Capítulo 1: Roteiro

1.1 O que é a Internet?

1.2 Borda da rede

- sistemas finais, redes de acesso, enlaces

1.3 Núcleo da rede

- comutação de circuitos, comutação de pacotes, estrutura da rede

1.4 Atraso, perda e vazão nas redes comutadas por pacotes

1.5 Camadas de protocolo, modelos de serviço

1.6 Redes sob ataque: segurança

1.7 História

Segurança de rede

- o campo da segurança de rede trata de:
  - como defender as redes contra ataques
  - como maus sujeitos atacam redes de computadores
  - como projetar arquiteturas imunes a ataques
- Internet não criada originalmente com (muita) segurança em mente
  - *visão original:* "um grupo de usuários mutuamente confiáveis conectados a uma rede transparente"
  - projetistas de protocolos da Internet brincando de "contar novidades"
  - considerações de segurança em todas as camadas!

Maus sujeitos podem colocar malware em hospedeiros via Internet

- malware pode entrar em um hospedeiro por vírus, worm ou cavalo de Troia.
- malware do tipo spyware pode registrar toques de teclas, sites visitados na Web, enviar informações para sites de coleta.
- hospedeiro infectado pode ser alistado em um botnet, usado para spam e ataques de DDoS.
- malware normalmente é autorreplicável: de um hospedeiro infectado, busca entrada em outros hospedeiros

- cavalo de Troia
  - parte oculta de algum software útil
  - hoje, normalmente em uma página Web

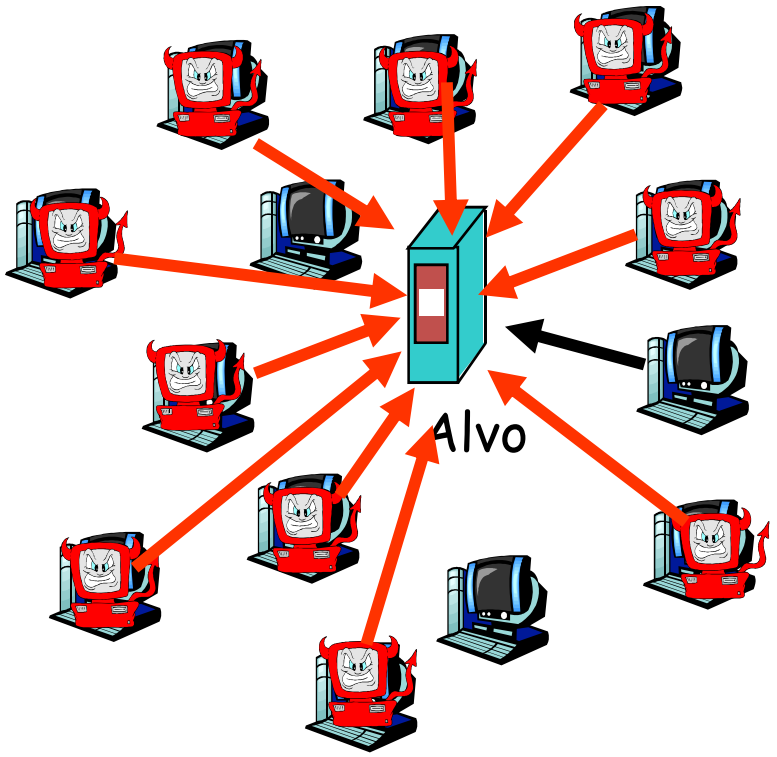
    (Active-X, plug-in)
- vírus
  - infecção ao receber objeto (p. e., anexo de e- -mail), executando ativamente
  - autorreplicável: propaga- -se para outros hospedeiros, usuários

- worm:
  - infecção recebendo passivamente objeto a ser executado
  - autorreplicável: propaga-se para outros hospedeiros, usuários

Maus sujeitos podem atacar servidores e infraestrutura de rede

- Denial of Service (DoS): atacantes deixam recursos (servidor, largura de banda) indisponíveis ao tráfego legítimo, sobrecarregando recurso com tráfego

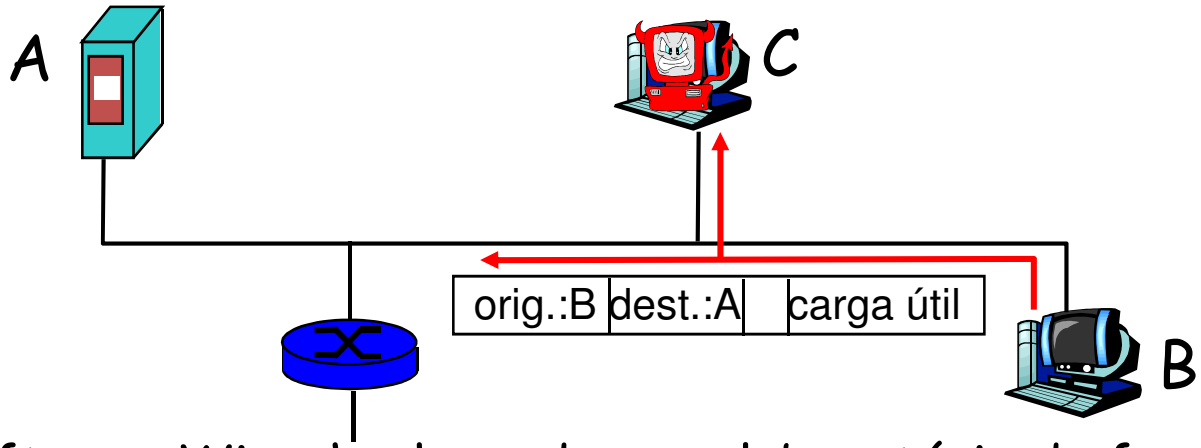
1. selecionar alvo
2. invadir hospedeiros na rede (ver botnet)
3. enviar pacotes para o alvo a partir dos hospedeiros comprometidos



Maus sujeitos podem farejar pacotes

Farejamento de pacotes:

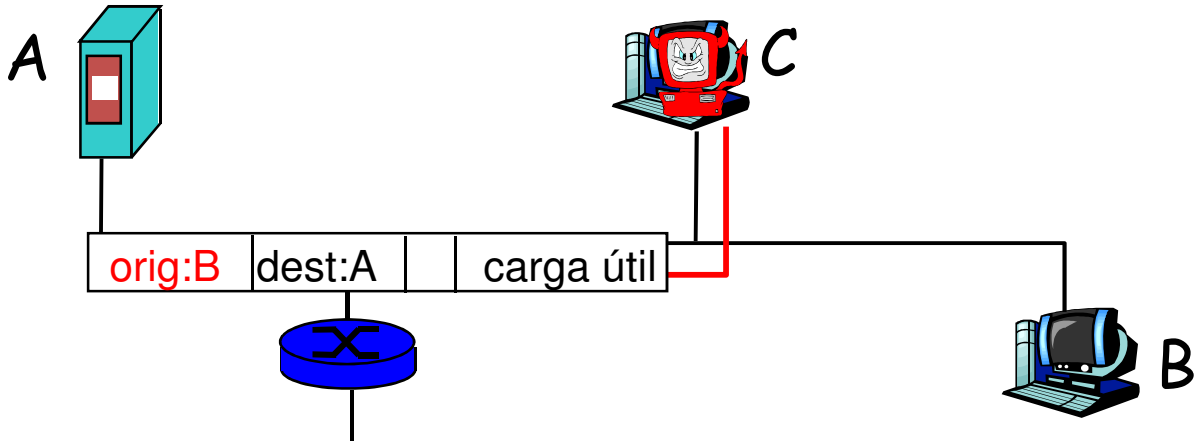
- meio de broadcast (Ethernet compartilhada, sem fio)
- interface de rede promíscua lê/registra todos os pacotes (p. e., incluindo senhas!) passando por



- software Wireshark usado para laboratório do farejador de pacotes do final do capítulo (gratuito)

Maus sujeitos podem usar endereços de origem falsos

- *IP spoofing:* enviar pacote com endereço de origem falso



Maus sujeitos podem gravar e reproduzir

- *gravar-e-reproduzir*: informação confidencial (p. e., senha), é usada mais tarde
  - quem tem a senha *é* esse usuário, do ponto de vista do sistema