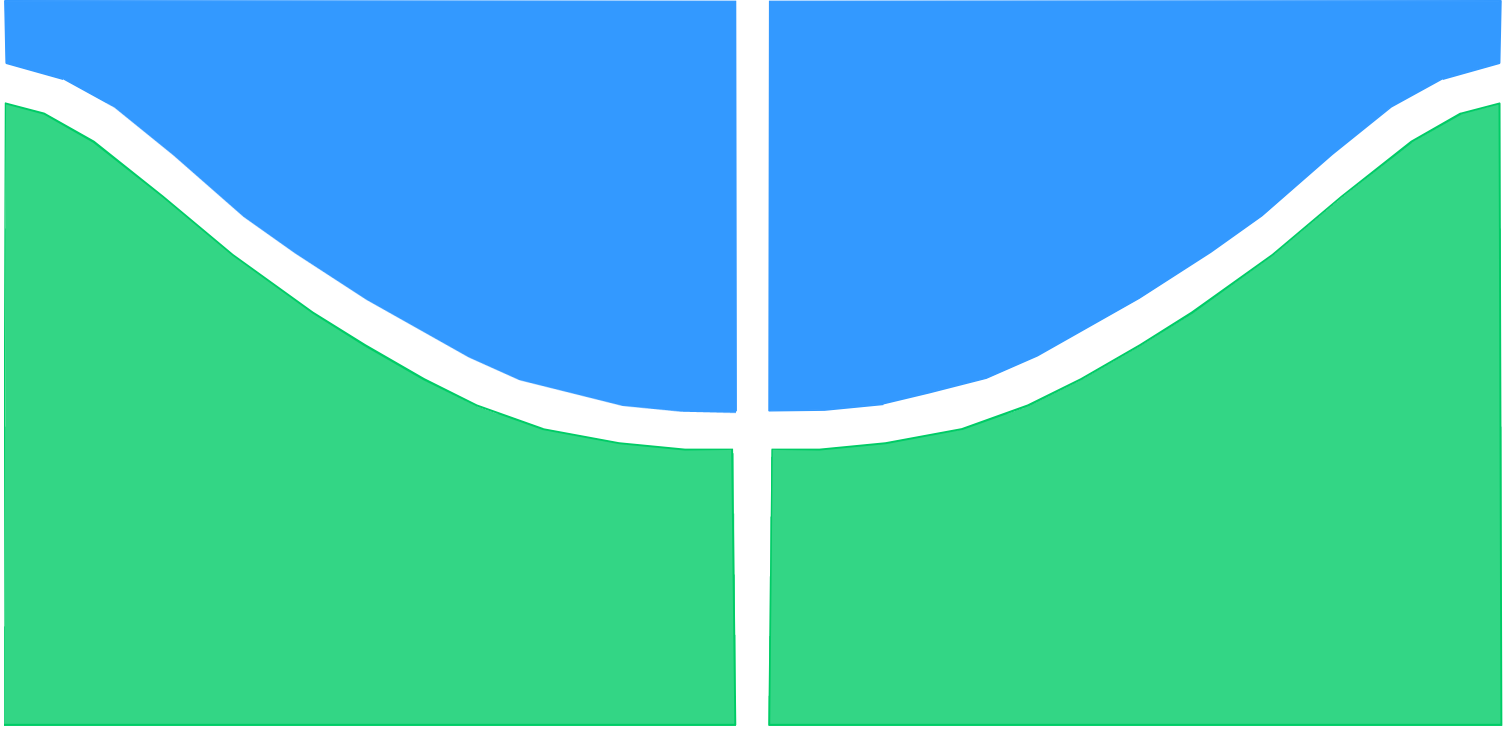

DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

RAFAEL SANTOS REIS

LEONARDO SANTIAGO SPÍNDULA THOMAZ

TRABALHO DE CONCLUSÃO DE CURSO EM ENGENHARIA DE REDES DE COMUNICAÇÃO

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

RAFAEL SANTOS REIS
LEONARDO SANTIAGO SPÍNDULA THOMAZ

ORIENTADORA: PROF. DRA. EDNA DIAS CANEDO
CO-ORIENTADOR: PROF. DR. LAERTE PEOTTA

TRABALHO DE CONCLUSÃO DE CURSO EM ENGENHARIA DE REDES DE COMUNICAÇÃO

BRASÍLIA, DF: JUNHO / 2015.

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

RAFAEL SANTOS REIS

LEONARDO SANTIAGO SPÍNDULA THOMAZ

TRABALHO DE CONCLUSÃO DE CURSO SUBMETIDO AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ENGENHEIRO DE REDES DE COMUNICAÇÃO.

APROVADO POR:

_____

PROFESSORA DOUTORA EDNA DIAS CANEDO, FGA/UNB (ORIENTADOR)

_____

PROF. DOUTOR LAERTE PEOTTA DE MELO, BANCO DO BRASIL (EXAMINADOR EXTERNO)

_____

PROF. DOUTOR RAFAEL TIMÓTEO DE SOUSA JÚNIOR, ENE/UNB (EXAMINADORA EXTERNA)

BRASÍLIA, DF, 23 DE JUNHO DE 2015.

FICHA CATALOGRÁFICA

REIS, RAFAEL SANTOS, LEONARDO SANTIAGO SPÍNDULA THOMAZ.
DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO [Distrito Federal], 2015.
XV, 69p., 210 x 297mm (ENE/FT/UnB, Engenharia de Redes de Comunicação, 2012).
Trabalho de Conclusão de Curso – Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. DNS
2. DNSSEC
3. Segurança

I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

REIS, R. S., L. S. S. T. (2015). DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO. Trabalho de Conclusão de Curso em Engenharia de Redes de Comunicação, Publicação ENE.DM-123/15, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 69p.

CESSÃO DE DIREITOS

AUTORES: RAFAEL SANTOS REIS

LEONARDO SANTIAGO SPÍNDULA THOMAZ

TITULO DA TESE: DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

GRAU / ANO: Engenheiro de Redes de Comunicação / 2015

Rafael Santos Reis
SQN 314 BL. G AP 211
Asa Norte
CEP: 70767-070 – Brasília – DF

Leonardo Santiago Spíndula Thomaz
QI 31 BL 13 AP 309 GUR 3
Guará 2
71065-310 – Brasília –DF

AGRADECIMENTOS

Leonardo Santiago Spíndula Thomaz

"Agradeço a Deus por tudo que me deu, aos meus pais por toda dedicação e sacrifício sem medidas que fizeram durante toda minha vida, aos meus irmãos Lucas e Fernanda por terem divido comigo tantos momentos importantes, à minha namorada Ariel por todo apoio, incentivo e amor que ofereceu durante este tempo, e aos meus colegas e amigos, Ricardo, Alysson e Rafael que me ajudaram muito durante toda a trajetória do curso de Engenharia. Sou muito grato a todos os professores, em especial, Laerte Peotta e Edna Canedo pela orientação deste trabalho."

Rafael Santos Reis

"Sou grato a todos aqueles que me ajudaram a chegar a este momento tão desejado. Agradeço, primeiramente, aos meus pais pelo incentivo e paciência que tiveram comigo durante os meus momento de dificuldade; à minha família por estarem presentes quando busquei conselhos ou simplesmente porque queria passar momentos juntos; aos meus amigos do ensino médio pela lealdade e crescimento que compartilhamos durante nossa jornada, especialmente a Gustavo Carvalho, Víctor Chagas, Vítor Makoto, João Victor de Paula, Matheus Oberg, Paulo Herrera, Amanda Panhol e Hugo Marello; ao grupo Ohana por todas as batalhas que encaramos juntos e por fazerem o curso de Engenharia de Redes tão mais divertido, especialmente a Leonardo Thomaz, Ricardo Gonçalves, Alysson Ribeiro, Annita de Oliveira, Carla Caldas; aos professores do Departamento de Engenharia Elétrica por todo o conhecimento compartilhado e pela paciência durante as aulas, especialmente Laerte Peotta e Edna Canedo.

Em memória de Maria de Lourdes Santos."

RESUMO

DNSSEC: ASPECTOS GERAIS DE SEGURANÇA, EFICIÊNCIA E ESTATÍSTICAS DE USO NO CONTEXTO BRASILEIRO

Autores: Rafael Santos Reis e Leonardo Santiago Spíndula Thomaz
Orientadora: Professora Dra. Edna Dias Canedo
Co-orientador: Professor Dr. Laerte Peotta
Trabalho de Conclusão de Curso em Engenharia de Redes de Comunicação
Brasília, 23 de Junho de 2015.

Este trabalho estuda o funcionamento dos sistemas DNS e DNSSEC, além de analisar alguns aspectos desses mecanismos, tais como desempenho, eficiência, estatísticas de uso e fraudes, incluindo técnicas de segurança em redes locais. O DNS é um dos principais pilares da Internet. Ataques bem-sucedidos a servidores responsáveis por este serviço podem gerar grandes prejuízos para empresas e até mesmo para usuários finais comuns. O estudo dos mecanismos DNS e DNSSEC é de fundamental importância para garantir as imunidades a esses sistemas e assegurar o bom funcionamento da Internet. Além disso, abordaremos conceitos gerais relacionados a segurança de redes, mencionando o funcionamento dos principais ataques e como evitá-los. Experimentos serão realizados a fim de evidenciar vunerabilidades do DNS que podem ser corrigidas pelo DNSSEC, além de uma metodologia de detecção de malware através do DNS.

ABSTRACT

DNSSEC: GERENAL ASPECTS OF SECURITY, EFFICIENCY ANALYSIS AND USE STATISTICS IN BRAZILIAN CONTEXT
Authors: Rafael Santos Reis e Leonardo Santiago Spíndula Thomaz
Supervisor: Professora Dr. Edna Dias Canedo
Trabalho de Conclusão de Curso em Engenharia de Redes de Comunicação
Brasília, 23 June 2015

This work studies the working of DNS and DNSSEC systems, besides analyze some aspects of those mechanisms, such as performance, efficiency analysis, use statistics and frauds, including local networks security techniques. The DNS is one of the pillars of the Internet. Successful attacks to servers responsible for this service may cause heavy losses to companies and even for regular final users. The study of DNS and DNSSEC mechanisms are of fundamental importance to guarantee immunities to these systems and to assure Internet's good functioning. Besides, we will approach general concepts related to network security, mentioning the workings of the main attacks and how to avoid them. Experiments will be performed to substantiate DNS vulnerabilities that can be corrected by using DNSSEC, furthermore a methodology to malware detection through DNSSEC.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

AD	*Authentic Data*
ARP	*Address Resolution Protocol*
ARPAnet	*Advanced Research Projects Agency Network*
ASCII	*American Standard Code for Information Interchange*
ASN	*Autonomous System Number*
AXFR	*Authoritative Transfer*
BIND	*Berkeley Internet Name Domain*
ccTLD	*Country Code Top Level Domain*
CD	*Checking Disabled*
CGI.Br	Comitê Gestor de Internet no Brasil
CNAME	*Canonical Name*
DAA	*Digest Access Authetication*
DDoS	*Distribuited Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DNAME	*Delegation Name*
DNS	*Domain Name System*
DNSKEY	*Domain Name System KEY*
DNSSEC	*Domain Name System SECurity extensions*
DoS	*Denial of Service*
DS	*Delegation Signer*
gTLD	*Generic Top Level Domain*
IANA	*Internet Assigned Numbers Authority*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ID	*Identification*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IXFR	*Incermental Transfer*
KSK	*Keys Signing Keys*
MAC	*Media Access Control*
MITM	*Man-In-The-Middle*
NSec	*Next secure*

RA	*Recursion Query Support Available*
RAM	*Random Access Memory*
RARP	*Reverse Address Resolution Protocol*
RFC	*Request For Comments*
RR	*Resource Record*
RRset	*Resource Record set*
RRSIG	*Resource Record SIGnature*
SLD	*Second Level Domain*
TCP	*Transmission Control Protocol*
TSIG	*Transaction Signatures*
TTL	*Time To Live*
TXT	*Text*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
ZSK	*Zones Signing Keys*

1 INTRODUÇÃO

A Internet foi criada baseando-se em modelos de camadas que possuem protocolos os quais executam tarefas específicas, padronizando o resultado de saída deste em um formato que será entendido pela próxima camada, independente do protocolo utilizado. Entre estes, existe o protocolo Internet Protocol (IP), utilizado na camada de rede, que é responsável pela a identificação de cada host de uma rede. A indentificação é feita por um número de 32 bits dividido em quatro octetos, por exemplo 192.168.0.1. Entretanto, esta identificação não é facilmente memorizada pelos usuários, principalmente pelos leigos.

A partir deste problema, surgiu o sistema *Domain Name System* (DNS), um dos mais importantes da Internet, que é responsável pela tradução de endereços escritos em ASCII em endereços IP's, tais como o descrito anteriormente, e vice versa. O DNS basea-se em uma base de dados hierárquica e distribuída, podendo usar uma memória cache para armazenar as consultas mais comuns, que agiliza muito o processo realizado, além de dificultar uma sobrecargar aos servidores envolvidos.

A eficiência e praticidade do DNS foi rapidamente notada e difundida, fazendo com que toda a internet utilizasse seus serviços para a resolução de nomes, principalmente em serviços web e e-mail. Apesar de seu ótimo funcionamento, o DNS não é perfeito. Como, por exemplo, ser vunerável a redundâncias, permitir que mais de um servidor armazene dados sobre um host ou zona.

Como o sistema DNS possui inúmeras vulnerabilidades, surgiu a necessidade de criar o *DNS Security Extensions* (DNSSEC). Esta extenção do DNS elimina grande parte das falhas de segurança deste sistema.

O protocolo DNS é uma das bases mais importantes de infraestrutura e é considerada crítica para o bom funcionamento da Internet (Hoepers, 2013). A tendência, especialmente no Brasil, é que este tipo de serviços seja cada vez mais utilizado, aumentando ainda mais a sua importância. Para isso, é necessário garantir que o DNSSEC seja implementado em todos os servidores DNS.

1.1 MOTIVAÇÃO

Como o DNS atingiu um patamar de suma importância nas comunicações entre computadores e passou a ser bastante difundido, esse serviço começou a ser alvo de disversos ataques, entre eles uma técnica conhecida como cache poisoning.

Então, foi desenvolvido o DNSSEC, que tenta solucionar as vulnerabilidades e garantir maior confiablilidade dos servidores DNS. Logo, entender o funcionamento do DNS e DNSSEC e seus conceitos é muito importante ao bom funcionamento da Internet.

O DNSSEC é uma ferramenta relativamente recente, e por ser de substancial valor para corrigir algumas vulnerabilidades do DNS, ainda necessita de estudos. O DNS foi proposto pela RFC 2535 de 1999, e ainda sim existem diversos servidores que não aplicam o protocolo corretamente, fazendo com que as falhas de segurança do DNS não sejam tratadas de forma apropriada.

1.2 OBJETIVOS DO TRABALHO

Os objetivos deste trabalho são explicar detalhadamente as operações do DNS e DNSSEC, definir conceitos de segurança de redes, revelar o funcionamento dos principais ataques existentes a este tipo de serviço atualmente, e realizar dois experimentos. Entre eles:

a. Executar um ataque de envenenamento de cache a um servidor DNS vulnerável e a outro servidor com o DNSSEC aplicado corretamente e realizar uma análise comparativa entre os dois.
b. Fazer um estudo sobre o panorama nacional no que se refere a segurança de DNS. Para isto será realizada uma varredura em todo o bloco de IPs reservado para o Brasil, levantando dados estatísticos sobre servidores de DNS abertos.

Será apresentado também, detalhes sobre a realização dos experimentos feitos assim como uma análise dos resultados obtidos. Além disso, será apresentada uma conclusão sobre todos os temas abordados neste trabalho.

1.3 ORGANIZAÇÃO DO TRABALHO

O Capítulo 2 oferece uma revisão dos principais conceitos sobre o protocolo DNS original, além de uma explicação detalhada sobre seu funcionamento e suas características.

No Capítulo 3 é apresentado algumas considerações sobre conceitos de segurança de redes. Além disso, exibiremos os principais ataques realizados a sistemas DNS evidenciando seus funcionamentos.

O Capítulo 4 detalha a operação do DNSSEC e de seus mecanismos de segurança.

O Capítulo 5 será sobre os experimentos realizados neste trabalho, explicando os procedimentos, e uma análise dos resultados obtidos.

No Capítulo 6 será realizada uma conclusão sobre este trabalho.

2 DOMAIN NAME SYSTEM (DNS)

O Domain Name System (DNS) ou Sistema de Nomes de Domínio é um dos pilares fundamentais da Internet. É um protocolo da camada de aplicação que utiliza a porta 53, com o uso do protocolo User Datagram Protocol (UDP) para consultas e o Transmission Control Protocol (TCP) para transferência de zonas, conceito que será explicado mais adiante. Sua função é traduzir nomes escritos em ASCII para endereços IP, facilitando a memorização de sites, e funciona basicamente como um banco de dados distribuído que utiliza uma hierarquia de servidores para realizar consultas de forma rápida e eficiente. (ALBITZ,LIU; 2005)

Vamos supor que um certo cliente queira acessar uma página web através de um browser. Sua máquina, que desconhece a URL desejada, enviará uma mensagem contendo o endereço do servidor DNS, como destino do pacote, e o nome a ser consultado, como conteúdo do pacote, pela porta 53 utilizado o protocolo de transporte UDP. Se o servidor for recursivo, ele verificará em seu cache o endereço e, caso encontre, responderá imediatamente a mensagem, caso contrário, fará uma consulta a outro servidor DNS que pode ser recursivo ou autoritativo. Se este novo servidor souber a resposta, ele responde com o endereço IP correspondente a URL, caso contrário, indicará outro servidor DNS a ser consultado. Servidores recursivos realizam a consulta para um resolver ou outro servidor recursivo, enquanto o autoritativo responde com um endereço IP relacionado a URL consultada, se o endereço consultado for de ser domínio, ou retorna um endereço IP de onde aquela formação pode ser encontra

Servidores de nome, como são chamados os servidores DNS, geralmente possuem informações completas sobre uma parte de todo espaço de domínios. Essas partes de domínios são chamada zonas que carregam as informações de um arquivo ou de outro servidor DNS. Pode-se dizer que este servidor de nome possui autoridade sobre essa zona, ou seja, é um servidor autoritativo.

Servidores DNS geralmente rodam sistemas operacionais UNIX com o software Berkeley Internet Name Domain (BIND).

2.1 HIERARQUIA DE DOMÍNIOS

A estrutura hierárquica de nomes, também conhecida como, árvore de nomes funciona de acordo com a Figura 1:

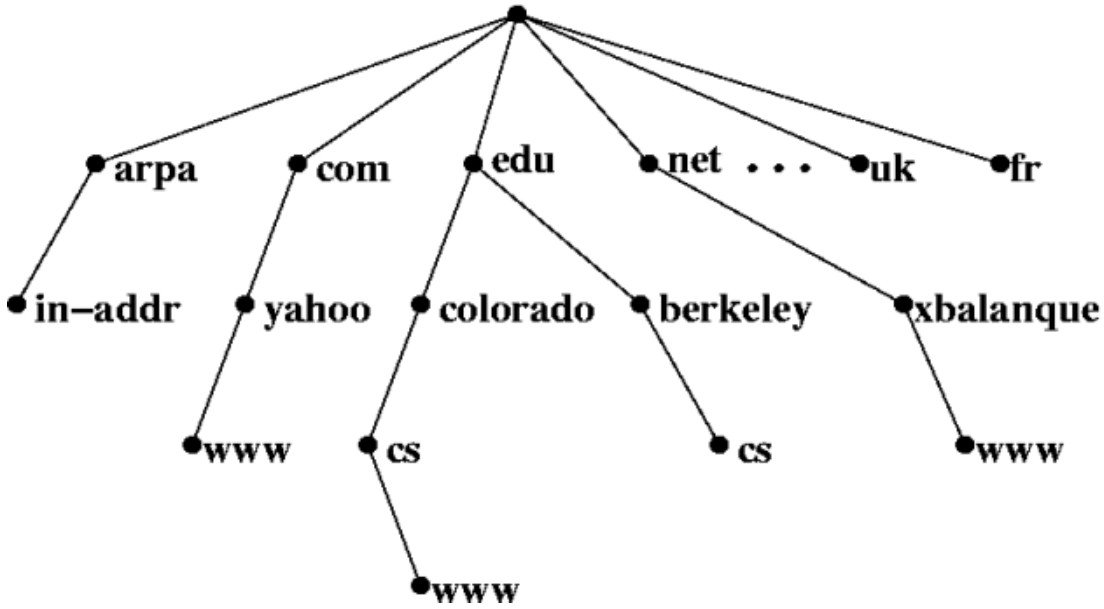

Figura 1 - Árvore de Nomes (O'REILLY, 2001)

Esta árvore descreve a estrutura do espaço de domínios. Os servidores no topo desta são chamados de servidores ou diretórios raiz e possuem apontadores para os servidores Top-Level Domain (TLD). Servidores TLD são os logo abaixo do root e apresentam apontadores aos Second-Level Domain, que são os servidores de segundo nível.

Os TLDs ser dividem em dois tipos: g TLD (generic Top-Level Domain), que são os servidores genéricos, e cc TLD (Country Code Top-Level Domain), que são os servidores territoriais. Os TLD eram divididos em sete domínios: .com, para corporações comerciais, .edu, para instituições de educação, .gov, para orgãos do governo, .mil, para organizações militares, .net, para de provedores de rede e internet, .org ,para entidades não-comerciais, e .int para organizações internacionais. Atualmente não existem restrições para o registro de domínios .net, e este pode ser usado como um segundo .com. Atualmente o .net é o terceiro domínio mais utilizado. (What Does .NET means?,VeriSign)

A combinação de TLDs com SLDs é chamada nome de domínio que é escrito da direita esquerda para a direita. O SLD vem à esquerda seguido do TLD, por exemplo, www.aprender.unb.br. O domínio .unb é o SLD e o .br é o ccTLD. Os nomes de cada componente podem ser de até 63 caracteres e todo conjunto não pode ultrapassar 255

caracteres. Além disso, o DNS não é case sensitive, ou seja, não diferencia letras maiúsculas de minúsculas. Por exemplo, www.aprender.unb.br exibe o mesmo resultado de WWW.APRENDER.UNB.BR.

2.2 ÓRGÃO REGULADOR, AUTORIDADES E DELEGAÇÕES

A *Internet Corporation for Assigned Names and Numbers* (ICANN) é uma organização sem fins lucrativos e âmbito internacional responsável pela distribuição de endereços IP, pelo o controle de TLDs e com o funções de administração central na rede de servidores. Além disso, é recebe e processa a todas as solicitações de novos TDLs e pedidos de mudança entre os TLDs. Antigamente, essas tarefas eram cumpridas pela *Internet Assigned Numbers Authority* (IANA) mediante a contratos com o governo dos Estados Unidos da América.

A cada nó de cada nível hierárquico da árvore de nomes são atribuídas autoridades que são responsáveis pela operação e gerencia de cada nó. Esta autoridade pode ser delegada a outros sub-domínios daquele nó. Essa delegação é uma das responsáveis pelas características de distribuição dos sistemas DNS devido a descentralização da administração. Como por exemplo, a identidade responsável por adotar procedimentos e políticas aos SLDs é delegada pelos administradores de TLDs.

2.3 FUNCIONAMENTO DO DNS

Durante a década de 70, a ARPAnet, precursora da Internet, consistia em uma pequena e amigável comunidade de algumas centenas de hosts. Um único arquivo, HOSTS.TXT armazenava o mapeamento host-IP de cada host conectado à ARPAnet e apenas um único servidor era responsável pela distribuição deste documento.

Com a implementação dos protocolos TCP/IP, a população de hosts da ARPAnet cresceu significamente ocasionando em diversos problemas: tráfego e carga (o único servidor não conseguia atualizar e distribuir o hosts.txt rápido o suficiente), colisões de nome (mais de um host podiam ter o mesmo nome, entretanto, no documento txt, o IP seria único para todos) e consistência (devido ao grande número de usuários, quando o hosts.txt chegava à determinado host, o arquivo já estaria desatualizado).

Atualmente, pra conseguir traduzir uma URL para IP, um cliente deve realizar uma consulta a um servidor DNS. Este processo é chamado de resolução de nome. O cliente que acessa um servidor de nome é chamado *resolver*. Softwares que rodam em um host e

necessitam de informações no espaço de domínio usam o *resolver*. O *resolver* é identificar a necessidade de um software usar os serviços de tradução de nome, interpretar a resposta deste servidor e retornar esta resposta ao programa que necessitou desta consulta.

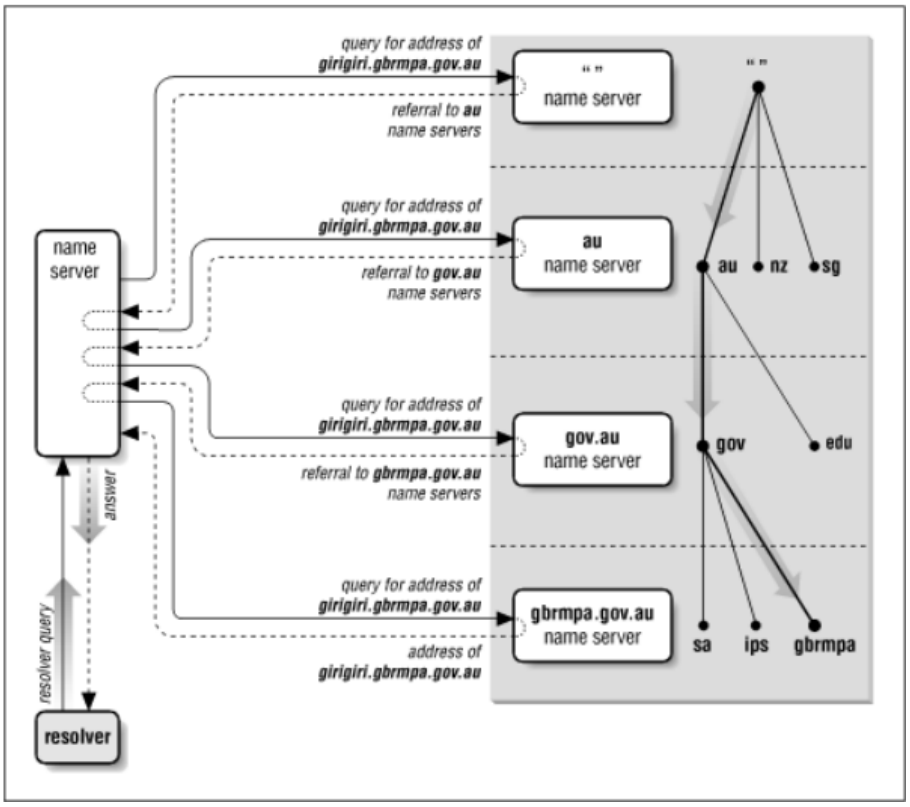

Figura 2 - Resolução de Nomes (DNS& BIND, 2005)

No exemplo da Figura 2, o cliente faz uma consulta ao servidor DNS local, através do resolver, a fim de traduzir o endereço girigiri.gbmpa.gov.au. Este servidor, então, faz uma pesquisa ao servidor raiz que responde com o endereço do *Country-Code Top-level Domain* (ccTLD) correspondente ao au. O servidor local, então faz a mesma consulta, mas desta vez, ao servidor au que responde com o endereço do servidor com autoridade ao domínio gov.au. A mesma consulta é realizada mais uma vez ao servidor gov.au que responde com o IP do servidor gbrmpa.gov.au. O DNS local realiza a mesma consulta ao servidor gbrmpa.gov.au que finalmente responde com o endereço equivalente à URL girigiri.gbmpa.gov.au. Por fim, o servidor local responde ao cliente o último resultado de sua consulta.

2.4 SERVIDORES RAIZ

Existem, atualmente, 13 servidores raízes espalhados pelo globo terrestre nomeados de A à M, onde cada letra corresponde a um único servidor raiz. Estes servidores são replicados em diversas localidades, entretanto corresponde a um mesmo IP. São no total 439 servidores onde 19 se encontram no Brasil e a maioria dos servidores se encontram espalhados pela Europa, somando um total de 139 servidores.

A distribuição dos servidores raízes se encontra no site www.root-servers.org e pode ser verificada na Figura 3.

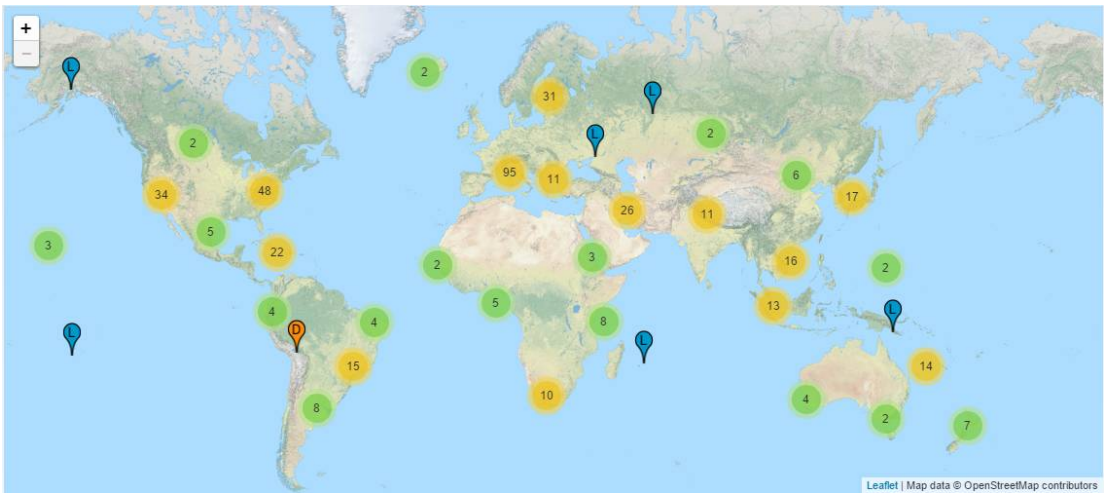

Figura 3 - Distribuição dos servidores raízes (ROOT-SERVERS.ORG, 2015)

No Brasil, existem 19 servidores raízes. A maioria desse servidores são de nome L e se encontram em Belém, Fortaleza, Natal, Salvador, Uberlândia, Belo Horizonte, São Gonçalo, Londrina, Curitiba e Florianópolis. Cada uma dessas cidades possui um único servidor raiz. As cidades que possuem mais de um servidor raiz são listados na tabela 1.

Cidade	Nome	Quantidade	IP	ASN	Operadores
Porto Alegre	I	1	192.36.148.17	29216	Netnod
	L	1	199.7.83.42	20144	ICANN
São Paulo	E	1	192.203.10	297	NASA Ames Research Center
	F	1	192.5.5241	3557	Internet Systems Consortium, Inc.
	L	2	199.7.83.42	20144	ICANN
Brasília	J	1	192.58.128.30	26415	Verisign, Inc.
	L	1	199.7.83.42	20144	ICANN

Tabela 1 - Servidores raízes no Brasil.

A Figura 4 evidencia as características de cada servidor raiz.

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Figura 4 - Características de servidores raiz (IANA, 2015)

A função desses servidores é indicar a lista de servidores autoritários pelo TLD de acordo com a consulta realizada por um servidor DNS qualquer.

Desde 2004, a ICANN é responsável por manter as listas de servidores para cada TLD atualizada, esta lista é chamada de arquivo *master*. Este arquivo é transmitido de forma segura para todos os servidores raízes de uma forma em que não pode ser visto publicamente. A Figura 5 mostra o como é realizada a distribuição do arquivo *master*.

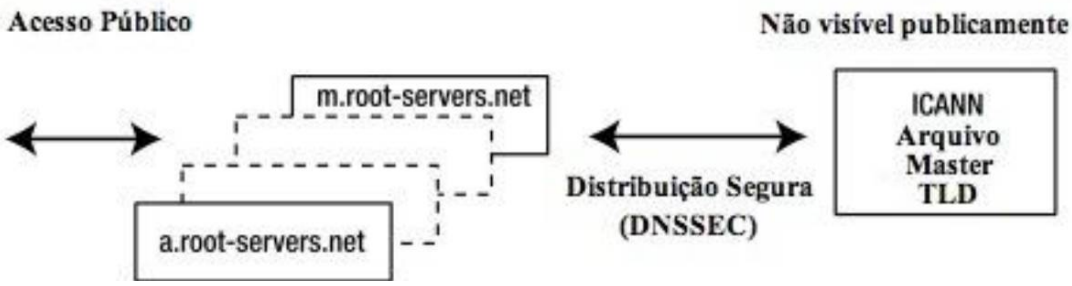

Figura 5 - Distribuição do arquivo *master* (FREIDMANN, 2010)

2.5 SERVIDORES TOP-LEVEL DOMAIN

Os servidores TLD são divididos em duas categorias: gTLD (Genéricos) e ccTLD (Territoriais). Estes servidores estão abaixo apenas dos servidores raízes na hierarquia DNS e são responsáveis por responder consultas com a lista de servidores SLD equivalente a requisição. Além disso, são responsáveis por manter estas listas atualizadas e distribui-las a outros TLDs.

2.5.1 Generic Top-Level Domain

Maior parte dos gTLDs são controlados pelo ICANN através de contrato. Além disso, existem dois tipos de entidades envolvidas com os gTLDs: os Operadores de Registro e os Registradores de Domínio (Registars).

Os Operadores de Domínio são responsáveis pela operação e gerenciamento de gTLDs segundo a contratos com o ICANN, onde para cada gTLD existe um operador. Além disso, recebem a lista de servidores SLD pelos Registradores e repassam ao nível inferior da hierarquia. Operadores podem ser também Registradores. Operadores não interagem com o público.

Quando solicitações são feitas aos gTLDs por servidores raízes, estes respondem com a lista de servidores do respectivo gTLD.

Os Registradores de Domínio ou *Registrars* são responsáveis pela a venda, renovação e registro de domínios ao público, também dependem de contratos com a ICANN. Atualmente, existem 150 *registrars* que comercializam domínios .com e .net.

O registrar mantém todas as informações necessárias, como nome do domínio registrado, nome e IP dos servidores autoritários pelo domínio, contatos administrativos e técnicos e etc, e são responsáveis por passar essa informações aos Operadores.

Ao receber um nome de domínio solicitado por um usuário, o *registrar* verifica a disponibilidade do nome com o operador de registros responsável pelo TLD correspondente. Caso esteja disponível, o *registrar* registra o nome junto ao operador, que o coloca em sua base de dados. Ninguém poderá registrar o mesmo nome durante o período de vigência que dura aproximadamente 10 anos. A Figura 6 mostra como é realizada a comunicação entre operadores e *registrars*.

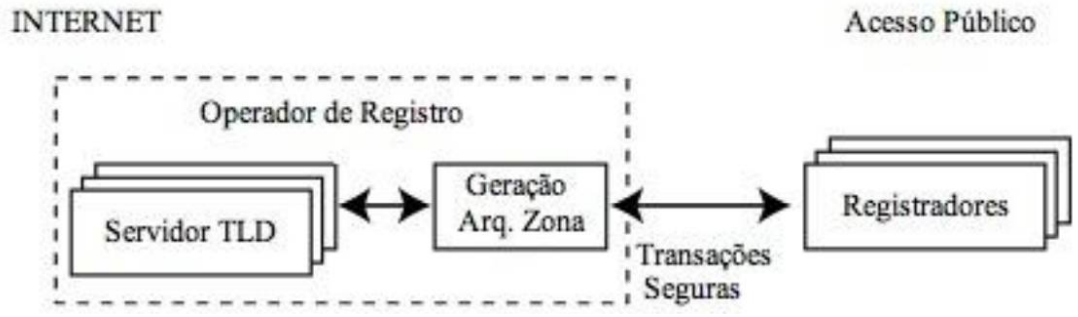

Figura 6 - Comunicação entre operadores e *registrars* (AITCHISON, 2005).

2.5.2 Country-Code Top-Level Domain

Os ccTLD ou Domínios Territoriais de Alto Nível também são controlados pela ICANN e consistem por dois caracteres que especificam o país de tal serviço. Como por exemplo .br (Brasil), .uk (Reino Unido) e .jp (japão).

A ICANN delega os cuidados dos ccTLD para autoridades a entidades respectivas de cada país chamadas de Gerenciadoras de Código. No Brasil, tal entidade Gerenciadora de Código é o Comitê Gestor de Internet no Brasil (CGI.Br).

A IANA mantém a lista de entidades responsáveis por cada domínio no site: http://www.iana.org/domains/root/db.

2.6 ZONAS, SERVIDORES MESTRES E ESCRAVOS.

Servidores de nome possuem informação total de uma parte do espaço de domínios. Estas partes correspondentes a um servidor de nome são chamadas zonas. A organização por zonas se faz necessária para distribuir a carga de requisições de domínio que chegam aos servidores de nível mais alto. Consequentemente, essa distribuição evita a sobrecarga de servidores, aumentando a disponibilidade de tal serviço. Além disso, a organização por zonas é uma estrutura que visa a descentralização da informação, a fim de prover mais agilidade, segurança e maior velocidade ao sistema. A Figura 7 representa bem o sistema de zoneamento.

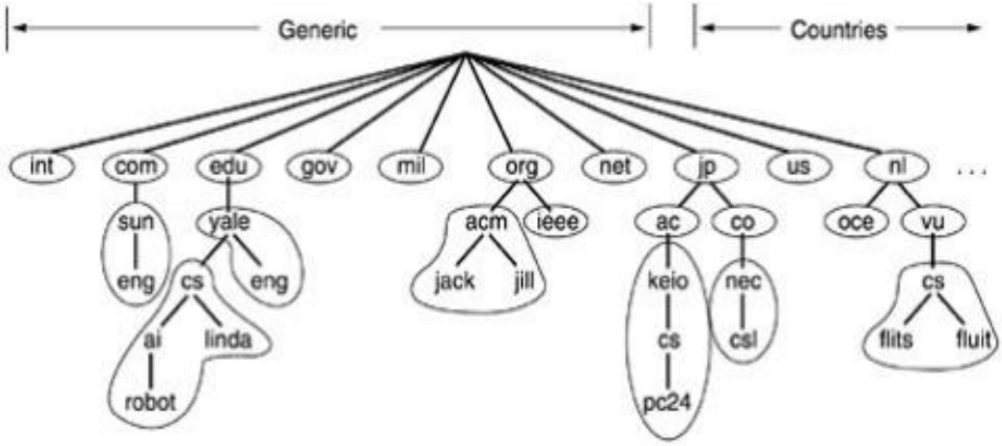

Figura 7 - Divisão em zonas (TENENBAUM, 2003)

O domínio eng.yale.edu possui um servidor de nomes yale.edu que atende a eng.yale.edu, mas não atende a cs.yale.edu pois estão localizados em zonas diferentes e cada um possui servidores de nomes diferentes. Caso haja uma solicitação para saber o endereço

IP de ai.cs.yale.edu, o domínio cs.yale.edu terá autoridade para respondê-lo, ou seja, possui o arquivo com as informações para essa solicitação. Já no caso de fazer uma pergunta a um servidor de nomes que não está em sua zona, o mesmo não terá autoridade para isso. Se ele possuir essa informação em cache, que pode ou não estar desatualizada, responderá de forma não autoritária. Caso ele não tenha a informação em cache de jeito algum, começa a mandar a solicitação a instâncias superiores. Na ordem, inicia-se pelo servidor raiz, servidor TLD, servidor SLD e assim por diante, até chegar ao endereço requisitado. (IWASA&; HILÁRIO, 2011)

Em cada zona existem pelo menos dois servidores, afim de evitar a falta de disponibilidade de serviço. Além disso, existem 2 tipos de servidores: o mestre e o escravo. O servidor mestre possui um arquivo de zona, ou seja, possui o arquivo que armazena todas as informações de respectiva zona. O servidor escravo possui uma cópia de seu respectivo arquivo de zona e sua função é responder consultas DNS caso o mestre falhe por algum problema (problemas de equipamento, serviço de Internet, etc....). Por motivos de segurança, é recomendado que pelo menos um servidor mestre não seja visível publicamente.

Qualquer atualização nos arquivos de zona de um servidor mestre provoca, automaticamente, atualizações nos arquivos do escravo também. Este processo de atualização dos arquivos do escravo é chamado de transferência de zona. Nessa transferência de zona, os arquivos que contém dados de domínios são copiados para o servidor escravo, exatamente como estavam no servidor mestre. Os servidores são considerados sincronizados quando não há necessidade de transferência de zona.

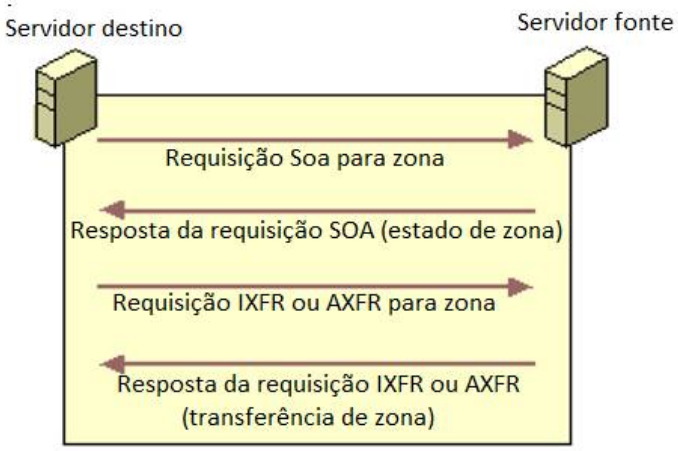

Figura 8 - Transferência de Zona (Adaptado de MICROSOFT, 2005)

A figura 8 representa o processo de transferência de zonas e pode ocorrer de duas formas: completa (AXFR) ou incremental (IXFR). A transferência incremental atualiza somente as informações que sofreram alterações, enquanto a transferência completa atualiza arquivo por inteiro. Nas transferências de zonas, é utilizado o protocolo TCP a fim de garantir a entrega aos servidores escravos.

2.7 USO DO CACHE EM DNS

Anteriormente, analisamos o processo realizado pelo resolver a fim de obter o endereço IP de um sistema final. Adotar a memória cache em servidores DNS faz com que o número de mensagens trocadas diminua drasticamente e assim otimizando todo o sistema de resolução de nomes.

Ao fazer solicitações, um servidor de nomes armazena tanto os nomes quanto os endereços em sua memória RAM. Assim, quando algum host fazer-lhe a mesma consulta, este servidor enviará a resposta, sem a necessidade de outra consulta. Este processo é responsável por toda otimização do tráfego do sistema DNS.

Quando essas informações são armazenadas no cache, são indexadas a elas um campo conhecido como Time To Live (TTL). Este campo é responsável indicar a permitir a permanência de tal informação durante certo período de tempo. Já que o mapeamento de endereços IP pode estar, ou não, em constante mudança, este processo evita que as informações estejam desatualizadas. O valor do TTL é de geralmente dois dias.

Apesar da eficiência do emprego de cache em DNS, esta técnica gera também algumas vulnerabilidades. O *cache poisoning* ou envenenamento de cache é um dos ataques que explora este método. O envenenamento de cache, assim como, outros ataques serão explicados mais adiante.

2.8 REGISTROS DE RECURSOS

Os campos de informação contidos nos arquivos de zona de cada servidor de nome são chamados de registros de recursos (RR). Os RR refletem informações importantes para a resolução de nomes, como, as URLs e IPs relacionados a aquele domínio. Em um mesmo domínio, pode existir um ou mais RRs relacionados a eles.

Basicamente, a resposta obtida por um servidor DNS nada mais é do que a *resource code* encontrada no servidor ocupado. Cada RR ocupa uma linha no arquivo de zona e é

divido em 5 campos, cada um com uma informação diferente, conforme com o quadro abaixo.

Figura 9 - Campos do RR (IWASA & HILÁRIO, 2011)

O campo *Name* é responsável por manter no nome do domínio associado ao endereço IP de uma máquina. Este campo precisa ser igual ao nome recebido pela requisição a fim de obter o resultado desejado.

O *TTL*, como citamos anteriormente, é responsável por indicar o tempo de vida daquela informação no arquivo de zona. Quando este campo é zerado, o registro de recurso que o contém é removido do arquivo. Caso ocorra uma consulta com mesmo nome e o registro foi apagado, pois seu TTL foi zerado, a informação é readicionada e, caso necessário, atualizada no arquivo.

Class representa o tipo de classe do registro armazenado. No caso da internet, este campo é, quase sempre, preenchido com o campo IN. Podem existir outros tipos de classe em um arquivo de zona, entretanto são difíceis de serem encontradas em servidores de nome.

O campo *Type* indica o tipo de RR que se tem. Existem vários tipos de registros, alguns obrigatórios e outros opcionais. A figura 10 exibe alguns tipos e suas descrições.

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Figura 10- Tipos de RR (TANEMBAUM, 2003)

O campo *Value* contém o endereço relacionado ao nome no campo *Name*. Este depende do campo *Type*.

O conjunto de RRs que possuem o mesmo nome de domínio, classe e tipo é chamado de *Resource Record Set* (RRset).

2.9 CONSULTAS DNS

2.9.1 Consultas Recursivas

Este tipo de consulta é a padrão a um servidor de nomes, ou seja, todos os servidores respondem este tipo de consulta e não são necessários *flags* de cabeçalho para indicar este tipo de resposta.

Uma consulta recursiva funciona da seguinte forma: o servidor de nomes solicitado realiza todas as outras consultas necessárias para obter a resposta e a transmite ou retorna um erro (problemas na rede, domínio inexistente, etc....). Neste tipo de consulta, o servidor realiza diversas transações de mensagens DNS com outros servidores até este obter a resposta desejada. A resposta da consulta indicará se os dados são autoritários ou são de cache.

Mesmo se o servidor não obter autoridade sobre o nome desejado, ou a informação em cache, ele iniciará a o processo de consulta fazendo solicitações a um servidor raiz. Após isso, o servidor raiz indicará os endereços IP dos servidores de maior nível. O servidor recursivo então, fará a consulta para aos TLDs e assim por diante.

O *Resolver*, instalado em todos PC, e o servidor de nomes planejam entre si o uso da consulta com recursividade, ou seja, bits de cabeçalho são incluídos na mensagem. O solicitação realizada com o bit *Recursion Desired (RS)* ativado e receberá a resposta do servidor, caso tenha suporte para este tipo de serviço, com o bit *Recursion Query Support Available (RA).*

Figura 11 - Consulta Recursiva (FREIDMAN,2010).

A figura 11 representa o funcionamento de uma consulta recursiva. Agora suponha que um usuário queira acessar uma página web www.exemple.com. Os passos realizados, segundo (FREIDMAN, 2010), utilizando uma consulta recursiva, que solicita a um servidor que possui suporte a este tipo de serviço, mas não possui autoridade em relação ao nome solicitado, são:

1. O usuário digita, no campo disponível em seu navegador, o endereço www.exemple.com
2. O *browser* envia uma solicitação ao *resolver* perguntando o endereço IP da URL desejada.
3. O *resolver* então solicita ao servidor local de nomes a resolução do endereço www.exemplo.com, com o bit RD ativado.
4. O servidor local procura em seu arquivo de nomes pelo endereço desejado, mas não o encontra.
5. O servidor local envia a solicitação a um servidor raiz.
6. O servidor raiz, que só realiza consultas iterativas, responde o servidor local com a lista de gTLDs responsáveis pelo domínio .com.
7. O servidor local escolhe um dos endereços da lista de acordo com um algoritmo (por exemplo menor *round trip time* – RTT) e refaz a solicitação
8. O servidor TLD suporta apenas consultas iterativas. Este responde com a lista de servidores de autoridade secundários (SLD) para exemple .com.
9. O servidor local então escolhe um dos SLDs e refaz a consulta.
10. O servidor autoritário solicitado responde com o endereço IP da URL desejada ao servidor local.
11. O servidor local envia ao *resolver* a resposta obtida.
12. O *resolver* envia a resposta ao browser.
13. Finalmente, o browser solicita a página web ao endereço IP de www.exemple.com.

Em geral, os servidores de nomes locais usados por máquinas de usuários devem responder de forma recursiva. Assim, evitam o retorno das respostas ao Resolver e aumentam a velocidade de resposta ao browser. (FREIDMAN,2010).

2.9.2 Consultas Iterativas

Neste caso, se o servidor obter a respostas, ele a enviará indicando se os dados são autoritários ou são do cache. Caso o contrário, ele enviará um erro (problemas de rede, domínio inexistente, dentre outros.) ou responderá com alguma informação útil, mas que

ainda não é a desejada. Neste tipo de consulta, caso o servidor não possuir a resposta, ele não realizará consultas no lugar do cliente.

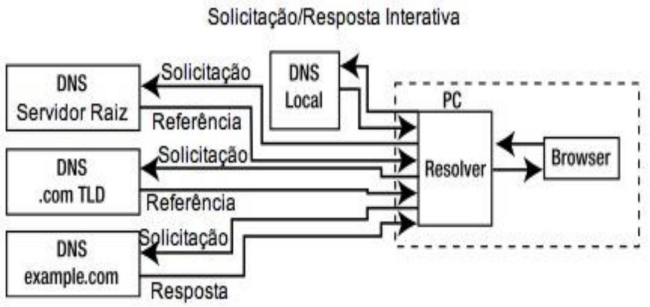

Figura 12 - Consultas Iterativas (FREIDMAN, 2010).

A figura 12 evidencia este processo para uma consulta de endereço para www.exemple.com. Os passos desta consulta, segundo (FREIDMAN, 2010), serão explicados a seguir, supondo que é uma solicitação iterativa simples a um servidor que não possui suporte recursivo ou autoridade de domínio exemple.com.

1. O usuário digita, no campo disponível em seu navegador, o endereço www.exemple.com
2. O *browser* envia uma solicitação ao *resolver* perguntando o endereço IP da URL desejada.
3. O *resolver* então solicita ao servidor local de nomes a resolução do endereço www.exemplo.com. O bit RD será irrelevante, pois o servidor não possui suporte à consulta recursivas.
4. O servidor solicitado procura pelo endereço requerido em sua tabela de endereços, armazenado no cache, mas não o encontrar. Este servidor, então, envia ao *resolver* uma lista de endereços de servidores raiz.
5. O *resolver* faz a consulta a um servidor raiz. O servidor local não é envolvido em nenhum dos passos seguintes.
6. O servidor raiz responde a requisição com a lista dos servidores gTLDs responsáveis por aquele domínio (.com).
7. O *resolver* seleciona um dos servidores da lista e refaz a consulta ao gTLD selecionado.
8. O servidor gTLD responde com a lista de servidores SLD responsáveis pelo domínio exemple.com.
9. O *resolver* refaz a solicitação desta vez ao servidor SLD selecionado na lista recebida.

10. O servidor autoritário responde para o *resolver* com o endereço IP de www.exemple.com
11. O *resolver* envia a resposta ao browser.
12. Finalmente, o browser solicita a página web ao endereço IP de www.exemple.com.

3 SEGURANÇA DE REDES DE COMPUTADORES E ATAQUES

3.1 VISÃO GERAL DE SEGURANÇA

Segurança pode ser definida como um contínuo processo de se proteger um objeto de um ataque. O tal objeto pode ser uma pessoa, uma organização, propriedade ou dados. Quando se considera um sistema computacional, sua segurança envolve a proteção de todos os seus recursos (KIZZA, 2005). O principal parte ao se desenvolver sistemas seguros é entender quais tipos de ameaças são aceitáveis e variam de acordo com o tipo de serviço e a quantidade de acessos e usuário ao servidor.

Para um servidor ser considerado seguro, eles deve cumprir certos objetivos básicos: confidencialidade, integridade, disponibilidade, autenticação, autorização e auditabilidade.

A integridade refere-se à proteção a mudanças não autorizadas. Os dados do transmissor têm que ser idênticos aos dados recebidos pelo transmissor. O conteúdo da mensagem não pode ser alterado, intencionalmente ou não.

No caso de sistemas DNS, a integridade é um conceito fundamental para sua segurança. Caso o um usuário solicite uma informação a um servidor que não adapta esta definição apropriadamente, o atacante pode alterar a resposta de uma consulta para um site malicioso podendo gerar sérios danos ao usuário.

A disponibilidade indica que um serviço é protegido a interrupções de serviço. Os dados do usuário devem se manter acessíveis. Este aspecto é comprometido a ataques de negação de serviço. Um servidor DNS, por exemplo, deve manter sua disponibilidade alta para poder realizar consultas solicitadas por usuários em qualquer período de tempo.

Ataques de negação de serviço podem causar prejuízos enormes, sejam no sentido econômico, por exemplo um ataque à bolsa de valores, ou criar outros problemas de segurança, visto que alguns operadores de serviço podem parar de monitorar e controlar determinado sistema.

Confidencialidade refere-se ao acesso indevido de usuários não autorizados à uma informação, como é o caso de grampos telefônicos e escutas. As mensagens devem ser codificadas para garantir que, mesmo se um atacante intercepta-las, elas não sejam possíveis de serem interpretadas por terceiros.

Este é aspecto é de fundamental importância, por exemplo, em serviços de correio eletrônico. Caixas postais eletrônicas devem estar sempre protegidas. Acessos indevidos à

mensagens de usuários podem provocar perdas financeiras, quebra de sigilo, dentre outros malefícios.

Autenticação refere-se a identificar a verdadeira identidade do usuário. Nas autenticações, são rastreados dados cadastrais dos usuário, no qual cada acesso é conhecido e registrado.

Garantir autorização ou controle de acesso permite ao sistema controle sobre ações e acessos a cada casta da hierarquia de usuários que deve ser definida pelo sistema. Um sistema que garante este aspecto, restringir e armazenar informações sobre modificações ocorridas no sistema. As permissões de cada casta na hierarquia também devem ser definidas no sistema. Por exemplo, um usuário comum deve ter mais restrições do que um administrador da rede.

A Auditabilidade trata da possibilidade de ser realizada uma auditoria e em obter-se um relatório das alterações e operações realizadas em tal sistema em certo período de tempo desejado. Conseguir um histórico completo das operações e do comportamento do sistema, tendo como base os registros de todas as ações relevantes, é o principal objetivo da auditabilidade. (IWASA & HILÁRIO, 2011).

Com um sistema que garante auditabilidade, é possível identificar o porquê comportamentos anormais acontecem no sistema, mesmo sem autenticação. A única diferença entre sistemas com e sem autenticação que oferecem auditabilidade é que no com autenticação é possível detectar o usuário malicioso, por exemplo, enquanto no outro, apenas se consegue verificar as ações maliciosas, mas não identifica o responsável por essas ações.

3.2 ATAQUES MAIS COMUNS

O Domain Name Service (DNS), originalmente, possuía algumas vulnerabilidades, entretanto, não havia muitas preocupações em garantir os requisitos de segurança citados anteriormente.

Além disso, algumas das maiores preocupações em sistemas DNS são deixar que seu método de consultas permaneça ágil e fazer com que o servidores de nomes aguentem atender um grande número de usuários sem que fiquem sobrecarregados. Ao se implementar algum tipo de segurança a sistemas DNS, o desempenho dessas preocupações cai devido ao custo computacional exigido pelos mecanismos de segurança. Logo, é importante balancear a agilidade dos servidores DNS com seus aspectos de segurança.

Nesta seção, mostraremos o funcionamento dos ataques mais conhecidos e importantes a sistemas DNS. Como medidas de segurança básicas a servidores DNS, devemos citar a importância de manter o BIND (Berkeley Internet Name Domain) sempre atualizado, além do uso do protocolo DNSSEC que entraremos em detalhes no próximo capítulo.

3.2.1 Ataque Man-in-the-Middle (MITM)

Como servidores DNS não possuíam mecanismos de autenticação, estes são vulneráveis ao ataque MITM, ou "homem do meio", que consiste em interceptar dados durante uma transmissão entre duas ou mais máquinas e o atacante repassa as mensagens interceptadas da forma que quiser, ou seja, modificando-as, rejeitando-as ou retransmitindo-as.

Neste tipo de ataque, o usuário se infiltra no meio da comunicação dos usuário, o que compromete os princípios de autorização e autenticação. Além disso, o usuário malicioso pode conseguir informações restritas, o que confronta o princípio da confidencialidade. Neste tipo de ataque, novas vulnerabilidades podem ser descobertas, além de trocas de senhas e protocolos de autenticações ficarem expostos.

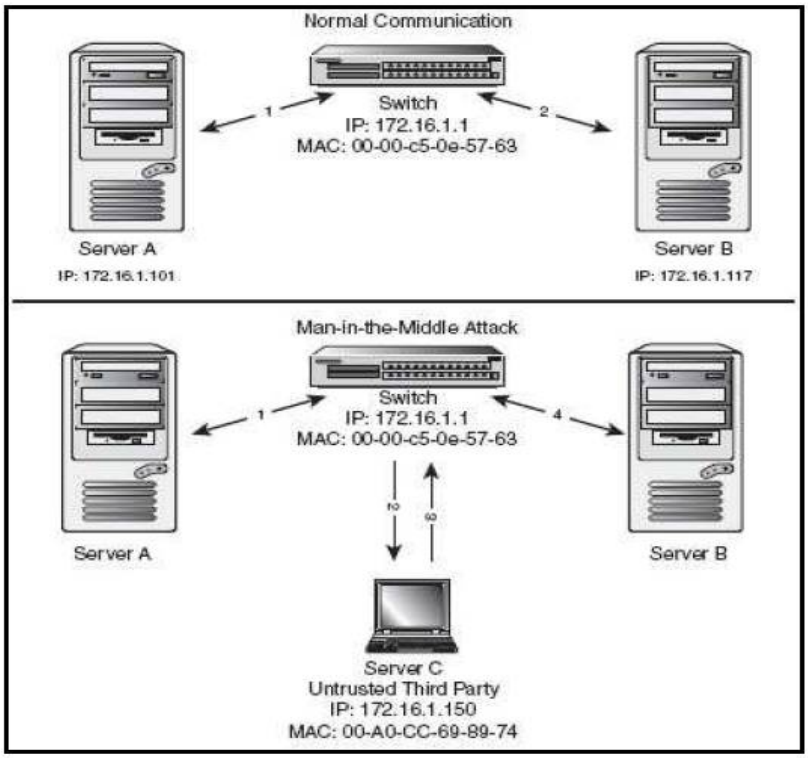

Figura 13 - Ataque Man-in-the-Middle (Hackpittsburgh, 2011)

A figura 13 evidencia o funcionamento de um ataque MITM. Neste exemplo, o servidor A quer se comunicar com o servidor B. O servidor C, que representa o atacante, captura as informações transmitidas por A e, automaticamente, são modificadas e retransmitidas em tempo real ao servidor B. Podemos notar que além do "envenamento" dos dados recebidos por B, o ataque ocorreu de forma que não possa ser detectada por A e B.

Neste tipo de ataque, o usuário malicioso consegue obter informações sobre a infraestrutura e funcionamento da rede, além do poder de forjar respostas maliciosas a usuários bem intencionados. Além disso, caso o atacante conseguir se situar entre um servidor DNS primário e outro secundário, ele poderá obter informações detalhadas sobre todas as zonas delegadas por estes servidores DNS.

3.2.2 Denial of Service (DoS)

Um ataque de negação de serviços tem como principal intenção fazer um servidor ficar indisponível. Este ataque consiste em sobrecarregar um servidor com inúmeras requisições de forma que não consiga responder mensagens de usuários legítimos e, por causa disso, o servidor fica inacessível e inoperante.

Outro possível objetivo de um ataque DoS é fazer que um servidor legítimo fique indisponível e, assim, substituir este servidor por um falso, fazendo com que este servidor ilegítimo responda e armazene mensagens enviadas a ele por usuários.

Mais de um host pode realizar um ataque de negação de serviço. Entretanto, quando o número de máquinas atacantes é muito alto e o ataque ocorre de forma coordenada, este tipo de ataque é chamado de negação de serviços distribuído, ou *distribuited denial of service (DDoS)*. Este tipo de ataque, geralmente, é composto por computadores infectados por *malwares* em diversas partes do globo terrestres (*botnet).* A figura 14 esquematiza um ataque DDoS.

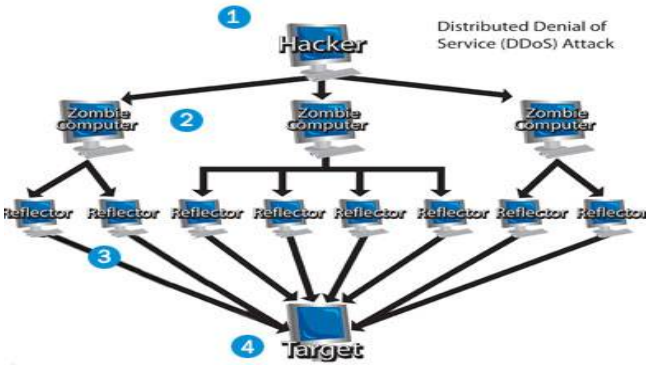

Figura 14 - Ataque DDoS (Mestre dos Sites, 2012)

3.2.3 Cache Poisoning

Conhecido por envenamento de cache, em países de língua portuguesa, este ataque consiste na modificação de *resource records(RR)*, de forma que, um endereço malicioso é associado a um nome DNS. Este ataque pode ser realizado apenas a consultas que utilizam servidores recursivos, ou seja, este afeta diretamente o servidor e não o usuário.

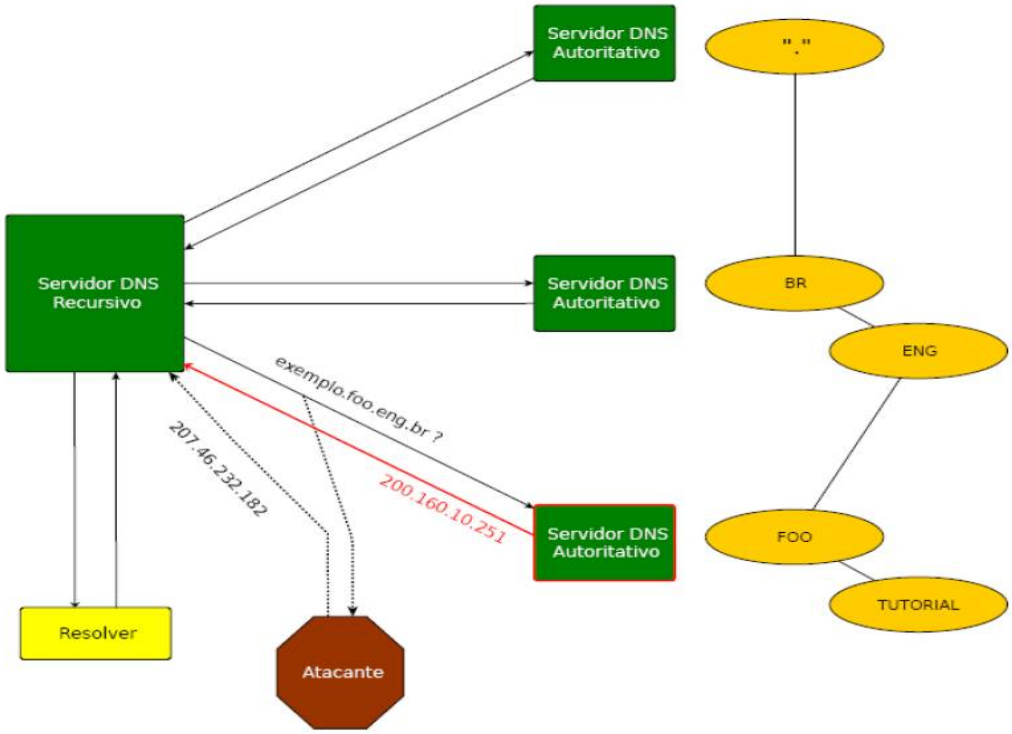

Figura 15 - Envenenamento de cache (CAMPOS, JUSTO, 2009)

A figura 15 esquematiza o envenenamento de cache. Relembrando a operação de uma consulta DNS recursiva, o usuário solicita a resolução de um nome para um servidor

recursivo, se este servidor não possuir a resposta da consulta, ele fará a pesquisa com outros servidor e retornará a resposta ao usuário. O atacante intercepta uma resposta de um servidor autoritário ao servidor recursivo substituindo o resultado da consulta por uma resposta com o mesmo nome contendo um endereço IP malicioso. O servidor, então, armazena esta resposta em seu cache e todos os usuários que solicitarem a resolução daquele nome serão redirecionados a um site malicioso durante a duração do TTL relacionado a esta informação.

Ao realizar este tipo de ataque, o usuário malicioso costuma infectar o RR com um site muito similar ao original a fim de a fraude não seja percebida pela vítima. Geralmente neste tipo de ataque são modificados os registros CNAME (*Canonical Name*), NS *(Name Server*) ou DNAME (*Delegation Name*).

3.2.4 Spoofing de DNS

Semelhante ao *cache poisoning*, o *spoofing* de DNS consiste em interceptar o tráfego DNS e através disto, o atacante substitui o tráfego legítimo por pacotes DNS forjados por ele. Com isso, o servidor pode, por exemplo, desviar o tráfego da vítima para um servidor malicioso que pode conter um site falso de uma instituição, por exemplo bancos. A diferença entre o *spoofing* de DNS e o *cache poisoning* é que na primeira, o ataque é diretamente no usuário, enquanto no segundo, a fraude é direcionada ao servidor.

A interceptação de tráfego DNS é fácil de ser realizada, pois esta não é criptografa e nem possui qualquer tipo de assinatura. De acordo com o RFC 1035, o cabeçalho DNS consiste em 16 bits responsável por identificar consultas e respostas. Uma consulta e a resposta dessa mesma consulta possuem identificadores iguais. As figuras abaixo identificam melhor essa situação utilizando o Wireshark que é um *sniffer* popularmente conhecido.

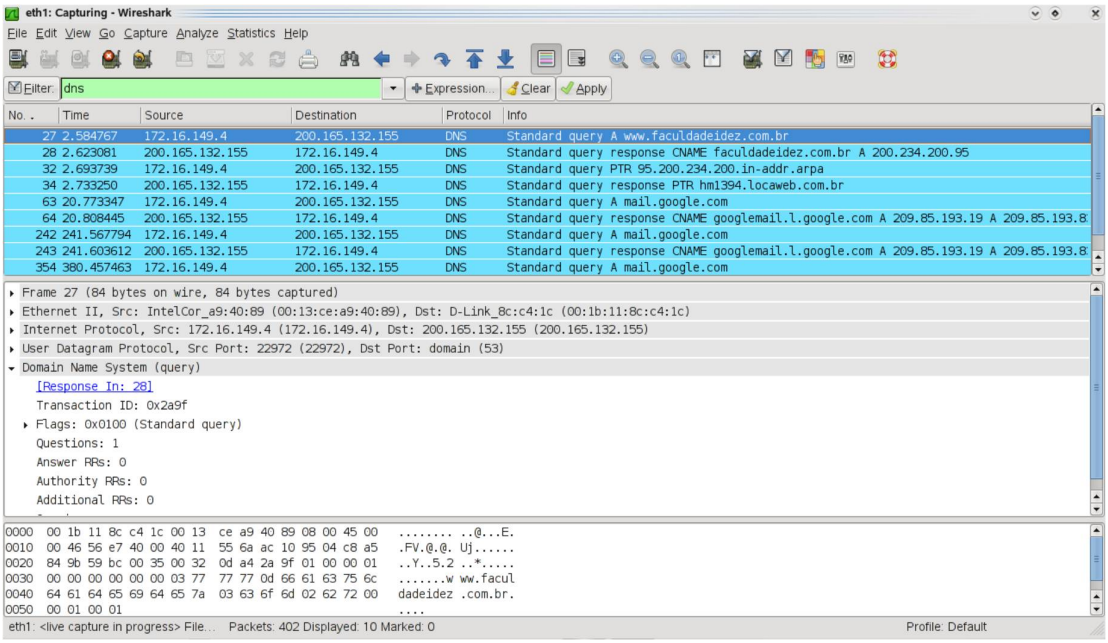

Figura 16 - Identificador de consulta (SILVA, SILVIO, 2009)

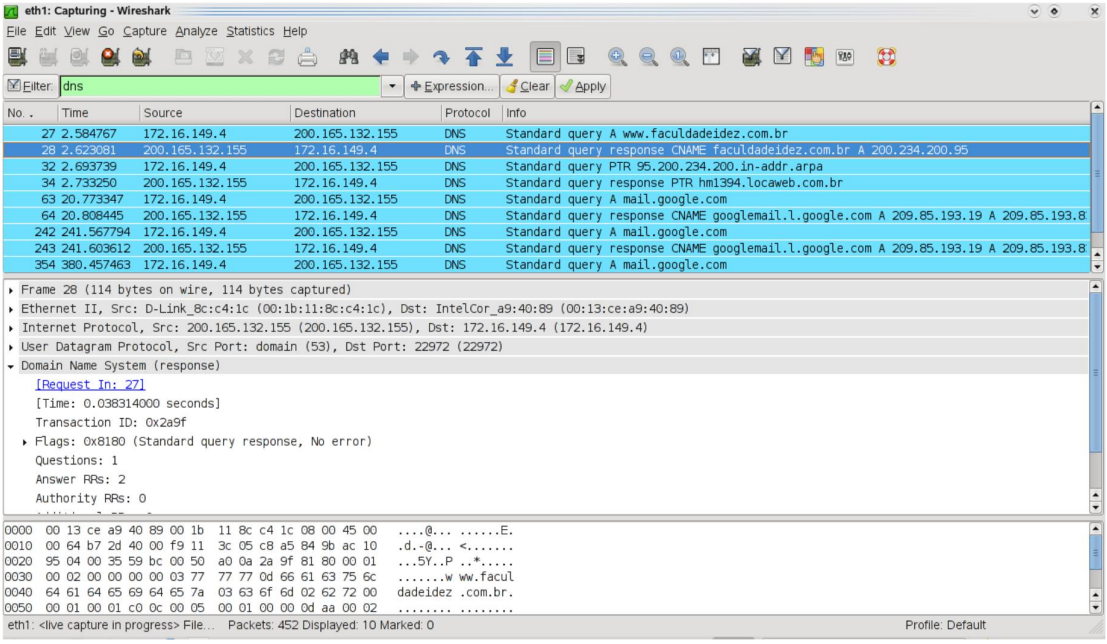

Figura 17 - Captura de tráfego (SILVA, SILVIO, 2009)

Nas duas consultas, verificamos que os identificadores são iguais e com o campo de identificação igual a 0x2a9f. O ataque consistem em forjar o campo ID da próxima consulta, ou seja, basta incrementar um ao valor capturado. Isto permite o atacante a falsificar e preparar o pacote para a próxima consulta.

Atualmente, as versões mais recentes do BIND possuem mecanismos que randomizam este campo para diferentes consultas DNS. Com estas funcionalidades, os riscos para este tipo de ataque são diminuídos consideravelmente.

3.2.5 ARP Spoofing

O ARP (*Adress Resolution Protocol*) é um dos principais protocolos da comunicação atual. Seu papel é a troca de informação do endereço MAC dos hosts da rede e realizar a tradução do endereço IP para endereço MAC. A operação inversa, resolução de endereço MAC para IP, é realizada pelo protocolo RARP. Para o funcionamento do ARP e RARP, são utilizadas quatro mensagens: o ARP *request*, ARP *reply*, RARP *request* e RARP *reply*.

O ARP *request* é a solicitação do endereço MAC que usa um determinado endereço IP. No ARP *reply*, algum computador retorna o endereço MAC correspondente ao endereço IP solicitado. O RARP *request* e *reply* são análogos ao ARP *request* e *reply* respectivamente. Por motivo de eficiência, sistemas operacionais armazenam endereços IPs e seus correspondentes endereços MAC em seu cache, na chamada tabela ARP.

Em ataques de ARP *spoofing*, o envio de blocos de consulta e/ou respostas falsas acabam interceptando todo o tráfego de rede ou, ainda, estes ataques podem "personificar" outras máquinas e modificar o fluxo de dados da rede. (MAURÍCIO, 2013). Este tipo de ataque é feito através do envenenamento do cache da tabela ARP.

As máquinas aceitam qualquer mensagem do tipo ARP *reply*, a fim de atualizar sua tabela ARP. Com isso, ao enviar um ARP *reply* falso, computadores atualizam suas tabelas ARP podendo redirecionar todo fluxo da rede. Ou seja, pode-se fazer com que um roteador, switch ou aplicação transmitam mensagens ao atacante ao invés de enviá-las ao destino original. O atacante pode, por exemplo, rejeitar as mensagens transmitidas a ele, provocando um ataque um DoS a partir de um ataque ARP *spoofing*. Além disso, o atacante pode analisar os pacotes transmitidos, modifica-los e reenviá-los ao destino original, afim de quebrar a criptografia deste pacote, resultando num ataque *man-in-the-middle*.

O ARP *spoofing* pode ser executado de duas formas:

- ✓ Unidirecional: envia-se um ARP *reply* falso a uma das vítima, os dados interceptados serão somente do usuário contaminado.
- ✓ Bidirecional: o ataque é realizado em todas as vítimas. Dessa forma, o atacante consegue redirecionar todo o fluxo de dados entre as vítimas.

As figuras 18, 19 e 20 exemplificarão um ARP *spoofing* em uma rede local.

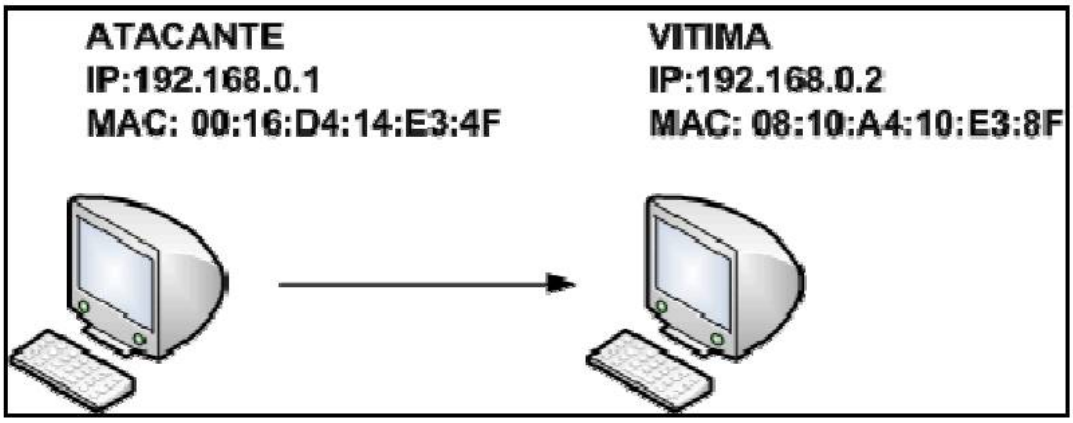

Figura 18 - *Echo request* falso (SILVA, MAURÍCIO, 2013)

Na figura 18, o atacante envia um *echo request*, a fim de atualizar a tabela ARP, utilizando um endereço IP qualquer, no caso, 192.168.10.

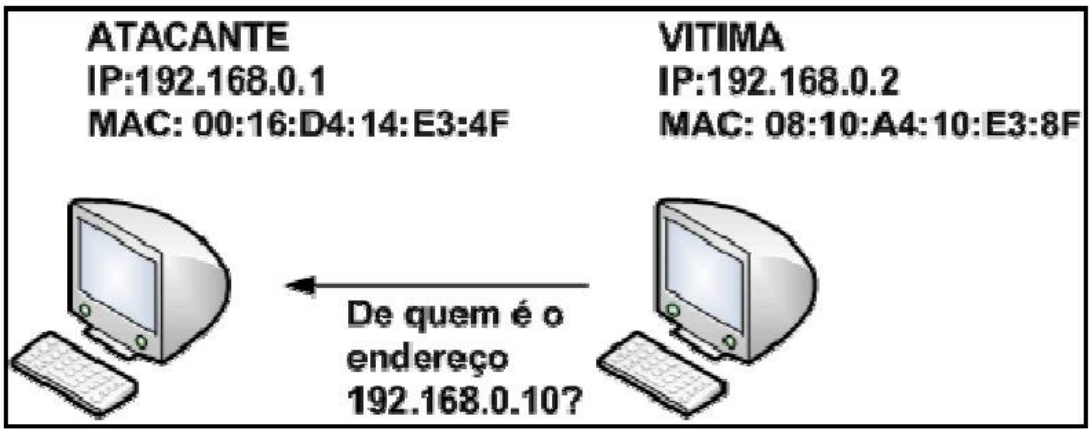

Figura 19 - ARP *request* forjado (SILVA, MAURÍCIO, 2013)

Na figura 19, a vítima envia um ARP *request* para obter o endereço MAC correspondente ao IP 192.168.0.10.

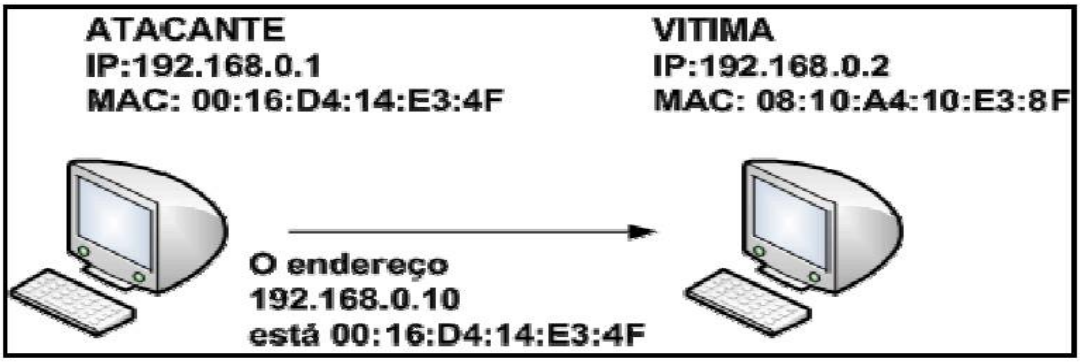

Figura 20 - ARP *reply* (SILVA, MAURÍCIO, 2013)

O atacante responde à vítima com um ARP *reply* constando que o endereço MAC do atacante corresponde ao endereço físico do endereço IP de 192.168.0.10. Após isso, o usuário malicioso passa a ser o gateway da vítima, assim, recebendo todos os dados recebidos e enviados por ela.

Este ataque pode ser utilizado para um servidor DNS malicioso substituir um servidor legítimo. O atacante pode obter diversas informações sobre a zona de autoridade daquele servidor, negar o serviço DNS de uma empresa, ou simplesmente responder consultas com IPs maliciosos.

3.2.6 DNS Amplification

Bastante comentado em 2009 após um site pornô eliminar seu rival da concorrência utilizando este ataque, a amplificação de DNS é um ataque que consiste no fato que pequenas consultas DNS podem gerar grandes pacotes UDP na resposta. Este ataque é realizado em um servidor recursivo.

O atacante realiza uma consulta DNS substituindo (*spoofing*) o endereço IP original pelo endereço da vítima, assim a resposta é redirecionada.

Originalmente nas especificações iniciais do DNS, os pacotes UDP tinham o tamanho limitado em 512 bytes, logo um consulta que costuma ter aproximadamente 60 bytes de tamanho, gera uma reposta que é 8,5 vezes maior. Com a adoção de novas extensões a sistemas DNS, uma simples consulta pode gerar uma resposta de 4000 bytes, que é equivalente a 60 vezes o tamanho de uma consulta.

Como consequência, este tipo de ataque pode ser interpretado como um ataque de negação de serviços, devido à sobrecarga causada as vítimas pelo usuário malicioso.

3.2.7 Transferência de Zonas e Atualizações Dinâmicas

Como vimos anteriormente neste trabalho, ao sofrer qualquer alteração ou atualização em seus arquivos de configuração de zona, ocorre a transferência de zona. Nesta, os servidores mestre replicam e transmitem as mudanças ocorridas aos servidores autoritativos escravos.

Como o tráfego dessa transferência, assim como todo o tráfego DNS, não é criptografado, informações importantes daquela zona são expostas e qualquer usuário mal intencionado pode interceptar e analisar esses dados, principalmente os *resource records*.

O *Dynamic Host Configuration Protocol* (DHCP) é o protocol responsável por distribuir endereços IPs automaticamente em uma rede. Quando um host perde ou recebe um endereço IP, o DHCP atualiza automaticamente o servidor DNS, adicionando ou removendo RRs nos arquivos de zona. Este processo é chamado de atualizações dinâmicas.

Com o uso do DHCP, o atacante pode usar atualizações dinâmicas para realizar um ataque DoS, remover intencionalmente um RR, além e realizar IP spoofing.

3.3 SOLUÇÕES DE SEGURANÇA EM SISTEMAS DNS

Nesta seção abordaremos alternativas para corrigir falhas de segurança do DNS, além do DNSSEC que será aprofundado no próximo capítulo.

3.3.1 Open DNS

Usado em servidores DNS recursivos, o Open DNS é uma solução gratuita que oferece muitas vantagens como controle de acesso para pais (*parental control*), filtragem de conteúdo, alta disponibilidade, alta velocidade, dentre outras. Usuários que desejam utilizar os serviços do Open DNS precisam apenas mudar as configurações de seu computador para usar um servidor DNS recursivo fornecido pelo Open DNS: 208.67.222.222 ou 208.67.220.220.

O Open DNS conta com uma comunidade chamada de "*The PhishTank Community*" que consta com mais de cinquenta mil especialistas em *phishing* espalhados pelo mundo. Esta característica é umas das principais vantagens desse sistema, pois esta comunidade trabalha para manter o uso seguro do Open DNS através do bloqueio e localização de sites fraudulentos que utilizam o ataque conhecido por *phishing*.

O *phishing* é um ataque que utiliza técnicas de engenharia social para furtar dados pessoais de usuários assim como credenciais de diversas contas de outros sites.

3.3.2 Transaction Signatures –TSIG

A assinatura de transação (TSIG) provê mecanismos de verificação da identidade de servidores DNS o qual quer se comunicar.

O TSIG tem como principal função garantir a autenticidade de atualizações dinâmicas do DNS (*dynamic updates*) e de transferências de zonas. O TSIG garante confiabilidade através de um sistema de chaves secretas compartilhadas entre a entidades comunicantes.

Entretanto, o uso do mecanismos de chave pública e privada para sistemas DNS (RFC 2535) se torna impraticável devido a sua complexidade e custo computacional. O TSIG possui funcionalidades parecidas com o DNSSEC.

4 DOMAIN NAME SYSTEM SECURITY EXTENSIONS (DNSSEC)

Ao receber uma resposta de uma consulta DNS, o cliente não consegue saber se o endereço IP resultante da consulta é integro e autêntico. Os resultados deste processo podem ter sido interceptados e substituídos, alterados ou podem ser realizados em um servidor que contenha uma memória cache contaminada.

A RFC 3833 (Threat Analysis of the Domain Name System (DNS), IETF) estuda as ameaças sujeitas ao sistema DNS e descreve as principais funcionalidades para se manter as integridade dos dados, além da autenticação da origem dos dados.

O DNSSEC é uma extensão de segurança do sistema DNS que tem como principal função garantir integridade e autenticidade durante as consultas realizadas, eliminando vulnerabilidades envolvidas na operação de consultas. Esta extensão se originou de um trabalho da Força Tarefa de Engenharia da Internet (IETF). Este mecanismo se apresenta como melhor solução para os problemas de segurança relacionados ao DNS. Quanto mais servidores DNS adotam esta solução, mais seguro se torna este tipo de serviço.

O DNSSEC resolve a maioria dos problemas relacionados à segurança do DNS. Neste protocolo são adotadas técnicas de criptografia assimétrica, onde os servidores que implantam o DNSSEC além de trocar o resultado das consultas, trocam também as chaves públicas de cada um. O programa que faz a verificação das assinatura digital é chamado de *validator* ou validador. O validador pode ser adotado em diferentes locais da estrutura DNS. Sua implementação em um servidor recursivo, por exemplo, garante que este não seja alvo de um ataque de envenenamento de cache. Além disso, o DNSSEC implementa novos campos nos *resource records* que evidenciaremos e explicaremos mais a diante.

Como mencionamos anteriormente, o DNSSEC implementa criptografia e assinatura digital através de chaves privadas e públicas a fim de prover integridade e autenticação, mas não garante confidencialidade pois os dados não são criptografados no DNSSEC.

Em geral, técnicas de criptografia são utilizadas para garantir confidencialidade, ou seja, proteger uma informação para que não consiga ser interpretada por usuários que não estejam envolvidos na comunicação. Para um usuário conseguir entender a mensagem enviada, é necessário que ele conheça a chave para, então, descriptografar a mensagem. No caso da criptografia assimétrica, são usadas duas chaves, uma para a codificação, chave

pública, e outra para a decodificação, a chave privada. A chave pública é divulgada livremente, mas a chave privada deve se manter em segredo, ou seja, apena o dono conhece seu valor. Suponha que um cliente A queria se comunicar com outro cliente B. A solicita a chave pública de B e cifra o pacote com ela. Após isso, A envia o pacote cifrado a B que decifra a mensagem com a chave privada de B.

Explicaremos mais adiante como o DNSSEC usa a criptográfica de chave pública para garantir autenticidade e integridade.

4.1 CARACTERÍSTICAS DO DNSSEC

No projeto do DNSSEC, também foi necessário um cuidado em seu desenvolvimento para que não alterasse a estrutura original do DNS. Com isso, o DNSSEC também implementa a maioria das interações entre zona pais e filhos, mas desta vez garantido autenticação e verificação de integridade das informações trocadas. Os mecanismos que adotam esses princípios do DNSSEC são as zonas de assinatura (*signed zones*) e o gerenciamento de ancoras de confiança (*trust anchor*). A figura 21 mostra as interações entre zonas pai e filho.

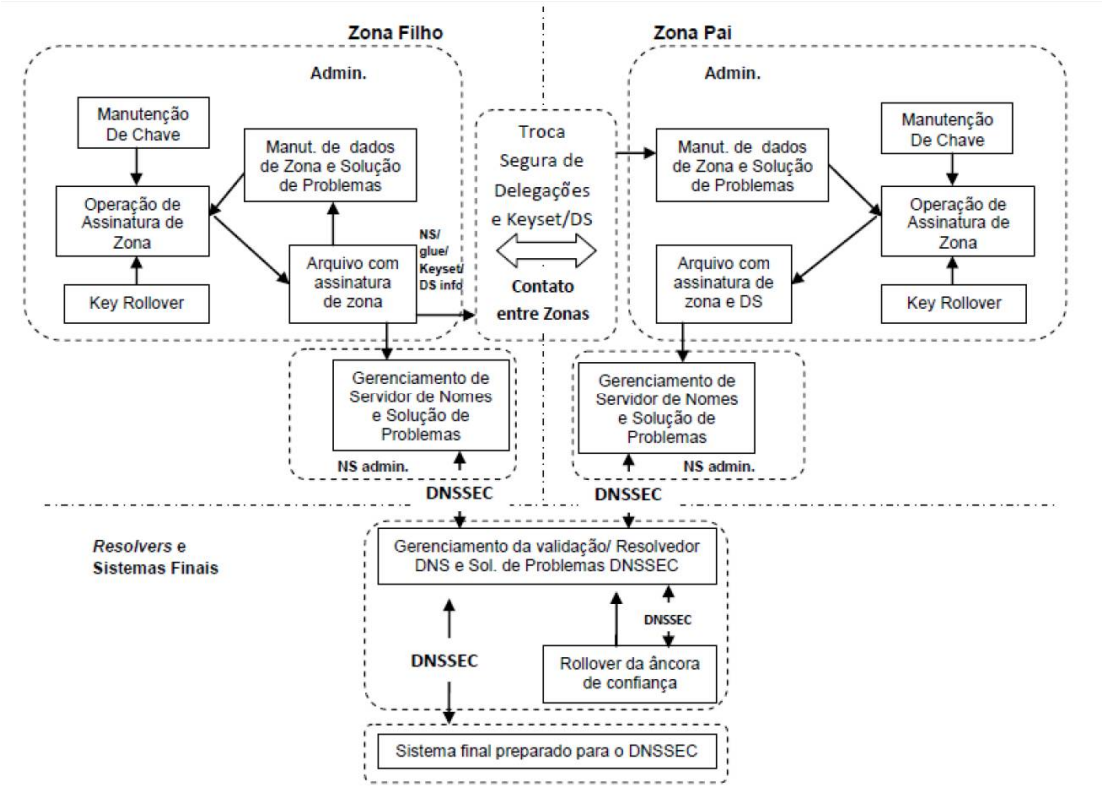

Figura 21 - Funcionamento e gerenciamento do DNSSEC (KRISHNASWAMY, 2009)

O trabalho do administrador de zona continua o mesmo do DNS normal, mas agora ele é responsável também por gerenciar novos registros além da verificação de autenticidade e integridade. Na sinalização de zonas são utilizados algoritmos de criptografia, onde chaves são criadas para cada zona DNS. Assim, com os novos procedimentos adotados, como gerenciamento, criação e validação de novos registros, além de manter algumas características do DNS, o DNSSEC pode ser considerado uma extensão segura do DNS.

No DNS simples, a manutenção de zonas consistia apenas na troca de RRs, além da atualização do número serial de zona quando necessário, entretanto no DNSSEC isso não é o suficiente. Trocar a assinatura digital entre os servidores na transferência é um fator muito importante já que esta assinatura é válida por um tempo limitado.

4.1.1 Key Rollover

A proteção das chaves do DNSSEC podem ser feitas de duas formas: online e offline. A chave off-line é mais segura que a online pois esta é gerenciada e armazenada por apenas um servidor. No caso da chave online, são utilizados dois ou mais servidores, o que aumenta a exposição da chave e riscos de falha em segurança. Entretanto esta técnica, apesar de não ser recomendada, é necessária para realização de algumas operações, como atualizações automáticas. O termo utilizado para a atualização da chave é chamada de *key rollover*.

Quanto maior a duração de uma chave em um sistema de segurança, mais tempo um atacante terá para decifra-la, aumentando a vulnerabilidade do sistema. Entretanto, ao se atualizar a chave, elementos no cache ainda estarão que utilizam a chave antiga. Este problema acarretará na eliminação da informação e na realização de novas requisições que seriam desnecessárias caso a chave antiga ainda fosse válida, diminuindo a eficiência de todo o sistema. Além disso, um resolver com a chave antiga pode descartar a resposta correta de uma consulta por não ter recebido as atualizações ainda.

Por esses motivos, o DNSSEC utiliza o KSK (*Keys Signing Keys*) e o ZSK (*Zones Signing Keys*). O KSK é responsável pela delegação segura entre zonas pai e a zona filha, enquanto o ZSK faz o mesmo processo para assinatura de chaves de zonas. Tanto as chaves do ZSK quanto as do KSK precisam ser trocados periodicamente, principalmente se a chave for corrompida. Quando chaves são trocadas, deve haver um aviso entre a zona pai e a zona filha sobre a troca. A interação das zonas durante um *key rollover* deve ser de forma ordenada e ocorrer em uma duração limitada. A zona pai garante que a que as informações de sua delegação sejam incluídas assim como as informações de suas zonas filhas. O *key rollover*

em um servidor raiz é mais complicado de ser realizado pois qualquer alteração nestes servidores, encadeiam alterações em toda estrutura do DNS.

Servidores recursivos que implementam o DNSSEC podem validar os resultados das consultas e são chamados de servidores recursivos validadores. Quando a validação ocorre no próprio cliente do sistema DNS, este cliente deve conter políticas de validação apropriadas, além de uma lista de chaves âncora de confiança, que devem ser atualizadas sem que as chaves listadas forem alteradas.

As responsabilidades do administrador em um sistema DNS que implementa o DNSSEC aumentam. Além das funções exercidas em um sistema DNS simples, o administrador é responsável pelo funcionamento do sistema de validação de acordo com as âncoras usadas e as políticas de validação, ou seja, ele é encarregado do monitoramento de erros e atualização de dados.

4.1.2 Digest Access Authetication (DAA)

A *Digest Access Authetication* (DAA) é um mecanismo que funciona com uma pergunta que o um servidor emite e o usuário responde. Seu funcionamento não consiste em um sistema de login e senha, mas sim em um algoritmo que usa uma função de hash para esta autenticação.

4.1.3 DNSSEC Resource Records

Como dissemos anteriormente, o DNSSEC implementa quatro novos RRs, cada um com uma função específica.

- *Resource Record Signature* (RRSIG): responsável pela assinatura digital *digest* usada para proteger o RRset. É criada usando-se o ZSK ou KSK que são obtidos durante a assinatura de zonas.
- *DNSKEY*: chave pública do DNS.
- *Delegation Signer*(DS): responsável pela delegação de zonas. Esta RR possui a autenticação do digest do DNSKEY
- *Next Secure*(NSec): indica o próximo nome válido no RRset.

O *Authentic Data*(AD) bit, ou bit de informação autêntica indica, que todos os dados da resposta foram autenticados ao receber uma requisição. O bit de *Checking Disabled*(CD) mostrar que os dados recebidos por um cliente não podem ser autenticados pelo resolver do

mesmo cliente que enviou a requisição. O DNSSEC faz uso de uma extensão EDNS0 que faz com que o tamanho do pacote de consulta UDP supere 512 bits e chaves de maior comprimento sejam usadas. Com o uso dessas técnicas, o DNSSEC é capaz de identificar um ataque *man-in-the-middle*, mas não é capaz de preveni-lo. Ao ser detectado o ataque, o servidor DNS descarta as informações recebidas pelo atacante.

4.1.4 Estados de segurança do DNS

A validação de mensagens DNS é construída pela verificação das assinaturas e das cadeias de confiança. Tendo isto em vista, o DNS verifica também se caso aconteceu algum tipo de problema na transferência, seja um ataque ou simplesmente um erro na transmissão, e avalia a mensagem e, a partir daí, toma realiza uma ação de acordo com o estado dos pacotes trocados. Os estados da informação são quatro

- Seguro: âncora de confiança (chave pública) da zona requisitadas está presente e é usada para validar com sucesso outras informações.
- Inseguro: a âncora está presente, mas os dados da resposta indicam que não há um link seguro na comunicação entre as zonas. Ou seja, a zona é assinada, mas o subdomínio delegado requisitado não é seguro ou assinado.
- Falso: a âncora está presente, mas o dados não foram validados com sucesso, ou seja, foram corrompidos.
- Indeterminado: a âncora não está presente no servidor do domínio solicitado.

O bit AD indica se o estado de segurança é seguro ou inseguro. Se o estado de segurança é falso ou indeterminado o pacote segue sem o bit AD. Se a informação possui a avaliação de estado como falsa, o pacote é retido mas não é transferida a outros servidores. O validador é responsável pela classificação de RRs nos estados citados a cima.

4.1.5 Cadeias de confiança

Para a checagem de uma chave de confiança é necessário que o *resolver* tenha a acesso a esta chave. Não é necessário que todas as zonas informem suas chaves ao resolver, pois isto causaria um sobrecarga na redes além de um RR muito grande que levaria muito tempo para ser analisado. Para a solução deste problema, são adotados o mecanismo de cadeia de confiança.

A cadeia de confiança funciona seguindo o *resource record* chamado *Delegation Signed*(DS), previamente explicado neste trabalho. Este ponteiro assegura uma chave segura de uma zona pai para uma zona filha. O DS nada mais é que o resultado da função *hash* da chave pública da zona filha assinada pela chave privada do pai. Através da verificação de assinatura neste ponteiro, um resolver valida o *hash* de uma chave pública de uma zona filha, assim garantindo sua validade.

Cada validador recebem inúmeras chaves em que uma pode ser escolhida para ser a chave pública, lembrando que esta chave pública tem duração limitada. Esta chave pública escolhida é chamada de âncora de confiança que é delegada para outras zonas seguras. Os validadores são responsáveis por determinar o número de delegações que compõe a cadeia de segurança. É necessário que a zona filha tenha sua assinatura válida, caso contrário, não será considerada segura e não existirá cadeia de confiança.

Ao se integrar a uma cadeia de confiança, um servidor DNS possuirá a chave privada do sistema e a cada resposta, que este servidor emitir, assinará com a chave privada e será decodificada pela chave pública correspondente, conforme a figura 22.

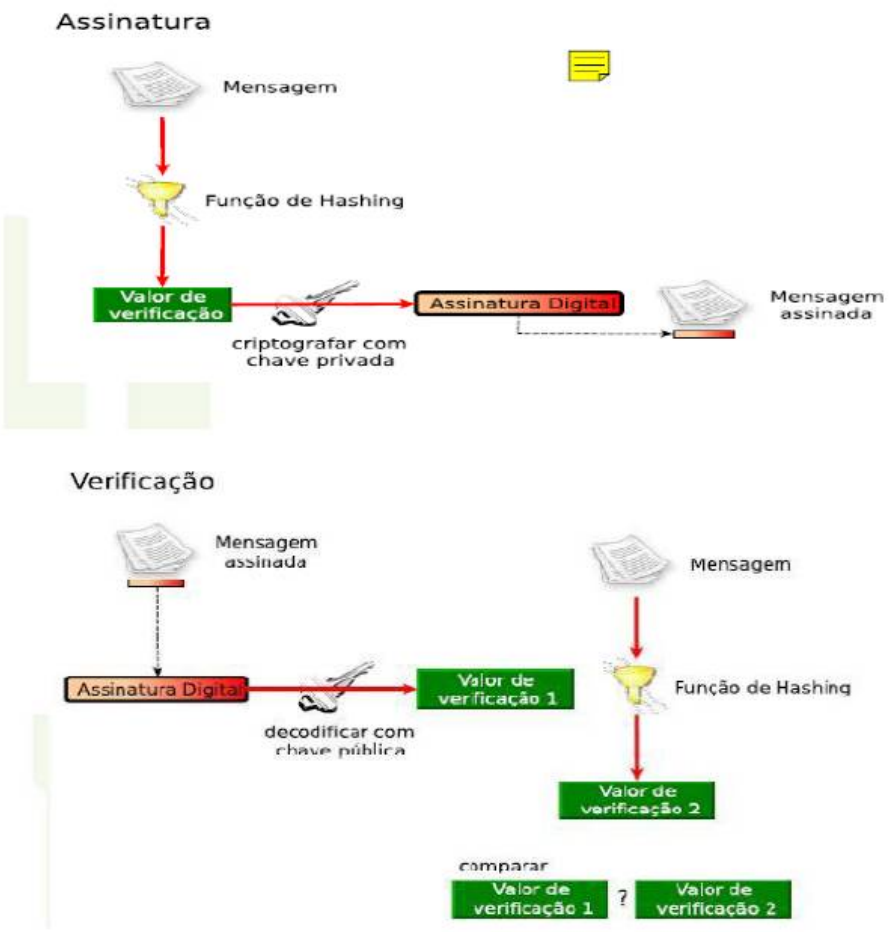

Figura 22 - Criptografia assimétrica ou de chave pública e privada (IWASA & HILÁRIO, 2011)

O destinatário decifra a mensagem trocada com a chave pública do remetente e fará uma comparação entre os dados decodificados e a informação recebida em claro. Se os campos forem idênticos, o servidor é confiável. É importante citar mais uma vez, o DNSSEC não provê confiabilidade, pois os dados são públicos e por isso não é necessário criptografar toda a mensagem. Este mecanismo citado previne um ataque de *spoofing*.

Com o uso de criptografia assimétrica, um servidor recursivo precisa obter a DNSKEY para a verificação de integridade da resposta. Existem duas formas de enviar a chave pública a eles:

-Informar a DNSKEY através de um RR de uma zona que não é recomendado pois caso a chave seja transmitida de forma segura, seria preciso uma validação anteriormente o

que é impossível. Se não for transmitida de forma segura, o sistema fica novamente vulnerável a *spoofing*.

- Transmitir a chave por algum sistema *ou-of-band*, como correio eletrônico, telefone dentre outros. Esta é a forma utilizada pelo DNSSEC. No BIND, âncoras de confiança são configuradas no arquivo named.conf.

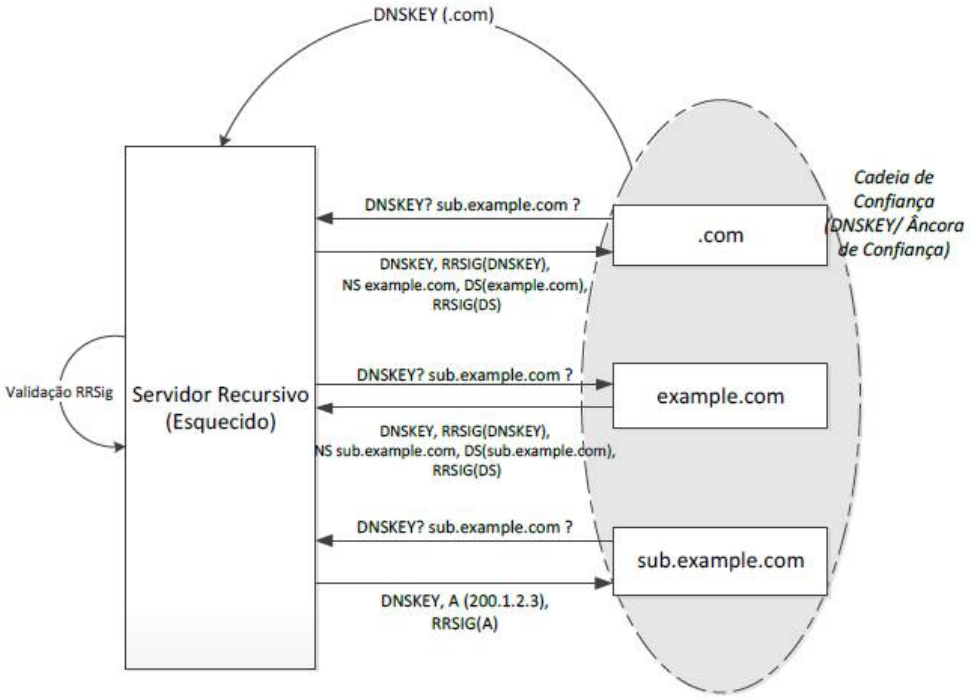

Figura 23 - Iterações DNSSEC (IWASA & HILÁRIO; 2011)

A figura 23 evidencia o funcionamento da emissão da chave pública para um servidor recursivo. Possuindo a DNSKEY de uma cadeia de confiança, o servidor recursivo faz uma solicitação para a resolução do nome **sub.exemple.com**. A requisição é direcionada ao servidor com autoridade sobre o domínio **.com**. Primeiramente, o servidor **.com** envia sua chave pública (DNSKEY) e sua assinatura (RRSIG) ao servidor recursivo. O servidor recursivo, que já possuía a DNSKEY, valida a RRSIG com a chave recebida e compara com a da RRSIG enviada. Se a decodificação for igual a sua própria DNSKEY, o servidor recursivo passa a confiar no servidor **.com**.

Após esse processo, o servidor recursivo envia ao servidor **.com** uma solicitação para descobrir o servidor que contém o endereço IP do nome **sub.exemple.com**. O servidor **.com** verifica a existência de de um ponteiro que contém **exemple.com** no RR *Delegation* Signed(DS) e responde com a assinatura e o endereço do NS do **exemple.com**, além de obter o *hash* de **exemple.com** e sua assinatura através do DS. As assinaturas usadas fora feitas

com a chave privada do servidor.com e pode ser verificada pelo servidor recursivo, utilizando a DNSKEY obtida. Este procedimento se repete até o servidor recursivo obter o endereço IP de **sub.exemple.com**.

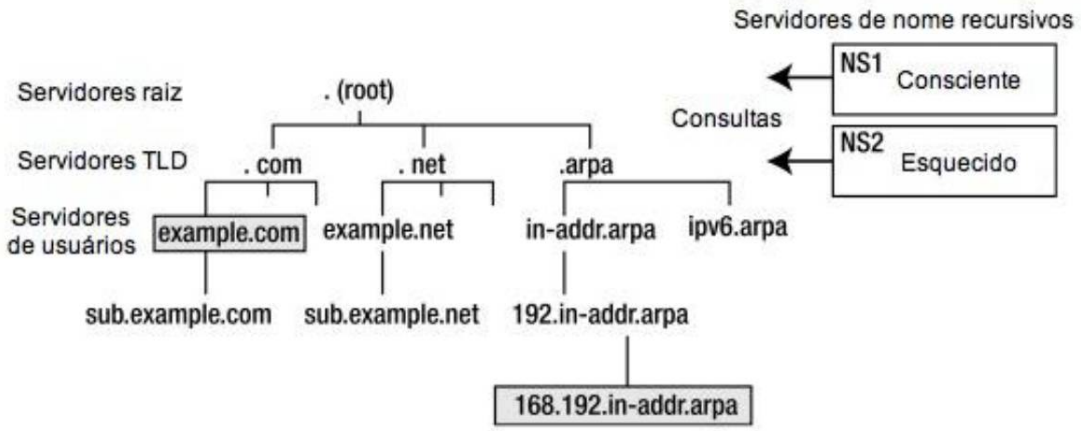

Figura 24 - Cadeias de confiança (FREIDMAN, 2010).

Através dos processos aqui explicados, um subdomínio pode se comunicar com sua zona pai criando uma delegação segura. O campo RR *Delegated Si*gned (DS) é utilizado neste caso.

Na figura 24, podemos a construção uma cadeia de confiança do domínio exemple.com entre sub.exemple.com, que é seu único subdomínio, e para que a cadeia seja efetivada, ambos precisam ser assinados. Um servidor recursivo valida suas requisições a partir de uma única âncora de confiança pelo rastreamento do RR DS na hierarquia mais alta do sistema.

O servidor NS1, que é consciente da segurança, realiza um requerimento para obter a chave pública de exemple.com, que a delegação de mais alta hierarquia na cadeia de confiança, e por consequência, a nova âncora cobre sub.exemple.com pois é a única zona filha de exemple.com. Caso algum domínio não seja assinado, ele continuará funcionando sem o DNSSEC, ou seja, funcionará de forma mais vulnerável.

4.1.6 Ferramentas DNSSEC

O DNSSEC faz uso de ferramentas que facilitam a administração do sistema. A figura 25 exemplifica o uso de algumas ferramentas bastante utilizadas.

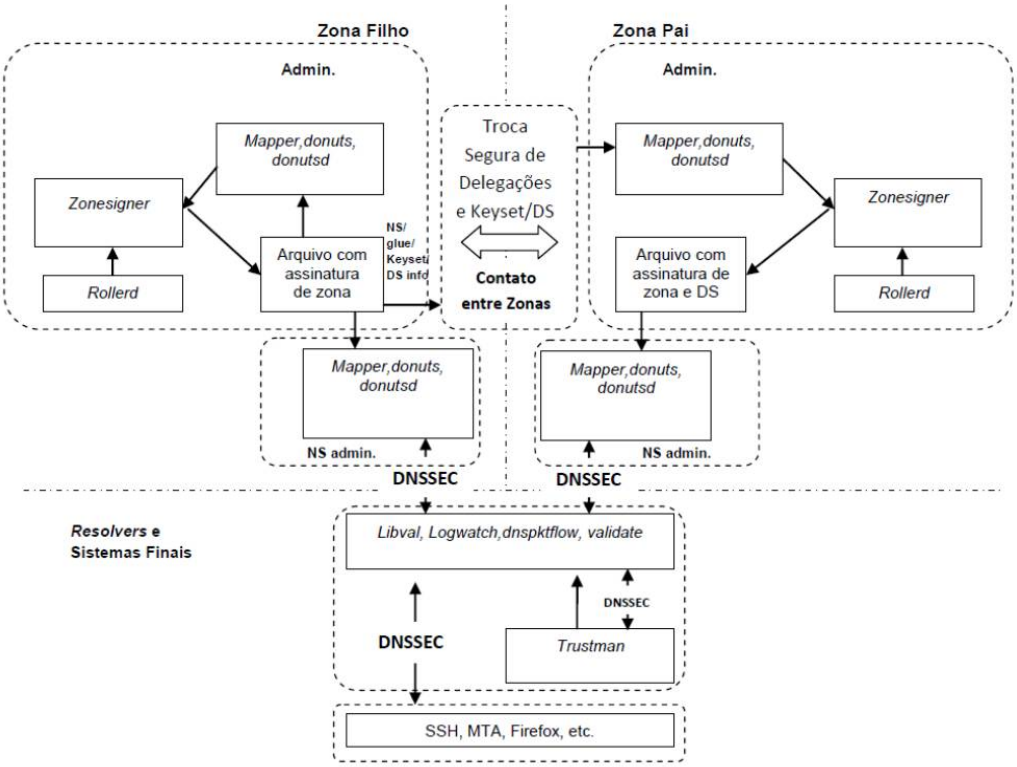

Figura 25 - Ferramentas DNSSEC (KRISHNASWAMY, 2009)

Abaixo serão especificadas algumas ferramentas e suas funcionalidades:

Zonesigner é uma ferramenta responsável pelo gerenciamento de chaves, arquivamento de registros e assinaturas de zonas. Este aplicativo é composto por arquivos chamados keyrec que especificam informações de assinaturas de zonas (*zone-specific records*) e geração de chaves (*key-specific records*).

Rollerd cuida dos procedimentos de *key rollover*. Ou seja, este aplicativo é responsável pela a validação de informações que usem uma chave antiga, logo após uma atualização de chaves.

Donuts e Donutsd são responsáveis para a verificação de integridade das mensagens trocadas no operador. Estes possuem arquivos que determinam regras que são baseadas nos princípios do DNSSEC e boas práticas.

Mapper é responsável por criar uma figura que corresponde a um mapa da zona relacionada à máquina que implementa esta funcionalidade. É também capaz de identificar onde ocorre alguma falha ou algo inesperado.

Trustman[1] é responsável pela verificação das âncoras de confiança das mensagens recebidas pelo cliente atualiza os dados se alguma mudança é detectada.

Logwatch é um grupo de scripts que fornecem uma forma de registro DNSSEC mais eficaz. Armazena os dados em logs facilita o entendimento das ocorrências em sua hierarquia.

Dnspktflow facilita a análise do fluxo de perguntas e repostas em uma zona, rastreando cada interação pelo histórico.

Valtidate é um programa que facilita na validação de pacotes e ajuda na análise de erros deste processo. Com este mecanismo, consegue se analisar detalhes da cadeia de confiança em sistemas DNSEC.

[1] Manual disponível na URL: https://www.dnssec-tools.org/wiki/index.php/Software_User_Manual e pode ser baixado em: http://sourceforge.net/projects/logwatch/. Links acessados em 26 de junho de 2015.

5 EXPERIMENTOS E ANÁLISE DE RESULTADOS

A fase experimental deste trabalho foi dividida em duas fases distintas para complementar o estudos dos diversos fatores que envolvem este assunto.

A primeira atividade consiste no estudo da eficiência do DNSSEC contra fraudes e envenenamento de cache, evidenciando, de maneira didática, o tipo de proteção que é fornecida com o uso deste mecanismo de segurança. Para isto, foram construídos dois ambientes virtualizados, um foi planejado com o DNS comum e outro com a utilização do DNSSEC para o servidor recursivo.

A segunda atividade proposta, está relacionada às estatísticas de uso do DNS e DNSSEC no Brasil e também inclui uma proposta de monitoramento de incidentes de envenenamento do cache.

5.1 FERRAMENTAS UTILIZADAS

Para os procedimentos experimentais, foram exploradas as ferramentas NMAP para efetuar a varredura de rede, DIG para verificação de recursividade e uso de DNSSEC, Virtual Box para criação dos cenários em máquinas virtuais. O sistema operacional usado em todas as máquinas virtuais do cenário foi o Ubuntu 12.04 LTS com o BIND9 como software para o serviço de DNS.

O NMAP é uma ferramenta clássica para varreduras de redes TCP/IP, com ela é possível especificar diversos parâmetros para otimizar e personalizar o "scanning" para obter o resultados esperado. Dentre estes parâmetros podemos determinar o protocolo da camada de transporte utilizado, portas de destino, listas de IPs, velocidade, tamanho do pacote, tempo limite de resposta etc.

O Dig é um cliente de DNS nativo de sistemas UNIX de derivação Debian, muito útil em depurações de resoluções de nomes, ele permite fazer uma consulta especificando cada campo ou tipo de entrada, como MX, AA, NS, com a opção de uso ou não de cache.

Os cenários dos experimentos foram criados utilizando o Virtual Box, que é um produto gratuito da Oracle que nos permite oferecer os recursos físicos de um computador, disco, memórias e interfaces de entrada e saída, para uma máquina virtual, assim precisamos apenas de um dispositivo físico para criar uma topologia virtual que integra diferentes sistemas operacionais.

5.2 ATIVIDADE I – CENÁRIO 1 – DNS VULNERÁVEL

Os dois cenários são compostos por três dispositivos clientes (Usuários), um servidor DNS operando no modo recursivo e um servidor DNS configurado para funcionar como autoritativo do domínio alvo, todos estes componentes com acesso total à internet. Com os dois cenários mostraremos que uma resposta DNS pode ser facilmente fraudada e que com recurso do DNSSEC podemos garantir a integridade e confiabilidade da consulta.

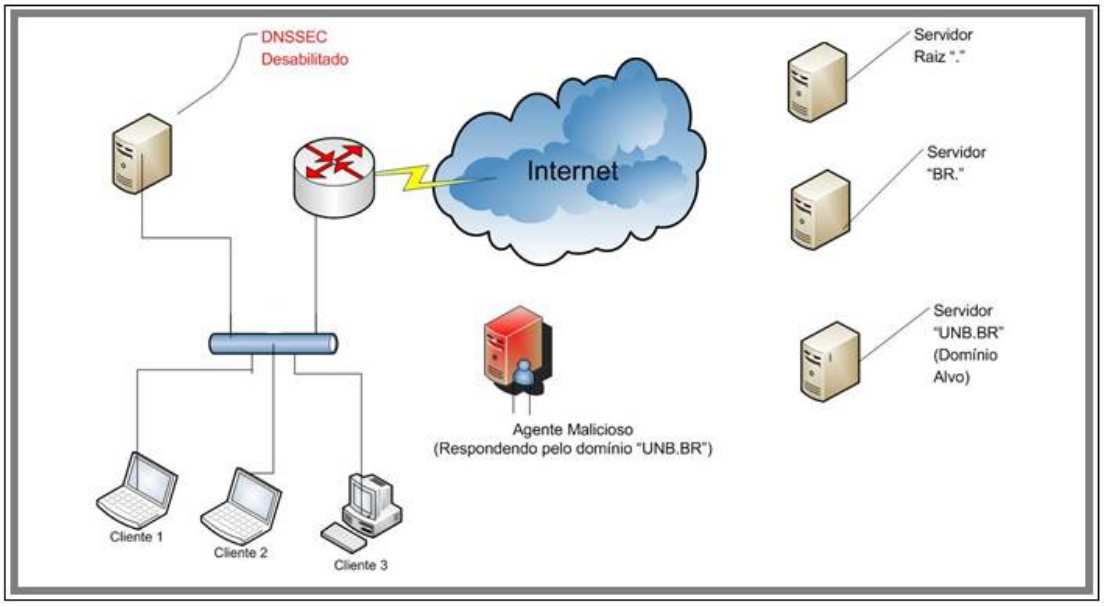

Figura 26 - Cenário 1-Atividade I

Usamos o domínio "UNB.BR" pelo fato do mesmo fazer uso do DNSSEC, mas este teste pode ser repetido para qualquer domínio com DNSSEC habilitado.

Nesta simulação um dos clientes faz um requisição do nome "www.unb.br" para o Servidor Recursivo, como já foi explicado anteriormente, o servidor do "BR." delega o domínio "UNB.BR." apontando as consultas do tipo "NS" para o(s) IP(s) do servidor(es) que contêm a zona deste domínio. O ataque vem logo depois desta etapa, no momento em que o Recursivo (sem DNESSEC) faz a consulta no IP que recebeu como resposta do .BR, o atacante intercepta a mensagem e dá uma falsa resposta, atribuindo o IP que lhe convém ao nome "www.unb.br". Feito isto o cache do Recursivo está contaminado com esta entrada falsa e consequentemente todos os clientes desta também terão esta resposta falsa.

Para melhor evidenciar o ataque foram feitas capturas de pacotes no modo PCAP, que podem ser visualizadas graficamente pelo software WIRESHARK e também capturas das telas dos clientes e evidencias pelo cliente NSLOOKUP:

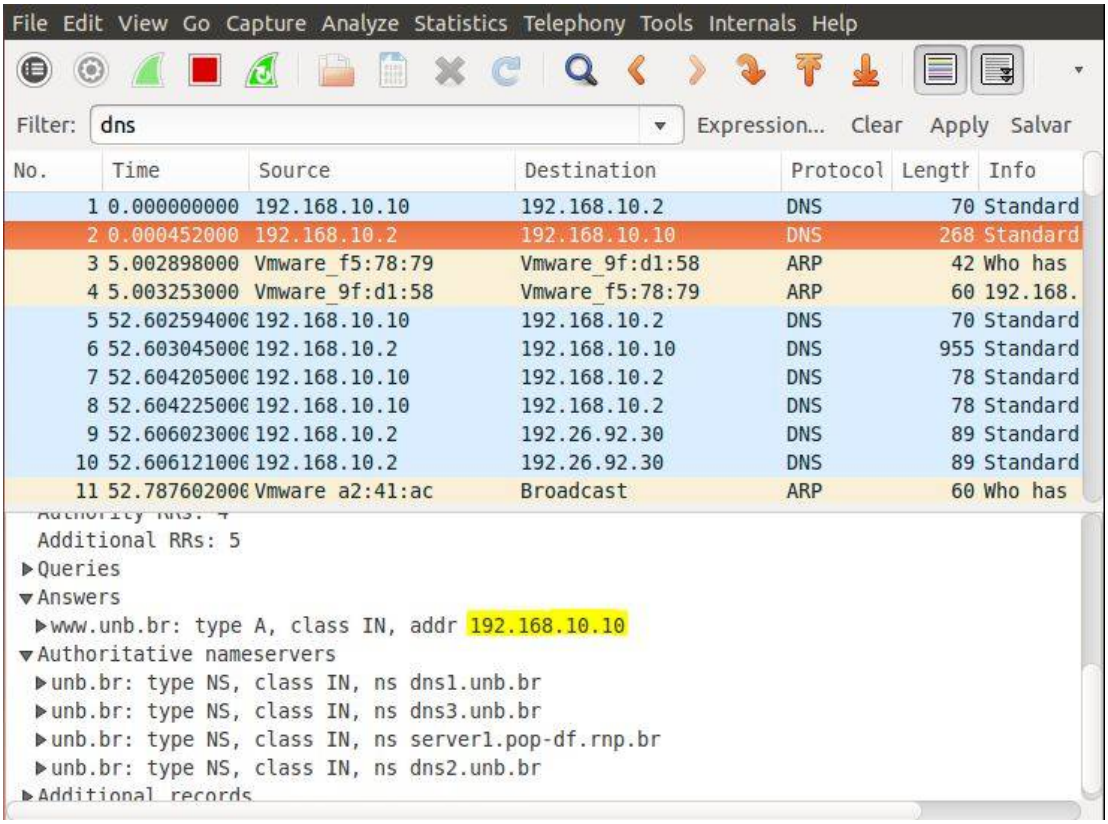

Figura 27 - Captura do Wireshark - Cenário I - Atividade I

Foi feita uma foto da saída do programa NSLOOKUP, para melhor visualizar a resposta do DNS Recursivo:

Figura 28 - Saída do NSLOOKUP - Cenário I - Atividade I

Na imagem a seguir, é possível ver em destaque o IP da resposta falsa enviada pelo dispositivo malicioso. Neste caso a fraude redireciona o cliente para o IP 192.168.10.10, mas este poderia ser qualquer outro de interesse do atacante. A seguir a figura mostra a página WEB que acessada quando o cliente acessa a URL www.unb.br:

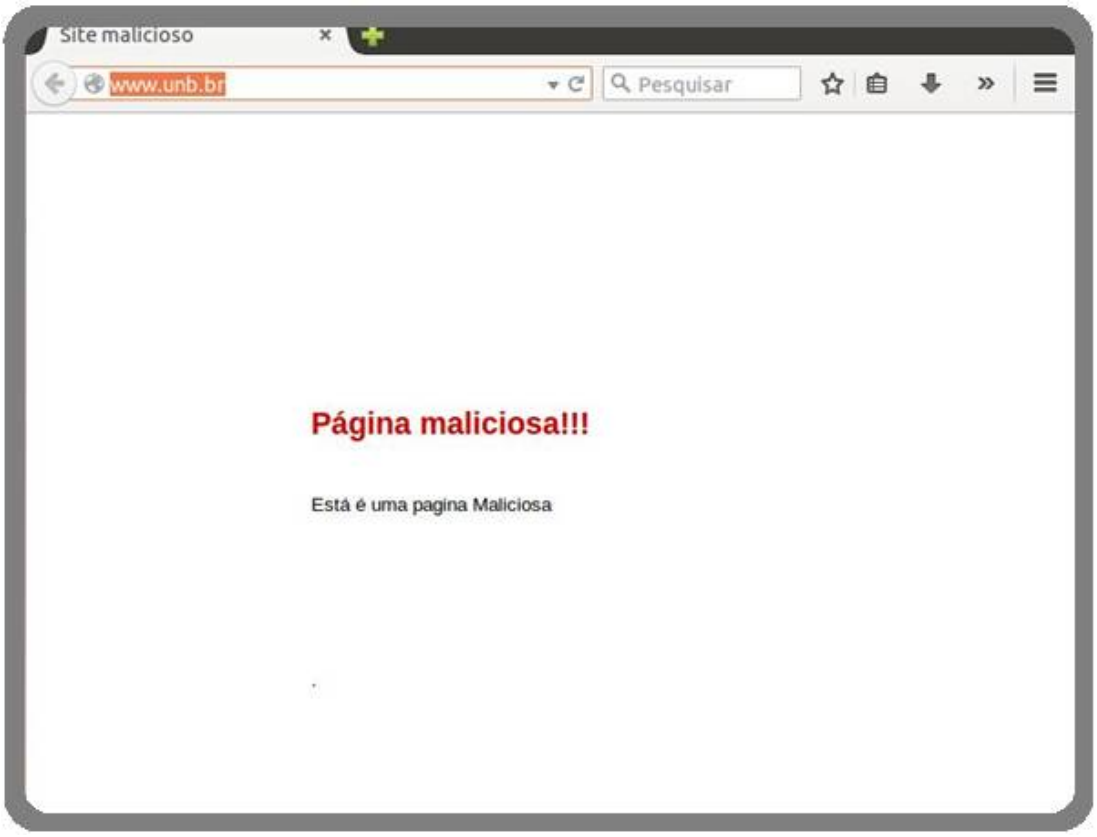

Figura 29 - Página Falsa - Cenário I - Atividade I

Esta página foi configurada em uma servidor WEB apache2, instalados em um UBUNTU 12.04 - LTS, apenas para fim de ilustração completa de uma ataque de envenenamento de cache DNS.

5.3 ATIVIDADE I – CENÁRIO 2 – DNSSEC

No próximo cenário(II), foi feita apenas uma alteração no Servidor Recursivo, no qual a validação de DNSSEC é habilitada.

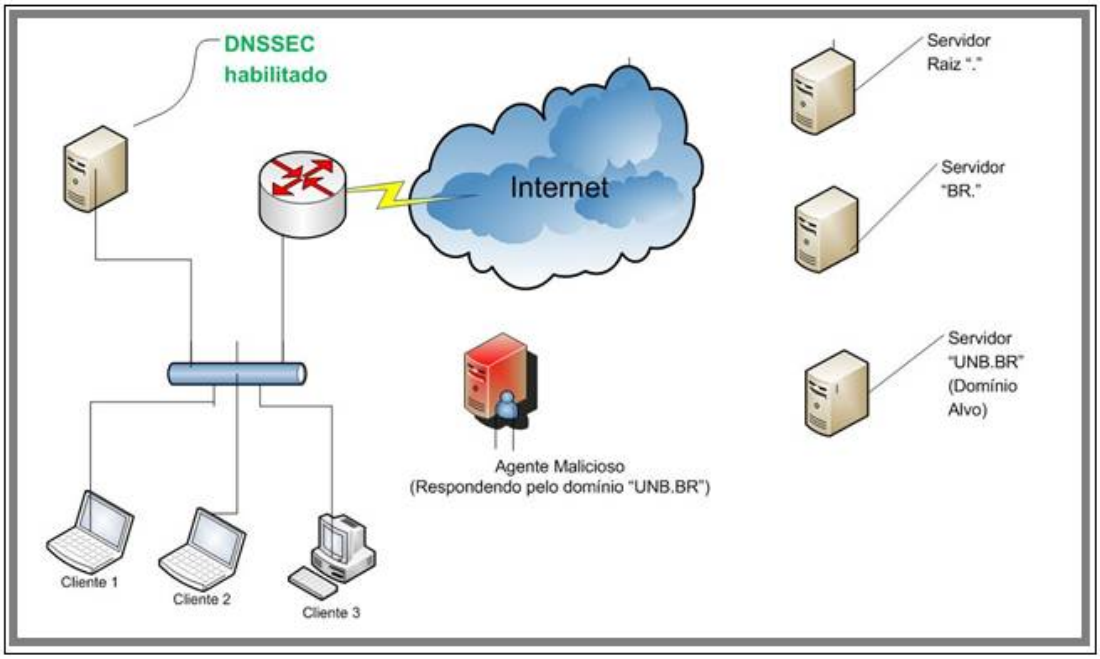

Figura 30 - Cenário II - Atividade I

Para habilitar o DNSSEC em um servidor Recursivo BIND9, deve-se editar o arquivo de configuração em "/etc/bind/named.conf" e retirar o comentário da linha "dnsse - validation auto" conforme a imagem abaixo:

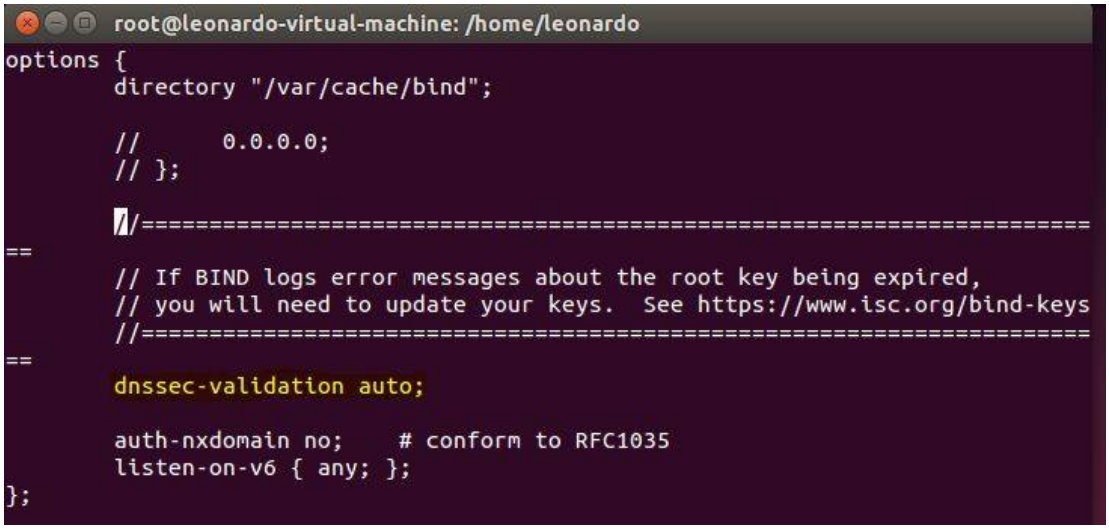

Figura 31- Cenário 2-Atividade I

No cenário, repete-se as mesmas consultas ao domínio "UNB.BR", efetuando o mesmo tipo de tentativa de fraude. O resultado é que durante o ataque não há nenhuma resposta fraudada, pois a integridade e a autenticidade foi garantida pelo DNSSEC.

Também foram capturados os pacotes no formato PCAP e telas dos clientes para validar o procedimento.

Na primeira tentativa de acesso à URL www.unb.br, obtivemos a resposta de que não foi possível resolver o nome em questão. No segunda acesso já obtivemos o endereço correto.

Este fato é explicado pelo fato de que a primeira resposta obtida não continha a chave fornecida pelo domínio pai, no caso o ".BR", assim a resposta foi descartada pelo servidor recursivo. O Bind9 registra os eventos de consultas DNS na pasta /var/log/syslog. Examinando este arquivo pudemos confirmar a recusa da resposta pela verificação de chaves:

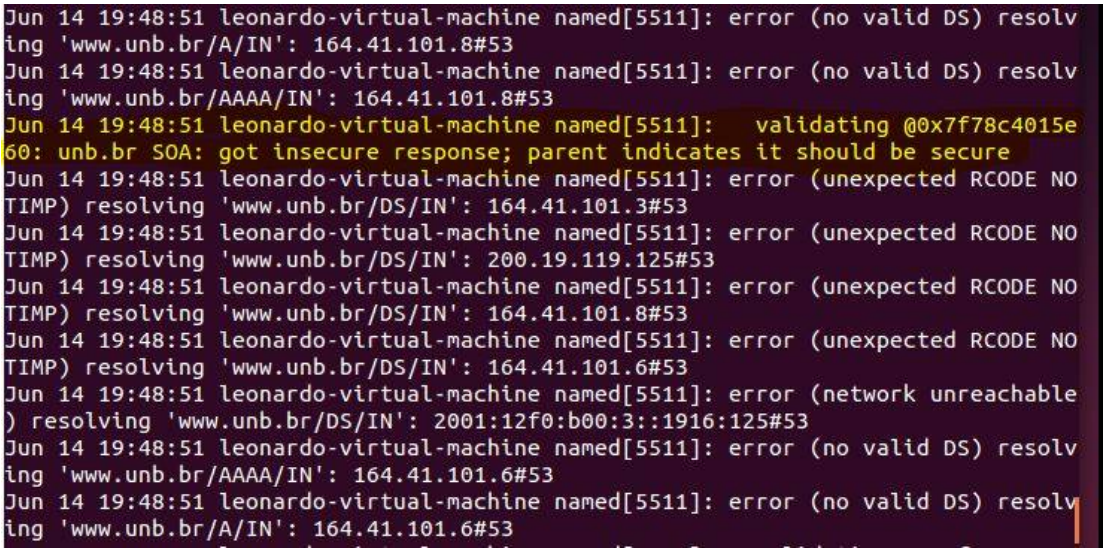

Figura 32 - Registros Syslog - Cenário 2 - Atividade I

Na ilustração acima, em destaque, validamos que a resposta foi recusada por que o domínio "Parent" informou que o domínio "UNB.BR" possui DNSSEC, entretanto não recebeu um resposta segura, assim deve ser descartada.

Com estes resultados, ficou provada a eficiência da extensão DNSSEC no incremento de segurança ao DNS, provendo integridade e autenticidade ao protocolo.

5.4 ATIVIDADE II

A segunda atividade proposta, está relacionada às estatísticas de uso do DNS e DNSSEC no Brasil e também inclui uma proposta de monitoramento de incidentes de envenenamento do cache.

Ao fim deste experimento teremos uma visão geral de como a segurança em relação ao DNS está sendo encarada no Brasil atualmente. Para isto, foi feita uma varredura em todos os blocos de endereços IPs do reservados ao Brasil, no período do dia primeiro de abril até o dia 28 de maio. A varredura foi feita de maneira distribuída, ou seja, a partir de diversas origens, para evitar problemas de bloqueios por firewalls da operadoras.

Neste experimento usamos as ferramentas NMAP, DIG e Notepad++, instaladas em um S.O. UBUNTU 12.4 LTS 64bits, processador Intel-I7 com 8 GBs de memória.

Para obter os dados de interesse, a varredura foi feita de maneira gradual. Primeiramente levantamos a quantidade servidores DNS públicos com a porta 53 aberta, desta lista diferenciamos servidores autoritativos e/ou recursivos. Destas duas listas retiramos informações de uso de DNSSEC, sistema operacional, software DNS e Versão do software.

Para as varreduras, o NMAP foi configurado com os seguintes parâmetros:

"nmap -Pn -n -T5 -p T:53 --open -iL Lista_de_IPs > Resultado", onde “-Pn" é para não executar o icmp request, "-n" para não fazer consulta reversa de DNS, "-T5" define a velocidade, “-p T:53" especifica a porta e o protocolo a ser inspecionado, "--open" filtra a saída para mostrar apenas os abertos.

O programa "DIG" foi usado para verificar a recursividade e também para checar o uso de DNSSEC.

Todos estes dados foram tratados e organizados para maior entendimento e geraram os seguintes resultados:

A) Na primeira fase foram identificados cerca de 45 mil servidores respondendo requisições na porta 53/TCP-UDP. Observação: Não significa que todos estes servidores estejam com serviço de DNS ativado, simplesmente respondem na porta 53.

B) Da lista acima, aproximadamente 7.500 (Sete Mil e quinhentos) são servidores recursivos.

C) Dentre os servidores recursivos abertos, 836 (Oitocentos e trinta e seis) estão aptos a responder requisições com a validação de DNSSEC. Esta fração representa cerca de 13% do total.

O resultado do Item 'A', é um dado puramente estatístico se analisado isoladamente, pois este valor representa a soma de diferentes tipos de serviço como, DNS recursivo, autoritativo, Relay e diversos serviços com porta não padronizada. Devemos ressaltar também que a maioria dos servidores DNS recursivos de redes locais não são públicos, obviamente por motivos de segurança e de performance.

No item 'B' podemos registrar uma quantia razoável de Recursivos abertos publicamente. Consideramos que a grande maioria destes sejam publicados indevidamente e sem intenção direta, pois vimos que a maioria destes são roteadores e equipamentos mal configurados. Estes servidores, como são abertos para toda a internet podem contribuir para a insegurança na rede, sendo facilmente usados em um ataque DoS amplificado.

O último resultado ('C'), nos mostra que a utilização de DNSSEC no Brasil ainda é baixa, porém devemos considerar também que a maioria destes servidores não são administrados, logo a implementação do DNSSEC seria uma segunda fase de incremento de segurança, já que muitos talvez em uma primeira análise não deveriam nem ser abertos para internet.

Em uma segunda fase desta atividade, foi proposto um "script" de monitoramento de incidentes de envenenamento de cache. O objetivo é detectar em tempo real a ocorrência de entrada fraudulenta em cache de algum servidor recursivo vulnerável.

Para facilitar o flagrante, filtramos a os servidores recursivos com a finalidade de gerar uma lista apenas com os mais vulneráveis. Então elaboramos uma lista de 20 prováveis alvos deste tipo incidente, dentre eles: bancos, seguradoras, governo, e demais sites que exigem autenticação para movimentação financeira.

O Script faz a resolução de cada nome da lista de alvos em todos os servidores vulneráveis e compara com uma base obtida anteriormente de maneira confiável. Sempre que existir uma entrada diferente da base, esta resposta é escrita em um arquivo de IPs suspeitos, para uma posterior verificação manual e individual.

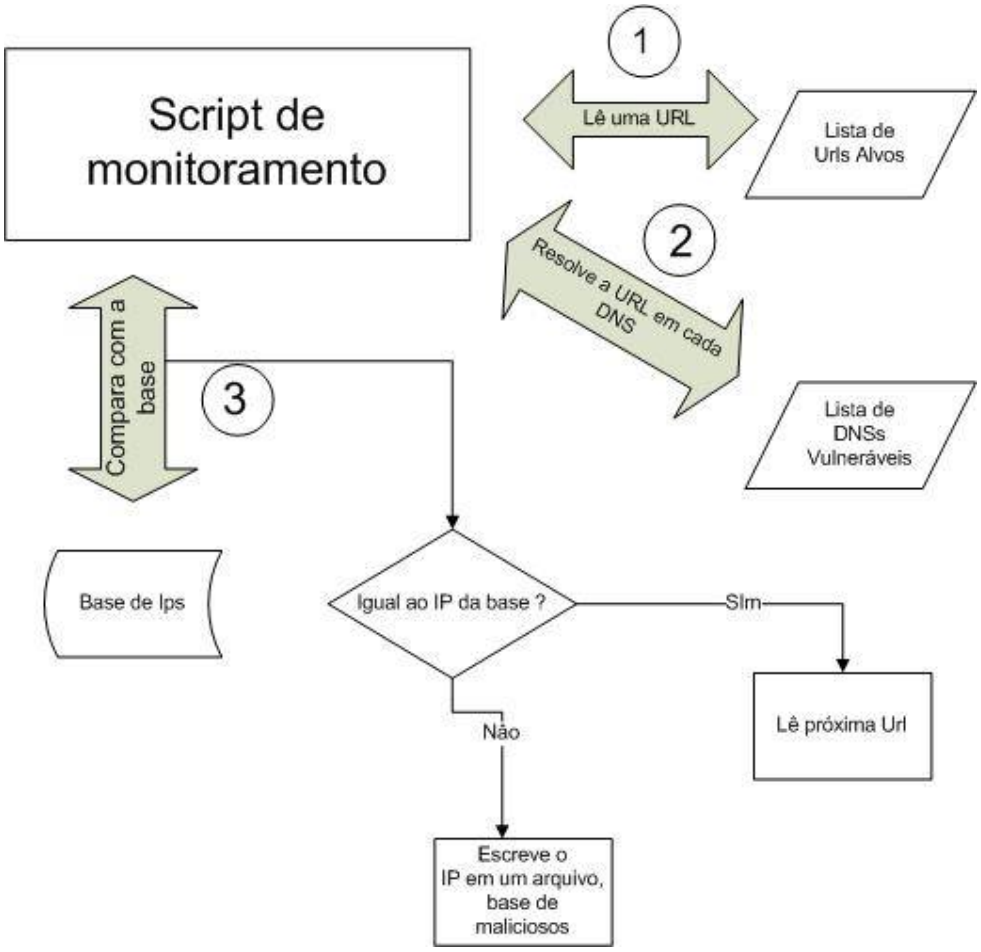

Figura 33 - Ilustração da rotina de monitoramento - Atividade II

Esta rotina foi executada continuamente durante 28 dias. A primeira entrada suspeita foi escrita após 14 dias de monitoramento. Ao final deste período o arquivo de entradas

suspeitas continha apenas 2 entradas, referentes ao mesmo domínio. O IP da resposta encontrada foi pesquisado em algumas listas de reputação, mas nenhuma informação foi encontrada.

Os resultados deste último experimento, mostram que este a rotina funciona bem, porém não obteve o sucesso esperado, talvez deva ser melhorada a escolha dos alvos a quantidade de servidores consultados e a duração.

6 CONCLUSÃO

O DNS é um protocolo que tornou mais amigável e gerenciável o acesso aos diversos hosts da Internet, já que é inviável a memorização de IPs. Seu funcionamento tornou-se vital para a grande rede e para todas as redes locais.

Como quase todos os protocolos de rede, o DNS está vulnerável a diversos ataques e incidentes de segurança. Portanto é essencial incrementar segurança neste sistema. Existem muitas medidas que podem ser tomadas para deixar este serviço mais seguro. Habilitar o DNSSEC, além de manter o software de DNS sempre atualizado, é a melhor maneira de prover segurança para a resolução de nomes.

Por todos os benefícios de segurança que o DNSSEC fornece, é altamente indicado o estudo de sua implementação principalmente em um ambiente de alta criticidade, onde a integridade e autenticidades das informações são requisitos importantes

Por meio da primeira atividade experimental, foi possível notar a efetividade do DNSSEC na proteção das transações de resolução de nomes. Foi exposto também o quão simples é a sua implementação em servidores recursivos, o que pode encorajar mais administradores a aderirem esta extensão segura, já que o sucesso do DNSSEC está diretamente associado à sua disseminação. Neste experimento também foi demonstrado que apesar da segurança contra alguns ataques, o DoS não pode ser evitado com este mecanismo, inclusive o efeito pode ser amplificado, já que o DNSSEC traz consigo uma carga um pouco mais de dados em cada requisição.

No cenário brasileiro em geral, as estatísticas não são muito boas em relação do DNS em geral, não só pelo fato de existir apenas 13,5 % de uso de DNSSEC no recursivos, mas pela quantidade de Servidores abertos para internet sem necessidade e pelos softwares desatualizados que ainda são usados em alguns servidores.

Dado este cenário, pode-se sugerir algumas políticas de segurança a nível nacional para melhorar estes aspectos. A principal delas seria a obrigatoriedade de uso do DNSSEC para um número maior de domínios, assim como já é feito para o domínio de bancos e “.jus”. Como foram detectados servidores de DNS abertos desnecessariamente, seria interessante uma intervenção do governo junto às operadoras para filtrar corretamente a porta 53 na internet, já que hospedar um serviço de DNS é dispensável para a grande maioria dos clientes de internet, que muitas vezes possuem inconscientemente um servidor disponível.

A administração do DNSSEC em servidores autoritativos pode trazer alguma complexidade, e isso explica por que é tão pouco utilizado. Já no caso dos servidores recursivos, não há nenhuma dificuldade em sua implementação e manutenção.

Em um trabalho futuro, poderia ser considerado a configuração de um servidor DNS aos modelos de um "*honey pot*", desta maneira poderia ser alimentada uma base de IPs maliciosos, e poderiam ser estudados novas vulnerabilidades que envolvem o DNS.

7 REFERÊNCIAS BIBLIOGRÁFICAS

AITCHISON, Ronald G. F. Pro DNS and BIND. New York: Apress, 2005.

ALBITZ, Paul; LIU, Cricket. DNS and BIND. 5th Edition. United States of America: O'Reilly Media, 2006

ATKINS, D. (1993). Threat Analysis of the Domain Name. IETF- RFC 3833.

COMER, D. E. Computer Networks and Internets. [S.l.]: Addison-Wesley, 2008.

DE CAMPOS, David Robert Camargo; JUSTO, Rafael Dantas. Tutorial DNSSEC. Versão 1.4.4. Disponível em <ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>. Acesso em 02 Junho 2015.

DINEV. T. (2006). Why spoofing is serious internet fraud. ACM.

DZUNG, D., NAEDELE, M., HOFF, T. P., & CREVATIN, M. (2005). Security for Industrial Communication Systems. Proceedings of the IEEE, Volume: 9, Issue: 6.

WESSELS, D., M. FOMENKOV. (2003). Wow, that's a lot of packets. Cooperative Association for Internet Data Analysis - CAIDA, San Diego Supercomputer Center, University of California, San Diego.

FRIEDMAN, A. D. (2010). Sistema de nomes de domínios: Estudo da insegurança sobre o contexto brasileiro. Projeto de Pós-graduação, Universidade Católica de Brasília, 70.

HACKPITTSBURGH. Network Securtiy: Man-In-The-Middle Attacks. 2011.Disponível em: <http://www.hackpittsburgh.org/wpcontent/uploads/2011/03/ManInThe-Middle.jpg>. Acesso em: 01 JUN 2015.

Hoepers, Cristine. (2013). Gestão de Incidentes e Resiliência das Infraestruturas Críticas de Internet. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil Núcleo de Informação e Coordenação do Ponto BR Comitê Gestor da Internet no Brasil.

ICANN, Internet Corporation for Assigned Names and Numbers. Disponível em: <http://www.icann.org/>. Acessado em: 13 Maio 2015.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS – ICANN. ICANN destaca vulnerabilidade do Sistema de Nomes de Domínio e fornece ferramentas: ICANN chama a atenção para importante problema de segurança na Internet. Disponível em <http://www.icann.org.br/announcements/announcement-06aug08.htm>. Acesso em: 30 Mai. 2015.

IWASA, A. M. DE A.; HILÁRIO, P. S. (2011). ANÁLISE DE SEGURANÇA EM DNS E PROPOSTAS DO MECANISMO DE DEFESA DO DNSSEC. Trabalho de Graduação

em Engenharia de Redes de Comunicação, Faculdade de Tecnologia, Universidade de Brasília, Brasília, DF, 69p

KIZZA, J. M. *Computer Network Security*. [S.l.]: Springer, 2005.

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet - Uma Abordagem Top-Down. [S.l.]: Pearson, 2010.

NOÇÕES BÁSICAS DE ZONAS TRANSFERÊNCIAS DE ZONAS, MICROSOFT https://technet.microsoft.com/pt-br/library/cc781340(v=ws.10).aspx, Acessado em 21 de maio de 2015.

O'REILLY;4th edition; 2001; ISBN 0.596.00158.4

P. VIXIE. (1999). Extension Mechanisms for DNS (EDNS0), RFC 2671, IETF.

ROOT SERVERS, IANA, https://www.iana.org/domains/root/servers < acesso em 15 de maio de 2015>

SEIXAS, P. R. L. UMA ANÁLISE DO PROTOCOLO DNS E SUAS EXTENSÕES. SIMPOETS, CEFET-GO,161-171, 2008

SILVA, Maurício Corvello da. Segurança em IPV6: Interceptação E neutralização de ataque ndp spoofing. -60p. Trabalho de Conclusão de Curso- Instituto Federal Sul-Rio-Grandense

SILVA, Sílvio Lucas da. Segurança em DNS: Investigando o DNSSEC através de experimento prático. - 69p. Monografia (Especialização em Segurança da Informação) –Faculdade de Tecnologia IBRATEC de João Pessoa.

VERISIGN, DOSSIÊ SOBRE O MERCADO DE DOMÍNIOS NA INTERNET. Volume 1, Edição 1, 2004

TANENBAUM, Andrew. Redes de Computadores. 4. ed. Rio de Janeiro: Campus Elsevier, 2003.

Threat Analysis of the Domain Name System (DNS) – RFC 3833, IET, https://tools.ietf.org/html/rfc3833 <acesso em 3 de junho de 2015>

WIJINGAARDS W. C. A., OVEREINDER B. J. (2009), Securing DNS: Extending DNS servers with DNSSEC Validator, *IEEE*.