Leçon 1

Comprendre les couches de sécurité

Objectifs d'apprentissage

Les élèves apprendront:

- fondamentaux de la sécurité
- Sécurité physique comme première ligne de défense

ODN compétences

• Comprendre les principes de sécurité de base.	1.1
• Comprendre la sécurité physique.	1.2

Résumé de la leçon - Notes de cours

Vous devriez commencer cette leçon par vous-même l'introduction et le cours.

Un bon endroit pour commencer est de discuter de ce que la sécurité est. Vous pouvez demander aux élèves ce qu'ils pensent est la sécurité et vous trouverez peut-être qu'il y aura de nombreuses définitions différentes en fonction de leurs points de vue et de l'expérience. Comme vous passez par ce cours, vous donner des exemples précis sur la façon de configurer ou activer la sécurité, mais la chose la plus importante que les élèves doivent apprendre est des concepts de sécurité afin qu'ils puissent les appliquer, peu importe quel système d'exploitation, serveur ou le périphérique est étant fixé.

La première partie de la leçon discute de la CIA, qui est court pour la confidentialité, l'intégrité et la disponibilité. La plupart des étudiants peuvent facilement voir est souvent utilisé la confidentialité et l'intégrité que la conception des administrateurs, mettre en œuvre et gérer la sécurité. Cependant, de nombreux étudiants ne peuvent voir la disponibilité du point de vue de la façon dont une attaque par déni de service peut faire un service, une application ou d'un serveur indisponible. Mais ils doivent aussi apprendre à faire face aux catastrophes, aussi.

La partie suivante de la leçon couvre les menaces et la gestion des risques. Les coûts de sécurité de l'argent, et vous avez seulement tant d'argent que vous pouvez dépenser pour sécuriser vos systèmes et données. Par conséquent, vous devez utiliser la gestion des menaces et des risques pour définir vos menaces actuelles et les risques et combien d'argent vous êtes prêt à dépenser pour faire face à ces risques et menaces.

Le concept suivant est le principe du moindre privilège, qui est souvent négligé au sein d'une organisation. La prochaine partie de la conversation se déplace alors d'attaquer la surface et les moyens que vous pouvez essayer de réduire la surface d'attaque afin qu'il y ait moins de chances d'être victime.

La discussion suivante porte sur l'ingénierie sociale, qui est devenu très répandu que l'utilisation de l'Internet a augmenté. Vous pouvez afficher un point fait qu'il est plus facile à utiliser sociale

ingénierie pour trouver quelqu'un pour révéler quelque chose que de pirater réellement ou pénétrer dans un système. Cela démontre que les utilisateurs peuvent souvent être le maillon le plus faible dans un système de sécurité.

Le concept suivant examine une approche de la couche lors du développement de la sécurité. Par conséquent, vous devez donner un aperçu des différentes catégories de sécurité, telles que la sécurité physique, contrôle d'accès, la sécurité informatique, la sécurité des appareils mobiles et des dispositifs et des lecteurs amovibles.

Mots clés

contrôle d'accès - Le processus de restreindre l'accès à une ressource aux seuls utilisateurs autorisés, des applications ou des systèmes informatiques.

surface d'attaque - L'exposition, les vulnérabilités accessibles et exploitables qu'un système ou la technologie a.

disponibilité - Décrit une ressource étant accessible à un utilisateur, l'application, ou d'un système informatique en cas de besoin. En d'autres termes, des moyens de disponibilité que lorsqu'un utilisateur a besoin d'être à l'information, il a la capacité de le faire.

confidentialité - La caractéristique d'un accès assurant des ressources est limité aux utilisateurs autorisés uniquement, des applications ou des systèmes informatiques.

défense en profondeur - L'utilisation de plusieurs couches de sécurité pour défendre vos actifs.

lecteur Flash - Un petit disque basé sur la mémoire flash.

intégrité - La cohérence, l'exactitude et la validité des données ou des informations. L'un des objectifs d'un programme de sécurité de l'information réussie est de faire en sorte que les données sont protégées contre toute modification non autorisée ou accidentelle.

keylogger - Un dispositif physique ou logique utilisé pour les frappes de capture.

dispositif mobile - Les petits appareils qui sont utilisés pour traiter l'information, envoyer et recevoir du courrier, emmagasinent d'énormes quantités de données, surfer sur Internet et interagir à distance avec des réseaux et des systèmes internes. Ils comprennent les ordinateurs portables, les PDA (assistants numériques personnels), et les téléphones intelligents.

principe du moindre privilège - Une discipline de sécurité qui exige qu'un utilisateur particulier, système ou application donner plus de privilèges que nécessaire pour remplir sa fonction ou d'un emploi.

périphérique amovible - Un dispositif de stockage qui est conçu pour être retiré d'un ordinateur sans éteindre l'ordinateur.

risque résiduel - Le risque qui reste après que des mesures ont été prises pour réduire la probabilité ou de minimiser l'effet d'un événement particulier.

risque - La probabilité qu'un événement se produise. En réalité, les entreprises ne sont concernés que sur les risques qui auraient un impact négatif sur l'environnement informatique.

l'acceptation des risques - L'acte d'identifier et prendre une décision éclairée d'accepter la probabilité et l'impact d'un risque spécifique.

l'évaluation des risques - Identifie les risques qui pourraient avoir un impact sur votre environnement.

la prévention des risques - Le processus d'élimination d'un risque en choisissant de ne pas participer à une action ou une activité.

gestion des risques - Le processus d'identification, l'évaluation et la hiérarchisation des menaces et des risques.

atténuation des risques - Prendre des mesures pour réduire la probabilité ou l'impact d'un risque.

transfert de risque - Le fait de prendre des mesures pour déplacer la responsabilité d'un risque à un tiers par l'assurance ou la sous-traitance.

ingénierie sociale- Une méthode utilisée pour accéder aux données, systèmes ou réseaux, principalement par le biais de fausses déclarations. Cette technique repose généralement sur la nature confiance de la personne attaquée.

menace - Une action ou événement qui pourrait entraîner la violation, d'une panne ou la corruption d'un système en exploitant des vulnérabilités connues ou inconnues.

Lesson 1

Comprendre les couches de sécurité

évaluation des connaissances

Choix multiple

Encerclez la ou les lettres qui correspondent à la meilleure réponse ou des réponses.

1. Lequel des éléments suivants sont des réponses valides de risque? (Choisissez tout ce qui correspond.)

une. Atténuation

b. Transfert

c. Investissement

ré. Évitement

2. Lequel des éléments suivants sont considérés comme des dispositifs ou des disques amovibles? (Choisissez tout ce qui correspond.)

une. iPod

b. netbook

c. clé USB

ré. Lecteur de disquette

3. Lequel des éléments suivants seraient considérés comme des mesures de sécurité appropriées pour le périmètre de la sécurité extérieure d'un bâtiment? (Choisissez tout ce qui correspond.)

une. Détecteur de mouvement

b. feux de lot Parking

c. Tourniquet

ré. Gardes de sécurité

4. Vous êtes en voyage d'affaires et vous dirigez vers dîner avec un client. Vous ne pouvez pas prendre votre ordinateur portable avec vous au restaurant. Que devez-vous faire avec l'appareil? (Choisissez la meilleure réponse.)

une. Verrouiller l'ordinateur portable dans le coffre de votre voiture.

b. Rangez l'ordinateur portable hors de la vue dans un tiroir de la commode.

c. Fixer l'ordinateur portable à un meuble avec un câble de sécurité pour ordinateur portable.

ré. Vérifiez l'ordinateur portable à la réception.

5. Le processus d'élimination d'un risque en choisissant de ne pas participer à une action ou une activité décrit laquelle des options suivantes?

une. Atténuation

b. Risque résiduel

c. Évitement

ré. Acceptation

6. Vous venez d'être promu chef de la sécurité pour votre entreprise de fabrication de pièces d'automobiles et que vous essayez d'identifier les technologies qui aideront à assurer la confidentialité de vos techniques de fabrication exclusives. Parmi les propositions suivantes sont des technologies que vous pouvez utiliser pour aider à cette entreprise? (Choisissez tout ce qui correspond.)

une. Le cryptage fort

b. Gardes de sécurité

c. un coffre-fort pour ordinateur portable

ré. L'authentification forte

7. L'acronyme CIA signifie que des éléments suivants?

une. La confidentialité, l'identité, le contrôle d'accès

b. La confidentialité, l'intégrité, le contrôle d'accès

c. La confidentialité, l'intégrité, la disponibilité

ré. Contrôle, l'identité, le contrôle d'accès

8. Vous avez été placé en charge du service de sécurité de l'entreprise et votre patron vous a demandé de l'aider à comprendre ce qu'on entend par les principes de sécurité de base. Laquelle de ces explications devraient vous donner à votre patron?

une. principes de sécurité de base font référence à la sécurité intérieure du périmètre lors de la mise en place d'un environnement de sécurité physique en couches.

b. principes de sécurité de base font référence aux principes de confidentialité, la disponibilité et l'intégrité.

c. principes de sécurité de base font référence à tirer parti des meilleures pratiques de sécurité.

ré. principes de sécurité de base font référence aux quatre méthodes de traitement des risques.

9. En tant que chef de la sécurité pour un petit traitement de dossiers médicaux entreprise, vous venez de terminer la mise en place de la sécurité physique pour votre nouveau bureau. En particulier, vous avez fait en sorte que le stationnement est allumé, que vous avez des gardes à la fois à la porte et en effectuant des patrouilles périodiques, et que vous avez des lecteurs de badges dans tout le bâtiment à des endroits clés. Vous avez également mis la technologie d'accès biométrique à la porte du centre de données. De plus, vous avez des caméras dans le parking, à l'entrée du bâtiment et à l'entrée des centres de données. Ce type de mise en œuvre est connue sous le nom: (. Choisissez la meilleure réponse)

une. contrôle d'accès.

b. principes de sécurité de base.

c. les meilleures pratiques de sécurité.

ré. défense en profondeur.

10. Qu'est-ce que vous appelez le processus de désactivation des services inutiles et les ports pour rendre un système plus sécurisé?

une. La réduction de la zone d'attaque de la surface

b. Un cheval de Troie d'atténuation

c. éviter la sécurité

ré. Défense en profondeur

Remplir les trous

1. **Confidentialité** est la caractéristique d'une ressource qui assure que l'accès est limité aux seuls utilisateurs autorisés, des applications ou des systèmes informatiques.

2. Si vous déployez des technologies pour restreindre l'accès à une ressource, vous pratiquez le principe de sécurité connu sous le nom **contrôle d'accès**

3. Le déploiement de plusieurs couches de la technologie de sécurité est appelé **défense profondeur** .

4. Une action ou événement qui pourrait entraîner la rupture, panne ou corruption d'un système en exploitant les failles connus ou inconnus est un (n) **menace** .

5. Vous venez de prendre un nouvel emploi en tant que gestionnaire des risques pour un support de taille société pharmaceutique, et votre première mission consiste à effectuer une évaluation formelle des risques. Vous les plus susceptibles d'enregistrer les résultats de votre évaluation des risques dans un (n) **registre des risques** .

6. Une secrétaire à votre bureau juste d'avoir au téléphone avec quelqu'un qui a dit il appelle le service informatique. L'appelant avait un certain nombre de questions sur la configuration de l'ordinateur du secrétaire, et il a demandé son nom d'utilisateur et mot de passe. Dans cette situation, le secrétaire était très probablement une victime **ingénierie sociale** .

sept. La cohérence, l'exactitude et la validité des données ou des informations est appelé **intégrité** .

8. Vous voyagez pour le travail et décidez d'utiliser un ordinateur dans l'hôtel centre d'affaires pour vérifier votre e-mail et payer plusieurs factures. Lorsque vous vous asseyez à l'ordinateur, vous remarquerez qu'il ya un connecteur supplémentaire entre le clavier et l'ordinateur. Vous avez probablement rencontré un (n) **keylogger** .

9. Vous êtes le gestionnaire des risques pour une banque régionale, et il vous suffit déployé un nouveau système de lecteur de badge pour faire face à un risque de contrôle d'accès. Bien que votre solution a atténué le risque, il y a encore un faible risque restant associée au contrôle d'accès. Ce risque est connu sous le nom **risque résiduel** .

dix. Plus la **surface d'attaque** d'un environnement particulier, plus le risque d'une attaque réussie.

évaluation des compétences

Scénario 1-1: Conception d'une solution de sécurité physique

Vous êtes le responsable de la sécurité pour une banque de taille moyenne. On vous a demandé de concevoir une solution de sécurité pour garder les intrus de la banque après les heures. Les trois domaines de la banque dont vous avez besoin pour sécuriser sont le stationnement, le périmètre du bâtiment, et la voûte. La liste des technologies que vous utiliseriez dans chacun de ces domaines.

Ce sont quelques-unes des technologies qui pourraient être utilisées dans chacun des domaines:

beaucoup de stationnement (périmètre extérieur):

- **Des caméras de sécurité**
- **feux de lot Parking**
- **clôture de périmètre**

- **Porte avec gardien**
- **Porte avec lecteur de badge d'accès**
- **patrouilles de la Garde**

périmètre du bâtiment (périmètre interne):

- **Serrures (portes extérieures, portes intérieures, les portes des bureaux, des bureaux, classeurs, etc.)**
- **Keypads**
- **Des caméras de sécurité**
- **Lecteurs de badges (sur les portes et les ascenseurs)**
- **bureau garde**
- **patrouilles de la Garde**
- **Détecteur de fumée**
- **Turnstiles**
- **sas**

Vault (zone sécurisée):

- **lecteurs de badges**
- **Keypads**
- **La technologie biométrique (scanner d'empreintes digitales, un scanner de la rétine, la reconnaissance vocale)**
- **Portes de sécurité**
- **scanners à rayons X**
- **Détecteur de métaux**
- **Appareils photo**
- **Les systèmes de détection d'intrusion (faisceau lumineux, infrarouge, micro-ondes et à ultrasons)**

Scénario 1-2: Sécurisation d'un appareil mobile

Vous êtes le responsable informatique pour une société de services juridiques de 5000 employés. Vous êtes en train de déployer de nouveaux appareils mobiles à votre service commercial. Quels sont les processus et les technologies utiliserez-vous pour garder ces systèmes sécurisés physiquement?

Certaines des technologies que vous pourriez utiliser comprennent:

- **stations d'accueil: Pratiquement toutes les stations d'accueil pour ordinateur portable sont équipés de dispositifs de sécurité. Cela peut impliquer une clé, un cadenas, ou les deux, selon le fournisseur et le modèle.**
- **câbles de sécurité portables: Utilisé conjointement avec le (Slot Universal Security) USS ces câbles attachent à un ordinateur portable et peut être enroulé autour d'un objet fixe comme un meuble.**
- **un coffre-fort pour ordinateurs portables: Ce sont des coffres-forts en acier spécialement conçus pour contenir un ordinateur portable et être fixé à un mur ou un meuble.**

- **logiciel de récupération de vol: Ces applications permettent le suivi d'un ordinateur volé afin qu'il puisse être récupéré.**
- **alarmes portables: Ce sont des alarmes de mouvement sensible que le son dans le cas où un ordinateur portable est déplacé. Certains sont également conçus conjointement avec un système de câble de sécurité pour qu'ils sonnent chaque fois que le câble est coupé. Vous devez également former vos employés sur les meilleures pratiques suivantes:**

- **Gardez votre équipement avec vous: Les appareils mobiles doivent être conservés avec vous chaque fois que possible. Cela signifie que vous devez garder vos appareils mobiles sur votre personne ou dans votre bagage à main lorsque vous voyagez. De même, gardez vos appareils mobiles à vos yeux lorsque vous passez par les postes de contrôle de l'aéroport.**
- **Utilisez votre coffre: Si vous voyagez en voiture et sont incapables de prendre votre appareil mobile avec vous, verrouiller dans le coffre lorsque vous vous garez. Ne laissez pas un appareil mobile en vue dans un véhicule sans surveillance, même pour une courte période de temps, et de ne jamais le laisser dans une nuit de véhicule.**

- **Utilisez le coffre-fort: Si vous séjournez dans un hôtel, verrouillez votre appareil mobile dans un coffre-fort si l'on est disponible.**

évaluation des compétences

Scénario 1-3: Regarder la confidentialité, l'intégrité et la disponibilité

Au sein de votre organisation, vous avez un serveur appelé Serveur1 qui exécute Windows Server 2008 R2. Sur Server1, vous créez et partagez un dossier appelé Data sur le lecteur C. Dans le dossier de données, vous créez un dossier pour chaque utilisateur au sein de votre organisation. Vous placez ensuite chèque de paie électronique de chaque personne dans son dossier. Plus tard, vous découvrez que John a pu entrer et changer certains des chèques de paie électroniques et autres, l'effacement. Expliquer que des composants de la CIA n'a pas été suivi dans ce scénario.

CIA signifie la confidentialité, l'intégrité et la disponibilité. Parce que John a pu voir les chèques de paie d'autres utilisateurs, la confidentialité n'a pas été respectée. De même, parce que John a pu changer les chèques de paie des autres, l'intégrité n'a pas été suivie. Enfin, parce que John a pu supprimer les chèques de paie, il a fait les chèques de paie non disponibles à certains des utilisateurs aussi bien.

Scénario 1-4: Examen ingénierie sociale

Vous travaillez pour la Contoso Corporation. Votre directeur veut que vous mettez ensemble une classe de formation sur la sécurité de l'utilisateur final. Pour commencer, utiliser l'Internet pour la recherche de trois cas ou des cas où des individus utilisés ingénierie sociale à la rupture dans un système, et la liste comment ils ont tenté d'obtenir l'accès.

Les réponses varieront. Mais quelques-uns des scénarios d'attaque d'ingénierie sociale courantes sont les suivantes:

- **Une personne téléphone ou de réparation FAI présente pour réparer vos lignes téléphoniques et demande d'accès à votre garde-robe de câblage.**
- **Une personne qui pose en tant qu'auditeur du siège social demande de mettre en place dans une salle de conférence avec un ordinateur et une connexion réseau.**
- **Une personne marche à quelqu'un qui travaille à la compagnie et dit qu'il a laissé ses clés ou un badge à la maison et il ne peut pas entrer dans une pièce sécurisée. Il demande si vous pouvez le faire entrer.**

Leçon 2

Authentification, autorisation et de comptabilité

Objectifs d'apprentissage

Les élèves apprendront:

- Authentification
- Droits et autorisations
- vérification des comptes
- Chiffrement

ODN compétences

• Comprendre l'authentification des utilisateurs.	2.1
• Comprendre les autorisations.	2.2
• Comprendre les politiques de vérification.	2.4
• Comprendre le chiffrement.	2,5

Résumé de la leçon - Notes de cours

Leçon 2 est une leçon clé dans le livre qui couvre l'authentification, l'autorisation et la comptabilité.

La première partie de la leçon authentification discute. Étant donné que les utilisateurs sont déjà familiers avec le nom d'utilisateur et mots de passe, il est un bon endroit pour commencer. Cependant, vous avez également besoin d'expliquer comment les mots de passe peuvent être facilement abusés ou fissurés. Vous pouvez alors discuter des attaques de force brute et les attaques de dictionnaire. La discussion sur les mots de passe couvrira les codes PIN, qui sont habituellement utilisés avec d'autres formes d'authentification.

La partie suivante de couvertures d'authentification ce que vous possédez ou possédez et ce que vous êtes. Qu'est-ce que vous possédez ou possédez présente et discute les certificats numériques, cartes à puce et des jetons de sécurité. Avec ce que vous authentifier êtes Introduit biométrie.

Puisque vous donne un aperçu de l'authentification, la partie suivante de la leçon décrit différentes implémentations d'authentification, y compris RADIUS, TACACS +, Active Directory, Kerberos et NTLM.

Après l'authentification, la leçon porte sur l'autorisation. Encore une fois, souligner que l'autorisation d'abord commencer par l'authentification. Vous serez alors couvrir certaines formes communes d'autorisation, tels que les droits de Windows et les autorisations, les autorisations NTFS, le partage des lecteurs et des dossiers, et le registre.

Pour d'autres données visent à protéger, la partie suivante de la leçon discute le chiffrement. En plus de discuter des types de cryptage, il aborde également les utilisations courantes de chiffrement,

y compris Encrypting File System (EFS), BitLocker, IPSec et réseau privé virtuel (VPN). Il aborde également les diverses formes d'authentification utilisés avec réseaux privés virtuels.

Pour compléter la leçon, la comptabilité ou la vérification est couvert. Soulignez que la vérification est ce qui est utilisé pour garder les administrateurs honnêtes et peut être largement utilisé dans les affaires judiciaires.

Mots clés

liste de contrôle d'accès (ACL) - Liste A de tous les utilisateurs et les groupes qui ont accès à un objet.

comptabilité - Aussi connu comme l'audit, est le processus de garder la trace de l'activité d'un utilisateur lors de l'accès aux ressources du réseau, y compris le temps passé dans le réseau, les services accessibles alors là, et la quantité de données transférées au cours de chaque session.

Active Directory - La technologie de service est un annuaire Active Directory créé par Microsoft qui offre une variété de services de réseau, y compris Lightweight Directory Access Protocol (LDAP), Kerberos basée et authentification unique (SSO) d'authentification unique, DNSbased nommer et d'autres informations sur le réseau et un emplacement central pour l'administration et la délégation de pouvoirs réseau.

part administrative - Un dossier partagé généralement utilisé à des fins administratives.

chiffrement asymétrique - Aussi connu comme la cryptographie à clé publique, utilise deux clés mathématiques pour le chiffrement. Une clé est utilisée pour chiffrer les données, tandis que le second est utilisé pour le déchiffrer.

vérification des comptes - Aussi connu comme la comptabilité, est le processus de garder la trace de l'activité d'un utilisateur lors de l'accès aux ressources du réseau, y compris le temps passé dans le réseau, les services accessibles alors là, et la quantité de données transférées au cours de chaque session.

authentification - Le processus d'identification d'un individu, généralement basée sur un nom d'utilisateur et mot de passe.

autorisation - Le processus d'objets donnant accès au système des individus en fonction de leur identité.

la biométrie - Une méthode d'authentification qui identifie et reconnaît les personnes en fonction de traits physiques, comme les empreintes digitales, reconnaissance faciale, iris, reconnaissance de la rétine et des analyses de reconnaissance vocale.

Pour Go- BitLocker Une nouvelle fonctionnalité dans Windows 7 qui permet aux utilisateurs de crypter les périphériques USB amovibles tels que les lecteurs flash et disques durs externes.

attaque de force brute - Un type d'attaque qui essaie autant de combinaisons possibles de caractères que le temps et permis de l'argent.

intégré dans les groupes - Les groupes par défaut qui sont inclus sous Windows ou Active Directory.

chaîne de certificats - également connu comme le chemin de certification, une liste des certificats utilisés pour authentifier une entité. Il commence avec le certificat de l'entité et se termine par le certificat CA racine.

liste de révocation de certificats (CRL) - Une liste des certificats (ou plus précisément, une liste des numéros de série de certificats) qui ont été révoqués ou ne sont plus valables et ne devrait donc pas être invoqué.

compte d'ordinateur - Un objet logique qui fournit un moyen d'authentification et de vérification d'accès d'un ordinateur à un réseau Windows, ainsi que l'accès aux ressources du domaine.

décryptage - Le processus de conversion des données de retour de format crypté à son format d'origine.

attaque par dictionnaire - Une forme de joindre qui tente tous les mots dans un ou plusieurs dictionnaires. Les listes de mots de passe communs sont généralement testés.

certificat numérique - Un document électronique qui contient une identité, comme un nom d'utilisateur ou de l'organisation, ainsi que d'une clé publique correspondante. Parce qu'un certificat numérique est utilisé pour prouver l'identité d'une personne, il peut également être utilisé pour l'authentification.

signature numérique - Un schéma mathématique qui est utilisé pour démontrer l'authenticité d'un message numérique ou d'un document. Il est également utilisé pour prouver que le message ou le document n'a pas été modifié.

un contrôleur de domaine - Un serveur Windows qui stocke une réplique du compte et des informations de sécurité d'un domaine et définit les limites du domaine.

utilisateur domaine - Un compte utilisateur stocké sur le contrôleur de domaine et vous permet d'accéder aux ressources du domaine, en supposant que vous a accordé des autorisations pour accéder à ces objets.

autorisations effectives - autorisations réelles lors de la connexion et l'accès à un fichier ou un dossier. Ils se composent d'autorisations explicites ainsi que toutes les autorisations héritées.

chiffrement - Le processus de conversion des données dans un format qui ne peut être lu par un autre utilisateur. Une fois qu'un utilisateur a crypté un fichier, ce fichier reste crypté automatiquement lorsqu'il est stocké sur le disque.

autorisation explicite - Autorisations accordées directement à un fichier ou un dossier.

groupe - Une collection ou une liste de comptes d'utilisateurs ou comptes d'ordinateur.

fonction de hachage - comme un cryptage à sens unique, ce qui signifie que, après quelque chose a été chiffré avec cette méthode, il ne peut pas être déchiffré.

autorisation héritée - Autorisations accordées à un dossier (objet parent ou d'un conteneur) qui se jette dans les objets enfants (sous-dossiers ou fichiers) à l'intérieur de ce dossier.

Sécurité IP (IPsec) - Une suite de protocoles qui fournit un mécanisme pour l'intégrité des données, l'authentification et la confidentialité pour le protocole Internet. Il est utilisé pour les données qui sont envoyées protègent entre les hôtes sur un réseau en créant des tunnels électroniques sécurisés entre deux machines ou appareils. IPsec peut être utilisé pour l'accès à distance, VPN, connexions serveur, les connexions LAN ou WAN connexions.

Kerberos - Le domaine par défaut protocole d'authentification réseau informatique, ce qui permet aux hôtes de prouver leur identité sur un réseau non sécurisé de manière sécurisée.

Clé - Peut être considéré comme un mot de passe, est appliqué mathématiquement en texte brut pour fournir de chiffrement ou texte crypté. Les différentes touches produisent différentes sorties cryptées.

compte utilisateur local - Un compte utilisateur qui est stocké dans la base de données Security Account Manager (SAM) sur l'ordinateur local.

serveur membre - Un serveur qui ne fonctionne pas en tant que contrôleur de domaine.

l'authentification multifactorielle - Lorsque deux ou plusieurs méthodes d'authentification sont utilisés pour quelqu'un authentifier.

nonrepudiation - Empêche une partie de nier les actions qu'il a menées.

NTFS - Le système de fichiers préféré pour le système d'exploitation Windows d'aujourd'hui.

La permission NTFS - autorisations vous permettent de contrôler les utilisateurs et les groupes peuvent accéder aux fichiers et dossiers sur un volume NTFS.

NTLM - Le protocole d'authentification par défaut pour Windows NT, les ordinateurs autonomes qui ne font pas partie d'un domaine, et les situations dans lesquelles vous authentifiez à un serveur en utilisant une adresse IP.

unités organisationnelles (OU) - Un conteneur utilisé dans Active Directory pour aider à organiser des objets dans un domaine et de minimiser le nombre de domaines.

propriétaire - Identité A qui commande un objet dont les autorisations sont définies sur l'objet et à qui les autorisations sont accordées.

mot de passe - Une série secrète de caractères qui permet à un utilisateur d'accéder à un fichier particulier, ordinateur ou programme.

autorisation - Définit le type d'accès accordé à un objet (un objet peut être identifié par un identificateur de sécurité) ou attribut d'objet.

numéro d'identification personnel (NIP) - Un mot de passe numérique secret partagé entre un utilisateur et un système qui peut être utilisé pour authentifier l'utilisateur au système.

l'infrastructure de clé publique (PKI) - Un système composé de matériel, des logiciels, des politiques et des procédures qui créent, gèrent, distribuent, utiliser, stocker et révoquer des certificats numériques. Au sein de l'infrastructure à clé publique, l'autorité de certification (CA) se fixe une clé publique avec les identités des utilisateurs respectifs et délivre des certificats numériques contenant la clé publique.

enregistrement - Une base de données centrale et sécurisée dans lequel Windows stocke toutes les informations de configuration matérielle, les informations de configuration logicielle, et les politiques de sécurité du système. Les composants qui utilisent le registre comprennent le noyau Windows, les pilotes de périphériques, programmes d'installation, profils matériels et des profils d'utilisateurs.

droite - Autorise un utilisateur d'effectuer certaines actions sur un ordinateur, telles que la connexion à un système interactif ou la sauvegarde des fichiers et des répertoires sur un système. Les droits des utilisateurs sont affectés par des politiques locales ou des stratégies de groupe Active Directory.

Secure Sockets Layer (SSL) - Un système cryptographique qui utilise deux clés pour Crypter les données, une clé publique connue de tous et une clé privée ou secrète connue uniquement du destinataire du message. La clé publique est publiée dans un certificat numérique, ce qui confirme l'identité du serveur web.

Sécurité Account Manager (SAM) - Une base de données de sécurité locale trouve sur la plupart des ordinateurs Windows.

jeton de sécurité - Un dispositif physique qu'un service informatique utilisateur autorisé est donnée pour faciliter l'authentification.

les autorisations de partage - autorisations attribuées à des dossiers ou des lecteurs partagés.

dossier partagé - Une technologie qui permet l'accès des fichiers de données sur le réseau.

connexion unique (SSO) - Une technologie qui vous permet de connecter une seule fois et d'accès multiple liés, mais les systèmes de logiciels indépendants, sans avoir à se connecter à nouveau.

carte à puce - Une carte format de poche avec des circuits intégrés intégrés constitués de composants de stockage de mémoire non volatile et peut-être dédié logique de sécurité.

chiffrement symétrique - Utilise une seule clé pour crypter et décrypter les données.

syslog - Une norme pour la journalisation des messages de programme accessibles par des dispositifs qui auraient pas autrement une méthode de communication.

compte d'utilisateur - Un objet logique qui permet à un utilisateur de se connecter à un ordinateur et un domaine.

réseau privé virtuel (VPN) - Une technologie qui relie deux ordinateurs à travers un réseau de widearea tel que l'Internet. Pour maintenir la connexion sécurisée est encapsulées et crypté les données envoyées entre les deux ordinateurs.

Lesson 2

Autorisation d'authentification et comptabilité

évaluation des connaissances

Choix multiple

Entourez la lettre qui correspond à la meilleure réponse.

1. Lequel des éléments suivants n'est pas une méthode d'authentification?

une. Quelque chose que l'utilisateur connaît

b. possède quelque chose que l'utilisateur ou possède

c. Chiffrement

ré. Que l'utilisateur est

2. Lequel des éléments suivants n'est pas un dispositif biométrique?

une. lecteur de mot de passe

b. scanner rétinien

c. lecteur d'empreintes digitales

ré. scanner visage

3. Lequel des services suivants est utilisé pour l'authentification centralisée, autorisation et comptabilité?

une. VPN

b. PGP

c. RAYON

ré. PKI

4. Quelle est la méthode d'authentification principale utilisée sur Microsoft Active Annuaire?

une. LDAP

b. Kerberos

c. NTLAN

ré. SSO

5. Le chronométreur maître et maître de mot de passe change dans un actif répertoire domaine est:

une. PDC Emulator.

b. DÉBARRASSER.

c. maître infrastructure.

ré. de schéma.

6. comptes d'utilisateurs locaux se trouvent dans:

une. Active Directory.

b. Enregistrement.

c. SAM.

ré. LDAP.

7. A (n) _____ autorise un utilisateur à effectuer certaines actions sur un ordinateur.

une. autorisation

b. Algorithme de cryptage

c. protocole d'authentification

ré. droite

8. Lequel des systèmes de fichiers suivants offre la meilleure sécurité?

une. GRAISSE

b. FAT32

c. NTFS

ré. EFS

9. Quelle autorisation NTFS est nécessaire pour les attributs de changement et les autorisations?

une. Controle total

b. Modifier

c. Lecture et exécution

ré. Écrire

dix. Quel type d'autorisation est accordée directement à un fichier ou un dossier?

une. Explicite

b. Hérité

c. Efficace

ré. Partager

11. Si vous copiez un fichier ou un dossier à un nouveau volume, quels sont les droits que le fichier ou le dossier ont?

une. Les mêmes autorisations qu'ils avaient avant.

b. Les mêmes autorisations que le dossier cible.

c. Les mêmes autorisations que le dossier source.

ré. Aucune autorisation à tous.

12. Laquelle des utilisations suivantes une ACL?

une. dossier NTFS

b. utilisateur Active Directory

c. Clé d'enregistrement

ré. les droits de connexion

13. Quel type de clé est une clé pour le chiffrement et une clé différente pour décryptage?

une. Symétrique

b. Asymétrique

c. Fonction hash

ré. PKI

14. Quelle infrastructure est utilisée pour assigner et valider les certificats numériques?

une. algorithme asymétrique

b. Active Directory

c. PKI

ré. VPN

15. Quelle technologie est utilisée pour chiffrer un fichier individuel sur un volume NTFS?

une. BitLocker

b. BitLocker To Go

c. PPTP

ré. EFS

Remplir les trous

Complétez les phrases suivantes en écrivant le mot correct ou des mots dans les espaces prévus.

1. A (n) **numéro d'identification personnel (NIP)** est un numérique secrète mot de passe partagé entre un utilisateur et un système qui peut être utilisé pour authentifier l'utilisateur pour le système.

2. Une carte format de poche avec des circuits intégrés embarqués qui est utilisé pour l'authentification est connu en tant que (n) **carte à puce** .

3. Un dispositif qui peut vous donner un second mot de passe pour se connecter à un système est un) **jeton de sécurité** .

4. **un contrôleur de domaine** détient une copie de la base de données centralisée utilisée dans Active Directory.

5. Par défaut, l'horloge de votre ordinateur ne doit pas être plus gros que **cinq** minutes ou vous pourriez avoir des problèmes avec l'authentification Kerberos.

6. A (n) **autorisation** définit le type d'accès sur un objet ou le propriétés d'un objet tel qu'un fichier NTFS ou une imprimante.

sept. **Hérité** autorisations flux d'un objet parent à un objet enfant.

8. Lorsque vous ne pouvez pas accéder à un dossier parce que quelqu'un a enlevé le autorisations afin que personne ne peut y accéder, vous devez prendre **la possession** du dossier.

9. La base de données centralisée qui détient plus de la configuration de Windows est connu sous le nom **enregistrement** .

dix. Pour suivre les activités d'un utilisateur dans Windows, vous devez activer **vérification des comptes** .

évaluation des compétences

Scénario 2-1: Comprendre les inconvénients de Biométrie

Vous êtes l'administrateur informatique pour la Contoso Corporation. Votre CIO veut que vous enquêtez sur l'utilisation possible de la biométrie à des fins de sécurité. Le CIO comprend

ce que la biométrie est et comment cette technologie peut être utilisée, mais il ne comprend pas les inconvénients potentiels de l'utilisation de la biométrie. Que devriez-vous lui dire?

Bien que la biométrie offre une sécurité renforcée, il est idéal pour toutes les situations. D'une part, des solutions biométriques coûtent beaucoup d'argent et devront être installés et mis sur toutes les portes que vous souhaitez protéger. En second lieu, vous devez configurer chaque utilisateur qui utilisera la biométrie, et vous devrez mettre en place au moins un poste de travail et un administrateur pour ajouter des utilisateurs au système biométrique. Vous aurez également besoin d'un endroit pour stocker la base de données. Ensuite, en tant que nouveaux employés commencent par votre organisation, vous devrez les ajouter au système. De plus, lorsqu'une personne quitte l'organisation, vous devrez désactiver ou supprimer son compte.

Scénario 2-2: Audit Limitation

Vous êtes l'administrateur informatique pour la Contoso Corporation. Votre CIO a besoin de savoir quand un utilisateur a accédé à un certain dossier. Cependant, ces informations ne sont pas disponibles parce que la vérification n'a pas été activé. Pour vous assurer que cela ne se reproduise pas à l'avenir, le CIO vous demande d'activer pour tout audit. Comment devez-vous répondre?

Pour que la vérification soit efficace, vous devez d'abord déterminer ce qui doit être vérifié, vous devez activer la vérification de cette activité, une tâche ou ressource. De plus, la vérification prend des ressources système. Par conséquent, si vous activez l'audit sur trop d'éléments, il va ralentir le système. En outre, si vous activez l'audit pour tout, vous remplirez rapidement les journaux, ralentir le système de manière significative, et quand vous avez besoin de trouver un événement spécifique, vous pourriez être submergé par la quantité d'informations qu'il ya à éplucher.

évaluation des compétences

Scénario 2-3: Regarder des autorisations NTFS

Connectez-vous en tant qu'administrateur sur un ordinateur exécutant Windows 7 ou Windows Server 2008. Créez un groupe appelé Les gestionnaires sur votre ordinateur. Maintenant, créez un compte d'utilisateur appelé JSmith et l'affecter au groupe des gestionnaires. Ensuite, créez un compte utilisateur appelé JHamid. Créez un dossier appelé SharedTest, et créer un fichier texte appelé test.txt dans le dossier SharedTest. Partagez le dossier. Attribuer Autoriser le contrôle total à tout le monde. Attribuer lecture et d'exécution au groupe des gestionnaires. Connectez-vous en tant que JHamid et essayez d'accéder au dossier \\ localhost \ SharedTest. Ensuite, connectez-vous comme JSmith et l'accès essayer le dossier \\ localhost \ SharedTest.

1. Connectez-vous en tant qu'administrateur.

2. Cliquez sur le bouton Démarrer, droit sur Poste de travail et sélectionnez Gérer.

3. Gestionnaire de serveur, développez Configuration et développez les utilisateurs locaux et groupes.

4. Faites un clic droit et sélectionnez Utilisateurs nouveaux utilisateurs.

5. Tapez le nom d'utilisateur comme JSmith, et attribuer un mot de passe Password01. Désélectionnez L'utilisateur doit changer le mot de passe à la prochaine connexion. Cliquez sur le bouton Créer.

6. Tapez le nom d'utilisateur comme JHamid et attribuer un mot de passe Password01. Désélectionnez L'utilisateur doit changer le mot de passe à la prochaine connexion. Cliquez sur le bouton Créer.

sept. Cliquez sur Groupes.

8. Faites un clic droit Groupes et cliquez sur Nouveau groupe. Pour le nom du groupe, tapez
Les gestionnaires. Cliquez sur le bouton Ajouter. Tapez JSmith, et cliquez sur le bouton OK. Cliquez sur le bouton Créer.

9. Cliquez sur le bouton Fermer pour fermer la boîte de dialogue du groupe.

dix. Cliquez-droit sur le bureau et sélectionnez Nouveau, puis cliquez sur le dossier. Tapez SharedTest et appuyez sur Entrée.

11. Cliquez-droit sur le dossier SharedTest et sélectionnez Propriétés.

12. Cliquez sur l'onglet Partage.

13. Cliquez sur le bouton Partage avancé.

14. Sélectionnez l'option Partager ce dossier.

15. Cliquez sur le bouton Autorisations.

16. Avec tout le monde sélectionné, cliquez sur le contrôle total et Allow cliquez sur OK.

17. Cliquez sur OK une fois de plus pour se rendre à la boîte de propriétés.

18. Cliquez sur l'onglet Sécurité.

19. Cliquez sur le bouton Modifier.

20. Cliquez sur le bouton Ajouter. Tapez gestionnaires et cliquez sur le bouton OK.

21. Cliquez sur le bouton OK pour fermer la boîte des autorisations.

22. Cliquez sur OK pour fermer la boîte de propriétés.

23. Double-cliquez sur le dossier SharedTest pour l'ouvrir.

24. Cliquez droit sur l'espace vide du dossier SharedTest et sélectionnez Nouveau puis Fichier texte. Tapez Test et appuyez sur Entrée.

25. Double-cliquez sur le fichier test.txt et tapez votre nom.

26. Connectez-vous en tant qu'administrateur et connectez-vous en tant que JHamid. Essayez d'accéder à la \\ localhost \ SharedTest et ouvrez le fichier test.txt.

27. Connectez-vous comme JHamid et vous connecter en tant JSmith. Essayez d'accéder à la \\ localhost \ SharedTest et ouvrez le fichier test.txt.

Scénario 2-4: Regarder EFS

Ajouter JHamid au groupe des gestionnaires vous établi dans l'exercice précédent. Maintenant, connectez-vous comme JSmith et chiffrer le fichier test.txt avec EFS. Enfin, connectez-vous comme JHamid et essayer d'accéder au fichier test.txt.

1. Connectez-vous en tant qu'administrateur.

2. Cliquez sur le bouton Démarrer, droit sur Poste de travail et sélectionnez Gérer.

3. Gestionnaire de serveur, développez Configuration et développez les utilisateurs locaux et groupes.

4. Cliquez sur Groupes.

5. Double-cliquez groupe gestionnaires.

6. Cliquez sur le bouton Ajouter. Tapez JHamid et cliquez sur le bouton OK.

sept. Cliquez sur OK pour fermer la boîte de propriétés.

8. Double-cliquez sur le dossier SharedTest.

9. Cliquez droit sur le fichier test.txt et sélectionnez Propriétés.

dix. Cliquez sur le bouton Avancé.

11. Cliquez sur Crypter le contenu pour les données sécurisé. Cliquez sur le bouton OK.

12. Cliquez sur le bouton OK pour Propriétés à proximité.

13. Lorsque l'ordinateur vous avertit sur ce qu'il faut chiffrer, cliquez sur OK.

14. Connectez-vous en tant qu'administrateur et connectez-vous en tant que JSmith.

15. Ouvrez le \\ localhost \ SharedTest et essayez d'ouvrir le fichier test.txt.

Lecon 3

Comprendre les politiques de sécurité

Objectifs d'apprentissage

Les élèves apprendront:

- Comment utiliser les stratégies de mot de passe pour améliorer la sécurité

ODN compétences

- Comprendre les politiques de mot de passe. 2.3

Résumé de la leçon - Notes de cours

Leçon 3 est une continuation de la leçon 2, de discuter plus sur les mots de passe et comment casser les mots de passe. Il a également la façon d'améliorer la sécurité de votre réseau en utilisant des mots de passe et comment vous pouvez imposer l'utilisation de mots de passe forts.

La première partie de la leçon traite des mots de passe forts et complexes. Soulignez que les mots de passe plus longs qui sont modifiés sont souvent plus difficiles à craquer. Toutefois, si les mots de passe deviennent trop longues, les utilisateurs peuvent essayer contourner la sécurité en écrivant leurs mots de passe et de les stocker près de leurs ordinateurs. Les stratégies de groupe sont également discutées pour appliquer ces paramètres.

La dernière partie de la leçon discute des attaques communes, y compris l'attaque de dictionnaire, les attaques par force brute, en utilisant renifleurs, keyloggers, et en essayant de deviner les mots de passe.

Mots clés

verrouillage de compte - Fait référence au nombre de tentatives de connexion incorrectes autorisées avant qu'un système verrouille un compte. Chaque mauvaise tentative de connexion est suivi par le mauvais compteur d'ouverture de session, et lorsque le compteur dépasse le seuil de verrouillage de compte, aucune autre tentative d'ouverture de session sont autorisés.

Mot de passe Cracked - Un mot de passe qui obtient l'accès à un fichier de mot de passe crypté à partir d'un poste de travail ou serveur. Une fois qu'il ou elle a accès, l'attaquant commence à tourner des outils de craquage de mots de passe sur le fichier, avec un oeil à briser autant de mots de passe que possible et les tirer parti de compromettre davantage le réseau et les systèmes de l'entreprise.

attaque par dictionnaire - Une attaque qui utilise un dictionnaire contenant une longue liste de mots de passe potentiels que l'attaquant tente alors en conjonction avec un ID utilisateur pour tenter de deviner le mot de passe approprié.

Objet de stratégie de groupe (GPO) - Un ensemble de règles qui permettent un contrôle granulaire de l'administrateur sur la configuration des objets dans Active Directory (AD), y compris les comptes d'utilisateurs, les systèmes d'exploitation, des applications et d'autres objets AD.

keylogger - Dispositif de logiciel ou de matériel qui capture les mots de passe et d'autres données critiques directement à partir du clavier.

mot de passe - Une série secrète de caractères qui permet à un utilisateur d'accéder à un fichier particulier, ordinateur ou programme.

renifleurs - Un logiciel spécialement conçu des applications (et dans certains cas) du matériel que les paquets de réseau de capture comme ils traversent un réseau, les afficher pour l'attaquant.

mot de passe fort - Mot de passe A qui est difficile à deviner, car il est long et a un mélange de différents types de caractères. Il a aussi assez aléatoire où il ne pouvait pas être facile à deviner.

Lesson 3

Comprendre les politiques de sécurité

évaluation des connaissances

Choix multiple

Encerclez la ou les lettres qui correspondent à la meilleure réponse ou des réponses.

1. Lequel des éléments suivants ne sont pas des contrôles de mot de passe valides? (Choisissez tout ce qui correspond.)

une. Age minimum Mot de passe

b. Maximum Password Age

c. Longueur maximale Mot de passe

ré. Compte Seuil de verrouillage

e. Histoire de passe

2. Lequel des éléments suivants serait un mot de passe acceptable sur un système Windows 7 Professionnel avec Password Complexity activé et réglé de longueur minimale du mot à huit? (Choisissez tout ce qui correspond.)

une. Summer2010

b. $$ Thx17

c. ^^ RGood4U

ré. Mot de passe

e. St @ rTr3k

3. Quel est le réglage maximal pour l'âge minimum de mot de passe?

une. 14

b. 999

c. 998

ré. 256

4. Vous configurez votre premier sécurisé Windows 7 Professional station de travail et vous définissez l'historique de mot de passe. Quels sont les paramètres minimum et maximum que vous pouvez utiliser? (Choisissez la meilleure réponse.)

une. 0, 14

b. 1, 14

c. 0, 24

ré. 1, 24

e. 0, 998

5. Lequel des éléments suivants sont des types d'attaques de mot de passe? (Choisir des réponses Deux)

une. Cracking

b. L'homme au milieu

c. Schtroumpf

ré. spoofing

e. Force brute

6. Une forme d'attaque de mot de passe par force brute utilise une longue liste de mots de passe prédéfinis. Qu'est-ce que cette forme d'attaque de force brute appelée? (Choisissez la meilleure réponse.)

une. Bible attaque

b. attaque Cracking

c. attaque deviner

ré. attaque par dictionnaire

7. En tant que chef de la sécurité pour un petit dossier médical société de traitement, vous soupçonnez qu'un concurrent attaquera votre réseau bientôt. Ayant travaillé dans l'entreprise pendant un certain temps, vous êtes à peu près sûr que ce concurrent va essayer de lancer une attaque contre le dictionnaire un de vos serveurs d'applications Windows. Vous voulez être sûr que votre concurrent ne peut pas entrer dans le serveur en utilisant cette méthode d'attaque. Quel réglage si vous réglez pour assurer cette attaque a une chance limitée au succès? (Choisissez la meilleure réponse.)

une. Le mot de passe minimum

b. Compte Seuil de verrouillage

c. Histoire de passe

ré. Maximum Password Age

8. Vous êtes le chef du service de sécurité de l'entreprise, et l'équipe Microsoft vous a demandé une aide à la définition des contrôles de mot de passe sur leur nouveau serveur autonome. Quel outil administratif devrait vous utiliser pour configurer ces paramètres?

une. Utilisateurs et ordinateurs Active Directory

b. Gestion d'ordinateur

c. Service de sécurité

ré. Stratégie de sécurité locale

9. Quels sont les deux nouvelles fonctionnalités introduites dans Windows Server 2008 qui permettent l'utilisation des politiques de mot de passe grains fins? (Choisissez tout ce qui correspond.)

une. Objet de la politique mondiale

b. Mot de passe Paramètres de conteneur

c. Mot de passe objet Paramètres

ré. Politique de mot de passe

10. Pourquoi utiliser un âge minimum de mot de passe?

une. Pour vous assurer que quelqu'un ne pense pas un mot de passe

b. Pour arrêter quelqu'un d'essayer encore et de deviner un mot de passe

c. Pour vous assurer que l'utilisateur ne réinitialise pas un mot de passe à plusieurs reprises jusqu'à ce qu'il peut réutiliser son mot de passe d'origine

ré. Pour réinitialiser automatiquement un mot de passe

Remplir les trous

1. Un ensemble de règles qui permet un contrôle granulaire de l'administrateur sur la configuration d'objets dans Active Directory (AD), y compris les comptes d'utilisateurs, les systèmes d'exploitation, des applications, et d'autres objets de l'AD, qui est connu en tant que (n) **Objet politique globale (GPO)** .

2. Le nombre de tentatives de connexion incorrectes autorisé avant une volonté du système verrouiller un compte est connu sous le nom **Compte Seuil de verrouillage** .

3. Le paramètre qui détermine le nombre de mots de passe uniques qui doivent être utilisé avant un mot de passe peut être réutilisé est le **Histoire de passe** .

4. Le type d'attaque qui utilise une longue liste de mots de passe potentiels est connu sous le nom (n) **attaque par dictionnaire** .

5. Lorsque vous utilisez un logiciel spécial pour lire les données qu'il est diffusé sur une réseau, vous êtes **reniflement** le réseau.

6. **compteur de verrouillage du compte après réinitialisation** a besoin d'être inférieur ou égale à la durée de verrouillage de compte.

sept. Le réglage le plus élevé que l'utilisation de verrouillage de compte Durée de boîte est **999** .

8. Dans Windows Server 2008 Active Directory, la **Stratégie de domaine par défaut** applique automatiquement si vous n'avez pas défini une politique de mot de passe à grain fin.

9. Les trois paramètres de configuration de verrouillage de compte sont **Compte durée lock-out** , **Seuil de verrouillage** , et **compteur de verrouillage du compte après réinitialisation** .

10. A **un service** compte est un type de compte que vous pouvez configurer afin que le mot de passe ne prend pas fin.

évaluation des compétences

Scénario 3-1: Comprendre à long mots de passe

une. Disons que vous avez un NIP de quatre chiffres. Chaque chiffre peut être 0, 1, 2, 3, 4, 5, 6, 7, 8 ou 9, soit un total de 10 chiffres possibles. Combien différents sont possibles PINs?

10 x 10 x 10 x 10 = 10.000 combinaisons

b. Disons que vous avez un mot de passe de quatre lettres et chaque caractère dans la mot de passe doit être une lettre minuscule (a-z). Il y a 26 lettres dans l'alphabet. Combien de mots de passe différents sont possibles?

26 x 26 x 26 x 26 = 456,976 combinaisons

c. Disons que vous avez un mot de passe de six lettres, et chaque caractère du mot de passe doit être une lettre minuscule (a-z). Combien de combinaisons différentes sont possibles?

26 x 26 x 26 x 26 x 26 x 26 = 308,915,776 combinaisons

ré. Disons que vous avez un mot de passe de huit lettres et chaque caractère dans la mot de passe doit être une lettre minuscule (a-z). Combien de combinaisons différentes sont possibles?

26 x 26 x 26 x 26 x 26 x 26 x 26 x 26 = 208,827,064,576 combinaisons

e. Disons que vous avez un mot de passe de huit lettres et chaque caractère dans la mot de passe doit être une lettre minuscule (a-z) ou une lettre majuscule (A-Z). Combien de combinaisons différentes sont possibles?

52 x 52 x 52 x 52 x 52 x 52 x 52 x 52 = 53,459,728,531,456 combinaisons

F. Disons que vous avez un mot de passe de huit lettres et chaque caractère dans la mot de passe doit être une lettre minuscule (a-z), une lettre majuscule (A-Z), un chiffre (0-9), ou un caractère spécial (~ ` ! @ # $% ^ & * () + = _- {[}] | \ :; » '<,> ou /).?. Combien de combinaisons différentes sont possibles?

94 x 94 x 94 x 94 x 94 x 94 x 94 x 94 = 6,095,689,385,410,816 combinaisons

Scénario 3-2: Modification des mots de passe

Imaginez que vous travaillez pour la Contoso Corporation. Votre DSI vous dit qu'il a juste obtenu un message sur son ordinateur en disant qu'il doit changer son mot de passe. Il veut savoir pourquoi il doit non seulement utiliser un tel mot de passe relativement longue, mais aussi pourquoi il faut changer ce mot de passe sur une base régulière. Que devriez-vous lui dire?

Une technique de piratage en essayant de trouver un mot de passe est d'essayer toutes les combinaisons possibles de personnages jusqu'à ce que vous arrive sur le mot de passe. Par conséquent, plus le mot de passe, plus les combinaisons d'un pirate informatique qui utilisent cette méthode devrait essayer. De plus, si vous utilisez un mot de passe qui nécessite des lettres majuscules, lettres minuscules, des chiffres et des caractères spéciaux, le pirate aurait aussi plus de combinaisons à essayer que si votre mot de passe inclus uniquement à l'aide des chiffres ou des lettres minuscules.

Un ordinateur peut être programmé pour essayer ces différentes combinaisons, et parce que les ordinateurs sont beaucoup plus rapides que les humains, ils peuvent passer par les listes de ces combinaisons beaucoup plus vite que nous pouvions rêver. En outre, les ordinateurs continuent de plus en plus rapides, ils peuvent accomplir cette tâche plus rapidement qu'auparavant. Par conséquent, en plus de garder votre mot de passe long, vous devez également modifier votre mot de passe souvent pour que les attaquants devront recommencer à essayer toutes les combinaisons possibles avec chaque nouveau mot de passe.

évaluation des compétences

Scénario 3-3: Gestion des utilisateurs

Se connecter à un ordinateur exécutant Windows 7 et créer un compte pour John Adams (JAdams) à l'aide du panneau de configuration. Ensuite, ajoutez JAdams au groupe Administrateur. Définir le mot de passe JAdams à Password01. Vérifiez les groupes qui JAdams est membre de l'utilisation du contrôle de gestion informatique.

1. Ouvrez une session sur un ordinateur fonctionnant sous Windows 7.
2. Cliquez sur **Début**. Puis clique **Panneau de configuration**. La fenêtre Panneau de configuration apparaît.
3. Cliquez sur **Comptes utilisateur,** ensuite **Comptes utilisateur** encore. L'utilisateur panneau de contrôle des comptes apparaît.
4. Cliquez sur **Gérer les comptes utilisateur,**. L'utilisateur boîte de dialogue Comptes apparaît.
5. Pour créer un nouveau compte, cliquez sur le **Ajouter** bouton. le **Ajouter un nouvel utilisateur** page apparaît.
6. Dans la zone de texte Nom d'utilisateur, tapez **JAdams;** puis cliquez sur le **Prochain** bouton.

7. **Utilisateur standard** sélectionné, cliquez sur le **terminer** bouton.

8. Clique le **Avancée** onglet, puis cliquez sur le **Avancée** bouton sous **Utilisateur avancé la gestion.** Les utilisateurs locaux et la console Les groupes doivent ouvrir.

9. Cliquez sur **Utilisateurs** sous Utilisateurs et groupes locaux.

dix. Clic-droit **Utilisateurs** et sélectionnez **Nouvel utilisateur.** Tous les utilisateurs locaux doivent apparaître.

11. Dans la zone de texte Nom d'utilisateur, tapez **JAdams.** Dans la zone de texte Nom complet, tapez **John Adams.** Indiquez un mot de passe **Pa s w0rd.** Clique le **Créer** bouton.

12. Clique le **Fermer** bouton pour fermer la page Nouvel utilisateur.

13. Clic-droit **JAdams** et sélectionnez **Propriétés.**

14. Clique le **Membre de** languette.

15. Clique le **Annuler** bouton pour fermer les propriétés JAdams.

16. Retour aux comptes d'utilisateurs dans le Panneau de configuration.

17. Cliquez sur **Gérer les comptes utilisateur,.**

18. Cliquez sur **JAdams** et cliquez sur **Propriétés.** Notez l'appartenance à un groupe de l'utilisateur.

19. Cliquez sur **D'accord** pour fermer la boîte de propriétés de JAdams.

20. Clique le **réinitialiser le mot de passe** bouton.

21. Dans le **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** zones de texte, le type **Password01** et cliquez sur **Changer le mot de passe.** Cliquez sur **D'accord** continuer.

22. Modifier le dos de mot de passe **Pa s w0rd.**

23. Cliquez **Début.** Puis clique **Panneau de configuration.** La fenêtre Panneau de configuration apparaît.

24. Cliquez sur **Système et sécurité > Outils administratifs.** Les Outils d'administration fenêtre apparaît. Vous pouvez également taper « Outils d'administration » dans la zone de recherche du menu Démarrer pour ouvrir directement.

25. Double-cliquez sur **Gestion d'ordinateur.** La console Gestion de l'ordinateur apparaît.

26. Élargir le **Utilisateurs et groupes locaux** dossier et sélectionnez la **Utilisateurs** sous-dossier. Une liste de les comptes utilisateur sur l'ordinateur apparaît.

27. Double-cliquez sur le **JAdams** compte d'utilisateur. boîte des propriétés JAdams apparaît. Les

28. Dans le **Nom complet** zone de texte, tapez **John Adams.** Assurez-vous que la **Mot de passe jamais arrive à expiration** case à cocher est claire. Sélectionnez le **Utilisateur doit changer le mot de passe à la prochaine ouverture de session** cochez la case puis cliquez sur **D'ACCORD.**

Scénario 3-4: Configuration d'une stratégie de sécurité locale

Sur un ordinateur fonctionnant sous Windows 7, ouvrez Gestion des stratégies de groupe pour accéder à la stratégie de groupe local. Voir la politique de mot de passe et compte Stratégie de verrouillage.

1. Ouvrez une session sur un ordinateur fonctionnant sous Windows 7.

2. Ouvrez Outils d'administration et sélectionnez Gestion des stratégies de groupe.

3. Cliquez sur le bouton Démarrer et tapez mmc dans le texte des programmes de recherche et les fichiers boîte. Appuyez sur Entrée . Si l'ordinateur demande êtes-vous sûr que vous voulez faire ce changement, cliquez sur Oui.

4. Ouvrez le menu Fichier et sélectionnez Ajouter / Supprimer un composant logiciel enfichable.

5. Sélectionnez la stratégie de groupe GPO Starter Editor et cliquez sur le bouton Ajouter. Quand l'ordinateur local apparaît, cliquez sur le bouton Terminer.

6. Cliquez sur le bouton OK pour fermer la Ajouter ou supprimer la boîte Snap-ins.

sept. Développez Stratégie de l'ordinateur local.

8. Développez stratégie ordinateur local, Configuration ordinateur, Paramètres Windows, Paramètres de sécurité, Stratégies de comptes, et la politique de mot de passe.

9. Sélectionnez Compte Stratégie de verrouillage.

dix. Fermez la console MMC.

leçon 4

Comprendre la sécurité des réseaux

Objectifs d'apprentissage

Les élèves apprendront à:

- Utilisez Firewalls dédiés pour protéger un réseau
- Contrôle d'accès avec la protection d'accès réseau (NAP)
- Utilisez isolement pour protéger le réseau
- Protéger les données avec la sécurité Protocole
- Sécuriser un réseau sans fil

ODN compétences

• Comprendre les pare-feu dédiés.	3.1
• Comprendre la protection d'accès réseau (NAP).	3.2
• Comprendre l'isolement du réseau.	3.3
• Comprendre la sécurité du protocole.	3.4
• Comprendre la sécurité sans fil.	1.4

Résumé de la leçon - Notes de cours

Leçon 4 couvre la sécurité du réseau, y compris en utilisant des routeurs, pare-feu et des protocoles aider à sécuriser un réseau. Avant de discuter de la technologie spécifique, la leçon présente le modèle OSI. Pour beaucoup d'étudiants, le modèle OSI est difficile à saisir au premier abord parce que ce n'est pas quelque chose qu'ils peuvent toucher et à gérer. Au lieu de cela, il est un moyen de décrire la technologie, des protocoles et des services et la façon dont ils interagissent les uns avec les autres. Il est toujours préférable à la fin en regardant le modèle TCP / IP, qui est une version simplifiée du modèle OSI et vous pouvez montrer comment il se rapporte à un paquet réel.

Ensuite, la leçon aborde différentes technologies dans la protection d'un réseau, en commençant par les pare-feu. Cela comprend l'examen des différents types de pare-feu et explique les meilleurs pare-feu d'aujourd'hui contiennent diverses fonctionnalités. Pendant que vous discutez de filtrage de paquets, il est un bon moment pour couvrir les applications communes et les ports qu'ils utilisent. La section se termine en discutant des pare-feu matériels et logiciels.

La partie suivante de la leçon discute NAP, la technologie de Microsoft que les contrôles qui peuvent accéder au réseau en fonction de certains attributs (comme ce que les mises à jour de Windows sont chargés et si l'ordinateur est équipé d'un logiciel antivirus à jour).

Après NAP, l'isolement est utilisé pour protéger le réseau, y compris l'utilisation des réseaux locaux virtuels (VLAN), les routeurs, les systèmes de détection d'intrusion, intrusion, protégerez les systèmes NAT, DMZ, VPN et IPSec. Ensuite, la leçon aborde différents types d'attaques et comment ils peuvent être

évité. La dernière partie traite de cours avec les réseaux sans fil, y compris SSID, WEP, WPA et WPA2.

Mots clés

pare-feu au niveau applicatif - Aussi connu sous le nom des serveurs proxy. Fonctionne en effectuant une inspection approfondie des données d'application car il traverse le pare-feu. Les règles sont définies par l'analyse des demandes des clients et des réponses d'application, puis appliquer le comportement de l'application correcte.

pare-feu au niveau du circuit - Généralement considéré comme la technologie de pare-feu de deuxième génération. Ils travaillent de façon similaire aux pare-feu-filtrage de paquets, mais ils fonctionnent au niveau des couches de transport et session du modèle OSI.

DMZ (zone démilitarisée) - Une configuration de pare-feu utilisée pour ordinateurs sécurisés sur un segment de réseau. Dans la plupart des zones démilitarisées, les hôtes sur la zone démilitarisée sont connectés derrière un pare-feu qui est connecté à un réseau public comme Internet.

DNS Security Extensions (DNSsec) - Il ajoute des dispositions de sécurité au DNS afin que les ordinateurs puissent vérifier qu'ils ont été dirigés vers des serveurs appropriés.

DNS empoisonnement - Une attaque contre les informations mises en cache sur votre serveur DNS.

usurpation d'adresse DNS - l'usurpation d'identité DNS se produit lorsqu'un attaquant est en mesure d'intercepter une requête DNS et de répondre à la demande avant que le serveur DNS est capable.

pare-feu - Un système qui est conçu pour protéger un ordinateur ou un réseau informatique contre les attaques réseau. Un pare-feu ne présente en filtrant les paquets de données qui sont traversant le réseau.

net miel - Une collection de honeypots utilisé pour présenter un attaquant avec un environnement d'attaque encore plus réaliste.

Pot de miel - Un piège pour les pirates.

pare-feu hôte - Un type de logiciel pare-feu installé sur un hôte et utilisé pour protéger l'hôte contre les attaques réseau.

Les systèmes de détection d'intrusion (IDS) - Une solution conçue pour détecter les activités non autorisées des utilisateurs, des attaques et des compromis de réseau.

systèmes de prévention des intrusions (IPS) - Une solution conçue pour détecter les activités non autorisées des utilisateurs, des attaques et des compromis de réseau qui peuvent également prendre des mesures pour empêcher une violation de se produire.

Adresse Mac - l'adresse physique ou matériel brûlé dans chaque carte réseau (par exemple, 964C-E5-48-78-C7).

Network Access Protection (NAP) - Une solution Microsoft qui permet aux administrateurs un moyen plus puissant pour contrôler l'accès aux ressources du réseau. Les contrôles du PAN sont basées sur l'identité de l'ordinateur client et si CONFORME informatiques avec les politiques de gouvernance de réseau configurées.

pare-feu de réseau - Une catégorie de pare-feu logiciel se compose d'applications installées sur les serveurs utilisés pour protéger les segments de réseau d'autres segments du réseau.

Interconnexion de systèmes ouverts (OSI) - Le modèle OSI est un modèle conceptuel, créé par l'Organisation internationale de normalisation (ISO) pour décrire une architecture de réseau qui permet le passage des données entre les systèmes informatiques. Bien que jamais pleinement utilisé comme modèle pour un protocole, le modèle OSI est néanmoins la norme pour discuter comment fonctionne en réseau.

cellule capitonnée - Un système qui attend un IDS pour détecter un attaquant, puis transfère l'attaquant à un hôte spécial où il ou elle ne peut pas faire des dommages à l'environnement de production.

pare-feu personnel - Un type de logiciel pare-feu installé sur un hôte et utilisé pour protéger l'hôte contre les attaques réseau.

Gestion de contenu sécurisé (SCM de) - Protection des logiciels contre les logiciels espions, le phishing, les virus et le spam e-mail.

l'usurpation d'identité - La mauvaise utilisation d'un protocole de réseau de commettre une mystification sur un hôte ou un dispositif de réseau.

stateful inspection - En plus d'examiner les informations d'en-tête des paquets qui traversent le pare-feu, une inspection stateful considère pare-feu d'autres facteurs pour déterminer si le trafic doit être autorisé à travers le pare-feu. stateful inspection détermine également si un paquet fait partie d'une session existante, et que les informations peuvent être utilisées pour décider d'autoriser ou refuser un paquet.

Gestion unifiée des menaces (UTM) - Un produit de sécurité complète qui inclut la protection contre les menaces multiples. Un produit UTM comprend typiquement un pare-feu, logiciel antivirus, filtrage de contenu et un filtre anti-spam en un seul ensemble intégré.

Lesson 4

Comprendre la sécurité des réseaux

évaluation des connaissances

Choix multiple

Encerclez la ou les lettres qui correspondent à la meilleure réponse ou des réponses.

1. Lequel devrait être examiné les éléments et les questions suivantes au moment de décider d'utiliser un pare-feu logiciel ou matériel? (Choisissez tout ce qui correspond.)

une. Système d'exploitation hôte

b. conflits d'application

c. Version du système d'exploitation

ré. l'efficacité du service de pare-feu

e. La stabilité

2. Lequel des éléments suivants sont des couches du modèle OSI? (Choisissez tout ce qui correspond.)

une. Physique

b. Contrôle

c. Application

ré. Réseau

e. Chiffrement

3. A quelle couche du modèle OSI ne routage se produisent?

une. Physique

b. Liaison de données

c. Transport

ré. Session

e. Réseau

4. Lequel des éléments suivants sont des types de pare-feu valides? (Choisissez la meilleure réponse.)

une. Virtuel

b. Réseau

c. le filtrage de paquets

ré. IPsec

e. Application

5. Laquelle des informations suivantes sont généralement examinées par un pare-feu stateful inspection?

une. l'adresse IP de l'hôte d'envoi

b. l'adresse IP de l'hôte de réception

c. l'adresse IP du routeur

ré. type de paquet de données

e. Taille du paquet de données

6. Quel est l'objectif du PAN? (Choisissez la meilleure réponse.)

une. NAP se traduit par des adresses IP privées à des adresses IP Internet routable.

b. NAP permet un pare-feu pour effectuer une inspection approfondie des paquets.

c. PAN fournit un mécanisme permettant d'effectuer une analyse de réseau sur les paquets capturés.

ré. contrôles NAP quels sont les systèmes autorisés à se connecter à un réseau.

7. Une attaque qui repose sur un utilisateur ayant exécuter un script malveillant embarqué dans une page web est quel type d'attaque? (Choisissez la meilleure réponse.)

une. L'homme au milieu

b. Force brute

c. Cross-site scripting

ré. injection SQL

8. Vous venez d'acheter un nouveau point d'accès sans fil pour votre petite entreprise de services informatiques, et vous voulez vous assurer que seuls vos systèmes sont capables de se connecter au réseau sans fil. À cette fin, vous activez le filtrage d'adresses MAC et mettez les adresses MAC de tous vos ordinateurs dans la table autorisée. A quelle couche du modèle OSI ne se produit ce filtrage?

une. Physique

b. Liaison de données

c. Réseau

ré. Transport

e. Session

9. Vous êtes l'agent de sécurité de l'information pour une fabrication de taille moyenne entreprise et votre équipe de vente vient de déployer une nouvelle application de commerce électronique pour permettre la vente directe de vos produits à vos clients. Pour sécuriser cette application, vous déployez un pare-feu d'application. A quelle couche du modèle OSI ne se produit ce filtrage? (Sélectionnez toutes les réponses applicables.)

une. Physique

b. Liaison de données

c. Réseau

ré. Présentation

e. Application

10. Lequel des éléments suivants sont des composants de protection d'accès réseau? (Choisissez tout ce qui correspond.)

une. Adresse MAC conformité

b. le respect de la politique de santé

c. mode d'accès limité

ré. Mode d'adresse IP

e. validation de l'état de santé

11. Lequel des éléments suivants sont des attaques par mot de passe? (Choisissez tout ce qui correspond.)

une. attaques Replay

b. Réseau des attaques

c. Brutes attaques de force

ré. L'homme dans les attaques du milieu

e. attaques par dictionnaire

12. Quel type d'attaque repose sur l'attaquant trompant l'hôte qui envoie en pensant que son système est l'hôte de réception, et l'hôte de réception en pensant que son système est l'hôte d'envoi? (Choisissez la meilleure réponse.)

une. Replay attaque

b. Attaque de force brute

c. L'homme dans l'attaque du milieu

ré. attaque de scriptage intersite

e. attaque par injection SQL

13. Lequel des systèmes suivants ne peuvent pas participer à une mise en œuvre du PAN? (Choisissez tout ce qui correspond.)

une. Windows 7 Édition Familiale

b. Windows 7 Édition Familiale Premium

c. Windows XP Service Pack 2

ré. Windows Vista Ultimate

e. Windows 7 Professionnel

14. Lequel des éléments suivants sont des utilisations communes pour un VPN?

une. Accès à distance

b. l'isolement du serveur

c. Détection d'intrusion

ré. connexions Extranet

e. isolement de domaine

15. Lequel des éléments suivants sont des types de protocoles de routage? (Choisissez tout ce qui correspond.)

une. vecteur lien

b. lien dynamique

c. lien Distance

ré. Vecteur de distance

e. état de liaison

Remplir les trous

1. Vous êtes un administrateur réseau, et vous venez d'être mis en charge de l'enregistrement de votre nom de domaine de l'entreprise et la mise en place du DNS afin que les gens sur Internet peuvent se rendre à votre site Web. Ici, **DNSSEC** peut être utilisé pour faire en sorte que vos entrées DNS ne sont pas empoisonnés par un attaquant.

2. Les deux la plupart des protocoles communs que vous pouvez utiliser pour créer un réseau privé virtuel sont **IPSec** et **SSL / TLS** .

3. Les trois types les plus courants de l'usurpation d'identité de protocole sont **ARP spoofing** , **DNS l'usurpation d'identité** , et **usurpation d'adresse IP** .

4. Le type d'attaque qui repose sur une faiblesse dans un système d'exploitation ou une application est connue en tant que (n) **attaque de vulnérabilité logicielle** .

5. Une attaque qui repose sur l'accès à un segment LAN physique est connu sous le nom un) **L'attaque de réseau** attaque.

6. Une attaque qui enregistre un flux de données, modifie et renvoie ensuite est connu en tant que (n) **attaque replay** attaque.

sept. Les deux types communs de traduction d'adresses réseau sont **statique** et **dynamique** .

8. Si vous configurez un réseau sans fil dans un environnement d'entreprise et vous souhaitez utiliser 802.1x et un serveur RADIUS pour sécuriser les connexions, vous devez utiliser **WPA / WPA2** clés.

9. Les quatre mécanismes utilisés par le PAN pour restreindre l'accès au réseau et appliquer des politiques sont **application IPsec** , **l'application 802.1x** , **l'application VPN** , et **l'application DHCP** .

10. (n) **pot de miel** peut être déployé pour distraire un attaquant de la critique systèmes sur votre réseau.

évaluation des compétences

Scénario 4-1: Utilisation de pare-feu Windows

Vous travaillez pour la Société ABC. Vous devez dire à un utilisateur comment ouvrir la console Pare-feu Windows sur un ordinateur exécutant Windows 7 et créer une règle entrante du pare-feu Windows qui permet Internet Explorer de communiquer sur les ports 80 et 443. Quelles sont les étapes ce suivi utilisateur?

1. Clique le **Début** bouton et ouvrez le **Panneau de configuration.**

2. Cliquez sur **Système et sécurité,** suivi par **Fenêtre pare-feu.**

3. Clique le **Allumez Pare-feu Windows ou désactiver** option.

4. Clique le **Retour** bouton.

5. Clique le **Autoriser un programme ou d'une fonction pare-feu Windows** option.

6. Clique le **Autoriser un autre programme** bouton.

7. Sélectionnez **Internet Explorer** et cliquez sur le **Ajouter** bouton.

8. Cliquez sur **D'ACCORD.**

9. Clique le **Réglages avancés** option.

10. Cliquez sur **Règles de trafic entrant.**

11. Clique le **Nouvelle règle** option.

12. Sélectionnez le **Port** option et cliquez sur le **Prochain** bouton.

13. Spécifiez le port 80 et 443, puis cliquez sur le **Prochain** bouton.

14. Avec le **Autoriser la connexion** option sélectionnée, cliquez sur le **Prochain** bouton.

15. Lorsqu'on lui a demandé quels profils pour permettre à cette règle, garder tous sélectionnés
et cliquez sur le **Prochain** bouton.

16. Pour le nom, spécifiez le **Interface Web,** et cliquez sur le **terminer** bouton.

17. Fermez Pare-feu Windows.

Scénario 4-2: Regarder une table de routage

Vous travaillez pour la Contoso Corporation, où vous avez un ordinateur exécutant Windows 7. Exécutez les commandes nécessaires pour afficher les routes actuelles. Maintenant, ajoutez un itinéraire à la 10.24.57.0 réseau en utilisant la passerelle 192.168.50.1, et afficher les routes pour confirmer qu'il a été ajouté. Enfin, supprimez la nouvelle route.

1. Clique le **Début** bouton et exécutez la commande suivante:

   cmd

2. À l'invite de commande, entrez la commande suivante:

   imprimer itinéraire

3. Pour ajouter une route au réseau 10.24.57.0 qui est envoyé à la 192.168.50.1
   voie, exécutez la commande suivante:

   route add 10.25.57.0 masque 255.255.255.0 0.0.0.0

4. Utilisez la commande d'impression de la route pour voir que le nouvel itinéraire est ajouté.

5. Pour supprimer cette route, exécutez la commande suivante:

   itinéraire supprimer 10.25.57.0

6. Voir la table de routage une fois de plus pour vérifier que l'itinéraire a été supprimé.

évaluation des compétences

Scénario 4-3: renifler Packets

Vous avez décidé que vous souhaitez développer une meilleure compréhension des paquets et la façon dont ils fonctionnent. Par conséquent, vous choisissez d'utiliser un renifleur de protocole fourni par Microsoft appelé Network Monitor pour analyser ces paquets. Quand vous regardez les paquets, vous souhaitez identifier les quatre parties principales qui composent la plupart d'entre eux. Quelles mesures prendriez-vous pour le faire?

1. Aller à http://www.microsoft.com.

2. Rechercher et télécharger Microsoft Network Monitor.

3. Double-cliquez sur le fichier MSI que vous venez de télécharger et installer
   Moniteur réseau.

4. Clique le **Début** bouton, ouvert **Outils administratifs,** et commencer à **Réseau Moniteur.**

5. A partir de la page de démarrage, cliquez sur le **Créer une nouvelle capture** languette.

6. Dans la fenêtre réseau, sélectionnez le ou les réseaux de que vous voulez capturer des images.

sept. Dans le menu Capture, cliquez sur le **Début** bouton.

8. Ouvrez un navigateur et allez à http://www.microsoft.com.

9. Cliquez sur **Arrêter la capture.**

dix. Ouvrez les images capturées et regardez tous les paquets capturés. Plus les paquets ont jusqu'à quatre parties. Les pièces suivantes sont affichées dans le Moniteur réseau:

- Ethernet
- tête IP
- en-tête TCP ou UDP
- Protocole de charge utile

Scénario 4-4: Recherche dans les ports

Vous parlez avec le CIO de votre entreprise. L'un des programmes dont elle a besoin l'accès à est sur un serveur qui se trouve sur la zone démilitarisée en utilisant les protocoles suivants:

Secure Shell (SSH)

Protocole de transfert Nouvelles du Réseau

Simple Network Management Protocol

NetBIOS session service

Network Time Protocol

Le CIO veut savoir ce qu'est un port et les ports sont impliqués dans ces protocoles. Que devriez-vous lui dire?

Les ports sont utilisés pour décrire un service ou d'un programme réseau qui est transporté par paquets de réseau. De cette façon, lorsqu'un paquet est reçu, le paquet peut être acheminé vers le composant logiciel correct. Les programmes répertoriés dans cet exercice utilisent les ports suivants:

Secure Shell (SSH)	TCP / UDP 22
Protocole de transfert Nouvelles du Réseau	TCP 119
Simple Network Management Protocol	TCP / UDP 161
NetBIOS session service	TCP / UDP 139
Network Time Protocol	TCP / UDP 123

leçon 5

La protection du serveur et le client

Objectifs d'apprentissage

Les élèves apprendront à:

- Protéger un ordinateur des logiciels malveillants
- Protéger l'ordinateur client
- Email protect
- Protéger un serveur
- Sécuriser Internet Explorer

ODN compétences

• Comprendre les logiciels malveillants.	2.6
• Comprendre la protection des clients.	4.1
• Comprendre la protection email.	4.2
• Comprendre la protection du serveur.	4.3
• Comprendre la sécurité Internet.	1.3

Résumé de la leçon - Notes de cours

Maintenant que vous avez couvert la protection du réseau, l'accent est mis sur la protection du serveur et le client. Ce sont les derniers blocs de construction dans l'élaboration d'un plan de sécurité informatique. La leçon commence par la protection des ordinateurs, y compris les serveurs de logiciels malveillants. Bien sûr, ici, vous devez mettre l'accent sur un logiciel antivirus à jour avec les mises à jour de sécurité mises à jour pour les systèmes d'exploitation (y compris Windows). Vous serez également couvrir les différents types de logiciels malveillants et comment ils peuvent entrer dans un système informatique ou d'un réseau. Pour protéger un ordinateur contre les logiciels malveillants et de contrôler l'accès, la partie suivante de la couverture de cours User Account Control (UAC) et Pare-feu Windows.

La partie suivante de la leçon discute e-mail et comment le protéger. Rappelez aux élèves qu'ils peuvent être une source de logiciels malveillants et ils peuvent jouer un rôle dans l'ingénierie sociale. Étant donné que tout utilisateur peut introduire des logiciels malveillants dans l'environnement réseau, la prochaine partie de la discussion porte sur Internet Explorer (car il est utilisé pour accéder à Internet).

La dernière partie de la leçon de protection discute le serveur par le durcissement du serveur.

Mots clés

adware- Tout logiciel qui joue automatiquement, affiche, publicités ou téléchargements à un ordinateur une fois le logiciel installé ou l'application est utilisée.

porte de derrière - Un programme qui donne à quelqu'un à distance, le contrôle non autorisé d'un système ou initie une tâche non autorisée.

filtre bayésien - Un des algorithmes spéciaux, tels que les filtres bayésiens, afin de déterminer si e-mail est considéré comme du spam.

zones de contenu - Zones utilisées pour définir et gérer la sécurité de l'aide lors de la visite des sites.

biscuit - Un morceau de texte stocké par le navigateur Web d'un utilisateur. Ce fichier peut être utilisé pour un large éventail d'objectifs, y compris l'identification de l'utilisateur, l'authentification et le stockage préférences du site et Contenu du panier.

logiciels malveillants (malware) - Le logiciel qui est conçu pour infiltrer ou affecter un système informatique sans le consentement éclairé du propriétaire. Le terme -malware‖ est généralement associée à des virus, vers, chevaux de Troie, les logiciels espions, rootkits et malhonnête adware.

Microsoft Baseline Security Analyzer (MBSA de) - Un outil logiciel fourni par Microsoft pour déterminer l'état de la sécurité d'un système en évaluant mises à jour manquantes de sécurité et les paramètres de sécurité lesssecure dans Microsoft composants Windows tels que Internet Explorer, le serveur Web IIS, et des produits tels que Microsoft SQL Server et Microsoft Office paramètres macro.

fichiers hors connexion - Des copies de fichiers réseau qui sont stockés sur votre ordinateur afin que vous puissiez y accéder lorsque vous n'êtes pas connecté au réseau ou lorsque le dossier réseau qui contient les fichiers n'est pas connecté.

pharming - Une attaque visant à rediriger le trafic d'un site à un faux site Web.

Hameçonnage - une technique basée sur l'ingénierie sociale, où les utilisateurs sont invités (généralement par courrier électronique ou des sites Web) pour fournir des renseignements personnels.

fenêtre pop-up - composant A utilisé sur les pages Web qui peuvent être utilisés dans le cadre d'un contrôle de sites Web utiles, mais peut aussi être utilisé pour des publicités ennuyeuses, et quelques-uns peuvent tenter de spyware de charge ou d'autres programmes malveillants.

rootkit - Logiciel A ou dispositif matériel conçu pour prendre le contrôle de niveau administrateur sur un système informatique sans être détecté.

Cadre stratégique de l'expéditeur (SPF) - Un système de validation de messagerie conçu pour éviter le spam de messagerie utilisant l'adresse source usurpation d'identité. SPF permet aux administrateurs de spécifier dans les enregistrements DNS SPF dans le DNS public qui les hôtes sont autorisés à envoyer des courriels à partir d'un domaine donné.

Spam - courrier indésirable qui est généralement envoyé non sollicité.

Spyware - Un type de logiciel malveillant est installé sur un ordinateur pour recueillir des informations personnelles ou les détails d'un utilisateur au sujet de ses habitudes de navigation, souvent à l'insu de l'utilisateur.

cheval de Troie - Un programme exécutable qui apparaît comme un programme souhaitable ou utile. Parce qu'il semble souhaitable ou utile, les utilisateurs sont trompés en chargement et l'exécution du programme sur leurs systèmes.

Contrôle de compte d'utilisateur (UAC de) - Une caractéristique qui a commencé avec Windows Vista et est fourni avec Windows 7. UAC aide à prévenir les modifications non autorisées à votre ordinateur- et ce faisant, il aide à protéger votre système contre les logiciels malveillants.

virus - Un programme qui peut se copier et d'infecter un ordinateur sans le consentement ou la connaissance de l'utilisateur.

canular - Un message avertissant le destinataire d'une menace de virus informatique inexistant, généralement envoyé comme un e-mail de chaîne qui indique au destinataire de le transmettre à tout le monde qu'il connaît. C'est une forme d'ingénierie sociale qui joue sur l'ignorance des gens et de la peur.

Windows Defender - Un logiciel de Microsoft qui vise à prévenir, supprimer et les logiciels espions de quarantaine dans Microsoft Windows.

fenêtre pare-feu - Un composant logiciel fourni avec Windows qui aide peut empêcher les pirates ou les logiciels malveillants (tels que les vers) d'avoir accès à votre ordinateur via un réseau ou sur Internet. Un pare-feu peut également aider à arrêter votre ordinateur d'envoyer des logiciels malveillants à d'autres ordinateurs.

Windows Server Update Server (WSUS) - Un système logiciel qui peut garder vos systèmes mis à jour avec les dernières mises à jour Windows et Office.

mises à jour Windows - Correctifs, service packs et les pilotes de périphériques mis à jour qui doivent être appliqués à un système Windows. En ajoutant des correctifs et des correctifs, vous garderez de Windows stable et sûr.

Ver de terre - Un programme d'auto-réplication qui copie lui-même à d'autres ordinateurs sur un réseau sans intervention de l'utilisateur.

Lesson 5

La protection du serveur et le client

évaluation des connaissances

Choix multiple

Entourez la lettre qui correspond à la meilleure réponse.

1. Quel type de logiciels malveillants sur lui-même des copies d'autres ordinateurs sans le consentement du propriétaire et supprimera souvent ou les fichiers corrompus?

une. Virus

b. Ver de terre

c. cheval de Troie

ré. Spyware

2. Quel type de programmes malveillants recueille des renseignements personnels ou l'historique de navigation, souvent à l'insu de l'utilisateur?

une. Virus

b. Ver de terre

c. cheval de Troie

ré. Spyware

3. Votre ordinateur semble être lent, et vous remarquerez que vous avez un autre page Web par défaut que d'habitude. Ce qui est très probablement la cause des problèmes?

une. Votre fournisseur d'accès Internet a ralenti votre connexion réseau.

b. Votre ordinateur a été infecté par des logiciels malveillants.

c. Vous ne l'avez pas mis à jour votre ordinateur.

ré. Vous avez accidentellement cliqué sur le bouton turbo.

4. En plus de l'installation d'un logiciel antivirus, vous devez toujours _____ pour protéger votre ordinateur contre les logiciels malveillants.

une. garder votre machine à jour avec les derniers correctifs de sécurité

b. redémarrez votre ordinateur sur une base régulière

c. changer votre mot de passe sur une base régulière

ré. usurper votre adresse IP

5. Un fond ensemble cumulatif testé de correctifs et d'autres correctifs est connu en tant que (n):

une. mise à jour recommandée.

b. Pack correctif.

c. service pack.

ré. mise à jour critique.

6. Quelle est la technologie utilisée par Windows pour empêcher toute modification non autorisée
votre système?

une. UAC

b. Mode protégé

c. Windows Defender

ré. ProtectGuard

sept. Lorsque vous utilisez contrôle de compte, ce qui suit exige administrative
les autorisations ou les droits?

une. Installation des mises à jour de Windows Update

b. Modification de la date et l'heure

c. Remise à zéro de la carte réseau

ré. Installation des pilotes de mise à jour Windows ou attaché avec le système d'exploitation

8. Quel mécanisme fonctionne lorsque vous essayez de changer l'affichage d'un ordinateur
paramètres et vous obtenez un pop-up demandant si vous souhaitez continuer?

une. fenêtre pare-feu

b. Mode protégé

c. Windows Update

ré. UAC

9. Quel logiciel pare-feu basé sur l'hôte est livré avec les versions actuelles de
Les fenêtres?

une. fenêtre pare-feu

b. Le mode protégé de Windows

c. UAC

ré. windows GuardIt

dix. Quel programme voulez-vous utiliser pour configurer IPsec de sur un ordinateur exécutant
Windows Server 2008?

une. Pare-feu Windows avec IPsec Plugin

b. Moniteur IPsec

c. Windows avec sécurité avancée

ré. IPsec console Configuration

11. Si vous avez des informations sensibles ou confidentielles stockées dans vos fichiers hors connexion,
il est recommandé que vous:

une. vider votre cache.

b. crypter les fichiers hors connexion.

c. Effacez vos cookies.

ré. exécuter ipconfig / renewip.

12. Vous déterminez que les courriels légitimes sont bloqués par votre Spam-
Dispositif de blocage. Que devrais tu faire?

une. Débusquer les éléments mis en quarantaine

b. Redémarrez le dispositif de blocage du spam

c. Ajoutez l'adresse ou le domaine de ces e-mails à la liste blanche

ré. Ajoutez l'adresse ou le domaine de ces e-mails à la liste noire

13. SMTP utilise le port TCP:

une. 43.

b. 25.

c. 80.

ré. 443.

14. Combien de zones de contenu sont là dans Internet Explorer?

une. 1

b. 2

c. 4

ré. 8

15. Dites que vous recevez un e-mail indiquant que votre compte a expiré et vient vous demandant de vous connecter à un site Web légitime, cherche à résoudre le problème. Ceci est probablement une instance de:

une. Hameçonnage.

b. pharming.

c. phaking.

ré. l'usurpation d'adresse IP.

Remplir les trous

Complétez les phrases suivantes en écrivant le mot correct ou des mots dans les espaces prévus.

1. **Des logiciels malveillants (malware)** est un logiciel qui est conçu pour infiltrer ou d'infecter un ordinateur, le plus souvent avec mauvaise intention.

2. A (n) **Ver de terre** est un programme d'auto-réplication qui se copie à d'autres ordinateurs tout en consommant les ressources du réseau.

3. programme antispyware de Microsoft est appelé **Windows Defender** .

4. Pour un logiciel antivirus soit efficace, il faut garder **à jour** .

5. Un exemple d'une (n) **canular** est un message indiquant à supprimer la fichier win.com parce qu'il est un virus.

6. Si vous souhaitez contrôler les mises à jour sont poussés à des clients au sein de votre organisation, vous pouvez utiliser **Windows Update Server (WUS)** ou **System Center Configuration Manager** .

sept. **bureau sécurisé** est quand on vous demande si vous voulez continuer avec un action et votre bureau est estompés et d'autres programmes sont temporaires Halted jusqu'à ce que vous approuvez le changement.

8. **Les fichiers hors connexion** sont des copies de fichiers réseau qui sont stockés sur votre ordinateur afin que vous puissiez y accéder lorsque vous n'êtes pas connecté au réseau.

9. **Spam** est un autre nom pour le courrier électronique indésirable.

dix. **Cadre stratégique de l'expéditeur (SPF)** est un système de validation de courrier électronique qui est conçu pour vérifier qu'un courriel provient du serveur de messagerie approprié.

évaluation des compétences

Scénario 5-1: Vérification de la sécurité physique

Vous venez de embauchage comme administrateur informatique pour la société ABC. En face de votre bureau, il y a une table avec sept serveurs physiques. Vous allez à votre patron et demandez pourquoi les serveurs sont à l'air libre et non verrouillé. Il dit qu'il se trouvent sur la table afin qu'ils puissent être facilement surveillés et surveillés. Comment devez-vous répondre à votre patron?

Si les gens ont un accès physique à un serveur, ils peuvent tirer sur ou câbles coupés ou arrêter un serveur, ce qui provoque un déni de service. De plus, s'ils enlèvent les disques durs d'un serveur, ils peuvent se connecter ce disque dur à un autre ordinateur dont ils sont un administrateur. Cela leur permettrait d'accéder à tous les fichiers sur le disque dur, y compris des informations confidentielles.

Scénario 5-2: Programmation backdoors

Vous avez été embauché en tant que consultant en sécurité pour la Contoso Corporation. Un jour, vous travaillez avec le CIO sur une nouvelle politique de sécurité globale pour l'entreprise. Bien que le CIO n'est pas un programmeur elle-même, elle veut comprendre comment elle peut garder les programmeurs de créer une porte dérobée sur les programmes qu'ils créent pour l'entreprise. Que lui dites-vous?

Lorsque vous avez des programmeurs qui créent des applications pour votre organisation, vous devez établir un processus d'examen et de vérification qui vérifiera leur travail. Cela comprend l'examen tout le code source.

évaluation des compétences

Scénario 5-3: Numérisation avec Microsoft Baseline Security Analyzer

Téléchargez et installez le nouveau Microsoft Baseline Security Analyzer sur un serveur Windows, puis analyser l'ordinateur pour les mises à jour de sécurité manquants et les paramètres de sécurité moins optimales.

1. Téléchargez et installez le nouveau Microsoft Baseline Security Analyzer. À l'heure actuelle, il est situé à http://www.microsoft.com/downloads/details.aspx?FamilyID=b1e76bbe-71df-41e88b52-c871d012ba78&displaylang=en.
2. Double-cliquez sur le fichier exécutable que vous avez téléchargé.
3. **Si vous êtes invité à installer le fichier, cliquez sur le Courir** bouton.
4. Lorsque l'écran de bienvenue apparaît, cliquez sur **Prochain.**
5. Cliquez sur **J'accepte le contrat de licence,** puis clique **Prochain.**
6. Lorsqu'on lui a demandé le dossier de destination, cliquez sur **Prochain.**
7. Cliquez sur **Installer.**
8. Lorsque le programme est correctement installé, cliquez sur **D'ACCORD.**
9. Cliquez sur **Début,** sélectionner **Tous les programmes,** et sélectionnez **Microsoft Baseline Security Analyseur.**
10. Cliquez sur **Numérisation d'un ordinateur.**
11. Cliquez sur le **Démarrer balayage** bouton.
12. Cliquez sur **Voir les résultats.**

Scénario 5-4: Regarder Windows Updates

Aller à http://www.microsoft.com/technet/security/bulletin/advance.mspx. Lire la Notification la plus récente de l'avance ou le plus récent bulletin de sécurité et d'examiner le résumé. Déterminer le nombre de bulletins de sécurité, il y a pour le mois le plus récent. Ensuite, exécutez Windows Update pour mettre votre système à jour avec les derniers correctifs.

Les réponses varieront. Mais pour exécuter Windows Update, procédez comme suit:

1. Clique le **Début** bouton, sélectionnez **Tous les programmes,** et sélectionnez **Windows Update**.
2. Cliquez sur le **Vérifier les mises à jour** bouton.
3. Cliquez sur le **mises à jour sont disponibles en option** option.
4. Sélectionnez le **Mises à jour facultatives** et cliquez sur le **D'accord** option.
5. Cliquez sur le **Installer les mises à jour** bouton.
6. Si nécessaire, cliquez sur **Redémarrer maintenant.**