Exercice 06-40 Sécurité accès poste de travail		
Chapitre	Sécurité réseau	Durée : 2x30’
Sujet	**Exercice théorique, sécuriser l’accès au poste de travail**	
Objectif(s)	A la fin de l’exercice, l’elève aura acquis les compétences suivantes : • Il est capable d’identifier les besoins en sécurité liés à un poste de travail, tant au niveau du poste client que du serveur. • Il est capable de donner aux utilisateurs des consignes claires sur le choix des mots de passe et sur la non transmission d’information sensibles • Il est capable d’établir une liste de statégies à mettre en place sur un serveur pour l’accès des utilisateurs à un poste client.	

Exercice 1

Dans le cadre de votre entreprise et en tant qu’employé au Service informatique, vous êtes chargés par votre responsable de préparer un document sur la sécurité que vous distribuerez et expliquerez ensuite aux utilisateurs de votre réseau. On vous demande de traiter des sujets suivants :

- Explication du phishing

  Selon Wikipedia : Le phishing (en français : hameçonnage) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. Elle peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

- Choix d’un mot de passe :
  - Complexe (min. 12 caractères) et comprenant des majuscules, minuscules, caractères spéciaux et chiffres.
  - Ne doit pas contenir de date, de prénom ou de noms, de mots qu’on trouve dans un dictionnaire.

- Règles de base en sécurité, pour empêcher l’accès non autorisé à son poste, y compris les cas les plus banals :

  Idéalement, il faudrait présenter et faire signer à l’utilisateur une charte informatique qui présente les règles à suivre (voir série précédente), en lien avec le surf sur Internet (préciser ce qui est permis ou non) et la sécurité de base :
  - Ne pas laisser son PC allumé sans écran bloqué
  - Ne pas diffuser son mot de passe, ni le laisser caché sur un post-it sous son clavier !
  - Changer régulièrement son mot de passe
  - Dans les émails, ne pas ouvrir les fichiers douteux provenant de sources non validées (risques d’installer des virus ou des Chevaux de Troie)
  - Ne pas installer de logiciel tiers, qui ne soit pas autorisé par l’entreprise.

Travail à réaliser

En vous aidant de vos connaissances acquises dans d'autres modules réseau et en utilisant Internet si nécessaire, vous devrez établir un document Word qui sera ensuite distribué aux utilisateurs :

- Votre document devra répondre aux exigences demandées par votre responsable (liste ci-dessus).
- Dans vos explications, soyez clairs et précis : l'information s'adresse à un public d'utilisateur, elle doit donc être utile et compréhensible
- N'oubliez pas de préciser les risques encourus si les consignes ne sont pas suivies.
- Citez les sources utilisées.

Exercice 2

Dans votre entreprise, vos serveurs tournent sous Windows Server 2012 R2. En tant qu'employé au Service informatique, vous êtes chargé par votre responsable d'améliorer la sécurité liée à l'accès aux comptes des utilisateurs. Pour cela, vous devrez vous renseigner sur les stratégies de sécurité qu'il est possible de mettre en place dans l'AD (Active Directory). Votre chef vous demande de préparer un document qui présentera les résultats de vos recherches.

L'AD permet de fixer les règles de sécurité suivantes :

- Choix de l'horaire de connexion de chaque utilisateur (ou groupe d'utilisateurs). Ainsi, un utilisateur ne pourra pas se connecter en dehors de ces heures de travail.
- Les groupes sont utilisés pour faciliter le travail d'administration.
- Pour le mot de passe :
  choix de la complexité,
  durée de validité (par exemple ; changer tous les 2 mois),
  nombre de mots de passe différents en arrière (le nouveau doit être différent des 12 derniers)
- Durée de connexion par session (appelé bail) : bail de 2 jours, par exemple. Après ce temps, l'utilisateur est déconnecté. Cette gestion est faite dans le DNS.
- Gestion des IP des machines en fonction des utilisateurs : il est possible de n'autoriser qu'un utilisateur (le directeur par exemple) pour un poste particulier

Droits NTFS (disques sous Windows) :

- Accès protégé à son compte réseau : seul l'utilisateur peut voit son propre compte, mais pas ses collègues.
- Préciser aussi quels dossiers seront accessibles pour quels types d'utilisateurs.

Travail à réaliser

En vous aidant de vos connaissances acquises dans d'autres modules réseau et en effectuant des recherches sous Internet, vous devrez établir un document Word que vous remettrez à votre chef. Les principaux points à traiter sont les suivants :

- Stratégie pour les mots de passe dans l'AD : niveau de difficulté, renouvellement, etc
- Paramètres du compte : horaire d'accès, machine réservée à un utilisateur, etc
- Cas des invités et des comptes qui ne sont plus utilisés
- Lorsque c'est possible, ajoutez des illustrations sur les opérations à effectuer

→ Pour vous aider, le site technique de Microsoft « technet.microsoft.com » vous fournira de nombreux renseignements.