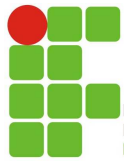
Segurança de Redes

Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 01
Fundamentos de Segurança

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"A arte de perceber de forma clara e real nossas mais íntimas intenções é uma das tarefas do processo evolutivo pelo qual todos estamos passando." (Hammed)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

O que Aprenderemos?

- O que é segurança da informação;
- Princípios desejáveis para os sistemas seguros;
- Estatísticas de incidência de segurança no Brasil;
- Principais desafio para a segurança da informação;
- Os personagens que exploram vulnerabilidades de segurança.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança da informação?

Consiste de **medidas para prevenir, detectar e corrigir violações de segurança** que envolvam o armazenamento e a transmissão de informações. Estas medidas visam oferecer aos sistemas de informação, pelo menos três principios de segurança básico: **integridade, disponibilidade e confidencialidade**.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Confidencialidade: assegurar que informações privadas e confidenciais não sejam reveladas para indivíduos não autorizados. Uma perda de confidencialidade seria a divulgação não autorizada de informação.

Integridade: prevenir-se contra a modificação ou destruição imprópria (sem autorização) de informações e programas. Além disso, assegurar que os sistemas executem as suas funcionalidades de forma ilesa, livre de manipulações deliberadas ou inadvertidas do sistema.

Disponibilidade: assegurar acesso e uso da informação e/ou serviços, ou seja, garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou sistema de informação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Conceitos Adicionais

Além da confidencialidade, integridade e disponibilidade, algumas aplicações no campo da segurança necessitam de características adicionais, são elas: **autenticidade, responsabilização e auditoria**.

Autenticidade: verificar que os usuários são quem dizem ser (garantia da identidade dos participantes da comunicação) e, além disso, que cada entrada no sistema vem de uma fonte confiável. A maioria dos sistemas atuais solicita uma senha, mas já existem sistemas mais modernos utilizando cartões inteligentes ou ainda características físicas, como retina, impressão digital e reconhecimento de voz.

Legalidade: Garantia de que a informação foi produzida em conformidade com a lei;

EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Conceitos Adicionais

Responsabilização ou Não Repúdio: garantir que as ações de uma entidade sejam atribuídas exclusivamente a ela. Desta forma, um agente não consiga negar uma ação que criou ou modificou uma informação, ou seja, temos que ser capazes de associar uma violação de segurança a uma parte responsável.

Os sistemas precisam manter registros de suas atividades a fim de permitir posterior análise forense, de modo a rastrear as violações de segurança, garantindo a responsabilização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os Desafios da Segurança de Computadores

- No desenvolvimento de um mecanismo ou algoritmo específico de segurança, é muito difícil considerar todos e quaisquer potenciais ataques a essas funcionalidades. Em muitos casos, os ataques bem-sucedidos são projetados para explorar uma fraqueza inesperada no mecanismo.
- Segurança de computadores e redes é, essencialmente, uma batalha de inteligência entre um criminoso que tenta encontrar buracos e o projetista ou administrador que tenta fechá-los. A grande vantagem que o atacante possui é que ele ou ela precisa encontrar uma simples brecha, enquanto o projetista tem que encontrar e eliminar todas as possíveis brechas para garantir uma segurança perfeita.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Os Desafios da Segurança de Computadores

- Existe uma tendência natural de uma parte dos usuários e gerentes de sistemas a perceber poucos benefícios com os investimentos em segurança, até que uma falha nela ocorra.
- A segurança requer um monitoramento regular, ou até mesmo constante, e isso é algo difícil com os curtos prazos e nos ambientes sobrecarregados dos dias de hoje.
- Muitos usuários, e até mesmo administradores de segurança, veem uma segurança forte como um impedimento à eficiência e à operação amigável de um sistema de informação ou do uso da informação.

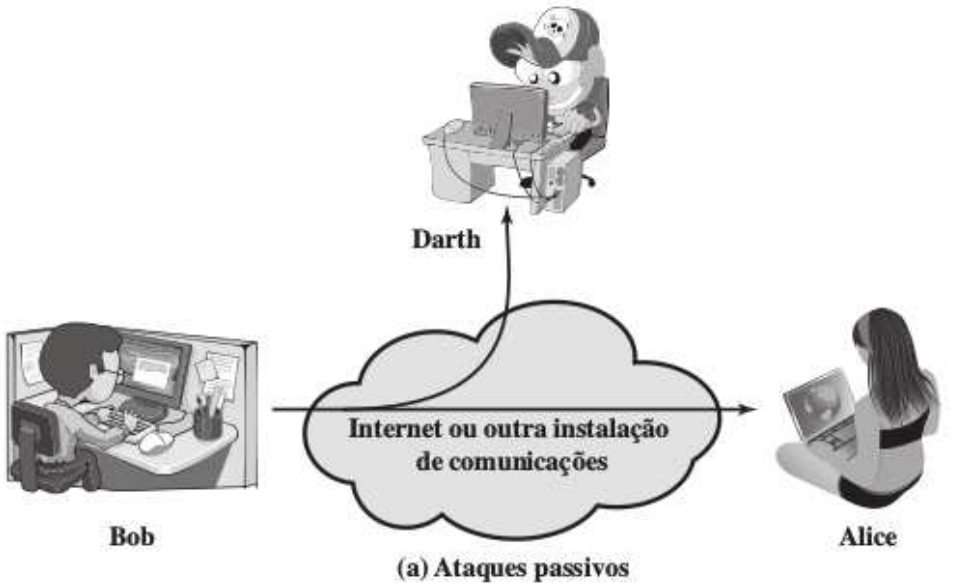
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ameaças e Ataques à Segurança

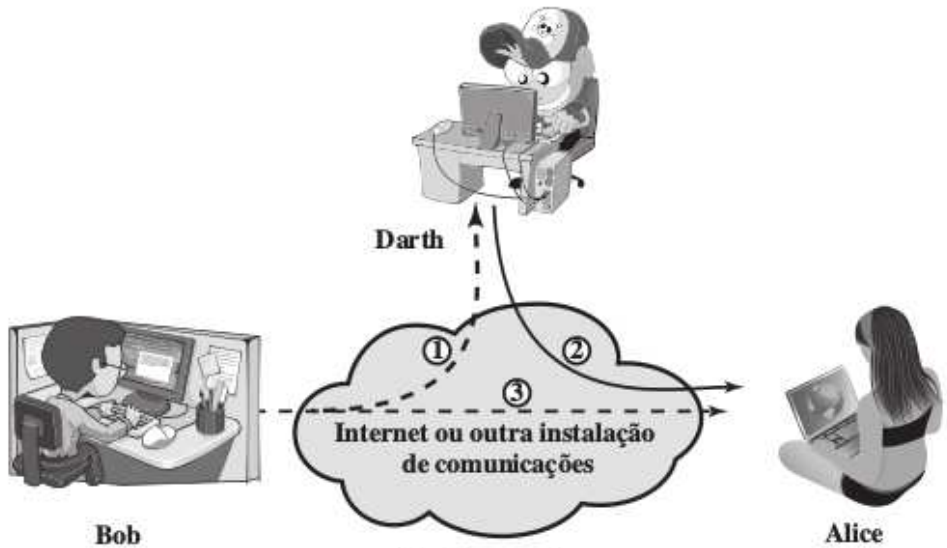
- Ameaça: é uma chance de violação da segurança que existe quando há uma circunstância, capacidade, ação ou evento que poderia quebrar a segurança e causar danos. ou seja, uma ameaça é um possível perigo a explorar uma vulnerabilidade.
- Ataque à segurança: qualquer ação que comprometa a segurança da informação pertencida a uma organização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Um ataque pode ser de forma passiva (interceptação, monitoramento e análise de pacotes) ou ativa (adulteração, fraude, reprodução e bloqueio).



(a) Ataques passivos



(b) Ataques ativos

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Mecanismos e Serviços de Segurança

- Mecanismo de segurança: um processo (ou um dispositivo incorporando tal processo) que é projetado para detectar, impedir ou recuperar-se de um ataque à segurança. Por exemplo, criptografia, assinatura digital, sistema de deteção de intruso, firewall.
- Serviço de segurança: um serviço de processamento ou comunicação que aumenta a segurança dos sistemas de processamento de dados e das transferências de informação de uma organização. Os serviços servem para frustrar ataques à segurança, e utilizam um ou mais mecanismos para isso. POr exemplo, autenticação, confidencialidade, controle de acesso.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Mecanismos e Serviços de Segurança

Incidente de segurança pode ser definido como uma ação que pode interromper os processos normais de negócio, em virtude de alguns aspectos da segurança da informação terem sido violados, seja intencionalmente ou não.

Em segurança de informação, a palavra Ativo refere-se a tudo que representa valor para a organização. Caso esse ativo seja violado, poderá trazer impactos negativos para o prosseguimento das atividades da organização. Podemos citar como ativos os programas, os equipamentos e informações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Profissionais de Segurança de Redes

O profissional que pretende atuar nessa área deve estar ciente de que ela é bastante dinâmica e envolve diversos setores da computação, como programação e desenvolvimento de sistemas, redes de computadores, sistemas operacionais e bancos de dados, entre outras. As Principais carreiras são:

- Pentester: se dedica a realizar testes de penetração é fazer a varredura de sistemas e encontrar vulnerabilidades que podem ser exploradas para obter acesso aos sistemas digitais;

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Profissionais de Segurança de Redes

- Perito Forense Digital: são responsáveis por investigar vários vazamentos de dados e incidentes de segurança, recuperar e examinar dados armazenados em dispositivos eletrônicos e reconstruir sistemas danificados para recuperar dados perdidos. Os peritos forenses também devem ajudar as autoridades a avaliar a credibilidade dos dados e fornecer consultoria especializada a profissionais do direito quando evidências eletrônicas são usadas em um caso legal.
- Engenheiro de Segurança: criação de processos que resolvam problemas de segurança na produção, a realização de testes de vulnerabilidade e até mesmo o desenvolvimento de scripts de automação que ajudarão a gerenciar e rastrear incidentes. Eles também são responsáveis por configurar, instalar e manter os sistemas de segurança e detecção de intrusões.

Profissionais de Segurança de Redes

- Analista de Segurança da Informação: administra ambientes computacionais e participa na definição da arquitetura tecnológica para segurança da informação. Analisa sistemas, levanta vulnerabilidades, mapeia riscos e implementa solução para a segurança de ambientes e dispositivos informatizados.
- Analista de Gestão de Incidentes: presta suporte aos processos de missão crítica de TI e monitora redes e servidores, acompanhando o incidente até seu tratamento e encerramento para garantir a disponibilidade de aplicações e serviços e integridade dos dados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Hacker, Cracker e outros personagens

Quem são as pessoas que fazem os ataques?

- Um *hacker* é apenas uma pessoa que detém muitos conhecimentos sobre a área de computação. Em geral, são pessoas interessadas em Sistemas Operacionais, *softwares*, segurança, internet e programação. Um *hacker* realiza ataques com interesse em descobrir coisas novas (inclusive vulnerabilidades em programas), mas não possui nenhuma motivação destrutiva.
- Cracker: é um *hacker* com propósitos maldosos de invadir e violar a integridade de sistemas. Este termo também é utilizado para programas utilizados para a mesma finalidade.
- *Script kiddies* ou *Lammer*: com pouco conhecimento de informática, usam *exploits* criados pelo *cracker* e executam ataques na internet.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Atividade

1. Pesquise na Internet empresas que trabalham especificamente com segurança da informação na grande Natal e/ou Rio Grande do Norte.
2. Pesquisa estimativas para os gastos com segurança da informação no mercado brasileiro.
3. Qual é a estimativa de custo das perdas mundiais devido a crimes e fraudes cibernéticas?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE