

Módulo 16: Fundamentos de segurança de rede

Versão original: Cisco Network Academy

Versão modificada: Eduardo Costa

Introdução às redes v7.0 (ITN)



Objetivos do módulo

Título do Módulo: Fundamentos de segurança de rede

Objetivo do Módulo: Configurar switches e routers com recursos de proteção de dispositivo para aumentar a segurança.

Título do Tópico	Objetivo do Tópico
Ameaças à segurança e vulnerabilidades	Explicar a necessidade de medidas básicas de segurança nos dispositivos de rede.
Ataques à rede	Identificar vulnerabilidades de segurança.
Mitigação de ataques à rede	Identificar técnicas gerais de mitigação.
Segurança de dispositivos	Configurar os dispositivos de rede com recursos de proteção de dispositivo para atenuar ameaças à segurança.

16.1 - Ameaças à segurança e vulnerabilidades



Tipos de ameaças

Ataques em uma rede podem ser devastadores e resultar em perda de tempo e dinheiro devido a danos ou roubo de informações ou ativos importantes. Os invasores podem obter acesso a uma rede através de vulnerabilidades de software, ataques de hardware ou adivinhando o nome de utilizador e a password de alguém. Os invasores que obtêm acesso modificando o software ou explorando vulnerabilidades são chamados de agentes de ameaças.

Depois que o agente da ameaça obtém acesso à rede, quatro tipos de ameaças podem surgir.

- Roubo de informações
- Perda e manipulação de dados
- Roubo de identidade
- Interrupção do serviço

Ameaças à segurança e vulnerabilidades

Tipos de vulnerabilidades

Vulnerabilidade é o grau de fraqueza em uma rede ou dispositivo. Algum grau de vulnerabilidade é inerente a routers, switches, desktops, servidores e até dispositivos de segurança. Normalmente, os dispositivos de rede sob ataque são os dispositivos finais (endpoints) tais como servidores e computadores desktop.

Há três tipos principais de vulnerabilidades ou pontos fracos:

- Vulnerabilidades tecnológicas podem incluir fraquezas do Protocolo TCP/IP, Deficiências do Sistema Operativo e Deficiências do Equipamento de Rede.
- As vulnerabilidades de configuração podem incluir contas de usuário inseguras, contas do sistema com passwords fáceis de adivinhar, serviços de Internet mal configurados, configurações por omissão e não seguras e equipamentos de rede mal configurados.
- As vulnerabilidades da Política de Segurança podem incluir a falta de uma política de segurança escrita, política, falta de continuidade de autenticação, controlos de acesso lógicos não aplicados, instalação de software e hardware e alterações que não seguem a política e um plano de recuperação de desastres inexistente.

Todas essas três fontes de vulnerabilidades podem deixar uma rede ou dispositivo aberto a vários ataques, incluindo ataques de código malicioso e ataques de rede.



Ameaças à segurança e vulnerabilidades

Segurança física

Se os recursos de rede puderem ser comprometidos fisicamente, um agente de ameaça poderá negar o uso de recursos de rede. As quatro classes de ameaças físicas são as seguintes:

- **Ameaças de hardware** - Isso inclui danos físicos a servidores, routers, switches, cablagem instalada e estações de trabalho.
- **Ameaças ambientais** – Inclui temperaturas extremas(muito quente ou muito frio) ou humidades extremas(muito humido ou muito seco).
- **Ameaças elétricas** - Isso inclui picos de tensão, tensão de alimentação insuficiente (quedas de energia), energia não condicionada (ruído) e perda total de energia.
- **Ameaças à manutenção** - Isso inclui o uso dos principais componentes elétricos (descarga eletrostática), falta de peças de reposição críticas, cabeamento incorreto e rotulagem inadequada.

Um bom plano de segurança física deve ser criado e implementado para resolver esses problemas.



16.2 Ataques à Rede

Tipos de malware

Malware é a abreviação de software malicioso. É um código ou software projetado especificamente para danificar, interromper, roubar ou infligir ações “ruins” ou ilegítimas em dados, hosts ou redes. Tipos de malware:

- **Vírus** - Um vírus de computador é um tipo de malware que se **propaga inserindo uma cópia de si mesmo noutro programa**. Dissemina-se de um computador para outro, deixando infecções por onde passa.
- **Worms** - os worms de computador são semelhantes aos vírus, pois replicam cópias funcionais deles mesmos e podem causar o mesmo tipo de dano. Ao contrário dos vírus, que necessitam que um ficheiro infectado se espalhe, worms são software independente e não necessitam de um programa hospedeiro ou ajuda humana para se propagarem.
- **Cavalos de Tróia (Trojan Horses)** - É um software prejudicial que parece legítimo. Ao contrário dos vírus e worms, os cavalos de Tróia não se reproduzem infectando outros ficheiros. Eles auto-replicam-se. Os cavalos de Tróia **espalham-se pela interação do utilizador**, tal como abrir um anexo de email ou fazer o download e executar um ficheiro da Internet.

Ataques de reconhecimento

Além de ataques de códigos mal-intencionados, também é possível que as redes se tornem vítimas de vários ataques à rede. Os ataques à rede podem ser classificados em três categorias principais:

- **Ataques de reconhecimento** – a detecção e o mapeamento de sistemas, serviços ou vulnerabilidades
- **Ataques de acesso** – a manipulação não autorizada de dados, do acesso ao sistema ou de privilégios do utilizador
- **Negação de serviço** - A desativação ou corrupção de redes, sistemas ou serviços.

Para ataques de reconhecimento, os atores externos de ameaças podem usar ferramentas da Internet, tais como o **nslookup** e **whois**, para determinar facilmente o espaço de endereçamento IP atribuído a uma determinada empresa ou entidade. Após a determinação do espaço de endereçamento IP, um agente de ameaça pode executar ping nos endereços IP disponíveis ao público para identificar os endereços que estão ativos.

Ataques de acesso

Os ataques de acesso exploram vulnerabilidades conhecidas em serviços de autenticação, serviços de FTP e serviços da Web para obter acesso a contas da Web, bancos de dados confidenciais e outras informações confidenciais.

Os ataques de acesso podem ser classificados em quatro tipos:

- **Ataques de password** - Implementados usando força bruta, cavalo de Tróia e farejadores de pacotes (packet sniffers)
- **Exploração de confiança** - Um agente de ameaça usa privilégios não autorizados para obter acesso a um sistema, possivelmente comprometendo o alvo.
- **Redirecionamento de porta**: - Um agente de ameaça usa um sistema comprometido como base para ataques contra outros alvos. Por exemplo, um ator de ameaça usando SSH (porta 22) para conectar-se a um **host comprometido A**. O **host A é confiável pelo host B** e, portanto, o ator de ameaça pode usar o Telnet (porta 23) para aceder a ele.
- **Man-in-the-middle** - O agente da ameaça está posicionado entre duas entidades legítimas para ler ou modificar os dados que passam entre as duas partes.

Ataques de negação de serviço

Os ataques de negação de serviço (Denial of service - DoS) são a forma de ataque mais divulgada e uma das mais difíceis de eliminar. No entanto, devido à facilidade de implementação e o facto de causarem danos potencialmente significativos, os ataques de negação de serviço merecem atenção especial dos administradores de segurança.

- Os ataques DoS assumem muitas formas. No final, impedem que pessoas autorizadas usem um serviço ao consumir recursos do sistema. Para prevenir ataques (DoS) é importante manter em dia as atualizações de segurança mais recentes para sistemas operativos e aplicações.
- Os ataques de DoS são um grande risco, porque interrompem a comunicação e causam perda significativa de tempo e dinheiro. Esses ataques são relativamente simples de desenvolver, mesmo por um invasor não capacitado.
- Um DDoS é semelhante a um ataque de DoS, mas é originado de várias fontes coordenadas. Por exemplo, um agente de ameaça cria uma rede de hosts infectados, conhecidos como zombies. Uma rede de zombies é chamada de botnet. O ator ameaça usa um programa de comando e controle (CNC) para instruir o botnet de zombies para realizar um ataque DDoS.

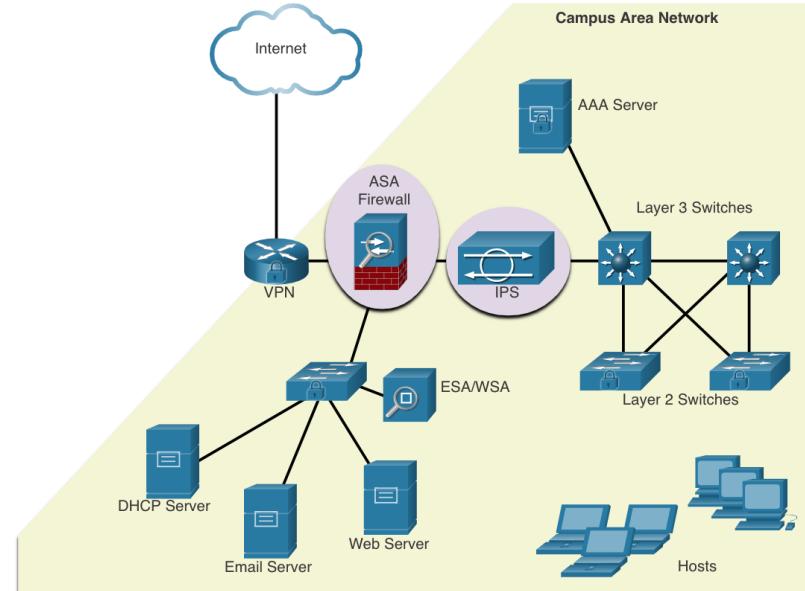
16.3 Mitigações de ataque à rede

A abordagem de defesa em profundidade

Para atenuar os ataques de rede, primeiro devem-se proteger os dispositivos, incluindo routers, switches, servidores e hosts. A maioria das organizações emprega uma abordagem de defesa em profundidade (também conhecida como abordagem em camadas) à segurança. Isso requer uma combinação de dispositivos e serviços de rede trabalhando em conjunto.

Vários dispositivos e serviços de segurança são implementados para proteger os usuários e ativos de uma organização contra ameaças TCP / IP.

- VPN
- Firewall ASA
- IPS
- ESA/WSA
- Servidor AAA



Manter Backups

Fazer backup de configurações e dados dos dispositivos é uma das maneiras mais eficazes de proteção contra a perda de dados. Os backups devem ser realizados regularmente, conforme identificado na política de segurança. Os backups de dados são, normalmente, armazenados noutro local, para proteger os meios de backup, se algo acontecer com a instalação principal.

A tabela mostra considerações de backup e suas descrições.

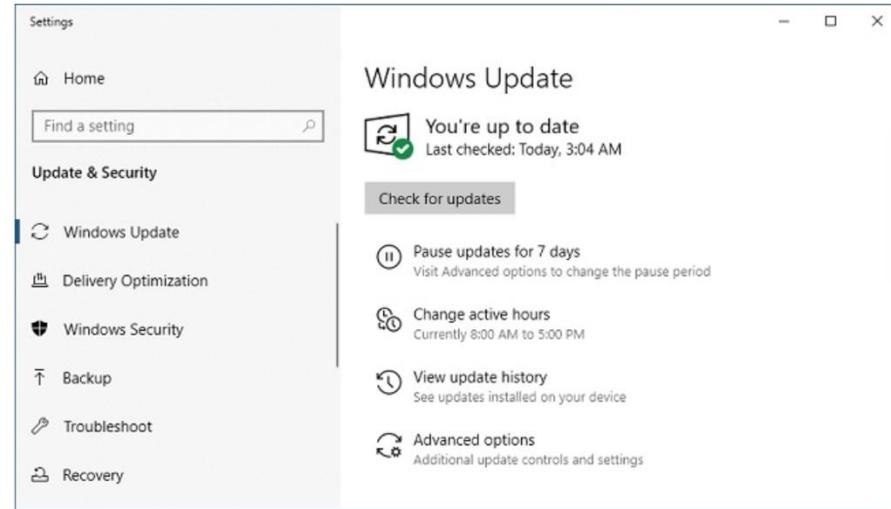
Considerações	Descrição
Frequência	<ul style="list-style-type: none">Realizar backups regularmente, conforme identificado na política de segurança.Backups completos podem ser demorados, portanto, realizar backups mensais ou semanais com backups parciais frequentes de ficheiros alterados.
Armazenamento	<ul style="list-style-type: none">Os backups devem ser sempre validados para garantir a integridade dos dados e validar os procedimentos de restauração dos ficheiros.
Segurança	<ul style="list-style-type: none">Os backups devem ser transportados para um local de armazenamento externo aprovado, em rotação diária, semanal ou mensal, conforme exigido pela política de segurança.
Validação	<ul style="list-style-type: none">Os backups devem ser protegidos usando passwords fortes. A password é necessária para restaurar os dados.

Atenuação de ataques à rede

Upgrades, atualizações e patches

Quando um novo malware é lançado, as empresas precisam manter as suas atuais versões de software antivírus atualizadas.

- O meio mais eficaz de reduzir um ataque de worm é baixar as atualizações de segurança do sistema operativo do fornecedor e corrigir todos os sistemas vulneráveis.
- Uma solução para o gestão de patches críticos de segurança é garantir que todos os sistemas finais baixem atualizações automaticamente.

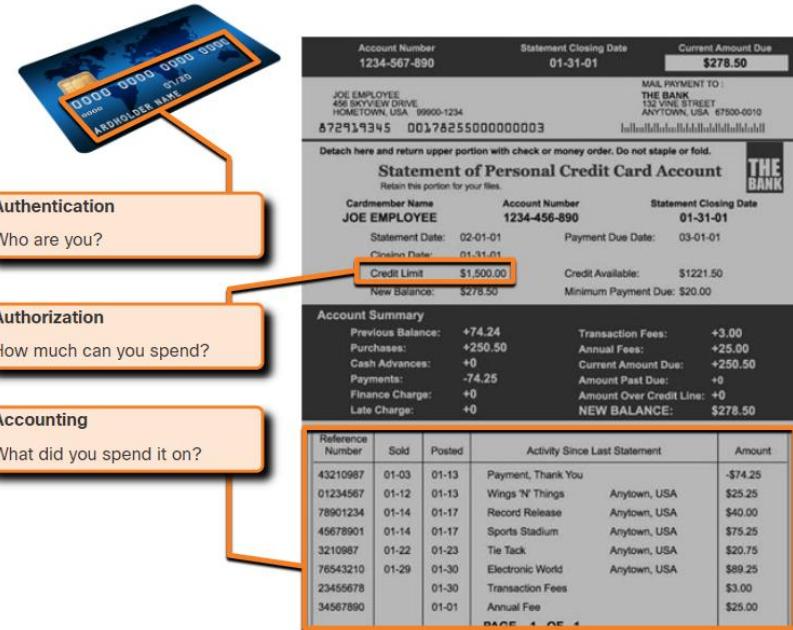


Atenuação de ataques à rede

Autenticação, autorização e accounting

Os serviços de segurança de rede de autenticação, autorização e contabilidade (AAA ou "triplo A") fornecem a estrutura principal para configurar o controlo de acesso nos dispositivos de rede.

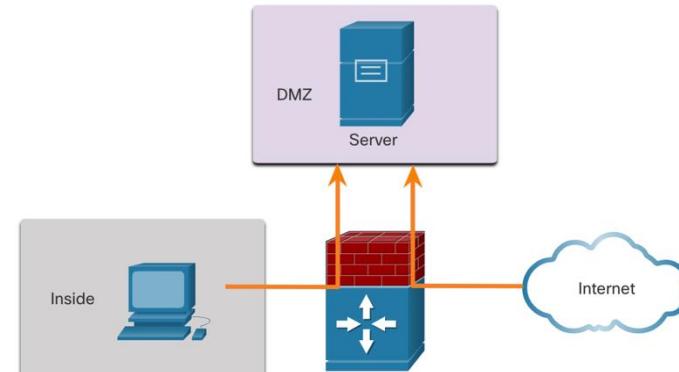
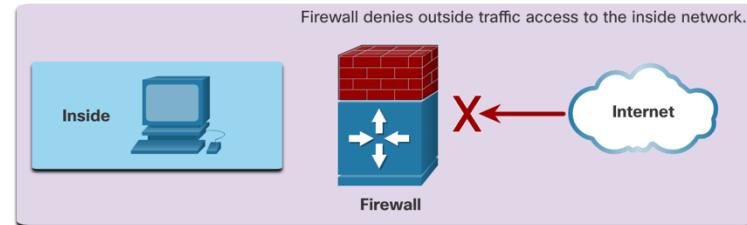
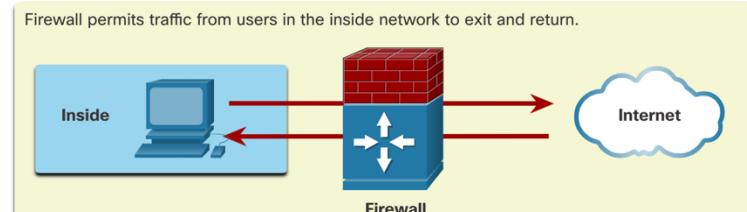
- O AAA é uma maneira de controlar quem tem permissão para aceder a uma rede (autenticar), quais ações podem executar enquanto acedem à rede (autorizar) e fazer um registo do que foi feito enquanto lá estão ligados (contabilidade).
- O conceito do AAA é semelhante ao uso de um cartão de crédito. O cartão de crédito identifica quem pode utilizá-lo, estipula um limite de uso e mantém o controle dos itens comprados pelo utilizador, como mostrado na figura.



Atenuação de ataques à rede Firewalls

As firewalls de rede estão localizadas entre duas ou mais redes, e controlam o tráfego entre elas, além de ajudar a evitar o acesso não autorizado.

Uma firewall poderia permitir que utilizadores externos tenham acesso controlado a serviços específicos. Por exemplo, os servidores acessíveis a utilizadores externos geralmente estão localizados numa rede especial chamada de zona desmilitarizada (DMZ). A DMZ permite que um administrador de rede aplique políticas específicas para hosts conectados a essa rede.



Atenuação de ataques à rede

Firewalls

Os produtos de firewall são fornecidos de várias formas. Esses produtos usam técnicas diferentes para determinar o que será permitido ou negado o acesso a uma rede.

Incluem:

- **Filtragem de pacotes** - Impede ou permite o acesso com base em endereços IP ou MAC
- **Filtragem de aplicações** - Impede ou permite o acesso de determinados tipos de aplicação com base nos números dos portos
- **Filtragem de URL** - impede ou permite o acesso a sites com base em URLs ou palavras-chave específicas
- **Inspeção de pacotes com estado (Stateful packet inspection - SPI)** - Os pacotes recebidos devem ser respostas legítimas às solicitações dos hosts internos. Os pacotes não solicitados são bloqueados, a menos que especificamente permitidos. O SPI também pode incluir o recurso de reconhecer e filtrar tipos específicos de ataques, como negação de serviço (DoS).

Segurança de dispositivos finais (endpoints)

Um endpoint, ou host, é um sistema de computador individual ou um dispositivo que atua como um cliente da rede. Os endpoints comuns são laptops, desktops, servidores, smartphones e tablets.

A segurança de dispositivos de endpoint é uma das tarefas mais desafiadoras de um administrador de rede, porque envolve a natureza humana. Uma empresa deve ter obrigatoriamente as políticas em vigor bem documentadas e os funcionários devem conhecer essas regras.

Os funcionários devem ser treinados para usarem corretamente a rede. As políticas em geral incluem o uso de software antivírus e prevenção contra invasões. Soluções de segurança de endpoints mais abrangentes baseiam-se no controle de acesso à rede.

16.4 Segurança de dispositivos

Segurança do dispositivo Cisco AutoSecure

As configurações de segurança são definidas com os valores por omissão quando um novo sistema operativo é instalado num dispositivo. Na maioria dos casos, esse nível de segurança é inadequado. Para routers Cisco, o recurso Cisco AutoSecure pode ser usado para ajudar a proteger o sistema.

Além disso, existem algumas etapas simples que podem ser executadas e que se aplicam à maioria dos sistemas:

- Nomes de utilizador e passwords por omissão devem ser trocados imediatamente.
- O acesso aos recursos do sistema deve ser restrito apenas aos indivíduos que estão autorizados a usá-los.
- Todos os serviços e aplicações desnecessários devem ser desativados e desinstalados assim que possível.
- Em geral, dispositivos vindos de fábrica ficaram em depósito por um período e não têm os patches mais atuais instalados. É importante atualizar todos os softwares e instalar todos os patches de segurança antes da implementação.



Passwords

É importante usar passwords fortes para proteger dispositivos de rede. As diretrizes padrão a serem seguidas são:

- Use uma password de pelo menos 8 caracteres, preferencialmente 10 ou mais caracteres.
- Use passwords complexas. Inclua uma combinação de letras maiúsculas e minúsculas, números, símbolos e espaços, se permitido.
- Evite as passwords com base em repetição, palavras comuns de dicionário, sequências de letras ou números, nomes de utilizador, nomes de parentes ou de animais de estimação, informações biográficas, como datas de nascimento, números de identificação, nomes de antepassados ou outras informações facilmente identificáveis.
- Deliberadamente, soletre errado uma password. Por exemplo, Smith = Smyth = 5mYth ou Security = 5ecur1ty.
- Altere as passwords periodicamente. Se uma password é inadvertidamente comprometida, a janela de oportunidade para que o invasor a use é limitada.
- Não anote as passwords e muito menos as deixe em locais óbvios, como em sua mesa ou no monitor.

Nos routers Cisco, os espaços à esquerda são ignorados nas passwords, mas os espaços após o primeiro caractere não são ignorados. Portanto, um método para criar uma password forte é utilizar a barra de espaço e criar uma frase feita de muitas palavras. Isso se chama uma frase secreta (passphrase). Uma frase secreta é geralmente mais fácil de lembrar do que uma senha simples. Também é maior e mais difícil de ser descoberta.

Segurança de Senha Adicional

Existem várias etapas que podem ser tomadas para ajudar a garantir que as passwords permaneçam secretas num router ou switch Cisco, incluindo estas:

- Encripte todas as passwords de texto sem formatação com o comando **service password-encryption**.
- Defina um comprimento mínimo aceitável de password com o comando **security passwords min-length** .
- Impedir ataques de adivinhação de password de força bruta com o comando **login block-for # attempts # within #** .
- Desative um acesso de modo EXEC privilegiado inativo após um período especificado de tempo com o comando **exec-timeout** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
password 7 03095A0F034F
exec-timeout 5 30
login
Router#
```

Segurança de dispositivos

Ativação do SSH

É possível configurar um dispositivo Cisco para suportar SSH usando as seis etapas a seguir:

1. **Configure um nome de host de dispositivo exclusivo.** Um dispositivo deve ter um nome de host exclusivo diferente do por omissão.
2. **Configure o nome do domínio IP.** Configure o nome de domínio IP da rede usando o comando **ip-domain name** no modo de configuração global.
3. **Gere uma chave para encriptar o tráfego SSH.** O SSH encripta o tráfego entre a origem e o destino. No entanto, para fazer isso, uma chave de autenticação exclusiva deve ser gerada usando o comando de configuração global **crypto key generate rsa general-keys módulos bits**. O módulo *bits* determina o tamanho da chave e pode ser configurado de 360 bits a 2048 bits. Quanto maior o valor de bit, mais segura a chave. No entanto, valores de bits maiores também levam mais tempo para encriptar e desencriptar informações. O tamanho mínimo recomendado do módulo é 1024 bits.
4. **Verifique ou crie um login na base de dados local.** Crie um nome de utilizador (login) na base de dados local usando o comando de configuração global **username**.
5. **Os utilizadores autenticam-se na base de dados local.** Use o comando no modo de configuração de linha específica **login local** para autenticar-se na linha vty usando a base de dados local.
6. **Habilite a entrada vty para sessões SSH.** Por omissão, nenhuma sessão de entrada é permitida nas linhas vty. Podem especificar-se vários protocolos de entrada, incluindo Telnet e SSH, usando o comando **transport input [ssh | telnet]**.

Desativar serviços não utilizados

Os routers e switches Cisco começam com uma lista de serviços ativos que podem ou não ser necessários na sua rede. Desative todos os serviços não utilizados para preservar os recursos do sistema, como ciclos de CPU e RAM, e impedir que os atores ameaçadores explorem esses serviços.

- O tipo de serviços que estão ativados por omissão varia dependendo da versão do IOS. Por exemplo, o IOS-XE normalmente terá apenas portas HTTPS e DHCP abertas. Você pode verificar isso com o comando **show ip ports all** .
- As versões do IOS anteriores ao IOS-XE usam o comando **show control-plane host open-ports** .

16.5 - Sumário

O que aprendi neste módulo?

- Depois de um agente ameaça obter acesso à rede, quatro tipos de ameaças podem surgir: roubo de informações, perda e manipulação de dados, roubo de identidade e interrupção do serviço.
- Há três vulnerabilidades principais: tecnológica, de configuração e de política de segurança.
- As quatro classes de ameaças físicas são: hardware, ambiental, elétrica e manutenção.
- Malware é a abreviação de software malicioso. É um código ou software projetado especificamente para danificar, interromper, roubar ou infligir ações “ruins” ou ilegítimas em dados, hosts ou redes. Vírus, worms e cavalos de Tróia são tipos de malware.
- Os ataques à rede podem ser classificados em três categorias principais: reconhecimento, acesso e negação de serviço.
- Para atenuar os ataques de rede, primeiro você deve proteger dispositivos, incluindo routers, switches, servidores e hosts. A maioria das organizações emprega uma abordagem de defesa em profundidade à segurança. Isso requer uma combinação de dispositivos e serviços de rede trabalhando em conjunto.
- Vários dispositivos e serviços de segurança são implementados para proteger os utilizadores e ativos de uma organização contra ameaças TCP / IP: VPN, firewall ASA, IPS, ESA / WSA e servidor AAA.



O que aprendi neste módulo? (continuação)

- Os dispositivos de infraestrutura devem ter backups dos ficheiros de configuração e imagens IOS num servidor de arquivos FTP ou similar. Se o computador ou um hardware de router falhar, os dados ou a configuração podem ser restaurados usando a cópia de backup.
- O meio mais eficaz de reduzir um ataque de worm é descarregar as atualizações de segurança do sistema operativo do fornecedor e corrigir todos os sistemas vulneráveis. Para gerir patches críticos de segurança, devemos garantir que todos os sistemas finais descarreguem as atualizações automaticamente.
- O AAA é uma forma de controlar quem acede uma rede (autenticar), o que pode fazer enquanto permanece nela (autorizar) e que ações realiza ao aceder a rede (accounting).
- As firewalls de rede estão localizadas entre duas ou mais redes, e controlam o tráfego entre elas, além de ajudar a evitar o acesso não autorizado.
- Proteger dispositivos finais é fundamental para a segurança da rede. Uma empresa deve ter políticas bem documentadas em vigor, que podem incluir o uso de software antivírus e prevenção contra intrusões no host. Soluções de segurança de endpoints mais abrangentes baseiam-se no controle de acesso à rede.

O que aprendi neste módulo? (continuação)

- Para routers Cisco, o Cisco AutoSecure pode ser usado para ajudar a proteger o sistema. Para a maioria dos SOs os nomes de utilizador e passwords por omissão devem ser alterados imediatamente, o acesso aos recursos do sistema deve ser restrito apenas aos indivíduos autorizados a usar esses recursos, e quaisquer serviços e aplicativos desnecessários devem ser desativados e desinstalados quando possível.
- É importante usar passwords fortes para proteger dispositivos de rede. Uma frase secreta (passphrase) é geralmente mais fácil de lembrar do que uma senha simples. Também é maior e mais difícil de ser descoberta.
- Nos routers e switches, encripte todas as passwords em texto simples, definindo um comprimento mínimo aceitável de senha, dissuadir ataques de adivinhação de password de força bruta e desabilite um acesso em modo EXEC privilegiado inativo após um período especificado.
- Configure dispositivos apropriados para suportar SSH e desative serviços não utilizados.