# Segurança em Redes

## Aula 12 - Segurança no Serviço de DNS e DNSSEC

# Apresentação

Nesta aula, iremos realizar uma breve revisão sobre o funcionamento do serviço de tradução de nomes da Internet (DNS) e apresentar as principais vulnerabilidades e tipos de ataques comumente realizados contra este serviço. Em seguida, estudaremos o DNSSEC, uma série de extensões adicionadas ao DNS tradicional, que possibilitam garantir a integridade e autenticidade dos dados trocados entre clientes e servidores deste serviço.

**Vídeo 01** - Apresentação

## Objetivos

Ao final desta aula, você será capaz de:

- Relembrar os conceitos de funcionamento do serviço de DNS.
- Identificar os principais problemas de segurança do serviço de DNS.
- Aprender quais são as extensões de segurança do serviço de DNS (DNSSEC).

# Conceito de DNS

Na disciplina de redes de computadores, você estudou alguns dos principais serviços disponíveis para os usuários da Internet. Alguns deles você talvez já conhecesse, como o serviço que possibilita o acesso à páginas web ou o que possibilita a troca de e-mails. Outro serviço estudado, que também é de extrema importância, é o DNS (*Domain Name System*), que a grosso modo, possibilita aos usuários da Internet, o acesso a servidores de qualquer outro serviço, utilizando para isto nomes simbólicos e fáceis de lembrar, ao invés de endereços IP. Você estudou a justificativa e objetivos do serviço de DNS, sua forma de funcionamento e até mesmo como implementá-lo na prática em um servidor Linux.

Agora, iremos mostrar que o DNS faz parte de um grupo de serviços existentes na Internet, que foram desenvolvidos com pouca (ou nenhuma) preocupação relacionada à segurança. Existem diversas justificativas para essa falta de "preocupação" com a segurança encontrada nesses serviços. Dentre elas podemos destacar o fato de que boa parte deles foram criados juntamente com a própria Internet, que era uma rede pequena e exclusivamente utilizada para pesquisa acadêmica, em que todos os usuários e computadores ligados eram conhecidos e "confiáveis".

Com a evolução e crescimento da Internet, principalmente nos últimos anos, esse cenário mudou completamente e surgiram os diversos problemas (e soluções) de segurança que estamos estudando ao longo desta disciplina. O serviço de DNS, como nós estudamos e conhecemos, não está imune a esses problemas, sendo atualmente alvo de diversos tipos de ataques. Alguns desses ataques são de tipos já conhecidos, como os de "*man-in-the-middle*", outros ainda não, como os de "*cache-poisioning*". Estes e outros tipos de ataques direcionados especificamente para o serviço de DNS tradicional serão estudados ao longo desta aula.

Conhecendo os novos problemas de segurança, passaremos a estudar formas de evitá-los. No caso do DNS, isso é possível pela utilização de uma série de extensões de segurança, incorporadas recentemente ao serviço original, e

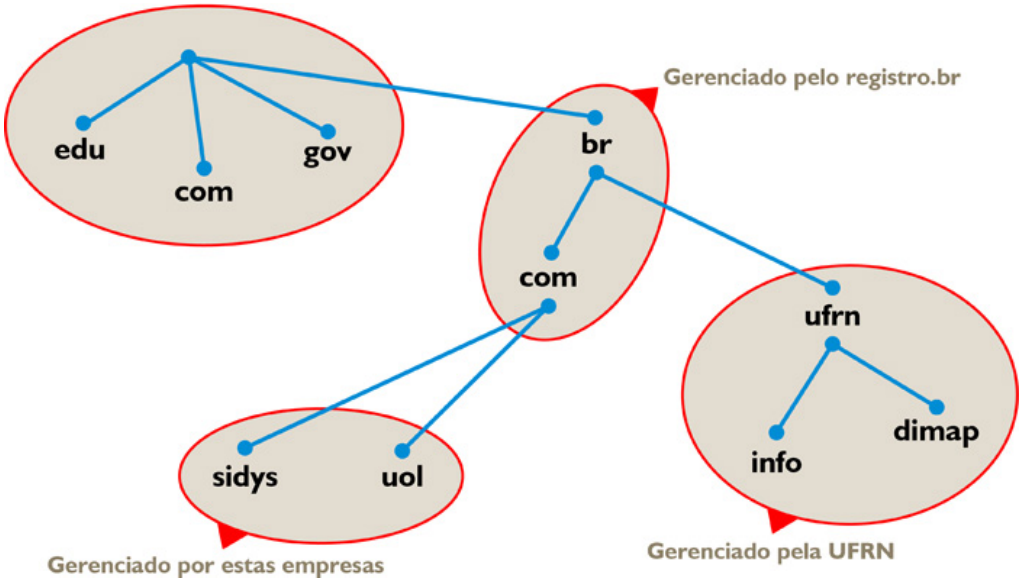
conhecidas como DNSSEC. Nesse caso, a segurança será provida pela possibilidade de verificar a integridade e autenticidade dos dados trocados entre clientes e servidores do serviço.

## Sistema de Nomes de Domínio (DNS)

Na disciplina de redes de computadores, você aprendeu que os protocolos da arquitetura TCP/IP utilizam endereços IP para identificar unicamente cada *host* conectado à rede. Essa solução é adequada apenas para os próprios computadores, mas para nós, usuários, é desejável utilizar nomes, que são bem mais fáceis de lembrar. Para solucionar esse problema, criou-se um serviço, cuja principal função é exatamente a atribuição de nomes simbólicos à endereços IP.

O serviço de DNS, conforme você já estudou, pode ser visto como um grande banco de dados distribuído e hierárquico, em que ficam armazenados registros, que por exemplo, atribuem um nome a um endereço IP. Dada a forma como o DNS funciona, a responsabilidade pela atribuição dos nomes às máquinas também é distribuída entre os servidores desse serviço. Dessa forma, embora uma consulta sobre qual endereço IP corresponde, atualmente, ao nome www.metropoledigital.ufrn.br possa ser realizada por qualquer cliente (ou mesmo servidor) desse serviço, uma alteração nessa correspondência só poderá ser realizada pelo administrador do servidor de DNS do Metrópole Digital. Tecnicamente, esta distribuição de responsabilidade é chamada de *delegação*. A **Figura 1** mostra uma parte da "árvore" de nomes do DNS, com seus respectivos responsáveis. Para reforçar, nela vemos que, apenas os administradores da empresa "terra" podem alterar as atribuições de endereços IP a nomes que terminem com terra.com.br.

**Figura 01** - Exemplo de hierarquia de nomes formando a árvore do DNS.

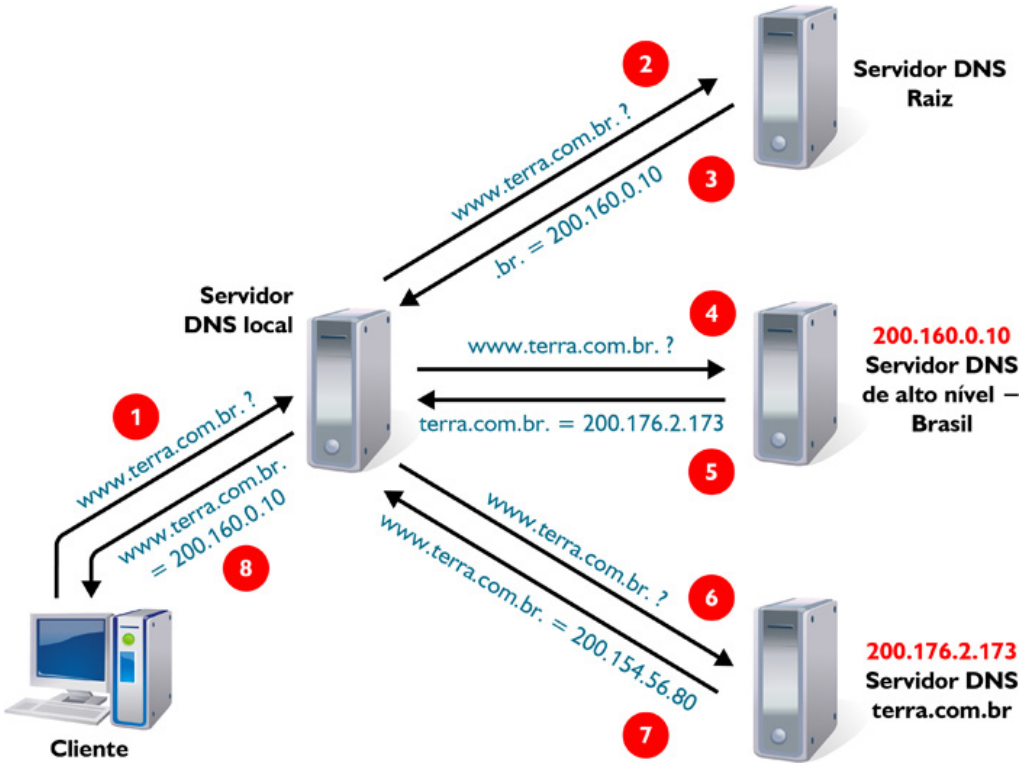



# O Processo de Resolução de Nomes

Para poder utilizar o serviço de DNS, o seu computador utiliza um cliente deste serviço, também chamado de *resolver*. Por ser um serviço muito básico, não é necessário que você instale nada em seu computador para poder utilizar o DNS. Em outras palavras, o *resolver* já vem instalado, juntamente com o windows, Linux etc., que você utiliza em sua máquina. O processo de resolução de nomes em si é chamado de tradução recursiva, sendo suas etapas exemplificadas na **Figura 2**

1. Cliente solicita ao DNS local a resolução do nome <www.terra.com.br>
2. DNS local pergunta www.terra.com.br a um DNS raiz
3. DNS raiz responde: **.br = 200.160.0.10**
4. DNS local pergunta www.terra.com.br ao DNS responsável por .br
5. DNS responsável por .br responde: **terra.com.br = 200.176.2.173**
6. DNS local pergunta www.terra.com.br ao DNS responsável por terra.com.br
7. DNS responsável por terra.com.br responde: **www.terra.com.br = 200.154.56.80**
8. DNS local envia resposta **www.terra.com.br = 200.154.56.80** ao cliente

**Figura 02** - Tradução DNS Recursiva.




# Zonas de DNS e Registros

Cada servidor de DNS será responsável por um ou mais domínios (tecnicamente, zonas de DNS), sendo o *software* mais utilizado o *Bind*. Na configuração desses servidores será criado um arquivo com as configuração de cada zona de DNS.

Seu conteúdo é, na verdade, formado de uma série de "registros" que, dependendo de seu tipo, podem atribuir um nome simbólico a um endereço IP, um novo apelido a um nome já existente etc.

**Vídeo 02** - Revisão DNS

# Atividade 01

Até agora estamos apenas revisando alguns conceitos fundamentais sobre o funcionamento do serviço de DNS. Isso é necessário para que você entenda corretamente o restante da aula. Dessa forma, revise um pouco mais o serviço de DNS, respondendo as perguntas a seguir:

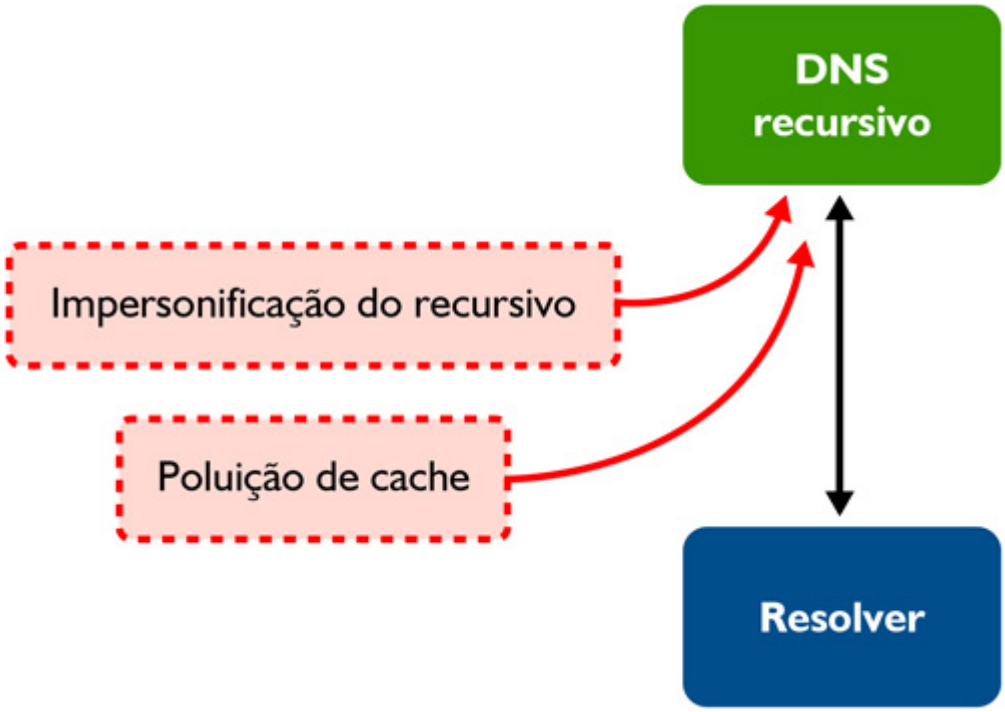
1. Qual a diferença entre um servidor de DNS principal e secundário?
2. Por que os servidores de DNS recursivos possuem uma cache?
3. Quais os principais tipos de registros que um administrador pode incluir em uma zona de DNS? Qual a função de cada um deles (cite pelo menos quatro exemplos)?

# Problemas de Segurança do Serviço de DNS

Os principais problemas de segurança encontrados atualmente no serviço de DNS são direcionados à comunicação entre *resolvers* e servidores de DNS recursivos, ou seja, aqueles que são responsáveis por receber requisições dos clientes e, através do processo de tradução recursiva, obter a resposta. Nesta aula, iremos estudar dois tipos de ataques, listados a seguir e mostrados na **Figura 3**:

1. Impersonificação do recursivo (um ataque do tipo *man-in-the-middle*);
2. Poluição de cache.

**Figura 03** - Principais problemas de segurança do serviço de DNS.

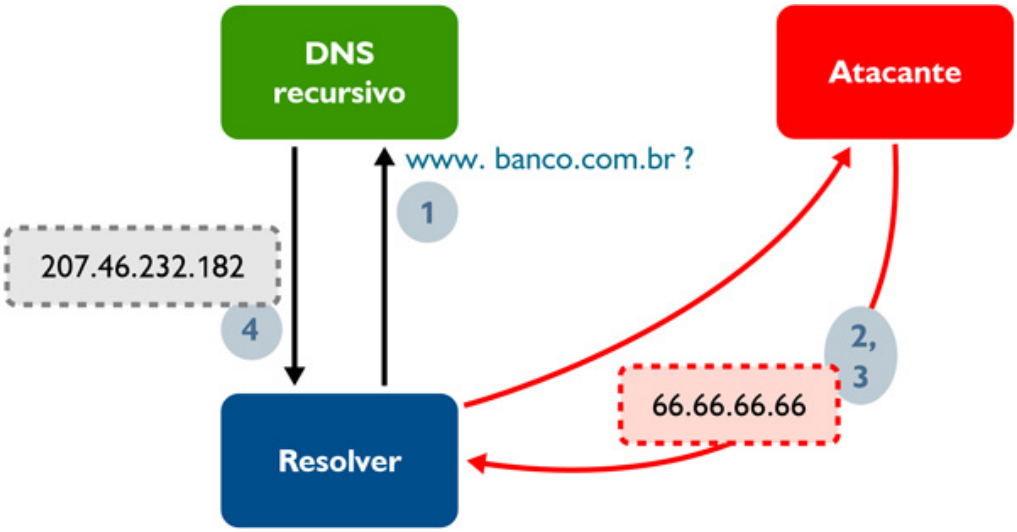



## Ataques de Impersonificação do Recursivo

Nesse tipo de ataque, o atacante tenta se fazer passar pelo servidor de DNS recursivo real utilizado pelo cliente. Como o serviço de DNS tradicional não realiza nenhum tipo de autenticação ou verificação de integridade, tudo que o atacante tem de fazer é: (1) capturar a requisição do cliente; (2) responder mais rápido que o servidor real. Por exemplo, o usuário tenta acessar a página de um banco fictício www.banco.com.br. Nesse momento ocorre a seguinte sequência de eventos, também vistos na Figura 4:

1. *Resolver* solicita ao servidor de DNS recursivo a resolução do nome;
2. Atacante captura esta requisição e responde rapidamente www.banco.com.br = 66.66.66.66. O endereço IP informado pelo atacante conterá, por exemplo, uma cópia falsa da página do banco, com o objetivo de roubar o número da agência, conta e senha;
3. O cliente recebe a resposta do atacante e acredita que ela veio do servidor de DNS recursivo;
4. Após algum tempo, o cliente recebe a resposta real do servidor de DNS recursivo www.banco.com.br = 207.46.232.182, mas a descarta por já ter recebido uma resposta anterior.

**Figura 04** - Impersonificação do recursivo.




## Ataques de Poluição de Cache

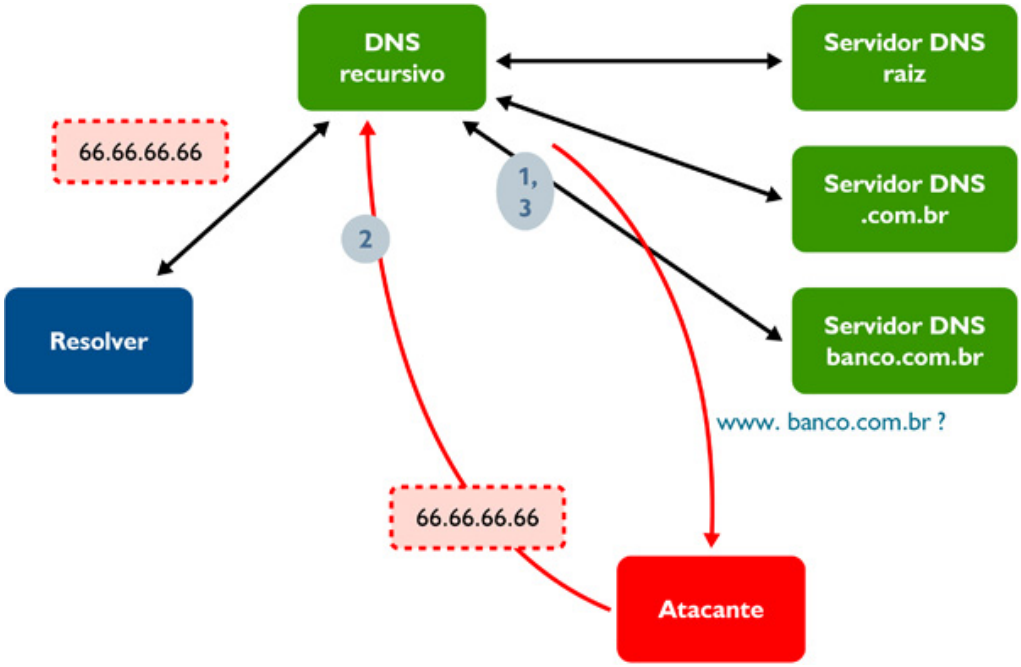
Este tipo de ataque é semelhante ao anterior e se baseia no mesmo princípio (atacante captura uma requisição e responde de forma mais rápida que o servidor real), contudo a poluição de cache é mais perigosa por ser direcionada para o próprio servidor de DNS recursivo. O servidor atacado irá receber uma resposta de um atacante e inserir a mesma em sua cache. Todas as requisições subsequentes de clientes, para esse mesmo endereço, serão respondidas com o endereço IP malicioso fornecido pelo atacante. No exemplo da **Figura 5** ocorrem os seguintes eventos:

1. Durante o processo de tradução recursiva, o DNS recursivo solicita ao servidor autoritativo a resolução do nome www.banco.com.br;

2. O atacante captura essa pergunta e responde rapidamente **www.banco.com.br = 66.66.66.66.** O DNS recursivo aceita a resposta e a guarda na cache, informando a mesma ao cliente atual, bem como a outros que por ventura solicitem a resolução desse mesmo nome;

3. O servidor de DNS autoritativo responde **www.banco.com.br = 207.46.232.182**, mas o servidor de DNS recursivo descarta essa resposta por já ter recebido uma anterior.

**Figura 05** - Poluição de cache.




# Atividade 02

1. Por que os ataques direcionados ao DNS podem ser considerados do tipo *man-in-the-midlle*?

# *Domain Name System SECurity extensions* (DNSSEC)

São um conjunto de extensões à tecnologia do DNS sendo implementadas, atualmente, de forma opcional, ou seja, o serviço de DNS tradicional continua a funcionar. Seu principal objetivo é prover maior segurança na comunicação entre *resolvers* e servidores de DNS garantindo a origem de uma resposta (ou seja, sua autenticidade), bem como sua integridade. Como, a priori, todas as informações contidas no serviço de DNS são públicas, o DNSSEC não necessita prover confidencialidade na comunicação.

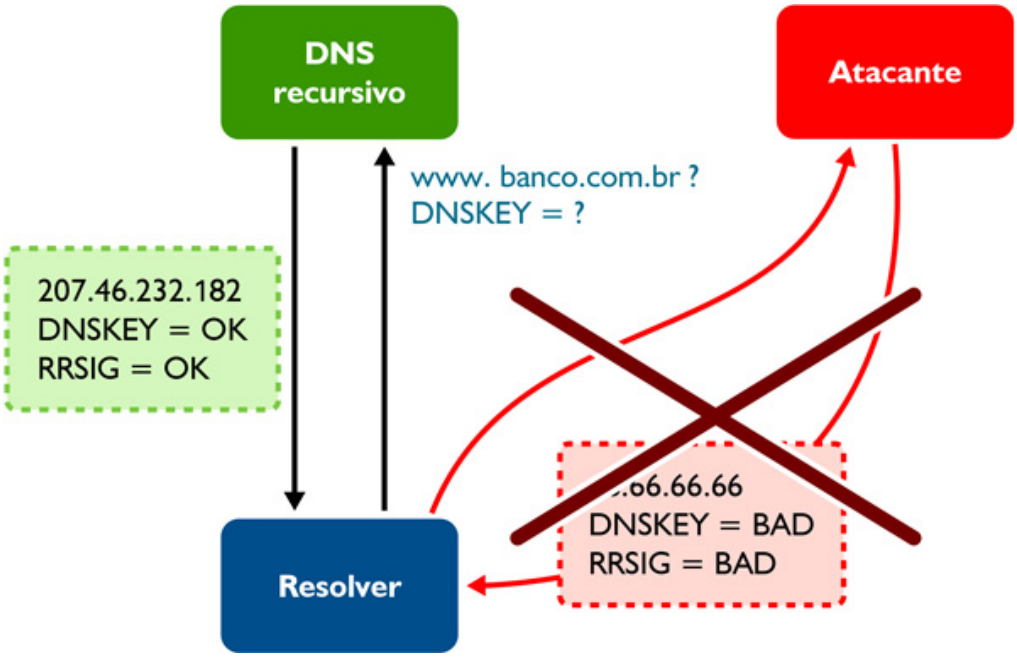
O DNSSEC utiliza o conceito de chaves de criptografia assimétrica (pública e privada). A autenticidade e integridade são providas pela assinatura digital dos registros existentes em uma zona de DNS. A assinatura é realizada utilizando a chave privada do servidor responsável pela zona de DNS (domínio) e pode ser

verificada por qualquer outro servidor ou *resolver*, utilizando para tanto a chave pública correspondente. A autenticidade de uma chave pública pode ser verificada por meio de um *hash* que fica armazenada na sua "zona pai". No caso dos exemplos das seções anteriores, um *hash* da chave pública da zona "banco.com.br" ficaria armazenada no responsável pela zona "com.br" e assim por diante, até se atingir os servidores de DNS raiz. Vale também explicar que DNSSEC não utiliza certificados digitais e as chaves (pública e privada) de uma zona de DNS nunca expiram, contudo as assinaturas dos registros existentes na zona possuem validade.

Na prática, o DNSSEC cria um novo conjunto de tipos de registro que podem estar presentes no arquivo de configuração de uma zona de DNS, sendo os mais importantes:

- **DNSKEY:** contém a chave pública da zona de DNS;
- **RRSIG:** contém a assinatura digital de um registro existente nessa zona de DNS;
- **DS:** contém um *hash* da chave pública de uma zona de DNS "filha". Por exemplo, o arquivo de configuração da zona de DNS "ufrn.br" deverá conter um registro do tipo DS para a zona "metropoledigital.ufrn.br".

**Figura 06** - Resposta de atacante descartada por assinatura da resposta incorreta.



Em ambas as situações da seção anterior, o atacante não teria como gerar uma resposta apropriada, pois, para isso, ele necessita da chave privada da zona "banco.com.br" que foi utilizada para assinar todos os seus registros. Ao receber uma resposta do atacante, o *resolver* ou servidor de DNS recursivo checaria a validade da assinatura dos registros contidos na mesma e ela não seria confirmada. A resposta do atacante seria, então, descartada (conforme mostrado na **Figura 6**) e o *resolver*, ou servidor recursivo, aguardaria o recebimento da resposta correta.

Atualmente, todos os principais servidores de DNS já suportam do DNSSEC. É tarefa de seus administradores realizarem as configurações necessárias para que ele seja habilitado para as zonas de DNS que estão sobre sua administração. No Brasil, todos os domínios abaixo do .br podem (e devem) utilizar DNSSEC, sendo inclusive obrigatório o seu uso nos registros que estiverem diretamente abaixo dos domínios.B.BR e .JUS.BR.

**Vídeo 03** - DNSSec

**Vídeo 04** - Configuração do DNSSec

# Atividade 03

**Pesquise**

Nesta aula, estudamos a teoria dos principais problemas de segurança relacionados ao serviço de DNS e a solução para os mesmos por meio do DNSSEC. Agora, que tal praticar um pouco? Pesquise na Internet como configurar um servidor de DNS (executando o *software* Bind), de modo que ele passe a utilizar o DNSSEC. Você verá que é bastante simples! Como dica, acesse a página http://dietinf.ifrn.edu.br/doku.php?id=corpodocente:carlosrocha:seguranca_de_redes e clique em "Segurança do Serviço DNS".

# Resumo

Nesta aula, você aprendeu mais sobre um dos serviços mais importantes da Internet, o de DNS. Inicialmente, realizamos uma breve revisão de suas principais funcionalidades. Em seguida, mostramos que atualmente o DNS é vulnerável a uma série de problemas de segurança. Boa parte deles se baseia na facilidade que um atacante tem de forjar uma resposta e direcioná-la a um cliente ou servidor do serviço. Por fim, estudamos sobre o DNESEC, uma de extensões de segurança, adicionadas ao DNS tradicional, que quando utilizadas impossibilitam a ação dos atacantes.

# Autoavaliação

1. Escreva sobre a importância de se prover segurança ao serviço de DNS. Dê exemplos de outros problemas de segurança que podem ocorrer devido a um ataque a esse serviço.

2. Por que não foi necessária a inclusão de mecanismos de criptografia no DNSSEC?

3. Nas alternativas a seguir, assinale Verdadeiro ou Falso:

   ( ) Os ataques ao serviço de DNS podem ser direcionados aos servidores recursivos.
   ( ) O DNSSEC protege a comunicação entre cliente, mas não entre servidores de DNS.
   ( ) DNS e DNSSEC são serviços incompatíveis, não podendo ser utilizados em conjunto.
   ( ) O DNSSEC garante a autenticidade de todas as respostas de servidores.

# Referências

BIND Nameserver. Disponível em: <http://www.isc.org/software/bind>. Acesso em: 23 ago. 2012.

TUTORIAL DNSSEC. Disponível em: <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>. Acesso em: 23 ago. 2012.