Ugo BEMBEN Informer les utilisateur 2023

Question 1 :

Je recommande d'utiliser un pare-feu pour filtrer les connexions internet au sein du réseau local du cybercafé. Je lui recommande de configuré un Windows Serveur 2016 car celui-ci pourras servir a plusieurs chose .

Question 2 :

Avec Windows Server 2016, vous pouvez utiliser les fonctionnalités de pare-feu de Windows pour autoriser ou bloquer l'accès à des sites spécifiques. Pour ce faire, vous devez configurer des règles de pare-feu pour autoriser ou bloquer les connexions en fonction de l'adresse IP de destination et/ou du port utilisé.

Pour autoriser l'accès à un site spécifique, vous devez créer une règle de pare-feu qui autorise la connexion en spécifiant l'adresse IP ou l'URL du site en question. Vous pouvez également utiliser des règles de pare-feu pour autoriser uniquement certaines applications ou services à accéder à Internet.

Pour bloquer l'accès à un site spécifique, vous devez créer une règle de pare-feu qui bloque la connexion en spécifiant l'adresse IP ou l'URL du site en question. Il est également possible de bloquer les connexions à des sites spécifiques en utilisant des listes de sites bloqués ou en utilisant des fonctionnalités de filtrage de contenu.

Question 3 :

Le pare-feu que j'ai proposé peut aider à prendre en charge les téléchargements illégaux en utilisant des règles de filtrage pour bloquer l'accès à certains sites de téléchargement illégaux ou aux protocoles de partage de fichiers utilisés pour télécharger illégalement des fichiers. Il peut également utiliser des listes de sites bloqués pour bloquer automatiquement l'accès à des sites connus pour héberger des contenus illégaux.

Question 4 :

Pour bloquer ou autoriser l'utilisation des supports USB via les stratégies de groupe, vous devez créer une GPO et configurer les paramètres de sécurité appropriés. Voici les étapes pour configurer une GPO pour bloquer l'utilisation des supports USB :

1. Ouvrez l'outil de gestion des stratégies de groupe (GPMC) sur un ordinateur qui exécute Windows Server.
2. Créez une nouvelle GPO ou sélectionnez une GPO existante à configurer.
3. Dans la console GPMC, développez l'arborescence de votre domaine et cliquez sur le noeud "Ordinateurs" pour sélectionner tous les ordinateurs sur lesquels vous voulez bloquer l'utilisation des supports USB.
4. Faites un clic droit sur la GPO créée et choisissez "Modifier"
5. Dans l'éditeur de stratégies de groupe, développez "Configuration ordinateur" -> "Modèles d'administration" -> "Système"
6. Dans l'arborescence de droite, recherchez "Politique de sécurité pour les périphériques de stockage amovibles"
7. Double cliquez sur la politique et configurez-la pour "Activé"
8. Dans la fenêtre de propriété, choisissez "Bloquer l'accès aux périphériques de stockage amovibles"
9. Appliquez la GPO et validez le bon fonctionnement de la stratégie.

Il est important de noter que cette méthode bloque tous les périphériques USB qui ne sont pas explicitement autorisés dans la GPO, il est donc important de planifier la mise en place de cette stratégie pour éviter de bloquer des périphériques nécessaires pour le fonctionnement de l'entreprise.

Question 5 :

Il existe plusieurs précautions supplémentaires que le responsable du cybercafé peut prendre pour s'assurer que la configuration de filtrage des connexions internet et de contrôle des supports USB est pérenne :

1. Sauvegarder régulièrement la configuration : Il est important de sauvegarder régulièrement la configuration du pare-feu et des stratégies de groupe pour pouvoir restaurer rapidement la configuration en cas de problème.
2. Mettre à jour régulièrement les logiciels et les signatures : Il est important de maintenir le pare-feu et les outils de sécurité à jour pour s'assurer qu'ils protègent contre les dernières menaces.
3. Utiliser des outils de surveillance et de rapport : Il est important d'utiliser des outils de surveillance pour surveiller les activités du réseau et les alertes de sécurité, et des outils de rapport pour évaluer les risques et les tendances de sécurité.
4. Sensibiliser les utilisateurs : Il est important de sensibiliser les utilisateurs aux risques de sécurité liés à l'utilisation d'Internet et des supports USB pour éviter les erreurs d'utilisation qui pourraient compromettre la sécurité du réseau.
5. Utiliser une architecture de sécurité défensive : Il est important de mettre en place une architecture de sécurité défensive en utilisant des couches de sécurité pour protéger contre les menaces internes et externes.
6. Test de la configuration : Il est important de tester régulièrement la configuration pour s'assurer qu'elle fonctionne correctement et qu'elle protège efficacement contre les menaces.

En utilisant ces précautions supplémentaires, le responsable du cybercafé peut s'assurer que la configuration de filtrage des connexions internet et de contrôle des supports USB est pérenne et protège efficacement le réseau contre les menaces.

Question 6 :

Windows Update est l'application native de Windows qui permet d'avoir une version récente du système d'exploitation. Cette application est intégrée à Windows et permet de télécharger et d'installer automatiquement les mises à jour de sécurité, les correctifs et les nouvelles fonctionnalités pour Windows.

Windows Update peut être configuré pour télécharger et installer automatiquement les mises à jour, ou pour demander l'autorisation avant de les installer. Il est recommandé de configurer Windows Update pour télécharger et installer automatiquement les mises à jour de sécurité pour assurer une protection efficace contre les vulnérabilités de sécurité. Il est également possible de configurer Windows Update pour télécharger uniquement les mises à jour importantes ou facultatives.

Question 7 :

Windows Update peut agir sur les failles de sécurité en téléchargeant et en installant automatiquement les mises à jour de sécurité pour corriger les vulnérabilités dans le système d'exploitation et les applications. Ces mises à jour de sécurité sont souvent créées par Microsoft pour corriger les failles de sécurité qui ont été découvertes dans le système d'exploitation et les applications.

En installant régulièrement les mises à jour de sécurité, Windows Update permet de protéger les postes de travail contre les vulnérabilités de sécurité qui pourraient être exploitées par des attackers pour prendre le contrôle des ordinateurs ou pour voler des informations confidentielles.

Question 8 :

Il existe plusieurs outils supplémentaires qui peuvent être installés sur un poste de travail pour garantir sa sécurité. Parmi eux un Antivirus pour garantir plus de sécurité.

**Lycée**

Question 1 :

L'ANSSI (Agence nationale de la sécurité des systèmes d'information) recommande les spécifications suivantes pour la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local :

1. Longueur minimale : Les mots de passe doivent avoir une longueur minimale de 8 caractères, idéalement 12 caractères ou plus pour une sécurité accrue.
2. Complexité : Les mots de passe doivent comporter des caractères alphanumériques (lettres et chiffres) ainsi que des caractères spéciaux tels que des signes de ponctuation, pour augmenter la complexité et la difficulté pour les pirates informatiques de deviner le mot de passe.
3. Interdiction de l'utilisation de mots courants : Les mots de passe ne doivent pas être basés sur des mots courants ou des informations personnellement identifiables, tels que les noms, les dates de naissance, les numéros de téléphone, etc.
4. Interdiction de l'utilisation de mots de passe utilisés antérieurement : Les utilisateurs ne doivent pas réutiliser les mêmes mots de passe pour différents comptes ou pour des mots de passe utilisés antérieurement.
5. Expiration des mots de passe: Les mots de passe doivent être expirés après un certain délai (généralement tous les 90 jours) et devoir être renouvelés pour éviter que des personnes non autorisées ne les utilisent après une possible divulgation ou une utilisation illégale.

Question 2 :

Il existe plusieurs recommandations à suivre pour la gestion des mots de passe durant les deux années de BTS. Ces recommandations incluent :

1. Utilisation de mots de passe forts et uniques : Les étudiants doivent utiliser des mots de passe forts et uniques pour chacun de leurs comptes (e-mails, réseaux sociaux, systèmes d'information de l'établissement, etc.) pour éviter que des personnes non autorisées ne puissent accéder à leurs comptes.
2. Utilisation d'une gestion de mots de passe : Il est recommandé d'utiliser une solution de gestion de mots de passe pour générer et stocker des mots de passe forts de manière sécurisée, et pour aider les utilisateurs à gérer leurs mots de passe.
3. Changement régulier des mots de passe : Les étudiants doivent changer régulièrement leurs mots de passe (généralement tous les 90 jours) pour éviter que des personnes non autorisées ne les utilisent après une possible divulgation ou une utilisation illégale.
4. Ne pas partager les mots de passe : Les étudiants ne doivent pas partager leurs mots de passe avec des personnes non autorisées ou les écrire dans des lieux accessibles aux autres, pour éviter que des personnes malveillantes ne les utilisent à leur insu.
5. Sensibilisation et formation : Il est important de sensibiliser les étudiants aux bonnes pratiques de sécurité pour la création de mots de passe et de les former à la création de mots de passe forts et à la gestion de leurs mots de passe.

Question 3 :

Il existe deux méthodes couramment utilisées pour définir un mot de passe par passphrase :

1. La méthode dite "d'expression" : Cette méthode consiste à utiliser une phrase ou une expression courante, comme une citation, une chanson ou une phrase personnelle, comme mot de passe. Par exemple, "Je suis le roi du monde" pourrait devenir "Jslrdm1" ou "JSRDM#1"
2. La méthode dite "d'acronyme" : Cette méthode consiste à utiliser les premières lettres d'une phrase ou d'une expression pour créer un acronyme comme mot de passe. Par exemple, "Je suis le roi du monde" pourrait devenir "Jslrdm1" ou "JSRDM#1".

Question 4 :

Il existe plusieurs manipulations qui ne sont pas souhaitables pour les étudiants lorsqu'ils utilisent des identifiants de connexion sur des navigateurs internet ou des logiciels spécifiques. Ces manipulations incluent :

1. Partager les identifiants de connexion : Il est important de ne pas partager les identifiants de connexion avec des personnes non autorisées, car cela peut entraîner une utilisation non autorisée ou illégale des comptes et une violation de la confidentialité des données.
2. Enregistrer les identifiants de connexion sur le navigateur ou dans des fichiers : Il est important de ne pas enregistrer les identifiants de connexion sur le navigateur ou dans des fichiers, car cela peut entraîner une utilisation non autorisée ou illégale des comptes et une violation de la confidentialité des données.
3. Utiliser des mots de passe faibles ou couramment utilisés : Il est important d'utiliser des mots de passe forts et uniques pour les identifiants de connexion, pour éviter que des personnes non autorisées ne puissent accéder aux comptes.
4. Utiliser les mêmes identifiants de connexion

Question 5 :

Dans l’exemple de ci-dessus il n’y a que 2 regles de mot de passe sont :

* La durée de vie maximal du mot de passe et de 42 jour
* Il est impossible d’enregistré un mot de passe non crypté

**Gestion des mot de passe :**

Question 4 :

****