

Informers les utilisateurs et mettre en œuvre les défenses appropriées

COMPÉTENCES

- Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter
- Identifier les menaces et mettre en œuvre les défenses appropriées

SAVOIRS ASSOCIÉS

- Sécurité des terminaux utilisateurs et de leurs données : principes et outils
- La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique

Situation professionnelle

M. Brillat, le directeur de la MSAP, sollicite HDesk'63 pour identifier les failles de sécurité potentielles liées aux pratiques des utilisateurs du télécentre. Il souhaite également des recommandations sur les solutions techniques de défense des équipements.

M. Hiram, votre directeur, vous confie les différentes missions de ce projet. Vous êtes chargé(e) d'informer les utilisateurs de la MSAP sur les **risques** associés à l'utilisation des ressources numériques du télécentre. Vous devez également identifier les menaces inhérentes à l'utilisation du télécentre en vue d'apporter les défenses appropriées.



➤ Voir présentation générale, p. 83

Informers les utilisateurs sur les risques et promouvoir les bons usages à adopter





M. Brillat souhaite compléter la charte informatique en vigueur dans la MSAP. Il est en effet nécessaire d'y insérer une rubrique sur les bonnes pratiques numériques, afin d'informer les utilisateurs du SI sur les risques associés à son utilisation et promouvoir les bons usages à adopter. Votre première mission consiste à réaliser un diagnostic des menaces inhérentes à l'utilisation du SI de la MSAP, liées à l'authentification et aux pratiques courantes telles que la lecture des courriels et l'utilisation d'applications métiers. Dans un second temps, vous complétez la charte informatique de la MSAP en y intégrant une rubrique « Bonnes pratiques numériques ».

Travail à faire

Vous disposez du relevé d'informations réalisé d'après l'observation des activités journalières des utilisateurs du télécentre (documents 1 à 4).

1. Identifiez les situations qui peuvent constituer un risque pour le SI de la MSAP.

- >  Fiche savoirs technologiques 4
- >  Documents 1, 2, 3 et 4

Vos observations ont permis de mettre en évidence un certain nombre de failles de sécurité dans le SI. Vous proposez des solutions pour y remédier.

2. Précisez les bonnes pratiques à adopter par les utilisateurs du télécentre.

- >  Fiche savoirs technologiques 4
- >  Documents 5 et 6

3. Proposez des solutions pour limiter les risques de l'utilisation d'une messagerie.

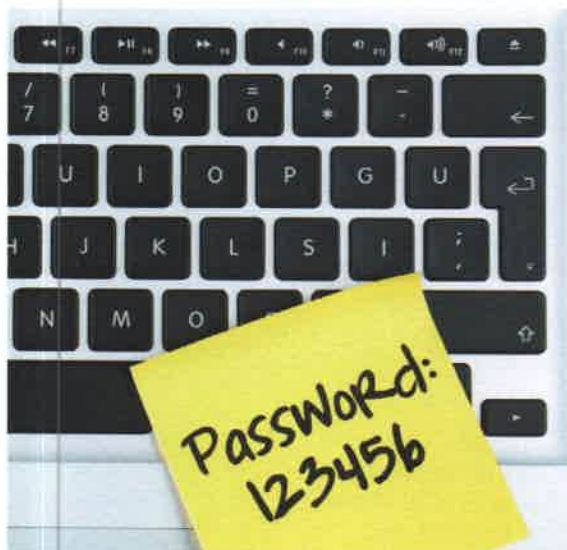
- >  Fiche savoirs technologiques 4
- >  Document 7

Un des axes de votre mission consiste à compléter la charte informatique de la MSAP en rédigeant la rubrique consacrée aux bonnes pratiques à adopter dans l'utilisation des outils numériques.

4. Rédigez la liste des points clés qui devront y figurer.

- >  Fiche savoirs CEJMA 6
- >  Document 8

Document 1 Le mot de passe utilisé par le prestataire Enedis



Document 2 La stratégie d'authentification pour accéder au SI de la MSAP

Les utilisateurs du SI de la MSAP qui désirent accéder aux services proposés par le télécentre doivent, dans un premier temps, réserver la ressource numérique souhaitée auprès de M. Jivon, l'administrateur réseau. Ce dernier intervient alors sur l'**Active Directory** (service centralisé d'identification et d'authentification pour un réseau d'ordinateurs utilisant le système Windows) pour créer un compte qui a pour identifiant le nom de l'organisme. À la première connexion, l'utilisateur est invité à modifier son mot de passe. Ainsi, pour toutes les prochaines réservations, l'intervenant possèdera ses données de connexion.

Document 3 Nomadisme et service BYOD dans le télécentre

BYOD (de l'anglais *Bring Your Own Device*) est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Les utilisateurs de la MSAP y sont autorisés dans le cadre de leurs missions. Dans ce cas, les partenaires (CLIC, MSA, etc.) sont en charge de la configuration de leurs applications.

M. Jivon n'a aucun moyen de vérifier la configuration de ces unités nomades. Si les partenaires de la MSAP souhaitent imprimer des documents, ils doivent les enregistrer sur un support amovible et se rendre au service reprographie pour l'impression. Un mot de passe leur est alors communiqué pour avoir accès à l'imprimante.



Missions professionnelles

Document 4 Un courriel reçu par la MSAP

La personne qui assure la permanence de la MSAP a cliqué sur le lien entouré ci-dessous.

De : Free@gmail.com
 À : permanence-marut@msap.fr
 Envoyé : Jeudi 11 décembre 202N 01.04.02
 Objet : Notification SZ27503S

free

Réf. : F4753898/26321908#0
 Votre identifiant abonné : 4753898

Paris, le 11/12/201N

Madame, Monsieur,

Il a été porté à notre attention que vos informations de facturation Freebox ne sont plus à jour. Pour cela nous vous prions d'accéder à votre espace personnel par le lien ci-dessous, et de mettre à jour toutes vos informations personnelles afin que vous aidiez à certifier votre compte.

Accédez à votre compte ici

Document 5 Un exemple de bonne pratique dans l'utilisation d'un mot de passe

Sur le site *How Secure Is My Password* (<https://howsecureismypassword.net>), la résistance du mot de passe **msap15** a été testé.

Le résultat de ce test indique :

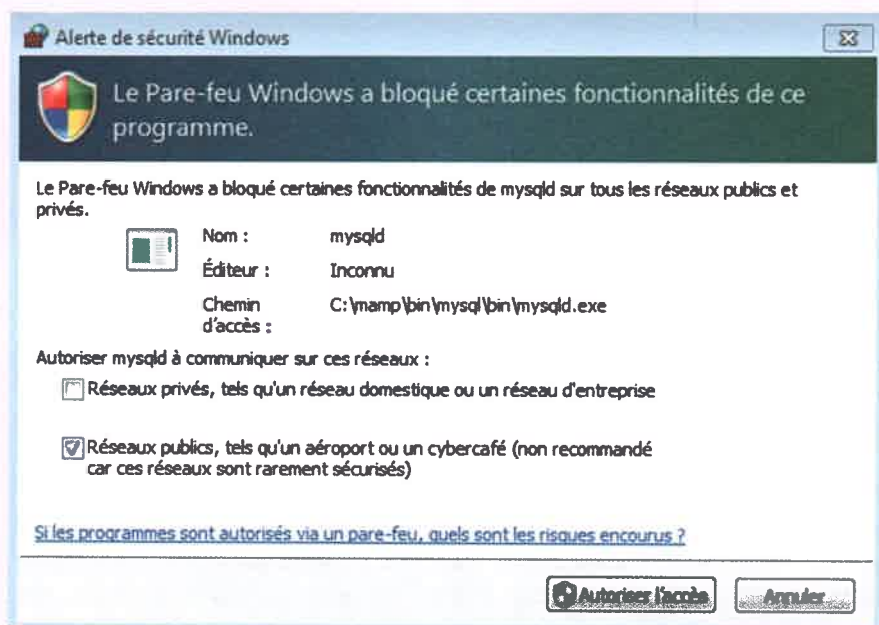


Un second test a été réalisé en ajoutant à ce mot de passe le caractère spécial « , » et en remplaçant le « a » par le signe « @ » : **Ms@p,1500**.



Document 6 Deux alertes de sécurité

Choisir la bonne réponse en cliquant sur le bouton approprié.



Fichier ouvert - Avertissement de sécurité

Nous ne pouvons pas vérifier l'identité du créateur de ce fichier.
Voulez-vous vraiment ouvrir ce fichier ?



Nom : Y:\Full Blu-Ray 2D 1\60 secondes chrono.iso

Type : Fichier ISO

De : Y:\Full Blu-Ray 2D 1\60 secondes chrono.iso

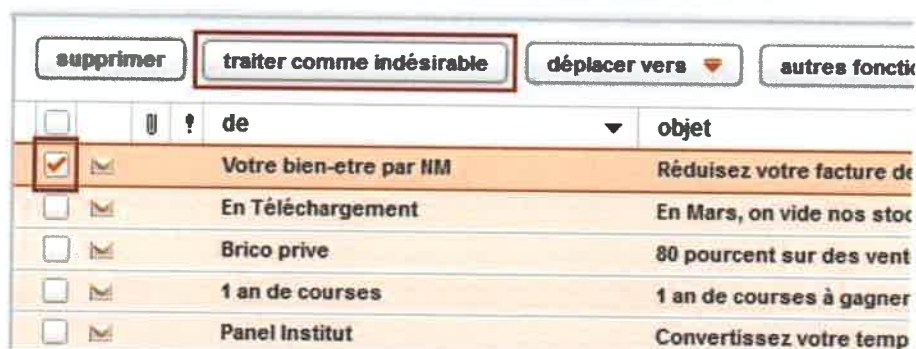


Ce fichier se trouve en dehors de votre réseau local. Les fichiers qui proviennent d'emplacements inconnus peuvent endommager votre PC. N'ouvrez ce fichier que s'il provient d'un emplacement approuvé.

[Quel est le risque encouru ?](#)

Document 7 Relevé d'utilisation d'une messagerie

Mme Asarchoun, chargée de clientèle à la MSAP, traite tous les jours les demandes d'informations de ses clients par courriel. Voici comment elle utilise sa messagerie professionnelle.



Document 8 Un extrait de la charte informatique de la MSAP

MSAP de la commune de Marut

Charte informatique

Introduction

Cette charte a pour vocation de présenter les bonnes pratiques à adopter au sein du système d'information de la MSAP et, plus particulièrement, au niveau du télécentre. Elle stipule les droits et devoirs de chaque utilisateur.

1. Ressources mises à disposition

Chaque utilisateur peut avoir accès à un espace de travail privatif ou collectif, avec une connexion Internet, un environnement bureautique Windows, un espace de reprographie et enfin une salle de visioconférence et de réunion. Un espace de stockage privatif est proposé sur le serveur de fichiers de la MSAP.

2. Les règles de sécurité en vigueur**a. Authentification sur les postes de travail**

Chaque utilisateur se voit attribuer un identifiant qui lui permettra de définir son mot de passe. L'identifiant est nominatif et ne peut être partagé avec un autre utilisateur. Le mot de passe est strictement confidentiel, le propriétaire est responsable de l'utilisation qui en est faite et s'engage à ne pas le communiquer à un tiers.

b. Configuration des environnements de travail

La configuration des postes de travail fournie dans les différents espaces de travail permet d'assurer la sécurité des utilisateurs et de leurs données. Il ne faut pas intervenir sur l'installation automatique des correctifs.

c. Environnement Internet

La connexion à certains sites pourrait fragiliser la sécurité du SI de la MSAP. Il faut donc être particulièrement vigilant dans la gestion de sa boîte de courriels professionnelle.

3. Conditions particulières liées à l'utilisation des outils nomades

L'utilisation des supports numériques personnels est autorisée. Cependant, leur configuration doit garantir la sécurité du SI de la MSAP. Ces supports ne doivent être utilisés que dans le cadre professionnel. Les téléchargements illicites sont interdits.

Je soussigné,, utilisateur des ressources numériques proposées par la MSAP de la commune de Marut, certifie avoir pris connaissance de la charte des bons usages de l'utilisation du SI de la MSAP, des droits et obligations qui en découlent et atteste que je suivrais les instructions précisées dans celle-ci.

Date :

Signature

Identifier les menaces et mettre en œuvre les défenses appropriées

Vous avez identifié un certain nombre de mauvaises pratiques qui provoquent des failles de sécurité et favorisent des attaques du SI. À la demande de M. Brillat, vous devez à présent apporter des solutions techniques pour protéger la MSAP.

Votre mission consiste à réaliser un diagnostic des moyens de défense déjà en place et à vérifier si les configurations sont adéquates. Vous disposez d'un relevé d'informations des configurations des postes de travail des bureaux de la MSAP, ainsi que de ceux relevant des pratiques BYOD.



Travail à faire

Dans un premier temps, vous réalisez un diagnostic des configurations actuelles.

1. Précisez la fonction de chacune de ces configurations.

- > Fiche savoirs technologiques 4
- > Documents 1, 2 et 3

Vos observations ont permis de mettre en évidence des failles de sécurité.

2. Identifiez les configurations à modifier pour garantir la sécurité du SI de la MSAP.

Le document 4 présente les différents outils installés sur quelques postes de travail de la MSAP. Vous préconisez à M. Brillat le déploiement de l'ensemble de ces outils sur tous les postes afin d'obtenir un parc homogène et plus sécurisé.

3. Analysez ces différents outils au regard des configurations étudiées précédemment en justifiant le rôle de chacun d'eux.

- > Fiche savoirs technologiques 4
- > Document 4

4. Précisez si l'ensemble de ces outils est nécessaire ou si certains peuvent être ignorés.

- > Fiche savoirs technologiques 4
- > Document 4

Même sensibilisés aux bonnes pratiques, les utilisateurs ne sont pas à l'abri d'une mauvaise manipulation ou d'une attaque malveillante. C'est pourquoi M. Brillat souhaite que vous lui proposiez un outil qui autorise ou non les connexions Internet vers certains sites. Il en a retenu deux, et vous demande votre recommandation.

5. Déterminez l'outil qui répond le mieux à la demande de M. Brillat. Justifiez votre réponse.

- > Fiche savoirs technologiques 4
- > Document 5

Dossier documentaire

Document 1 La sécurisation des connexions Internet

Voici des captures d'écrans de la configuration d'un poste de travail situé dans le bureau 4. Ce poste de travail est utilisé par les partenaires de la MSAP qui bénéficient d'une connexion Internet et d'un accès au réseau local pour la sauvegarde de leurs données.

Protection en temps réel

Ce paramètre permet d'identifier et d'empêcher l'installation ou l'exécution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement.

✗ La protection en temps réel est désactivée, ce qui rend votre appareil vulnérable.

☐ Désactivé

Protection dans le cloud

Offre une protection renforcée et plus rapide grâce à l'accès aux données de protection les plus récentes dans le cloud. Fonctionne de manière optimale une fois la soumission automatique d'échantillons activée.

☒ Activé

Notifications de protection contre les virus et menaces

Recevoir des notifications à caractère informatif

☐ Désactivé

- ☐ Activités récentes et résultats d'analyse
- ☐ Des menaces ont été détectées, mais aucune action immédiate n'est nécessaire
- ☐ Les fichiers ou les activités sont bloqués

Paramètres de protection contre les virus et menaces

Document 2 La sécurisation des connexions aux réseaux et des applications

Voici une capture d'écran de la configuration d'un poste de travail situé dans la salle multimédia. Ce poste de travail est utilisé par les partenaires de la MSAP lors de formations professionnelles, mais aussi par les utilisateurs du public lors des créneaux en accès libre.

Connexions entrantes

Bloque les connexions entrantes sur un réseau privé.

☐ Bloque toutes les connexions entrantes, y compris celles de la liste des applications autorisées.

☐ Désactivé

Contrôle des applications et du navigateur

Protection d'applications et sécurité en ligne.

Vérifier les applications et les fichiers

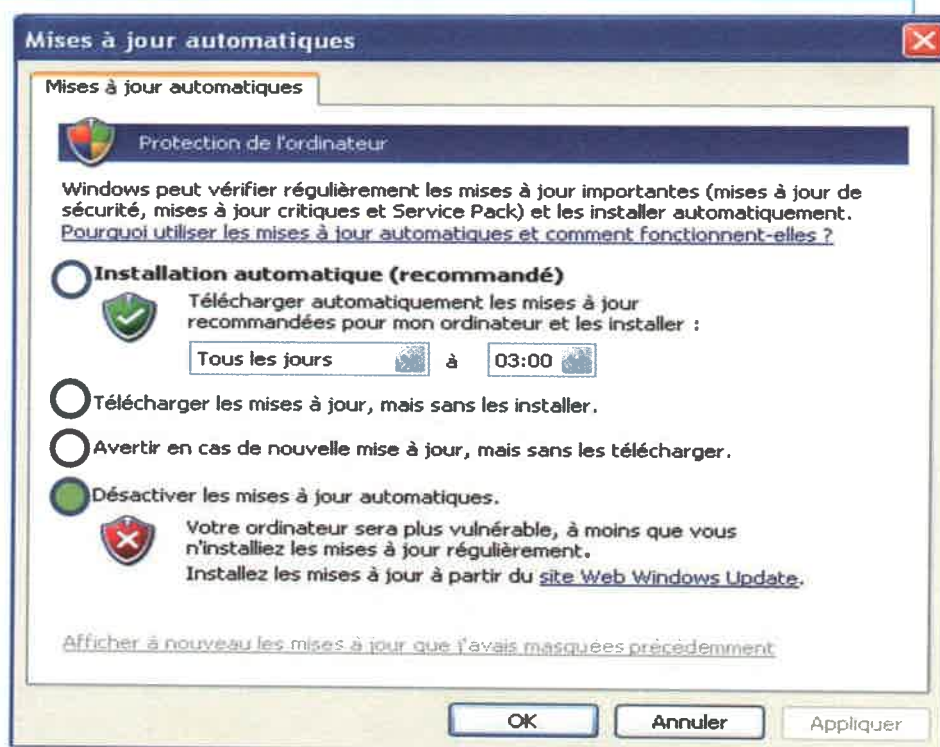
Le filtre Windows Defender SmartScreen aide à protéger votre appareil en recherchant les applications et les fichiers non reconnus à partir d'Internet.

⚠ La fonctionnalité Vérifier les applications et les fichiers est désactivée, ce qui rend votre appareil vulnérable. Ignorer

- ☐ Refuser
- ☐ Avertir
- ☒ Désactivé

Document 3 La configuration système d'un poste de travail nomade

Voici une capture d'écran de la configuration d'un ordinateur portable d'un partenaire utilisé en réseau avec le SI de la MSAP.



Document 4 Les outils de sécurisation d'un poste de travail

Voici la liste des outils potentiellement utilisables au sein du télécentre de la MSAP.



Document 5 Les deux outils retenus par M. Brillat



Proxy Switcher

Un **proxy** est un serveur vers lequel tout le trafic Web est aigüillé. Il contient une **base de données** qui bloque automatiquement la connexion à certains sites (*Accept* ou *Deny*). Ce serveur peut également être configuré pour appliquer des règles sur d'autres protocoles, comme FTP par exemple.

OpenDNS

OpenDNS Home Internet Security

OpenDNS Home Internet Security permet de bloquer certains contenus provenant d'Internet. En se connectant à un compte et en bloquant des catégories entières de contenus, à configurer ou à choisir selon ses besoins, on peut sécuriser les appareils connectés au réseau.

➤ Voir lexique BTS SIO, p. 221

1





Informez les utilisateurs sur les risques et promouvez les bons usages à adopter

>  Fiche savoirs technologiques 4

M. Brillat souhaite réaliser un audit sur la sécurité des identifiants de connexion pour s'assurer que la sensibilisation des utilisateurs a été efficace. Pour cela, il décide de faire réaliser des tests d'usurpation des éléments de connexion.
Pour réaliser cette tâche, vous devez disposer d'une machine virtuelle sous Windows 10 et d'une distribution Kali Linux (Free 2019, par exemple).


ÉTAPE 1 Préparation des tests

Plusieurs étapes sont préalables à la réalisation des tests : préparer les différents environnements de tests, récupérer la base **SAM** (Security Account Manager, « gestionnaire des comptes de sécurité ») et la sauvegarder dans un fichier.

1. Présentez le type d'audit que vous allez réaliser auprès de la MSAP.
>  Document 1
2. Préparez la machine virtuelle Windows de test en reprenant les éléments mentionnés dans le guide de configuration.
>  Document 2
>  Fiche méthode 3, p. 207
3. Configurez l'environnement de travail Kali et sauvegardez la partition Windows selon les différentes commandes indiquées.
>  Document 3

ÉTAPE 2 Première réalisation des tests

Votre environnement de travail est maintenant prêt. Vous allez réaliser deux types de tests (« **force brute** » et « **crackmap** ») qui vous permettront de trouver ou non les identifiants et mots de passe de chaque compte. Le compte administrateur sera également testé par défaut.

4. Exécutez les différents tests proposés par l'outil John the ripper. Pour cela, appuyez-vous sur les indications détaillées fournies.
>  Document 4
5. Notez les identifiants trouvés et tirez les conclusions qui en découlent.

ÉTAPE 3 Seconde réalisation des tests

6. Modifiez le mot de passe du compte Enedis afin de renforcer la sécurité de cette authentification.
7. Proposez, d'après vos observations, au moins un critère qui permette d'améliorer la sécurité des mots de passe.

> Voir lexique BTS SIO, p. 221

Document 1 L'audit et les tests de pénétration

White Hat		Grey Hat		Black Hat	
Le pentesteur travaille en étroite collaboration avec le DSI et l'équipe technique du SI. Il dispose de l'ensemble des informations.		Le test sera réalisé au départ avec un nombre limité d'information. On se place par exemple dans la situation où l'on est un utilisateur du SI.		Le testeur se met réellement dans la peau d'un attaquant externe et commence son test d'intrusion en ayant le moins d'information possible sur la cible.	

Document 2 Le guide de configuration de la machine virtuelle Windows de test

- 1 Sur la machine virtuelle Windows 10, s'authentifier avec le compte administrateur pour créer deux comptes supplémentaires :
 - ENEDIS, avec un mot de passe de moins de huit caractères alphanumériques (exemple : judo15) ;
 - MSA, avec un mot de passe de plus de huit caractères alphanumériques.
- 2 Indiquer dans les paramètres de la VM qu'au lancement de la machine virtuelle, le *boot* (démarrage) sera réalisé sur le lecteur de disque.
- 3 Choisir l'ISO de la machine virtuelle Kali comme support.

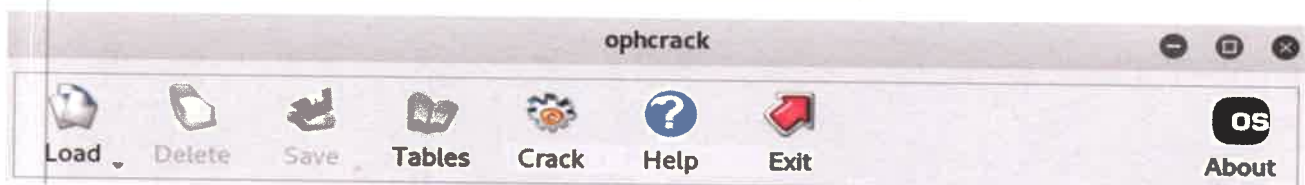
Document 3 La préparation de l'environnement Kali

Avant d'utiliser les différents outils proposés par la distribution Kali, il est nécessaire de réaliser plusieurs configurations :

- 1 Modifier le clavier QWERTY en AZERTY avec la commande `setxkbmap fr`.
- 2 Repérer la partition Windows avec la commande `fdisk -l`. Généralement, les différentes partitions sont représentées par le mot `sda` suivi d'un numéro. Il est probable que la partition la plus volumineuse soit celle recherchée. Noter le numéro de la partition, qui sera utile par la suite.
- 3 Monter la partition Windows identifiée précédemment dans Kali : `mount -t ntfs /dev/sdax /mnt` (où x représente le numéro de la partition et `mnt` le dossier de destination).
- 4 Avant de commencer les tests, il convient de récupérer les identifiants et mot de passe des différents utilisateurs stockés dans la base SAM : elle contient les identifiants des comptes utilisateurs ainsi que leur mot de passe sous forme de haches - algorithme MD5.

Avec l'outil **OPHCRACK** :

- Bouton **LOAD** → Encrypted SAM → `mnt\Windows\System32\Config`



- Bouton **SAVE** → `\mnt\mdp.txt`

➤ Voir lexique BTS SIO, p. 221

Document 4 Tests à l'aide de l'outil John the Ripper

John the Ripper permet de tester la robustesse des mots de passe en utilisant plusieurs types d'attaques :

- à l'aide d'un dictionnaire ou Wordlist, qui correspond à un fichier avec un ensemble de mot de passe prédéfinis ;
- en testant l'ensemble des combinaisons possibles (en quelque sorte, une attaque en force brute).

Commandes	Explications
<code>john --wordlist /mnt/mdp.txt</code>	Test par dictionnaire Par défaut, le dictionnaire est <code>password.lst</code>
<code>john --wordlist=NomDictionnaire.ext /mnt/mdp.txt</code>	Il est possible de choisir un autre dictionnaire comme <code>rockyou.txt</code>
<code>john --wordlist=NomDictionnaire.ext --rules /mnt/mdp.txt</code>	Pour demander des combinaisons hybrides (exemple : a ↔ @)
<code>john --incremental /mnt/mdp.txt</code>	Pour un test incrémental
<code>john --show /mnt/mdp.txt</code>	Permet d'afficher les mots de passe récupérés

Remarques :

- Le dictionnaire `Rockyou.txt` se trouve dans le dossier `wordlists` : `/usr/share/wordlists`. Il doit être dézippé (gunzip).
- Le dictionnaire `password.lst` se trouve dans le dossier `john` : `/usr/share/john`. Ce dictionnaire peut être modifié par l'ajout de ses propres mots de passe. Dans le cas où les mots de passe ne sont pas connus, on peut deviner qu'un utilisateur aura utilisé le lieu + son nom + un chiffre pour constituer son mot de passe : `msapMsa2`. Utiliser pour cela la commande : `nano password.lst`.

```

GNU nano 2.8.7                               File: password.lst                               Modified

#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011. It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first). It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see http://www.openwall.com/wordlists/
mspMsa2
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer

[ Read 3559 lines ]

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line

```

Identifier les menaces et mettre en œuvre les défenses appropriées



- > Fiche savoirs technologiques 4
- > Fiche méthode 1, p. 203

M. Brillat voudrait mettre en place une veille informationnelle sur les mises à jour et les correctifs logiciels liés au système Windows. Vous êtes en charge de la préparation de cette veille.

1. Définissez les objectifs de la veille informationnelle pour répondre à la demande de M. Brillat.

> Document 1

M. Brillat a sélectionné un certain nombre de sources d'information, qu'il vous soumet. Cette liste n'est pas exhaustive. Elle ne contient pas l'ensemble des sources disponibles : elle est centrée sur les outils numériques.

> Document 2

2. Identifiez les différentes ressources numériques qui permettront de collecter les informations, en précisant si on peut les qualifier d'information de qualité. Pour cela, vous dresserez un tableau comparatif des différentes sources, en utilisant les critères suivants : rapidité d'accès, fiabilité, actualité et pertinence.

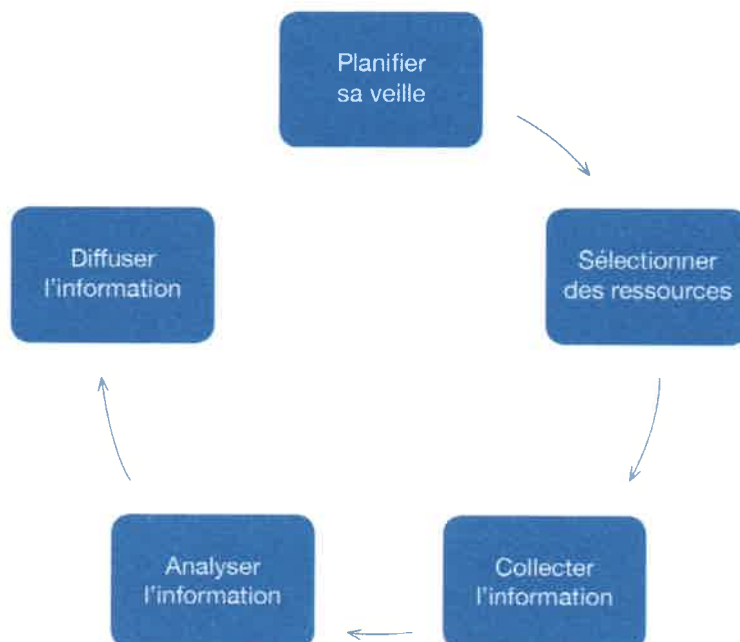
3. Comparez les trois outils de curation présentés dans le document 2, en vous aidant du tableau comparatif du document 3.

> Documents 3 et 4

> Tableau comparatif des outils de veille numérique : www.lienmini.fr/6988-401

4. Indiquez de quelle manière vous allez diffuser ces informations. Vous expliquerez les cibles ainsi que les canaux et les supports de communication utilisés.

Document 1 Les étapes de la veille informationnelle



Document 2 Des sources d'information sur Internet

Internet propose un grand nombre de possibilités pour accéder à de l'information. Voici une liste des principales sources :

- flux Atom ;
- newsletters, files d'actualité ;
- forums, communautés de pratique ;
- réseaux sociaux et réseaux sociaux d'entreprise ;
- système de syndication et de curation ;
- système d'alertes «push» et «pull».

Document 3 Des agrégateurs de flux Internet

M. Brillat a retenu trois outils de curation et de syndication de l'information.



Document 4 Tableau comparatif des outils de veille numérique

Nom	Flux		Outils				Notifications		Avantages	Inconvénients	Web	Desktop	Mobile
	RSS	ATOM	Newsletters	Forums	Communauté	Réseau Social	Push	Pull					

La sécurité des terminaux utilisateurs et de leurs données

I Définition

Sécuriser un terminal utilisateur et ses données implique de :

- réaliser des configurations système qui permettent de se protéger des attaques ;
- installer des applications et des matériels qui empêchent toute intrusion ;
- définir avec les utilisateurs les bonnes pratiques à adopter.

II La configuration du système : quelques règles à respecter

Système d'exploitation	<ul style="list-style-type: none"> - Configurer les mises à jour automatiques - Installer les correctifs et les mises à jour
Applications	<ul style="list-style-type: none"> - Autoriser les applications vérifiées (Logiciels reconnus) - Isoler les applications obsolètes - Interdire les téléchargements de sources inconnues - Limiter les modules optionnelles
Exécution automatique	Désactiver les ports et lecteurs
Boot sur périphériques externes	Désactiver le boot et insérer un mot de passe

III Les applications et matériels spécifiques

Antivirus	Logiciel chargé de détecter et de stopper les <i>malwares</i> connus : virus, vers, <i>keylogger</i> , chevaux de Troie, etc. Il fonctionne avec une <i>base de données</i> qui contient les signatures des <i>malware</i> connus. Exemples : Bitdefender, Avast, Norton, Kapersky.
Antispam	Le <i>spam</i> (ou courriel indésirable, ou pourriel) est une communication électronique non sollicitée. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. Exemples : Altospam, Postbox, McAfee.
Pare-feu (firewall)	Il inspecte les paquets réseaux entrants et sortants et implémente un mécanisme de filtrage basé sur des règles. Il ne transmet pas les paquets qui ne les respectent pas. On distingue les pare-feux matériels (pour un réseau) et les pare-feux logiciels (pour un poste de travail). Exemples : Sophos, Stormshield, ZoneAlarm.
Coffre-fort numérique (ou portefeuille de mots de passe)	Il permet de centraliser ses mots de passe en les protégeant par un seul mot de passe fort. Exemples : KeyPass ou 1Password.
Système d'authentification unique (en anglais <i>Single Sign-On</i>, SSO)	Un seul formulaire d'authentification permet d'accéder à l'ensemble des services de sa session utilisateur.
Mobile Device Management (« gestion des terminaux mobiles »)	Application qui permet la gestion d'une flotte d'appareils nomades. Son objectif est d'harmoniser les outils numériques avec des programmes et applications à jour et une sécurité correcte (présence d'un antivirus ou autre dispositif de sécurisation contre les <i>malwares</i>).

IV

La promotion des bonnes pratiques

1. L'authentification

L'**authentification** permet de protéger le SI contre les attaques par dictionnaire, force brute, **table arc-en-ciel**.

Recommandations ANSSI pour obtenir une authentification forte								
R1	Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.							
R2	Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.)							
R3	Ne demandez jamais à un tiers de créer pour vous un mot de passe.							
R4	Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.							
R5	Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.							
R6	Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.							
R7	Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle.							
R8	Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.							
+	Choix du mot de passe :							
Au moins 12 caractères de types différents, idéalement une passphrase (passe de phrase ou phrase secrète). Pour cela deux méthodes :								
• La méthode phonétique : « J'ai acheté huit CD pour cent euros cet après-midi » deviendra : ght8CD%E7am.								
• La méthode des premières lettres : la citation « un tient vaut mieux que deux tu l'auras » donnera : 1tvmQ2tl'A.								
+	Authentification à double facteurs :							
<table><tr><td>Quelque chose que je sais</td><td>Quelque chose que je possède</td><td>Quelque chose que je suis</td></tr><tr><td><ul style="list-style-type: none">• Mot de passe• Tracé de verrouillage</td><td><ul style="list-style-type: none">• <i>One time password</i> : mot de passe temporaireExemple : Token SafeNet</td><td><ul style="list-style-type: none">• Empreinte biométrique</td></tr></table>			Quelque chose que je sais	Quelque chose que je possède	Quelque chose que je suis	<ul style="list-style-type: none">• Mot de passe• Tracé de verrouillage	<ul style="list-style-type: none">• <i>One time password</i> : mot de passe temporaire Exemple : Token SafeNet	<ul style="list-style-type: none">• Empreinte biométrique
Quelque chose que je sais	Quelque chose que je possède	Quelque chose que je suis						
<ul style="list-style-type: none">• Mot de passe• Tracé de verrouillage	<ul style="list-style-type: none">• <i>One time password</i> : mot de passe temporaire Exemple : Token SafeNet	<ul style="list-style-type: none">• Empreinte biométrique						

www.ssi.gouv.fr.

2. Les bons usages sur Internet

Navigateurs	<ul style="list-style-type: none"> • Utiliser des protocoles SSL/TLS. • Effacer l'historique de navigations, les fichiers temporaires, les cookies.
Accès Internet	<p>Un proxy (serveur mandataire) est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour éviter les sites malveillants. Il permet :</p> <ul style="list-style-type: none"> • l'authentification des utilisateurs et la journalisation des requêtes ; • la mise en cache des pages consultées sur Internet afin d'accélérer les navigations, la mise en place de pare-feux ; • la sécurité par filtrage des paquets (entrant/sortant).
Courriels	<ul style="list-style-type: none"> • Désactiver l'exécution des liens hypertextes et l'affichage des images. • Être très vigilant avec les courriels dont les émetteurs sont inconnus et avec certains types de contenus. • Marquer les indésirables comme tels afin d'affiner la politique de détection des <i>spams</i>. • Si besoin, créer une adresse poubelle.

➤ Voir lexique BTS SIO, p. 221

La sécurité des équipements personnels des utilisateurs et de leurs usages

I Le rôle de la charte informatique

Une charte informatique a pour objectif de fixer les droits et les obligations en matière d'utilisation du système d'information au sein d'une organisation. Elle est obligatoire dès lors qu'une organisation est amenée à traiter des données à caractère personnel.

II La structure d'une charte informatique

Généralement, la charte se présente sous la forme d'un document à portée juridique, dans lequel des instructions sont clairement définies.

1. Objectifs
<ul style="list-style-type: none"> • Les usages autorisés des ressources numériques • Les règles de sécurité en vigueur • Les mesures de contrôle prises par l'organisation
2. Définitions claires et précises
<ul style="list-style-type: none"> • Définition des termes clés pour éviter les interprétations divergentes <p> Exemple : définition du terme authentification</p>
3. Objet et portée
<ul style="list-style-type: none"> • Sur quoi la charte porte-t-elle (droits et devoirs des utilisateurs) ? <p> Exemple : obligation de longueur du mot de passe</p> <ul style="list-style-type: none"> • À qui est-elle destinée ?
4. Usages
<ul style="list-style-type: none"> • Les moyens informatiques et les outils numériques mis à disposition • Les règles et les pratiques autorisées • Les besoins auxquels doit répondre le système d'information
5. Devoirs des utilisateurs
<ul style="list-style-type: none"> • Bon sens dans les pratiques • Respect d'obligations techniques spécifiques
6. Les mesures de contrôle
<ul style="list-style-type: none"> • Liste des mesures de contrôle • Conditions dans lesquelles elles sont mises en œuvre
7. Sanctions
<ul style="list-style-type: none"> • Échelle de sanctions disciplinaires (proportionnelle à la gravité) • Sanctions civiles et pénales
8. Opposabilité de la charte
<ul style="list-style-type: none"> • Acceptation écrite par les utilisateurs • Annexion au règlement intérieur • Annexion au contrat d'entreprise et au contrat des prestataires

III

Le cadre juridique de la charte

La charte informatique doit être portée à la connaissance des salariés. Pour cela, l'employeur peut la présenter par voie d'affichage au sein de l'entreprise ou en remettre un exemplaire à chacun des salariés. La charte informatique s'applique à l'ensemble des utilisateurs du SI, quel que soit leur statut.

Ce document peut être opposable aux salariés de l'entreprise s'il est annexé à un règlement intérieur (l'employeur n'a pas obligation de faire signer la charte) ou au contrat de travail. La date d'entrée en vigueur de la charte doit être indiquée explicitement. Si elle est postérieure à un contrat de travail, un avenant devra être établi.

L'organisation peut imposer un droit de regard et de contrôle sur les pratiques des utilisateurs, par exemple en s'appuyant sur les fichiers journaux (*logs* des accès et modifications des fichiers), les connexions entrantes et sortantes à Internet et à la messagerie électronique, les appels téléphoniques, etc.

IV

Le cas particulier du nomadisme

L'organisation du travail dans les entreprises est aujourd'hui bouleversée par l'avènement de nouvelles habitudes de travail liées à l'apparition du BYOD, du COPE et du CYOD :

BYOD <i>Bring Your Own Device</i>	COPE <i>Corporate Owned Personnally Enabled</i>	CYOD <i>Choose Your Own Device</i>
L'employeur autorise l'utilisation des équipements privés pour exercer les missions professionnelles.	L'entreprise fournit des équipements nomades et réalise la configuration.	Le salarié choisit son matériel mais sa configuration reste à la charge de l'employeur.

Ces nouvelles habitudes de travail doivent être prises en compte dans la rédaction de la charte informatique. En effet, elles impliquent et génèrent des contraintes supplémentaires. La CNIL formule des recommandations, notamment pour la protection des données personnelles.

La responsabilité de l'employeur joue également lorsque les données de l'entreprise sont stockées dans le matériel informatique personnel du salarié. L'employeur doit donc prendre les mesures nécessaires contre les risques relatifs à la confidentialité des données, aux intrusions et aux virus, et les mentionner dans la charte informatique.

Entre autres, il pourra spécifier :

- les appareils éligibles au BYOD ;
- les conditions d'utilisation de ces appareils ;
- les applications utilisables via un matériel personnel ;
- les documents accessibles par le biais d'un appareil personnel, etc.



Retrouvez ce QCM
en version interactive
www.lienmini.fr/6988-402

1 Une charte informatique stipule :

- ☐ les obligations des signataires.
- ☐ les sanctions applicables.
- ☐ les modalités de diffusion de celle-ci.

2 Une charte informatique doit obligatoirement être affichée dans les locaux de l'entreprise.

- ☐ Vrai
- ☐ Faux

3 La charte informatique s'applique :

- ☐ aux salariés de l'entreprise uniquement.
- ☐ aux seuls utilisateurs du système d'information.
- ☐ à l'ensemble du personnel, quel que soit son statut hiérarchique.

4 La charte informatique est opposable au salarié :

- ☐ par annexion au règlement intérieur.
- ☐ par annexion au contrat de travail.
- ☐ quelle que soit la date d'entrée en vigueur.

5 L'organisation à l'initiative de la charte peut imposer un droit de contrôle sur :

- ☐ la journalisation des accès et des modifications de fichiers.
- ☐ les connexions à Internet.
- ☐ les appels téléphoniques.
- ☐ la messagerie électronique.

6 La sécurité des postes de travail comprend la configuration :

- ☐ des systèmes d'exploitation.
- ☐ des applications.
- ☐ des matériels physiques.

7 La sécurité des postes de travail ne concerne pas l'accès aux données.

- ☐ Vrai.
- ☐ Faux

8 Un antivirus permet :

- ☐ de filtrer les connexions entrantes dans un réseau local.
- ☐ de filtrer les connexions sortantes d'un réseau local.
- ☐ d'identifier les signatures des *malwares*.
- ☐ de relayer les demandes de connexions vers les serveurs web.

9 Un pare-feu permet :

- ☐ de filtrer les connexions entrantes dans un réseau local.
- ☐ de filtrer les connexions sortantes d'un réseau local.
- ☐ d'identifier les signatures des *malwares*.
- ☐ de relayer les demandes de connexions vers les serveurs web.

10 Un serveur proxy permet de restreindre l'affichage de sites internet.

- ☐ Vrai
- ☐ Faux



> Fiche savoirs technologiques 4

Situation



Cyber'Ops, situé à Lyon, est un cybercafé accueillant principalement une clientèle d'adolescents. M. Archi, le gérant, souhaite installer un outil qui pourrait sécuriser les équipements et les usages des clients en contrôlant les connexions Internet. En effet, les sites sensibles, comme les sites pornographiques, à caractère discriminatoire ou encore religieux, ne doivent pas pouvoir être consultés.

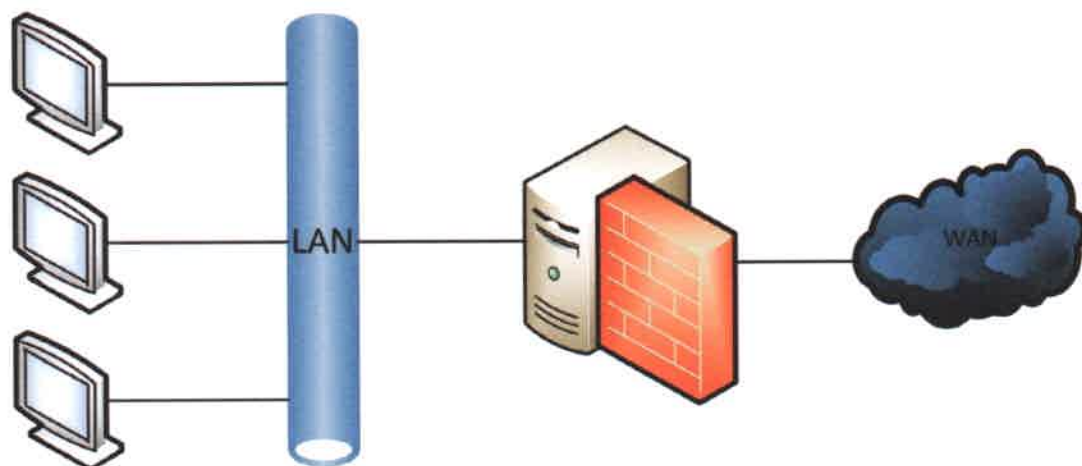
- 1 En vous appuyant sur les informations fournies en annexe, recommandez à M. Archi un outil à configurer au sein de son réseau local pour filtrer les connexions Internet.
- 2 Expliquez de quelle manière cet outil autorise ou non la demande de connexion à un site spécifique.

Les adolescents sont également tentés d'utiliser ce lieu anonyme pour réaliser des téléchargements illicites (musique en MP3, vidéos, etc.).

- 3 Montrez comment l'outil que vous avez proposé peut prendre en charge ces pratiques.
- 4 Précisez s'il permet de se protéger contre les intrusions des *malwares*.

Annexe

Outils de sécurisation



3

Développer une configuration système



> Fiche savoirs technologiques 4

Situation

M. Archi ne peut surveiller en permanence les pratiques des utilisateurs sur leurs postes de travail (par exemple, l'utilisation de supports USB). Il doit donc prendre des précautions pour empêcher des utilisations frauduleuses de ces périphériques. Il souhaiterait que ces différentes configurations puissent être opérationnelles automatiquement, sans intervention quotidienne de sa part.

- 1 Indiquez comment M. Archi peut intervenir sur les postes de travail pour contrôler l'utilisation des supports USB.
- 2 Expliquez quelle précaution supplémentaire il doit prendre pour être certain que la configuration réalisée précédemment soit pérenne.

L'intégrité de l'environnement des postes de travail repose également sur un système d'exploitation non obsolète et exécutant des applications toujours mises à jour, c'est-à-dire toujours en maintenance et sans faille de sécurité.

- 3 Indiquez quelle application native sous Windows permet d'avoir une version récente du système d'exploitation.
- 4 Démontrez que celle-ci peut également agir sur les failles de sécurité.
- 5 Précisez quel outil supplémentaire peut être installé sur un poste de travail pour garantir sa sécurité.

4

Promouvoir les bonnes pratiques



> Fiche savoirs technologiques 4

Situation

M. Onnier est professeur au lycée Ada Lovelace à Saint-Maurice. Il intervient dans les classes de BTS SIO. Quotidiennement, les étudiants utilisent les ressources du réseau informatique de l'établissement. M. Onnier souhaite rédiger un guide des bonnes pratiques afin d'encadrer les usages de ses étudiants et, ainsi, les responsabiliser.



- 1 En vous appuyant sur les informations données par l'ANSSI, indiquez les spécifications qui doivent être mentionnées dans le guide au sujet de la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local.
 > Guide de l'hygiène informatique : www.lienmini.fr/6988-403
 > Guide des mots de passe : www.lienmini.fr/6988-404
- 2 Précisez les recommandations à suivre pour la gestion de ces mots de passe durant les deux années du BTS.
- 3 Expliquez les deux méthodes utilisées pour définir un mot de passe par *passphrase* (passe de phrase ou phrase secrète).

...

Les étudiants seront souvent amenés à utiliser des identifiants de connexion sur des navigateurs Internet ou des logiciels spécifiques lors de leurs différents travaux.

4 Indiquez quelles manipulations ne sont pas souhaitables, et expliquez pourquoi.

M. Onnier propose à ses étudiants d'utiliser des machines virtuelles sous Windows 10 lors de leurs activités. Il vous demande d'étudier les options de sécurité locales proposées par ce système d'exploitation.

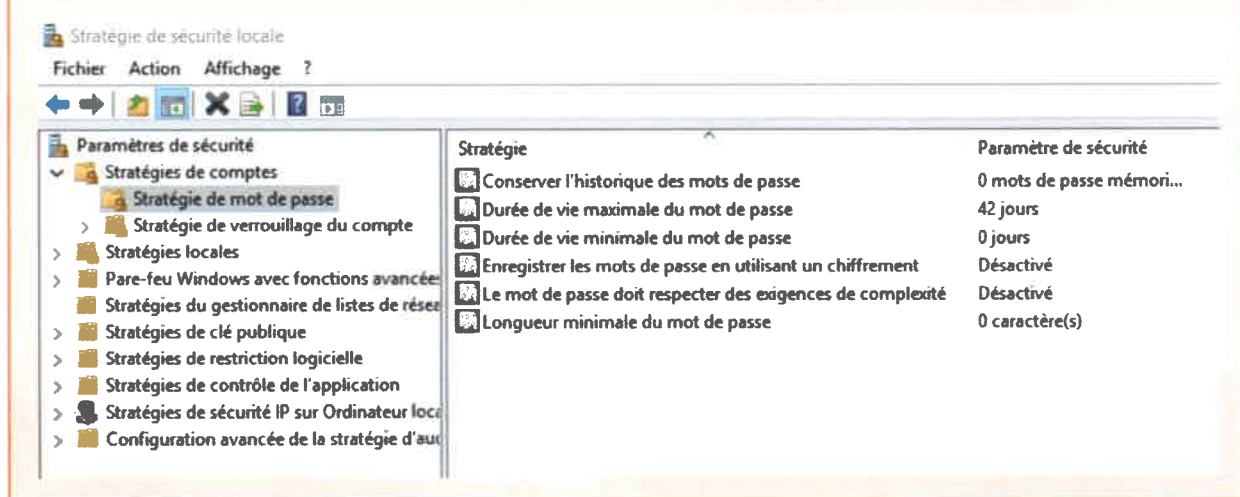
5 Expliquez le rôle des différentes stratégies de sécurité locales présentées en annexe.

M. Onnier vous demande de créer un compte intitulé « etudiant_sio » sur une machine virtuelle Windows 10 et de tester ces stratégies.

6 Appliquez ces stratégies sur le compte donné par M. Onnier en définissant un mot de passe.

Annexe

Stratégie de sécurité locale



5

Gérer les mots de passe



> Fiche savoirs technologiques 4

Situation

M. Onnier est conscient qu'il peut être parfois fastidieux pour les étudiants de mémoriser tous les mots de passe qu'ils auront à utiliser durant leurs deux années de scolarité sur l'ensemble des connexions serveurs et matériel. C'est pourquoi il souhaite que vous lui proposiez une analyse de l'outil KeyPass.

> Site keepass.info : www.lienmini.fr/6988-405

1 Consultez le tutoriel sur l'utilisation de Keepass :

> Utiliser Keepass pour gérer ses mots de passe : www.lienmini.fr/6988-406

2 Installez l'outil KeyPass sur une machine virtuelle (voir travaux en laboratoire 1, p. 94).

3 Testez les fonctionnalités de l'outil.

4 Dressez un tableau indiquant les avantages et les inconvénients de celui-ci.