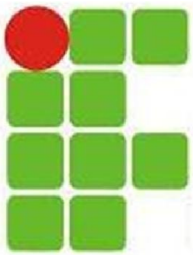
Informática

Professor: Diego Oliveira



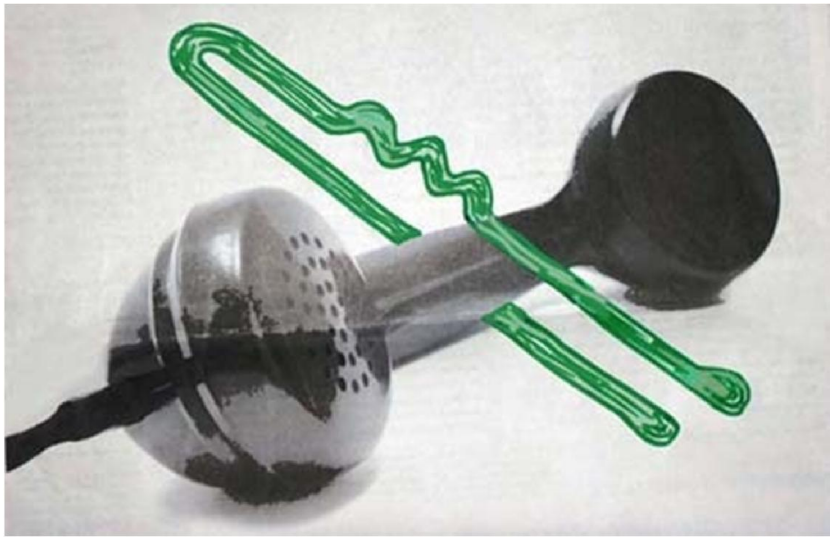
Conteúdo 02:
Segurança da Informação

Conteúdo da Aula

- Tipos de Ataque
- Golpes na Internet
- Ataques na Internet
- Malwares
- Spam
- Outros Riscos
- Mecanismos de Segurança
- Segurança de Redes

Interceptação

- Ataca a confidencialidade da informação
- O maior exemplo é o grampo telefônico que permite a um terceiro não autorizado a escuta da conversa



Interrupção

- Ataca a disponibilidade do serviço
- O exemplo clássico é o DDoS (Distributed Denial of Service) que derruba os serviços temporariamente

Modificação

- Ataca a integridade da informação
- Um exemplo é a alteração de contas online ou dados locais por terceiros não autorizados

Golpes na Internet

- Roubo de Identidade
- Phishing
- Pharming
- Hoax (Boato)
- Sites de e-commerce
- Sites de namoro

Ataques na Internet

- Exploração de vulnerabilidades
- Varredura em redes (Scan)
- E-mail Spoofing
- Interceptação de tráfego (Sniffing)
- Força Bruta
- Defacement
- Negação de Serviço (Denial of Service – DoS)

Malwares

- **Mal**icious Soft**ware**
  - Vírus
  - Worms
  - Bot e BotNet
  - Spywares
  - Adware
  - Cavalos-de-Tróia
  - Bombas Lógicas
  - Backdoor
  - Rootkit

Vírus

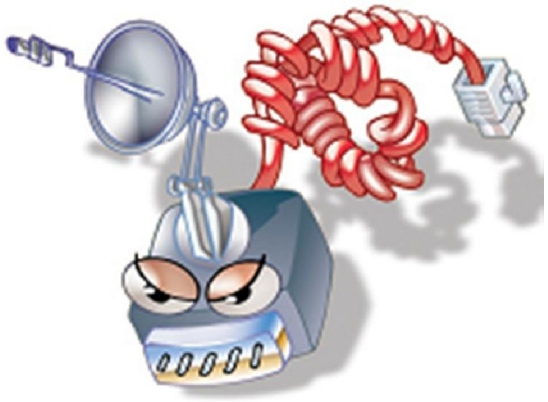
- Programa malicioso
- O vírus se replica em arquivos do PC
- Precisa de um hospedeiro para reprodução
- Se reproduz geralmente no mesmo PC
- Pode realizar diversas atividades
  - Desativar portas USB
  - Aumentar processamento
  - Usar memória RAM

Worm

- Capaz de se propagar automaticamente através da rede
- Não precisa de outros programas para se replicar e propagar

- Sua replicação explora as vulnerabilidades
- Consume recursos e degrada o desempenho
- Capaz de gerar negação de serviço (DoS)

Bot



- É capaz de se propagar automaticamente
- É um WORM controlado remotamente
- Uma rede infectada com bots é uma **BotNet**
- Promove DoS ou então facilita roubo de informações, envio de SPAM e outras atividades maliciosas

Trojan Horses

- Executa ações clandestinas
- Deve ser executado para entrar em ação
- Pode conter:
  - Vírus
  - Worm
  - Keylogger
  - Outros
- Não se propagam automaticamente

Spywares

- Violam a confidencialidade
- Monitoram atividades do sistema
- São capazes de enviar dados pela rede
- Há diversas utilidades, desde vigiar um companheiro até roubar dados de uma conta bancária e o dinheiro

Keyloggers

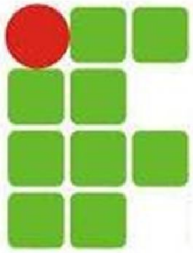
- Lêem os dados do teclado
- Podem ser em SW ou HW
- Os dados do teclado são salvos e enviados pela internet para o endereço da pessoa que o instalou e configurou.

Screenloggers

- Lêem os dados da tela
- Capturam as telas quando o usuário do computador clica usando o mouse.
- São úteis para ver a senha no caso de um teclado virtual do *internet banking*
- Também podem enviar os dados por e-mail

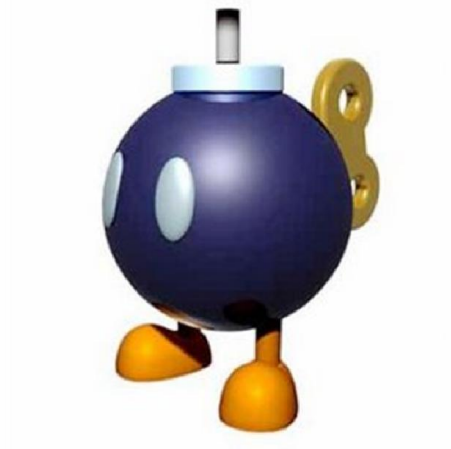
Adware

- **Ad**vertisement
- Tem a intenção de forçar a compra de um produto
- Se incorporam a softwares legítimos para parecerem corretos
- Podem executar programas maliciosos por trás



Bomba Lógica

- Explode quando deixa de ser alimentada
- Precisa de um hospedeiro
- Usada por funcionários para evitar demissão
- Também pode ser utilizada para garantir futuros serviços



Backdoor

- É uma brecha deixada propositalmente para que se possa voltar ao computador previamente invadido
- Pode estar contida em um programa modificado
- Netbus e BackOrifice
- O computador não precisa ter sido invadido para ter um backdoor

Rootkit

- Programas para apagar os rastros de uma invasão
- É utilizado para manter o acesso privilegiado a uma máquina
- Ajuda o invasor a permanecer conectado à máquina invadida de maneira não-detectável

Spam

- Spam é um e-mail não solicitado
- Problemas causados por ele:
  - Perda de mensagens
  - Conteúdo ofensivo
  - Gasto de tempo
  - Impacto na banda
  - Investimento extra em recursos

Outros Riscos

- Cookies
- Códigos Móveis
- Janelas de Pop-up
- Plugins e extensões
- Links Patrocinados
- Banners de Propaganda
- P2P
- Compartilhamento de recursos

Mecanismos de Segurança

- Política de Segurança
- Notificação de Incidentes
- Contas e Senhas
- Criptografia
- Backups
- Logs
- Ferramentas antimalware
- Firewall
- Antispam

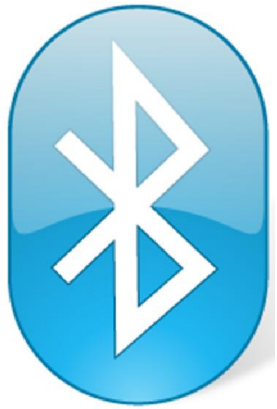
Segurança de Redes

- Wi-Fi
- Bluetooth
- Banda Larga
- Firewall
- VPN
- IDS e IPS

Wi-Fi

- **Wi**reless **Fi**delity
  - WEP (Wired Equivalent Privacy):
    - Primeiro mecanismo de segurança lançado
    - É considerado frágil
  - WPA (Wi-Fi Protected Access):
    - Mecanismo desenvolvido para substituir o WEP
    - É o nível mínimo de segurança recomendado
  - WPA-2:
    - Possui criptografia mais forte que o WPA
    - É o mecanismo mais recomendado

Bluetooth



- Padrão para dados e voz via radiofreqüência
- Trabalha somente em pequenas distâncias
- Deve ser ativado somente no momento da utilização e depois desligado
- O nome padrão do dispositivo deve ser alterado, assim como o PIN
- O uso em locais públicos deve ser evitado

Banda Larga

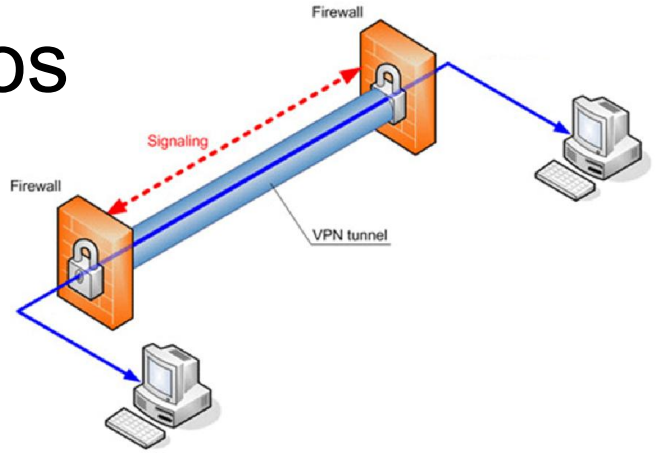
- É um tipo de conexão com capacidade acima da discada
- Acima de 100kbps já é banda larga
- O nome dos equipamentos de rede e suas senhas padrão devem ser alterados
- O acesso remoto deve ser desativado para uma maior segurança

Firewall

- Controle de autenticação
- Registro de tráfego
- Basicamente trabalham analisando as portas para onde os pacotes vão
- Dividem-se em:
  - Filtros de Pacotes
  - Proxies

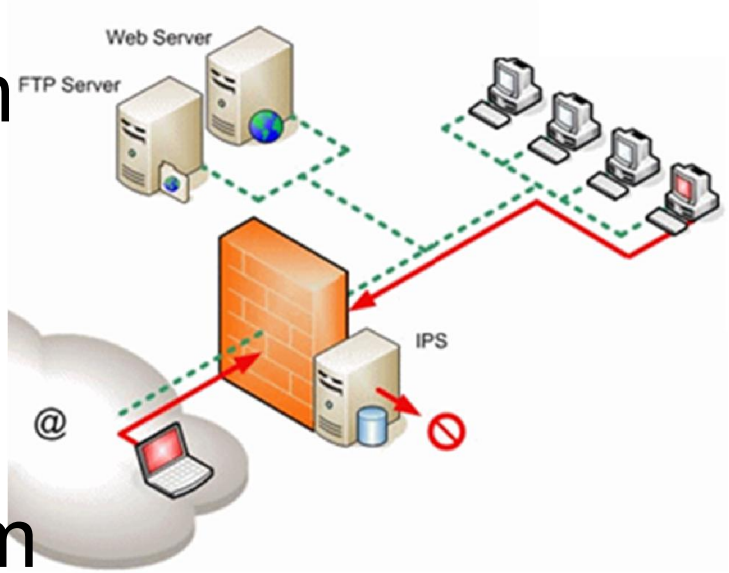
VPN

- Virtual Private Network
- Não requer recursos alugados (Virtual)
- Uso por uma única empresa (Privada)
- Tunelamento por criptografia
- Garante confidencialidade, integridade e autenticidade



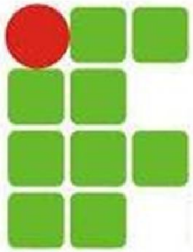
IDS e IPS

- Intrusion Detection System
  - Complemento do Firewall
  - Emite alertas
  - É uma ferramenta passiva
- Intrusion Protection System
  - Pode ficar antes ou depois do Firewall
  - Fora fica exposta, dentro permite o ataque
  - É uma ferramenta ativa
- Análise de tráfego pode dar **falso positivo**



Indicações

- Cartilha de Segurança do CERT.BR:
  - http://cartilha.cert.br/
- Programas Recomendados:
  - Avira Antivirus
  - RegClean
  - NoScript
  - Adblock Plus
  - Secunia Personal Software Inspector



Perguntas?