INSTITUTO FEDERAL
PIAUÍ

# Técnicas de Ataque

SEGURANÇA DA INFORMAÇÃO

**Prof. Silvino Marques**
silvinomarques@ifpi.edu.br

# Introdução

- Já vimos que vulnerabilidades têm sido amplamente utilizadas por atacantes para roubo de informações confidenciais e invasões de redes corporativas.
  - Muitos ataques estão relacionados com vulnerabilidades presentes na **infraestrutura da aplicação**.
  - Mas uma grande parte dos ataques ocorre por conta de vulnerabilidades presentes na **própria aplicação**.

# Ataques

Geralmente divididos nos seguintes tipos:

- Pelo alvo geral do ataque (aplicações, redes ou misto)
- Se o ataque é ativo ou passivo
- Pelo mecanismo de ataque (quebra de senha, exploração de código, ...)

Ataques Ativos

- DoS, DDoS, buffer overflow, inundação de SYN, SQL Injection, XSS, etc..

Ataques Passivos

- Pesquisa de vulnerabilidades, sniffing, ...

Ataques de Senha

- Força bruta, Dicionário, *Rainbow Tables*

Código malicioso (malware)

- Vírus, trojans, worms, ...

# Ataques Ativos

## DoS/DDoS

- Objetivo é reduzir a qualidade de serviço a níveis intoleráveis;
- Um tanto mais difícil quanto maior for a infraestrutura do alvo;
- Enquanto DoS é de fácil execução e pode ser corrigido, DDoS é de difícil execução e não pode ser evitado;
- Tipos
  - Consumo de Recursos (largura de banda, CPU, RAM, ...)
  - Pacotes malformados (todas as flags ligadas)

# DoS - Ataques de refletor

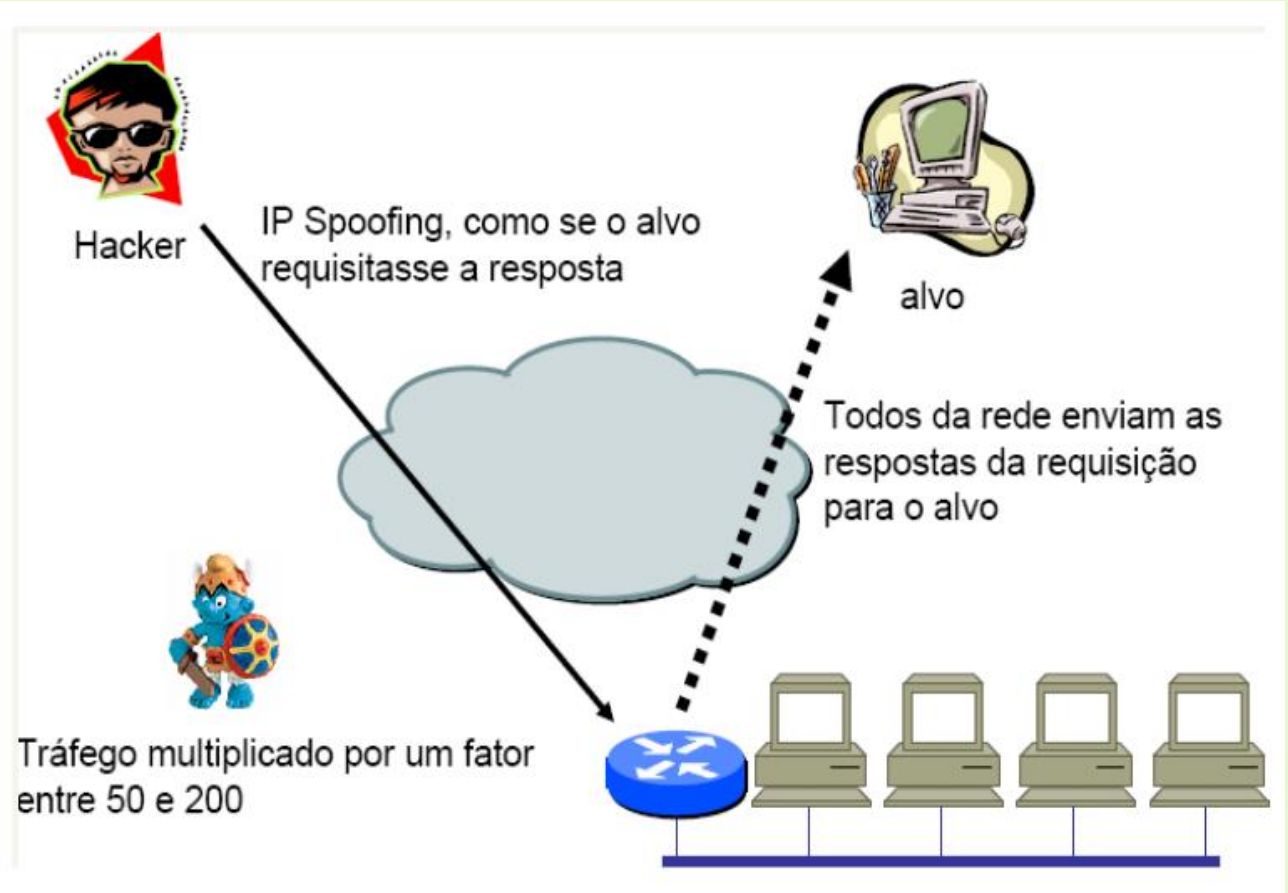
- Em um ataque de refletor, uma máquina envia muitos pedidos com um endereço de origem falsificado (*spoofing*) para uma máquina intermediária;
- Esse endereço falsificado é o endereço da máquina que se quer atacar;
- As máquinas intermediárias enviam respostas dos pedidos à máquina atacada, sem intenção de fazer isso;
  - Exemplos – DNS, SNMP, ICMP echo, etc
- Uma rede pode evitar ser usada como origem do ataque, proibindo a saída de pacotes com endereços de origem que não pertençam a ela.

# DoS - Ataques de amplificador

- É semelhante ao ataque de refletor, mas usa uma rede inteira como intermediária para gerar pedidos para a máquina atacada;
- Isso é realizado enviando pacotes ICMP ou UDP para endereços de broadcast;
  - A esperança é que cada máquina que receba o pacote, responda para a máquina atacada;
  - Dessa forma, um único pacote pode ser multiplicado várias vezes, inundando a máquina atacada;
- Uma rede consegue evitar ser usada como amplificador, proibindo pacotes de broadcast direcionados nos roteadores;

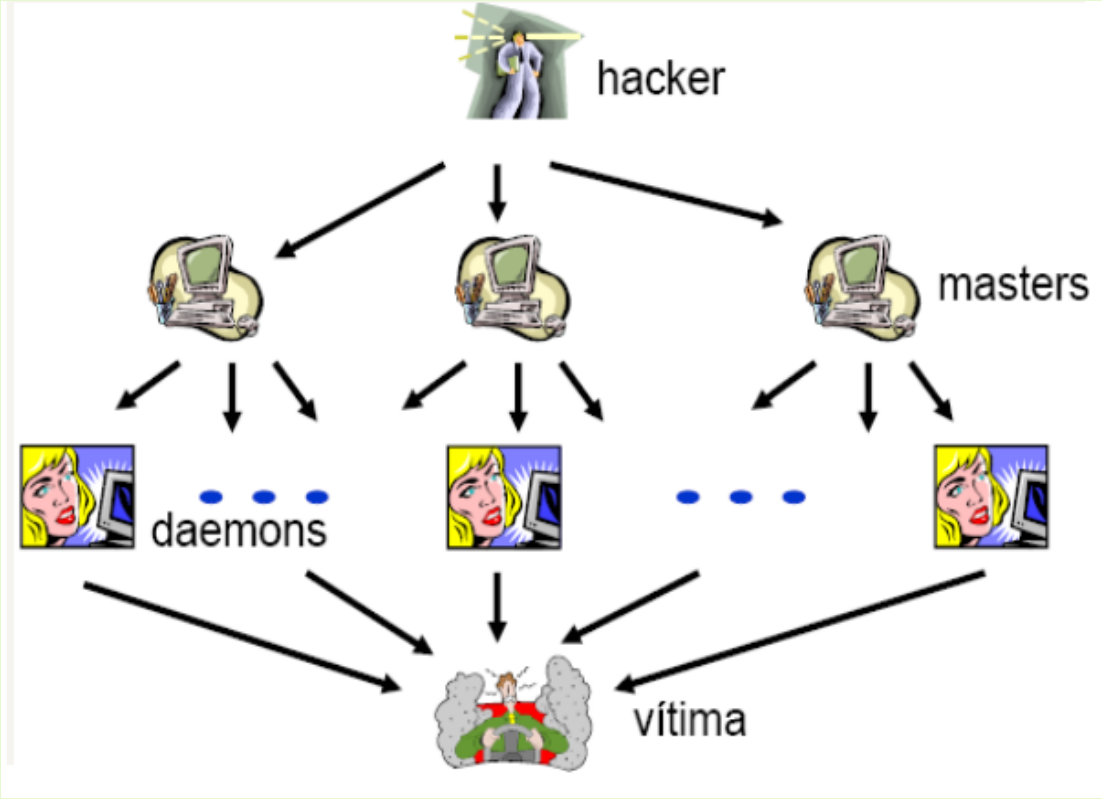
# Exemplo

- Ataque Smurf
  - Ataque pelo qual um grande número de pacotes ping é enviado para o endereço IP de broadcast da rede, tendo como origem o endereço de IP da vítima (IP spoofing).



# DDoS - Distributed DoS

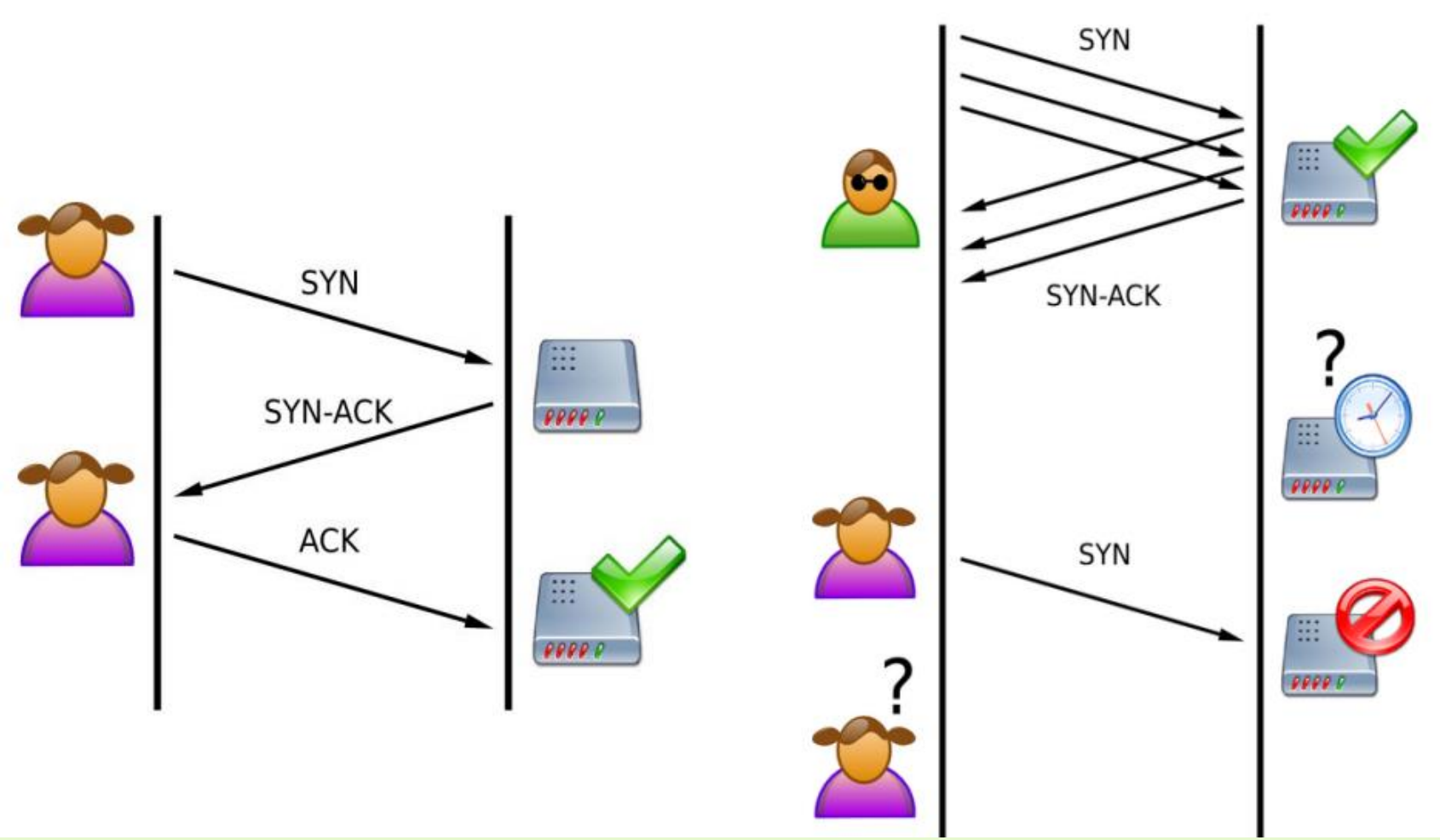
- Um ataque proveniente de uma única máquina geralmente não é capaz de causar dano a uma rede ou servidor;
- Nos DoS distribuídos o atacante coordena um grande grupo de máquinas para que ataquem simultaneamente um único servidor;



# Inundação de SYN

- Em um ataque de inundação de SYN (*syn flood*), um atacante inicia muitas conexões TCP em um curto período de tempo;
- Ele usa um endereço falsificado e a conexão em três fases do TCP (*three-way handshake*) não é completada;
  - O servidor atacado fica com muitas conexões incompletas “presas”, que são liberadas por um temporizador (entre 2 a 4 minutos)
  - Durante o ataque, o servidor fica praticamente impossibilitado de atender outras conexões, porque a sua tabela de conexões esgota a capacidade máxima;

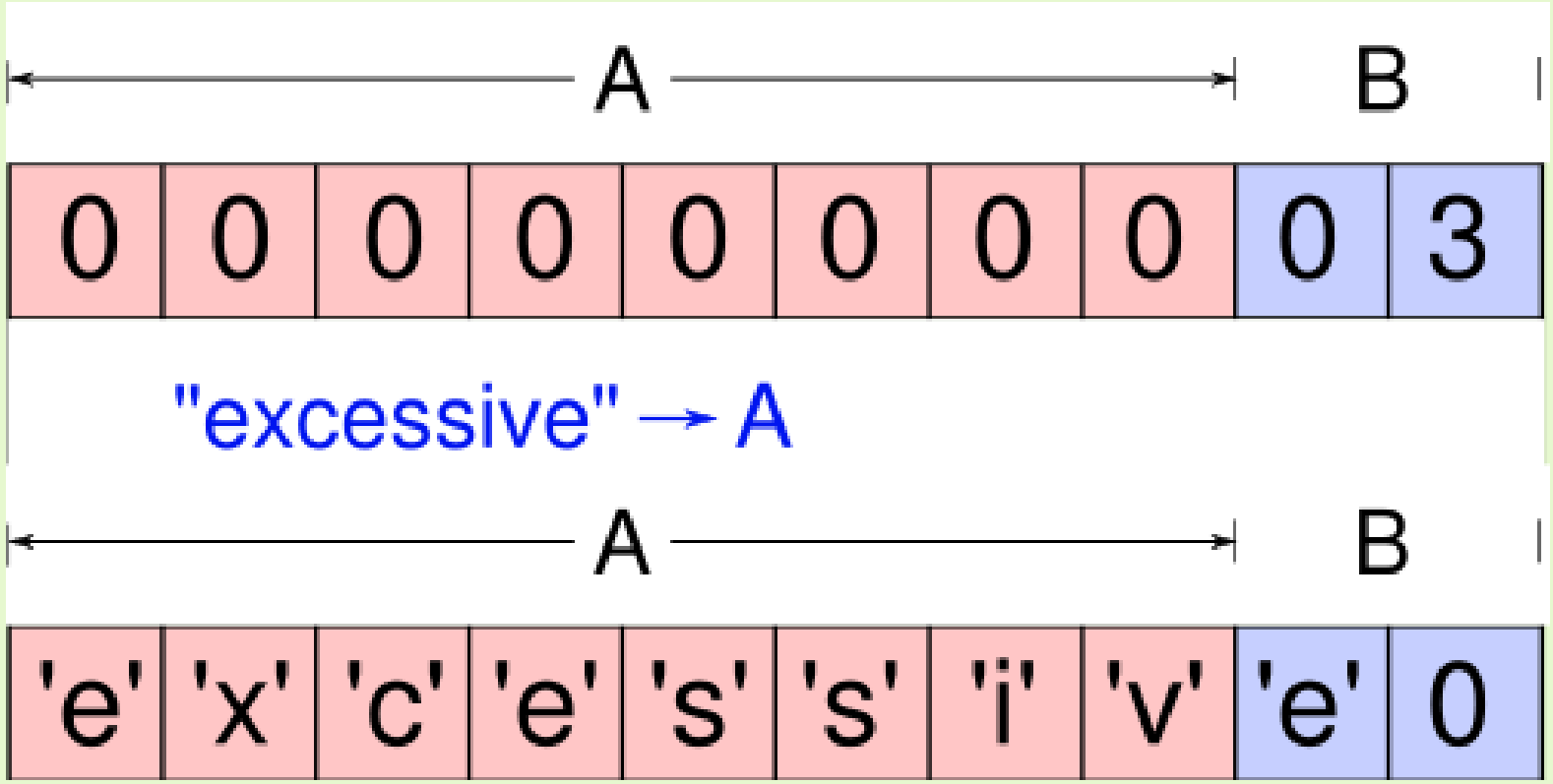
# Inundação de SYN



# Buffer Overflow

- Atacante explora bugs de implementação, nos quais o controle do buffer não é feito adequadamente. Envia mais dados do que o buffer pode manipular;
- Possibilidade de execução de comandos arbitrários, perda ou modificação dos dados, perda do controle do fluxo de execução;
  - Sobrescrever o próprio código em execução
  - Tem como objetivo executar algum código, ou conseguir acesso privilegiado

# Exemplo




✓ Vídeo Demonstrativo

Você já parou para pensar
o que acontece se você
assistir esse vídeo até o fim?

# Injeção de SQL

- É um dos tipos de vulnerabilidades decorrentes do mal processamento de entradas;
- Atacante insere código malicioso na aplicação para alterar seu comportamento original;
  - Apesar de ser um ataque simples e antigo, ainda há muitas aplicações vulneráveis e uma atenção especial deve ser dada a essa vulnerabilidade.

# Injeção de SQL

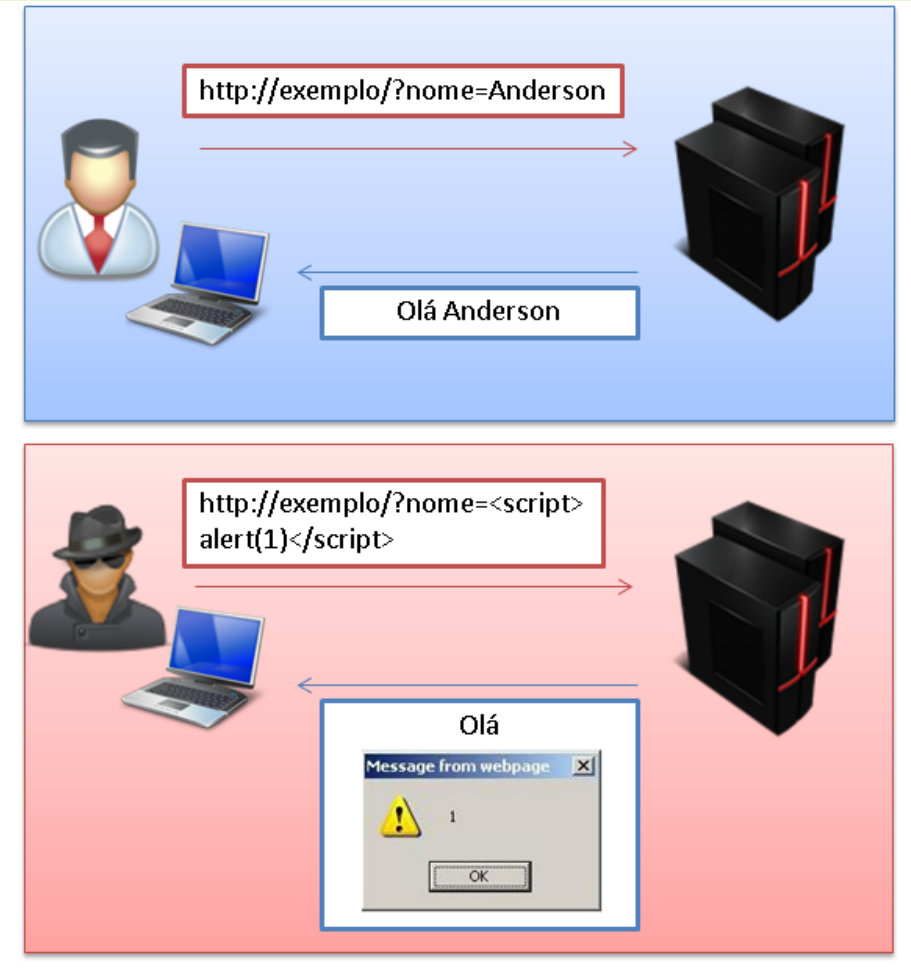
```
select * from user_data
        where last_name = '' or 1=1--'
```

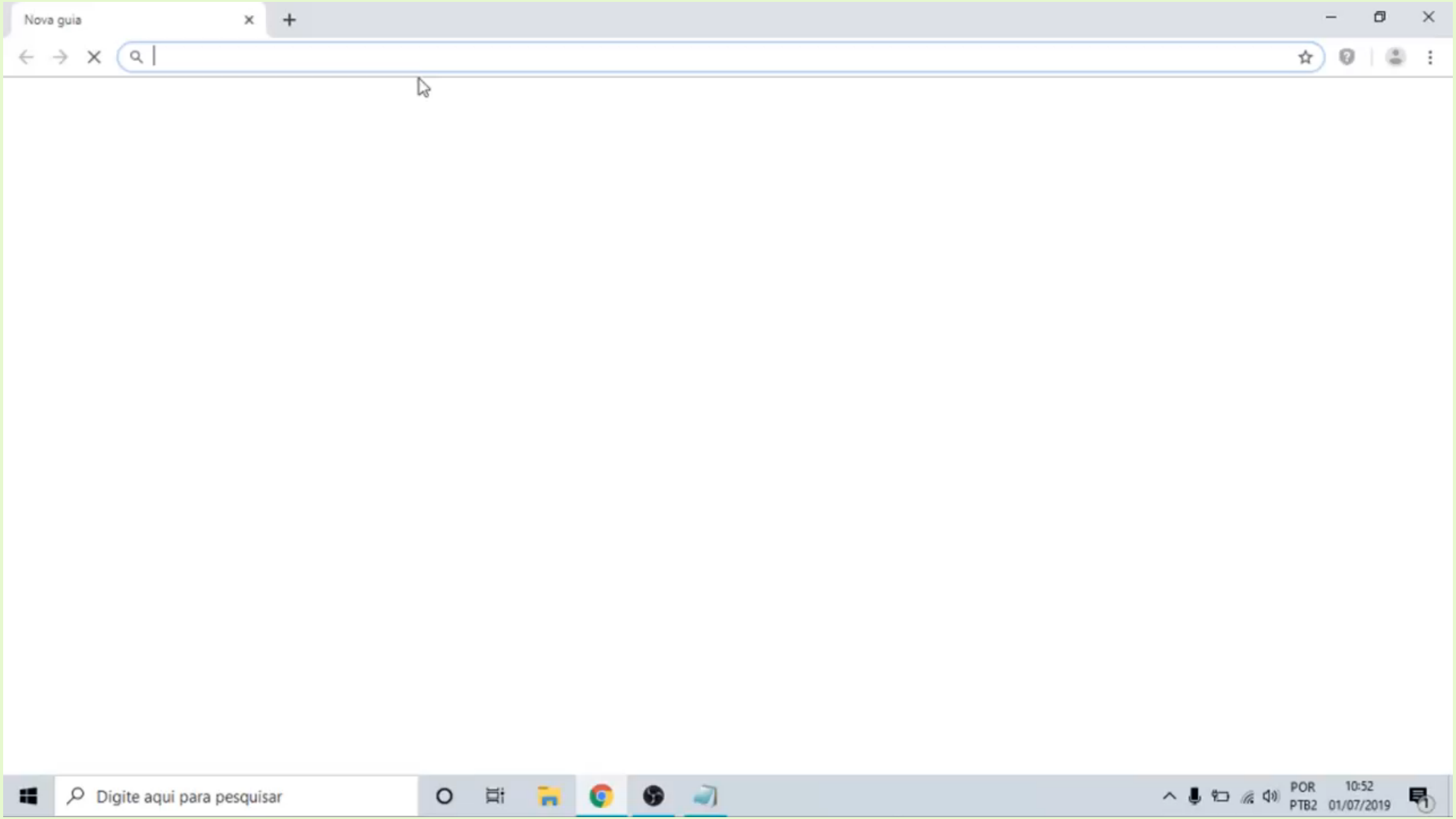
Enter your last name: ' or 1=1;-- Go!

| USERID | FIRST_NAME | LAST_NAME | CC_NUMBER | CC_TYPE | COOKIE | LOGIN_COUNT |
|---|---|---|---|---|---|---|
| 101 | Joe | Snow | 987654321 | VISA | | 0 |
| 101 | Joe | Snow | 2234200065411 | MC | | 0 |
| 102 | John | Smith | 2435600002222 | MC | | 0 |
| 102 | John | Smith | 4352209902222 | AMEX | | 0 |
| 103 | Jane | Plane | 123456789 | MC | | 0 |
| 103 | Jane | Plane | 333498703333 | AMEX | | 0 |
| 10312 | Jolly | Hershey | 176896789 | MC | | 0 |
| 10312 | Jolly | Hershey | 333300003333 | AMEX | | 0 |
| 10323 | Grumpy | White | 673834489 | MC | | 0 |
| 10323 | Grumpy | White | 33413003333 | AMEX | | 0 |
| 15603 | Peter | Sand | 123609789 | MC | | 0 |
| 15603 | Peter | Sand | 338893453333 | AMEX | | 0 |
| 15613 | Joesph | Something | 33843453533 | AMEX | | 0 |

# XSS – Cross Site Scripting

- É uma vulnerabilidade comumente encontrada em aplicações web, que permite a injeção de códigos no lado do cliente, ou seja, altera a página apenas no computador do usuário.
- Ex:

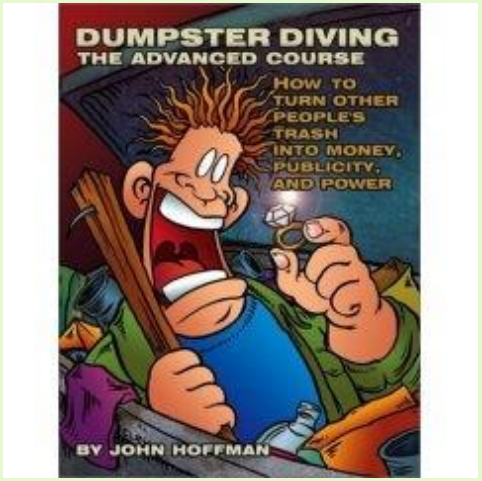



Nova guia
Digite aqui para pesquisar
POR
PTB2
10:52
01/07/2019

# *Defacements*

- Pichações de Sites
  - Invasão a servidores web e troca da página principal
  - Geralmente o objetivo é somente a pichação (visibilidade)

# Outros ataques




*Dumpster Diving/Trashing*

- Documentos sensíveis mal descartados
- Informações em hardwares obsoletos
- Falta de Política de Classificação da Informação

Engenharia social

- Normalmente relevada nos esquemas de segurança
- Utiliza-se do orgulho e necessidade de auto reconhecimento, intrínseco do ser humano

***"Um computador não estará seguro nem quando desligado e trancado em uma sala, pois mesmo assim alguém pode ser instruído a ligá-lo."***

[ Kevin Mitnick – A arte de enganar/The Art of Deception ]

# Ataques Passivos

Normalmente utilizado antes de um ataque ativo

Pesquisa de Vulnerabilidades

- Pesquisa por Portas/Serviços
  - http://www.insecure.org – Nmap


Escuta (sniffing)

- Extremamente difícil a detecção
- Senhas em texto claro, comunicações não encriptadas
- WireShark (Lin/Win), TCPDump (Lin)
  - http://www.wireshark.org
  - http://www.tcpdump.org


# Links Interessantes

- Ferramentas de aprendizagem/simulação
  - ✓ Hacksplaining
  - ✓ TryHackMe
- Projeto OWASP;
  - ✓ OWASP Top Ten;
  - ✓ OWASP Zed Attack Proxy (ZAP);

# Referências Bibliográficas

**Introdução a Segurança de Computadores** – Michael T. GOODRICH, Roberto TAMASSIA. Porto Alegre, RS, Brasil. 2013.

**Segurança de Redes em Ambientes Cooperativos** – Emilio T. NAKAMURA, Paulo L. GEUS. São Paulo, SP, Brasil. 2007.