FAM

Segurança de dados e Auditoria de Sistemas

O QUE VEREMOS HOJE....

- Tipos de ataques mais comuns

AGENDA

Motivação

Porque atacar?

Quem são os atacantes?

O que os ataques exploram?

Qual o impacto para a organização?

Tipos de Ataques:

- IP Spoofing
- Buffer overflow
- Seqüestro de Sessão
- Denial of Service

SEGURANÇA

Ataques às redes corporativas podem gerar perdas de mais de US$2 mi

Grandes corporações enfrentam custos mais altos que as empresas de pequeno e médio porte, que registram aproximadamente US$ 92 mil por incidente.

DA REDAÇÃO

29 de novembro de 2013 - 09h54

Um ataque direcionado bem-sucedido contra uma grande empresa pode causar danos de até 2,4 milhões de dólares, de acordo com uma pesquisa

PORQUE ATACAR?

- Curiosiodade.
- Diversão.
- Obtenção de ganhos financeiros.
- Espionagem industrial.
- Vingança (ex-funcionários, funcionários descontentes).
- Desafio.

QUEM SÃO OS ATACANTES?

- Hackers.
- Crackers.
- White Hat.
- Funcionários/ Ex-funcionários insatisfeitos.

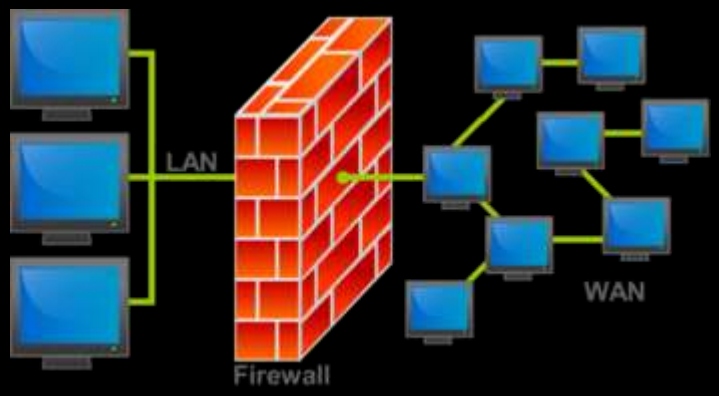
O QUE OS ATAQUES EXPLORAM?

- Bugs no desenvolvimento.
- Senhas fracas.
- Mau uso de ferramentas/serviços legítimos.
- Configuração inadequada de recursos.
- IDS mau implementado.

"Ferramentas existentes vão proteger somente contra os ataques conhecidos"

IDS - INTRUSION DETECTION SYSTEM

IDS x



QUAL O IMPACTO PARA A ORGANIZAÇÃO?

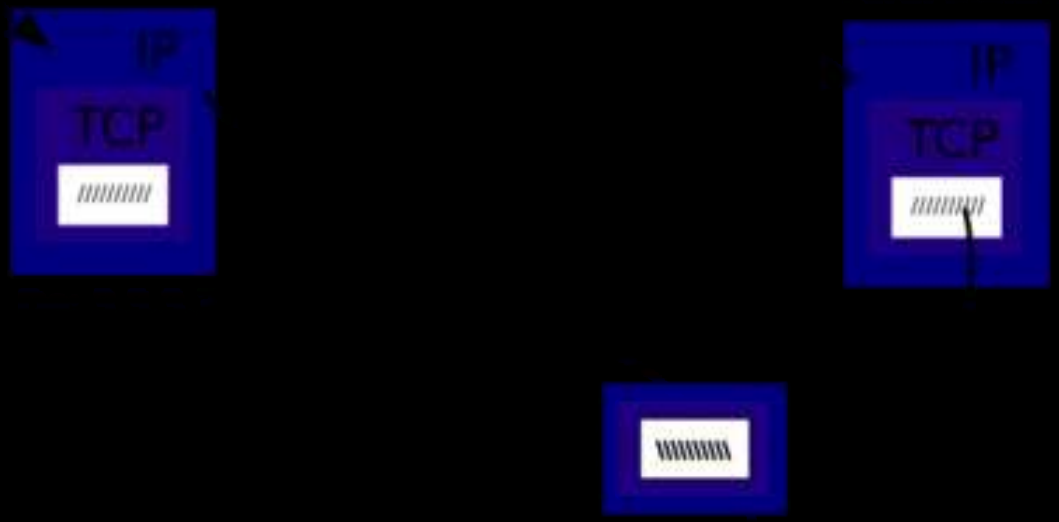
- Vazamento de informações confidenciais.
- Modificação indevida de dados.
- Indisponibilidade de serviço.
- Fraude, perdas financeiras.
- Reputação prejudicada.
- Perda de negócios, clientes e oportunidades.

"Algumas perdas são irreversíveis"

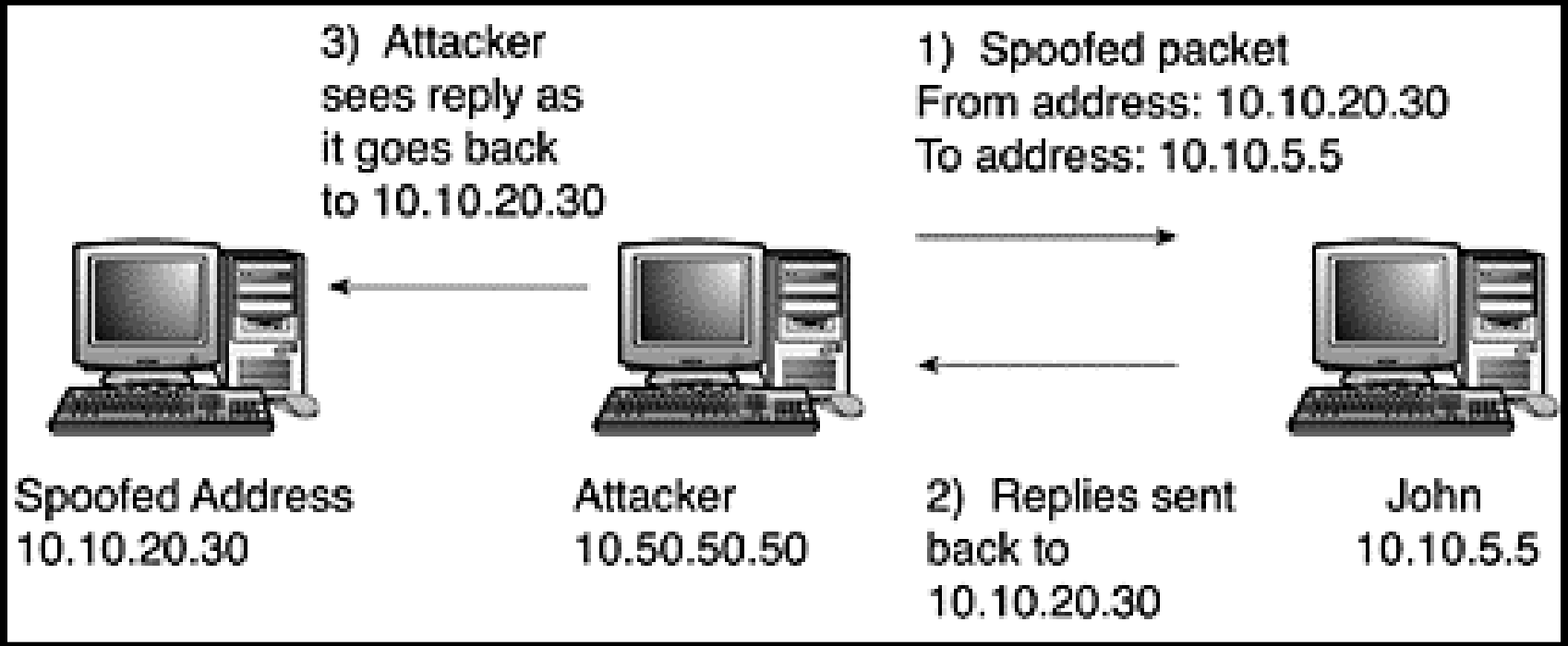
TIPOS DE ATAQUES

- IP Spoofing
- Buffer Overflow
- Seqüestro de Sessão
- Denial of Service

IP SPOOFING



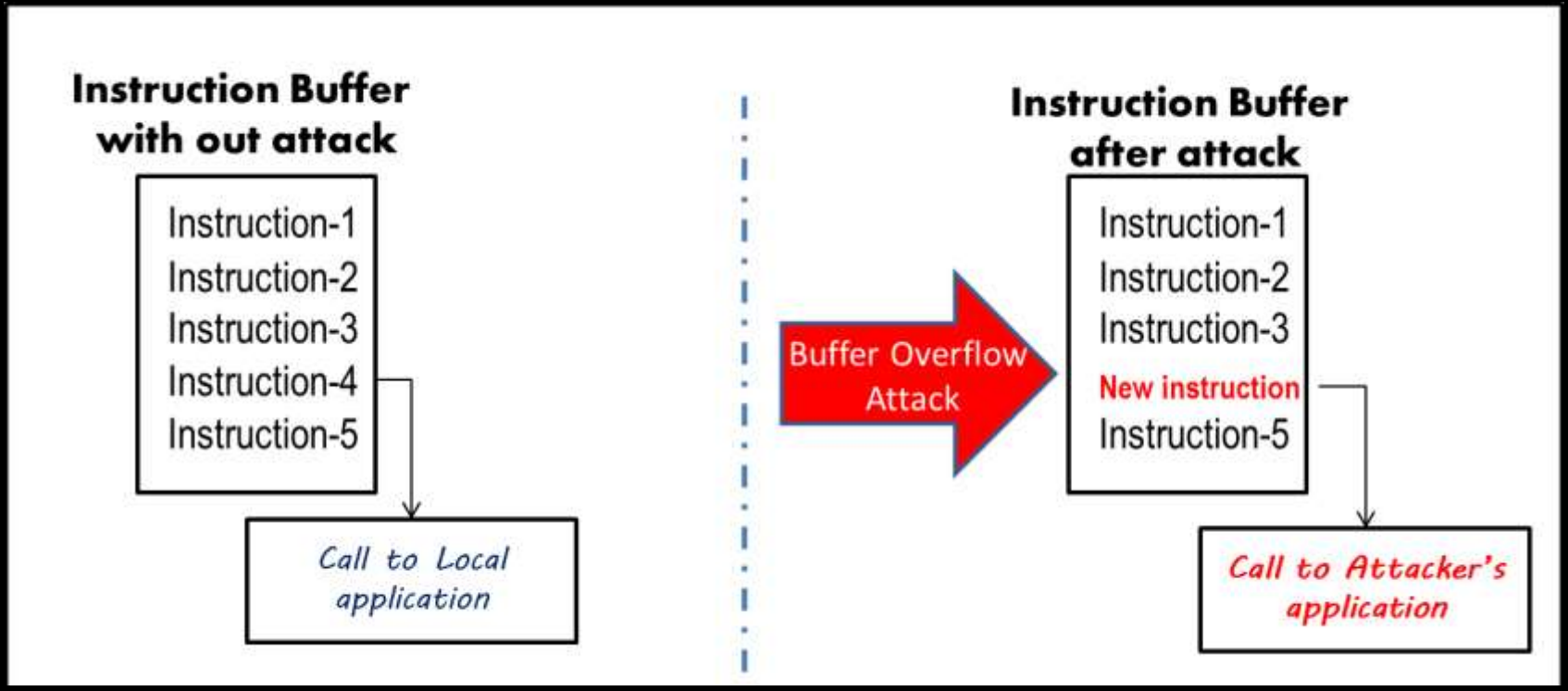
IP Spoofing - Como é feito?



IP SPOOFING - MEDIDAS PREVENTIVAS E CORRETIVAS

- Limitar o acesso as configurações da máquina.
- Utilizar filtros ingress e egress.

BUFFER OVERFLOW



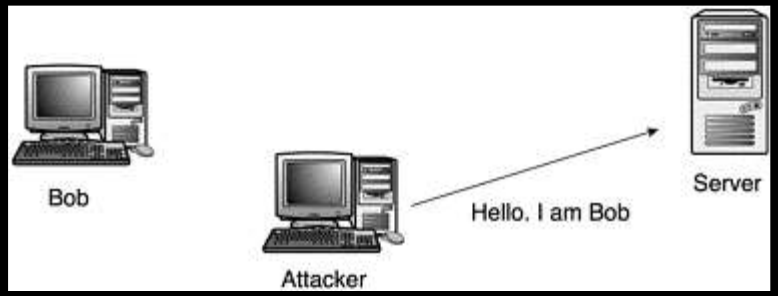
BUFFER OVERFLOW - MEDIDAS PREVENTIVAS E CORRETIVAS

- Revisão nos códigos fonte.
- Execução de sistemas com o menor privilégio.
- Utilização de IPS - Intrusion Prevention System.

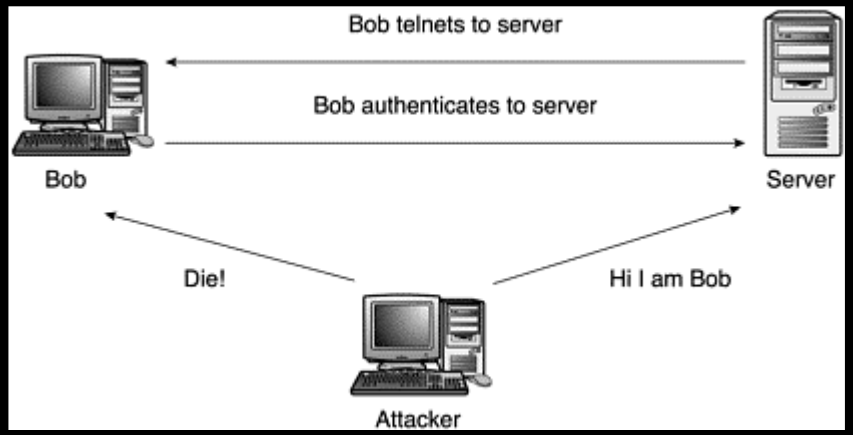
SEQÜESTRO DE SESSÃO - COMO É FEITO?

- Atividades necessárias para seqüestro da conexão
  - Encontrar o alvo.
  - Encontrar uma sessão ativa.
  - Executar a predição da sequência que são trocadas entre as máquinas.
  - Tornar o computador offline.
  - Assumir a sessão.

IP SPOOFING X SEQÜESTRO DE SESSÃO



IP Spoofing

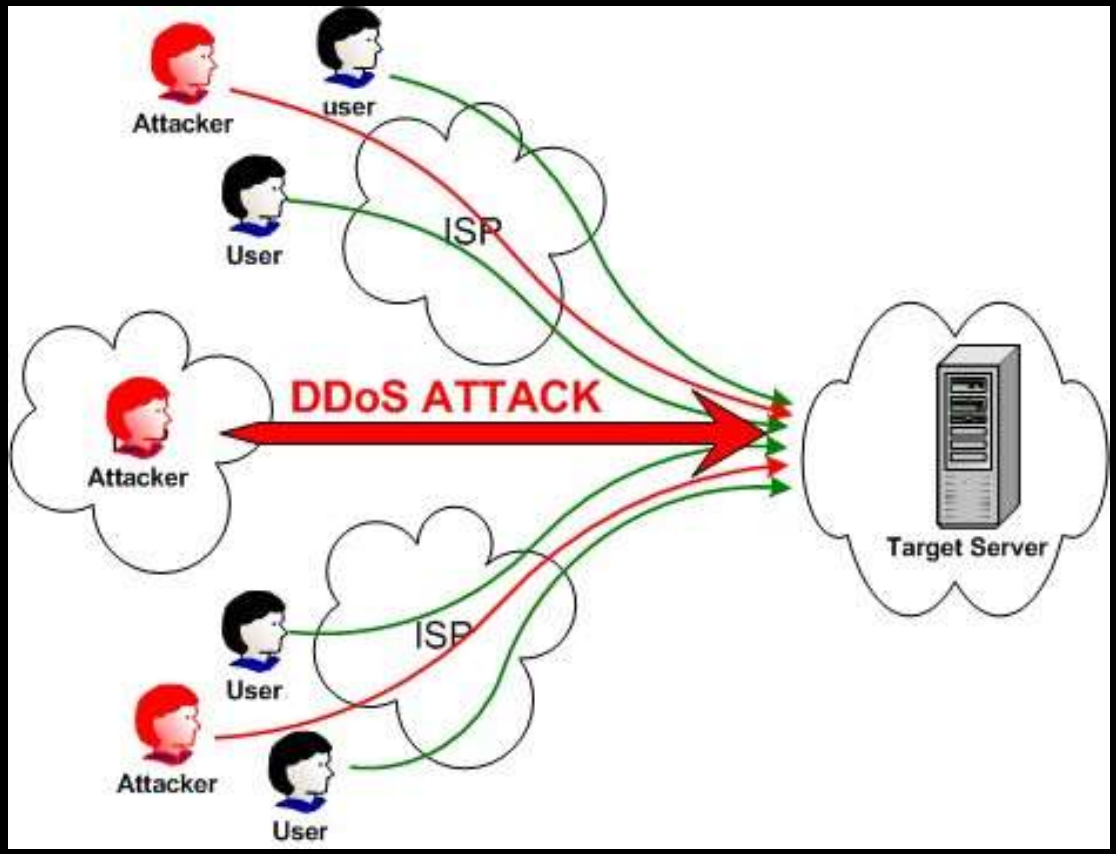


Seqüestro de Sessão

SEQÜESTRO DE SESSÃO - MEDIDAS PREVENTIVAS E CORRETIVAS

- Utilização de criptografia.
- Utilização de um protocolo seguro.
- Limitar o número de conexões entrantes.
- Minimizar acesso remoto.
- Adotar autenticação forte (menos efetivo).

DENIAL OF SERVICE - DEFINIÇÃO

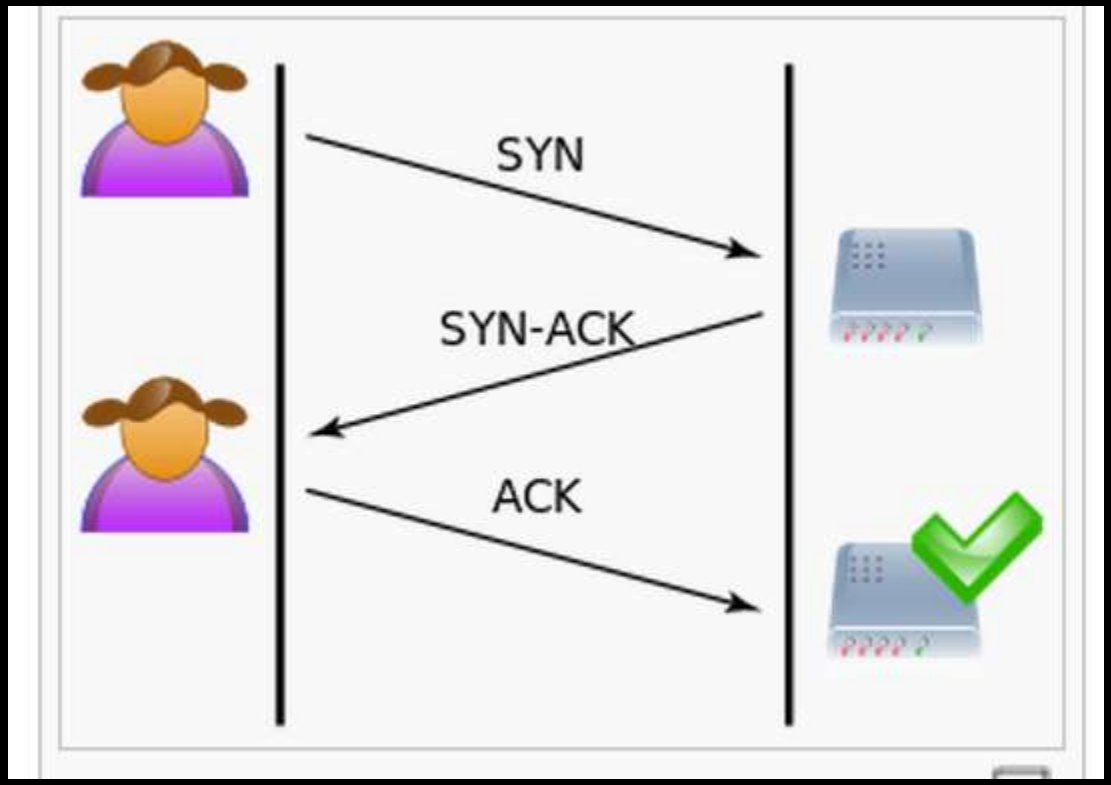


DENIAL OF SERVICE - COMO É FEITO?

- Um tipo de DoS:

- SYN Flooding

DENIAL OF SERVICE - SYN FLOODING



DENIAL OF SERVICE - SYN FLOODING

- Ações preventivas:

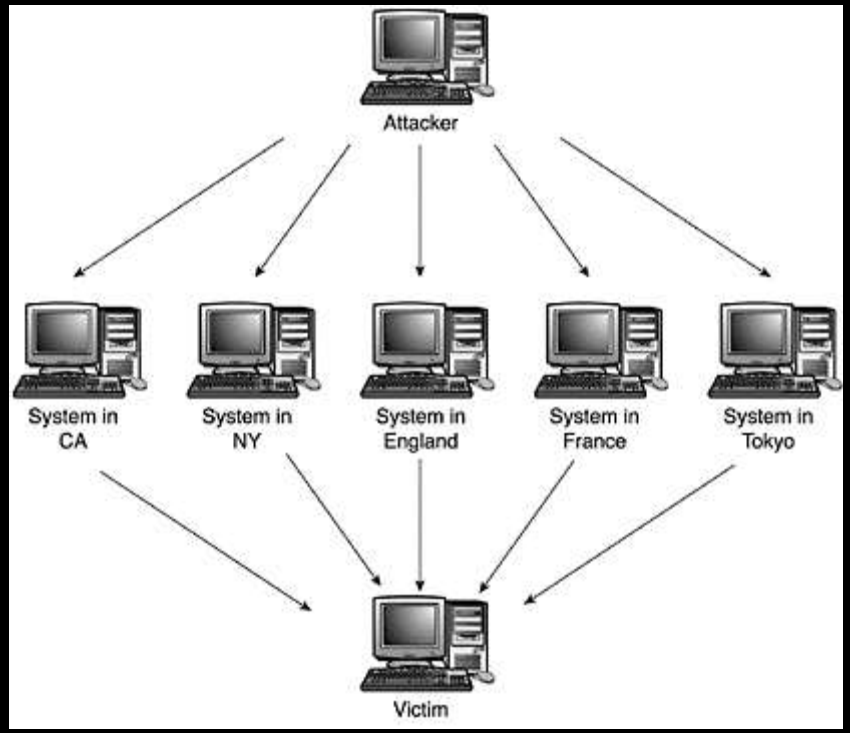
- Comparação das taxas de requisição e conexões em aberto.

- Estabelecer time out da conexão.

- Aumentar a fila de conexões.

DISTRIBUTED DENIAL OF SERVICE - DDOS

- Diversos hosts sendo atacados simultaneamente.
- Ataque de difícil contenção.



DENIAL OF SERVICE - MEDIDAS PREVENTIVAS E CORRETIVAS

- Design robusto e efetivo da rede.
- Limitar a largura de banda.
- Manter os sistemas atualizados.
- Executar a menor quantidade de serviços ativo.
- Permitir somente o tráfego necessário.
- Bloquear o endereço IP.