

BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS
Option : Solutions d'infrastructure, systèmes et réseaux

**U6 – CYBERSÉCURITÉ DES SERVICES
INFORMATIQUES**

SESSION 2022

Durée : 4 heures
Coefficient : 4

Matériel autorisé :

Aucun matériel ni document est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 16 pages, numérotées de 1/16 à 16/16
(sans compter la page de garde).

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 0 sur 16

Cas MYON

Ce sujet comporte 16 pages dont un dossier documentaire de 9 pages.
La candidate ou le candidat doit à vérifier qu'il est en possession d'un sujet complet.

Barème :

Dossier A	Sécurisation de l'infrastructure	45 points
Dossier B	Sécurisation des serveurs et des services	35 points
	Total	80 points

Dossier documentaire

Documents communs à tous les dossiers	8
Document 1 : Schéma du réseau du site de Lesquin.....	8
Document 2 : Schéma du réseau du site de Mâcon	8
Document 3 : Description de l'infrastructure réseau de la société Benoit Myon	9
Document 4 : Principe d'adressage des réseaux locaux virtuels (Lesquin et Mâcon).....	9
Documents associés au dossier A	10
Document A1 : Commutateur / Passerelle de sécurité XG-7100-1U	10
Document A2 : Règles de redirection de port NAT (<i>port forwarding</i>) du commutateur SW1.....	10
Document A3 : Règles de pare-feu (<i>firewall</i>) coté externe (WAN) du commutateur SW1.....	10
Document A4 : Modèle de fiche de signalisation d'incident (document ITIL).....	11
Document A5 : Assignment des ports du commutateur SW2	11
Document A6 : IDS Outil de détection d'intrusions - Snort.....	12
Document A7 : Contrôleur Wifi WC7500	13
Document A8 : Conservation des données techniques de connexion	13
Documents associés au dossier B	14
Document B1 : Serveur NAS RS2418RP	14
Document B2 : Niveaux RAID	14
Document B3 : Présentation de l'utilitaire sudo	15
Document B4 : Vulnérabilité de l'utilitaire sudo	16
Document B5 : Script de mise à jour de sudo	16
Document B6 : Procédure de chiffrement des courriels	16

Présentation du contexte

La société Benoît Myon est spécialisée dans le transport de marchandises sur l'axe nord - sud de la France, l'Espagne et l'Italie.

L'entreprise existe depuis 1954 et dispose à présent d'une flotte de plus de 500 camions. Le siège social, ainsi que les principaux services, sont à Lesquin près de Lille. Un plateau technique et logistique a été construit à Mâcon, il y a 11 ans.

L'entreprise Benoît Myon est organisée en différents services :

- Les services techniques, à Lesquin et Mâcon, assurent la maintenance des tracteurs et des remorques (le stock de pièces détachées principal est à Lesquin).
- Le service informatique de Lesquin, composé de 6 personnes, assure le développement en interne de logiciels métiers, ainsi que la maintenance et l'exploitation des infrastructures systèmes et réseaux. La responsable du service informatique est Mme Carlier.
- Les autres services, qui sont tous à Lesquin, couvrent les domaines commercial, logistique, ressources humaines et comptabilité.

Le secteur du transport routier est extrêmement concurrentiel, aussi la société Benoît Myon doit pouvoir compter sur la sécurité de son système d'information.

De ce fait elle a contacté un prestataire informatique, l'entreprise de services du numérique ADS pour auditer son système d'information et proposer des améliorations en fonction des résultats de l'audit.

ADS dispose de 50 collaborateurs, techniciens ou ingénieurs spécialisés notamment dans l'audit et la mise en place de bonnes pratiques informatiques, qui garantissent la sécurité informatique de ses clients.

En tant que personne collaboratrice d'ADS, vous avez la charge de la mise en conformité de la société Benoît Myon.

Vous vous appuyerez sur le dossier documentaire mis à votre disposition.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 2 sur 16

DOSSIER A : SÉCURISATION DE L'INFRASTRUCTURE

L'audit de l'infrastructure système et réseau de l'entreprise Benoît Myon a soulevé divers points sur lesquels l'attention des dirigeants a été alertée :

- la sécurité du réseau de vidéosurveillance,
- la sécurité de la migration d'une application,
- la sécurité du réseau sans-fil.

Tous les points relevés par le prestataire ADS font l'objet d'une étude approfondie et de modifications de l'infrastructure auxquelles vous êtes associé(e).

Mission A.1 – Étude du réseau de vidéo-surveillance

L'entreprise Benoît Myon a mis en place un système de vidéosurveillance multi-sites avec enregistrement. Mme Carlier s'interroge sur la sécurité de ce système suite à des remarques du prestataire ADS.

La vidéosurveillance repose sur l'utilisation de 12 caméras IP sur le site de Lesquin et de 4 autres sur le site de Mâcon. Un enregistreur numérique, dont la référence est NVR4432-4KS2, stocke les vidéos sur 2 disques durs de 6 To en miroir (RAID niveau 1). Les vidéos sont conservées pendant 10 jours.

Les caméras IP de Mâcon transmettent leurs données à travers le réseau privé virtuel (VPN) qui relie les deux sites.

Pour aider à la localisation rapide des failles de sécurité, un schéma simplifié du réseau où ne figurent que les appareils concernés par le système vidéo s'avère utile.

Question A1.1

Représenter le schéma réseau sur lequel figureront tous les équipements concernés par les flux vidéo et les réseaux locaux virtuels (VLAN) associés.

Question A1.2

Expliquer pourquoi, dans le cas de l'entreprise Benoît Myon, il y a peu de risque de prise de contrôle d'une des caméras IP par un pirate via internet ou par un utilisateur local malveillant.

Mission A.2 – Migration et sécurisation de l'accès à une application métier

Une application métier pour système Android, développée en interne, permet aux chauffeurs d'échanger avec l'entreprise. La partie serveur de cette application est située sur le serveur physique Lxd1. Les protocoles et ports utilisés par cette application sont les suivants :

- Protocole HTTPS : 443
- Port utilisé sur le réseau interne : 5000
- Port utilisé sur internet : 5433

Tout le trafic venant d'internet arrive sur le port extérieur (réseau étendu, aussi appelé WAN - *wide area network*) du commutateur de niveau 3 SW1. La fonction routeur / pare-feu (*firewall*) de ce commutateur est sollicitée. Un extrait des tables de translation d'adresses (NAT) et de filtrage est fourni dans le dossier documentaire.

L'application métier, installée sur le serveur Lxd1, devra être migrée vers le serveur Lxd2 pour assurer sa disponibilité pendant les opérations de maintenance prévues sur le serveur Lxd1 le mois prochain. Les opérations risquent de se dérouler sur plusieurs jours.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 3 sur 16

Question A2.1

Indiquer quelles seront les modifications nécessaires à apporter sur les tables de translation et/ou de filtrage du commutateur SW1.

Cependant, en consultant les journaux du pare-feu, vous constatez qu'une attaque a eu lieu depuis le début de la journée sur le port 443 du serveur Lxd1. Le pirate cherche à trouver le mot de passe de l'un des sites *web* par la méthode de la force brute. De nombreuses tentatives d'authentification sont réalisées à partir de l'adresse source 193.14.78.1, puis, une minute plus tard, de nouvelles tentatives à partir de l'adresse source 5.49.250.12. Le pirate attend ensuite 10 minutes puis recommence avec les mêmes adresses IP. Seul le port 443 est attaqué.

Question A2.2

Indiquer quelles sont les modifications à réaliser sur la table de filtrage du pare-feu pour bloquer les attaques de ce pirate. *Vous préciserez l'emplacement de ces nouvelles règles dans la table.*

Les attaques pouvant se reproduire, madame Carlier vous demande de proposer une solution permettant d'automatiser cette procédure.

Question A2.3

Proposer, en l'argumentant, une solution logicielle pour protéger les serveurs contre ce genre d'attaque.

Dans le cadre des recommandations ITIL¹ de l'entreprise, vous devez déclarer tous les incidents qui surviennent. La fiche de déclaration d'incident propre à l'entreprise Benoit Myon figure dans le dossier documentaire (document A4).

Chaque case du document dispose d'un repère qui lui est propre. Par exemple, [n19] signifie qu'un vol de document ou de fichier a eu lieu.

Pour les cases [i11], [n24] et [u7], il faut le cas échéant, ajouter une courte phrase de description.

Question A2.4

Indiquer les repères des cases qu'il faut cocher dans le document pour déclarer précisément l'attaque qui vient d'être subie sur le port 443 de l'un des serveurs *web*.

Pour renforcer la sécurité de la zone démilitarisée (DMZ), vous proposez d'ajouter un service de détection d'intrusion (IDS). Votre choix se porte sur l'installation d'un hôte Debian dans la zone démilitarisée (DMZ) avec le logiciel Snort. Dans la documentation, on vous demande de mettre une interface réseau en mode promiscuité (*promiscuous*).

Question A2.5

- a) Expliquer le mécanisme d'une interface réseau en mode promiscuité.
- b) Indiquer les réglages à réaliser sur un ou plusieurs commutateurs du site de Lesquin afin de pouvoir analyser tout le trafic à destination de la zone démilitarisée.

Un test de connectivité (commande *ping*) vers un serveur *web* peut être le signe d'une tentative d'attaque. Aussi, vous décidez que le service IDS déclenche une alerte en cas de commande *ping* vers l'un des serveurs *web*.

Question A2.6

Rédiger les règles Snort qui déclenchent une alerte si un test de connectivité (commande *ping*) est réalisé vers le serveur Lxd1 ou le serveur Lxd2.

¹ bibliothèque pour l'infrastructure des technologies de l'information

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 4 sur 16

Mission A.3 – Sécurisation du réseau sans-fil (Wifi)

Le service technique de Lesquin permet d'assurer la maintenance de 35 véhicules simultanément. Les mécaniciens utilisent des tablettes numériques pour renseigner une application métier hébergée sur le serveur Lxd1. Cette application permet de connaître les opérations de maintenance, l'état des stocks de pièces de rechange et de visualiser les notices techniques.

La couverture du réseau sans-fil est réalisée par un contrôleur Wifi modèle WC7500 et 5 points d'accès modèle WAC720, reliés directement au contrôleur (en connexion filaire).

Le réseau Wifi permettant de connecter les tablettes n'autorise pas l'accès à internet. Le contrôleur est actuellement configuré de manière basique en ayant activé uniquement le mode WPA-PSK (*passphrase* - phrase secrète unique).

Le prestataire ADS a suggéré à Mme Carlier d'envisager l'utilisation d'un serveur RADIUS pour assurer l'authentification au réseau Wifi.

Le serveur nommé « Windows2016 », qui héberge l'annuaire Active Directory, assure également le rôle de serveur d'authentification de type RADIUS (via le service NPS – *Network Policy Server*). Les mécaniciens qui utilisent le réseau sans-fil, pourraient donc être authentifiés par le serveur RADIUS à l'aide de leur compte sur l'annuaire Active Directory.

Question A3.1

Déterminer quels sont les avantages d'utiliser un serveur RADIUS associé au service Active Directory.

L'authentification par serveur RADIUS étant maintenant configurée, Mme Carlier vous demande de renforcer la sécurité du réseau sans-fil et notamment de déterminer la configuration optimale pour le contrôleur Wifi.

Question A3.2

Lister au moins deux autres mesures qui doivent être prises pour que le réseau Wifi de Lesquin soit davantage sécurisé.

Le serveur nommé « Debian10 » assure le service de journalisation *syslog*. Ce service centralise les journaux d'événements de l'ensemble des serveurs (Windows et Linux) et des équipements actifs. Le contrôleur Wifi transmet en temps réel l'ensemble de ses journaux vers le service *syslog*.

Mme Carlier veut vérifier que la collecte des données à caractère technique dans les journaux est conforme à la réglementation.

Question A3.3

Indiquer les obligations réglementaires françaises et/ou européennes concernant la conservation des données à caractère technique des journaux du contrôleur Wifi.

Madame Carlier se demande s'il est possible de mettre en place un accès Wifi vers internet pour les visiteurs, sans compromettre la sécurité du réseau et sans modifier les obligations réglementaires.

Vous proposez la mise en place d'un portail captif avec utilisation de bons d'échange (*vouchers*). Les bons d'échange du Wifi seront remis à l'accueil contre l'adresse électronique, le nom et la société du visiteur.

Question A3.4

Expliquer les contraintes que l'utilisation d'un système de « bons d'échange » va engendrer en termes de réglementation et de sécurité.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 5 sur 16

DOSSIER B : SÉCURISATION DES SERVEURS ET DES SERVICES

Les informaticiens de l'entreprise assurent quotidiennement une veille informatique concernant les vulnérabilités qui peuvent survenir en surveillant les services et les fonctionnalités installés sur les serveurs afin de prendre les mesures de sécurisation nécessaires.

Le prestataire ADS a également réalisé des audits sur la plupart des serveurs. Des améliorations de la sûreté et de la sécurité des serveurs ainsi que de nouvelles procédures d'utilisation des services à destination des salariés doivent être mises en place.

Mission B.1 – Amélioration de la sûreté du serveur de stockage

Mme Carlier vous demande d'analyser et de proposer des améliorations au système de sauvegarde de l'entreprise.

Le serveur de stockage en réseau (NAS – *network attached storage*) RS2418RP est équipé de 12 disques de 2 To configurés de façon à répartir les données (configuration RAID niveau 0). Il est utilisé pour faire des sauvegardes régulières de toutes les applications, machines virtuelles et fichiers journaux (*logs*) de l'entreprise. La quantité de données stockées avoisine actuellement 18 To.

Question B1.1

- a) Indiquer pourquoi la configuration en RAID niveau 0 n'assure pas la sûreté des données.
- b) Proposer le niveau RAID à utiliser sur le serveur NAS qui assurerait la meilleure sûreté tout en répondant aux contraintes de volume. *Vous justifierez votre réponse notamment par le calcul du volume utile.*

Le serveur « Windows2016 » stocke ses données sur une grappe locale de disques configurée en RAID niveau 5, composée de 3 disques de 4 To.

Question B1.2

Expliquer pourquoi il est nécessaire de faire des sauvegardes du serveur « Windows2016 » vers le serveur NAS.

Le serveur NAS étant situé dans le même local que les autres serveurs, il serait souhaitable d'avoir une sauvegarde du serveur NAS sur un serveur éloigné physiquement de Lesquin.

Pour cela, vous proposez la location d'un serveur dédié chez l'hébergeur français PWI.

Question B1.3

Donner au moins un élément juridique et un élément technique à Mme Carlier qui justifient le choix d'un hébergeur français.

Les serveurs proposés par l'hébergeur PWI permettent d'utiliser les protocoles de communication suivants : HTTP, HTTPS, FTP, FTPS, SFTP, SSH, SCP

Question B1.4

Proposer un protocole sécurisé pour transférer les données entre Lesquin et la nouvelle solution de stockage. *Justifier la réponse.*

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 6 sur 16

Mission B2 – Mise en place de délégation de droits

Des délégations de droits doivent être mises en place sur les différents serveurs sous Linux. Cela permettra à chaque personne du service informatique de réaliser des tâches d'administration sur les différents serveurs (gestion d'un service, modification de la configuration réseau d'une machine, installation de paquets, etc.) en se connectant avec son propre compte utilisateur. Cela contribue au principe de moindre privilège².

Ces délégations pourraient être gérées à l'aide de l'utilitaire *sudo*. Mme Carlier vous charge d'étudier la pertinence de cette solution.

Question B2.1

Expliquer en quoi l'utilisation de l'utilitaire *sudo* permet de contribuer au principe du moindre privilège.

L'utilitaire *sudo* a fait l'objet de plusieurs vulnérabilités, dont une est décrite dans le dossier documentaire.

Question B2.2

- a) Expliquer les risques liés à la faille de sécurité CVE-2019-14287 décrite dans le dossier documentaire.
- b) Indiquer les machines potentiellement concernées par cette faille de sécurité pour l'entreprise.

La faille de sécurité décrite peut être corrigée en appliquant la mesure préconisée à savoir la mise à jour vers la dernière version de l'utilitaire.

Un script a été récupéré sur le site *web* officiel de l'utilitaire *sudo*. Avant de l'exécuter, madame Carlier vous demande de vérifier les actions de ce script.

Question B2.3

Expliquer l'utilité des lignes 3, 4 et 5 du script.

Mission B3 – Sécurisation de la messagerie

La pandémie de Covid-19 a obligé plusieurs salariés des services administratifs à travailler à distance. Un ordinateur portable de l'entreprise leur a été remis afin qu'ils poursuivent leur activité professionnelle. La communication a été basée principalement sur la messagerie électronique.

Actuellement, le service de messagerie est sécurisé par un chiffrement de type TLS entre le client et le serveur de messagerie.

Une réflexion est menée pour vérifier le niveau de sécurité de ce service.

Question B3.1

- a) Préciser l'intérêt d'une sécurisation des échanges entre un client de messagerie et un serveur de messagerie en utilisant le protocole TLS.
- b) Indiquer si, en cas de vol de l'identifiant et du mot de passe de messagerie d'un salarié, la protection du contenu des courriels est garantie avec la seule utilisation du protocole TLS.
Justifier la réponse

Il a été décidé de renforcer la sécurité du service de messagerie par la mise en place d'un chiffrement des courriels. Dans un contexte de transport routier très concurrentiel, cette évolution est essentielle pour l'entreprise.

Chaque salarié(e) s'est vu remettre une procédure concernant le chiffrement des courriels.

Vous devez préparer une réunion pour expliquer cette évolution à la direction de l'entreprise.

Question B3.2

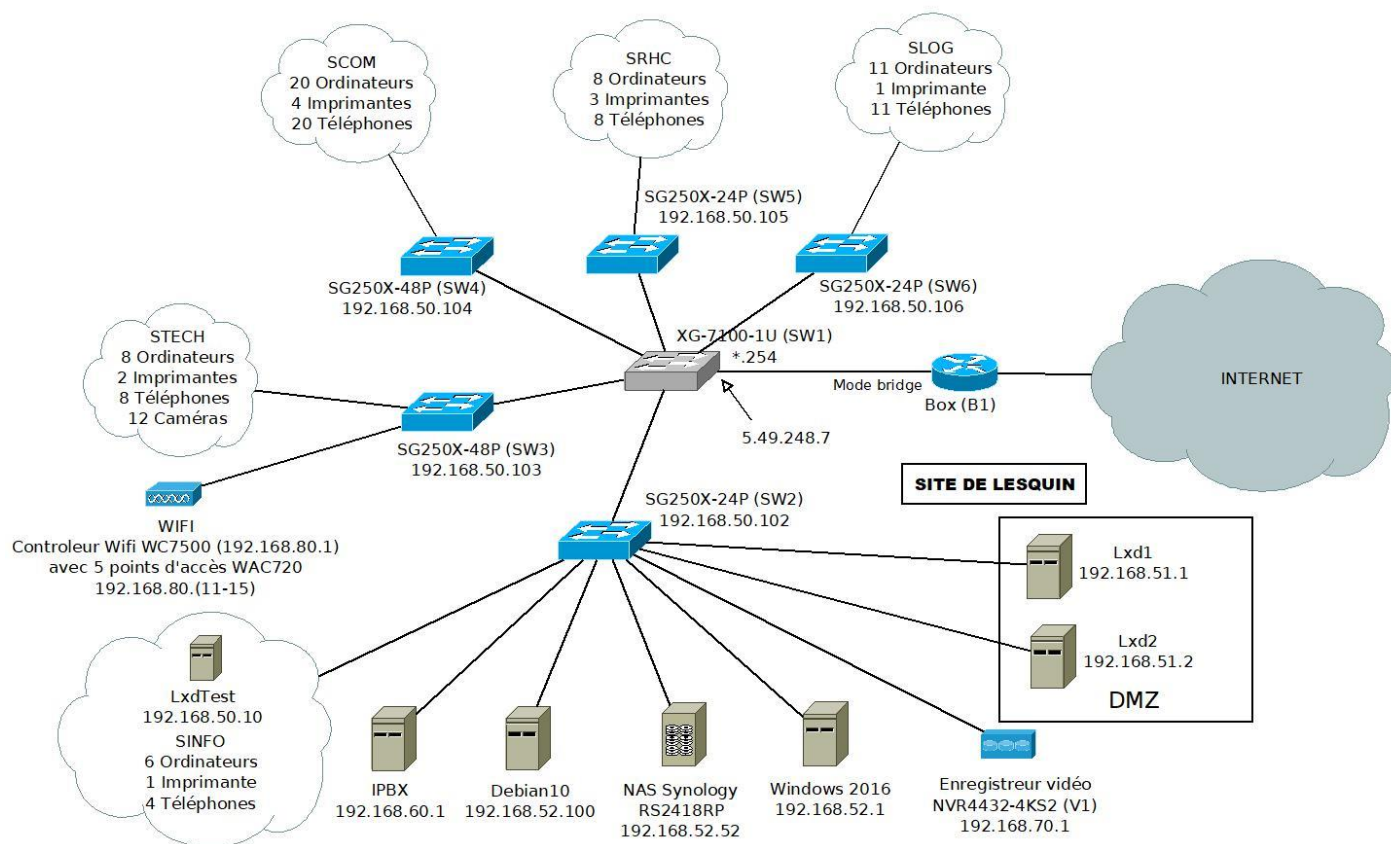
Citer les objectifs remplis en termes de sécurité par le chiffrement des courriels par rapport à la solution précédente.

² Le principe de « moindre privilège » implique de restreindre les droits d'accès d'un utilisateur précis dans l'entreprise, afin qu'il n'ait accès qu'à ce qui lui est nécessaire pour effectuer son travail. (source : <http://blog.wallix.com/fr/principe-de-moindre-privilège>).

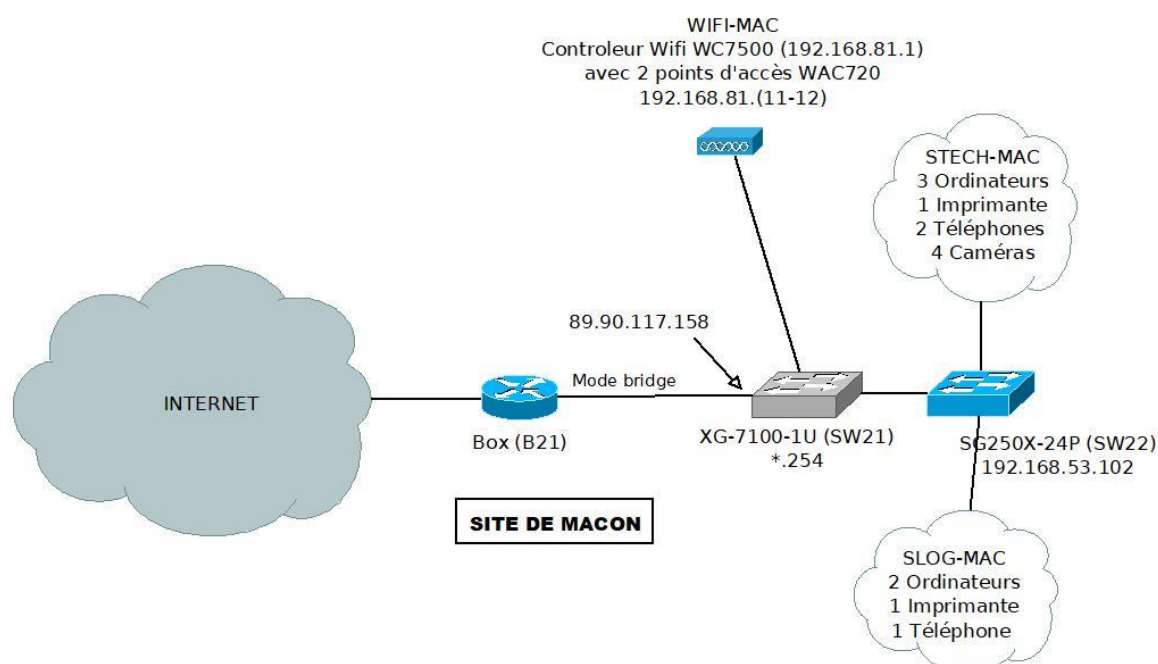
DOSSIER DOCUMENTAIRE

Documents communs à tous les dossiers

Document 1 : Schéma du réseau du site de Lesquin



Document 2 : Schéma du réseau du site de Mâcon



Document 3 : Description de l'infrastructure réseau de la société Benoit Myon

L'entreprise utilise de nombreux réseaux locaux virtuels (VLAN) pour segmenter le réseau. La relation entre ces différents réseaux locaux virtuels est assurée par la partie routeur/pare-feu (*firewall*) des équipements de sécurité XG-7100-1U ; ces équipements sont en effet multifonctions, à la fois commutateur, routeur et pare-feu.

Les autres commutateurs SG250X-24P ou SG250X-48P sont des simples commutateurs administrables de niveau 2, munis de ports avec alimentation électrique par câble Ethernet (*power over Ethernet* - PoE) pour la téléphonie. Ces commutateurs sont capables de gérer des réseaux locaux virtuels (VLAN).

L'accès fibre à internet se fait via des boîtiers d'opérateurs (*box*). Le débit fourni par ces équipements ne descend jamais en dessous de 400 Mbps symétrique.

Les boîtiers sont connectés en mode pont³ sur les commutateurs XG-7100-1U. L'adresse IP publique faisant partie du réseau étendu (WAN) est donc configurée directement sur ceux-ci.

Les caméras sont connectées par réseau filaire.

Un réseau privé virtuel (VPN) sous forme de tunnel IPsec (*internet protocol security*)⁴, géré par les équipements XG-7100-1U, permet d'établir une liaison sécurisée entre les sites de Lesquin et de Mâcon.

L'adressage dynamique est assuré par les équipements XG-7100-1U, par l'intermédiaire d'une réservation d'adresse pour chaque client.

Document 4 : Principe d'adressage des réseaux locaux virtuels (Lesquin et Mâcon)

Id	Désignation	VLAN	Réseau	Commutateurs
SLOG	Service logistique de Lesquin	10	192.168.10.0/24	SW1-6
SLOG-MAC	Service logistique de Mâcon	11	192.168.11.0/24	SW21-3
SCOM	Service commercial (Lesquin)	20	192.168.20.0/24	SW1-4
STECH	Service technique de Lesquin	30	192.168.30.0/24	SW1-3
STECH-MAC	Service technique de Mâcon	31	192.168.31.0/24	SW21-3
SRHC	Ressources Humaines et comptabilité	40	192.168.40.0/24	SW1-5
SINFO	Service informatique de Lesquin	50	192.168.50.0/24	SW1-2
SINFO-DMZ	DMZ	51	192.168.51.0/24	SW1-2
SINFO-LAN	SERVEURS	52	192.168.52.0/24	SW1-2
SINFO-MAC	Service informatique de Mâcon	53	192.168.53.0/24	SW21-3
TEL	Téléphonie de Lesquin	60	192.168.60.0/24	SW1-2, SW1-3, SW1-4, SW1-5, SW1-6
TEL-MAC	Téléphonie de Mâcon	61	192.168.61.0/24	SW21-3
VIDEO	Caméras vidéo de Lesquin	70	192.168.70.0/24	SW1-2, SW1-3
VIDEO-MAC	Caméras vidéo de Mâcon	71	192.168.71.0/24	SW21-3
Wifi	Wifi de Lesquin	80	192.168.80.0/24	SW1-3
Wifi-MAC	Wifi de Mâcon	81	192.168.81.0/24	SW21-2
WAN	Entrée/Sortie vers Internet	4090		SW1-1, SW21-1

L'adresse de passerelle de chaque réseau local virtuel (VLAN) est la dernière adresse hôte disponible sur chaque réseau.

³ En anglais *bridge*, le pont d'un boîtier opérateur (*Box*) permet de transmettre directement les trames (niveau 2) sans utiliser la fonction de routage.

⁴ IPsec est un ensemble de protocoles utilisant des algorithmes permettant le transport sécurisé sur un réseau.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 9 sur 16

Documents associés au dossier A

Document A1 : Commutateur / Passerelle de sécurité XG-7100-1U

Détails de la partie commutateur

- Compatible 802.1Q
- 2 ports 10 Gbps (Intel)
- 8 ports 1 Gbps (Marvell)
- 2 ports cachés sont reliés à la partie routeur/firewall, via un agrégat de liens à 5 Gbps (lagg0)
- Par défaut, le port eth1 est configuré comme un port de réseau étendu - WAN.



Détail de la partie routeur – pare-feu (*firewall*)

- Mémoire de 8 Go extensible jusqu'à 24 Go.
- Stockage du système d'exploitation sur une carte eMMC de 32 Go. Ajout d'un disque M.2 possible.
- Administration via un port USB, un accès SSH, ou une interface HTTPS.
- Solution complète de routage inter-VLAN.
- Services réseau : DNS, DHCP, VPN. Possibilité d'ajouter des paquets logiciels complémentaires.
- Pare-feu : Filtrage sur les différents réseaux et/ou les différents VLAN. Enregistrement des journaux.

Document A2 : Règles de redirection de port NAT (*port forwarding*) du commutateur SW1

Interface	Protocole	Adresse source	Port source	Adresse destination	Port destination	Adresse NAT	Port NAT
eth1	tcp	*	*	5.49.248.7	80	192.168.51.1	80
eth1	tcp	*	*	5.49.248.7	443	192.168.51.1	433
eth1	tcp	*	*	5.49.248.7	5433	192.168.51.1	5000

Document A3 : Règles de pare-feu (*firewall*) coté externe (WAN) du commutateur SW1

Numéro	Protocole	IP source	Port source	IP destination	Port destination	Règles
10	tcp	*	*	192.168.51.1	80	allow
20	tcp	*	*	192.168.51.1	443	allow
30	tcp	*	*	192.168.51.1	5000	allow
9999	*	*	*	*	*	deny

Document A4 : Modèle de fiche de signalisation d'incident (document ITIL)

ÉLÉMENT CONCERNÉ PAR L'INCIDENT :

[i1] Serveur	[i7] Système d'exploitation
[i2] Poste de travail	[i8] Messagerie
[i3] Tablette	[i9] Navigateur web
[i4] Imprimante	[i10] Logiciel bureautique
[i5] Équipement de réseaux	[i11] Autre :
[i6] Logiciel métier	

NATURE DE L'INCIDENT :

[n1] Perte de service ou de fonctionnalités.	[n14] Perte accidentelle des fichiers journaux (logs)
[n2] Mauvais fonctionnement du système.	[n15] Erreur pendant le processus de saisie
[n3] Mauvais fonctionnement d'un logiciel.	[n16] Arrêt d'un logiciel critique dû à un bug
[n4] Mauvais fonctionnement du matériel.	[n17] Vol d'équipement informatique
[n5] Dégradation de performances du réseau.	[n18] Vol ou altération d'un support amovible
[n6] Détection d'un virus.	[n19] Vol de documents (ou de fichier)
[n7] Antivirus désactivé ou non à jour.	[n20] Tentative de cyberattaque
[n8] Violation d'un droit d'auteur (ou d'une licence).	[n21] Fonctionnement défectueux d'un logiciel
[n9] Divulgence des données confidentielles	[n22] Dégradation du service internet
[n10] Divulgence d'informations relatives à la vie privée	[n23] Saturation d'un système (disque\mémoire)
[n11] Accès non autorisé	[n24] Autre :
[n12] Harcèlement par courriel (spam)	
[n13] Modification accidentelle ou malveillante d'un fichier partagé	

En cas d'activités illégales, de menaces ou harcèlement, le service Ressources Humaines a-t-il été contacté ?

[r1] Oui	[r2] Non	[r3] Ne s'applique pas
------------	------------	--------------------------

Des données sensibles ou critiques ont-elles été compromises ?

[c1] Oui	[c2] Non	[c3] Ne s'applique pas
------------	------------	--------------------------

Quelles mesures ont été appliquées dans l'urgence ?

[u1] Aucune	[u5] Redémarrage de l'équipement
[u2] Déconnexion du réseau	[u6] Sauvegarde des données
[u3] Déconnexion du courant électrique	[u7] Autre :
[u4] Balayage du disque dur avec l'antivirus Client	

Document A5 : Assignment des ports du commutateur SW2 (extrait)

N° port	Équipement connecté	N° VLAN	Mode
1	IPBX	60	Non étiqueté
2	Debian10	52	Non étiqueté
3	NAS Synology	52	Non étiqueté
4	Windows2016	52	Non étiqueté
5	Enregistreur vidéo	70	Non étiqueté
6	LxdTest	50	Non étiqueté
...			
21	Lxd1	51	Non étiqueté
22	Lxd2	51	Non étiqueté
23	Debian Snort	51	Non étiqueté
24	SW1	*	802.1q (Étiqueté)

Document A6 : IDS Outil de détection d'intrusions - Snort

Les outils de détection d'intrusions (IDS) permettent de détecter les attaques/intrusions du réseau sur lequel ils sont placés. Ce sont des outils complémentaires aux pare-feux, scanners de failles et anti-virus.



Les outils de détection d'intrusions réseaux (*Network IDS*) analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (exemple : carte réseau en mode promiscuité - *promiscuous*). Ensuite, les paquets sont décortiqués puis analysés. En cas de détection d'intrusion, des alertes peuvent être envoyées.

Pour effectuer ces analyses, la solution Snort se fonde sur des règles. Cette solution est fournie avec certaines règles de base, cependant il est souhaitable d'écrire des règles complémentaires.

Les règles Snort officielles portent un identificateur unique (nombre entre 1 et 1 000 000). La première règle personnelle doit donc avoir l'identificateur 1 000 001.

Exemple de règle

`alert tcp 19.7.1.1 any -> 192.168.1.0/24 80 (msg:"Ceci est un test"; sid:1000001; rev:1;)`

En tête

alert	Action de la règle (alert)
tcp	Protocole qui est analysé (tcp, udp, icmp)
19.7.1.1	Adresse source (adresse IP, réseau ou any)
any	Port source (numéro de PORT ou any)
->	Direction. De la source vers la destination ("->" ou "<-")
192.168.1.0/24	Adresse destination (adresse IP, réseau ou any)
80	Port destination (numéro de PORT ou any)

Options

msg:"Ceci est un test"	Message qui est remonté en cas d'alerte.
sid:1000001	Identificateur unique de la règle.
rev:1	Numéro de version

Document A7 : Contrôleur Wifi WC7500

CONFIGURATION IP ET VLAN

Serveur/relais DHCP :

- Serveur DHCP intégré.
- Plusieurs serveurs/pools DHCP peuvent être ajoutés pour divers VLAN (jusqu'à 64).

VLAN pour le contrôleur Wifi :

- Un VLAN d'administration (ID VLAN configurable).



SÉCURITÉ Wifi

Protocoles d'authentification client :

- Ouvert, WEP, WPA/WPA2-PSK.
- Protocoles 802.11i/WPA/WPA2 professionnels avec interface standard vers serveur AAA/RADIUS.
- ACL MAC basées sur le serveur AAA local ou le serveur Radius externe.

Portail captif :

- Portail captif intégré disponible pour l'authentification client dans un profil sécurisé.
- Mode d'authentification par mot de passe : base d'utilisateurs locaux disponible, nom d'utilisateur/mot de passe attribués par un réceptionniste virtuel.
- Mode serveur Radius externe : authentification RADIUS externe pour les clients du portail captif.
- Mode bon d'échange : inscription des invités par adresse électronique. Les informations saisies (nom, adresse de courriel, nom de société) sont conservées localement.
- Extraction des journaux d'activité invité.

ADMINISTRATION

Interface d'administration :

- HTTP, SNMP v1/v2c, Telnet, Secure Shell (SSH).

Journalisation et génération de rapports :

- Enregistrement des événements de connexion/déconnexion aux points d'accès Wifi (date/heure, adresse MAC de l'hôte, mode de connexion).
- Si un serveur Syslog est présent sur le réseau, le contrôleur Wifi peut envoyer tous les journaux. Les journaux sont également disponibles et téléchargeables via l'interface utilisateur (fichier d'exportation de journal).

Document A8 : Conservation des données techniques de connexion

Conservation des journaux (logs) : la législation en la matière

Selon la loi concernant les journaux (logs) dans l'article 6 II, décrétee le 24 mars 2006, pour les FAI, l'obligation de préserver les données est valable pour une durée optimale d'un an. Au-delà de ce délai, ces données peuvent être anonymisées.

Qui est concerné par la conservation des journaux (logs) ?

Les institutions concernées par cette conservation sont tout d'abord **les fournisseurs d'accès internet ou FAI**, ainsi que les hébergeurs. Selon la loi antiterroriste du 23 janvier 2006, cette obligation ne concerne pas uniquement les FAI, mais est aussi applicable à toute personne physique ou morale qui procure un accès internet. Et ce, même s'il s'agit d'un accès octroyé à titre gratuit.

Source : The Bodyguard Magazine

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 13 sur 16

Documents associés au dossier B

Document B1 : Serveur NAS RS2418RP

Général

Type de périphérique Serveur NAS
Connectivité hôte Gigabit Ethernet

Extension/connectivité

Baies d'extension 12 x échangeable à chaud - 2.5" / 3.5"

Réseaux

Protocole de liaison
de données 10Mb LAN, 100Mb LAN, GigE

Protocole réseau /
transport PPTP, L2TP, iSCSI, FTP, NFS

Compatibilité des services
réseau Microsoft Active Directory (AD), système de fichiers *Internet standard Microsoft* (SMB), système de fichiers distribués NFS, FTP, protocole AFP, *Web-based Distributed Authoring and Versioning* (WebDAV), *Calendaring Extensions to WebDAV* (CalDAV)

Caractéristiques Prise en charge du protocole LDAP, *wake on LAN* (WOL), prise en charge de Syslog, analyse antivirus, serveur vidéo, assistance *Access Control List* (ACL), serveur de messagerie, station de surveillance, sauvegarde sur *cloud*, serveur VPN

Protocole de gestion à
distance SNMP, Telnet, SSH

Protocoles sécurisés TLS

Contrôleur de stockage

Type RAID

Type d'interface SATA 6Gb/s

Niveau RAID RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, JBOD



Document B2 : Niveaux RAID

Raid	nb. de disques	tolérance de panne	capacité perdue
0	2 mini.	aucune	aucune
1	2	1 disque	50%
5	3 mini.	1 disque	1 disque
6	4 mini.	2 disques	2 disques
10	4 mini.	1 disque par Raid 1	50%
Jbod	2 mini.	aucune	aucune

Document B3 : Présentation de l'utilitaire sudo

(Extrait du guide de l'ANSSI RECOMMANDATIONS DE SÉCURITÉ RELATIVES À UN SYSTÈME GNU/LINUX)

Sudo est un utilitaire installé lorsqu'il y a un besoin de déléguer des droits et privilèges à différents utilisateurs. Cette délégation repose sur la possibilité pour un utilisateur donné d'exécuter une commande préalablement définie avec les privilèges d'un autre utilisateur. Il est donc important de se préoccuper de sa sécurité au niveau de sa configuration, car le fait de donner le droit à un utilisateur d'exécuter certaines commandes peut lui attribuer plus de privilèges et de prérogatives qu'initialement nécessaires.

Voici le contenu du fichier `/etc/sudoers.d/INFO` qui définit les délégations attribuées aux informaticiens :

```
User_Alias INFO = adumas, msix
Cmnd_Alias NET = NOEXEC: sudoedit /etc/network/interfaces, sudoedit /etc/resolv.conf, /sbin/ifup, /sbin/ifdown
INFO SRV1 = (root) NET
```

User_Alias : on regroupe un ensemble d'utilisateurs sous le nom INFO comprenant les comptes utilisateurs « adumas » et « msix ».

Cmnd_Alias : on regroupe un ensemble de commandes en attribuant un alias (ici **NET**). Dans cet exemple, ces commandes permettent de modifier la configuration réseau d'un serveur. On précise les chemins absolus des commandes. **NOEXEC** : empêchera le contournement de la politique de sécurité, en empêchant le lancement d'un environnement *shell* d'échappement (invite de commande).

INFO SRV1 = (root) NET signifie qu'on autorise les utilisateurs définis dans l'alias INFO (adumas et msix) à modifier la configuration réseau du serveur, si la commande est exécutée sur le serveur **SRV1**. Les utilisateurs « adumas » et « msix » pourront exécuter les commandes définies dans l'alias **NET** et ils les exécuteront avec les droits de l'administrateur « root », qui est le compte administrateur du système.

Remarques :

- **sudoedit** est un éditeur de texte.
- **interfaces** est le fichier de configuration des interfaces réseau pour certaines distributions telle que Debian GNU/Linux.
- **resolv.conf** est le fichier contenant l'adresse du ou des serveurs DNS.
- **ifdown** et **ifup** sont deux commandes sous Linux à exécuter successivement pour recharger la configuration d'une carte réseau.

Pour pouvoir exécuter la commande **ifdown** par exemple, l'utilisateur « adumas » doit préfixer la commande par l'instruction **sudo** :

```
adumas@SRV1:~$ sudo ifdown enp0s3
[sudo] password for adumas:
```

L'utilisateur « adumas » saisit son mot de passe personnel pour pouvoir prendre les droits administrateur « root » le temps de l'exécution de la commande **ifdown** qui va désactiver la carte réseau.

Il est également possible de mettre en place une journalisation : chaque utilisateur lançant des commandes d'administration avec son propre compte, celles-ci sont enregistrées et on peut ainsi savoir qui a lancé quelle commande et à quel moment.

Exemple d'évènements enregistrés sur le serveur SRV1 :

```
mai 11 11:08:46 2020 : adumas : TTY=/dev/pts/0 ; CWD=/home/adumas ; USER=root ;
TSID=000003 ; COMMAND=sudoedit /etc/resolv.conf
mai 11 11:10:43 2020 : msix : TTY=/dev/pts/0 ; CWD=/home/msix ; USER=root ;
TSID=000005 ; COMMAND=/sbin/ifdown enp0s3
```

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 15 sur 16

Document B4 : Vulnérabilité de l'utilitaire sudo

(Extraits du site [sudo.ws](https://www.sudo.ws))

Vulnérabilité référencée CVE-2019-14287 : CVE (*Common Vulnerabilities and Exposures*) est une liste des vulnérabilités publiquement connues, relatives à la cyber sécurité. Chaque vulnérabilité est référencée par un identifiant standardisé de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro d'identifiant) constituant une référence mondiale.

Dans les versions de sudo jusqu'à la version 1.9, un attaquant pouvait contourner la politique de sécurité en lançant la commande sudo de la façon suivante : `sudo -u#-1 commande`. Ici, l'utilisateur d'identifiant -1 n'existe pas, mais cela permettait, avec les versions de sudo antérieures à la 1.9, de lancer une commande avec des droits de l'administrateur root. Cette faille de sécurité a été corrigée, une mise à jour de la version installée de sudo est donc à effectuer. Une façon plus sûre de remédier à cette faille est l'installation de la dernière version de l'utilitaire disponible à cette adresse :

https://www.sudo.ws/sudo/dist/packages/1.9.3p1/sudo_1.9.3-2_amd64.deb

<https://www.sudo.ws/sudo/dist/packages/1.9.3p1/> est l'adresse du serveur en ligne.

`sudo_1.9.3-2_amd64.deb` est le nom du fichier à télécharger et à installer.

Document B5 : Script de mise à jour de sudo

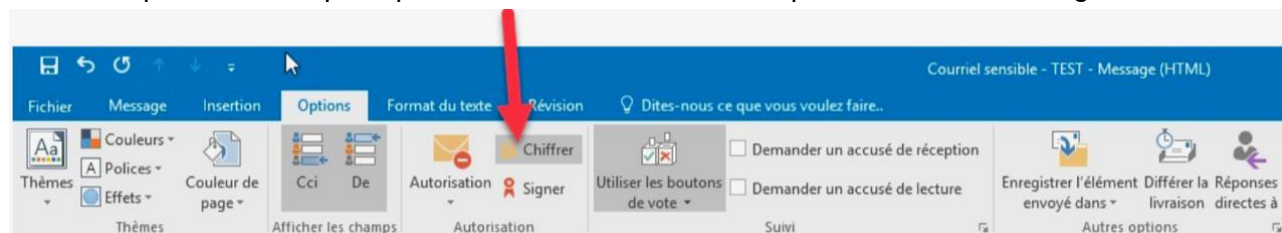
N° ligne	Instruction sous Linux	Commentaire
1	<code>version=\$(sudo -V head -1 cut -d" " -f4 cut -d"." -f2)</code>	Extrait le deuxième chiffre de la version de sudo (8 si la version est 1.8.21p2) et l'affecte à la variable « version ».
2	<code>if [\$version -le 8]; then wget https://www.sudo.ws/sudo/dist/packages/1.9.3p1/sudo_1.9.3-2_amd64.deb; fi</code>	
3	<code>empreinteAttendue="fcb3dc908d04fc2630d441958c0149c4e5acbe dc43f0aa01a7173af363d24b2e"</code>	
4	<code>empreinteFichierTéléchargé=\$(sha1sum sudo_1.9.3-2_amd64.deb)</code>	
5	<code>if [\$empreinte -eq \$empreinteCalculée]; then dpkg -i sudo_1.9.3-2_amd64.deb; fi;</code>	

wget : télécharger un ensemble logiciel (package).

dpkg -i installer un package.

Document B6 : Procédure de chiffrement des courriels

Le client de messagerie utilisé est le logiciel Outlook. L'expéditeur choisit son destinataire dans l'annuaire LDAP de l'entreprise et avant d'envoyer son courriel, il clique sur le bouton **Chiffrer** présent dans les options. La clé publique du destinataire est utilisée pour chiffrer le message.



Le destinataire reçoit le courriel chiffré sur son client de messagerie. Sa clé privée est nécessaire pour lire le contenu du courriel. Cette clé privée est présente sur son **badge d'identification personnelle** (chaque salarié dispose d'une carte à puce BIP). S'il ne présente pas sa carte, le courriel ne pourra pas être lu.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS – Option A	SESSION 2022
U6 – Cybersécurité des services informatiques	Durée : 4 heures
Code sujet : 22SI5SISR-NC	Page 16 sur 16