Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Departamento de Computação e Sistemas

Júlio César dos Santos Simião

Análise e Criação de Algoritmos para Garantia de Segurança em Servidores DNS

João Monlevade
2017

Júlio César dos Santos Simião

Análise e Criação de Algoritmos para Garantia de Segurança em Servidores DNS

Monografia apresentada ao curso de Sistemas de Informação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina "Trabalho de Conclusão de Curso II".

Orientador: Theo Silva Lins

João Monlevade

2017

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

ATA DE DEFESA

Aos 31 dias do mês de março de 2017, às 16 horas e 00 minutos, na sala C304 do Instituto de Ciências Exatas e Aplicadas, foi realizada a defesa de Monografia pelo aluno Júlio César dos Santos Simião, sendo a Comissão Examinadora constituída pelos professores: Prof. Mestre Theo Silva Lins, Prof. Doutor Vinícius Fernandes Soares Mota e Prof. Mestre Marlon Paolo Lima.

O candidato apresentou a monografia intitulada: *"Análise e Criação de Algoritmos para Garantia de Segurança em Servidores DNS"*. A comissão examinadora deliberou, por unanimidade, pela aprovação do candidato, com nota 9,5 (NOVE E MEIO), concedendo-lhe o prazo de 15 dias para incorporação das alterações sugeridas ao texto final.

Na forma regulamentar, foi lavrada a presente ata que é assinada pelos membros da Comissão Examinadora e pelo graduando.

João Monlevade, 31 de março de 2017.

Theo Silva Lins

Prof. Mestre Theo Silva Lins
Professor Orientador/Presidente

Prof. Doutor Vinícius Fernandes Soares Mota
Professor Convidado

Marlon Paolo Lima

Prof. Mestre Marlon Paolo Lima
Professor Convidado

Júlio César dos Santos Simião

Júlio César dos Santos Simião
Graduando

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

Curso de Sistemas de Informação

FOLHA DE APROVAÇÃO DA BANCA EXAMINADORA

Análise e Criação de Algoritmos para Garantia de Segurança em Servidores DNS

Júlio César dos Santos Simião

Monografia apresentada ao Instituto de Ciências Exatas e Aplicadas da Universidade Federal de Ouro Preto como requisito parcial da disciplina CSI499 – Trabalho de Conclusão de Curso II do curso de Bacharelado em Sistemas de Informação e aprovada pela Banca Examinadora abaixo assinada:

Prof. Mestre Theo Silva Lins
DECSI - UFOP

Prof. Doutor Vinícius Fernandes Soares Mota
DECSI - UFOP

Prof. Mestre Marlon Paolo Lima
DECSI - UFOP

João Monlevade, 31 de março de 2017.

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

TERMO DE RESPONSABILIDADE

Eu, Júlio César dos Santos Simião,
declaro que o texto do trabalho de conclusão de curso intitulado "Análise e Criação de Algoritmos para Garantia de Segurança em Servidores DNS" é de minha inteira responsabilidade e que não há utilização de texto, material fotográfico, código fonte de programa ou qualquer outro material pertencente a terceiros sem as devidas referências ou consentimento dos respectivos autores.

João Monlevade, 31 de março de 2017

Júlio César dos Santos Simião
Assinatura do aluno

Aos meus familiares e amigos, pelo apoio e incentivo.

Agradecimentos

Agradeço primeiramente aos meus familiares, em especial minha mãe Maria do Carmo e minhas tias Maria das Graças e Geralda, por todo o apoio, carinho e incentivo recebido. Aos meus amigos do SANTA CRUZ que sempre estiveram comigo durante a realização desse sonho. Aos irmãos da república Vira-Lata pelos incontáveis bons momentos de estudo, descontração e amizade.Aos amigos da faculdade e de João Monlevade, em especial Carol, Lucas, Hugo e Michele. A INCOP por me mostrar uma nova visão de gestão e economia voltada ao bem estar do ser humano e não ao capitalismo. Ao movimento #OCUPAUFOP pelos grandes momentos de discussão politica e criação de pensamento crítico.A Universidade Federal de Ouro Preto pelo suporte oferecido a partir de seu programa de assistência, pelo ensino público, gratuito e de qualidade.

"It always seems impossible until is done". (Nelson Mandela)

Resumo

Desde a sua criação, a Internet recebe cada vez mais acessos, e atualmente bilhões de computadores estão conectados à rede. A Internet é uma rede IP e devido a infinidade de *websites* existentes atualmente seria impossível para um ser humano lembrar todos os endereços IPs que irá utilizar. O DNS é responsável por realizar a tradução da URL de determinada página digitada pelo usuário no IP correspondente que será interpretado pelo navegador, portanto realiza um trabalho muito importante para facilitar o acesso a páginas web. O DNS segue sendo alvo para invasores que desejam obter alguma vantagem para agir de forma fraudulenta. Nesse sentido, foi proposto nesse trabalho a criação de um algoritmo com o objetivo de determinar a autenticidade de um servidor DNS, como contribuições há o desenvolvimento de uma página web e de uma extensão para o navegador Google Chrome onde o usuário poderá realizar consultas para obter mais informações sobre o servidor DNS. **Palavras-chaves**: *dns*. autenticidade. *pharming*.

Abstract

Since its inception, the Internet has been receiving more and more accesses, and currently billions of computers are connected to the network. The Internet is an IP network and due to the plethora of existing websites it would be impossible for a human to remember all the IP addresses that they will use. The DNS is responsible for translating the URL of a certain page entered by the user into the corresponding IP that will be interpreted by the browser, so it performs a very important function to facilitate access to web pages. DNS remains a target for attackers who want to gain some advantage in order to act fraudulently. In this sense, it was proposed in this work the creation of an algorithm with the objective of determining the authenticity of a DNS server, as contributions there is the development of a web page and an extension to the Google Chrome browser where the user can make queries to obtain More information about the DNS server.

Key-words: dns. authenticity. pharming.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

BIND	Berkeley Internet Name Domain
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
IP	Internet Protocol
LAN	Local Area Network
PXE	Preboot eXecution Environment
TFTP	Trivial File Transfer Protocol
URL	Uniform Resource Locator

Sumário

1 Introdução

Desde a sua criação a Internet recebe cada vez mais acessos, atualmente bilhões de computadores estão conectados à rede. Diariamente uma infinidade de *websites* são criados e acessados para diversos propósitos. A Internet é uma rede IP. Cada *host* é associado a um endereço IP que deve ser conhecido por qualquer outro *host* que deseja se comunicar. Mas seria impossível para um ser humano lembrar todos os endereços IP que irá utilizar na Internet (CARLI, 2003), por exemplo, para se acessar www.pf.gov.br, o usuário precisaria digitar em seu navegador o IP 200.169.41.77.

Em (EC-COUNCIL, 2009) e (CARLI, 2003) o DNS é definido como servidores responsáveis por realizar a tradução da URL de determinada página web digitada pelo usuário no IP correspondente que será interpretado pelo navegador. A essência do DNS é a criação de um esquema hierárquico e atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído (TANENBAUM; WETHERALL; ELIZONDO, 2012).

Devido a sua importância para facilitar o acesso aos sites disponíveis na Internet o DNS segue sendo um alvo para invasores que desejam obter alguma vantagem para agir de forma fraudulenta, sendo assim é necessário garantir a sua segurança.

De acordo com (TANENBAUM; WETHERALL; ELIZONDO, 2012) o *DNS Spoofing* é uma ação muito comum que é utilizada para enganar um servidor DNS, fazendo-o instalar um falso endereço IP, nesta prática o invasor ataca o servidor de nomes responsável pelo domínio de um site e altera o endereço IP relacionado com o site desejado pelo usuário para o seu IP (EC-COUNCIL, 2009).

Um cache que contém um endereço intencionalmente falso é chamado de *cache poisoning* (TANENBAUM; WETHERALL; ELIZONDO, 2012). Uma de suas consequências é o *pharming*. O *pharming* é um tipo específico de *phishing* que de acordo com (KARLOF et al., 2007) é definido como um ataque onde o usuário é atraído para um site semelhante ao desejado. O ataque de *pharming* ocorre quando o redirecionamento para páginas falsas é feita por meio de alterações no servidor DNS (CERT.BR, 2012). Dessa forma, o usuário poderá ser vítima de roubo de informações confidenciais como login, senhas, dados bancários e pessoais.

Uma outra forma que o usuário pode ser alvo de *pharming* é quando o servidor DNS configurado em sua máquina, modem ou roteador é alterado para o IP correspondente ao computador do invasor, dessa forma ao solicitar acesso a determinadas páginas web irá receber páginas semelhantes a desejada e poderá ter seus dados capturados.

O trabalho propõe a concepção de uma algoritimo capaz de identificar a autenticidade de um servidor DNS e a criação de uma página web e extensão google chrome para auxiliar na consulta de informações referente ao servidor DNS pesquisado pelo usuário.

1.1 Objetivos

A partir dos problemas listados e da importância do DNS na utilização da Internet ultimamente, o presente trabalho tem como objetivo geral a criação de um algoritmo capaz de determinar a autenticidade de um servidor DNS.

Como objetivos específicos do trabalho se encontram a criação de ferramentas como uma extensão para Google Chrome que irá realizar a verificação em tempo real dos resultados obtidos ao se consultar um servidor DNS, criação de um página web responsável por realizar consultas.

Os testes realizados e os resultados obtidos durante o desenvolvimento serão apresentados ao decorrer do presente trabalho.

1.2 Contribuições do Trabalho

Nos últimos anos o número de casos de vítimas virtuais vem crescendo, o *phishing* e o *pharming* são técnicas que se assemelham no modo de atuação, ambas tem o objetivo de entregar ao usuário uma página idêntica a solicitada com o objetivo de capturar seus dados e informações confidenciais.

Sendo o *pharming* um ataque resultante de alterações no DNS, o algoritmo proposto tem o objetivo de oferecer ao usuário uma forma de verificação do serviço DNS configurado em sua máquina para o acesso a páginas web, e dessa forma diminuir o risco de um possível uso de um servidor DNS falso e consequentemente o acesso a sites que possuem o objetivo de capturar os seus dados sigilosos.

Dessa forma, o presente trabalho irá contribuir oferecendo:

1. Extensão para o navegador Google Chrome: Ao fazer uso desta extensão o usuário poderá especificar o servidor DNS configurado em sua máquina. Dessa forma, a extensão irá realizar uma comparação na resposta obtida ao realizar a consulta a página web atual utilizando o servidor inserido pelo usuário e servidores conhecidos e seguros.

2. Página Web: Criação e hospedagem de um site onde o usuário após especificar o servidor DNS pode realizar consultas e obter informações referente ao servidor.

1.3 Método de Pesquisa

Nesta seção serão apresentadas e descritas as atividades realizadas para o desenvolvimento do trabalho. Elas podem ser organizadas conforme as etapas:

(i) Levantamento bibliográfico sobre o DNS afim de identificar vulnerabilidades, exemplificar os crimes virtuais existentes especificando os que utilizam o DNS e citar os tipos de DNS que podem ser utilizados atualmente.

(ii) Instalação *Honeypot*: Foi definida o tipo da *honeypot* a ser instalada, qual o serviço DNS escolhido e qual a vulnerabilidade disponível para os atacantes.

(iii) Ferramentas utilizadas: Para realizar as etapas posteriores foram utilizadas as seguintes ferramentas: fpdns, nmap, TCPdump.

(iv) Base de dados contendo DNS reais: A partir de uma faixa aleatória de IP foi criado um *scanner* responsável por verificar quais IPs possuem um servidor DNS em funcionamento.

(v) DNS falsos: Existem atualmente uma infinidade de algoritmos em diferentes linguagens que executam o serviço de respostas de um servidor DNS. Foram selecionados *scripts* na linguagem Python que foram executados e os resultados armazenados.

(vi) Configuração do DNS para redirecionamentos de sites: Durante a execução dos DNS falsos as configurações padrões foram alteradas para que quando o usuário digitasse a url desejada fosse redirecionado para outras páginas.

(vii) Acompanhar o trafego com TCPdump: Para capturar os pacotes de consultas e respostas realizadas durante a execução dos DNS falsos foi utilizado o *sniffer* TCPdump.

(viii) Criação do algoritmo: A partir da analise dos resultados obtidos durante os DNS reais e DNS falsos, foi possível identificar algumas diferenças entre os tipos de DNS. Dessa forma, o algoritmo aborda essas diferenças para determinar a autenticidade do servidor DNS.

(ix) Página Web: Criação de uma página Web responsável por realizar consultas no servidor DNS especificado pelo usuário, as seguintes consultas podem ser realizadas: verificar se a porta padrão está aberta, verificar versão do servidor e comparar respostas entre DNS conhecidos como Google e openDNS e o IP inserido pelo usuário.

(x) Extensão navegador Google Chrome: Concepção de uma extensão para o navegador Google Chrome responsável por realizar consulta em tempo real para o site que o

usuário está acessando naquele momento e comparar a resposta obtida com DNS conhecidos.

1.4 Organização do Trabalho

Seção destinada a demonstrar a organização do trabalho.

O primeiro capítulo é composto por esta introdução, onde os objetivos gerais e específicos são demonstrados, as contribuições que podem ser obtidas com a execução do trabalho e a metodologia utilizada.

O segundo capítulo diz respeito ao referencial teórico.

No terceiro capítulo há a apresentação dos trabalhos relacionados.

O desenvolvimento realizado é retratado no quarto capítulo.

O quinto e último capítulo é dedicado a conclusão e trabalhos futuros.

2 Referenciais teóricos

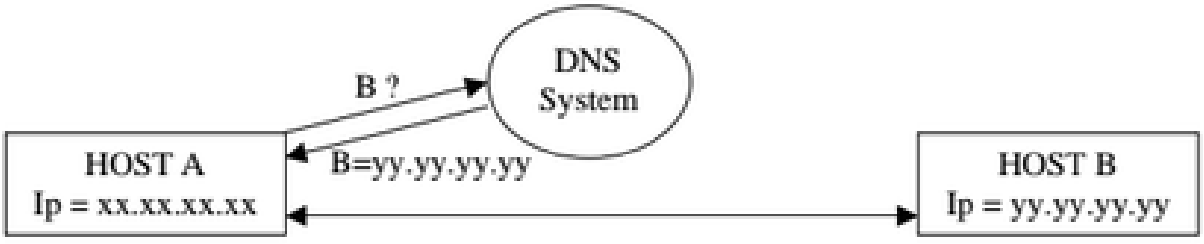
2.1 Domain Name System

O sistema de nomes de domínio (DNS) é um componente crítico na infraestrutura da Internet, isso ocorre porque a maioria dos serviços de rede e aplicações necessitam da tradução de nomes de domínio para endereços IP. Como resultado, mesmo que apenas uma pequena parte da infraestrutura do DNS se torne indisponível por um curto período de tempo pode ter um efeito sobre o resto da Internet (GUO; CHEN; CHIUEH, 2006)

Devido a sua importância quase todas as aplicações da Internet contam com o sistema de nomes de domínio (DNS) para o bom funcionamento. De acordo com (DECCIO et al., 2009) o papel realizado pelo DNS de traduzir nomes para endereços é especialmente fundamental para os usuários, que são em grande parte acostumados a reconhecer "locais"da Internet utilizando palavras humanamente amigáveis, como por exemplo "www.facebook.com", títulos e abreviaturas, em vez do endereço IP numérico "157.240.0.35". O DNS também é necessário para entrega de e-mail, descoberta de serviços e identificação de *hosts*.

A Figura 1 demonstra um exemplo simplificado do funcionamento de um servidor DNS, o *host* A deseja-se conectar ao *host* B, mas a princípio o IP de B não é conhecido por A. Dessa forma, o *host* A realiza uma consulta ao DNS e descobre o IP de B e a conexão pode ser realizada.

Figura 1 – Exemplo simplificado de funcionamento DNS

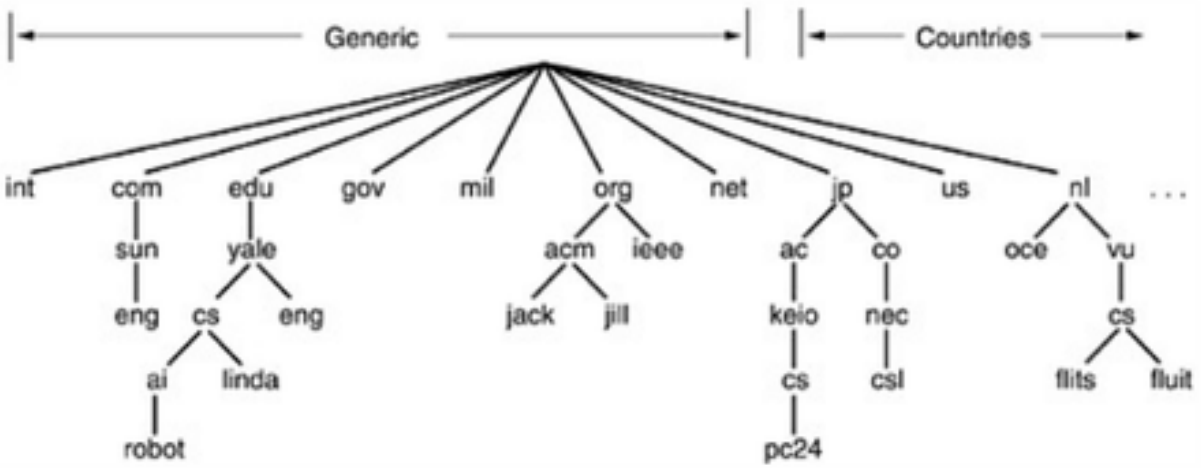


Fonte: (CARLI, 2003)

Conforme (LU; LIU, 2009) o DNS fornece um mapeamento automático entre o nome simbólico e o endereço IP equivalente, implementando um espaço de nomes hierárquico para objetos de Internet os classificando em domínios. Cada domínio é divido em subdomínios, e assim por diante. Todos os domínios são organizados como uma estrutura de árvore. Os domínios de nível superior vêm em duas divisões: genéricos e países. Cada domínio controla todos os sub-domínios sob ele o que pode ser verificado na Figura 2. Isso faz com que a autonomia seja um recurso do DNS. Dessa forma cada domínio é autorizado

para atribuir nomes para *hosts* ou para alterar esses nomes sem informar uma autoridade central.

Figura 2 – Fragmento de uma hierarquia DNS

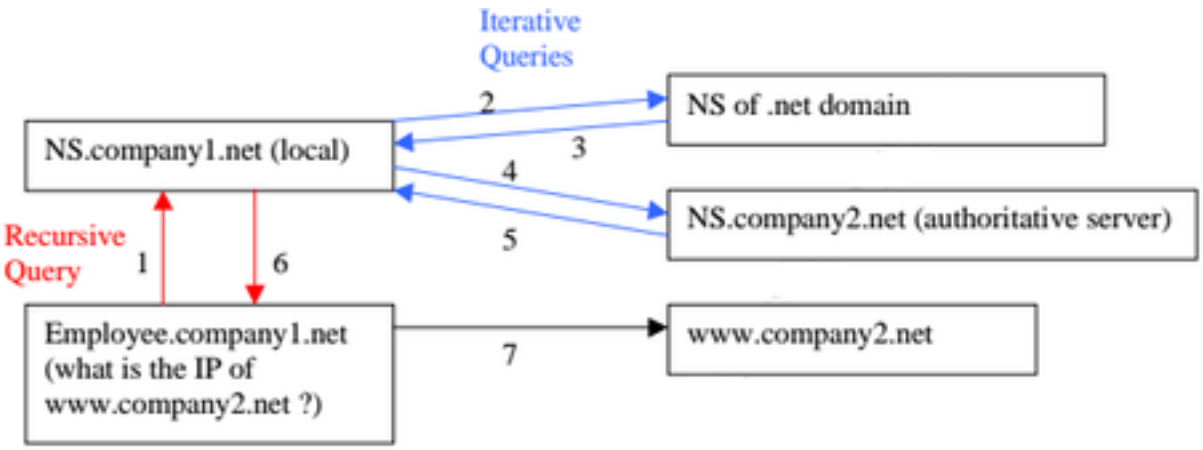


Fonte: (TANENBAUM et al., 2003)

Quando uma consulta é feita a um servidor DNS, a mesma pode ser resolvida de duas formas: interativa e recursiva. Conforme (CARLI, 2003) em uma consulta recursiva o cliente deseja a resposta ou uma mensagem de erro. O *host* consultado deve fazer o que for preciso para encontrar a resposta: consultar outros servidores até obter as informações ou até que a consulta de nome falhe.Utilizando a consulta interativa é solicitado uma resposta se o servidor conhece. Caso a resposta não seja conhecida, o cliente receberá a informação de qual servidor pode ter a resposta.

A figura 3 exemplifica os tipos possíveis de consultas realizadas por um servidor DNS.

Figura 3 – Exemplo tipos de consulta



Fonte: (CARLI, 2003)

2.1.1 BIND

BIND é um software de código aberto distribuído pela *Internet System Consortium* que implementa o DNS . O BIND contém todos os softwares necessários para fazer e responder perguntas relacionados a tradução de nomes.

A distribuição BIND possui três partes:

- Resolver
- Servidor de autoridade de nome de domínio
- Ferramentas operacionais e de diagnóstico.

O software está disponível para download em <https://www.isc.org/downloads/bind>.

2.1.2 DNSMASQ

DNSMASQ é um DNS leve, TFTP, PXE e servidor DHCP. É destinado para oferecer DNS e DHCP para uma LAN. DNSMASQ aceita questões DNS e as responde a partir de um cache local pequeno ou as encaminha para um DNS real e recursivo. Carrega o conteúdo de /etc/hosts para que nomes de *hosts* locais que não aparecem no DNS global possam ser resolvidos e também responde a consultas DNS para *hosts* DHCP configurados. Ele também pode atuar como servidor DNS autoritário para um ou mais domínios, permitindo que nomes locais apareçam no DNS global. Sendo ainda possível ser configurado para fazer validação DNSSEC.

O software está disponível em <http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html>.

2.1.3 Microsoft DNS

O DNS do Azure é um serviço de hospedagem para domínios DNS, fornecendo resolução de nomes usando a infraestrutura do Microsoft Azure. Ao hospedar os domínios no Azure, os usuários podem gerenciar os registros DNS usando as mesmas credenciais, APIs, ferramentas e cobrança que seus outros serviços da Azure. Não se trata de um software de código aberto, dessa forma é necessário que o usuário contrate os serviços.

O software está disponível para consulta em <https://azure.microsoft.com/pt-br/services/dns>.

2.1.4 Open DNS

Open DNS é um serviço de DNS gratuito disponível globalmente. Para o usuário que deseja utilizar os servidores Open DNS para a resolução de nomes em seus computadores podem encontrar os IPs referentes a estes servidores e outras informações de serviços *premium* em <https://www.opendns.com>.

2.2 CRIMES VIRTUAIS

Atualmente inúmeros computadores estão conectados a internet, ao mesmo tempo que sua utilização traz vantagens tanto para usuários comuns e empresas, esse ambiente se torna um lugar para que crimes virtuais aconteçam. De acordo com (SAINI; RAO; PANDA, 2012) o termo crime virtual pode ser definido como um ato cometido ou omitido em violação de uma lei, se caracteriza como uma atividade criminal que faz uso de computadores.

2.2.1 Engenharia Social

A engenharia social é definida por (NAKAMURA; GEUS, 2007) como técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança.

2.2.2 Web Defacement

Web defacement ocorre quando um intruso maliciosamente altera a *web page* do alvo a ser atacado inserindo ou substituindo dados provocativos e frequentemente ofensivos. A alteração da *web page* de uma organização expõe os visitantes a informações enganosas até que a alteração não autorizada seja descoberta ou corrida (KARLOF et al., 2007).

A técnica de *web defacement* também pode ser utilizada aliada a ataques como *phishing* e *pharming*.

2.2.3 Phishing

De acordo com (KARLOF et al., 2007) *phishing* pode ser definido como um ataque que utiliza a engenharia social em que o usuário é atraído para um site semelhante ao desejado. O objetivo geral é o roubo de identidade, com o propósito de obter ganhos financeiros o atacante tenta enganar o usuário a revelar os seus dados credenciais, informações pessoais ou dados bancários.

Segundo (CERT.BR, 2012) o *phishing* ocorre por meio do envio de mensagens eletrônicas que:

- tentam se passar pela comunicação oficial de uma instituição conhecida;
- procuram atrair a atenção do usuário;
- informam que a não execução dos procedimentos descritos pode acarretar sérias consequências;
- tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio de acessos a páginas falsas.

2.2.4 Pharming

(CERT.BR, 2012) define o *pharming* como:

Tipo específico de *phishing* que envolve a redireção da navegação do usuário para sites falsos, por meio de alterações no serviço DNS. Esta redireção pode ocorrer:

- por meio do comprometimento do servidor DNS do provedor que você utiliza;
- pela ação de códigos maliciosos projetados para alterar o comportamento do serviço de DNS do seu computador;
- pela ação direta de um invasor, que venha a ter acesso às configurações do serviço DNS do seu computador ou modem de banda larga.

2.3 TIPOS DE ATAQUES

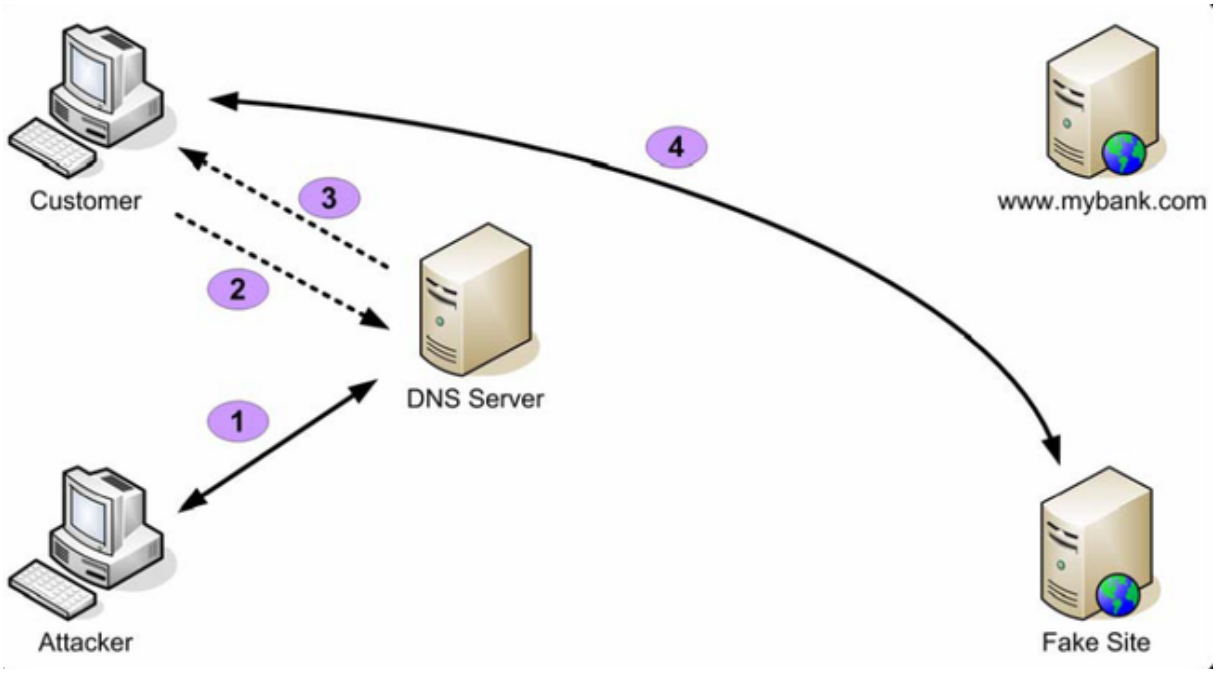
2.3.1 DNS Spoofing

DNS Spoofing é melhor descrito como um servidor DNS fazendo uso de uma informação falsa vindo de um *host* que não é a autoridade por aquela informação. É uma ameaça de segurança significativa para organizações que não tenham tomado medidas para se proteger. *DNS Spoofing* pode permitir que atacantes tenham acesso a e-mails, usuários podem ser direcionados para a página web incorreta e ser uma porta de entrada para um ataque de DDoS (SAX, 2000).

De acordo com (CARLI, 2003) *DNS Spoofing* é o termo que se refere a ação de responder uma requisição DNS que é direcionada para outro servidor (o servidor DNS "real"). Isso pode ser em uma troca entre servidores ou em um dialogo entre cliente e servidor.

DNS Spoofing ocorre quando o atacante se coloca como um *host* confiável na rede com o objetivo de obter acesso de todos recursos que um *host* real possui (JANBEGLOU; ZAMANI; IBRAHIM, 2010). Na Figura 4 é possível visualizar a resolução de nomes após esse tipo de ataque.

Figura 4 – Resolução de nomes após o DNS ser vitima de DNS spoofing



Fonte: (OLLMANN, 2005)

2.3.2 Cache Poisoning

Quando o endereço IP não é conhecido para o servidor DNS local isso requer muito trabalho. Se uma determinada página web é acessada várias vezes o trabalho de resolução de nomes é executado frequentemente. Dessa forma, é utilizado o conceito de cache. No momento em que o DNS realizar todo o trabalho para resolver um endereço IP ele irá salvar o resultado em uma cache. Dessa maneira, quando uma próxima consulta é realizada para o mesmo IP o DNS pode simplesmente verificar os valores contidos em cache, evitando que todo o trabalho seja realizado novamente (RACKI, 2008).

De acordo com (RACKI, 2008) o ataque de cache *poisoning* ou envenenamento de cache ocorre quando um atacante modifica os endereços de IP em uma cache de um servidor DNS. Após essa alteração todas as requisições futuras para aquele servidor DNS podem ser enviadas para aonde o atacante quiser.

O processo de cache *poisoning* é explicado em (OLLMANN, 2005) e pode ser visualizado na Figura 5.:

1. O invasor consulta o servidor DNS para o endereço IP de um *host* que é gerenciado por um servidor de nomes de propriedade do invasor. Qual o endereço IP para "www.attackerowned.com?"

2. O cache do servidor DNS não possui uma entrada para "www.attackerowned.com"e para resolver o endereço IP precisa consultar o servidor DNS autoritário para

"www.attackerowned.com". Esse servidor pertence ao atacante.

3. O servidor DNS do atacante informa para o cache do servidor DNS que o endereço IP de "www.attackerowned.com"é 200.1.1.10. Adicionalmente, o servidor DNS do atacante também inclui registros de resolução adicionais falsos como:

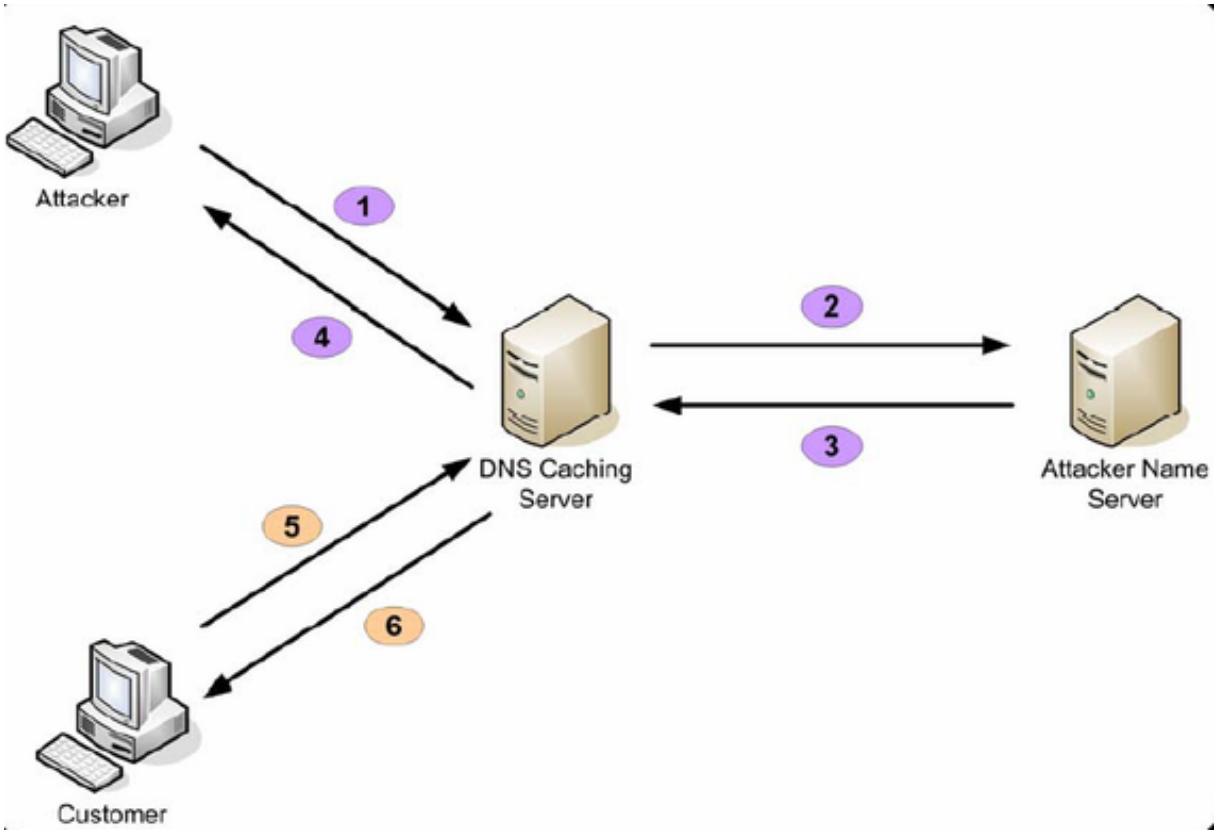
   - www.mybank.com is 200.1.1.11
   - mail.mybank.com is 200.1.1.11
   - secure.mybank.com is 200.1.11

4. O cache do servidor DNS responde a consulta original do atacante que o endereço IP de "www.attackerowned.com"é 200.1.1.11. Este resultado em conjunto com os registros adicionais é salvo na cache do servidor DNS.

5. Em outro momento, um usuário qualquer que também utiliza o cache do servidor DNS consulta o endereço IP de "www.mybank.com".

6. O cache do servidor DNS responde a consulta do usuário com a informação falsa salva: O endereço IP de "www.mybank.com"é 200.1.1.11 em vez do endereço verdadeiro 150.10.1.21.

Figura 5 – O processo de DNS caching poisoning



Fonte: (OLLMANN, 2005)

2.3.3 Alterando as configurações de roteadores

Roteadores são um jeito popular que usuários podem criar redes *wireless* em suas residências. Infelizmente, após visitar uma página web maliciosa ou não alterar as credenciais padrões de acesso as configurações do roteador, uma pessoa pode tornar o seu roteador um alvo fácil para ataques, configurações no roteador podem ser alteradas incluindo os servidores DNS utilizado pelos membros da rede (STAMM; RAMZAN; JAKOBSSON, 2007).

Alterando informações referente ao servidor DNS o novo valor configurado será o responsável por realizar as traduções de nome em IP. Dessa forma, o usuário poderá ser vítima de *pharming* e ter informações pessoas e bancárias enviadas ao invasor.

3 Trabalhos Relacionados

A abordagem apresentada em (NICOMETTE et al., 2011) se asemelha ao presente trabalho, pois uma *honeypot* de alta interação foi utilizada para analisar o comportamento dos atacantes após ganharem acesso a máquina utilizando ataques via SSH.

Em (CARLI, 2003) é apresentado o funcionamento do DNS para a tarefa de resolução de nomes e explicado as diferentes formas que um servidor DNS pode ser atacado, o artigo separa os ataques em dois tipos: ataques de protocolo e ataques de servidor. O artigo também apresenta recomendações que podem ser implementadas no BIND para garantir a segurança em um servidor DNS.

O objetivo apresentado em (JALALZAI; SHAHID; IQBAL, 2015) foi de discutir as vulnerabilidades de segurança. O DNS apresenta uma grande importância para a comunicação na internet, os autores introduziram uma estrutura criptografada configurada em um *framework* de código aberto, incorporando DNSSEC com software BIND que aborda os problemas de integridade e disponibilidade DNS estabelecendo uma cadeia de confiança DNS usando dados digitalmente assinados.

O trabalho proposto nesse artigo se assemelha aos apresentados anteriormente, pois propõe uma forma para se garantir a segurança na utilização de servidores DNS, entretanto a abordagem encontrada nestes trabalhos relacionados não incluem a autentificação do DNS que está sendo utilizado para a resolução de nomes, proposta esta que será desenvolvida no presente trabalho.

4 Desenvolvimento

4.1 Honeypot

Uma *honeypot* de acordo com (SEIFERT et al., 2007) pode ser definida como um dispositivo seguro que tem como objetivo atrair atividades maliciosas para si mesmo. Capturar essa atividade maliciosa permite estudá-la para entender as operações e motivações dos atacantes, e consequentemente ajudar a aprimorar a segurança de computadores e redes.

Uma *honeypot* é classificada de acordo com o grau de interação disponibilizada para o atacante, sendo dividido em dois níveis: alto e baixo.(SPITZNER, 2003)

Segundo (NICOMETTE et al., 2011) *honeypots* de baixa interação são úteis para promover dados quantitativos sobre ameaças maliciosas e informações de alto nível sobre padrões de ataques na Internet, entretanto não são apropriadas para monitorar atividades onde o atacante toma o controle da máquina da vitima escolhida como alvo e tenta progredir no processo de intrusão para obter privilégios adicionais. Este objetivo pode ser atingido com a utilização de *honeypots* de alta interação que oferecem serviços reais para os atacantes interagirem o que a torna mais perigosa quando comparada com a de baixa interação. Uma *honeypot* de alta interação pode corresponder a um sistema operacional físico ou máquinas virtuais.

Utilizando a metodologia apresentada em (NICOMETTE et al., 2011) uma *honeypot* de alta interação foi criada para receber ataques via SSH. O serviço escolhido para ser monitorado foi um servidor DNS utilizando BIND9 e o sistema operacional Linux Mint 17.2.

A partir da análise realizada na *honeypot* foi possível identificar uma série de conexões via SSH, sendo a *honeypot* utilizada para acessar outras máquinas, as informações deixadas pelo atacante estavam contidas em pastas temporárias, e foi possível identificar quais seriam as próximas máquinas a serem atacadas e quais combinações de senhas seriam utilizadas.

Utilizando os logs de sistema, logs gerados pelo BIND9 e capturando os pacotes utilizando a ferramenta TCPdump foi possível verificar que O serviço DNS instalado na *honeypot* foi utilizado por algumas máquinas para realizar a tradução de nomes.

4.2 Ferramentas utilizadas

Durante a etapa de desenvolvimento foram utilizadas ferramentas que viabilizaram a conclusão de cada etapa, as ferramentas utilizadas foram:

- TCPDump

  O TCPDump é uma ferramenta que captura o tráfego de rede, no presente trabalho a ferramenta foi utiliza para capturar a troca de informações entre o servidor DNS e um cliente.

  A ferramenta está disponível em: <http://www.tcpdump.org/>.

- FPDNS

  O FPDNS é uma ferramenta que retorna remotamente a versão de um servidor DNS.

  Disponível em: <https://github.com/kirei/fpdns>.

- NMAP

  O NMAP é uma ferramenta de exploração de rede e segurança que também realiza *scanner* de portas, no presente trabalho o NMAP foi utilizado para verificar a versão do servidor DNS. A ferramenta está disponível em: <https://nmap.org>.

- TELNET

  O TELNET é um protocolo que permite simular um terminal a distância, na etapa de desenvolvimento o comando foi utilizado para realizar conexões a porta 53 dos servidores DNS.

4.3 DNS reais

Etapa destinada a criação da base dados contendo servidores DNS em execução, para atingir tal objetivo foi realizado a criação de um *scanner* na linguagem Python.

O *scanner* possui a função de receber uma determinada faixa de IP escolhida aleatoriamente contendo apenas os dois primeiros campos preenchidos, gerar uma lista válida de IPs e consultar cada valor verificando se o endereço contém a porta 53 que por padrão é destinada para DNS).

Para tal verificação foi utilizado o comando telnet na forma: "telnet IP 53", ao receber que a conexão foi realizada com sucesso o endereço IP é salvo em uma lista chamada dnsencontrados.txt.

Após essa etapa concluída foi necessário determinar quais versões estavam em execução nos IPs encontrados, foram os utilizados os comandos "fpdns IP"e "nmap -sV -p 53 IP".

Estes IPs juntamente com suas versões formam a base de dados de DNS reais que serão utilizados no algoritmo como um dos passos para determinar a autenticidade de um servidor. A tabela 1 mostra uma parcela dos servidores encontrados.

Tabela 1 – Versões DNS reais

Servidor	Versão
200.155.001.002	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.001.022	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.001.200	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.001.201	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.001.227	NLnetLabs NSD 1.0 alpha (uncertain)
200.155.003.154	Microsoft DNS
200.155.006.044	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.006.056	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.226	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.233	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.235	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.237	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.241	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.242	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.243	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.247	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.249	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.007.250	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.012.022	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.012.178	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.012.179	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.016.140	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.017.010	ISC BIND 9.2.3rc1 – 9.6.1-P1
200.155.017.011	ISC BIND 9.2.3rc1 – 9.6.1-P1

4.4 DNS falsos

Existem atualmente vários *scripts* em diferentes linguagens que executam serviços DNS e que permitem alterações durante sua execução pra realizar desde a tradução de nomes ao redirecionamento de sites.Essa etapa teve como objetivo realizar a busca e execução desses *scripts*.

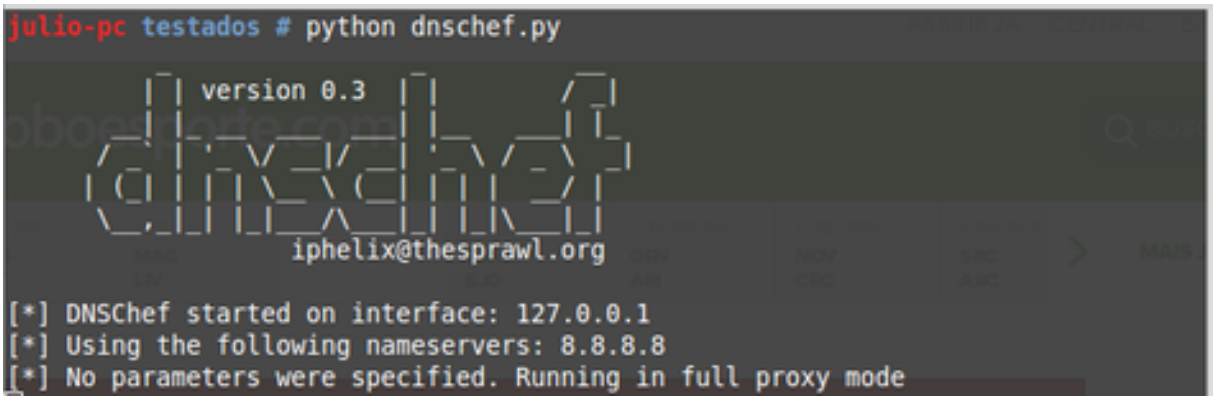
Os *scripts* escolhidos estão na linguagem Python, e podem ser encontrados em uma simples busca online. Após a execução dos *scripts* foi decidido que o DNSCHEF será utilizado nas próximas etapas.

4.4.1 DNSCHEF

DNSCHEF é um Proxy DNS altamente configurável para testes de penetração e análise de *malware*. Pode ser utilizado para forjar pedidos de determinado site para apontar para uma máquina local com o intuito de encerramento ou interceptação em vez de um *host* real solicitado pelo usuário.(DNSCHEF, 2017)

A figura 6 demonstra a execução inicial do DNSCHEF sem nenhum parâmetro adicional inserido.

Figura 6 – Execução DNSCHEF



Sem parâmetros adicionais todas as requisições serão encaminhadas para um servidor DNS acima que por padrão é 8.8.8.8.

4.5 Configuração do DNS para redirecionamento de sites

Nessa etapa o objetivo a ser atingido foi redirecionar as solicitações do usuários a determinados sites para outras páginas web. Dessa forma, dois tipos de redirecionamentos foram realizados:

(i) Redirecionar solicitação do usuário para outra páginas web:

(ii) Redirecionamento para página falsa criada

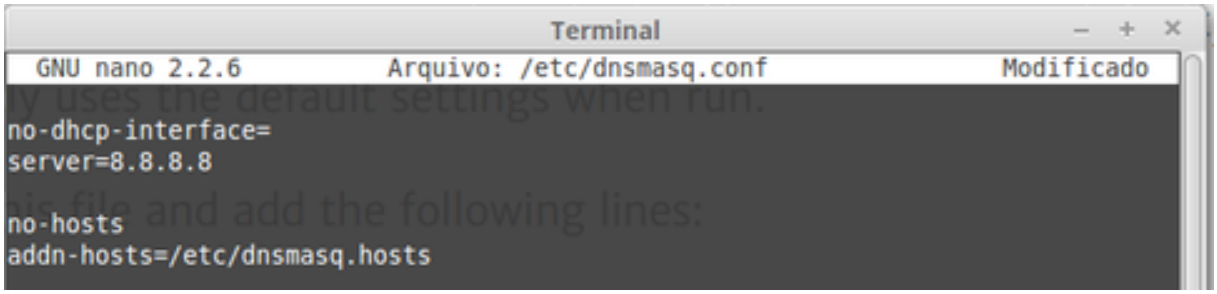
4.5.1 Configurando DNSMASQ

A execução foi realizada no Linux Mint 17.2, distribuição onde o DNSMASQ já vem instalado, para se realizar a configuração para o redirecionamento foi necessário seguir os seguintes passos:

1. Configurar DNSMASQ

Ao iniciar sua execução o DNSMASQ lê automaticamente o seu arquivo de configuração, sendo assim o primeiro passo deve ser criar ou modificar adicionando as seguintes linhas, conforme figura 7.

Figura 7 – Primeiro passo configurar DNSMASQ

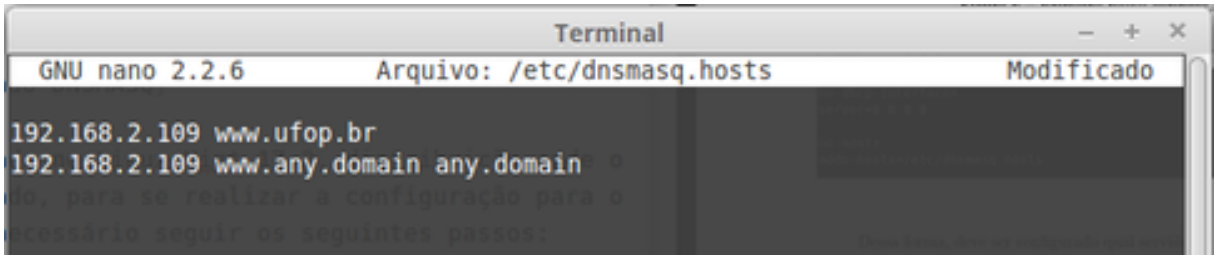


Dessa forma, deve ser configurado qual servidor DNS será responsável por responder as consultas que não forem atendidas pelo DNSMASQ, informar o caminho de onde as entradas de respostas que se deseja redirecionar se encontram.

2. Criar arquivo de respostas

Arquivo contém todas as entradas e respectivas respostas pelo qual o DNSMASQ é responsável por responder, deve se seguir o padrão de cada entrada em uma linha onde separado por um espaço é informado o endereço IP e o/os domínios correspondentes, conforme figura 8.

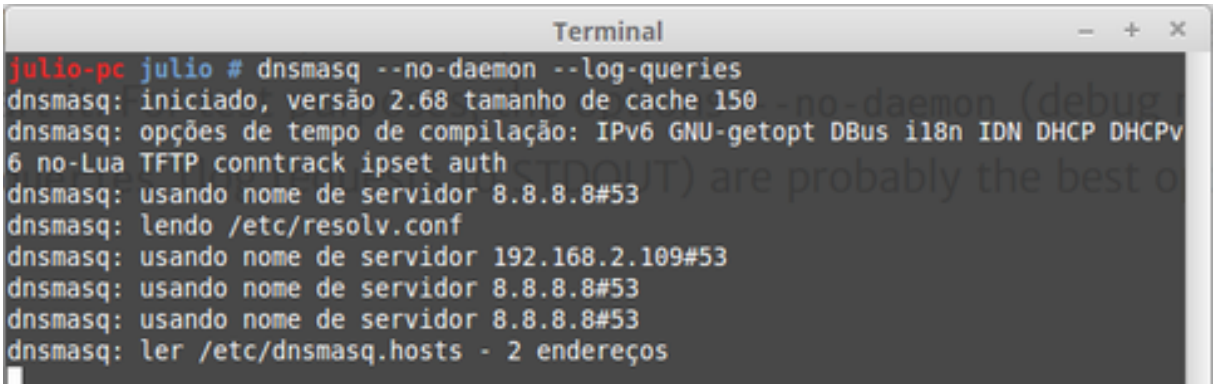
Figura 8 – Segundo passo configurar DNSMASQ



3. Executar

Após realizar a configuração adequada do DNSMASQ é realizado a execução, um exemplo de comando para execução é "dnsmasq –log-queries". Desse modo, o DNSMASQ será iniciado utilizando as configurações realizadas e logs serão gerados e cada requisição realizada poderá ser acompanhada, execução exemplifica na figura 9.

Figura 9 – Execução DNSMASQ, habilitada opção de ver logs na tela



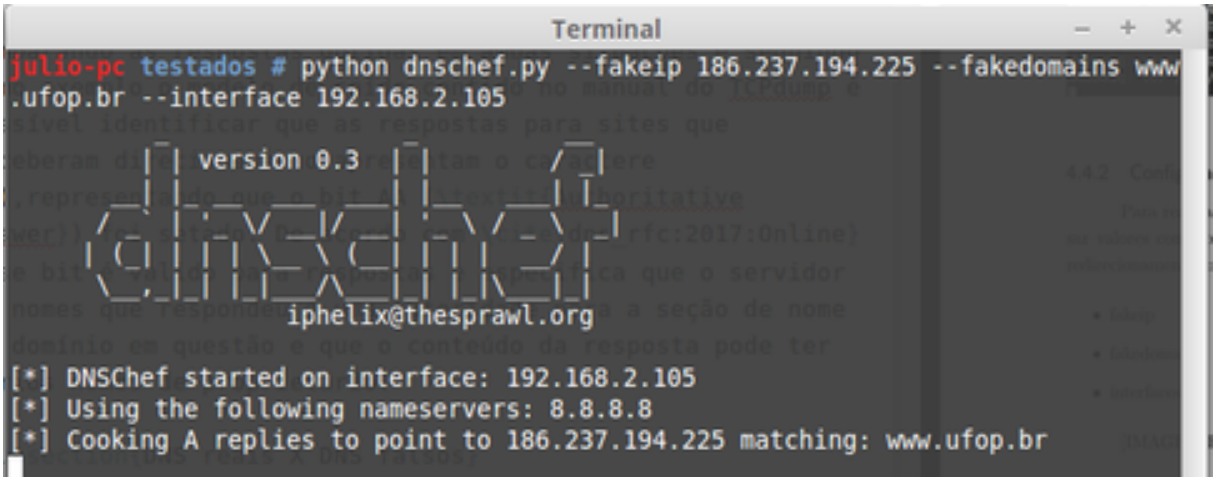
4.5.2 Configurando DNSCHEF

Para realizar a configuração do DNSCHEF basta no momento da execução passar valores como parâmetros, o DNSCHEF possui várias opções, mas para realizar o redirecionamento foi utilizado:

- fakeip
- fakedomain
- interfaces

A execução do DNSCHEF utilizando os parâmetros descritos acima pode ser verificada na figura 10.

Figura 10 – Execução DNSCHEF



4.6 Acompanhar o tráfego com TCPdump

Após o servidor DNS estar configurado e em funcionamento, foi realizado o acompanhamento das solicitações feitas e respondidas,para esse fim foi utilizado TCPdump.

De acordo com (TCPDUMP, 2017) o formato de saída padrão do TCPdump para requisições e respostas para nome de serviços em pacotes UDP é:

src > dst: id op? flags qtype qclass name (len)

src > dst: id op rcode flags a/n/au type class data (len)

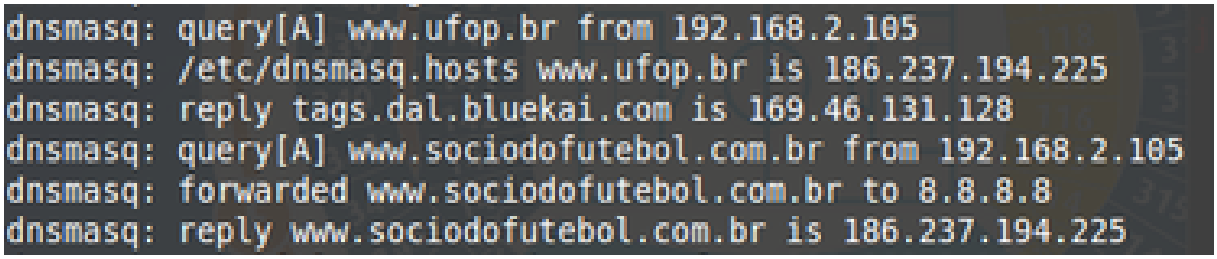
O comando utilizado para iniciar o tcpdump foi "tcpdump -vvv -i wlan0 udp port 53", o resultado obtido foi salvo em arquivos para posterior análise.

As figuras 11,12,13,14 mostram uma parcela dos arquivos de saída, nessas figuras é possível identificar os passos necessários para a resolução de nomes e quando o redirecionamento ocorre.

Duas situações foram realizadas:

1. Cliente e servidor DNS são a mesma máquina.

Figura 11 – Log de execução DNSMASQ



Analisando o tráfego é possível verificar que ao receber as consultas o tanto DNSMASQ e DNSCHEF verifica as configurações definidas, caso a resposta esteja contida o endereço IP é retornado, caso não esteja a solicitação é encaminhado ao servidor DNS.

2. Cliente e servidor DNS em máquinas distintas.

Figura 12 – Log de execução DNSMASQ no servidor

```
00:00:05.326856 IP 192.168.2.117.55997 > 192.168.2.106.domain: 23473+ A? www.ufop.br. (29)
00:00:00.000045 IP 192.168.2.117.55997 > 192.168.2.106.domain: 10358+ AAAA? www.ufop.br. (29)
00:00:00.000008 IP 192.168.2.117.37048 > 192.168.2.106.domain: 54648+ A? www.ufop.br. (29)
00:00:00.000237 IP 192.168.2.106.domain > 192.168.2.117.55997: 23473* 1/0/0 A 186.237.194.225 (45)
00:00:00.000202 IP 192.168.2.106.51896 > google-public-dns-a.google.com.domain: 15738+ AAAA? www.ufop.br. (29)
00:00:00.000358 IP 192.168.2.106.domain > 192.168.2.117.37048: 54648* 1/0/0 A 186.237.194.225 (45)
```

Figura 13 – Log de execução DNSMASQ no cliente

```
00:00:05.312912 IP 192.168.2.117.55997 > 192.168.2.106.domain: 23473+ A? www.ufop.br. (29)
00:00:00.000034 IP 192.168.2.117.55997 > 192.168.2.106.domain: 10358+ AAAA? www.ufop.br. (29)
00:00:00.001174 IP 192.168.2.117.37048 > 192.168.2.106.domain: 54648+ A? www.ufop.br. (29)
00:00:00.012374 IP 192.168.2.106.domain > 192.168.2.117.55997: 23473* 1/0/0 A 186.237.194.225 (45)
00:00:00.000545 IP 192.168.2.106.domain > 192.168.2.117.37048: 54648* 1/0/0 A 186.237.194.225 (45)
00:00:00.243695 IP 192.168.2.106.domain > 192.168.2.117.55997: 10358 1/1/0 CNAME paralamas.ufop.br. (107)
```

Figura 14 – Log de execução DNSCHEF no servidor

```
00:00:05.159745 IP 192.168.2.117.41291 > 192.168.2.106.domain: 19320+ A? www.ufop.br. (29)
00:00:00.000044 IP 192.168.2.117.41291 > 192.168.2.106.domain: 34668+ AAAA? www.ufop.br. (29)
00:00:00.001210 IP 192.168.2.117.58524 > 192.168.2.106.domain: 63937+ A? www.ufop.br. (29)
00:00:00.000404 IP 192.168.2.106.domain > 192.168.2.117.41291: 19320* 1/0/0 A 186.237.194.225 (45)
00:00:00.002173 IP 192.168.2.106.domain > 192.168.2.117.58524: 63937* 1/0/0 A 186.237.194.225 (45)
00:00:00.000136 IP 192.168.2.106.59572 > google-public-dns-a.google.com.domain: 34668+ AAAA? www.ufop.br. (29)
```

Figura 15 – Log de execução DNSCHEF no cliente

```
00:00:05.157733 IP 192.168.2.117.41291 > 192.168.2.106.domain: 19320+ A? www.ufop.br. (29)
00:00:00.000033 IP 192.168.2.117.41291 > 192.168.2.106.domain: 34668+ AAAA? www.ufop.br. (29)
00:00:00.001478 IP 192.168.2.117.58524 > 192.168.2.106.domain: 63937+ A? www.ufop.br. (29)
00:00:00.001527 IP 192.168.2.106.domain > 192.168.2.117.41291: 19320* 1/0/0 A 186.237.194.225 (45)
00:00:00.002132 IP 192.168.2.106.domain > 192.168.2.117.58524: 63937* 1/0/0 A 186.237.194.225 (45)
00:00:00.131640 IP 192.168.2.117.50554 > 192.168.2.106.domain: 31331+ A? www.sociodofutebol.com.br. (43)
```

O redirecionamento é realizado quando o usuário solicita acesso a página web www.ufop.br (200.139.128.55) e o mesmo é redirecionado para www.sociodofutebol.com.br (186.237.194.225)

Comparando as respostas obtidas em ambas situações e seguindo como exemplo o modelo de saída contido no manual do TCPdump é possível identificar que as respostas para sites que receberam direcionamento apresentam o caractere (*), representando que o bit AA (*Authoritative Answer*) foi setado. De acordo com (RFC1035, 2017) esse bit é valido para respostas e especifica que o servidor de nomes que respondeu é uma autoridade para a seção de nome de domínio em questão e que o conteúdo da resposta pode ter vários nomes de proprietário.

4.7 Criação do algoritmo

Com o intuito de identificar as principais diferenças entre a base de dados de DNS reais e os *scripts* falsos em execução, foram utilizados comandos para obter informações como portas abertas e versão do DNS encontrada. Os comandos utilizados foram TELNET, NMAP e FPDNS.

A partir da análise dos resultados obtidos, foi possível identificar as seguintes diferenças:

- Porta 53
- Versão DNS

Dessa forma, o algoritmo desenvolvido se encontra na linguagem Python e aborda essas diferenças para determinar a autenticidade do servidor DNS.

Inicialmente é verificado se a porta 53 encontra-se aberta para o servidor que se deseja consultar, essa verificação é importante pois, ao analisar a base de dados em

comparação aos DNS falsos foi constatado que durante a sua execução os *scripts* não mantinha a porta 53 aberta.

Após a verificação da porta, é realizada uma consulta para verificar se a versão do DNS encontrada está presente na lista de servidores confiáveis, que inicialmente é composta por GOOGLE DNS, OPENDNS, BIND. Uma segunda lista denominada de falsos foi criada, essa lista recebe o servidor que ao passar pelos testes teve sua autenticidade negada.

Os passos realizados pelo algoritmo são:

1. Usuário insere endereço IP para consulta.
2. Verificação se o valor inserido é válido.
3. Consulta se a porta 53 encontra-se aberta.
4. Verifica a versão do servidor DNS.
5. Compara se a versão encontrada do servidor DNS encontrada está presente no registro de versões confiáveis.
6. Retorna o resultado das consultas realizadas e da comparação de versões ao usuário.
7. A partir da resposta obtida nas etapas anteriores o servidor DNS é classificado como falso ou verdadeiro e o seu valor é armazenado no respectivo arquivo.

4.8 Página Web

Criação de uma página Web responsável por realizar consultas no servidor DNS especificado pelo usuário, as seguintes consultas podem ser realizadas:

- Consulta a porta 53: Verifica se a porta 53 está aberta no servidor DNS inserido pelo usuário.
- Consultar versão: Consultar a versão do servidor DNS inserido pelo usuário.
- Testar site: Usuário insere um site que deseja consultar a resposta obtida a partir do DNS inserido, essa resposta será então comparada a resposta obtida em outros servidores DNS conhecidos como Google e openDNS.

As figuras 16 e 17 mostram a página web em funcionamento, sendo a tela inicial responsável por receber o IP e exibir as opções que serão escolhidas pelo usuário, e a tela de respostas pela exibição da consulta feita ao IP inserido.

Figura 16 – Tela inicial site

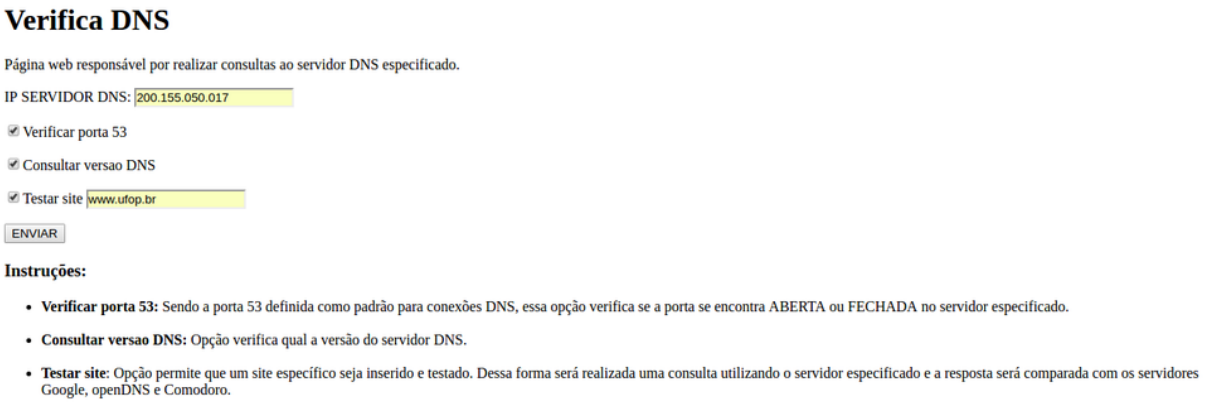
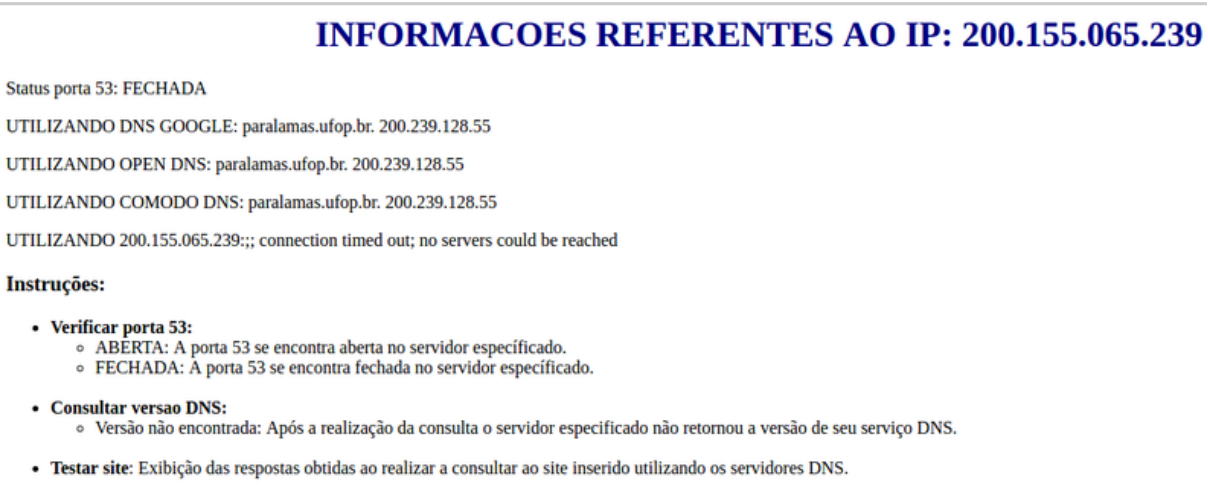


Figura 17 – Tela de respostas



O endereço da página web é: <www.verificadns.com.br>.

4.9 Extensão navegador Google Chrome

Concepção de uma extensão para o navegador Google Chrome responsável por realizar consulta em tempo real para o site que o usuário está acessando naquele momento e comparar a resposta obtida com DNS conhecidos.

Ao clicar na extensão os seguintes passos são realizados.

1. Usuário insere o servidor DNS que deseja consultar.
2. A URL da página *web* que está sendo acessada naquele momento é armazenada.
3. Resolução da URL em seu endereço IP correspondente utilizando o servidor DNS especificado pelo usuário.

4. Comparação da resposta obtida na etapa anterior com a resolução feita por servidores conhecidos: Google DNS e OpenDNS.

   Duas respostas possíveis são obtidas após a execução da extensão:

- OK: O resultado de todas as consultas realizadas é o mesmo.
- Verificar DNS: O servidor especificado apresentou resposta diferente para a página *web* inserida.

  O download da extensão pode ser realizado em: <www.verificadns.com.br>.

5 Conclusão e Trabalhos Futuros

Devido a sua importância para facilitar o acesso aos sites disponíveis na Internet o DNS segue sendo um alvo para invasores que desejam obter alguma vantagem para agir de forma fraudulenta, sendo assim é necessário garantir a sua segurança.

O presente trabalho demonstrou tipos de ataques onde o DNS pode ser alvo e possíveis consequências ao usuário como perda de informações pessoais ou bancárias.

O algoritimo desenvolvido no presente trabalho tem como objetivo identificar a autenticidade de um servidor DNS, como contribuições do trabalho há o desenvolvimento de uma página web e de uma extensão para o navegador Google Chrome onde o usuário poderá realizar consultas para obter mais informações sobre o servidor DNS.

Trabalhos futuros incluem aprofundamento nos resultados obtidos ao capturar o trafego utilizando o TCPdump, afim de identificar diferenças na resolução de nomes no cliente e no servidor e a disponibilização do algorítimo para ser executado diretamente em dispositivos de rede como roteadores.

Referências

CARLI, F. Security issues with dns. *Retrieved October*, v. 3, p. 2005, 2003. Citado 5 vezes nas páginas 17, 21, 22, 25 e 29.

CERT.BR. Cartilha de segurança para internet. 2012. Citado 3 vezes nas páginas 17, 24 e 25.

DECCIO, C. et al. Quality of name resolution in the domain name system. In: *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*. [S.l.: s.n.], 2009. p. 113–122. ISSN 1092-1648. Citado na página 21.

DNSCHEF. 2017. Disponível em: <http://thesprawl.org/projects/dnschef/>. Citado na página 34.

EC-COUNCIL. *Computer Forensics: Investigating Network Intrusions and Cyber Crime*. [S.l.]: Nelson Education, 2009. Citado na página 17.

GUO, F.; CHEN, J.; CHIUEH, T. cker. Spoof detection for preventing dos attacks against dns servers. In: *26th IEEE International Conference on Distributed Computing Systems (ICDCS'06)*. [S.l.: s.n.], 2006. p. 37–37. ISSN 1063-6927. Citado na página 21.

JALALZAI, M.; SHAHID, W.; IQBAL, M. Dns security challenges and best practices to deploy secure dns with digital signatures. In: IEEE. *Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on*. [S.l.], 2015. p. 280–285. Citado na página 29.

JANBEGLOU, M.; ZAMANI, M.; IBRAHIM, S. Redirecting network traffic toward a fake dns server on a lan. In: *3rd IEEE International Conference on Computer Science and Information Technology*. [S.l.: s.n.], 2010. p. 429–433. Citado na página 25.

KARLOF, C. et al. Dynamic pharming attacks and locked same-origin policies for web browsers. In: ACM. *Proceedings of the 14th ACM conference on Computer and communications security*. [S.l.], 2007. p. 58–71. Citado 2 vezes nas páginas 17 e 24.

LU, Z.; LIU, J. Design and implementation of dynamic domain name system based on bind. In: IEEE. *Computer Network and Multimedia Technology, 2009. CNMT 2009. International Symposium on*. [S.l.], 2009. p. 1–4. Citado na página 21.

NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de redes em ambientes cooperativos*. [S.l.]: Novatec Editora, 2007. Citado na página 24.

NICOMETTE, V. et al. Set-up and deployment of a high-interaction honeypot: experiment and lessons learned. *Journal in Computer Virology*, v. 7, n. 2, p. 143–157, 2011. ISSN 1772-9904. Disponível em: <http://dx.doi.org/10.1007/s11416-010-0144-2>. Citado 2 vezes nas páginas 29 e 31.

OLLMANN, G. *The pharming guide: Understanding & preventing DNS-related attacks by phishers, Aug 2005*. 2005. Citado 2 vezes nas páginas 26 e 27.

RACKI, C. Dns cache poisoning. 2008. Citado na página 26.

RFC1035. 2017. Disponível em: <https://www.ietf.org/rfc/rfc1035.txt>. Citado na página 38.

SAINI, H.; RAO, Y. S.; PANDA, T. Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, v. 2, n. 2, p. 202–209, 2012. Citado na página 24.

SAX, D. Dns spoofing (malicious cache poisoning). *URL: http://www. sans. org/rr/firewall/DNS_spoof. php November*, v. 12, 2000. Citado na página 25.

SEIFERT, C. et al. Honeyc-the low-interaction client honeypot. *Proceedings of the 2007 NZCSRCS, Waikato University, Hamilton, New Zealand*, Citeseer, p. 1–8, 2007. Citado na página 31.

SPITZNER, L. *Honeypots: tracking hackers*. [S.l.]: Addison-Wesley Reading, 2003. v. 1. Citado na página 31.

STAMM, S.; RAMZAN, Z.; JAKOBSSON, M. Drive-by pharming. In: SPRINGER. *International Conference on Information and Communications Security*. [S.l.], 2007. p. 495–506. Citado na página 28.

TANENBAUM, A. S. et al. Computer networks, 4-th edition. *ed: Prentice Hall*, 2003. Citado na página 22.

TANENBAUM, A. S.; WETHERALL, D. J.; ELIZONDO, A. V. R. *Redes de computadoras*. [S.l.]: Pearson Educación, 2012. Citado na página 17.

TCPDUMP. 2017. Disponível em: <http://www.tcpdump.org/tcpdump_man.html>. Citado na página 37.