Módulo 4 - Aulas 1 e 2

Módulo 4: Controles de acesso

Aula 1: Gerenciamento de identidade e acesso

Objetivos

- [x] Compreender os fundamentos do gerenciamento de identidade e acesso.
- [x] Explorar os diferentes fatores e atributos de autenticação.
- [x] Analisar o design de autenticação e multifator de autenticação.

Conceitos

- [x] Fatores de Autenticação: Knowledge, Ownership e Biometric Factor.
- [x] Atributos de Autenticação: Local, Comportamental, Baseado em Conhecidos.
- [x] Design de Autenticação e Multifator de Autenticação.

Introdução

Sejam todos muito bem-vindos à aula de Gerenciamento de Identidade e Acesso. Nesta aula exploraremos conceitos essenciais que formam a base do gerenciamento de identidade e acesso a sistemas. Vamos desvendar os processos de identificação, autenticação, autorização e accounting (IAAA) e buscaremos entender como esses elementos interagem para garantir a integridade e a segurança dos sistemas digitais que permeiam nosso cotidiano.

Nosso foco será direcionado para os fatores de autenticação, onde abordaremos o knowledge factor, ownership factor e biometric factor. Estes, por sua vez, representam importantes elementos do gerenciamento de identidade, oferecendo diferentes abordagens para a validação da identidade digital.

Veremos também os atributos de autenticação, explorando não apenas o local e comportamental, mas também a autenticação baseada em algo que você exibe e em alguém que você conhece. Compreenderemos como esses atributos adicionam camadas de segurança à autenticação, adaptando-se aos desafios dinâmicos do cenário cibernético.

Além disso, estudaremos o conceito de design de autenticação e exploraremos usos práticos. Será apresentado o conceito de multifator de autenticação, bem como seu papel na mitigação de riscos e proteção contra ameaças cibernéticas cada vez mais sofisticadas.

Conceitos em Projetos de Autenticação

A autenticação forte é a primeira linha de defesa na batalha para proteger os recursos da rede. Mas a autenticação não é um processo único. Existem diferentes métodos e mecanismos, alguns dos quais podem ser combinados para formar soluções mais eficazes. O profissional de segurança de rede deve familiarizar-se com as tecnologias de identificação e autenticação. Isto pode ajudá-lo a selecionar, implementar e oferecer suporte àquelas que são apropriadas para o seu ambiente.

Um projeto de autenticação refere-se à criação e implementação de um sistema para verificar e validar a identidade de usuários antes de conceder acesso a determinados recursos, sistemas ou informações. A meta é criar sistemas seguros e eficientes capazes de proteger contra acessos não autorizados, garantindo a integridade e confidencialidade das informações em ambientes digitais.

Gerenciamento de identidade e acesso

O gerenciamento de identidade e acesso (IAM, do inglês Identity and Access Management) é uma disciplina de segurança da informação que se concentra em garantir a segurança, a eficiência e a conformidade nas interações de usuários com

sistemas digitais. Este processo abrange desde a criação e manutenção de identidades digitais até o controle dos privilégios de acesso associados a essas identidades.

Um sistema de controle de acesso é o conjunto de controles técnicos que governam como os sujeitos podem interagir com os objetos. Os sujeitos, neste sentido, são usuários, dispositivos ou processos de software ou qualquer outra coisa que possa solicitar e ter acesso a um recurso. Os objetos são os recursos. Podem ser redes, servidores, bancos de dados, arquivos e assim por diante. Um sistema de gerenciamento de identidade e acesso (IAM) pode ser descrito em termos de quatro processos principais:

1. **Identificação**: A identificação refere-se ao processo de estabelecer a presença digital única de um usuário em um sistema. Significa atribuir uma identidade única, geralmente por meio de um nome de usuário ou ID exclusivo. Envolve a criação de uma conta ou ID que represente o usuário, dispositivo ou processo na rede.

Importância: A identificação é o primeiro passo para a construção de perfis digitais, permitindo que o sistema reconheça e diferencie usuários individuais.

2. **Autenticação**: A autenticação é o processo de verificar se a identidade apresentada é legítima. Isso geralmente é realizado por meio de credenciais, como senhas, tokens ou métodos biométricos. É a prova de que um sujeito é quem afirma ser quando tenta acessar o recurso.

Importância: A autenticação assegura que apenas usuários autorizados tenham acesso aos recursos do sistema, fortalecendo a segurança.

3. **Autorização**: A autorização determina as permissões e privilégios concedidos a um usuário autenticado. Ela estabelece quais direitos os sujeitos devem ter sobre cada recurso e fazer cumprir esses direitos. Baseia-se nas políticas de segurança e no perfil do usuário.

Importância: A autorização garante que os usuários tenham acesso apenas aos recursos e informações relevantes às suas funções e responsabilidades.

4. **Contabilidade**: Accounting, ou contabilidade, refere-se ao registro e monitoramento das atividades do usuário. Rastrear o uso autorizado de um recurso ou o uso de direitos por um sujeito e alertar quando o uso não autorizado for detectado ou tentado. Isso cria uma trilha de auditoria que pode ser usada para análise de segurança e conformidade.

Importância: O accounting reforça a responsabilidade e fornece uma visão abrangente das ações realizadas no sistema, contribuindo para a detecção precoce de atividades suspeitas.

O IAM permite definir os atributos que compõem a identidade de uma entidade, como finalidade, função, habilitação de segurança e muito mais. Posteriormente, esses atributos permitem que os sistemas de gerenciamento de acesso tomem decisões informadas sobre conceder ou negar acesso a uma entidade e, se concedido, decidir o que a entidade tem autorização para fazer. Por exemplo, um funcionário individual pode ter sua identidade em um sistema IAM. A função do funcionário na empresa influencia sua identidade, como em que departamento o funcionário está e se ele é o gerente.

Os servidores e protocolos que implementam essas funções são chamados de autenticação, autorização e contabilidade (AAA). O uso do IAM para descrever processos e fluxos de trabalho empresariais está se tornando cada vez mais predominante à medida que a importância da fase de identificação é mais reconhecida.

Gerenciamento de Identidades.

Fatores de autenticação

Os fatores de autenticação referem-se aos métodos e elementos utilizados para verificar a identidade de um usuário antes de conceder acesso a sistemas, dispositivos ou informações sensíveis. Esses fatores oferecem diferentes abordagens para assegurar que a pessoa ou entidade que está se autenticando é realmente quem afirma ser. Cada um deles desempenha um papel essencial na criação de sistemas de autenticação robustos, e muitas implementações bem-sucedidas combinam vários desses elementos para criar uma defesa multicamadas contra acessos não autorizados. Existem muitas tecnologias para definir credenciais e podem ser categorizadas como fatores, como mostrado a seguir:

1. **Autenticação baseada no que você conhece (Knowledge Factor)**: A autenticação baseada no Knowledge Factor envolve o uso de informações que o usuário conhece para validar sua identidade. Isso comumente inclui senhas, personal identification numbers (PIN) ou respostas a perguntas específicas. Uma passphrase é uma senha mais longa composta por várias palavras. Ela tem a vantagem de ser mais segura e fácil de lembrar. No entanto, desafios incluem a necessidade de criar senhas robustas e a gestão adequada para evitar vulnerabilidades.

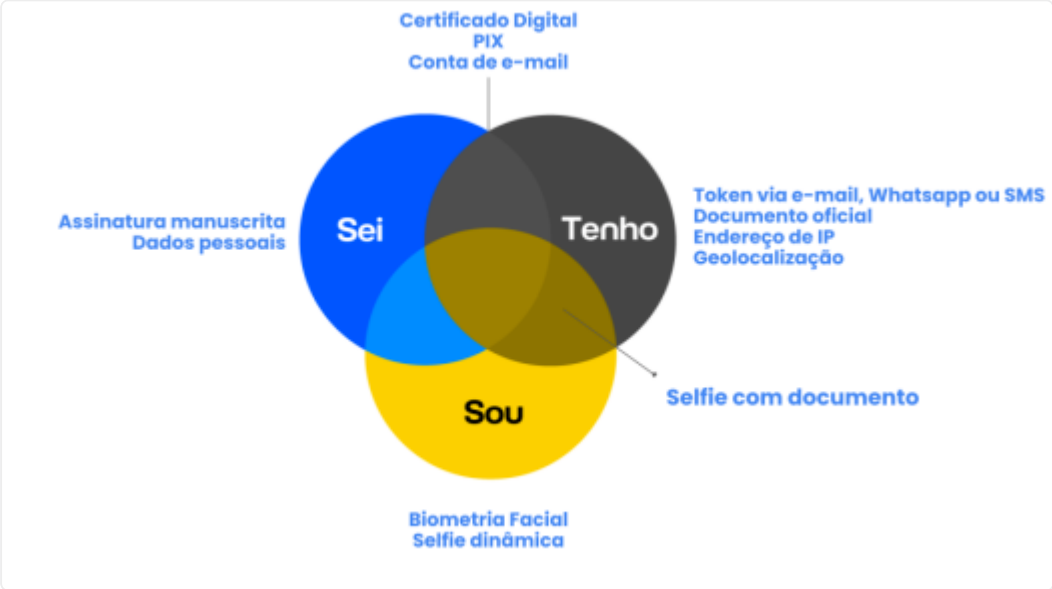
Exemplos: Senhas de contas online, códigos PIN de cartões bancários ou respostas a perguntas de segurança, como o nome do primeiro animal de estimação.

2. **Autenticação baseada em algo que você tem (Ownership Factor)**: A autenticação baseada no Ownership Factor requer que o usuário possua um objeto específico para confirmar sua identidade. Isso pode incluir cartões inteligentes, tokens de segurança ou dispositivos físicos. O Ownership Factor acrescenta uma camada extra de segurança, uma vez que um invasor teria que possuir fisicamente o objeto para obter acesso. Isso é comum em ambientes corporativos, onde cartões de acesso ou tokens geram códigos temporários para autenticação.

Exemplos: Cartões de acesso magnético, tokens de autenticação por tempo limitado ou chaves de hardware.

3. **Autenticação baseada no que você é ou faz (Biometric Factor)**: A autenticação baseada no Biometric Factor utiliza características únicas do corpo ou comportamentos individuais para confirmar a identidade. Isso engloba impressões digitais, reconhecimento facial, íris, voz e até mesmo padrões de digitação. O Biometric Factor oferece uma abordagem altamente personalizada, uma vez que cada indivíduo possui características únicas. No entanto, desafios incluem a necessidade de sistemas robustos para lidar com avarias ou falsificações biométricas.

Exemplos: Desbloqueio de smartphones por reconhecimento facial, leitores de impressões digitais para acesso a edifícios ou autenticação por voz em sistemas de segurança.



Fatores de Autenticação.

Desenho de autenticação

O desenho de autenticação refere-se à criação e implementação de estratégias, políticas, processos e sistemas que verificam e validam a identidade de usuários antes de conceder acesso a meios ou informações. Este design abrange uma variedade de métodos e tecnologias para assegurar que apenas usuários autorizados possam interagir com recursos específicos. São várias as tecnologias disponíveis, mas o design de autenticação deve utilizar a mais adequada para cada caso de uso. A seleção de uma tecnologia precisa atender aos requisitos de confidencialidade, integridade e disponibilidade:

- **Confidencialidade**: Em termos de autenticação, é crítica porque, se as credenciais da conta vazarem, os agentes de ameaça podem se passar pelo titular da conta e agir no sistema com quaisquer direitos que possuam.
- **Integridade**: Significa que o mecanismo de autenticação é confiável e não é fácil para os agentes de ameaça contornarem ou enganarem com credenciais falsas.
- **Disponibilidade**: Significa que o tempo necessário para autenticação não impede os fluxos de trabalho e é bastante fácil para os usuários operarem.

Aplicação Prática:

- Políticas de Senhas e Senhas Fortes: A implementação de senhas robustas, combinada com políticas efetivas de gerenciamento de senhas, é uma prática comum no design de autenticação. Senhas complexas, autenticação em dois fatores e expiração regular de senhas são elementos-chave.
- Biometria: Sistemas que utilizam características únicas do corpo, como impressões digitais, reconhecimento facial ou voz, exemplificam o design de autenticação avançado. Esses métodos oferecem uma camada adicional de segurança, pois são baseados em atributos únicos de cada indivíduo.
- Tokenização: A geração de códigos temporários por meio de tokens físicos ou aplicativos autenticadores representa uma abordagem eficaz no design de autenticação. Esses códigos dinâmicos garantem que apenas quem possui o dispositivo específico possa realizar a autenticação.

Autenticação Biométrica.

Multifator de autenticação

O Multifator de Autenticação (MFA) é uma abordagem de segurança que exige que os usuários forneçam mais de uma forma de verificação de identidade para acessar um sistema ou recurso. Em vez de depender apenas de uma única credencial (como senha), o MFA incorpora múltiplos fatores, aumentando significativamente a robustez da autenticação. É uma estratégia eficaz para mitigar os riscos associados a acessos não autorizados, proporcionando camadas adicionais de proteção. Ao compreender e implementar o MFA, organizações e usuários individuais podem elevar significativamente a segurança de suas contas e sistemas. Exemplos de usos para reforçar a segurança:

- **Senha + Token**:
- Cenário: Um usuário fornece sua senha convencional e, simultaneamente, um código gerado por um token físico ou aplicativo autenticador.
- Reforço de Segurança: Mesmo se a senha for comprometida, o acesso ainda é negado sem o token adicional.
- **Impressão Digital + Senha**:
- Cenário: Além de digitar uma senha, o usuário precisa autenticar sua identidade por meio de uma leitura de impressão digital.
- Reforço de Segurança: Combinação de algo que o usuário sabe (senha) com algo que o usuário é (impressão digital), aumentando a segurança.
- **Reconhecimento Facial + Confirmação via Dispositivo**:
- Cenário: Após o reconhecimento facial, o usuário recebe uma notificação no dispositivo móvel para confirmar a autenticação.
- Reforço de Segurança: A validação biométrica é combinada com um fator de propriedade (dispositivo móvel) para garantir uma autenticação mais segura.

Multifator de Autenticação.

Atributos de autenticação

Comparado aos três principais fatores de autenticação, um atributo de autenticação é uma propriedade ou fator não exclusivo, ou seja, que não pode ser usado independentemente.

1. **Autenticação baseada no Local**: A autenticação baseada no local valida a identidade do usuário com base em sua localização física. Isso pode envolver o uso de dispositivos de geolocalização, como GPS, para confirmar se o usuário está em uma área específica. A autenticação pode também medir algumas estatísticas sobre onde você está. Pode ser uma localização geográfica medida através do serviço de localização de um dispositivo, ou pode ser por endereço IP. O endereço IP de um dispositivo pode ser usado para se referir a um segmento de rede ou pode ser vinculado a uma localização geográfica usando um serviço de geolocalização. Entre as possibilidades dentro de uma rede, a localização física por porta, LAN virtual (VLAN) ou rede Wi-Fi também pode ser o meio para a autenticação baseada no local.

Em todos os casos, a autenticação baseada em localização não é usada como fator de autenticação primário, mas pode ser usada como mecanismo de autenticação contínua ou como recurso de controle de acesso. Por exemplo, se um usuário inserir as credenciais corretas em um gateway VPN, mas seu endereço IP mostrar que ele/ela está em um país diferente do esperado, controles de acesso poderão ser aplicados para restringir os privilégios concedidos ou recusar completamente o acesso. Outro exemplo é quando um usuário parece fazer login em locais geográficos diferentes que o tempo de viagem tornaria fisicamente impossível.

Exemplos de uso:

- Acesso a Redes Corporativas: Garantir que o acesso a redes corporativas sensíveis seja concedido apenas quando o usuário estiver em locais predefinidos.
- Transações Financeiras: Reforçar a segurança ao autorizar transações apenas se o usuário estiver fisicamente próximo ao ponto de compra.

2. **Autenticação baseada em comportamento (algo que você pode fazer)**: Este tipo de autenticação leva em consideração os padrões de comportamento do usuário, como a velocidade de digitação, a forma como segura um dispositivo ou a maneira como navega em uma página. Características comportamentais, como a maneira como você anda ou segura o smartphone, podem identificá-lo de maneira única em um número considerável de atividade. Embora esse fator seja impraticável para autenticação primária, ele pode ser usado para autenticação contextual e contínua para garantir que um dispositivo continue a ser operado pelo proprietário.

Exemplos de uso:

- Verificação Contínua: Sistemas que monitoram constantemente o comportamento do usuário, exigindo reautenticação se houver desvios significativos.
- Prevenção contra Ameaças Internas: Identificar comportamentos suspeitos que podem indicar atividades maliciosas dentro da organização.

3. **Autenticação baseada em algo que você exibe (comportamental)**: A autenticação comportamental considera como um usuário interage com interfaces digitais, analisando padrões como movimentos do mouse, velocidade de cliques e até mesmo a maneira como digita. Algo que você exibe também se refere à autenticação e autenticação baseada em comportamento, com ênfase específica em traços de personalidade. Por exemplo, a maneira como você usa aplicativos para smartphones ou mecanismos de pesquisa na web pode estar de acordo com um padrão de comportamento que pode ser capturado pela análise de aprendizado de máquina como um modelo estatístico. Se outra pessoa usar o dispositivo, seu comportamento será diferente e esse padrão anômalo poderá ser usado para bloquear o dispositivo e exigir nova autenticação.

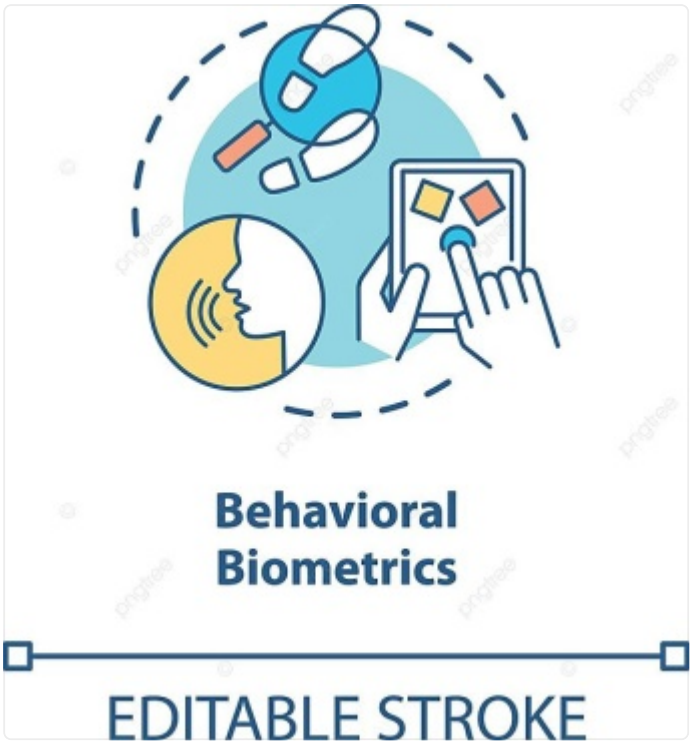
Exemplos de uso:

- Prevenção de Fraudes: Identificação de possíveis atividades fraudulentas com base em variações no comportamento do usuário.
- Identificação Contínua: Sistemas que adaptam a autenticação com base no comportamento observado ao longo do tempo.

4. **Autenticação baseada em alguém que você conhece**: Este conceito envolve a autenticação com base no conhecimento de relações pessoais ou redes sociais. Pode incluir perguntas sobre pessoas conhecidas ou a validação por meio de contatos de confiança. Um esquema de autenticação de alguém que você conhece usa um modelo de rede de confiança, onde novos usuários são garantidos por usuários existentes. À medida que o usuário participa da rede, sua identidade fica mais estabelecida. Um exemplo é o modelo descentralizado de web de confiança, usado pela Pretty Good Privacy (PGP) Corp. como alternativa à PKI. O PGP é um software de criptografia de chave pública altamente seguro, originalmente escrito por Philip Zimmermann. Tornou-se um padrão de fato para a criptografia de correio eletrônico (e-mail) na internet.

Exemplos de uso:

- Recuperação de Conta: Verificação de identidade por meio de informações sobre pessoas conhecidas durante processos de recuperação de conta.
- Acesso a Informações Sensíveis: Utilização de conhecidos como uma camada adicional de autenticação em sistemas sensíveis.



Biometria Comportamental.

Conclusão

Nesta aula abrangente sobre Gerenciamento de Identidade e Acesso, vimos desde os conceitos fundamentais de identificação, autenticação, autorização e accounting (IAAA) até a exploração de diversos fatores e atributos de autenticação, cada tópico foi desenhado para proporcionar uma compreensão holística e prática.

Compreendemos a importância vital do design de autenticação, reconhecendo-o como o alicerce que sustenta a proteção contra acessos não autorizados. O multifator de autenticação emergiu como uma estratégia indispensável, elevando a segurança através da implementação de múltiplos fatores de verificação.

Além dos métodos convencionais, vimos os atributos de autenticação, como a base em localização, comportamento, exibição e conhecimento pessoal. Essas nuances adicionais não apenas reforçam a autenticação, mas também proporcionam uma resposta adaptativa a um cenário de ameaças em constante evolução.

Que este conhecimento sirva como uma sólida fundação, capacitando-os a enfrentar desafios crescentes no mundo da segurança cibernética. Parabéns pelo

empenho nesta aula. Sigamos fortalecendo a cibersegurança em cada passo da jornada.

Aula 2: Autenticação baseada em conhecimento

Objetivos

- [x] Compreender os conceitos e métodos de autenticação em Windows e Linux.
- [x] Explorar Single Sign-On e os protocolos PAP, CHAP, MS-Chap authentication.
- [x] Analisar ataques de senha, incluindo força bruta e de dicionário, assim como estratégias de gerenciamento de autenticação.

Conceitos

- [x] Autenticação: Local, de rede e remota, abordando ambientes Windows e Linux.
- [x] Single Sign-On (SSO) e protocolos como PAP, CHAP, MS-Chap authentication.
- [x] Ataques de senha e estratégias de gerenciamento de autenticação.

Introdução

Bem-vindos à aula sobre Autenticação Baseada em Conhecimento. Neste encontro, abordaremos as complexidades e fundamentos dos processos de autenticação, explorando desde autenticação local, de rede e remota até os diferentes ambientes Windows e Linux. A segurança da informação é um pilar crítico nos dias de hoje, e compreender os mecanismos de autenticação é essencial para fortalecer nossos sistemas.

Ao longo desta aula, veremos tecnologias como a do Single Sign-On (SSO) e dos protocolos PAP, CHAP, MS-Chap authentication, entendendo como esses recursos contribuem para a segurança dos dados. Além disso, abordaremos os desafios

enfrentados, examinando ataques de senha, tais como força bruta e de dicionário, e discutiremos estratégias robustas de gerenciamento de autenticação.

Em nossa trajetória de aprendizado não apenas entenderemos a importância da autenticação, mas também veremos soluções e práticas que garantem ambientes seguros e confiáveis.

Implementando Autenticação Baseada em Conhecimento

A autenticação baseada em conhecimento refere-se principalmente à criação de credenciais de usuários com mecanismos de acesso à conta baseados em senha. Configurar protocolos de autenticação baseados em senha e fornecer suporte a usuários com problemas de autenticação é uma parte importante da função de segurança da informação. Neste tópico, você aprenderá como funcionam alguns protocolos de autenticação comuns e como eles podem ser configurados por meio de técnicas de quebra de senha.

Autenticação Local, de Rede e Remota

Um dos recursos mais importantes de um sistema operacional é o provedor de autenticação, que é a arquitetura de software e o código que sustenta o mecanismo pelo qual o usuário é autenticado antes de iniciar um shell. Isso geralmente é descrito como login (Linux) ou logon ou sign-in (Microsoft). A autenticação baseada em conhecimento, usando uma senha ou número de identificação pessoal (PIN), é o provedor de autenticação padrão para a maioria dos sistemas operacionais.

1. **O processo de login**: É uma sequência de passos pelos quais um usuário fornece suas credenciais para acessar um sistema, aplicativo ou recurso protegido. Essas credenciais geralmente consistem em um nome de usuário (ou identificador) e uma senha ou PIN, mas também podem incluir outros fatores, como autenticação biométrica (impressão digital, reconhecimento facial) ou tokens de segurança.

A autenticação baseada em conhecimento depende de hashes criptográficos. Uma senha em texto simples geralmente não é transmitida ou armazenada em um banco de dados de credenciais devido ao risco de comprometimento. Em vez disso, a senha é armazenada como um hash criptográfico. Quando um usuário insere uma senha para efetuar login, um autenticador converte o que é digitado em um hash e o transmite para uma autoridade. A autoridade compara o hash enviado com o do banco de dados e autentica somente se eles corresponderem. Aqui estão os passos típicos envolvidos no processo de login:

- **Identificação do Usuário**: O usuário fornece um identificador exclusivo, como um nome de usuário, endereço de e-mail ou número de identificação.
- **Fornecimento de Credenciais**: O usuário informa a senha associada ao identificador fornecido. Em alguns casos, podem ser necessários passos adicionais, como a inserção de um código de autenticação ou o uso de métodos biométricos.
- **Envio das Credenciais ao Sistema**: As informações de identificação e credenciais são enviadas ao sistema de autenticação, seja localmente no dispositivo ou em um servidor remoto.
- **Validação das Credenciais**: O sistema verifica a correspondência entre as credenciais fornecidas e aquelas armazenadas em sua base de dados. Se as credenciais são válidas, o usuário é autenticado.
- **Concessão de Acesso**: Uma vez autenticado com sucesso, o sistema concede ao usuário acesso aos recursos, serviços ou informações autorizados.
- **Geração de Sessão**: Uma sessão é estabelecida para o usuário, permitindo a interação contínua com o sistema sem a necessidade de autenticação repetida durante um período específico.

2. **Autenticação Local**: A autenticação local refere-se ao processo de verificar a identidade de um usuário em um dispositivo específico. Neste cenário, o usuário interage diretamente com o sistema, como um computador pessoal ou um dispositivo móvel, para ganhar acesso aos recursos locais.

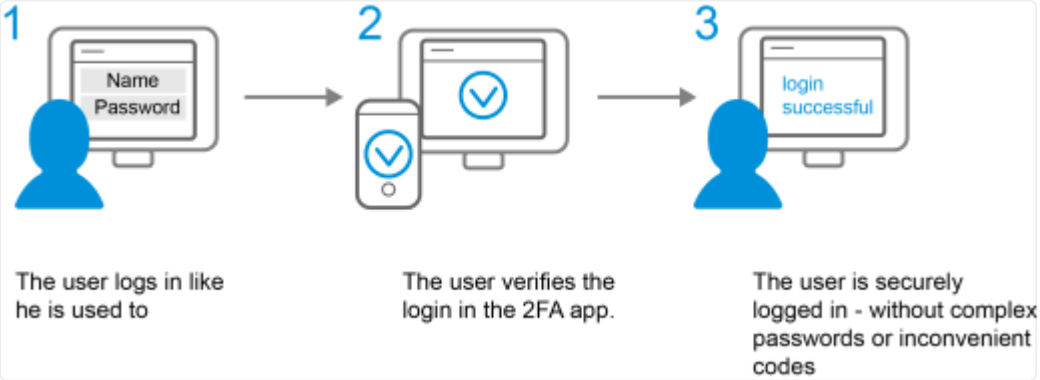
Implementação Prática: Exemplo comum é a utilização de senhas ou PINs para acessar um computador pessoal. Além disso, em dispositivos mais avançados, a autenticação biométrica, como leitores de impressões digitais em smartphones, exemplifica a segurança local.

3. **Autenticação de Rede**: A autenticação de rede expande o escopo para incluir o acesso a recursos compartilhados em uma rede corporativa. Nesse caso, a verificação de identidade não ocorre no dispositivo local, mas sim em um servidor central, como o Active Directory no ecossistema Windows.

Implementação Prática: Em ambientes corporativos, um exemplo seria o uso do protocolo LDAP (Protocolo de Acesso a Diretório Leve) para autenticar usuários em um servidor centralizado. Outro exemplo é em um ambiente corporativo que utiliza o Active Directory (AD), os usuários autenticam suas credenciais em um servidor central ao ingressar na rede. Em ambos os casos permite que os recursos compartilhados, como servidores de arquivos, impressoras e aplicativos sejam acessados, garantindo a integridade e a segurança dos dados.

4. **Autenticação Remota**: A autenticação remota permite a validação da identidade de usuários que buscam acessar recursos a partir de locais geograficamente distintos. Isso é essencial para organizações com equipes distribuídas globalmente ou que permitem o trabalho remoto.

Implementação Prática: A utilização de VPNs (Redes Privadas Virtuais) é um exemplo notável. Usuários remotos se conectam à rede corporativa através de uma conexão segura, estabelecendo um túnel criptografado que permite a autenticação remota como se estivessem fisicamente na sede da empresa.



Autenticação Remota.

Autenticação no Windows e Linux

1. **Autenticação no Windows**: Envolve uma complexa arquitetura de componentes, mas os seguintes cenários são típicos:

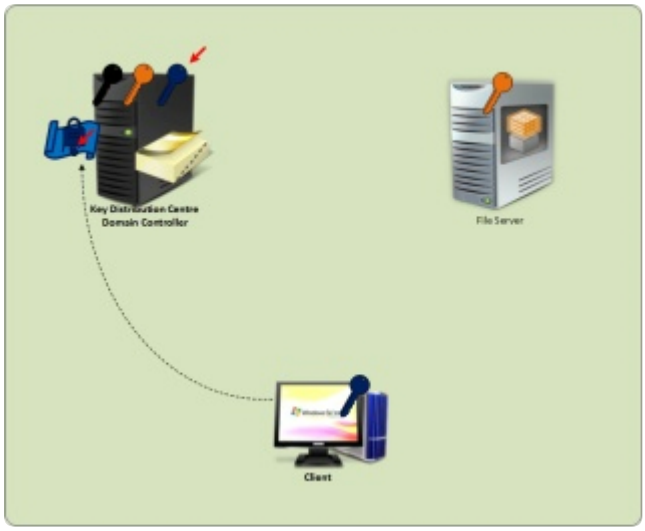
- **Sign-in Local**: A autenticação local é realizada no próprio dispositivo, onde o usuário fornece suas credenciais diretamente para acessar recursos específicos. Isso pode incluir senhas, PINs ou até mesmo métodos biométricos, dependendo da configuração do dispositivo. A Autoridade de Segurança Local (LSA) compara a credencial enviada a um hash armazenado no banco de dados do Security Accounts Manager (SAM), que faz parte do registro. Isso também é conhecido como logon interativo. O Local Security Authority (LSA) no Windows é um componente do sistema operacional. Ele é responsável pela implementação de políticas de segurança locais, pela autenticação de usuários, controles de acesso e pela manutenção de informações de segurança no nível local do sistema.
- **Autenticação de Rede no Windows**: A autenticação de rede no Windows é amplamente gerenciada pelo Active Directory (AD). Nesse contexto, quando um usuário tenta acessar recursos compartilhados em uma rede corporativa, as credenciais são verificadas por um controlador de domínio no AD. Essa abordagem centralizada facilita a aplicação consistente de políticas de segurança em toda a rede e permite a gestão eficiente de usuários e grupos. O LSA passa as credenciais de autenticação para um serviço de rede. O sistema preferencial para autenticação de rede é baseado em Kerberos, mas os aplicativos de rede herdados podem usar a autenticação NT LAN Manager (NTLM).

Papel do Kerberos na autenticação: O Kerberos é um protocolo de autenticação forte que visa proporcionar uma forma segura de autenticar usuários em redes. Ele é especialmente utilizado em ambientes que fazem parte de um domínio do Active Directory. O Kerberos utiliza um modelo de bilhete para autenticação. Quando um usuário se autentica no domínio, ele emite um "Ticket de Serviço" (TGT - Ticket Granting Ticket). Esse ticket é então usado para solicitar outros tickets de serviço para acessar recursos específicos, sem a necessidade de reautenticação. É um protocolo altamente seguro, pois utiliza técnicas de criptografia para proteger as credenciais dos usuários durante a autenticação e a comunicação entre os sistemas. Ele minimiza o risco de ataques como "replay attacks" e "man-in-the-middle attacks".

Papel do NTLM na autenticação: O NTLM é um protocolo de autenticação mais antigo que ainda é suportado no Windows por razões de compatibilidade. No entanto, não oferece o mesmo nível de segurança que o Kerberos. Ele utiliza um desafio-resposta para autenticação. Quando um usuário tenta acessar um recurso,

o servidor emite um desafio ao qual o cliente responde com uma versão hasheada da senha. Embora o NTLM forneça uma forma básica de autenticação, ele tem limitações significativas em termos de segurança. As senhas são armazenadas no formato de hash reversível, o que pode ser mais vulnerável a ataques, e ele não oferece as mesmas proteções contra ataques sofisticados que o Kerberos.

- **Autenticação Remota no Windows**: Para a autenticação remota no Windows, tecnologias como o Protocolo de Área Segura (SSTP) para VPNs podem ser empregadas. Os usuários remotos autenticam-se por meio de uma conexão segura, geralmente utilizando certificados digitais ou outros métodos seguros, permitindo que a autenticação ocorra como se estivessem fisicamente na rede corporativa. Isso é particularmente relevante em cenários onde a equipe precisa acessar recursos da empresa de locais externos.



Autenticação com Kerberos.

2. **Autenticação no Linux**: O processo de login no Linux inclui:

- **Login local**: No Linux, a autenticação local envolve o uso de senhas, chaves de autenticação SSH ou outros métodos, dependendo da configuração específica do sistema. O arquivo "/etc/passwd" e o "/etc/shadow" são comumente utilizados para armazenar informações de usuários locais. Os nomes das contas de usuários locais são armazenados no etc/passwd. Quando um usuário efetua login em um shell interativo local, a senha é verificada em um hash armazenado no /etc/shadow.
- **Autenticação de Rede no Linux**: O login interativo em uma rede pode ser realizado usando Secure Shell (SSH). Com o SSH, o usuário é autenticado usando chaves criptográficas em vez de uma senha. A autenticação de rede no

Linux pode também ser configurada por meio do Pluggable Authentication Modules (PAM). Isso permite a flexibilidade na escolha de métodos de autenticação para diferentes serviços de rede. Além disso, a integração com serviços de diretório, como o LDAP, pode ser implementada para autenticar usuários em uma rede centralizada.

- **Autenticação Remota no Linux**: A autenticação remota no Linux pode ser realizada através de protocolos seguros, como SSH (Secure Shell). Usuários remotos autenticam-se usando chaves SSH ou senhas, permitindo a execução segura de comandos e a transferência de arquivos de forma remota. Esse método é amplamente utilizado em administração de servidores Linux localizados em data centers ou em nuvens. Um módulo de autenticação conectável (PAM) é um pacote para habilitar diferentes provedores de autenticação, como login com cartão inteligente. A estrutura PAM também pode ser usada para implementar autenticação em servidores de redes.

Autenticação no Linux.

Single sign-on (SSO)

Um sistema de logon único (SSO) permite que o usuário se autentique uma vez em um dispositivo local e seja autenticado em servidores de aplicativos compatíveis sem precisar inserir credenciais novamente. É uma solução de autenticação que permite que um usuário acesse vários sistemas ou aplicativos com uma única autenticação. Em vez de exigir que o usuário faça login separadamente em cada serviço, o SSO autentica o usuário uma vez e concede acesso aos demais serviços sem a necessidade de autenticação adicional. Isso não apenas simplifica a

experiência do usuário, mas também melhora a segurança, pois reduz o número de senhas que um usuário precisa gerenciar. O Single Sign-On é implementado em diferentes ambientes e sistemas usando diferentes padrões e protocolos, como OAuth, OpenID Connect e SAML (Security Assertion Markup Language), dependendo dos requisitos e das características do ambiente de implantação. No Windows, o SSO é fornecido pela estrutura Kerberos. As etapas do Processo de Single Sign-On podem incluir:

- **Autenticação Inicial**: O processo começa quando o usuário realiza a autenticação inicial em um dos serviços conectados ao sistema SSO. Normalmente, isso envolve o fornecimento de credenciais, como nome de usuário e senha.
- **Emissão de Token de Sessão**: Após a autenticação bem-sucedida, o sistema SSO emite um token de sessão para o usuário. Esse token é um identificador único que contém informações sobre a autenticação do usuário.
- **Armazenamento Seguro do Token**: O token de sessão é armazenado de forma segura no lado do cliente (geralmente em um cookie ou armazenamento local do navegador) e no lado do servidor. Esse armazenamento seguro permite que o sistema valide a identidade do usuário durante todo o processo de sessão.
- **Acesso a Outros Serviços**: Quando o usuário tenta acessar outros serviços ou aplicativos conectados ao sistema SSO, o token de sessão é apresentado. Em vez de exigir novas credenciais, o serviço utiliza o token para verificar a autenticidade do usuário.
- **Renovação de Token**: Periodicamente, o token pode ser renovado para garantir a segurança contínua. Isso geralmente é feito sem interrupção para o usuário, mantendo a experiência SSO sem a necessidade de reautenticação frequente.
- **Logout Único (Single Logout)**: Quando o usuário decide encerrar a sessão, o SSO realiza um logout único, revogando o acesso a todos os serviços conectados simultaneamente. Isso garante que o usuário seja desconectado de todos os serviços associados ao SSO com apenas uma ação.

Single Sign-on.

Protocolos de Autenticação (PAP, CHAP, MS-Chap)

1. **PAP (Password Authentication Protocol)**: PAP é um protocolo de autenticação simples onde as credenciais (nome de usuário e senha) são enviadas ao servidor em texto simples durante a autenticação. É considerado menos seguro, pois as informações são transmitidas sem criptografia. O PAP é mais adequado para ambientes onde a segurança não é a principal preocupação, como em redes dial-up. Redes de discagem (dial-up) historicamente usaram o PAP, mas seu uso tem diminuído devido às preocupações com segurança. É menos comum em ambientes modernos devido à sua vulnerabilidade a ataques de captura de dados. É utilizado também como mecanismo de autenticação básico em HTTP.
2. **CHAP (Challenge Handshake Authentication Protocol)**: CHAP é um protocolo de autenticação mais seguro que utiliza um desafio e resposta durante o processo. O servidor envia um desafio ao cliente, que responde com uma versão criptografada da senha combinada com o desafio. CHAP é mais seguro do que o PAP porque não envia senhas em texto simples pela rede. Ele é usado em conexões ponto a ponto, como em conexões PPP (Point-to-Point Protocol) em redes dial-up e VPNs onde a segurança da senha é uma preocupação.
3. **MS-CHAP (Microsoft Challenge Handshake Authentication Protocol)**: MS-CHAP é uma variação do CHAP desenvolvida pela Microsoft. Ele aprimora a segurança adicionando suporte à troca de senhas criptografadas. MS-CHAP é frequentemente usado em ambientes Microsoft, especialmente em VPNs. Versões mais recentes, como MS-CHAPv2, oferecem melhor segurança.

Comparação de Características e Aplicabilidades

- PAP é o menos seguro, pois as senhas são enviadas sem criptografia. CHAP e MS-CHAP são mais seguros devido à troca de desafios e respostas criptografadas.
- PAP é adequado para ambientes de baixa segurança. CHAP e MS-CHAP são preferíveis em ambientes onde a segurança é uma prioridade, como em conexões VPN.
- MS-CHAP, sendo desenvolvido pela Microsoft, é mais comum em ambientes Windows, enquanto CHAP é um padrão mais amplo suportado por uma variedade de plataformas.

Ataques de senha

Quando um usuário escolhe uma senha, a senha é convertida em um hash usando uma função criptográfica, como MD5 ou SHA. Isso significa que, em teoria, ninguém, exceto o usuário (nem mesmo o administrador do sistema), conhece a senha, porque o texto simples não deve ser recuperável a partir do hash. Há vários tipos de ataques de senha como veremos a seguir:

1. **Ataque de texto simples/não criptografado**: Um ataque de texto simples/não criptografado (plaintext/unencrypted attack) explora o armazenamento de senhas ou um protocolo de autenticação de rede que não usa criptografia. Esse tipo de ataque ocorre quando as senhas são transmitidas ou armazenadas em formato legível, sem qualquer forma de criptografia. Os atacantes podem interceptar ou acessar diretamente essas senhas. Os exemplos incluem PAP, autenticação HTTP/FTP básica e Telnet. Esses protocolos não devem ser usados. As senhas nunca devem ser salvas em um arquivo não gerenciado. Um tipo comum de violação de credenciais são as senhas incorporadas no código do aplicativo que foram posteriormente carregadas em um repositório público. Sempre utilize comunicações seguras (HTTPS) para transmitir senhas e armazene-as de maneira segura, utilizando técnicas de hash e criptografia adequadas.
2. **Ataques Online**: Um ataque de senha online ocorre quando o agente da ameaça interage diretamente com o serviço de autenticação – um formulário de login na web ou gateway VPN, por exemplo. O invasor envia senhas usando um banco de dados de senhas conhecidas (e variações) ou uma lista de senhas que foram quebradas offline. Os ataques online envolvem tentativas automáticas e contínuas de login em uma conta, geralmente usando força bruta ou dicionário.

Atacantes exploram a capacidade de realizar tentativas repetidas para encontrar a combinação correta de nome de usuário e senha. Uma forma de evitar esse tipo de ataque é implementando bloqueios automáticos após várias tentativas mal sucedidas, utilizar autenticação de dois fatores (2FA) e encorajar o uso de senhas fortes.

3. **Pulverização de Senhas**: A pulverização de senhas é um ataque on-line horizontal de força bruta. Isso significa que o invasor escolhe uma ou mais senhas comuns (por exemplo, “senha” ou “123456”) e as testa em conjunto com vários nomes de usuário. Neste tipo de ataque, o invasor tenta poucas combinações de senhas em várias contas, evitando detecção automática. Ao limitar o número de tentativas por conta, os atacantes evitam bloqueios automáticos, tornando mais difícil a detecção de atividades suspeitas. Para tentar evitar este tipo de ataque monitore padrões de login, implemente bloqueios baseados em comportamento e utilize ferramentas de detecção de pulverização de senhas.
4. **Ataques Offline**: Ataques offline envolvem a obtenção de informações de autenticação armazenadas localmente, como hashes de senhas, permitindo tentativas de quebra sem interação com o sistema alvo. Um invasor pode obter acesso a bancos de dados de senhas comprometidos e usar técnicas offline, como ataques de força bruta ou dicionário. Uma maneira de evitar esses ataques é armazenando senhas de maneira segura, utilizando técnicas de hash fortes e mantendo sistemas e bancos de dados protegidos contra acessos não autorizados.

Como e por que acontece o ataque:

Um ataque offline significa que o invasor conseguiu obter um banco de dados de hashes de senha. Uma vez obtido o banco de dados de senhas, o cracker não interage com o sistema de autenticação. O único indicador desse tipo de ataque (além do erro de conta no caso de um ataque bem-sucedido) é um log de auditoria do sistema de arquivos que registra a conta maliciosa que acessa um desses arquivos. Os atores da ameaça também podem ler credenciais da memória do host; nesse caso, o único indicador confiável pode ser a presença de ferramentas de ataque em um host. Se o invasor não conseguir obter um banco de dados de senhas, um sniffer de pacotes poderá ser usado para obter a resposta do cliente a um desafio do servidor em um protocolo como NTLM ou CHAP/MS-CHAP. Embora esses protocolos evitem enviar o hash da senha diretamente, o ID da resposta derivou dela de alguma forma. Os crackers de senhas podem explorar os pontos

fracos de um protocolo para calcular o hash e combiná-lo com uma palavra do dicionário ou forçá-lo com força bruta.

5. **Ataques de Força Bruta**: Alguns ataques de senha exploram credenciais fracas escolhidas pelos usuários. Outros podem explorar vulnerabilidades no mecanismo de armazenamento. Um ataque de força bruta tenta todas as combinações possíveis no espaço de saída para corresponder a um hash capturado e adivinhar o texto simples que o gerou. O espaço de saída é determinado pelo número de bits usados pelo algoritmo (MD5 de 128 bits ou SHA256 de 256 bits, por exemplo). Quanto maior o espaço de saída e quanto mais caracteres forem usados na senha de texto simples, mais difícil será calcular e testar cada hash possível para encontrar uma correspondência. Os ataques de força bruta são fortemente limitados pelo tempo e pelos recursos computacionais e, portanto, são mais eficazes na quebra de senhas curtas. No entanto, ataques de força bruta distribuídos em vários componentes de hardware, como um cluster de placas gráficas de última geração, podem ter sucesso na quebra de senhas mais longas.
6. **Ataques de Dicionário**: Ataques de força bruta tentam todas as combinações possíveis de senhas, enquanto ataques de dicionário usam uma lista de palavras comuns. Um ataque de dicionário pode ser usado onde há uma boa chance de adivinhar o valor provável do texto simples, como uma senha não complexa. O software gera valores de hash a partir de um dicionário de textos simples para tentar combinar um com um hash capturado. Atacantes exploram a previsibilidade de senhas comuns ou sequências alfanuméricas, tentando exaustivamente todas as combinações. Uma forma de evitar é reforçando políticas de senhas, promovendo o uso de senhas complexas e implementando bloqueios automáticos após tentativas mal sucedidas.
7. **Ataque Híbrido**: O ataque híbrido de senha usa uma combinação de ataques de dicionário e de força bruta. É direcionado principalmente contra senhas ingênuas com complexidade inadequada, como "james1". O algoritmo de quebra de senha testa palavras e nomes de dicionário em combinação com uma máscara que limita o número de variações a serem testadas, como a adição de prefixos e/ou sufixos numéricos. Outros tipos de algoritmos podem ser aplicados, com base no que os hackers sabem sobre como os usuários se comportam quando são forçados a selecionar senhas complexas que eles realmente não querem que sejam difíceis de lembrar. Outros exemplos podem incluir a substituição de “s” por “S” ou “o” por “0”. Ataques híbridos otimizam a eficácia do ataque. Os atacantes buscam equilibrar a eficiência de um ataque de força bruta com a previsibilidade de padrões de senha comuns. Para inibir essas

ações incentive a criação de senhas únicas e complexas, além de utilizar bloqueios automáticos e monitoramento proativo contra padrões de ataque híbridos.

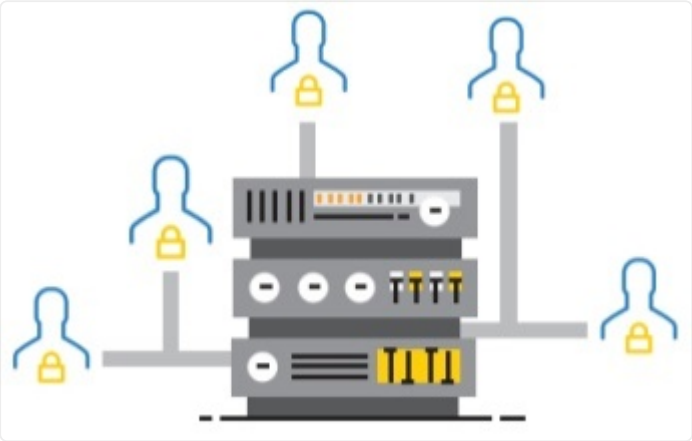
Ataques de senhas.

Gerenciamento de autenticação

Os usuários geralmente adotam práticas inadequadas de gerenciamento de credenciais que são muito difíceis de controlar, como usar a mesma senha para redes corporativas e sites de consumidores. Isso torna a segurança da rede corporativa vulnerável a violações de dados desses sites. Uma solução de gerenciamento de autenticação para senhas mitiga esse risco usando um dispositivo ou serviço como proxy para armazenamento de credenciais. O gerente gera uma senha forte e exclusiva para cada conta baseada na web. O usuário autoriza o gerente a se autenticar em cada site usando uma senha mestra. Os gerenciadores de senhas podem ser implementados com um token de hardware ou como um aplicativo de software:

- **Chave de senha**: Tokens USB para conexão com PCs e smartphones. Alguns podem usar comunicações de campo próximo (NFC) ou Bluetooth, bem como conectividade física.
- **Cofre de senhas**: Gerenciador de senhas baseado em software, normalmente usando um serviço de nuvem para permitir acesso de qualquer dispositivo. É provável que uma chave USB também use um cofre para backup. A maioria dos

sistemas operacionais e navegadores implementam cofres de senhas nativos. Os exemplos incluem o Windows Credential Manager e o ICloud Keychain da Apple.



Cofre de senhas.

Conclusão

Nesta aula, exploramos o tema do gerenciamento de autenticação, abordando estratégias eficazes, políticas de senha, e ferramentas tecnológicas avançadas. A autenticação é o portão de entrada para a segurança digital, e adotar práticas robustas é essencial para proteger informações sensíveis e manter a integridade dos sistemas.

Ao adotar estratégias como a autenticação multifatorial, que adiciona camadas de segurança, e ao implementar políticas de senhas que promovem complexidade e rotação regular, estamos construindo uma defesa resiliente contra ameaças cibernéticas. A conscientização dos usuários sobre a importância das práticas seguras de autenticação é uma peça crucial nesse quebra-cabeça.

Além disso, exploramos tecnologias avançadas, como autenticação biométrica e o uso de protocolos seguros, que oferecem soluções inovadoras para os desafios contemporâneos de segurança. A adaptação constante às últimas tendências e a integração de soluções de gerenciamento de senhas proporciona uma abordagem holística para fortalecer a autenticação. A incorporação de monitoramento contínuo, bloqueios automáticos inteligentes e a análise de contexto durante a autenticação contribuem para a detecção precoce de atividades suspeitas.

Em resumo, ao adotar práticas e tecnologias avançadas, mantemos a confidencialidade, integridade e disponibilidade dos sistemas, criando um ambiente digital resiliente diante das ameaças emergentes. Parabéns por ter finalizado mais esta importante etapa.