Introdução à Segurança da Informação

Ameaças e Vulnerabilidades parte III e Ataques Cibernéticos

Prof. Dr. Daniel Caetano

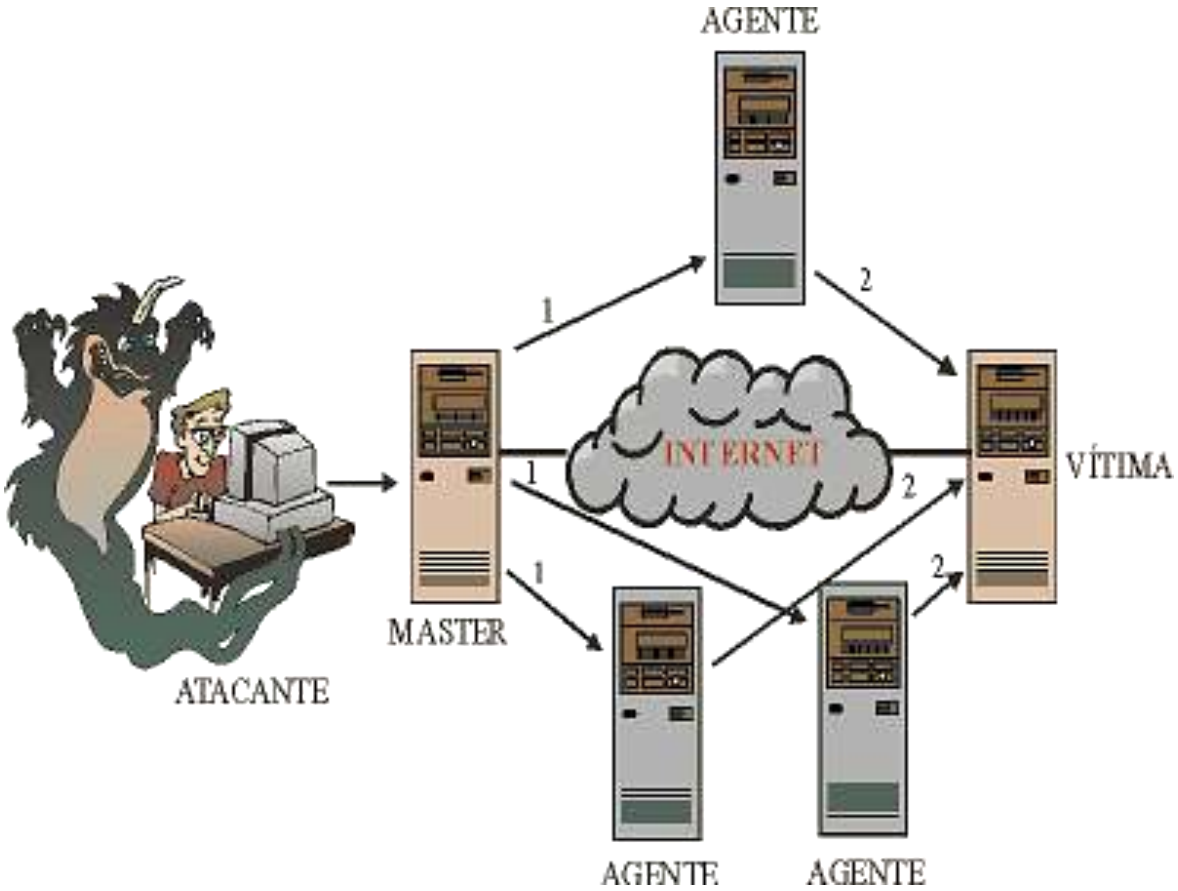
2021 - 1

Compreendendo o problema

- **Situação:** só no Brasil, ocorrem em média 17 tentativas de fraude por segundo (Serasa Experian), a maioria pela internet.

Quais os principais golpes na Internet?

Anatomia de um ataque

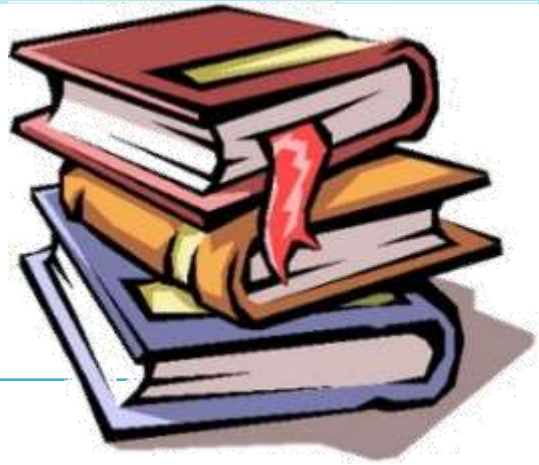


https://video.cisco.com/video/5175269310001

Objetivos

- Tomar contato com os principais tipos de ataques à segurança das informações
- Conhecer as principais vulnerabilidades
- Tomar contato com sistemas de identificação de vulnerabilidades

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 4)
Biblioteca Virtual	Fundamentos de Segurança da Informação: com base na ISO 27001 e 27002, do item 12.4 a 12.5
Material Didático	Gestão de Segurança da Informação, Caps 2 e 3
Leitura Adicional	Pra quem não leu ainda: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf (Cartilha do CERT, caps. 2 a 6) https://www.netacad.com/ (Introduction to Cybersecurity - Cisco)

VULNERABILIDADES

Vulnerabilidades

- O que são?
  - Pontos fracos existentes nos ativos

  - Quando explorados, afetam
    - Integridade, disponibilidade e confidencialidade.

Vulnerabilidades

- Não seriam um problema se...
  - Não houvesse ameaças que as explorem
  - Mas as ameaças existem!

  - E com a evolução...
    - As vulnerabilidades tendem a aumentar

Pontos fracos devem ser eliminados!

Identificando Vulnerabilidades

- Identificar falhas de segurança
- Ponto de partida?
  - Lista de ativos (soft, hard, processos, pessoas...)
  - Lista de ameaças

- Processos
  - Fontes de vulnerabilidades
  - Testes de segurança
  - Lista de verificação de requisitos
- Segundo ABNT
  - Testes e simulações (incluindo invasão)
  - Auditorias em códigos fonte

PRINCIPAIS VULNERABILIDADES

Tipos de Vulnerabilidades

- São 7 os tipos de vulnerabilidades:
  1. Naturais
  2. Físicas
  3. Hardware
  4. Software
  5. Armazenamento
  6. Comunicação
  7. Humanas

1. Vulnerabilidades Naturais

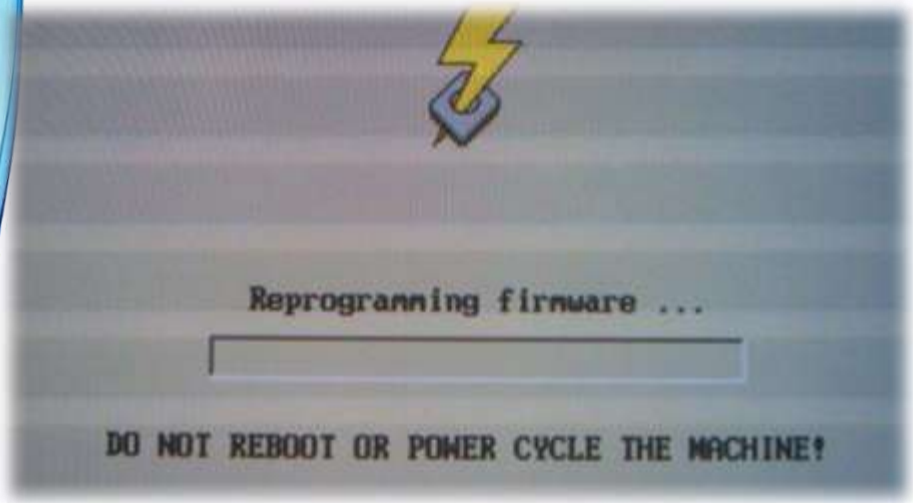
- São aquelas decorrentes de fenômenos naturais e que trazem riscos para equipamentos e informações
  - Ex. : inundações, terremotos, maremotos...

2. Vulnerabilidades Físicas

- São ambientes que possuem pontos fracos em nível de espaço físico, comprometendo a segurança dos equipamentos e informações
  - Ex.: espaço inadequado para trabalho, falta de extintores de incêndio, pessoas não autorizadas transitando no local...

3. Vulnerabilidades de Hardware

- São aquelas relacionadas à defeitos de fabricação ou configuração inadequada podendo permitir ataques
  - Ex.: falta de atualização de firmware, equipamentos mal dimensionados...



4. Vulnerabilidades de Software

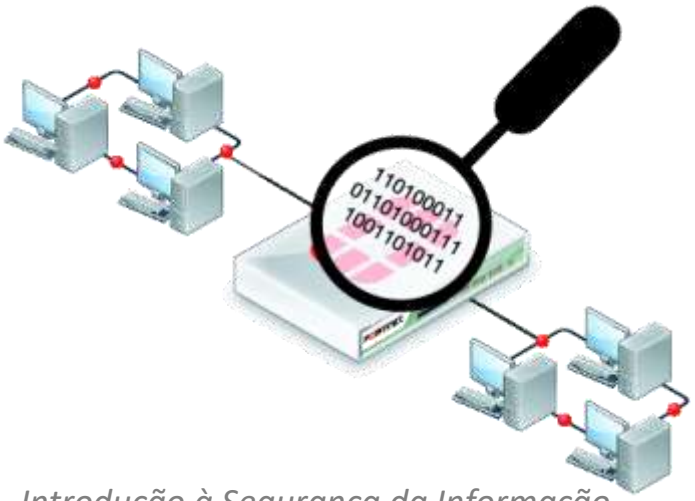
- Falhas em programas que permitam acesso não autorizado aos equipamentos.
  - Ex.: aplicativos mal configurados, programas de e-mail que permitem execução de código, programas desatualizados...

5. Vulnerabilidades de Armazenamento

- Falha ou uso inadequado do suporte físico, podendo comprometendo a segurança dos dados
  - Ex.: equipamento além da vida útil, defeitos de fabricação, prazo de validade das mídias...

6. Vulnerabilidades de Comunicação

- São as relacionadas ao tráfego de informação, seja por cabo de cobre, fibra, ondas de rádio ou satélite, permitindo eventuais intervenções de terceiros.
  - Ex.: Sniffer na rede, interrupção da comunicação...



7. Vulnerabilidades Humanas

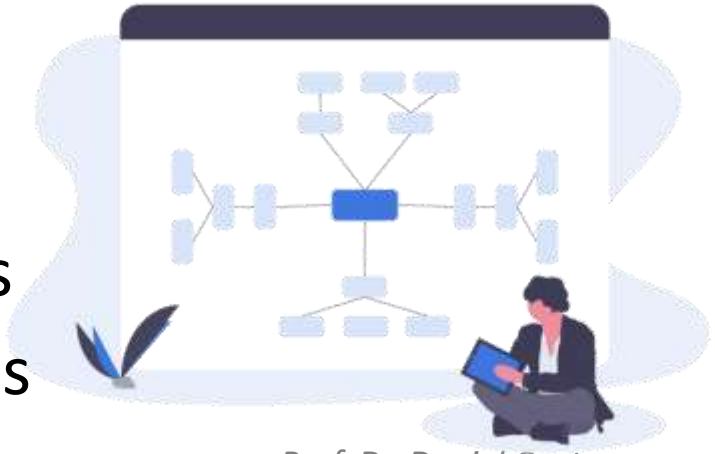
- São aquelas relacionadas à atitudes humanas inadequadas, intencionais ou não, que possam colocar em risco a segurança da informação
  - Ex.: Uso de senhas fracas, compartilhamento de credenciais, desconhecimento da política de segurança, funcionários descontentes...

Ferramentas para Análise de Vulnerabilidades

Por Que Usar Ferramentas?

- Não há como evitar 100% dos ataques
- Análise de Risco
  - Permitir identificar os maiores riscos
    - Probabilidade x Impacto
    - Associados à ameaças e **vulnerabilidades**
  - Base em vulnerabilidades conhecidas...
    - E as desconhecidas?

- Mapear as vulnerabilidades
  - Para mitigá-las ou eliminá-las
  - Sempre observando os custos



Quais Ferramentas?

- Prevenção Básica
  - Antivírus/Antimalware: identifica, desativa ou elimina esses tipos de ameaças. Atua no lado da “ameaça”
  - Firewall: controla o que entra e sai em um equipamento ou uma rede. Atua no lado da “vulnerabilidade”
  - Comunicação segura (SSL/HTTPS): codifica os dados ponta a ponta. Atua no lado da “vulnerabilidade”
- Ferramentas de busca
  - Scanners: identificam vulnerabilidades
    - Maneira automatizada

Exemplos de Ferramentas

- NMAP
  - Detecta portas abertas no equipamento
  - Base para teste de firewall e sistemas de intrusão
- LanGuard
  - Registra eventos de rede e pesquisa vulnerabilidades na rede
  - Indica correções para as vulnerabilidades
- NESSUS
  - Cliente-Servidor, analisa vulnerabilidades remotas
  - Plugins para testes de vulnerabilidades específicas

Exemplos de Ferramentas

- Lynis
  - Analisa vulnerabilidades em geral, gerando um relatório de ações para corrigí-las
- Chkrootkit / rkhunter
  - Verifica se arquivos do sistema estão comprometidos
- Tripwire
  - Registra mudanças em arquivos e gera relatórios periódicos sobre as mesmas

Exemplos de Ferramentas

- SSL Test (SSL Labs)
  - Analisa vulnerabilidades nas conexões SSL
  - https://www.ssllabs.com/ssltest/
- ImmuniWeb
  - Verifica falhas em sites, aplicativos etc
  - https://www.immuniweb.com/
- Zaproxy
  - Verifica falha em sites
  - https://www.zaproxy.org/

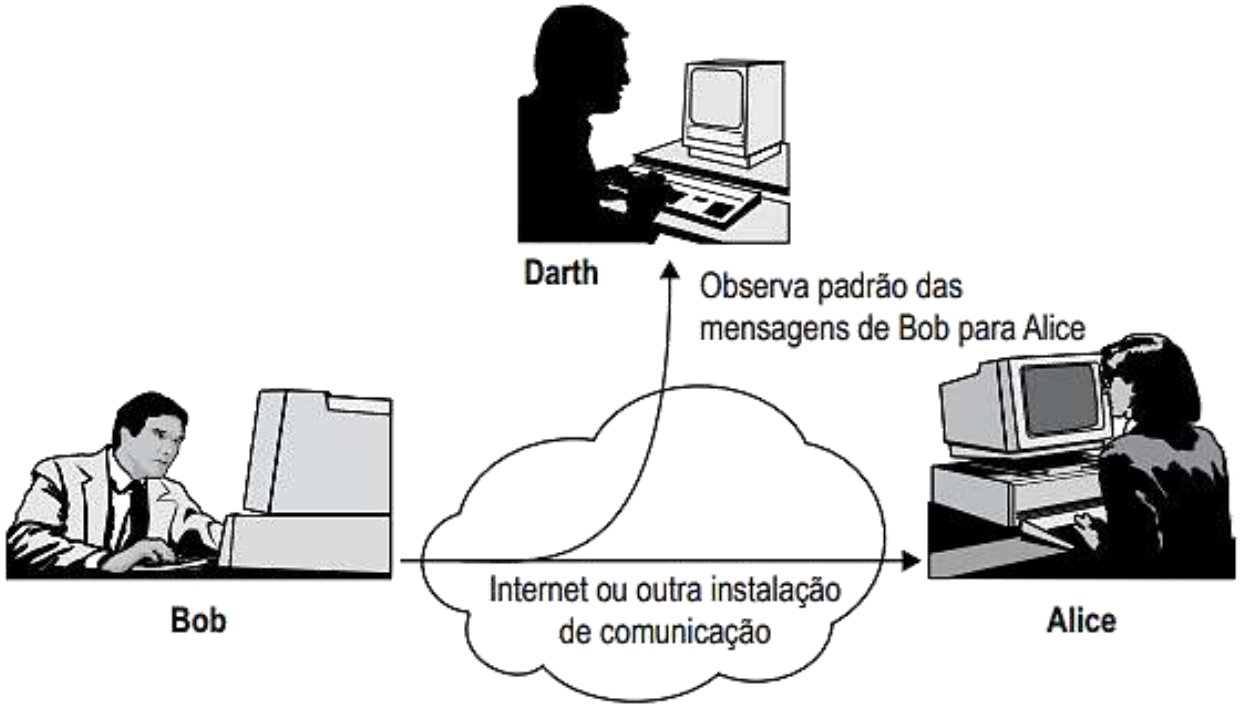
Ataques à Segurança da Informação

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 várias vulnerabilidades
  - Pode se usar de várias técnicas

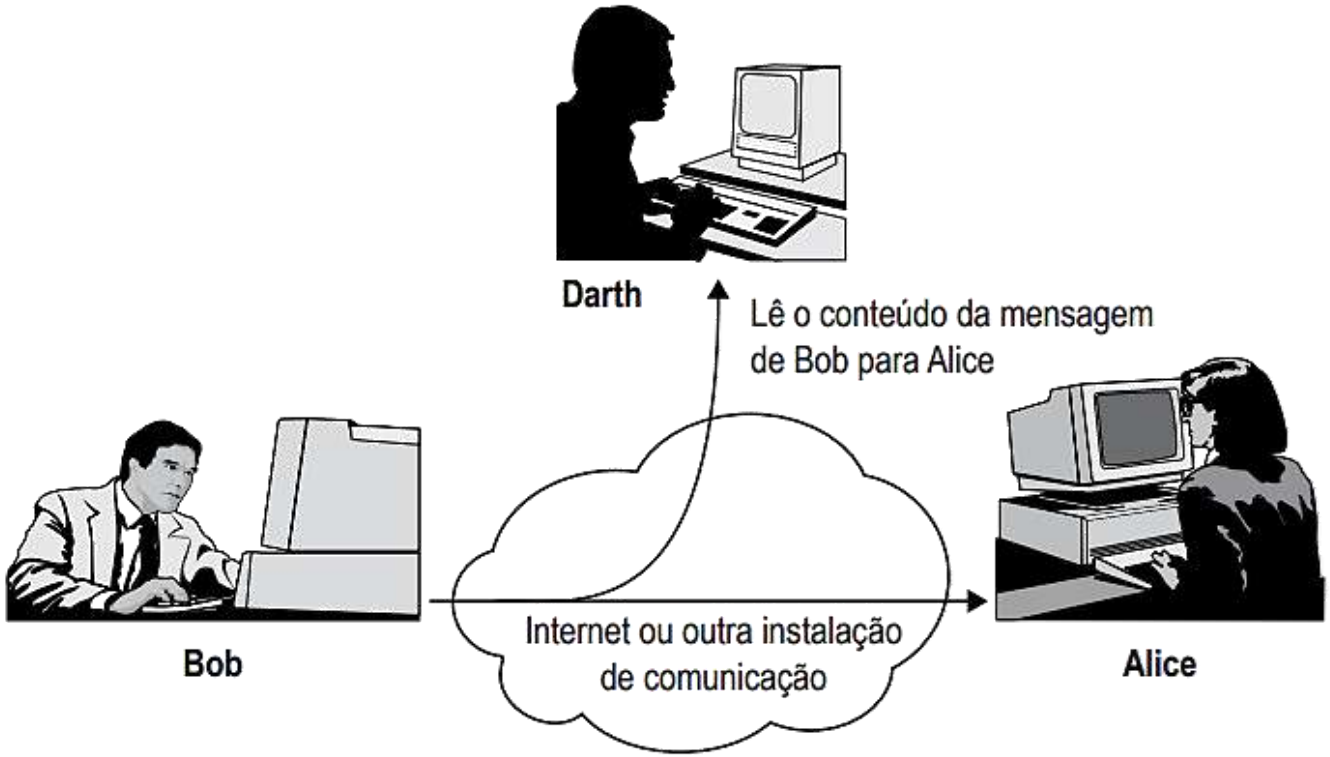
Ataques Passivos

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



Ataques Passivos

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

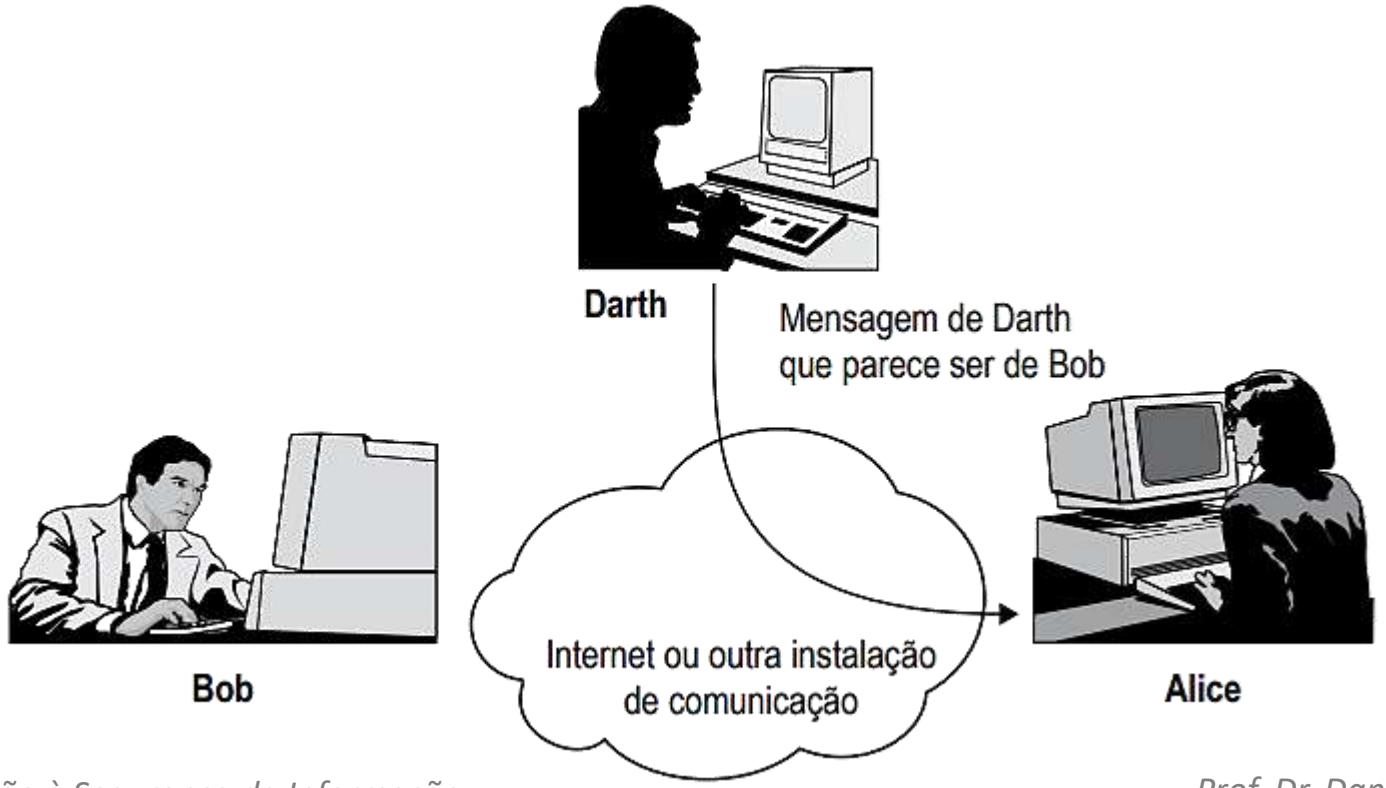


Ataques Passivos – Como Evitar

- 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

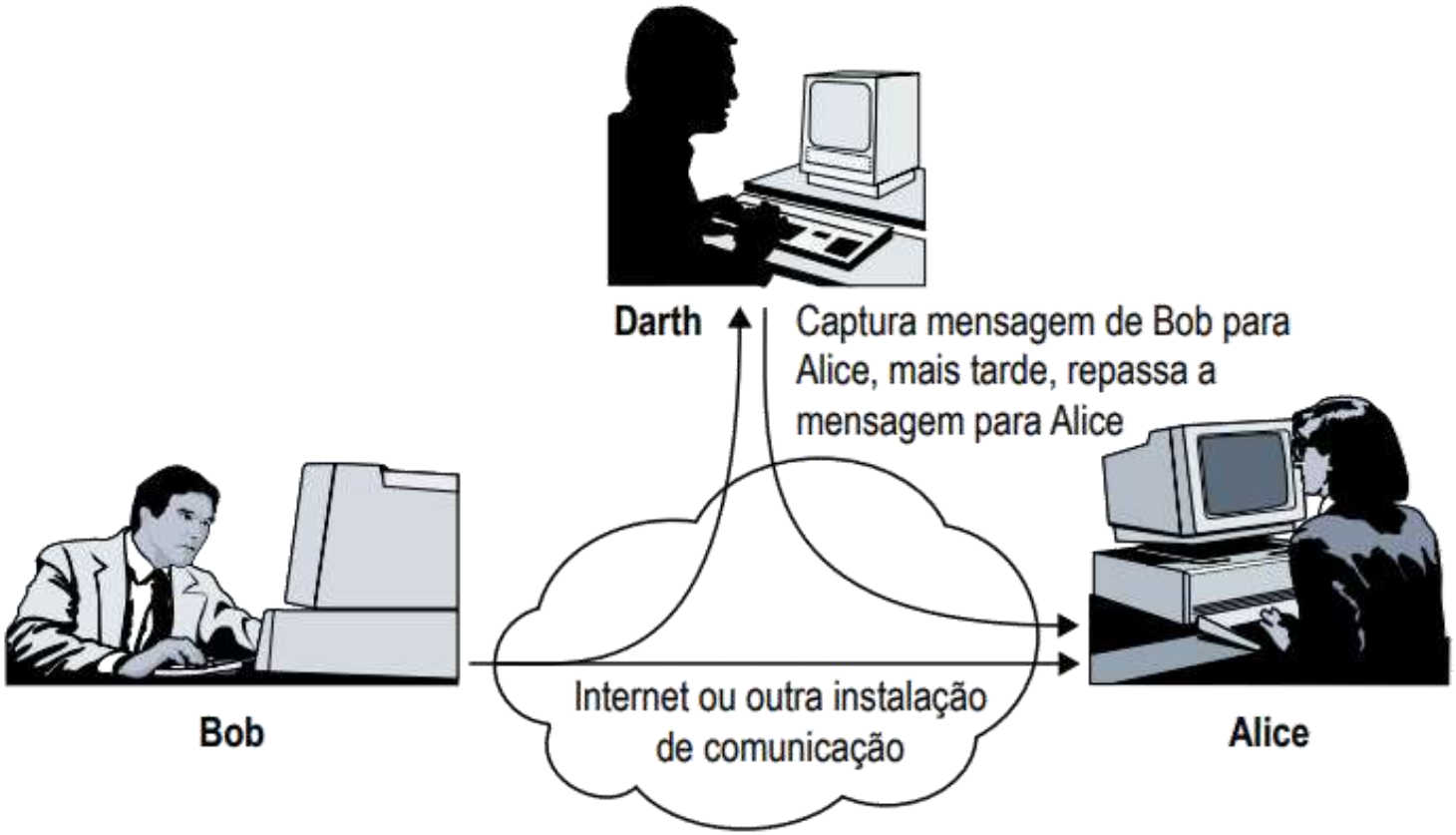
Ataques Ativos

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



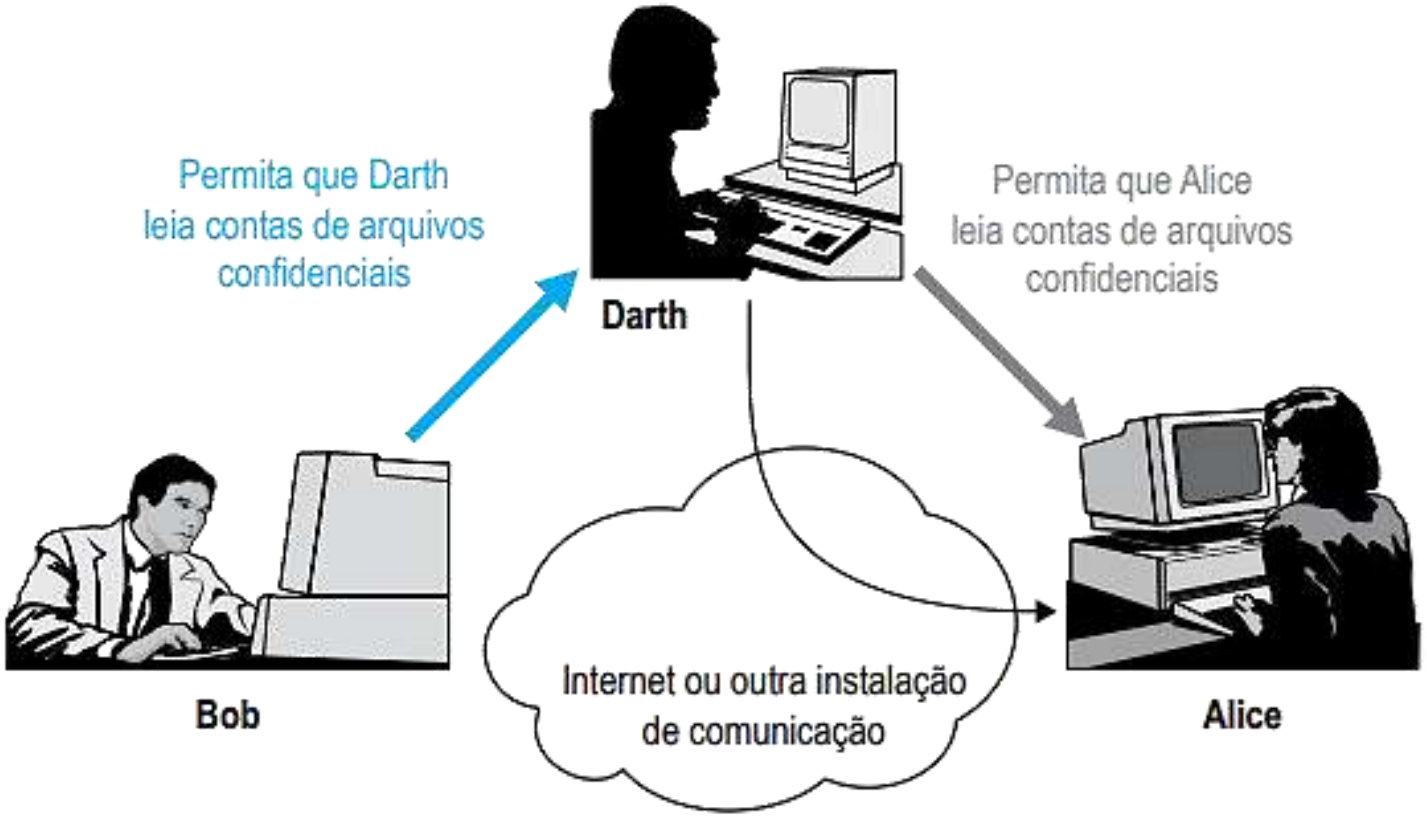
Ataques Ativos

- Repetição
  - Meio: captura mensagem e retransmite após



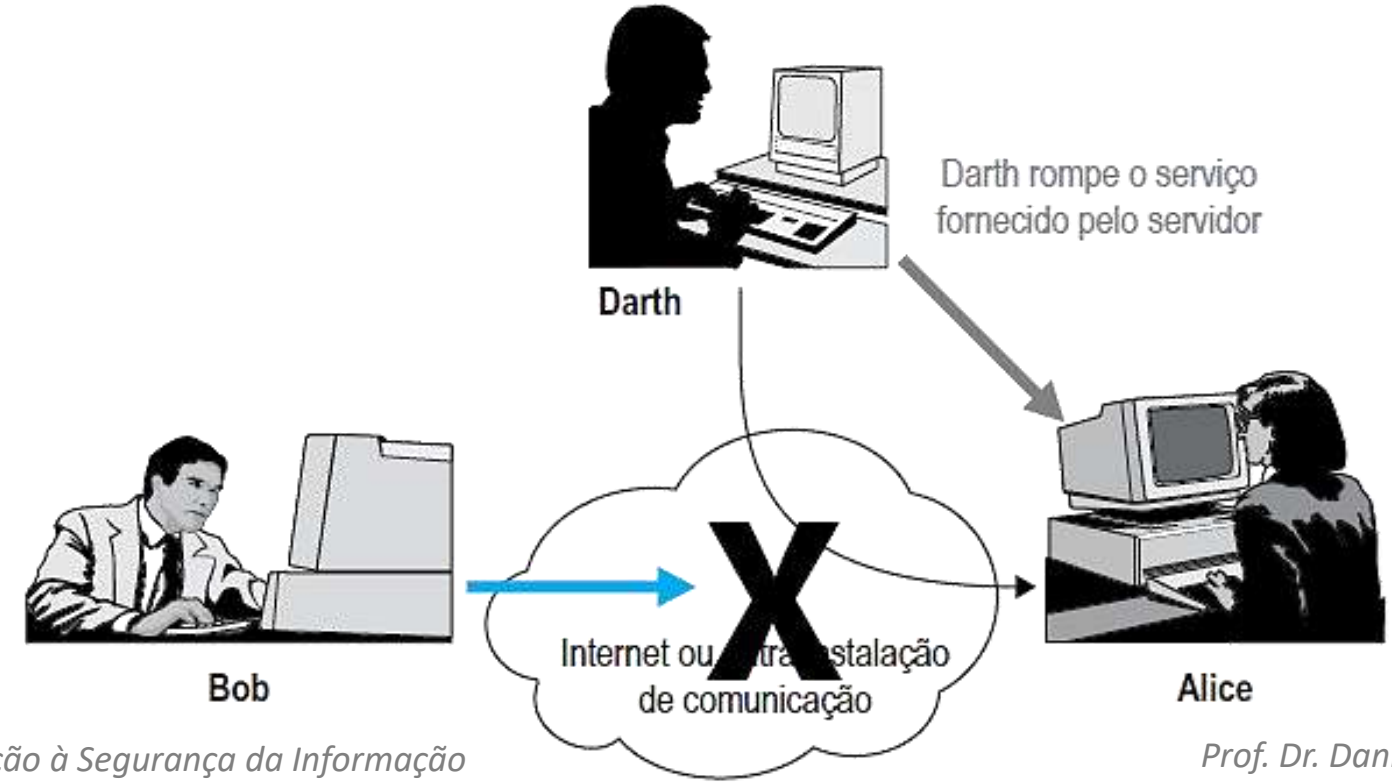
Ataques Ativos

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



Ataques Ativos

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



Outros Ataques Ativos

- *Defacement*
  - Adulteração de website/serviço
- *Injection (SQL Injection, XSScripting etc.)*
  - Executar código no servidor explorando falha
- Invasão... vários tipos. Exemplos:
  - Acesso por força bruta/dicionário (ou eng. social)
  - *Wardriving / Warbiking / Warjogging*
    - Buscar WiFi vulnerável de carro/bike/a pé
  - *Warkitting*
    - Como acima, mas para aplicar *rootkit* no roteador

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

Golpes e Fraudes

- Ludibriar o usuário
  - Usuário fornece dados sensíveis
- Tipos comuns
  - Scam/Phishing: site falso, usualmente por mensagems (e-mail, sms, WhatsApp, notificações)
    - Bancos (recadastramento, etc.)
    - Sites de compras, receita federal etc.
  - *Pharming*: site falso – alteração no hosts/DNS
    - Mais grave que *phishing*!
    - Bancos (recadastramento, etc.)
    - Sites de compras, receita federal etc.

Golpes e Fraudes

- Tipos comuns
  - Sequestro: roubo de identidade de aplicativos (WhatsApp, por exemplo)
    - Variante: sequestro de sessão (*Session Hijacking*)
      - Força bruta x acesso por cookie x cálculo
  - Aluguel de Conta: uso de conta para golpes
  - Falso Pagamento: comprovantes adulterados
  - *Hoax*
    - Boatos que induzem ação do usuário
    - Apócrifos ou de autoria duvidosa, conteúdo apelativo
    - Exploram lado emocional

Golpes e Fraudes – Como Evitar

- Atenção aos detalhes
  - Endereço do link, confirme os depósitos no banco...
- Nunca entre em sites por link no e-mail
  - Sempre digitando na barra de endereços
- Confira o certificado digital
  - Cadeado do navegador
- Procure se o site é confiável
  - Reclame aqui, eBit, Seguro & Confiável
  - Confira endereço físico, CNPJ etc.

IoT e Segurança

IoT e Segurança

- O que é IoT?
  - Internet of Things
  - “Internet das Coisas”
- Esse mundo do “tudo interligado”
- Comunicação sem intervenção do usuário

Que desafios de segurança isso traz?

Mentimeter

Anatomia de um ataque IoT

https://youtu.be/TWX0m8bdwqQ

ATIVIDADE AVALIATIVA

Atividade Avaliativa [para casa!]

- Grupos de 4 a 7, vale 2,0 ponto na AV1
- Revejam o vídeo

  https://youtu.be/TWX0m8bdwqQ

- O que deve ser feito:
  - Uma apresentação de slides
  - Listar membros do grupo no 1º slide
  - Tipos de ataques, alvos, vulnerabilidades, ações
- Entrega pelo Teams
  - Até 25:59 do dia 03/05/2021 (para valor total)

ATIVIDADE

Atividade

- Grupos – 15 minutos
  - Conforme canais do Teams
- Pesquise e discuta com seu grupo e elabore uma lista com os mais importantes (para o grupo):
  - 2 tipos de malware
  - 2 tipos de golpes ou ataques pela internet
- Quando chegar a vez do grupo, apresente os tipos selecionados e explique porque o grupo os considera os mais importantes.

ENCERRAMENTO

Resumo e Próximos Passos

- Tipos de ataques...
  - E dicas para evitá-los
- Principais vulnerabilidades
- Ferramentas para detecção
  - Prevenção e scanners
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Mecanismos de Controle
  - Segurança Física x Lógica
  - Controle de Acesso

PERGUNTAS?