Microsoft Technology Associate

TECNOLOGIA MICROSOFT ASSOCIATE

Guia de Estudo do Aluno

EXAME 98-367

Conceitos básicos de segurança

Microsoft

Preparação para a certificação do MTA

TECNOLOGIA MICROSOFT ASSOCIATE (MTA)

GUIA DE ESTUDO DO ALUNO PARA PROFISSIONAIS DE TI

98-367 Conceitos básicos de segurança

Autores

Michael Teske (Administração e Segurança do Windows Server). Michael ensina no Programa de Especialista de Rede há 10 anos na Northeast Wisconsin Technical College e está envolvido como um engenheiro há 15 anos. Ele tem uma paixão pelo ensino e tecnologia e adora ajudar as pessoas a encontrar a felicidade em uma carreira. Mike acredita que a tecnologia de aprendizagem deve ser divertida, mas reconhece que o campo de rede está em constante mudança e pode desafiar até mesmo os alunos mais brilhantes. Mike também trabalha como um consultor independente para várias pequenas empresas no nordeste do Wisconsin e aprecia trazer a experiência do mundo real para a sala de aula diariamente. Michael se tornou conhecido como "o cara da Microsoft" no campus. O objetivo de Michael é continuar a ensinar tecnologia de rede com o mesmo entusiasmo e paixão por muitos anos para vir e ajudar seus alunos encontrar a mesma alegria e paixão que ele encontrou em um setor e uma carreira surpreendentes. Mike é o autor do Kit de Revisão para o Exame do Windows Server no Exame do MTA Série de Kits de Revisão.

Patricia Phillips (Autora principal e Gerente de projeto). Patricia ensinou ciência da computação por 20 anos em Janesville, Wisconsin. Ela foi membro do Conselho Consultivo Nacional para o Corpo Docente de Ensino Fundamental e Médio da Microsoft e editou o site MainFunction da Microsoft para professores de tecnologia por dois anos. Nos últimos cinco anos ela trabalhou com a Microsoft em diversas funções relacionadas ao desenvolvimento de currículo para o Ensino Fundamental e Médio e programas piloto incluindo web design no Expression Studio e desenvolvimento de jogos com XNA. Em seu papel como autora e editora, Patricia escreveu diversos artigos e um manual do aluno sobre tópicos como ciência da computação, web design, e lógica computacional. Atualmente ela é editora do boletim informativo da Associação de Professores de Ciência da Computação , chamado "the Voice" (a Voz).

Conteúdo

Introdução

MTA valida conceitos de tecnologia de blocos de construção e ajuda os alunos a explorar, descobrir e seguir carreiras bem-sucedidas em Tecnologia da Informação (TI) de uma maneira estimulante e recompensadora! Como um primeiro passo na série Microsoft Technology Certification, esta nova certificação inicial dá aos alunos confiança, credibilidade e diferenciação.

Explore opções de carreira em TI sem comprometer muito tempo e recursos Os exames MTA validam o conhecimento principal em tecnologia que hoje está em demanda por empresas no mundo todo. Se você quiser explorar a possibilidade de se tornar um administrador de rede, engenheiro de software, desenvolvedor para web, ou analista de banco de dados, o MTA inicia você no caminho certo.

Prepare-se para competir Um pequeno investimento em TI pode ir longe no mercado de trabalho hoje em dia. Certificar-se como MTA ajuda você a construir uma fundação sólida para prepará-lo para os estudos intermediários de tecnologia e para as certificações MCTS (Microsoft Certified Technology Specialist). Ele pode também ajudá-lo a competir em admissões para faculdades e impulsionar seu planejamento de carreira em TI!

Capacite-se Como primeiro passo para se tornar um MCTS, o MTA mostra seu compromisso com tecnologia enquanto conecta você com uma comunidade de mais de cinco milhões de Profissionais Certificados Microsoft . Aprenda com eles e mostre-lhes o que você sabe ao certificar-se como MTA!

Este Guia do aluno de estudo para o MTA serve como uma ferramenta de estudo para ajudar alunos a preparar-se para seu exame de certificação do MTA. Os desafios para os estudantes se baseiam em situações da vida real para cada um dos tópicos importantes abordados no exame. Apesar da conclusão bem-sucedida dos exercícios do guia de estudos não garantir que você passará seu exame MTA, esta é uma excelente maneira de avaliar sua aptidão para fazê-lo e criar confiança de que você sabe o que está fazendo no dia do exame.

Desejo a você tudo de bom em sua preparação para uma carreira bem-sucedida em tecnologia!

Victoria Pohto

Victoria Pohto

Gerente de marketing de produto do MTA

Planejamento de carre

A maioria das soluções ou infraestrutura de TI construídas com base em tecnologias Microsoft requer proficiência em um ou todos os seguintes produtos, muitas vezes chamados de “The Microsoft Stack”.

- Microsoft Windows® Server® como data center ou plataforma de desenvolvimento
- Microsoft SQL Server® como plataforma de dados e BI (Business Intelligence)
- Microsoft Visual Studio® como o conjunto de ferramentas de gerenciamento do ciclo de vida de aplicativos

O MTA é o ponto inicial das certificações de tecnologia da Microsoft, oferecendo a tecnólogos aspirantes o conhecimento básico essencial para ter êxito em estudos continuados e uma carreira bem-sucedida em tecnologia.

Preparar-se e certificar-se como MTA ajuda você a explorar uma variedade de percursos profissionais em tecnologia, sem investir muito tempo e dinheiro em uma carreira especializada. Quando você encontrar um caminho que é certo para você, os produtos de aprendizagem e certificação Microsoft podem ajudá-lo a preparar-se e guiá-lo no planejamento a longo prazo de sua carreira.

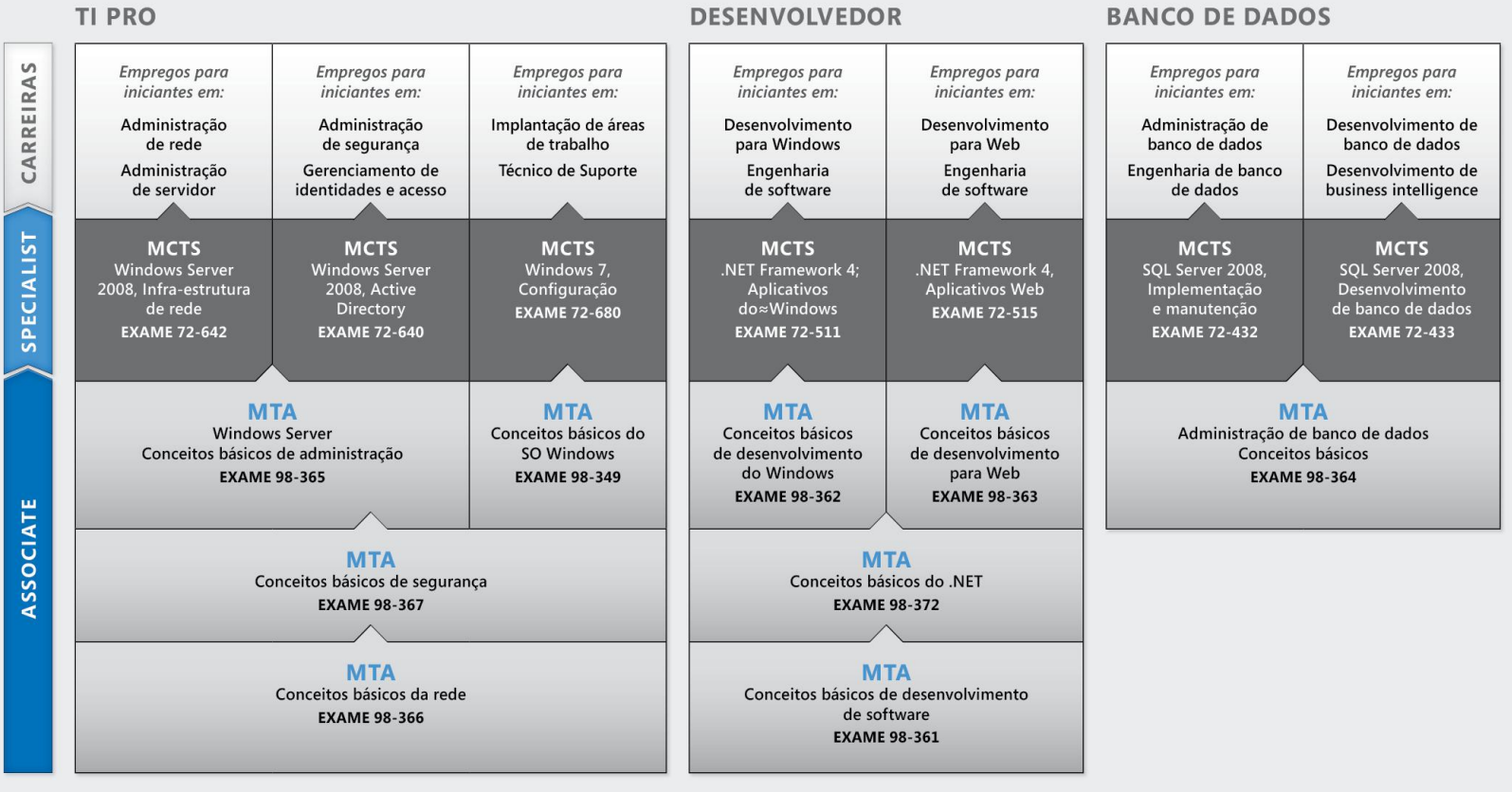
Se você já sabe que quer começar a construir uma carreira em tecnologia, a preparação e certificação como MTA é o ponto inicial recomendado. Certificar-se pelo mostra que você tem uma firma que tem um conhecimento dos conceitos fundamentais de TI essenciais para o sucesso com certificações intermediárias e certificações como a do MCTS (Microsoft Certified Technology Specialist). Além do mais, as certificações Microsoft demonstram o compromisso do indivíduo em investir em si mesmo e a confiança em levar seu conhecimento e habilidades ao próximo nível com uma credencial reconhecida pelo setor.

O MTA não é uma “certificação de carreira”, ou seja, que os empregadores reconheçam você como "pronto para ser contratado", mas é o primeiro passo na direção deste objetivo de carreira e pode ajudar você a se diferenciar frente a um estágio ou comitê de admissão de faculdade. Ao preparar-se para seu primeiro emprego visando a tecnologia, certifique-se de que você está equipado com uma credencial MCTS – a certificação de nível intermediário que valida as habilidades com produtos e tecnologia Microsoft.

A trilha de Certificação do MTA na próxima página mostra a você os exames MTA recomendados antes de obter alguma das certificações de tecnologia intermediárias da Microsoft, os MCTS.

Caminhos de certificação do Microsoft Technology Associate

O MTA é a primeira etapa na série Microsoft® Technology Certification. (O MTA é recomendável, mas não é um pré-requisito para os exames de MCTS.) Uma certificação é obtida a cada exame aprovado. Guias de Estudo do Aluno gratuitos estão disponíveis para download em **www.certiport.com/mta.**



Para obter roteiros completos do Microsoft Certification, visite
http://www.microsoft.com/learning/certification

Explorar funções do cargo

Escolher uma carreira é uma grande decisão e nem sempre é fácil, mas você não está sozinho! A Microsoft criou um site de carreiras para ajudar os alunos a compreender as opções e possibilidades ao seguir uma carreira em TI. O site também conecta você a recursos de aprendizado, comunidades de estudantes de tecnologia e muito mais para ajudá-lo a se preparar para uma carreira em tecnologia.

Para visualizar graficamente sua carreira em tecnologias Microsoft, acesse *www.microsoft.com/learning/career/en/us/career-org-charts.aspx*.

Administrador de banco de dados

Como um administrador de banco de dados, você será responsável por bancos de dados importantes que atingem diversas plataformas e ambientes. Você trabalha muito bem em equipe e se dá bem num ambiente de ritmo acelerado. Você constrói bancos de dados complexos, altamente escaláveis que satisfazem as necessidades de negócios e requisitos de segurança. Você é um especialista em otimizar, manter e resolver problemas de bancos de dados, mas também em projetar soluções de arquivamento, distribuição de dados e alta disponibilidade.

Administrador de servidor

Como administrador de servidor, você é responsável por implementar e gerenciar algumas das mais importantes tecnologias de sua organização – os servidores. Você usa ferramentas de monitoramento extensivo e de criação de perfis para gerenciar a rede e ajustar os sistemas a fim de otimizar seus níveis de desempenho. Você é um especialista em Active Directory®, e tem um conhecimento extenso sobre protocolos de rede, segurança de arquivos e diretórios.

Técnico de suporte do computador

Considere começar sua carreira em TI tornando-se um técnico de suporte ao cliente. Você não precisa de nenhuma experiência de trabalho formal, mas uma empresa pode exigir que você saiba como instalar, administrar e resolver problemas de sistemas operacionais em um ambiente de rede doméstico com desktops, laptops e impressoras. Como um técnico de suporte do cliente, você também lidará com suporte de problemas de redes, vírus, softwares mal-intencionados e hardware. Você normalmente encontrará este cargo em pequenas e médias organizações.

Explorar funções do cargo

Desenvolvedor para web

Como um desenvolvedor para web, você é especialista no uso de ferramentas e linguagens de programação dinâmica que dão vida à web. Você pode trabalhar independentemente ou fazer parte de uma equipe que construa e integre websites interativos, aplicativos e serviços, tanto para sites internos como públicos. Seu papel é fazer tudo funcionar, isto é, desenvolver aplicativos para web e testá-los em vários navegadores, aprimorando-os e modificando-os conforme necessário para garantir ao usuário a melhor experiência possível. Como um desenvolvedor para web, você pode também fazer a arquitetura de websites, projetar aplicativos dirigidos por dados e encontrar soluções cliente-servidor eficientes. Você precisa ter um conhecimento extenso sobre o ciclo de vida de desenvolvimento de software e ser capaz de comunicar o status, problemas e resoluções de projetos.

Desenvolvedor para Windows

Um desenvolvedor para cliente Windows, o mínimo que se espera é saber otimizar o código Windows e rastrear bugs. Mas também é necessário sabe usar o Microsoft Visual Studio® e o Microsoft .NET framework para projetar, desenvolver, testar e instalar aplicativos baseados em Windows que rodam tanto em servidores corporativos como em desktops. Seus talentos principais incluem a compreensão de diversos modelos de aplicativos do Windows e aplicativos para n-camadas e a compreensão de como trabalhar com programação orientada a objeto, algoritmos, dados estruturas e multithreading. Desenvolvedores Windows têm um conhecimento extenso sobre princípios de engenharia de software, ciclos de vida de software e princípios de segurança.

Recursos online adicionais para novos desenvolvedores:

http://msdn.microsoft.com/beginner

http://msdn.microsoft.com/rampup

Imagine Cup

A Imagine Cup é a principal competição mundial de tecnologia para alunos na qual os participantes do mundo todo podem aprender novas habilidades, fazer amigos e mudar o mundo. As competições incluem Projeto de software, Desenvolvimento Embarcado, Design de jogos, Mídia Digital e Windows Phone 7. As mentes jovens mais brilhantes aproveitam a força da tecnologia para dar conta dos problemas mais árduos do mundo.

www.imaginecup.com

Valor da certificação

A tecnologia desempenha uma função em praticamente tudo que fazemos. Nos vinte e tantos anos em que a Microsoft vem certificando pessoas em seus produtos e tecnologias, milhões de pessoas ganharam conhecimento, perícia e credenciais para aprimorar suas carreiras, otimizar soluções de negócios e criar inovação dentro de praticamente todo setor social e de negócios imaginável. Os gerentes de contratação de TI (Tecnologia da Informação) de hoje estão cada vez mais usando credenciais profissionais, tais como a certificação Microsoft, para identificar candidatos de TI adequadamente habilitados. A certificação se torna uma maneira de diferenciar facilmente candidatos qualificados em meio a um mar de currículos.

A perspectiva de emprego para profissionais de TI, como mencionada num estudo preparado pelo BLS (Gabinete de Estatísticas do Trabalho) da Secretaria do Trabalho dos EUA, é positiva! O BLS indica um aumento que será "mais rápido do que a média para todas as ocupações até 2014" para Especialistas em Suporte de Computador, Engenheiros de Sistemas, Administradores de Banco de Dados e Engenheiros de Software.

Uma mensagem significativa resultante desse estudo é que as habilidades de ICT (Tecnologia de informação e comunicações) são o bilhete de entrada para o mercado de trabalho, independentemente do país, setor ou função do cargo. A tecnologia da informação é claramente uma área na qual vale a pena investir tempo, recursos e educação — e a certificação de tecnologia é uma parte essencial do processo de educação, validando a perícia no produto e tecnologia como resultado de suas experiências de aprendizagem.

As certificações em TI da Microsoft oferecem validação objetiva para profissionais, desenvolvedores e operadores de informações em TI quanto à sua habilidade de executar com sucesso funções essenciais de TI. As certificações Microsoft representam um espectro rico e variado de conhecimento, funções de cargos e responsabilidades. Além disso, a obtenção de uma certificação específica oferece validação objetiva da habilidade do candidato em executar com sucesso funções críticas de TI. Adotado por profissionais da indústria no mundo todo, a certificação Microsoft continua como uma das maneiras mais eficazes para ajudar a atingir objetivos de carreira em longo prazo.

MTA 98-367

CONCEITOS BÁSICOS DE SEGURANÇA

1

Noções básicas das camadas de segurança

NESTE CAPÍTULO

Compreender os princípios básicos de segurança

SITUAÇÃO: A Blue Yonder Airlines tem se expandido nos últimos 18 meses e recentemente passou por uma auditoria de segurança para garantir que o sistema técnico seja seguro. Várias áreas que requerem melhorias foram identificadas. O CIO pediu a Toni Poe, consultor de segurança da Blue Yonder Airlines, para fornecer o treinamento de segurança essencial para a equipe da linha de frente. O objetivo é minimizar o risco de ameaças potenciais à segurança, educando os funcionários na área de engenharia social, bem como alguns princípios básicos de segurança.

Toni avaliou os direitos de segurança de cada funcionário relacionados ao acesso ao computador e o acesso ao perímetro. Toni observa que alguns funcionários têm privilégios elevados para acessar o site da intranet da Blue Yonder Airlines. Ele também sabe que é importante salientar o triângulo Confidencialidade, Integridade e Disponibilidade no seu treinamento.

1. **Toni planeja implementar o princípio do privilégio mínimo. Como isso afetará os funcionários?**
   - **a.** os funcionários manterão o seu acesso atual a todos os recursos
   - **b.** será concedido aos funcionários o menor conjunto de privilégios para os recursos
   - **c.** os funcionários terão que fazer logon como administrador para ter acesso aos seus recursos
2. **Qual seria um exemplo de fornecimento de disponibilidade no que se refere ao treinamento de segurança?**
   - **a.** certificar-se de que todas as estações de trabalho estejam ligadas
   - **b.** certificar-se de que todos os funcionários tenham participação total no trabalho
   - **c.** proteger contra um ataque de Negação de Serviço Distribuído
3. **Qual seria um exemplo de engenharia social?**
   - **a.** **ligar** para um funcionário fingindo ser outra pessoa para obter informações que podem fornecer acesso a informações confidenciais
   - **b.** desenvolver o reconhecimento social das ameaças de segurança dentro de uma organização
   - **c.** criar um site de redes sociais

dica

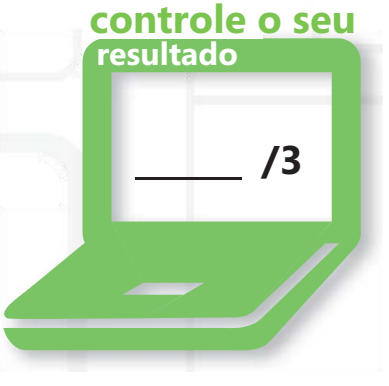
Engenharia social não está relacionado a redes sociais. O principal objetivo de um hacker é obter o máximo de informações explorando o lado humano da segurança.

Respostas

1. Implementar o princípio do privilégio mínimo significa que:
   b. será concedido aos funcionários o menor conjunto de privilégios para os recursos
2. Fornecer disponibilidade no que se refere ao treinamento de segurança significa:
   c. proteger contra um ataque de Negação de Serviço Distribuído
3. Um exemplo de engenharia social poderia incluir:
   a. ligar para um funcionário fingindo ser outra pessoa para obter informações que podem fornecer acesso a informações confidenciais

Detalhes essenciais

- O triângulo **CIA (Confidencialidade, Integridade e Disponibilidade)** é o conceito de garantir a prevenção da divulgação não autorizada de informações, da modificação errônea de informações, e a prevenção de retenção não autorizada de informações e recursos.
- O **princípio do privilégio mínimo** requer que cada sujeito em um sistema receba o mais restrito conjunto de privilégios (ou menor acesso) necessário para o desempenho de tarefas autorizadas.
- **Engenharia social** é qualquer tipo de comportamento que podem ajudar inadvertidamente ou deliberadamente um invasor a obter acesso a senha de usuário ou outras informações confidenciais.



AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/library/cc875841.aspx**

Compreender a segurança física

SITUAÇÃO: Erin Hagens acaba de ser promovida a oficial de segurança do Woodgrove Bank. Esta posição implica uma responsabilidade enorme para a segurança de informações e dinheiro do cliente, sem mencionar a reputação do banco. Esta função exige que ela esteja em conformidade com uma longa lista de requisitos para proteger o Woodgrove Bank. A agência reguladora do setor bancário informou a Erin que o banco passará por uma auditoria de segurança para garantir que este esteja em conformidade com os regulamentos e as normas do setor. Erin compreende a solicitação e deve fazer seu processo de auditoria para fornecer todas as informações que os reguladores precisam enquanto procuram potenciais falhas de segurança. Sua maior preocupação é a segurança física dos sistemas do banco.

1. **O que Erin pode fazer para garantir a segurança física dos computadores desktop do banco?**
   - **a.** desabilitar o uso de disquetes ou unidades USB usando políticas de grupo
   - **b.** ter um guarda em posição em cada área cúbica
   - **c.** obter mecanismos de trava para cada desktop para que não possa ser levado
2. **Erin tem uma preocupação na qual as pessoas possam se autenticar nos servidores no data center. O que ela pode fazer para impedir que usuários normais façam logon nesses sistemas?**
   - **a.** certificar-se de que o servidor esteja bloqueado
   - **b.** remover todos os teclados de todos os servidores
   - **c.** criar uma política de grupo que se aplique aos servidores para Negar Logon Local a todos os usuários não administrativos
3. **O que Erin pode fazer para impedir o uso de key loggers no banco?**
   - **a.** garantir que os terminais estejam bloqueados e fazer uma inspeção periódica das portas nos sistemas
   - **b.** nada – Erin não pode controlar o que é conectado aos seus computadores
   - **c.** converter todos os computadores em monitores sensíveis ao toque

dica

Pode não ser financeiramente viável ou fisicamente possível para o banco para converter todos os sistemas em telas sensíveis ao toque.

Respostas

1. Para garantir a segurança física dos computadores desktop, Erin pode:
   a. **desabilitar o uso de disquetes ou unidades USB usando políticas de grupo.** A maioria dos computadores possui um mecanismo para conectar um dispositivo de bloqueio nos desktops; porém, desabilitar as unidades USB e os disquetes desabilita uma maior ameaça.
2. Para impedir que usuários normais façam logon nos sistemas, Erin pode:
   c. **criar uma política de grupo que se aplique aos servidores para Negar Logon Local a todos os usuários não administrativos.** Um maior problema é a presença de pessoas no data center com acesso físico. No entanto, usuários normais não devem ter a capacidade de fazer logon local.
3. Para impedir o uso de key loggers no banco, Erin terá que:
   a. **garantir que os terminais estejam bloqueados e fazer uma inspeção periódica das portas nos sistemas**

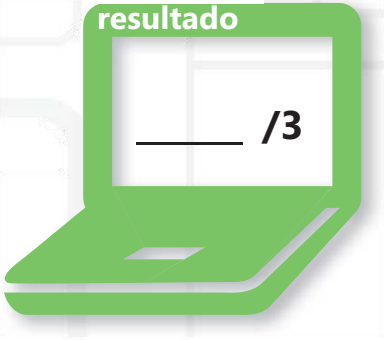
Detalhes essenciais

- **Keystroke logging** (geralmente conhecido como **key logging**) é o processo de gravar as teclas pressionadas em um teclado, frequentemente sem o conhecimento dos usuários.
- **Os controles de acesso** são os mecanismos que limitam o acesso a determinados itens de informações ou a determinados controles baseados nas identidades de usuários e sua associação em vários grupos de segurança predefinidos.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/library/bb457125.aspx**
- **http://www.microsoft.com/smallbusiness/security.aspx**

controle o seu resultado



Compreender a segurança da Internet

SITUAÇÃO: Terry Adams é o administrador de área de trabalho da Tailspin Toys. Para se manter atualizado com as últimas tecnologias de Internet, a Tailspin Toys decidiu atualizar seus navegadores para o IE (Internet Explorer) 8. Terry quer certificar-se de que eles usem muitos dos recursos de segurança embutidos no navegador, mantendo a funcionalidade dentro da intranet da empresa. Terry também gostaria de instruir seus usuários a serem bons "cidadãos da Internet" e praticarem navegação segura na Web. Ele sabe que a primeira linha de defesa em segurança na Internet é um usuário informado e hábil.

1. **Terry deseja configurar o recurso Zona da Internet no IE 8 de maneira que os usuários possam acessar facilmente o conteúdo na intranet local, mantendo um alto nível de segurança. O que ele deve fazer?**
   - **a.** criar uma rede de perímetro e certificar-se de que o site da intranet esteja localizado aqui e tenha um único PC em cada departamento com a atribuição IBPC (PC para Navegação na Intranet)
   - **b.** ir para as Opções da Internet, selecionar Segurança e adicionar o site da intranet à lista de Sites de Intranet Local
   - **c.** imprimir o conteúdo do site da intranet semanalmente e distribui-lo nos malotes
2. **O que Terry pode dizer à sua equipe para procurar no site para ter certeza de que eles estão em um site seguro?**
   - **a.** um cadeado no canto inferior direito do navegador e **https://** na barra de endereços
   - **b.** as informações de contato no site
   - **c.** eles não devem estar navegando em sites seguros porque você não pode confiar em nenhum site
3. **Qual é o nível de segurança definido na zona Sites Restritos?**
   - **a.** baixo; os sites são restritos e, portanto, não são uma preocupação
   - **b.** alto; desabilita a maioria dos recursos, tem o máximo de segurança e protege contra o conteúdo prejudicial
   - **c.** médio; um bom equilíbrio entre muito restrito e muito aberto

dica

O nível padrão na zona sites restritos é definido como Alto.

Respostas

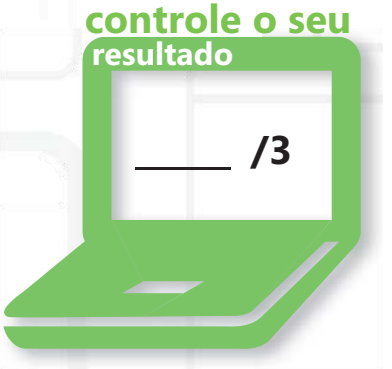
1. Para configurar o recurso Zona da Internet no IE 8 e permitir que os usuários naveguem facilmente na intranet local, Terry deve:
   b. ir para as Opções da Internet, selecionar Segurança e adicionar o site da intranet à lista de Sites de Intranet Local
2. Para certificar-se de que eles estejam em um site seguro, os funcionários podem procurar:
   a. um cadeado no canto inferior direito do navegador e https:// na barra de endereços. Isso não garante que o site é seguro. No entanto, é um começo.
3. O nível de segurança na zona Sites Restritos é:
   b. alto; desabilita a maioria dos recursos, tem o máximo de segurança e protege contra o conteúdo prejudicial

Detalhes essenciais

- Uma **zona da Internet** contém sites que não estão em seu computador ou intranet local ou que ainda não estão atribuídos a outra zona. O nível de segurança padrão é Médio.
- Um **site seguro** é um site com a capacidade de oferecer transações seguras, garantindo que números de cartão de crédito e outras informações pessoais não sejam acessíveis a partes não autorizadas.

AJUDA RÁPIDA

- **http://support.microsoft.com/kb/174360**



Compreender a segurança sem fio

SITUAÇÃO: Pilar Ackerman é o administrador de sistemas da Fourth Coffee, uma cadeia nacional de lojas de café muito popular e rentável. A concorrência no negócio de lojas de café é feroz! Para manter uma vantagem competitiva, a Fourth Coffee planeja adicionar o acesso sem fio aberto, de alta velocidade para seus clientes e o acesso sem fio seguro para os funcionários em todas as 200 lojas da Fourth Coffee. Pilar é confrontado com vários problemas de segurança e deve garantir que o tráfego da empresa esteja seguro. Além disso, ele está sob pressão para tornar este novo recurso uma estratégia vencedora.

1. **Qual é o protocolo mais seguro que Pilar pode implementar para garantir que o tráfego da empresa seja criptografado?**
   - **a.** WEP (Wired Equivalent Privacy)
   - **b.** WPA (WiFi Protected Access) 2
   - **c.** EAP (Extensible Authentication Protocol)
2. **Além de criptografar o tráfego sem fio da empresa, o que mais Pilar pode fazer para adicionar outro nível de segurança?**
   - **a.** implementar o isolamento de ponto de acesso e ocultar o SSID (Service Set Identifier)
   - **b.** desativar os pontos de acesso da empresa quando os clientes chegarem
   - **c.** habilitar a filtragem MAC
3. **Pilar gostaria que seus funcionários fossem independentes na solução dos próprios problemas deles com conexões sem fio antes de contatá-lo. Que etapa de solução de problemas básicos ele pode instruí-los a executar?**
   - **a.** reiniciar os computadores
   - **b.** aplicar um ciclo de energia nos pontos de acesso sem fio
   - **c.** clicar com o botão direito do mouse no ícone de rede na bandeja do sistema e selecionar Solucionar Problemas

dica

Aplicar o ciclo de energia no ponto de acesso desconectaria outros usuários da rede.

Respostas

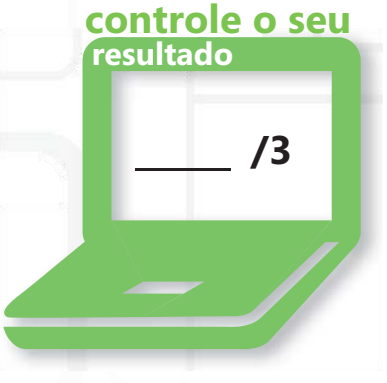
1. O protocolo mais seguro que Pilar pode implementar para garantir que o tráfego da empresa seja criptografado é:
   b. WPA (WiFi Protected Access) 2. O EAP é um recurso de segurança que controla a autenticação e o WPA é mais seguro que o WEP.
2. Pilar pode adicionar outro nível de segurança:
   a. implementando o isolamento de ponto de acesso e ocultando o SSID (Service Set Identifier). A filtragem MAC é uma opção; porém, os endereços MAC podem ser "falsificados" ou "alterados". Ocultar o SSID é uma medida simples de segurança que pode ser implementada.
3. Pilar pode instruir à equipe para solucionar problemas:
   c. clicando com o botão direito do mouse no ícone de rede na bandeja do sistema e selecionando Solucionar Problemas

Detalhes essenciais

- Um **SSID (Service Set Identifier)** é um identificador único de 32 caracteres anexado ao cabeçalho de pacotes enviados sobre uma WLAN que age como uma senha quando um dispositivo móvel tenta se conectar às estações de comunicação em uma LAN sem fio.
- **O WPA (Wi-Fi protected access)** é um padrão de Wi-Fi projetado para melhorar os recursos de segurança de WEP.
- **O WEP (Wired equivalent privacy)** é um sistema de algoritmo de criptografia incluído como parte do padrão 802.11, desenvolvido pelo Institute of Electrical and Electronics Engineers como uma medida de segurança para proteger LANs sem fio contra a interceptação casual.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/magazine/2005.11.securitywatch.aspx**
- **http://windows.microsoft.com/pt-BR/windows-vista/Quais-são-os-diferentes-métodos-de-segurança-da-rede-sem-fio**
- **http://www.windowsnetworking.com/articles_tutorials/Securing-Wireless-Network-Traffic-Part1.html**



2

Noções básicas sobre a segurança do sistema operacional

NESTE CAPÍTULO

- 2.1A Compreender a autenticação do usuário
- 2.1B Compreender a autenticação do usuário
- 2.2 Compreender as permissões
- 2.3 Compreender as políticas de senha
- 2.4 Compreender as políticas de auditoria
- 2.5A Compreender a criptografia
- 2.5B Compreender a criptografia
- 2.6 Compreender o malware

Compreender a autenticação do usuário

SITUAÇÃO: Jim Hance é um administrador de segurança da Coho Winery. Uma variedade de ameaças de segurança ocorreu ao longo dos últimos meses e a gerência está preocupada. Eles não podem ter um sistema em risco; seus clientes esperam um site confiável e seguro. Jim está analisando as políticas de segurança da Coho Winery para determinar onde a empresa pode precisar de políticas mais fortes ou, pelo menos, para atualizar as políticas e medidas de segurança existentes. Sua primeira tarefa é determinar os pontos fortes da empresa relacionados à autenticação de usuários.

1. **Jim sabe que as senhas de alta segurança são um elemento essencial no plano de segurança. Que características compõem uma senha de alta segurança?**
   - **a.** contém 7 ou mais caracteres; não contém o nome de usuário, nome real ou nome da empresa
   - **b.** contém números sequenciais incorporados ao nome da empresa
   - **c.** contém o sobrenome e o endereço de email do usuário
2. **Que protocolo pode ser usado para proteger a autenticação de estações de trabalho e computadores na rede?**
   - **a.** TCP/IP
   - **b.** Kerberos
   - **c.** LDAP (Lightweight Directory Access Protocol)
3. **Que estratégia Jim pode implementar para reduzir o número de vezes em que um usuário teria que autenticar para acessar um recurso específico?**
   - **a.** autenticação de dois fatores
   - **b.** certificados digitais
   - **c.** SSO (Logon Único)

dica

Reduzir o número de vezes em que um usuário tem que autenticar pode reduzir as possibilidades de interceptação de suas credenciais.

Respostas

1. Uma senha de alta segurança:
   a. **contém 7 ou mais caracteres; não contém o nome de usuário, nome real ou nome da empresa**
2. Para proteger a autenticação de estações de trabalho e computadores na rede, Jim pode usar:
   b. **Kerberos**
3. Para reduzir o número de vezes em que um usuário teria que autenticar para acessar um recurso específico, Jim pode implementar:
   c. **SSO (Logon Único)**

Detalhes essenciais

- **A autenticação** é o processo de obter credenciais de identificação, como um nome e uma senha de um usuário e validar essas credenciais em alguma autoridade, como em um banco de dados.
- **Kerberos** autentica a identidade de usuários que tentam fazer logon em uma rede e criptografa as suas comunicações por meio da criptografia de chave secreta.
- **LDAP (Lightweight directory access protocol)** é um protocolo de rede desenvolvido para trabalhar nas pilhas TCP/IP para extrair informações de um diretório hierárquico, como o X.500.
- **O serviço RADIUS** é um protocolo de Internet no qual um servidor de autenticação fornece a autorização e as informações sobre autenticação a um servidor de rede ao qual um usuário está tentando se vincular.

AJUDA RÁPIDA

- **http://www.microsoft.com/windowsserver2008/en/us/ad-main.asp**
- **http://web.mit.edu/Kerberos/#what_is**
- **http://technet.microsoft.com/en-us/library/bb463152.aspx**

Compreender a autenticação do usuário

SITUAÇÃO: O GDI (Graphic Design Institute) tem mais de 30.000 alunos. A segurança das informações pessoais dos alunos, incluindo dados financeiros, endereço, contatos familiares, necessidades especiais de saúde, e notas, é a primeira prioridade da equipe de administração da rede. No entanto, nos últimos meses, os dados dos alunos foram comprometidos em várias ocasiões. Os dados pessoais foram exibidos em um site de redes sociais, causando muito constrangimento para a equipe de rede. Os diretores do GDI pediram ao administrador da rede, Todd Rowe, para implementar medidas de autenticação mais fortes para os alunos, além de proibir que a equipe de TI faça logon com privilégios elevados. Todd tem várias opções, mas está necessidade de manter os processos razoavelmente fáceis para a equipe de assistência técnica.

1. **Todd deseja implementar as autenticações de dois fatores. Qual ele pode usar?**
   - **a.** cartão inteligente e senha do usuário
   - **b.** duas senhas
   - **c.** duas IDs de usuário com duas senhas
2. **Que serviço a equipe do GDI pode usar para substituir o logon com privilégios elevados?**
   - **a.** Área de Trabalho Remota
   - **b.** Logon Secundário - Executar Como
   - **c.** Gerenciador de Usuários para Domínios
3. **Qual é a desvantagem de usar a identificação biométrica?**
   - **a.** o usuário deve ter mãos
   - **b.** o custo é proibitivo para muitas organizações
   - **c.** uma verificação de retina pode ser falsificada

dica

A identificação biométrica é extremamente segura; porém, os dispositivos para suporte à biometria têm custo proibitivo.

Respostas

1. Para implementar as autenticações de dois fatores, Todd pode usar:
   a. **cartão inteligente e senha do usuário**
2. Em vez de fazer logon com privilégios elevados, a equipe pode usar:
   b. **Logon Secundário - Executar Como**
3. Uma desvantagem de usar a identificação biométrica é:
   b. **o custo é proibitivo para muitas organizações**

Detalhes essenciais

- Um **certificado** é uma credencial eletrônica que autentica usuários na Internet e em intranets.
- **PKI (Infraestrutura de Chave Pública)** é um esquema assimétrico que usa um par de chaves para criptografia: a chave pública criptografa os dados e a chave secreta correspondente os descriptografa.
- O comando **Executar Como** permite que um usuário execute ferramentas e programas específicos em qualquer estação de trabalho com permissões diferentes das fornecidas pelo logon atual do usuário.
- Etapas para alterar sua senha:
  - Pressione <control><alt><delete> e selecione Alterar Senha
- Etapas para usar o Logon Secundário ou Executar Como. . .
  - Clique com o botão direito no ícone do aplicativo e selecione Executar como Administrador

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/library/cc782756(WS.10).aspx**
- **http://technet.microsoft.com/pt-br/library/cc756862(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc261673(office.12).aspx**

Compreender as permissões

SITUAÇÃO: Fabrikam, Inc. sofreu recentemente uma reorganização básica e uma variedade de mudanças corporativas. Shawn Richardson é o administrador de rede na Fabrikam e recebeu a tarefa de alinhar os servidores da empresa com a nova realidade organizacional. Na primeira etapa, Shawn concluiu uma auditoria de segurança dos servidores de arquivos do Microsoft® Windows Server® 2008 R2 e determinou que a segurança de pastas e compartilhamentos precisa ser revisada com base na reorganização corporativa. Shawn deve apresentar seu plano para a gerência e fornecer direções para os membros de sua equipe terminarem o projeto.

1. **Shawn observou que o sistema de arquivo não está protegido em alguns compartilhamentos. Qual é a configuração padrão de permissão quando um compartilhamento é criado?**
   - **a.** todos com permissão de Leitura
   - **b.** administradores com a permissão Controle Total
   - **c.** todos com a permissão Controle Total
2. **Por que Shawn deve impor o UAC (Controle de Conta de Usuário) no domínio?**
   - **a.** para que ele possa controlar as contas de usuário
   - **b.** para ajudar a impedir alterações não autorizadas em computadores no domínio
   - **c.** para permitir que os usuários se autentiquem com a senha de administrador para executar uma tarefa administrativa
3. **Que recurso (também disponível com os objetos do Active Directory) facilitará o trabalho de Shawn quando ele reatribuir permissões por não ter que atribuir permissões a todas as pastas pai e filha?**
   - **a.** arquivos em lotes
   - **b.** herança
   - **c.** membros da equipe

dica

A herança permite a propagação de direitos ou permissões de um objeto pai para um objeto filho. Este recurso pode ser bloqueado ou removido.

Respostas

1. Quando um compartilhamento é criado, a permissão padrão é:
   a. **todos com permissão de Leitura**
2. Shawn deve impor o UAC (Controle de Conta de Usuário) no domínio porque:
   b. **isso ajudará a impedir alterações não autorizadas em computadores no domínio**
3. O trabalho de Shawn pode ser facilitado durante a reatribuição de permissões usando:
   b. **herança**

Detalhes essenciais

- **As permissões** incluem Controle Total, Modificar, Leitura e Execução, Listar Conteúdo da Pasta, Leitura, e Gravação, e podem ser aplicadas aos objetos de pastas e arquivos. As permissões também podem ser aplicadas aos objetos do Active Directory.
- **A herança** é o conceito de permissões que são propagadas para um objeto a partir de um objeto pai. A herança é encontrada nas permissões do sistema de arquivos e nas permissões do Active Directory. Ela não se aplica às permissões de compartilhamento.
- **NTFS (New Technology File System), FAT e FAT32.** A principal diferença entre os sistemas de arquivos NTFS e FAT é a capacidade de aplicar a segurança no sistema de arquivos. É possível conceder ou negar diversas permissões no NTFS. O NTFS também oferece suporte à capacidade de criptografar dados.
- **As permissões de compartilhamento e do NTFS** são aplicadas com base em como o recurso é acessado. As permissões de compartilhamento são eficazes quando o recurso está sendo acessado por meio da da rede, enquanto as permissões do NTFS são eficazes o tempo todo. Quando as permissões de compartilhamento e do NTFS são aplicadas ao mesmo recurso, a permissão mais restrita ganha.

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/library/cc730772.aspx**
- **http://technet.microsoft.com/pt-br/library/cc771375.aspx**
- **http://technet.microsoft.com/pt-br/library/cc770906(WS.10).aspx**

Compreender as políticas de senha

SITUAÇÃO: Jay Hamlin recebeu a difícil tarefa de impor políticas de senhas de alta segurança para a Wingtip Toys. Ele compreende a necessidade de usar senhas complexas com comprimento mínimo, mas está com dificuldades em fazer a equipe entender como a segurança de toda a organização Wingtip Toys pode depender destes requisitos e alguns mais que ele pretende exigir. Ele também deve determinar quantas vezes um usuário pode tentar fazer logon antes de ter sua conta bloqueada, com que frequência os usuários devem alterar as senhas, e com que frequência os usuários podem reutilizar senhas favoritas.

Seu plano de uma Política de Complexidade de Senha inclui os seguintes critérios para senhas:

- Não pode conter o nome de logon do usuário
- Deve ter pelo menos 6 caracteres
- Deve conter três dos seguintes quatro tipos de caracteres: caractere minúsculo, maiúsculo, numérico e especial

1. **Que dilema Jay está enfrentando quando ele torna seus requisitos de senha muito difíceis?**
   - **a.** uma senha complexa pode ser difícil de adivinhar e difícil de lembrar
   - **b.** Jay não terá mais amigos no trabalho
   - **c.** os usuários não usarão as senhas

2. **O que a política de tempo de vida máximo da senha significa?**
   - **a.** determina a idade que o usuário deve ter para criar a senha
   - **b.** refere-se à período antes da senha ter que ser alterada
   - **c.** refere-se ao tempo de vida que a senha deve ter antes que o usuário tenha permissão para alterá-la

3. **O que acontece quando você define o valor de Aplicar Histórico de Senhas para 10?**
   - **a.** o usuário tem 10 tentativas para validar sua senha
   - **b.** a senha deve ser usada por pelo menos 10 dias antes que possa ser alterada
   - **c.** o sistema armazena as últimas 10 senhas e não permitirá que o usuário reutilize qualquer uma das últimas 10

dica

O histórico de senhas impede que os usuários reutilizem suas senhas.

Respostas

1. O dilema que Jay enfrenta com os requisitos difíceis de senha é que:
   a. **uma senha complexa pode ser difícil de adivinhar e difícil de lembrar**
2. Tempo de vida máximo da senha:
   b. **refere-se à período antes da senha ter que ser alterada**
3. Quando você define o valor de Aplicar Histórico de Senhas para 10:
   c. **o sistema armazena as últimas 10 senhas e não permitirá que o usuário reutilize qualquer uma das últimas 10**

Detalhes essenciais

- **O bloqueio de conta** é um recurso de segurança no Windows que bloqueará uma conta de usuário se um número de tentativas de logon com falha ocorrer em um determinado período de tempo, com base em configurações de bloqueio de política de segurança.
- Um **ataque a senha** é um ataque em um computador ou rede no qual uma senha é roubada e descriptografada ou é revelada por um programa de dicionário de senha.
- **A detecção de senha** é uma técnica empregada pelos invasores para capturar senhas interceptando pacotes de dados e procurando suas senhas.
- O Microsoft Windows Server 2008 permite as políticas refinadas de senha, que permitem a atribuição mais flexível de políticas de senha na organização por meio do Active Directory®.

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/library/cc784090(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/cc875814.asp**

Compreender as políticas de auditoria

SITUAÇÃO: A rede da Margie's Travel deve ser muito segura. Os arquivos contêm informações de clientes, incluindo números de cartão de crédito, datas de nascimento e endereços, além de fotocópias dos passaportes. O roubo de identidade seria uma possibilidade real se o sistema fosse invadido. Obviamente, este não é um risco aceitável para Margie's Travel.

Arlene Huff é o administrador de sistemas da Margie's Travel. A empresa solicitou a ela que rastreie que tenta fazer logon no sistema e em que horários as tentativas ocorrem. Eles também pediram que ela crie um sistema para rastrear quando os arquivos confidenciais são abertos e por quem. Arlene aceitou contente essa tarefa e não fez nenhuma reclamação.

1. **Arlene deseja registrar em log quando alguém não consegue fazer logon no sistema como administrador, mas por que ela deseja registrar em log quando são alguém também consegue?**
   - **a.** para determinar se e quando alguém estiver se autenticando com êxito com privilégios elevados
   - **b.** para certificar-se de que eles conseguem entrar sem problemas
   - **c.** para monitorar o espaço da unidade no computador
2. **Onde os eventos de auditoria de arquivos são gravados quando a auditoria está habilitada?**
   - **a.** log de eventos de auditoria
   - **b.** pfirewall.log
   - **c.** log de eventos de segurança
3. **Por que é importante proteger adequadamente os logs de auditoria?**
   - **a.** para que os hackers em potencial não possam excluir os logs de eventos para cobrir seus rastros
   - **b.** não é importante, ninguém olha para os logs de auditoria
   - **c.** para que somente o pessoal autorizado possa exibir os arquivos de log

dica

Hackers de computador especializados modificação os logs de auditoria quando eles terminarem de obter as informações para que pareça que eles nunca estiveram lá.

Respostas

1. Arlene deseja armazenar em log quando alguém consegue se autenticar no sistema, bem como quando não:

a. para determinar se e quando alguém estiver se autenticando com êxito com privilégios elevados.

Se alguém falhou quatro vezes e teve êxito na quinta vez, isso pode indicar uma atividade de hacker.

2. Os eventos de auditoria de arquivos habilitados são:

c. log de eventos de segurança

3. É importante proteger adequadamente os logs de auditoria

a. para que os hackers em potencial não possam excluir os logs de eventos para cobrir seus rastros

Detalhes essenciais

- **A auditoria** é o processo que um sistema operacional usa para detectar e registrar eventos relacionados a segurança, como uma tentativa de criar, acessar ou excluir objetos (arquivos e diretórios).
- Uma **política de auditoria** é uma política que determina os eventos de segurança a serem relatados para o administrador de rede.
- O **log de segurança**, que pode ser gerado por um firewall ou outro dispositivo de segurança que lista eventos que poderiam afetar a segurança, como tentativas de acesso ou comandos, e os nomes dos usuários envolvidos.

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/library/dd408940(WS.10).aspx**
- **http://technet.microsoft.com/en-us/library/dd349800(WS.10).aspx**

Compreender a criptografia

SITUAÇÃO: A Adventure Works expandiu recentemente sua equipe de vendas móvel. A equipe de gerenciamento reconheceu recentemente as considerações de segurança exclusivas associadas às centenas de computadores laptop localizados simultaneamente em centenas de locais sem segurança.

David Johnson é o administrador de rede responsável pela equipe de vendas móvel da Adventure Works. A equipe de gerenciamento chamou a atenção dele recentemente sobre aos dados confidenciais que poderiam cair nas mãos da concorrência, se qualquer um dos computadores laptop fosse roubado ou extraviado. Ele deve ter uma solução que possa garantir a confidencialidade dos dados em estações móveis que executam o Windows® 7 Enterprise – e precisa dela depressa!

1. **O que David pode habilitar para certificar-se de que seus dados estejam seguros?**
   - **a.** EFS (Encrypting File System)
   - **b.** protetor de tela protegido por senha
   - **c.** BitLocker
2. **O que deve ser configurado para garantir que o armazenamento BitLocker® possa ser recuperado?**
   - **a.** a identificação pessoal do vendedor e as credenciais de logon
   - **b.** o BitLocker para usar os agentes de recuperação de dados
   - **c.** o Secret Retrieval Agent
3. **Quais são as considerações que David terá que ponderar ao decidir se deseja usar o BitLocker?**
   - **a.** a conscientização e autodisciplina da equipe de vendas
   - **b.** a implantação de hardware porque o BitLocker exige uma partição reservada para o sistema
   - **c.** é tão fácil que não há nenhuma consideração séria

dica

O Bitlocker que uma partição reservada para o sistema seja criada durante uma instalação padrão.

Respostas

1. Para certificar-se de que os dados estejam seguros, David deve habilitar:
   c. BitLocker
2. Para garantir que os dados protegidos possam ser recuperados, caso o armazenamento protegido pelo BitLocker seja movido para outro computador, o administrador deve criar e armazenar adequadamente:
   b. o BitLocker para usar os agentes de recuperação de dados
3. Ao usar o BitLocker, o administrador deve considerar:
   b. a implantação de hardware porque o BitLocker exige uma partição reservada para o sistema

Detalhes essenciais

- **a criptografia de unidade do BitLocker (ToGo)** é um recurso de proteção de dados disponível no Windows Server 2008 R2 e em algumas edições do Windows 7.
- **EFS (Encrypting File System)** é um recurso do Windows que permite armazenar informações no seu disco rígido em um formato criptografado.
- **Criptografia** é o processo de criptografar dados para evitar acessos não autorizados, especialmente durante a transmissão.

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/windows/dd408739.aspx**
- **http://technet.microsoft.com/pt-br/library/cc732774.aspx**
- **http://technet.microsoft.com/pt-br/library/ee706523(WS.10).aspx**
- **http://technet.microsoft.com/pt-br/library/ee706518(WS.10).aspx**

Compreender a criptografia

SITUAÇÃO: A proprietária da Southridge Video tem grande orgulho na estreita relação que ela tem com os gerentes das muitas filiais ao longo da costa. A comunicação semanal é a chave para manter as relações e se manter no topo da evolução e dos desafios dos negócios.

O proprietário e os gerentes gostariam de substituir sua conferência telefônica matinal às segundas por uma conferência de vídeo matinal às segundas entre a sede da empresa e as muitas filiais. Eles solicitaram que o administrador de WAN, Jeff Wang, crie uma solução econômica. A solução tem de funcionar entre os escritórios das filiais; portanto, ter uma conexão dedicada entre os escritórios é muito caro. A melhor solução é usar a conexão com a Internet de cada escritório.

1. **O que criará uma conexão segura sobre uma rede desprotegida?**
   - **a.** VPN (Rede Virtual Privada)
   - **b.** configurar o recurso de retorno de chamada em seu Servidor de Roteamento e Acesso Remoto
   - **c.** usar um site de redes sociais para realizar as reuniões de conferência
2. **Jeff precisa decidir entre o protocolo PPTP ou o protocolo L2TP. Que protocolo é mais seguro?**
   - **a.** PPTP
   - **b.** L2TP
   - **c.** nenhum dos dois, ambos passam as informações em texto não criptografado
3. **O que é um certificado público?**
   - **a.** um prêmio dado em reconhecimento das políticas de segurança empresarial superior
   - **b.** parte de uma criptografia de duas partes que não é compartilhada com outras partes
   - **c.** uma instrução assinada digitalmente que é frequentemente usada para autenticação e para proteção de informações em redes abertas

dica

Um certificado de chave particular é uma parte da criptografia de duas partes que reside no computador de origem e não é compartilhada.

Respostas

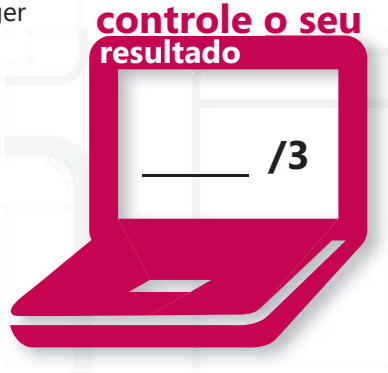
1. Uma conexão segura sobre uma rede desprotegida pode ser criada com um(a):
   a. **VPN (Rede Virtual Privada)**
2. O protocolo mais seguro é:
   b. **L2TP.** O PPTP usa o MPPE para segurança, que é menos seguro do que o L2TP, e usa o IPsec como seu método de criptografia.
3. Um certificado público é:
   c. **uma instrução assinada digitalmente que é frequentemente usada para autenticação e para proteção de informações em redes abertas**

Detalhes essenciais

- **Protocolo L2TP com IPSec** é uma combinação do PPTP e do L2F que usa o IPsec para criptografia.
- O usuário guarda o segredo da **chave particular** e usa-o para criptografar assinaturas digitais e decifrar mensagens recebidas.
- O usuário divulga a **chave pública** para o público, que pode usá-la para criptografar as mensagens a serem enviadas para o usuário e para decifrar a assinatura digital do usuário.
- Uma **VPN (rede virtual privada)** é um túnel seguro em execução sobre uma rede pública, como a Internet que usa a tecnologia de criptografia para proteger os dados contra interceptação e compreensão por usuário não autorizados.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/library/cc700805.aspx**



Compreender o malware

SITUAÇÃO: A Consolidated Messenger trabalha com as opiniões de clientes sobre muitos setores de negócios. Cada dia eles recebem milhares de emails de clientes felizes e infelizes, que são direcionados para os indivíduos apropriados nas empresas do cliente.

Mary Kay Anderson é o administrador de sistemas da Consolidated Messenger. A empresa teve vários surtos de vírus na rede que parecem ter sido propagados por email. Eles solicitaram que Mary Kay produza uma sessão "almoce e aprenda" para ensinar à equipe da Consolidated Messenger sobre softwares e emails mal-intencionados. Mary Kay recebeu a tarefa de encontrar uma solução que protegerá melhor o sistema.

1. **O que os funcionários devem fazem quando recebem um email suspeito de um cliente ou colega de trabalho que contém um hiperlink incorporado?**
   - **a.** excluir o email e contatar a Mary Kay e o cliente ou colega
   - **b.** clicar rapidamente no hiperlink para ver o que pode ocorrer para avaliar a ameaça sozinhos
   - **c.** encaminhar o email a outros colegas de trabalho informando-os que o email não é legítimo
2. **O que Mary Kay pode fazer para impedir que emails suspeitos entrem em sua rede?**
   - **a.** instalar o Microsoft® Forefront® e o Threat Management Gateway, e configurá-lo para bloquear emails suspeitos
   - **b.** desabilitar o email na Internet
   - **c.** ameaçar os colegas de trabalho que eles serão demitidos se encaminharem qualquer email
3. **Que ferramenta a Mary Kay pode baixar para remover software mal-intencionado (malware)?**
   - **a.** RSAT (Ferramentas de Administração de Servidor Remoto)
   - **b.** Ferramenta de Remoção de Software Mal-Intencionado da Microsoft
   - **c.** qualquer ferramenta de software de segurança anunciada na Web – elas são todas iguais

dica

Uma ferramenta de remoção de software mal-intencionado está incluída nas atualizações do Windows.

Respostas

1. Quando os funcionários recebem um email suspeito que contém um hiperlink incorporado, eles devem:
   a. **excluir o email e contatar a Mary Kay e o cliente ou colega.** Nunca encaminhe um email com conteúdo suspeito. Se um email tiver um anexo ou link, contate o remetente e verifique se ele ou ela enviou a mensagem.
2. Para impedir que emails suspeitos entrem na rede, Mary Kay pode:
   a. **instalar o Microsoft Forefront e o Threat Management Gateway, e configurá-lo para bloquear qualquer email suspeito.** O Exchange Server possui várias ferramentas de filtragem de spam. O Forefront e o TMG são medidas de segurança adicionais para proteger melhor o sistema.
3. Para remover software mal-intencionado (malware), Mary Kay pode baixar:
   b. **Ferramenta de Remoção de Software Mal-Intencionado da Microsoft**

Detalhes essenciais

- Um **bot** é um programa que executa alguma tarefa em uma rede, especialmente uma tarefa que seja repetitiva ou demorada.
- Um **rootkit** é uma coleção de programas de software que um invasor pode usar para obter acesso remoto não autorizado a um computador e lançar ataques adicionais.
- **Spyware** é o software às vezes chamado de spybot ou software de rastreamento. Spyware usa outras formas de software e programas enganosos que conduzem determinadas atividades em um computador sem obter consentimento apropriado do usuário.
- Um **trojan** é um programa que parece ser útil ou inofensivo, mas que contém código oculto projetado para explorar ou danificar o sistema no qual ele é executado.
- Um **worm** usa código mal-intencionado de auto-propagação que pode ser distribuído automaticamente a partir de um computador para outro através de conexões de rede.

AJUDA RÁPIDA

- **http://www.microsoft.com/downloads/details.aspx?FamilyId=F24A8CE3-63A4-45A1-97B6-3FEF52F63ABB&displaylang=en**
- **http://support.microsoft.com/kb/889741**

3

Noções básicas sobre a segurança da rede

NESTE CAPÍTULO

Compreender os firewalls dedicados

SITUAÇÃO: Matt Berg recebeu várias certificações Microsoft e é agora o seu próprio patrão como consultor independente de segurança. A Trey Research contratou seus serviços para realizar uma avaliação da segurança de sua rede. A Trey Research tem vários servidores que estão expostos na Internet e teme que sua rede interna possa estar vulnerável a um ataque. Eles têm um firewall de perímetro único, mas não sabem se isso é suficiente. O trabalho de Matt é avaliar a situação e fazer recomendações em como a Trey Research pode proteger seus dados.

1. **O que Matt deve recomendar que a Trey Research faça com seus servidores expostos à Internet?**
   - **a.** criar uma rede de perímetro para isolar esses servidores da rede interna
   - **b.** terceirizar os serviços associados
   - **c.** nenhuma ação é necessária, os servidores estão muito bem onde eles estão na rede interna
2. **O firewall de perímetro único é suficiente para a Trey Research?**
   - **a.** sim, um único firewall fornece mais do que a proteção necessária em qualquer ambiente
   - **b.** não, as preocupações da Trey Research são justificadas. Eles devem ter diversos dispositivos de segurança que oferecem "defesa abrangente" para sua organização, além de permitir firewalls e antivírus de software para a estação de trabalho
   - **c.** não, eles também devem criar uma DMZ
3. **A inspeção de pacotes com e sem estado proporciona uma maior segurança?**
   - **a.** uma inspeção de pacotes sem estado porque é mais eficiente e pode interromper mais pacotes
   - **b.** nenhuma das duas, elas não fornecem nenhum tipo de segurança
   - **c.** com estado porque ela inspeciona os pacotes conformes eles passam pela conexão

dica

A inspeção de pacotes sem estado é um tipo mais rápido de segurança e exige menos memória, mas não é totalmente confiável.

Respostas

1. Matt deve recomendar que a Trey Research:
   a. **criar uma rede de perímetro para isolar esses servidores da rede interna.** Os servidores e dispositivos expostos à Internet não devem residir em uma rede interna. Eles devem ser segmentados ou isolados em uma parte segura da rede.
2. O firewall de perímetro único é suficiente para a Trey Research?
   b. **não, as preocupações da Trey Research são justificadas. Eles devem ter diversos dispositivos de segurança que oferecem "defesa abrangente" para sua organização, além de permitir firewalls e antivírus de software para a estação de trabalho.** Não existe uma solução única pode proteger uma rede; porém, proporcionar diversas camadas de segurança reduz a exposição da empresa.
3. A melhor escolha de inspeção de pacotes é:
   c. **com estado porque ela inspeciona os pacotes conformes eles passam pela conexão**

Detalhes essenciais

- Um **firewall** é um sistema de segurança destinado a proteger a rede de uma organização contra ameaças externas, como hackers, oriundas de outra rede, como a Internet.
- **A filtragem de pacotes** é o processo de controle de acesso à rede baseado em endereços IP. Os firewalls irão, muitas vezes, incorporar filtros que permitem ou negam a usuários a capacidade de entrar ou sair da LAN (rede local).
- Um **servidor proxy** é um equipamento de segurança que gerencia tráfego de Internet para e de uma rede local e pode fornecer outros recursos, como cache em documento e controle de acesso.

AJUDA RÁPIDA

- **http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx**
- **http://technet.microsoft.com/en-us/library/cc700828.aspx**
- **http://technet.microsoft.com/en-us/library/cc700820.aspx**

Compreender a NAP (Proteção de Acesso à Rede)

SITUAÇÃO: A Adventure Works é um dos maiores fornecedores do país de equipamento esportivo sofisticado. Vinte e cinco vendedores da Adventure Works viajam pelo país vendendo os equipamentos a varejistas. Eles voltam para a sede da empresa toda sexta-feira com seus laptops para participar de reuniões e treinamento.

Allie Bellew é o administrador de rede da Adventure Works e gostaria de implementar um método que garanta que os dispositivos móveis estejam em um bom estado de "saúde" da segurança quando eles acessam a rede corporativa durante as reuniões de sexta-feira.

1. **Que controle ou estratégia Allie pode implementar para garantir a saúde da segurança?**
   - **a.** proteção de Acesso à Rede, que verificará a integridade de cada dispositivo móvel
   - **b.** verificações de vírus toda vez que os vendedores fazem logon
   - **c.** recriar imagem de cada laptop antes de conectá-lo à rede
2. **Além de proteger contra um laptop infectado por vírus, o que mais a NAP pode fazer?**
   - **a.** proteger contra perda de dados
   - **b.** mais nada, isso é simplesmente uma verificação de vírus glorificada
   - **c.** verificar a integridade completa do dispositivo, verificando se ele tem as atualizações de software ou alterações de configuração mais recentes
3. **O que Allie pode fazer sobre os computadores que não são compatíveis com NAP?**
   - **a.** atualizar os computadores que não são compatíveis
   - **b.** definir exceções no NAP para aqueles dispositivos que não são compatíveis
   - **c.** impedir que estes dispositivos usem a rede

dica

Exceções podem ser definidas para os sistemas "necessários para a missão"até que eles possam ser atualizados.

Respostas

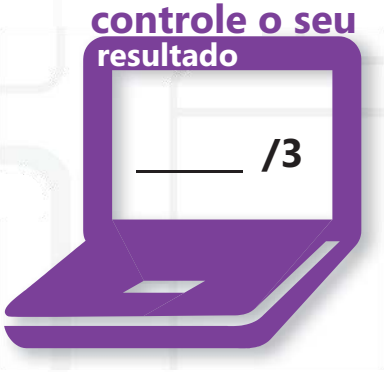
1. Allie pode implementar:
   a. **Proteção de Acesso à Rede, que verificará a integridade de cada dispositivo móvel**
2. Além de proteger contra um laptop infectado por vírus, a NAP pode:
   c. **verificar a integridade completa do dispositivo, verificando se ele tem as atualizações de software ou alterações de configuração mais recentes.** Os sistemas que não receberam as atualizações podem ser tão problemáticos quanto os sistemas infectados por malware.
3. Para os computadores que não são compatíveis com NAP, Allie deve:
   b. **definir exceções no NAP para aqueles dispositivos que não são compatíveis**

Detalhes essenciais

- **A NAP (Proteção de Acesso à Rede)** é uma nova plataforma e solução que controla o acesso aos recursos da rede baseado em uma identidade de computador do cliente e conformidade com a política de governança corporativa.
- **Os pontos de imposição da NAP** são computadores ou dispositivos de acesso à rede que usam a NAP ou podem ser usados com a NAP para solicitar a avaliação de um estado de integridade do cliente NAP e fornecer acesso restrito ou comunicação à rede.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/network/cc984252.aspx**
- **http://technet.microsoft.com/en-us/network/bb545879.aspx**
- **http://www.microsoft.com/windowsserver2008/pt/br/nap-faq.aspx**



Compreender o isolamento de rede

SITUAÇÃO: Coho Winery está no ramo de vinícolas há três gerações. Eles continuam a produzir vinho de qualidade dos mesmos vinhedos e nas mesmas adegas antigas. Até a maioria de sua organização de negócios permaneceu a mesma por décadas. Agora é hora de atualizar o lado corporativo da Coho com as novas tecnologias relacionadas com sua infraestrutura de manutenção de dados.

Karen Berg recebeu a tarefa de avaliar a infraestrutura de rede da Coho Winery e de fornecer recomendações baseadas em suas necessidades específicas:

- A maioria dos funcionários precisa de acesso à Internet.
- Os computadores na vinícola estão isolados e não precisam de acesso à Internet.
- Os funcionários que "trabalham em casa" devem ter acesso à Rede Virtual Privada usando a Segurança de IP.

1. **O que Karen pode fazer para impedir que os computadores da fábrica da vinícola obtenham acesso à Internet?**
   - **a.** criar uma VLAN que não permite o acesso à Internet mas está truncada à rede principal
   - **b.** configurar manualmente cada computador para que ele não tenha um gateway
   - **c.** remover o Internet Explorer dos computadores
2. **Que tecnologia Karen terá que implementar para permitir o acesso à Internet para funcionários do escritório sem expô-los à Internet?**
   - **a.** configurar um computador direto que tem um endereço de IP público para que possa acessar a Internet
   - **b.** fornecer a cada usuário de escritório um modem dial-up para estabelecer uma conexão com a Internet
   - **c.** implementar um roteador para executar a Conversão de Endereços de Rede que permitirá que vários endereços particulares participem de uma rede pública
3. **Que função do Microsoft Windows Server 2008 R2 pode realizar o acesso à Internet e a solução de VPN?**
   - **a.** DHCP
   - **b.** Serviço de Área de Trabalho Remota
   - **c.** Serviço de Roteamento e Acesso Remoto

dica

A maioria dos sistemas operacionais de servidor têm alguma forma de tecnologia de roteamento. Os requisitos mínimos incluem ter várias NICs (placas de interface da rede).

Respostas

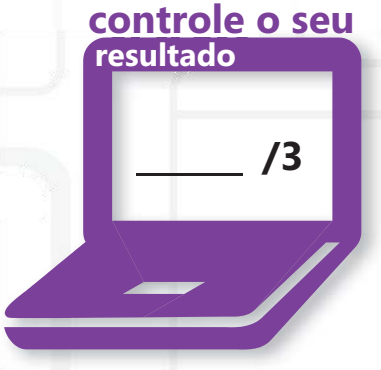
1. Para impedir que os computadores da fábrica obtenham acesso à Internet, Karen pode:
   a. **criar uma VLAN que não permite o acesso à Internet mas está truncada à rede principal**
2. Para permitir o acesso à Internet para funcionários do escritório sem expô-los à Internet, Karen pode:
   c. **implementar um roteador para executar a Conversão de Endereços de Rede que permitirá que vários endereços particulares participem de uma rede pública.** A maioria dos roteadores sem fio no varejo executam a Conversão de Endereços de Rede ou a Conversão de Endereços de Porta, que permitirá que os dispositivos de rede domésticos (Xbox, laptops etc.) tenham acesso à Internet.
3. O Microsoft Windows Server 2008 R2 pode realizar o acesso à Internet e a solução de VPN com:
   c. **(RRAS) Serviço de Roteamento e Acesso Remoto.** O RRAS pode servir como uma VPN e o gateway de Internet. O acesso à VPN pode ser protegido usando vários protocolos de segurança, incluindo o IPsec.

Detalhes essenciais

- **A NAT (Conversão de Endereços de Rede)** é o processo de conversão entre endereços IP usados em uma intranet ou rede privada e outros endereços IP.
- **O roteamento** é o processo de encaminhamento de pacotes entre redes, da origem ao destino.
- Uma **VLAN (LAN Virtual)** é um grupo de hosts com um conjunto comum de requisitos que se comunicam como se fossem anexados ao mesmo domínio de difusão, independentemente da sua localização física.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/network/bb531150.aspx**
- **http://technet.microsoft.com/en-us/network/bb545655.aspx**
- **http://www.microsoft.com/downloads/en/details.aspx?FamilyID=7E973087-3D2D-4CAC-ABDF-CC7BDE298847&displaylang=en**
- **http://pt.wikipedia.org/wiki/Virtual_LAN**



Compreender o isolamento de rede

SITUAÇÃO: Arlene Huff é o administrador de sistemas da Margie's Travel e tem estado bastante ocupado nas últimas semanas protegendo os dados da empresa e de clientes. Ocorreram atividades suspeitas na rede, mas felizmente as ações de Arlene para rastrear os usuários da rede protegeram o sistema. Mas o desafio de proteger os dados confidenciais é uma tarefa contínua.

A proprietária da empresa, Margie, gostaria que os agentes de viagens remotos tivessem acesso à rede corporativa para que possam verificar o email e publicar os compromissos agendados para aquele dia. Margie decidiu permitir que os agentes de viagem usem seus computadores domésticos, mas quer ter certeza de que as informações estão seguras. A segurança das informações de clientes é sua primeira prioridade.

1. **Qual seria a melhor solução geral para Margie's Travel?**
   - **a.** implementar um servidor VPN para permitir o acesso remoto pelos agentes de viagens
   - **b.** configurar um banco de modem e fazer com que os agentes de viagens comprem modems para seus computadores domésticos para que possam discar para o escritório
   - **c.** não há uma solução para o que Margie deseja

2. **Qual é o risco em potencial de ter os agentes de viagens usarem seus computadores domésticos para acessar a VPN?**
   - **a.** nenhum, a VPN resolve tudo e criptografa os dados
   - **b.** os agentes de viagens podem esquecer de desconectar, o que manterá a conexão VPN aberta, impedindo que outros se conectem
   - **c.** simplesmente ter uma VPN não evita que possíveis vírus e malware no computador doméstico infectem a rede

3. **Arlene está preocupada que supostos invasores possam penetrar a VPN. O que ela pode configurar para "seduzir" os invasores para compreender melhor os seus métodos?**
   - **a.** um honeypot fora da rede de perímetro, que é um programa falsificado que pode emular uma VPN ou serviço
   - **b.** um site de fantasia que diz "Nada para se ver aqui"
   - **c.** uma VPN falsa que nunca responde

dica

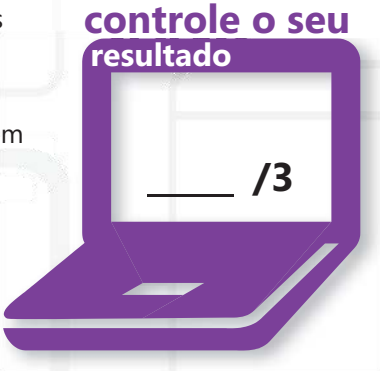
Honeypots estão localizados em toda a Internet e são usados para descobrir métodos que os invasores podem usar para comprometer o sistema.

Respostas

1. A melhor solução geral para Margie's Travel é:
   a. **implementar um servidor VPN para permitir o acesso remoto pelos agentes de viagens.** Ela pode configurar a VPN para usar vários métodos de criptografia.
2. O risco em potencial de ter os agentes de viagens usarem seus computadores domésticos para acessar a VPN é que:
   c. **simplesmente ter uma VPN não evita que possíveis vírus e malware no computador doméstico infectem a rede.** Arlene pode usar o Acesso Direto, novo no Windows 7 e no Windows Server 2008 R2, para ajudar a reduzir os possíveis riscos.
3. Para "seduzir" os invasores para compreender melhor os seus métodos, Arlene pode criar:
   a. **um honeypot fora da rede de perímetro, que é um programa falsificado que pode emular uma VPN ou serviço**

Detalhes essenciais

- Uma **rede de perímetro** (também conhecida como DMZ, zona desmilitarizada, e subrede filtrada) é uma rede lógica ou física que contém e expõe os serviços externos de uma organização para uma rede maior, não confiável, geralmente a Internet.
- **O protocolo IPsec** é um padrão de segurança de protocolo de Internet que oferece um mecanismo de segurança de camadas IP baseado em política geral ideal para a fornecer a autenticação host a host. As políticas do IPsec são definidas como tendo regras e configurações de segurança que controlam o fluxo de dados de entrada.
- **Os nós da VPN (rede virtual privada)** em uma rede pública, como a Internet, se comunicam usando a tecnologia de criptografia para que as mensagensestejam as seguras e não sejam interceptadas ou compreendidas por usuários não autorizados, como se os nós estivessem conectados por linhas particulares.



AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/network/dd420463.aspx**

Compreender a segurança do protocolo

SITUAÇÃO: Desde que Todd Rowe, o administrador da rede no Graphic Design Institute, implementou medidas de segurança mais fortes para proteger os dados dos alunos, o número de vazamentos relatados caiu para zero! A administração está satisfeita, mas Todd sabe que é uma batalha constante manter os dados protegidos contra ataques.

O amigo de Todd, Neil Black, é um especialista nos métodos usados para atacar repositórios de dados particulares. Todd solicitou que Neil fizesse uma apresentação para os funcionários da administração e do escritório sobre a segurança da rede, as medidas de segurança de protocolo, os métodos de ataque e a prevenção. Todd sabe que uma equipe informada é parte da estratégia completa de prevenção e interceptação de ataques.

1. **Que tipo de ataque configura um computador para que ele apareça como outro computador em uma rede confiável usando o endereço IP ou o endereço físico?**
   - **a.** falsificação de identidade
   - **b.** falsificação de computador
   - **c.** ataque de camada de aplicativos
2. **Que protocolo de segurança pode ajudar a proteger os dados para não serem modificados, corrompidos ou acessados sem autorização?**
   - **a.** DNSSEC
   - **b.** IPsec (Segurança de IP)
   - **c.** NetBIOS
3. **Que tipo de ataque envenena uma rede ou computador até o ponto onde o sistema fique inutilizável?**
   - **a.** ataque ao intermediário
   - **b.** ataque a senhas
   - **c.** ataque DOS (de negação de serviço)

dica

Existem várias formas de ataques DOS (de negação de serviço) distribuído que pode impedir que um computador, servidor ou aplicativo funcione.

Respostas

1. Um ataque que configura um computador para aparecer como outro computador em uma rede confiável é:
   a. **falsificação de identidade**
2. O protocolo de segurança que pode ajudar a proteger os dados para que não sejam alterados, danificados ou acessados sem autorização é:
   b. **IPsec (Segurança de IP).** O IPSec pode ser usado não só para a segurança da VPN, mas também com o tráfego de rede local. 80 por cento dos ataques à segurança vêm de dentro da organização. Pressupor que os dados dentro do firewall do perímetro estão seguros é uma suposição perigosa.
3. Um ataque que envenena uma rede ou computador até o ponto onde o sistema fique inutilizável é um:
   c. **ataque DOS (de negação de serviço)**

Detalhes essenciais

- **Falsificação** é o ato de monitorar o tráfego de rede quanto a dados, como senhas ou informações de configuração com texto não criptografado.
- **Falsificação de identidade (falsificação de endereço IP)** ocorre quando o invasor determina e usa um endereço IP de uma rede, computador ou componente de rede sem ser autorizado a assim proceder.
- **O protocolo IPsec** oferece suporte a recursos, como integridade dos dados no nível da rede, confidencialidade dos dados, autenticação da origem dos dados e proteção contra reprodução. Devido ao IPsec ser integrado à camada da Internet (camada 3), ele proporciona segurança para quase todos os protocolos no conjunto TCP/IP.
- **O DNS (Sistema de Nomes de Domínio)** é um banco de dados hierárquico, distribuído que contém mapeamentos entre nomes e outras informações, como endereços IP. O DNS permite que usuários localizem recursos na rede convertendo nomes legíveis por humanos fáceis, como *www.microsoft.com* para endereços IP aos quais os computadores podem se conectar.

AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/library/cc959354.aspx**
- **http://technet.microsoft.com/en-us/library/ee649205(WS.10).aspx**

4

Noções básicas sobre o software de segurança

NESTE CAPÍTULO

Compreender a proteção do cliente

SITUAÇÃO: Jeff Hay é o administrador de rede da Tailspin Toys. Durante o período de menos vendas de brinquedos, a equipe de tecnologia da Tailspin é mantida ocupada mantendo e atualizando os diversos sistemas em preparação para o pico de muitas vendas do feriado.

Jeff está ansioso para ter este tempo para fazer manutenção de todos os computadores e atualizar o software. Ele está preocupado com os funcionários da empresa instalarem software a partir da Internet. Jeff percebe que o uso de software antivírus de boa reputação pode fazer muito. A rede consiste em uma mistura de Windows XP, Windows 7 e Windows Server 2008 R2.

1. **O que Jeff pode fazer para garantir que os computadores tenham as atualizações de segurança mais recentes?**
   - **a.** implementar o Windows Software Update Services para controlar todas as atualizações Microsoft para os sistemas operacionais e qualquer produto da Microsoft em uso
   - **b.** chegar cedo todas as segundas-feiras e executar o Windows Update em cada computador
   - **c.** enviar email para os funcionários da empresa e instruí-los a realizar as atualizações do Windows, durante o horário de almoço
2. **O que Jeff pode fazer para impedir que os funcionários da empresa baixem e instalem software da Internet?**
   - **a.** habilitar o Controle de Conta de Usuário em todos os computadores com Windows 7, além de configurar as políticas de restrição de software
   - **b.** enviar um email com palavras fortes com a Política de Uso da Internet anexa a todos os usuários
   - **c.** desabilitar o acesso à Internet para todos os usuários
3. **Qual o método Jeff deve usar para identificar o software da Internet nas Políticas de Restrição de Software?**
   - **a.** regra de hash
   - **b.** regra de caminho
   - **c.** regra de zona

dica

A regra de hash cria uma soma de verificação de hash baseada no executável. A regra de caminho restringe o software localizado em um determinado caminho.

Respostas

1. Para garantir que os computadores tenham as atualizações de segurança mais recentes, Jeff pode:
   a. **implementar o Windows Software Update Services para controlar todas as atualizações Microsoft para os sistemas operacionais e qualquer produto da Microsoft em uso**
2. Para impedir que os funcionários da empresa baixem e instalem software da Internet, Jeff pode:
   a. **habilitar o Controle de Conta de Usuário em todos os computadores com Windows 7, além de configurar as políticas de restrição de software**
3. Para identificar o software da Internet nas Políticas de Restrição de Software, Jeff pode usar:
   c. **regra de zona**

Detalhes essenciais

- **O antivírus** é um programa de computador que verifica a memória de um computador e o armazenamento em massa para identificar, isolar e eliminar vírus, e também que examina os arquivos de entrada em busca de vírus assim que o computador os recebe.
- **O UAC (Controle de Conta de Usuário)** ajuda a impedir que programas mal-intencionados (malware) danifiquem um computador e ajuda organizações a implantar uma área de trabalho melhor gerenciada. Com o UAC, os aplicativos e as tarefas são sempre executados no contexto de segurança de uma conta não-administrador, a menos que o administrador autorize especificamente o acesso no nível de administrador ao sistema.

AJUDA RÁPIDA

- **http://www.microsoft.com/security_essentials/market.aspx**
- **http://technet.microsoft.com/en-us/library/bb457141.aspx**
- **http://technet.microsoft.com/en-us/library/bb456987.aspx**
- **http://windows.microsoft.com/pt-br/windows7/what-is-user-account-control**

Compreender a proteção de email

SITUAÇÃO: Recentemente, a Coho Winery teve uma série de problemas com spam de email; alguns funcionários até rezaram para identificar o furto de identidade através de tentativas de phishing. John Kane é o administrador de sistemas da Coho Winery e a tarefa de solucionar problemas caiu diretamente em uma mesa. Após pesquisar, ele desenvolveu algumas soluções. John pretende resolver esses problemas implementando várias medidas de segurança e, mais importante, fornecendo algumas instruções muito necessárias para a empresa no que se refere às práticas recomendadas ao usar o email.

1. **O que John pode fazer para ajudar a reduzir a quantidade de spam que chega em seu servidor do Microsoft Exchange?**
   - **a.** no mínimo, habilitar a pesquisa inversa do DNS no servidor virtual SMTP
   - **b.** desabilitar o email na Internet
   - **c.** alterar seu nome de domínio
2. **O que os usuários da Coho devem fazer quando eles recebem um email de uma empresa conhecida com uma solicitação para clicar no link para "verificar as informações da conta"?**
   - **a.** excluir o email
   - **b.** encaminhar para o resto da empresa com um aviso para não clicar no link
   - **c.** clicar no link, porque eles "sabem" que é esta uma mensagem legítima com base no nome da empresa
3. **Além de habilitar as pesquisas inversas do DNS, o que mais John pode fazer para proteger seu servidor Exchange?**
   - **a.** habilitar a Descoberta Automática
   - **b.** adicionar a SPF (Sender Policy Framework)
   - **c.** atualizar o software antivírus

dica

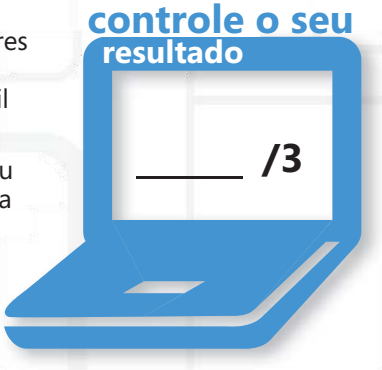
O software antivírus em um servidor de emails não fornece proteção contra spam.

Respostas

1. Para ajudar a reduzir a quantidade de spam que chega em seu servidor do Microsoft Exchange, John pode:
   a. **no mínimo, habilitar a pesquisa inversa do DNS no servidor virtual SMTP.** Configurar o sistema para fazer uma pesquisa inversa do DNS faz uma verificação cruzada do nome do domínio com um registro PTR, que é o endereço IP associado ao nome do domínio. Se o endereço IP não for correspondente ao registro associado ao nome do domínio, ele não será entregue.
2. Quando os usuários recebem um email de uma empresa conhecida com uma solicitação para "verificar as informações da conta", eles devem:
   a. **excluir o email.** As empresas não solicitarão as informações da conta por meio de email atualmente. Os usuários devem ser diligentes quando recebem um email como este. Eles também podem ligar para a empresa para alertá-la sobre a mensagem.
3. Além de habilitar as pesquisas inversas do DNS, John pode:
   b. **adicionar a SPF (Sender Policy Framework).** A SPF permite que o administrador configure o servidor para estabelecer quem tem permissão para enviar emails do seu domínio.

Detalhes essenciais

- **O spam** é email não solicitado, não desejado enviado por alguém com o qual o destinatário não tem qualquer relação pessoal ou comercial.
- **Phishing e pharming** são técnicas usadas para enganar os usuários de computador para que eles revelem informações pessoais ou financeiras.
- Um **registro SPF** é uma extensão do protocolo SMTP que impede que os autores de spam falsifiquem os campos De em mensagens de email verificando se o endereço IP no cabeçalho de SMTP Recebido tem autorização para enviar email pelo domínio do remetente.
- **A falsificação** é a representação de um remetente de email, uma conexão IP ou um domínio quefaz com que uma mensagem de email pareça que foi originada de um remetente diferentedo remetente real da mensagem.



AJUDA RÁPIDA

- **http://technet.microsoft.com/en-us/exchange/dd251269.aspx**
- **http://www.microsoft.com/athome/security/email/phishing/video1.mspx**
- **http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.mspx**

Compreender a proteção do servidor

SITUAÇÃO: Há alguns anos, a HI (Humongous Insurance) reorganizou sua infraestrutura de negócios e de tecnologia. Alfons Parovsky foi recentemente contratado como o administrador de servidor da HI. Os registros sobre as atualizações de segurança são incompletos e ele não deseja que falhas de segurança importantes ocorram durante seu período como administrador. Para ter certeza de que tudo está à altura dos padrões, Alfons decidiu realizar imediatamente uma avaliação da segurança do datacenter. Ele gostaria de garantir que os servidores atendam todos os requisitos de segurança necessários e que estão sendo atualizados regularmente. Alfons também deseja certificar-se de que a HI não tenha nenhuma exposição às redes em seus locais remotos.

1. **Que ferramenta Alfons pode usar para avaliar se os servidores da HI têm qualquer vulnerabilidade relacionada ao sistema operacional e ao software instalado?**
   - **a.** Microsoft Baseline Security Analyzer
   - **b.** Visualizador de Eventos
   - **c.** Monitor de Recursos
2. **Que serviço Alfons pode habilitar para garantir que os servidores estejam recebendo todas as atualizações de software necessárias?**
   - **a.** Windows Backup Service
   - **b.** Serviço de Roteamento e Acesso Remoto
   - **c.** Windows Software Update Service
3. **O que Alfons pode fazer para garantir que o domínio esteja protegido em locais remotos?**
   - **a.** instalar um controlador de domínio Somente Leitura nos locais remotos
   - **b.** remover todos os servidores nos locais remotos e fazer com os que funcionários transfiram arquivos usando email
   - **c.** impor políticas de senha de alta segurança nos locais remotos usando as senhas refinadas

dica

As senhas de alta segurança não reduzem a exposição de um controlador de domínio.

Respostas

1. Para avaliar se os servidores da HI têm qualquer vulnerabilidade relacionada ao sistema operacional e ao software instalado, Alfons pode usar:
   a. **Microsoft Baseline Security Analyzer.** O MBSA é uma ferramenta fácil de usar que pode fornecer comentários e recursos instantâneos para identificar as possíveis vulnerabilidades em servidores e estações de trabalho. Ele analisa o sistema operacional e qualquer software Microsoft instalado.
2. Para garantir que os servidores estejam recebendo todas as atualizações de software necessárias, Alfons pode habilitar:
   c. **Windows Software Update Service.** Alfons pode criar um grupo separado para seus servidores para que ele possa gerenciar de forma seletiva que atualizações serão instaladas e quando.
3. Para garantir que o domínio esteja protegido em locais remotos, ele pode:
   a. **instalar um RODC (controlador de domínio Somente Leitura) nos seus locais remotos.** O RODC (controlador de domínio Somente Leitura) é um novo tipo de controlador de domínio no sistema operacional Windows Server 2008. Com um RODC, as organizações podem implantar facilmente um controlador de domínio em locais onde a segurança física não pode ser garantida.

Detalhes essenciais

- **A atualização dinâmica de DNS** permite que os computadores cliente DNS registrem e atualizem dinamicamente seus registros de recursos com um servidor DNS sempre que ocorrerem alterações.
- **O MBSA (Microsoft Baseline Security Analyzer)** é uma ferramenta projetada para o profissional de TI que ajuda as pequenas e médias empresas a determinarem seu estado de segurança de acordo com as recomendações de segurança da Microsoft e fornece orientação específica para remediação.
- **O WSUS (Windows Server Update Services)** permite que os administradores de tecnologia da informação implantem as atualizações de produtos Microsoft mais recentes nos computadores que executam o sistema operacional Windows.

AJUDA RÁPIDA

- **http://technet.microsoft.com/pt-br/security/cc184923.aspx**
- **http://technet.microsoft.com/pt-br/security/cc185712.aspx**
- **http://technet.microsoft.com/pt-br/library/cc755058(WS.10).aspx**