Reconhecimento e Mapeamento

Ementa

- Reconhecimento e Mapeamento
  - Tipos de falhas
  - Auditorias Web
  - WHOIS
  - DNS
  - Newsgroups e Anúncios de Empregos
  - Redes Sociais
- Fases do Mapeamento
  - Mapeamento de portas
  - Identificação do Sistema Operacional e Versão
- Identificação da Aplicação
  - Identificando Infra-estrutura Web
    - Load Balancers
    - WAF
    - Servidores Web
  - Identificação do Fluxo de Funcionamento
  - Identificação dos pontos de entrada

Reconhecimento e Mapeamento

- São as primeiras fases de um ataque
- **Reconhecimento**: pesquisa sobre a aplicação para determinar o foco dos ataques
  - Informações sobre a arquitetura da aplicação
  - Informações sobre a infra-estrutura

Reconhecimento e Mapeamento

- São as primeiras fases de um ataque
- **Mapeamento**: entender como a aplicação interage com a infra-estrutura
  - Checagens de versão da aplicação
  - Checagem de interação com outros conteúdos e dependências externas

Tipos de falhas

- Exposição de Informações
- Falhas de Configuração e Manutenção
- Falhas de Validação de Dados
- Falhas de Disponibilidade

Exposição de Informação

- Expõe informações sobre a aplicação, infra-estrutura, correções...

Falhas de Configuração e Manutenção

- Relacionadas a erros ou más práticas de configuração e manutenção

Falhas de Validação de Dados

- Relacionadas a não validação ou validação de forma incorreta dos dados enviados a aplicação

Falhas de Disponibilidade

- Relacionada ao controle que a aplicação tem sobre seu uso

Tipos de Teste

- BlackBox: sem conhecimento prévio do ambiente
- WhiteBox: com conhecimento prévio do ambiente (código fonte)
- GrayBox: com conhecimento prévio do ambiente, porém sem conhecimento a nível de código

Onde os atacantes obtém os dados?

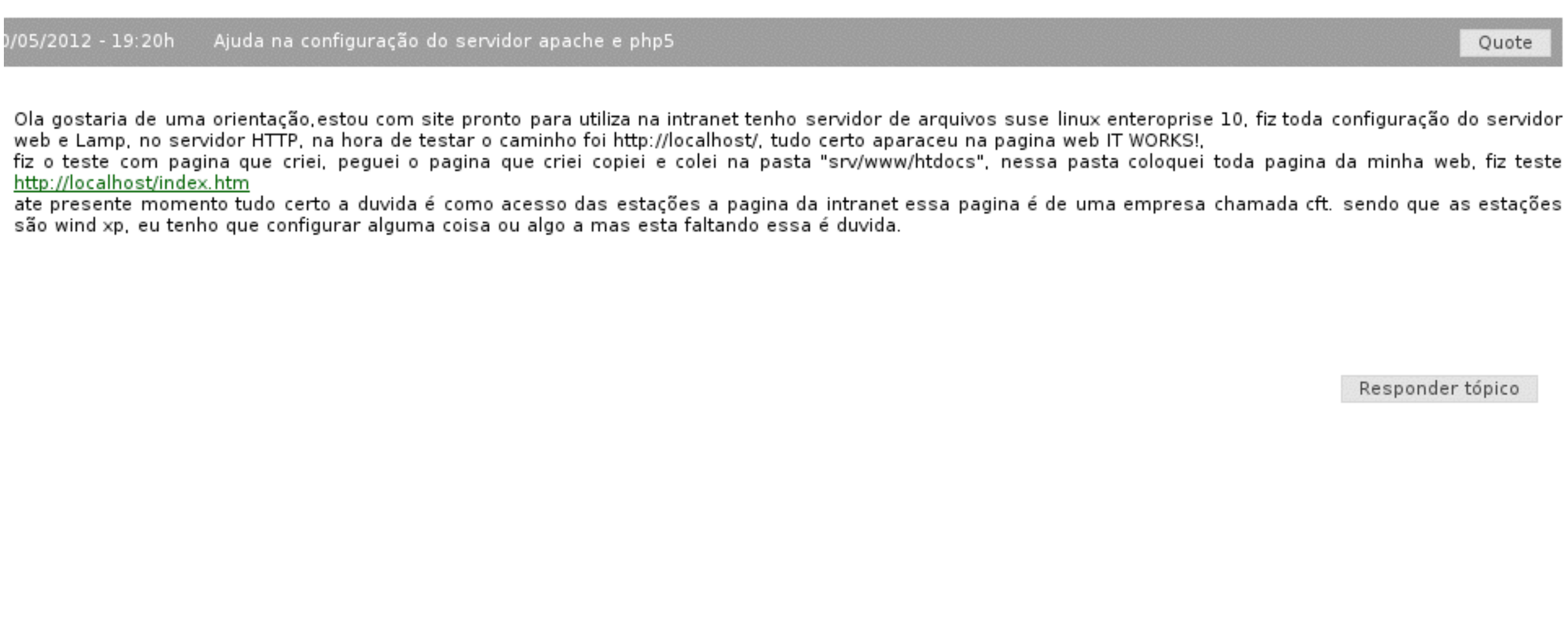
- WHOIS: Serviço largamente utilizado para prover a identificação para blocos de endereço IP.

Onde os atacantes obtém os dados?

- DNS: Sistema distribuído para tradução de nomes em endereços IP

Onde os atacantes obtém os dados?

- Listas de discussão e Anúncios de Emprego



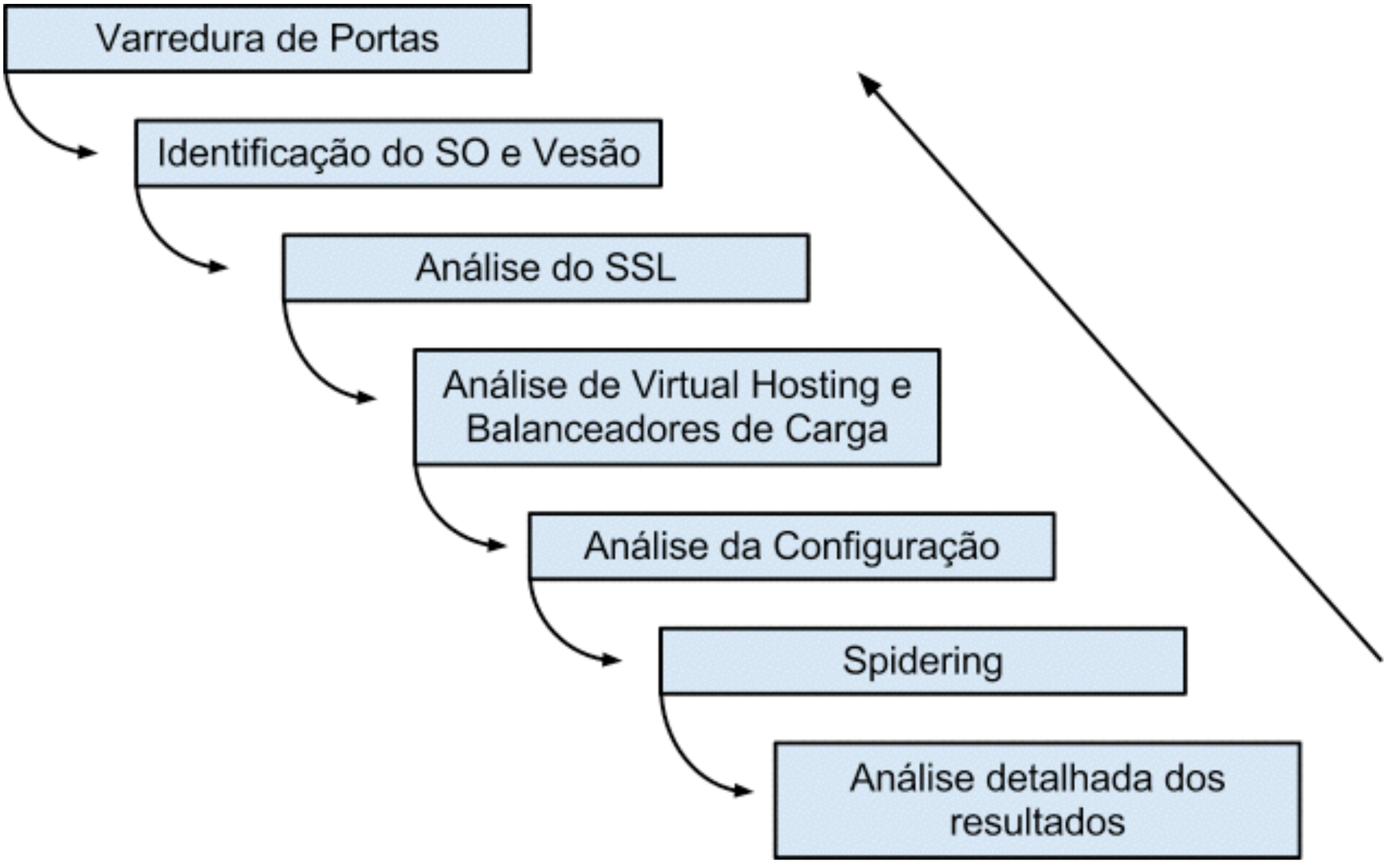
Gerente de T.I. (v603232)

Código da vaga:	v603232
Nível hierárquico:	Pleno
Local:	Cajamar / SP / BR
Data de expiração:	19 de Setembro de 2012

Principais Responsabilidades
- Desenvolver e implementar estratégias para o ambiente de tecnologia da informação e de telecom visando atender as necessidades da América do Sul.
- Contribuir para o alinhamento da área de tecnologia da informação (TI) com as estratégias de negócio da empresa, prestando suporte nos processos de mudanças.
- Manter a rede corporativa de dados compatível com as demandas atuais das áreas de negócio continentais e globais da empresa, efetuar constantes revisões tecnologias visando aprimoramento contínuo dos serviços de telecomunicação.
- Gerenciar técnica e administrativamente os projetos dos sistemas de informação, de infra estrutura e de telecomunicação, garantindo que os dados possam ser acessados pelos clientes internos para atividades operacionais e tomada de decisão.
- Manter contato com clientes internos e externos, participando do planejamento de mudanças nos negócios da empresa e fornecendo o suporte necessário para a melhoria na utilização dos recursos.

Requisitos
- Ensino Superior Concluído;
- Mandatório Inglês avançado/ fluente (espanhol será considerado um diferencial);
- Gerenciamento de Equipes;
- Conhecimentos gerais em:
1. ERP, preferencialmente Oracle/JDE Enterprise One Versão 8. Ou acima (ideal versão 9)
2. Plataforma Windows : Banco de Dados (SQL-2005 ;SQL-2008);Exchange 2003 ou acima (desejável versão 2010); Active Directory;
3. Aplicaçoes Web e a respectiva infra-estrutura de segurança ;
4. Redes de Dados (locais e remotas) , de Voz e de Imagem

Fases do Mapeamento



Varredura de portas

- A importância da varredura de portas está na descobertas dos serviços habilitados e possivelmente vulneráveis que possam ser alvos de uma futura investida.

Varredura de portas

- Abra o Terminal e digite:

```
telnet scanme.nmap.org 22
```

Identificação de SO e Versão

- Abra o Terminal e digite:

```
telnet scanme.nmap.org 22
```

Identificação de SO e Versão

- Abra o Terminal e digite:

```
telnet scanme.nmap.org 80
OPTIONS * HTTP/1.1
```

Análise do SSL

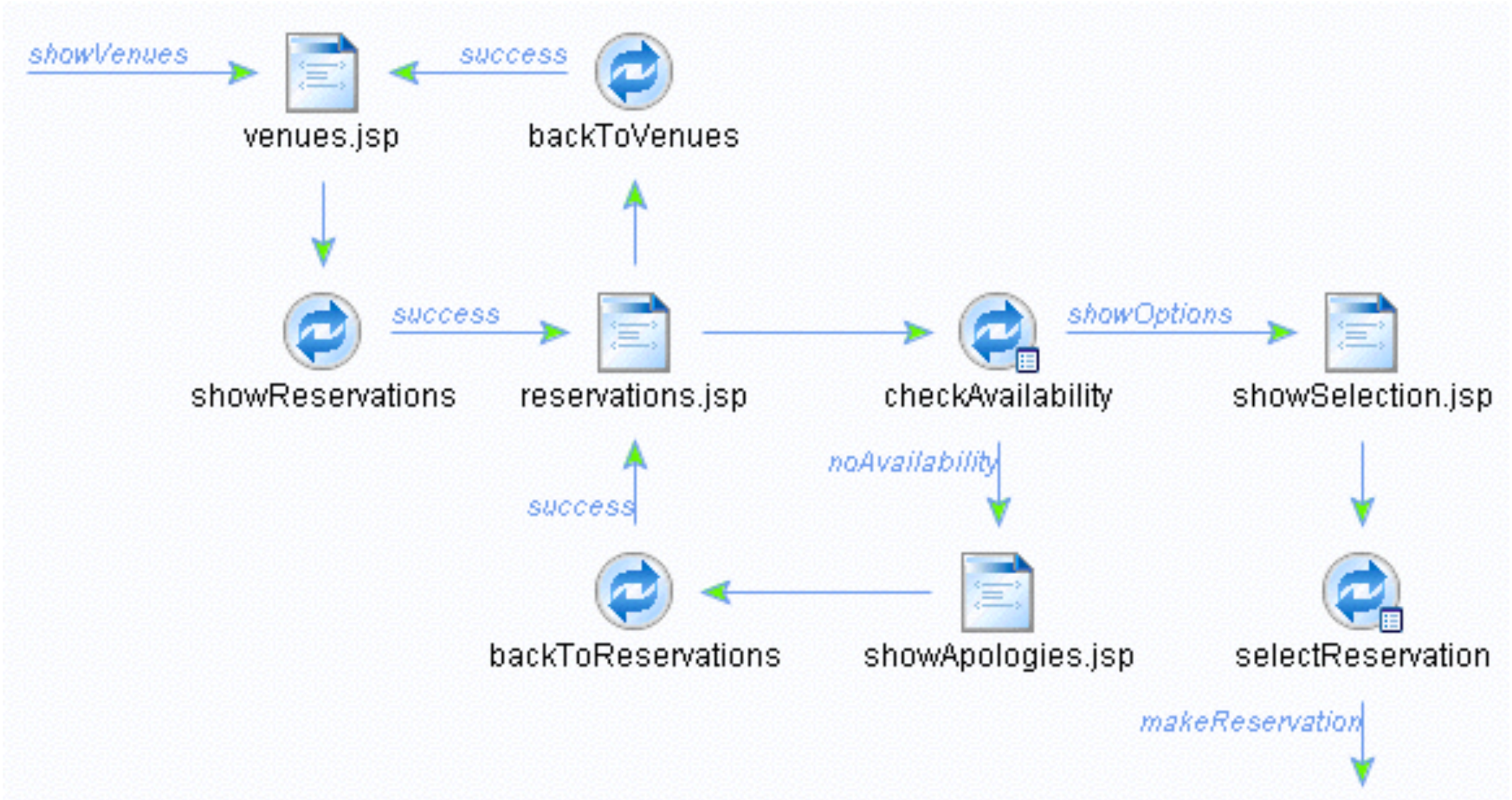
- Abra o Navegador e digite:

https://www.ssllabs.com/ssltest

Infra-estrutura Web

- Balanceadores de Carga
- WAF - Web Application Firewall
- Servidores Web

Identificação do Fluxo de Funcionamento



Identificação dos pontos de entrada de informação

- Identificar onde os clientes enviam dados para a aplicação
- Esses pontos serão futuros alvos de tentativas de ataque
- Ferramentas geralmente tem essa funcionalidade conhecida como “spidering”

Duvidas?