établissement
- le RSSI
- le chef du DSI

#Note :

Objet : Rappel sur les usages des stockages amovibles (clés usb, disques durs externes, etc)

Pour votre information,
les stockages amovibles sont, bien que pratiques dans leur usage de transmission de documents, des vecteurs de contaminations avérés pour votre système d'information. Certaines informations liées au fonctionnement de l'établissement pourraient être stockées sur ces supports, et en cas de perte ou de vol, la sécurité de l'établissement pourrait être compromise.

Quelques règles à respecter :

1. Privilégier au maximum l'échange de document par les outils du ministère
2. Ne jamais connecter un support amovible de source inconnue ou extérieure à l'établissement
3. Scanner la clé à l'aide de la station blanche avant de la connecter sur votre poste
4. Chiffrer les données sur la clé
5. Stocker vos clés usb en lieu sûr.

Je reste à disposition pour toute information.

Plan d'action sur la traçabilité des clés USB et procédures

1. Interdire l'utilisation de clés USB dans certaines zones de l'établissement (à définir selon la sensibilité)
   Exemple : zone de détention, sur les équipements de sûreté

2. Utiliser uniquement des clés ou support USB chiffrés afin de limiter la compromission des données en cas de perte ou vol

3. Mise en place d'une station blanche (ou décontamination) pour les clés usb

4. Prise de connaissance d'une charte d'usage des systèmes d'information

5. Fourniture et reprise des supports par un interlocuteur défini avec procès verbal de remise.

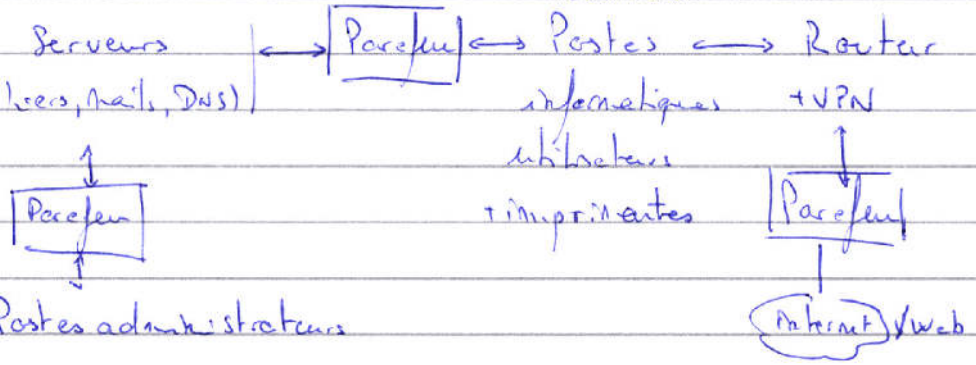
Cas n°2 :

Question :

a) Les sites étant distants de plusieurs kilomètres, il paraît difficilement concevable de les relier directement par fibre optique privée.
Pour relier les sites, il faudra employer une connexion internet avec l'utilisation d'un VPN.

b) Un routeur et un firewall (pare-feu)

c)



Question 2

1. La téléphonie utilise des ports d'entrée différents (T2, ip trunk). L'architecture réseau classique des ordinateurs n'est pas forcément adaptée.
Un IPBX sera nécessaire pour gérer la téléphonie

2. Si le réseau téléphonique est séparé du réseau classique de l'entreprise, il faudra doubler certains équipements : pare-feu, serveurs de messagerie vocale, équipements/postes d'administration. (Sans comptabiliser les baies, les câbleurs, les ports réseaux)

3. Si le réseau téléphonique doit être intégré, il faut établir/mettre en place une connexion spécifique pour ce réseau (VPN, pare-feu, routeur)

4. Il faut autant de postes téléphoniques que de postes informatiques (maintenance, coût, maintien opérationnel)

Question 3

Le poste du technicien peut être configuré avec un VPN afin de se connecter à son réseau d'entreprise.
Une autre solution serait d'utiliser un bastion avec un WAF (Web application Firewall)