Introdução à Segurança da Informação

Ameaças e Vulnerabilidades – Parte I

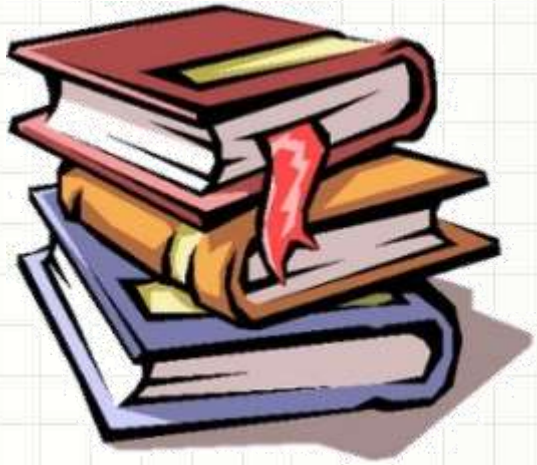
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Conhecer as principais ameaças
- Entender o mecanismo de atuação das ameaças
- Tomar contato com os principais tipos de ataques à segurança das informações

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 5)
Material Didático	Gestão de Segurança da Informação, Cap 3.
Leitura Adicional	https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf (Cartilha do CERT, pra quem não leu ainda!)

Contexto

Ameaças à Informação: Contexto

- Segurança da Informação...
  - É uma preocupação antiga!

Ameaças à Informação: Contexto

- O mundo mudou muito nas últimas décadas
  - Documentos são digitais
  - Processos são digitais
  - Uso da “nuvem”
  - Dispositivos “sempre online”
  - Todos os dispositivos sempre online...!

Maior Exposição!

Ameaças à Informação: Contexto

- Os “armários”, hoje em dia, são digitais!

Ameaças à Informação: Contexto

- Política de Segurança da Informação (PSI)
  - Regulatória x Informativa x Consultiva
  - Procedimentos e obrigações
    - Quem pode/deve o quê
  - Imprescindível!

Ameaças à Informação: Contexto

- Fontes para uma PSI (ABNT)
  - Princípios, objetivos e necessidades da organização
  - Legislação vigente (LGPD, por exemplo)
  - Avaliação de riscos
    - Identificar ameaças e vulnerabilidades

Ameaças à Segurança das Informações

Ameaças à Segurança

- Potencial de violação à segurança
  - Circunstância, ação ou evento
    - → quebra da segurança

Ameaças à Segurança

- Ameaça Organizacional
  - Situações externas
  - Tempo presente ou futuro
  - Podem afetar a empresa negativamente.

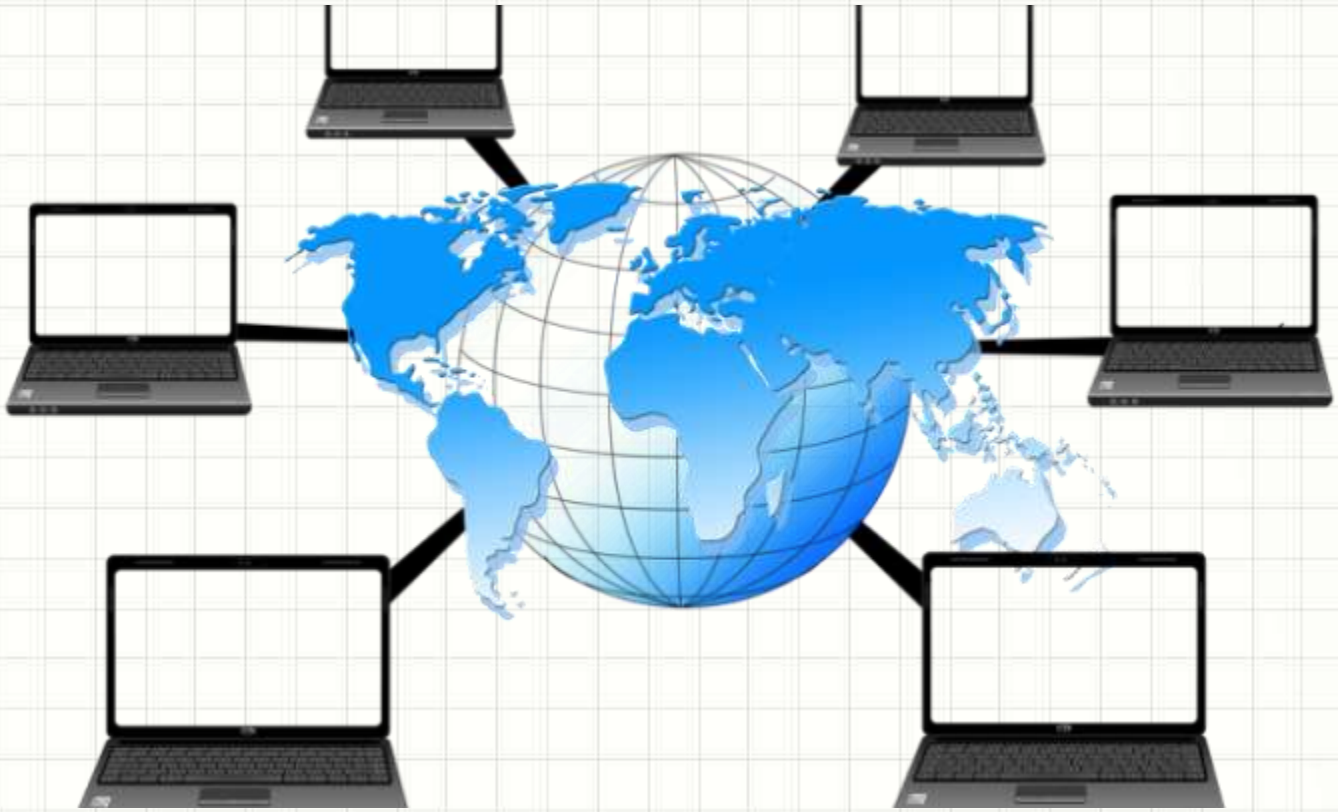
Eliminar, minimizar ou evitar

Ameaças à Segurança Organizacional

- Referem-se à perda de:
  - Integridade
    - Informação exposta ao manuseio não autorizado
  - Confidencialidade
    - Informação exposta à visualização não autorizada
  - Disponibilidade
    - Informação deixa de estar acessível no momento necessário às atividades do negócio

Ameaças à Rede ou Sistemas

- As informações e processos digitais...
  - Dependem do uso de redes e sistemas
- Ameaças podem focar nesses elementos



Aparte: Hackers x Crackers

- Hackers
  - Muito conhecimento em TIC
  - Conhecimento avançado de programação
  - Conhecimentos de eletrônica, psicologia etc...
  - Ação: dentro da legalidade(?)
  - Motivação: avanço tecnol.(?), causa(?)...

- Crackers
  - Conhecimento como o dos hackers
  - Ação: quebra da legalidade
  - Motivação: notoriedade, vingança, ganhos...

Aparte: Hackers x Crackers

- Na terminologia hackers
  - Chapéu Branco (White Hat)
  - Chapéu Preto (Black Hat)
  - Chapeu Cinza (Gray Hat)
    - Fins do White Hat
    - Meios do Black Hat



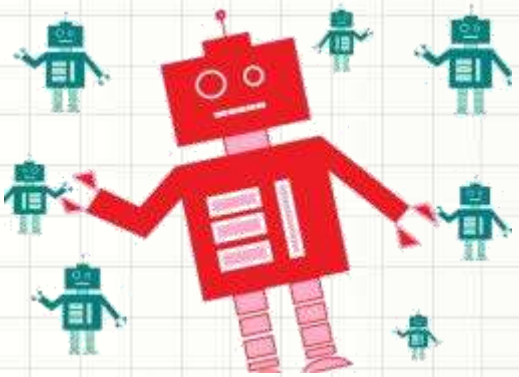
PRINCIPAIS TIPOS DE AMEAÇAS

Principais Tipos de Ameaças

- Pessoas mal intencionadas!
- Softwares do tipo "*malware*"
  - **Mal**icious Soft**ware**
  - Software que se infiltra na máquina de forma ilícita
    - Causa danos, alterações ou roubo de informações
  - Como se infiltram?
    - Vulnerabilidades de programas existentes
    - Auto-execução de mídias infectadas
    - Acesso a páginas web com navegadores vulneráveis
    - Ação direta de atacantes
    - Execução de arquivos infectados.

Principais Tipos de Ameaças

- Principais tipos de *malware*
  - Vírus
  - *Worms*
  - *Bots* e *Botnets*
  - *Spywares*
  - *Trojans*



Malwares - Vírus

- Programas que alteram softwares instalados
- Propagação: execução de arquivos infectados
  - Mídias Removíveis (Disquetes, pen drives...)
  - Comunicação (E-mails, mensagens...)
  - Repositórios
- Tipos
  - Vírus em executável (mais comum em e-mails)
  - Vírus de script (em geral vem por e-mail também)
  - Vírus de macro (em geral em documentos)
  - Vírus de smartphone (mensagens MM ou por BT).

Malwares - Worms

- Programas que alteram softwares instalados
- Propagação: automática
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores
- Processo
  - Identifica os computadores alvos
  - Envia cópias
  - Ativação (automática ou por ação do usuário)
  - Volta ao primeiro passo...

Malwares - Bots

- Programas que permitem controle da máquina
  - Por meio da rede!
  - Computador vira um “zumbi”
  - Pode-se comandar vários: Botnet

- Propagação: automática (tipo de *worm*)
  - Explorando vulnerabilidades
- Em geral consomem muitos recursos
  - Da rede e dos computadores... Quando ativos!

Malwares - Spyware

- Programas que permitem monitorar a máquina
  - Envia informação de interesse para terceiros
- Propagação: pode ser
  - Automática (worm)
  - Execução pelo usuário (vírus)
- Tipos comuns
  - Keylogger: captura as teclas pressionadas
  - Screenlogger: captura a tela da aplicação
  - Adware: mostrar propagandas

Malwares - Trojan

- Programa “legítimo”, inclui “surpresas”
  - Cartões virtuais, jogos, cracks
- Propagação: execução pelo usuário (vírus)
- Tipos comuns de Trojans
  - Downloader: baixa/exec. códigos maliciosos
  - Dropper: executa códigos maliciosos embutidos
    - Proxy: instala ou age como servidor proxy
    - Spy/Banker: instala age como spyware
  - Backdoor: habilita um backdoor (acesso remoto)
  - DoS: permite desferir ataques (bot)
  - Destrutivo: apaga coisas, formata discos...
  - Clicker: redireciona a navegação do usuário.

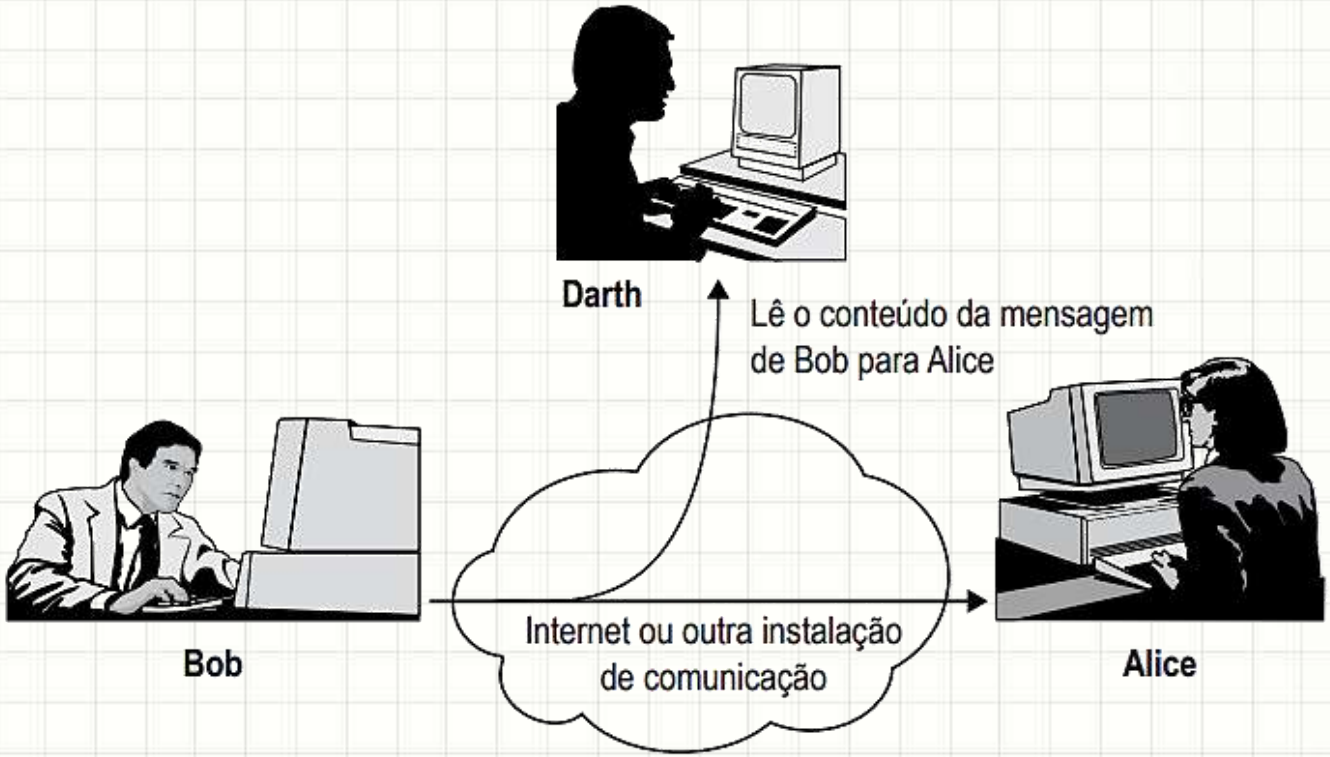
Ataques à Segurança das Informações

Ameaça x Ataque

- Ameaça
  - Potencial para a violação
  - Circunstância, capacidade, ação ou evento
  - Pode explorar uma vulnerabilidade
- Ataque
  - Tentativa de violação da PSI
  - Normalmente explora vários vulnerabilidades
  - Pode se usar de várias técnicas

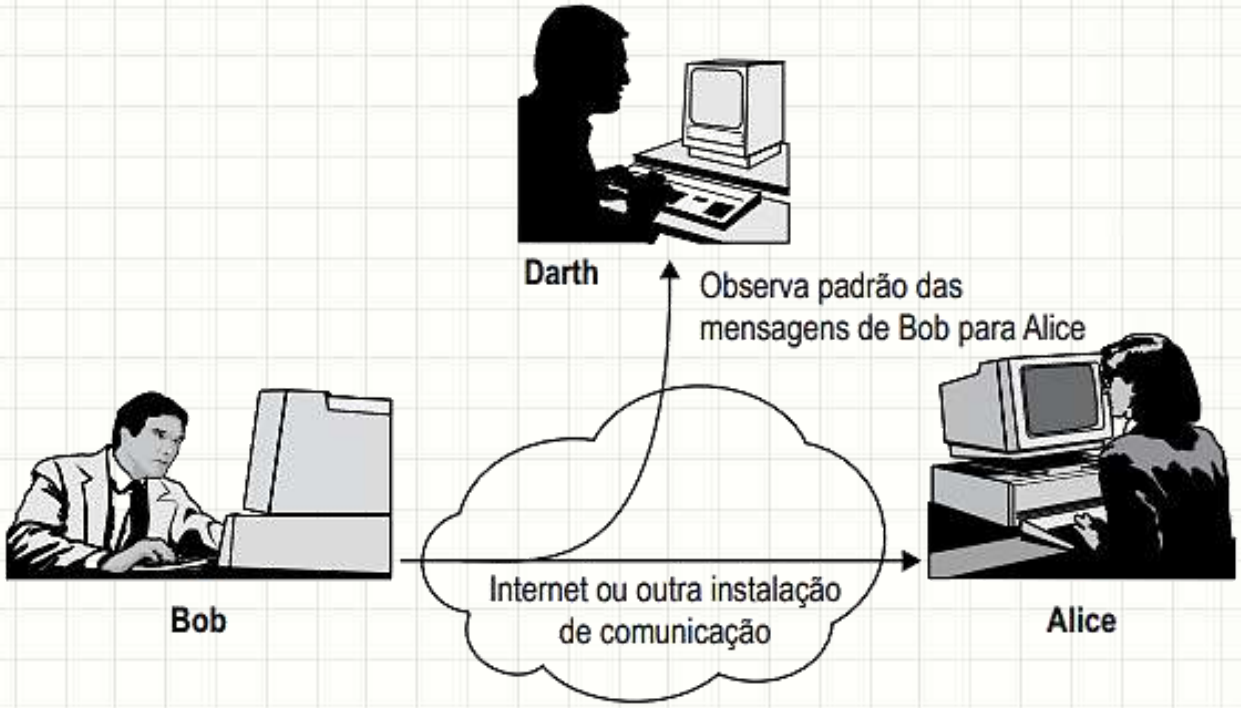
Ataques Passivos

- Monitorar transmissões
  - Objetivo: obter informações transmitidas
  - Meio: telefonia, e-mail, arquivos transferidos...



Ataques Passivos

- Análise de tráfego
  - Objetivo: obter informações sobre comunicações
  - Meio: analisar a troca e tipo de mensagens

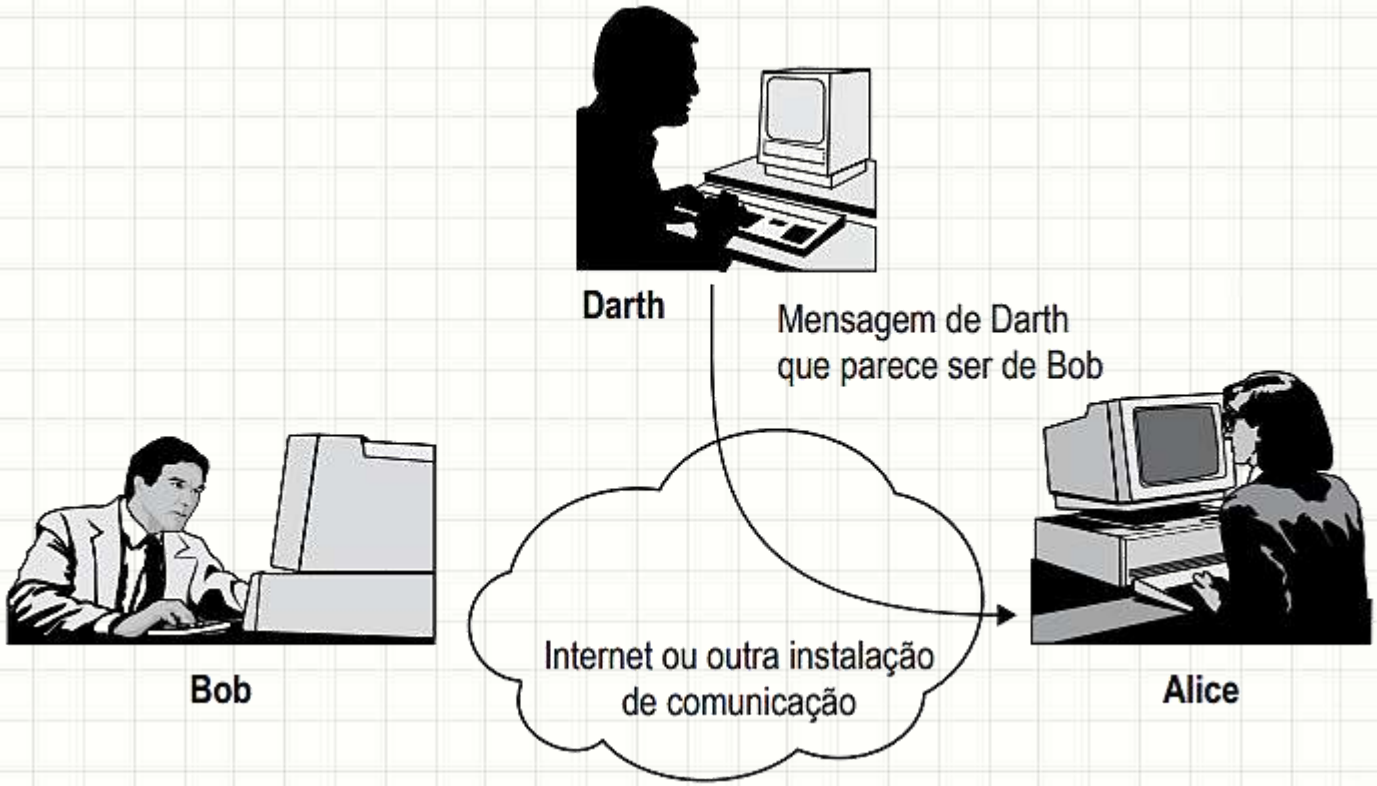


Ataques Passivos – Como Evitar

- Detecção difícil
  - Sem alterações nos dados
  - Padrão de tráfego normal (aparentemente)
  - Emissor e receptor não cientes
  - Prevenir ao invés de identificar.
- Medidas de segurança
  - Criptografia do conteúdo...
    - Não impede acompanhamento do padrão
  - Criptografia ponta-a-ponta
    - Mecanismos para garantir as pontas

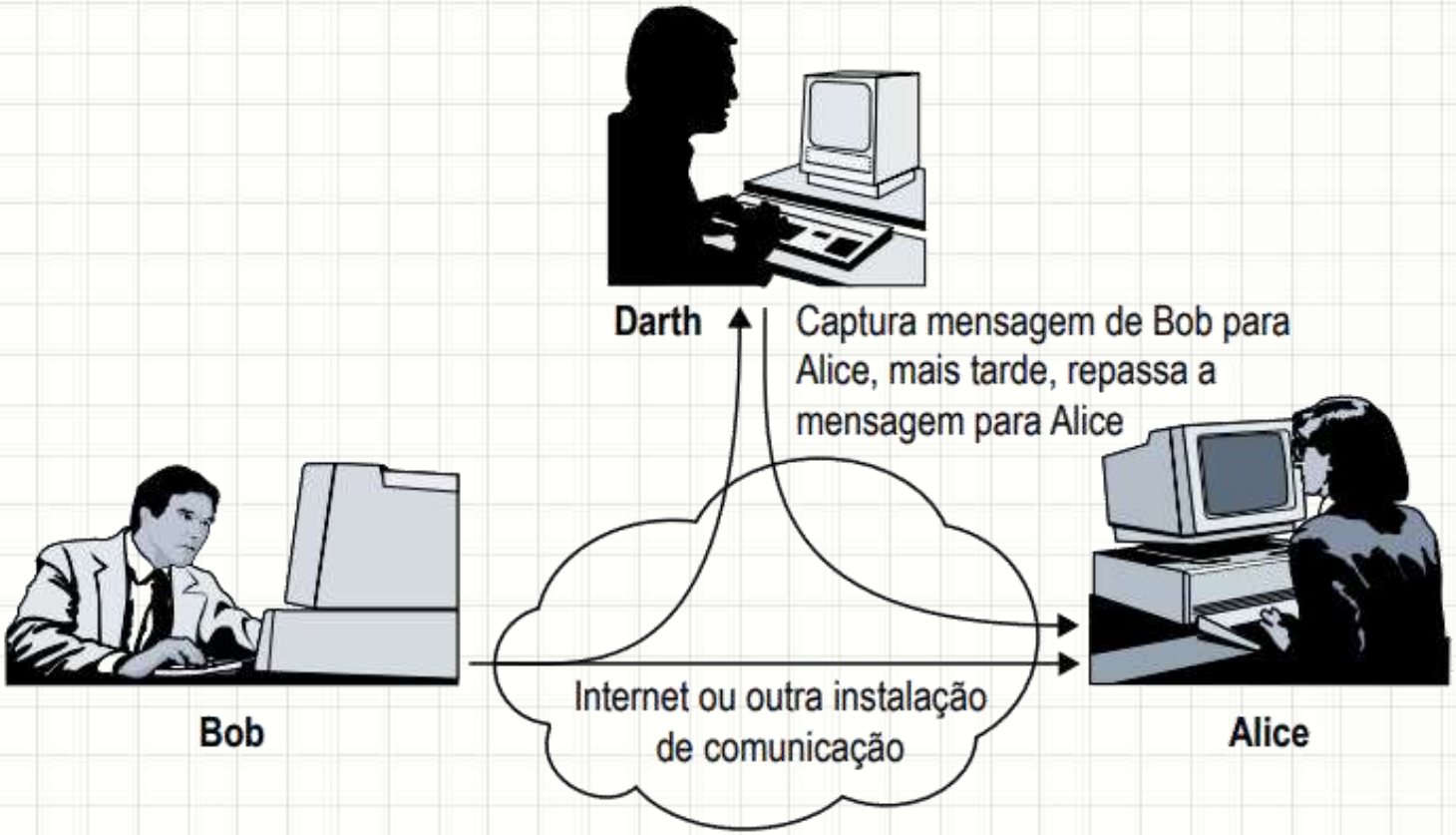
Ataques Ativos

- Personificação (ou Disfarce)
  - Meio: faz-se passar por outra pessoa
  - Em geral é porta para outros ataques ativos



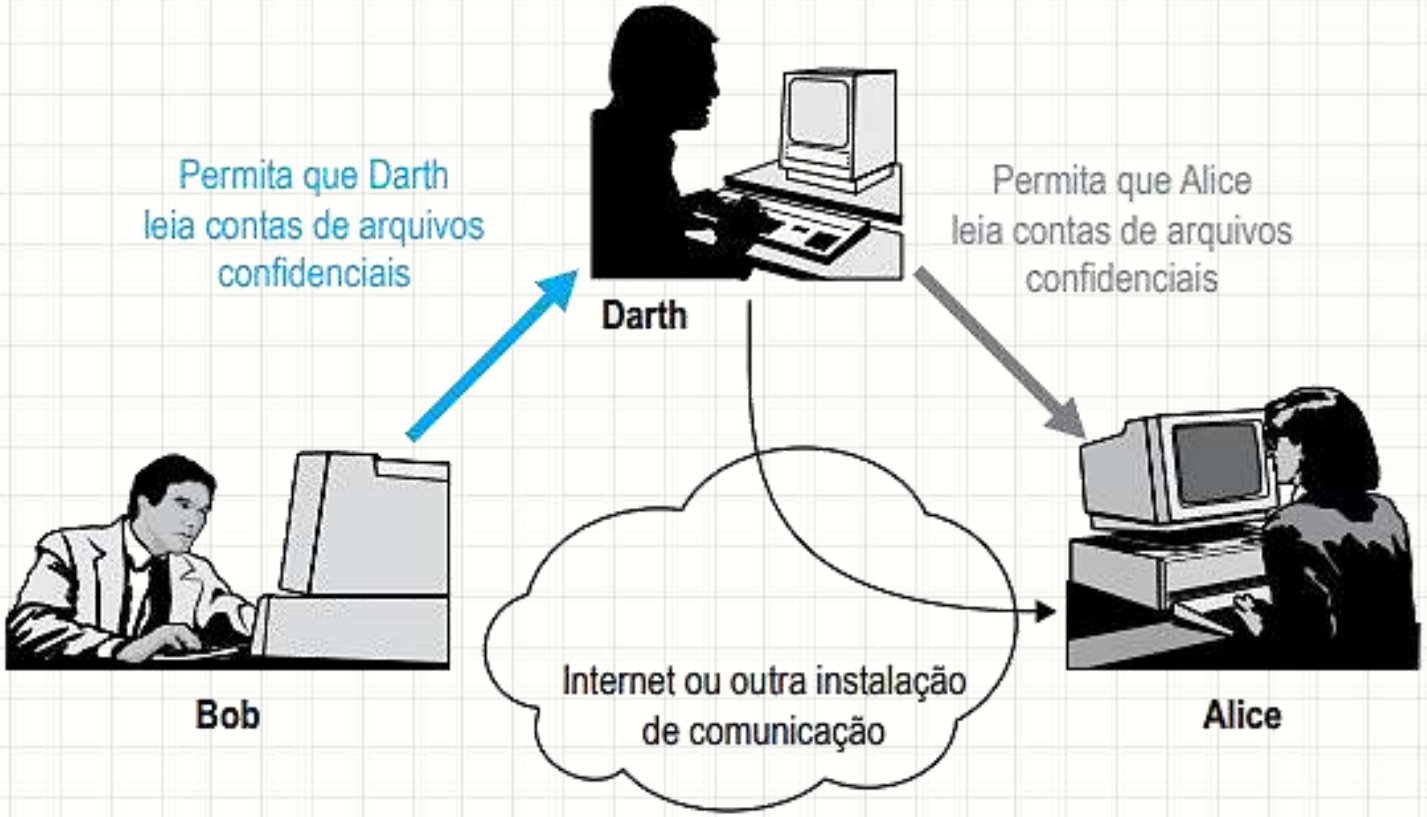
Ataques Ativos

- Repetição
  - Meio: captura mensagem e retransmite após



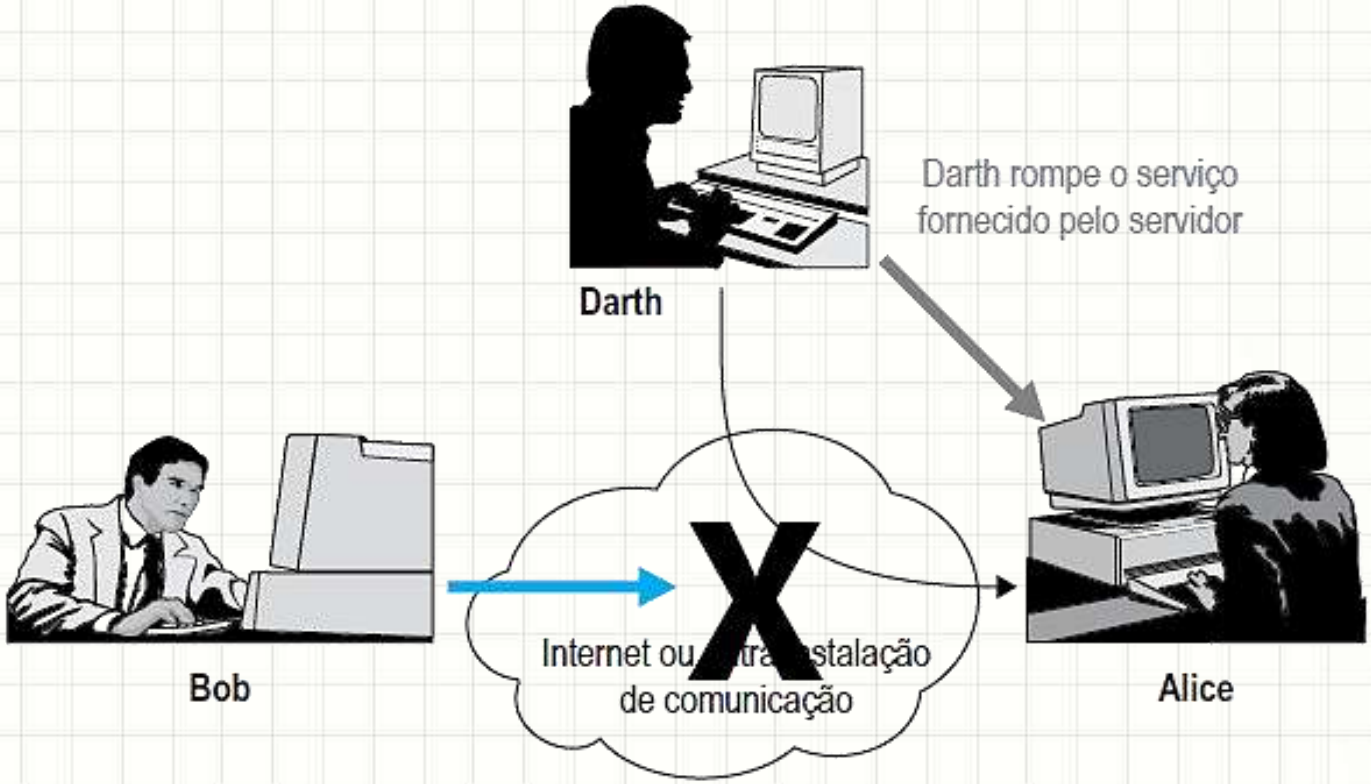
Ataques Ativos

- Modificação de Mensagens (Men in the Middle)
  - Meio: captura mensagem, altera e retransmite



Ataques Ativos

- Negação de Serviço (DoS)
  - Impedir acesso a algum serviço
  - Meio: inúmeras conexões ao serviço



Ataques Ativos – Como Evitar

- Detecção pode intimidar
  - Ajuda na prevenção
- Medidas de segurança
  - Muito difícil impedir
    - Muitas vulnerabilidades!
  - Detectar e reagir
    - Recuperar interrupções e atrasos
  - Assinatura digital/criptografia ponta-a-ponta ajuda
    - Mecanismos para garantir as pontas

QUESTÕES

Questão 1

01. Existem três fontes principais para que uma organização identifique seus requisitos de segurança. Sobre esta afirmação, leia as asserções e assinale a alternativa correta.

I. A primeira fonte é um conjunto de princípios, objetivos e necessidades para o processamento da informação;

II. A segunda fonte é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais;

III. As duas primeiras fontes são utilizadas como referências para desenvolver a principal fonte de requisitos de segurança, que é derivada da avaliação de riscos.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções I, II e III estão corretas.

Questão 2

02. As ameaças à segurança de uma organização estão sempre relacionadas com a perda de uma ou mais das seguintes características, as quais:

I. Perda de integridade.

II. Perda de confidencialidade.

III. Perda de performance.

a) Está correta somente a asserção I.

b) Está correta somente a asserção II.

c) Está correta somente a asserção III.

d) Estão corretas somente as asserções I e II.

e) Estão corretas somente as asserções II e III.

Conclusões

Resumo e Próximos Passos

- Ameaças x Ataques
- Principais tipos
  - E suas características
- Mecanismos para evitar...
  - Ameaças e ataques

- Vulnerabilidades
  - Quais são as principais?
  - Como identificá-las?
  - Como agir a respeito?

PERGUNTAS?