Conceitos básicos de Segurança de Redes

---

1. Introdução

Proteger a infraestrutura de rede inclui proteger fisicamente os dispositivos que fornecem conectividade de rede e impedir o acesso não autorizado ao software de gerenciamento que reside nelas. Também é necessário proteger as informações contidas nos pacotes transmitidos pela rede e as informações armazenadas nos dispositivos conectados à rede.

Existem três requisitos principais para realizar tal tarefa.

- **Confidencialidade:** Confidencialidade dos dados significa que apenas os destinatários pretendidos e autorizados podem acessar e ler os dados.
- **Integridade:** A integridade dos dados garante aos usuários que as informações não foram alteradas na transmissão da origem até o destino.
- **Disponibilidade:** A disponibilidade de dados garante aos usuários acesso oportuno e confiável aos serviços de dados para usuários autorizados.

A segurança da rede é parte integrante da rede de computadores, independentemente da rede estar localizada em uma casa com uma única conexão à Internet ou se é uma corporação com milhares de usuários. Os dados devem ser protegidos e ao mesmo tempo, ter uma qualidade de serviço que os usuários esperam da rede.

Existem várias ameaças externas comuns às redes.

- **Vírus, worms e cavalos de Tróia:** Estes contém software ou código malicioso em execução no dispositivo do usuário.
- **Spyware e Adware:** Estes são tipos de software que são instalados no dispositivo de um usuário. O software, em seguida, coleta secretamente informações sobre o usuário.
- **Ataques de dia zero:** Também chamados de ataques de hora zero, ocorrem no primeiro dia em que a vulnerabilidade se torna conhecida.
- **Ataques de ator de ameaça:** Uma pessoa mal intencionada ataca dispositivos de usuários ou recursos de rede.
- **Ataques de negação de serviço:** Estes ataques atrasam ou até mesmo travam aplicativos e processos em um dispositivo de rede
- **Interceptação de dados e roubo:** Estes ataques capturam informações privadas da rede de uma organização.
- **Roubo de identidade:** Esse ataque rouba as credenciais de login de um usuário para acessar informações privadas.

Não existe solução única para proteger a rede da variedade de ameaças existentes. A segurança deve ser implementada em várias camadas, com uso de mais de uma solução. Uma implementação de segurança para redes domésticas é bem básica, geralmente utilizando-se apenas de antivírus, antispyware e firewall, ao contrário de empresas e organizações, que além disso, utilizam-se de sistemas dedicados, ACLs, IPS e VPNs.

2. Antivírus e Antispyware
Estes serviços de aplicação ajudam a proteger os dispositivos finais contra a infecção por software malicioso.

3. Filtragem por Firewall
A filtragem por firewall bloqueia o acesso não autorizado dentro e fora da rede. Isso pode incluir um sistema de firewall baseado em host que impede o acesso não autorizado ao dispositivo final ou um serviço básico de filtragem no roteador doméstico para impedir o acesso não autorizado.

4. Sistemas de Firewall dedicados
Fornecem recursos de firewall mais avançados que podem filtrar grandes quantidades de tráfego com mais granularidade.

5. Lista de Controles de Acesso (ACLs)
Filtram ainda mais o acesso e o encaminhamento de tráfego com base em endereços e aplicativos IP.

6. Sistemas de Prevenção de Intrusão (IPS)
Identificam ameaças de rápida disseminação, como ataques de dia zero.

7. Redes Privadas Virtuais (VPN)
Fornece acesso seguro a uma organização para trabalhadores remotos.

Existem três principais vulnerabilidades ou fraquezas:
- Política tecnológica
- Configuração
- Segurança

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.

8. Vulnerabilidades Tecnológicas

Vulnerabilidade	Descrição
Ponto fraco do protocolo TCP/IP	Protocolo de Transferência de Hipertexto (HTTP), Protocolo de Transferência de Arquivo (FTP) e ICMP (Internet Control Message Protocol) são inerentemente inseguros Protocolo de Gerenciamento de Rede Simples (SNMP) e Protocolo de Transferência de Correio Simples (SMTP) estão relacionados à estrutura inerentemente inseguros em que o TCP foi projetado

Pontos fracos dos sistemas operacionais	Cada sistema operacional tem problemas de segurança, o que deve ser tratado UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8 Eles estão documentados na Equipe de resposta a emergências de computadores (CERT) arquivados em https://www.cert.org
Pontos fracos dos equipamentos de rede	Vários tipos de equipamentos de rede, como roteadores, firewalls e têm deficiências de segurança que devem ser reconhecidas e protegidas contra. Suas fraquezas incluem proteção por senha, falta de autenticação, protocolos de roteamento e falhas de firewall

9. Vulnerabilidades de Configuração

Vulnerabilidade	Descrição
Contas de usuário não protegidas	As informações da conta de usuário podem ser transmitidas de forma expondo nomes de usuário e senhas a atores ameaçadores
Contas do sistema com senhas facilmente descobertas	Esse problema comum é o resultado de senhas de usuário mal criadas
Serviços de Internet mal configurados	Ativar JavaScript em navegadores da Web permite ataques por meio de JavaScript controlados por atores ameaçadores ao acessar sites não confiáveis. Outras fontes potenciais de deficiências incluem terminal mal configurado, serviços FTP ou servidores Web (por exemplo, Microsoft Internet Information Service (IIS) e Apache HTTP Server)
Configurações padrão não seguras nos produtos	Muitos produtos têm configurações padrão que criam ou habilitam furos na segurança
Equipamento de rede configurado incorretamente	As configurações incorretas do próprio equipamento podem causar problemas significativos de segurança. Por exemplo, listas de acesso mal configuradas,protocolos de roteamento ou as cadeias de caracteres da comunidade SNMP podem criar ou habilitar falhas na segurança

10. Vulnerabilidade de Política

Vulnerabilidade	Descrição
Falta de uma política de segurança por escrito	Uma política de segurança não pode ser aplicada ou aplicada de forma consistente se não for escrita
Política	Batalhas políticas e guerras territoriais podem dificultar a implementação de uma política de segurança consistente

Falta de continuidade da autenticação	Senhas mal escolhidas, facilmente quebradas ou padrão podem permitir acesso não autorizado à rede
Controles de acesso lógico não aplicados	O monitoramento e auditoria inadequados permitem ataques e uso não autorizado a continuar, desperdiçando recursos da empresa. Isso pode resultar em ação judicial ou rescisão contra técnicos de TI, gerenciamento de TI ou até mesmo empresa liderança que permite que essas condições inseguras persistam
A instalação e as alterações de hardware e de software não seguem a política	Alterações não autorizadas na topologia de rede ou instalação de aplicativo não aprovado pode criar ou habilitar falhas na segurança
O plano de recuperação de desastres não existe	A falta de um plano de recuperação de desastres permite o caos, pânico e confusão ocorra quando acontecer um desastre natural ou um ator ameaçador ataca o empreendimento

Uma área vulnerável da rede igualmente importante a considerar é a segurança física dos dispositivos. Se os recursos de rede puderem ser fisicamente comprometidos, um agente de ameaça poderá negar o uso de recursos de rede.

As quatro classes de ameaças físicas são as seguintes:

- **Ameaça de hardware:** Isso inclui danos físicos a servidores, roteadores, switches, instalações de cabeamento e estações de trabalho
- **Ameaças ambientais:** Isso inclui extremos de temperatura (muito quente ou muito frio) ou extremos de umidade (muito úmido ou muito seco)
- **Ameaças elétricas:** Isso inclui picos de tensão, tensão de alimentação insuficiente (quedas de energia), energia não condicionada (ruída) 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

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 descoberta e o mapeamento de sistemas, serviços ou vulnerabilidades
- **Ataques de acesso:** A manipulação não autorizada de dados, acesso ao sistema ou privilégios do usuário
- **Negação de serviço:** A desativação ou corrupção de redes, sistemas ou serviços

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. Um ataque de acesso permite que indivíduos obtenham acesso não autorizado a informações que eles não têm o direito de visualizar. Os ataques de acesso podem ser classificados em quatro tipos: ataques de senha, exploração de confiança, redirecionamento de portas e o intermediário.

11. Ataques de senha

Os atores de ameaças podem implementar ataques de senha usando vários métodos diferentes como ataques de força bruta, ataques de cavalo de tróia e até sniffers de pacotes.

12. Exploração de confiança

Em um ataque de exploração de confiança, um agente de ameaça usa privilégios não autorizados para obter acesso a um sistema, possivelmente comprometendo o alvo.

13. Redirecionamento de porta

Em um ataque de redirecionamento de porta, um agente de ameaça usa um sistema comprometido como base para ataques contra outros alvos.

14. Ataques intermediários (MitM)

Em um ataque Homem no meio, o agente da ameaça é posicionado entre duas entidades legítimas para ler ou modificar os dados que passam entre as duas partes.

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

Os ataques DoS assumem muitas formas. E, por fim, impedem que pessoas autorizadas usem um serviço ao consumir recursos do sistema. Para prevenir ataques (DoS) é importante manter em dia as mais recentes atualizações de segurança para sistemas operacionais e aplicações.

15. Ataques DoS

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 conduzir, mesmo por um invasor não capacitado.

16. Ataques DDoS

Um DDoS é semelhante a um ataque de DoS, mas é originado de várias fontes coordenadas.

Para atenuar os ataques de rede, primeiro você deve proteger dispositivos, incluindo roteadores, switches, servidores e hosts. A maioria das organizações emprega uma abordagem de defesa profunda (também conhecida como abordagem em camadas) à segurança.

Vários dispositivos e serviços de segurança são implementados para proteger os usuários e ativos de uma organização contra ameaças TCP/IP, como VPN, ASA firewalls, IPS, ESA/WSA, servidores AAA e outros.

Fazer backup de configurações e dados do dispositivo é uma das maneiras mais eficazes de se proteger contra a perda de dados. O backup de dados armazena uma cópia das informações de um computador em uma mídia removível de backup que pode ser guardada em um local seguro.

Os backups devem ser realizados regularmente, conforme identificado na política de segurança. Os backups de dados são, normalmente, armazenados em outro local, para proteger a mídia de backup, se algo acontecer com a instalação principal. Hosts Windows têm um utilitário de backup e restauração. É importante que os usuários façam backup de seus dados em outra unidade ou em um provedor de armazenamento baseado em nuvem.

A tabela abaixo mostra considerações de backup e suas descrições.

Considerações	Descrição
Frequência	Realizar backups regularmente, conforme identificado na segurança política de TI da empresa Backups completos podem ser demorados, portanto, executar mensalmente ou backups semanais com backups parciais frequentes de arquivos alterados
Armazenamento	Valide sempre os backups para garantir a integridade dos dados e validar os procedimentos de restauração de arquivos
Segurança	Os backups devem ser transportados para um armazenamento externo, aprovado, em uma rotação diária, semanal ou mensal, conforme exigido pela política de segurança
Validação	Os backups devem ser protegidos usando senhas fortes. A senha é necessária para restaurar os dados

Manter-se atualizado com os desenvolvimentos mais recentes pode levar a uma defesa mais eficaz contra ataques à rede. Quando um novo malware é lançado, as empresas precisam manter as suas atuais versões de software antivírus atualizadas.

A administração de vários sistemas envolve a criação de uma imagem de software padrão (sistema operacional e aplicações com autorização para uso nos sistemas do cliente) que é implantada em sistemas novos ou atualizados. No entanto, os requisitos de segurança são alterados e os sistemas já implantados podem precisar ter patches de segurança atualizados instalados.

Uma solução para o gerenciamento de patches críticos de segurança é garantir que todos os sistemas finais baixem atualizações automaticamente.

É importante usar senhas fortes para proteger os dispositivos de rede. Estas são as diretrizes padrão a serem seguidas:

- Use um comprimentos e senha de pelo menos oito caracteres, de preferência 10 ou mais caracteres. Uma senha mais longa é uma senha mais segura
- Use senhas complexas. Inclua uma combinação de letras maiúsculas e minúsculas, números, símbolos e espaços, se permitido
- Evite as senhas com base em repetição, palavras comuns de dicionário, sequências de letras ou números, nomes de usuário, 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 senha.
- Altere as senhas periodicamente. Se uma senha for inconscientemente comprometida, a janela de oportunidade para o agente de ameaças usar a senha é limitada
- Não anote as senhas e muito menos as deixe em locais óbvios, como em sua mesa ou no monitor.

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

Senhas fortes são úteis apenas se forem secretas. Existem várias etapas que podem ser tomadas para ajudar a garantir que as senhas permaneçam secretas em um roteador e switch Cisco, incluindo estes:

- Criptografando todas as senhas de texto sem formatação
- Definindo um tamanho mínimo aceitável de senha
- Detecção de ataques de adivinhação de senha de força bruta
- Desativando um acesso de modo EXEC privilegiado inativo após um período específico.