UNIVERSIDADE FEDERAL DO MARANHÃO

Programa de Pós-Graduação em Ciência da Computação

Robson Everton Sousa

Uma Abordagem para Identificação e Análise Forense de Ataques DNS

São Luís
2023

Robson Everton Sousa

Uma Abordagem para Identificação e Análise Forense de Ataques DNS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciência da Computação, ao Programa de Pós-Graduação em Ciência da Computação, da Universidade Federal do Maranhão.

Programa de Pós-Graduação em Ciência da Computação

Universidade Federal do Maranhão

Orientador: Prof. Dr. Samyr Beliche Vale

São Luís - MA

2023

Ficha gerada por meio do SIGAA/Biblioteca com dados fornecidos pelo(a) autor(a).
Diretoria Integrada de Bibliotecas/UFMA

Everton Sousa, Robson.
Uma Abordagem para Identificação e Análise Forense de Ataques DNS / Robson Everton Sousa. - 2023.
87 p.

Orientador(a): Samyr Beliche Vale.
Dissertação (Mestrado) - Programa de Pós-graduação em Ciência da Computação/ccet, Universidade Federal do Maranhão, São Luís, 2023.

1. Computação forense. 2. Crimes informáticos. 3. Redes de computadores. I. Beliche Vale, Samyr. II. Título.

Robson Everton Sousa

Uma Abordagem para Identificação e Análise Forense de Ataques DNS

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Ciência da Computação, ao Programa de Pós-Graduação em Ciência da Computação, da Universidade Federal do Maranhão.

Dissertação
São Luís - MA,25 de Agosto de 2023.

Prof. Dr. Samyr Beliche Vale
Orientador
Universidade Federal do Maranhão

Prof. Dr. Francisco José da Silva e Silva
Avaliador Interno
Universidade Federal do Maranhão

Prof. Dr. Vinicius Ponte Machado
Avaliador Externo
Universidade Federal do Piauí

São Luís - MA
2023

Gostaria de expressar minha gratidão a todos que contribuíram para que esse resultado fosse possível. Agradeço aos meus pais, irmãos, esposa, filha, amigos e aos meus professores. Seu apoio e incentivo foram fundamentais ao longo dessa jornada.

Agradecimentos

Primeiramente agradeço a Deus pela realização pessoal e pela oportunidade de aprendizado e realização profissional.

Agradeço aos meus pais, João e Maria, pelo amor, dedicação e educação, meus, muito obrigado.

Agradeço a minha esposa, Santana, e à minha querida filha, Cecília, por seu apoio, alegrias e motivação ao longo dessa jornada.

Ao meu orientador Prof. Dr. Samyr Béliche Vale, pela paciência, apoio, incentivo e confiança durante essa jornada. Agradeço imensamente pela oportunidade de aprendizado e pela sua valiosa contribuição.

E, por fim, gostaria de agradecer à Universidade Federal do Maranhão (UFMA) e aos docentes, especialmente aos professores do PPGCC, que compartilharam seus conhecimentos comigo. Também sou grato ao corpo técnico da UFMA, em particular à equipe da Superintendência de Tecnologia da Informação (STI), que, juntamente com a administração superior, indicou e disponibilizou solução tecnológica para que o curso pudesse ocorrer durante a pandemia da COVID-19. Agradeço a todos que estiveram envolvidos direta ou indiretamente nesta formação. Muito obrigado a todos.

"Maior que a tristeza de não haver vencido
é a vergonha de não ter lutado."
(Rui Barbosa)

Resumo

Os Servidores de Resolução de Nomes de Domínios (DNS) realizam uma função fundamental no estabelecimento do acesso a páginas web. Em virtude de sua importância, são alvos constantes de ataques cibernéticos, os quais visam apagar ou substituir alguns dos seus registros, causando enormes prejuízos para usuários, empresas e instituições pelo mundo. No que tange ao cenário brasileiro, para inibir esses tipos de ataques, vige um dispositivo legal que tipifica penalmente a invasão de dispositivos informáticos conectados à rede mundial de computadores, o que inclui os ataques ao serviço de DNS. Apesar da previsão legal, a identificação dos ataques cibernéticos constitui-se uma difícil tarefa, haja vista depender da correta aplicação de meios de proteção e monitoramento dos serviços de rede, bem como da extração e interpretação de dados que permitem a identificação dos elementos constituintes do fato delituoso. Nessa perspectiva, o presente trabalho propõe uma abordagem computacional forense para identificar automaticamente a ocorrência de ataque do tipo DNS CachePoisoning, fazendo a subsunção dos elementos que constituem o ataque ao dispositivo legal, a fim de identificar a ocorrência de um crime.

Palavras-chave:Computação forense; Crimes informáticos; Redes de computadores.

Abstract

Domain name resolution servers (DNS) perform a key function in establishing access to web pages. Because of their importance, they are constant targets for cyber-attacks, which aim to erase or replace some of their records, causing huge losses for users, companies and institutions worldwide. In Brazil, to prevent such attacks, a legal provision is established that criminally typifies the invasion of computer devices connected to the World Wide Web, which includes attacks on the DNS service. Still, cyber-attack identification is difficult as it depends on the correct application of means of protection, monitoring of network services and extraction and interpretation of data that allow the identification of criminal factors. The present work proposes a computational forensics approach to automatically detect the occurrence of a DNS cache poisoning attack, subsuming the elements that constitute the attack to the legal device, thus identifying the occurrence of a crime.

Keywords: Computer forensics; Computer crimes; Computer networks.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

DDoS: Distributed Denial of Service - Negação de Serviço Distribuído

DNS: Domain Name Server - Servidor de Domínio

DNSSEC: Domain Name System Security Extensions - Extensões de Segurança do Sistema de Nomes de Domínio

DMZ: Demilitarized Zone - Área Desmilitarizada

FQDN: Fully Qualified Domain Name - Nome de Domínio Totalmente Qualificado

Firewall: Firewall - Parede de Fogo

ICANN: Internet Corporation for Assigned Names and Numbers - Corporação da Internet para Atribuição de Nomes e Números

IDS: Intrusion Detection System - Sistema de Detecção de Intrusões

IANA: Internet Assigned Numbers Authority - Autoridade para Atribuição de Números da Internet

ID: Identification - Identificação

IP: Internet Protocol - Protocolo de Internet

IoT: Internet of Things - Internet das Coisas

LAN: Local Area Network - Rede de Área Local

OSI: Open Systems Interconnection - Interconexão de Sistemas Abertos

PCAP: Packet Capture - Captura de Pacotes

SIEM: Security Information and Event Management - Gerenciamento de Informações e Eventos de Segurança

SLD: Second-Level Domain - Domínio de Segundo Nível

TCP: Transmission Control Protocol - Protocolo de Controle de Transmissão

TCP/IP: Transmission Control Protocol/Internet Protocol - Protocolo de Controle de Transmissão/Protocolo de Internet

TLD: Top-Level Domain - Domínio de Nível Superior

TTL: Time to Live - Tempo de Vida

UDP: User Datagram Protocol - Protocolo de Datagrama de Usuário

WAN: Wide Area Network - Rede de Área Ampla

Sumário

1 Introdução

As redes de computadores são um conjunto de redes conectadas que permitem a comunicação e compartilhamento de recursos entre dispositivos, desde pessoas físicas até grandes corporações. Essa tecnologia tem transposto fronteiras e permitido que diferentes indivíduos mantenham e construam novos relacionamentos. Além disso, destacam-se as possibilidades e a criação de novas tecnologias e inovações, as quais impulsionam o desenvolvimento de diversos setores da economia mundial. No entanto, essas facilidades trazem consigo perigos, como a ameaça de criminosos que buscam capturar informações pessoais e institucionais. É fundamental, portanto, investir em segurança da informação e modernizar o sistema judicial dos países, para encontrar soluções e compensar danos causados por violações de direitos por meio da tecnologia. Em resumo, as redes de computadores são essenciais para a vida das pessoas, mas é necessário estar atento aos riscos e agir para proteger os direitos individuais e coletivos.

O suporte para o desempenho da rede é composto por um conjunto de tecnologias-padrão, protocolos de segurança e comunicação criados para fins específicos, mas que se tornaram alvo de escaladas criminosas. Dentre essa estrutura da internet, pode-se listar o padrão teórico, o modelo OSI e o padrão implementado TCP/IP. Essa estrutura prevê critérios de segurança para redes de computadores, porém alguns deles não foram observados, pois criminosos os viram como uma oportunidade para cometerem crimes. Contudo, em contrapartida a essa abordagem criminosa, existem os profissionais de segurança, a comunidade científica e empresas de segurança da informação que estão sempre dedicados a prover uma forma segura para que os dados sejam mantidos fora do alcance dos criminosos.

De acordo com Zhang et al. (2021), o DNS é uma das infraestruturas mais importantes da Internet e tem em seu cerne a missão de realizar o mapeamento e a convenção entre o nome de domínio e o endereço IP. Apesar de sua grande importância, o protocolo em questão apresenta pontos de fragilidade no que tange a sua segurança, pois, no início da construção do DNS, algumas questões de segurança não foram consideradas.

Conforme Houser et al. (2021), a primeira versão do DNS não considerou que este protocolo fosse suscetível a crimes cibernéticos. Com isso, ao longo dos anos, ele tem sido alvo de diversos ataques. Kim e Reeves (2020) evidenciam que esses ataques podem ser listados da seguinte forma: adulteração de dados DNS, inundação de dados DNS, abuso de DNS e estrutura do servidor DNS.

Os serviços suportados pelo DNS contemplam entidades públicas e privadas, como órgãos do governo e instituições financeiras. Esse vasto uso do protocolo em questão chama

a atenção dos cibercriminosos que invadem sistemas institucionais. “Em 31 de março de 2012, o Anonymuos tentou deixar toda a internet off-line com a Operação Blackout. O objetivo dessa operação era tirar do ar os 13 servidores-raiz usando um ataque de Amplificação de DNS” (LISKA; STOWE, 2016, p. 51). Essa tentativa não foi bem-sucedida em decorrência do baixo conhecimento da estrutura do DNS pelo grupo participante, pois um ataque dessa magnitude à robusta estrutura do DNS requer poderio tecnológico e um vasto conhecimento do seu funcionamento.

Conforme reportam Liska e Stowe (2016), um ataque de negação de serviço resultou em um impacto bastante significativo para o continente europeu, pois foi lançado contra os servidores ccTLD .tr — servidor de nome raiz da Turquia —, que ficou desconectado do resto do mundo por toda a internet. Esse ataque gerou um efeito colateral que degradou os serviços e deixou a Turquia isolada do resto do mundo. Em razão disso, 400 mil domínios se tornaram inacessíveis, gerando fortes consequências para a Europa, pois os servidores de nome .tr também fazem parte da cadeia de DNS da Europa.

De acordo com Haran (2020), um fato consistente é visto na mídia brasileira: quando hackers invadiram o sistema de saúde brasileiro utilizando-se do ataque DNS hijacking para induzir usuários a baixarem um APP falso sobre a Covid-19. Segundo Aquino (2021) o Ministério da saúde também sofreu ataques onde pelo menos 50 TB de dados foram parar nas mãos de cibercriminosos que utilizaram a estrutura do DNS para acessar essas informações. Grande parte desses ataques é direcionada a instituições financeiras e outros segmentos com o intuito de coletar informações sensíveis, financeiras e outras.

De acordo com os estudos de Naqash et al. (2012), durante sua construção, a arquitetura DNS não projetou os critérios de segurança necessários para evitar o recebimento de dados falsificados. Nesse contexto, Hmood et al. (2015) ressaltam que, utilizando-se dessa vulnerabilidade, um invasor pode comprometer um servidor DNS introduzindo informações forjadas no cache dos resolvedores de nome de domínio e, com isso, alteram parâmetros referenciais para deixá-lo indisponível ou desviar seu tráfego para o endereço malicioso.

O ataque a servidores DNS é tão recorrente que, segundo Alharbi et al. (2019), aproximadamente 92% das redes analisadas em suas pesquisas estão sujeitas a pelo menos um tipo de envenenamento de cache DNS. Isso foi atestado mediante avaliação de 97% dos resolvedores que operam de forma aberta; 74% das redes corporativas por meio de servidores de e-mail; e 68% dos ISPs medidos por meio de rede de anúncios.

Medidas de contenção foram desenvolvidas para superar os avanços dos ataques, uma dessas contenções foi o protocolo DNS Security Extensiong (DNSSEC), o qual implantou mecanismo de assinatura digital de criptografia de chave pública.

Conforme ressaltado por Kim e Reeves (2020), apesar das vantagens do DNSSEC, estudos comprovam que essa técnica não ganhou tanta adesão, pois apenas 31% seguem todas as etapas de validação da extensão e 39% dos domínios não usam uma chave criptográfica forte. Outro ponto bastante precário, é que 82% dos resolvedores solicitaram os registros do DNSSEC, e apenas 12% desses tentaram validar o os registros do DNSSEC.

De acordo com Vaz, Rizzetti e Filho (2021), em resposta às ameaças às redes de computadores, o mercado oferece ferramentas especializadas em proteção que têm a capacidade de capturar evidências e fornecer informações auditáveis, com o objetivo de comprovar a ocorrência de um incidente. Essas ferramentas possibilitam a visualização de informações relacionadas a acessos indevidos registrados por meio de logs — que são arquivos de texto passíveis de análise automatizada ou por profissionais de segurança de redes. Um exemplo amplamente utilizado para a detecção de intrusões em redes é o IDS (Sistema de Detecção de Intrusão).

De acordo com Cardoso (2018), essa ferramenta tem a capacidade de capturar e analisar o tráfego de dados em uma rede, seja em um computador específico ou em um protocolo específico. Sendo assim, ela pode ser utilizada como uma segunda linha de defesa, complementando o Firewall e fornecendo alertas para o gestor de rede. Os registros de logs contêm informações como a data e hora em que a mensagem de log foi gerada, bem como a identificação da origem (endereço IP ou nome da máquina) dos envolvidos no ataque.

Essas práticas dos criminosos podem ser monitoradas por ferramentas de segurança da informação que possuem a capacidade de registrar as ações dos criminosos para possível análise, pois os seus registros, ou melhor, suas impressões digitais são passíveis de investigações e, com isso, possibilitam a investigação dos casos de ataques de redes e, consequentemente, o DNS.

Considerando o supracitado, a computação forense é um importante recurso para a apuração dos crimes informáticos, visto que é capaz de reunir evidências para direcionar a polícia judiciária a apresentar evidências criminais perante os órgãos operadores do direito.

Apesar do IDS e outras ferramentas de segurança registrarem as atividades nas redes, incluindo eventuais ataques, esses registros são armazenados em arquivos de .log, atualizados dinamicamente. Normalmente, nenhum tratamento é realizado aos dados ali gerados, servindo apenas como informativo para o administrador de rede.

De acordo com análise realizada por Cantanhede e Vale (2020), os dados oriundos dos logs do IDS são capazes de apresentar evidências de atividades delituosas, mas não são de fácil compreensão, pois é necessário o auxílio de um especialista em segurança de redes para auxiliar na descoberta e interpretação desses dados.

A legislação penal brasileira, por intermédio da Lei Nº 14.155/2021, que alterou o Código Penal Brasileiro, prevê sanções para a invasão de dispositivos informáticos com a

intenção de obter, adulterar ou apagar informações ou de instalar vulnerabilidades em dispositivos informáticos conectados ou não à Internet.

Em virtude das recentes atualizações legais, não foi encontrada uma solução que auxiliasse o investigador não especialista em segurança de redes a identificar os registros de eventuais ataques armazenados nas ferramentas de segurança e monitoramento.

Essa pesquisa tem como objeto principal a identificação desses eventos ocorridos em infraestruturas de redes, bem como a captura e a interpretação dos dados que caratcterizam as ações ali praticadas pelo hacker, para — após sua análise — avaliar se houve ou não crime, de acordo com a legislação penal brasileira.

1.1 Objetivos

O objetivo deste trabalho consiste em desenvolver uma abordagem capaz de, a partir da ocorrência de ataques de invasão ao serviço de DNS, capturar os dados da invasão fornecidos pelo IDS e identificar, através de seus registros, os elementos que caracterizam o cometimento do delito, realizar a associação dos fatos ocorridos com a norma incriminadora, registrá-los em um banco de dados e gerar um relatório forense, que servirá de prova da ocorrência do fato e dos elementos que caracterizam a invasão de dispositivo informático. Ademais, será proposto o desenvolvimento de uma ferramenta que colete os dados, realize a subsunção do fato à norma e gere o relatório pericial.

1.1.1 Objetivos Específicos

Analisar os sinistros de redes contra o DNS notificados pelo sistema de detecção de intrusão com intuito de identificar a autoria, a técnica de invasão que foi utilizada, o endereço lógico de origem e destino (autor do delito), horário (tempo do crime), serviços atingidos e os danos causados. Interpretar os dados da invasão, a fim de identificar as atividades delituosas e sua extensão, nos termos da legislação brasileira em vigor, as quais podemos elencar no artigo 154-A do Código Penal brasileiro. Elaborar um documento em linguagem acessível aos operadores do direito e demais interessados em identificar o autor do fato ocorrido, as consequências geradas para as Instituições, a fim de tomarem decisões judiciais cabíveis.

1.1.2 Contribuições

Destacam-se como principais contribuições:

- A proposição de uma abordagem forense em ataques ao servidor DNS e geração de um relatório forense de forma automatizada e armazenamento das evidências do delito em uma base de dados de evidências de crimes cibernéticos.

- A construção de uma ferramenta forense que auxilia na coleta de evidências desses ataques de invasão ao servidor DNS.
- Em suma, a pesquisa contribui para o avanço do conhecimento na área de segurança da informação direcionada para a análise forense, pois fornece uma ferramenta forense especializada para investigação de crimes cibernéticos relacionados a servidores DNS. A ferramenta FORDNS, desenvolvida durante a pesquisa, contribui de forma sistemática e eficaz para a análise forense em servidores DNS, o que pode ajudar a identificar a autoria, a técnica de invasão, o endereço IP de origem e destino, horário, serviços de rede atingidos (servidores) e os danos causados em casos de ataques de DNS cache poisoning.

1.2 Organização do Trabalho

Este trabalho está estruturado da seguinte forma:

- O Capítulo 2 descreve trabalhos relacionados ao tema.
- O Capítulo 3 trata da fundamentação teórica das técnicas utilizadas.
- O Capítulo 4 apresenta as etapas adotadas durante a abordagem proposta para este trabalho.
- O Capítulo 5 trata sobre os resultados obtidos e discussões em relação aos experimentos realizados.
- O Capítulo 6 apresenta as considerações finais sobre os resultados, trabalhos futuros e o artigo científicos desenvolvido.

2 Trabalhos Relacionados

Para uma pesquisa bibliográfica bem-sucedida, Wazlawick (2020) sugere começar com o Mapeamento Sistemático da Literatura (MSL). Essa abordagem tem um escopo mais amplo e tem como objetivo compreender a pesquisa em uma determinada área, sem necessariamente responder a perguntas específicas. Geralmente, envolve uma análise mais superficial de um grande número de artigos, permitindo identificar tendências, lacunas e áreas de foco na pesquisa dentro daquela área. Após realizar o MSL e obter uma visão geral, é recomendável prosseguir com a Revisão Sistemática da Literatura (RSL), que envolve a análise detalhada de um conjunto significativo de artigos primários para responder a perguntas de pesquisa específicas. Essa sequência auxilia na estruturação eficaz da pesquisa, começando com uma ampla compreensão da área antes de se aprofundar em tópicos específicos.

Esta pesquisa envolveu uma abordagem sistemática para identificar e selecionar os trabalhos relacionados que fornecem uma base para a compreensão do contexto no qual este estudo se insere. Isso incluiu a Identificação da Base de Dados, seleção de estudos relevantes, análise e categorização, bem como a identificação de relações e lacunas.

- **Identificação da Base de Dados:** Iniciou-se a pesquisa consultando diversas bases de dados acadêmicas, como Scopus, IEEE Xplore e Google Scholar, entre outras conforme tabela 1. Utilizou-se termos de busca específicos relacionados à segurança cibernética, ataques ao servidor DNS, análise forense e aspectos legais. Os termos de busca incluíram palavras-chave como "ataques de DNS,forensic analysis,"ferramentas de segurança de redes e outras variações relevantes. Além da consulta a essas bases de dados, foram consultados livros físicos e digitais, bem como o repositório de dissertações da UFMA.

- **Seleção de Estudos Relevantes:** Após a busca inicial, realizou-se uma análise dos títulos e resumos de cada trabalho, com o objetivo de identificar sua pertinência em relação ao tema desta pesquisa. Foram selecionados os estudos que se relacionavam com o escopo da pesquisa.

- **Análise e Categorização:** Uma vez identificados os estudos relevantes, procedeu-se a uma análise dos trabalhos com o propósito de identificar suas contribuições específicas. Os trabalhos foram categorizados em áreas como ataque ao servidor DNS, passando para ataques de DNS cache poisoning, análise forense em dispositivos computacionais, redes de computadores, considerações legais relacionadas à legislação de crimes informáticos, aspectos de segurança em redes de computadores e a avaliação

das principais ferramentas disponíveis. Em uma etapa subsequente, realizou-se uma pesquisa específica sobre as ferramentas de detecção de intrusão.

- **Identificação de Relações e Lacunas:** Após categorizar os trabalhos, foram analisadas suas relações e lacunas, identificando como cada estudo se conecta aos outros e onde existem espaços em branco na literatura. Essa análise permitiu traçar um panorama das pesquisas relacionadas e entender onde a pesquisa desenvolvida nesta dissertação se encaixa.

Tabela 1 – Algumas das Principais Fontes de Pesquisas

Fonte de Informação	**Endereço Online**	**Tipo de Base**
Google Scholar	scholar.google.com	Motor de Busca
IEE Xplore	ieeexplore.ieee.org	Base Bibliográfica
ACM Digital Library	dl.acm.org	Base Híbrida
Springer Link	link.springer.com	Base Bibliográfica
Scopus	www.scopus.com	Motor de Busca
Wiley Online Library	onlinelibrary.wiley.com	Base Híbrida

Fonte: Adaptada de (WAZLAWICK, 2020)

2.1 Trabalhos Relacionados e Lacunas

Antes de listar os trabalhos relacionados, vale a pena ressaltar que ao longo dessa pesquisa foram consultados diversos trabalhos, mas resolveu-se listar nesta seção alguns dos trabalhos que serviram como referência para a estruturação da pesquisa.

1. No contexto complexo da segurança cibernética, a detecção do sequestro de DNS apresenta desafios significativos. Houser et al. (2021) abordam esses desafios em duas vertentes e utilizam relatórios de DNS passivo para identificar características de ataques conhecidos, Kim e Reeves (2020) fornecem uma visão geral das vulnerabilidades e ataques ao DNS, além de orientarem sobre possíveis medidas de mitigação.

   Embora esses estudos forneçam uma análise detalhada dos impactos negativos associados ao DNS, é importante ressaltar que a legislação penal é um aspecto crucial a ser considerado. Nesse sentido, este trabalho orienta enquadrar os crimes relacionados ao sequestro de DNS na Lei de Crimes Informáticos (Lei 12.737/2012) no Brasil. É relevante destacar que o artigo 154-A do Código Penal brasileiro foi introduzido por essa lei e posteriormente passou por modificações significativas com a aprovação da Lei 14.155/2021. Essas alterações abrangem crimes como invasão de dispositivos informáticos, estabelecendo penas mais duras para os infratores.

2. A pesquisa realizada por Studiawan, Sohel e Payne (2019) destaca que os eventos registrados e armazenados em arquivos de sistemas, ou seja, os logs são provas

aproveitáveis para comprovação de um crime e, dessa forma, a sua validade se torna aceitável para o judiciário. Esse trabalho vasculha e analisa diversas pesquisas da área forense. O artigo faz uma busca de análise forense em que diversas metodologias foram analisadas e comparadas e cujos autores mencionam desde um framework genérico à necessidade de criação de um framework específico. Algo a ressaltar nesta pesquisa é sobre a forte campanha feita sobre a validade dos logs para análise forense. Apesar dessa orientação sobre a validade dos logs e seu armazenamento seguro, não se tratou de uma análise forense com o intuito de correlacionar com um dispositivo jurídico que fosse capaz de apontar casos de invasão e armazenamento dos casos de delitos e geração de um relatório forense de fácil compreensão tanto para o judiciário quanto para as demais partes interessadas — vítimas e criminosos.

3. Zhang et al. (2021) apresentam ataques de envenenamento de cache DNS, nos quais os invasores contornam as defesas de segurança de roteadores domésticos e injetam registros de nomes de domínios falsificados. Eles demonstram que modelos populares de roteadores domésticos, como D-Link, Linksys, dnsmasq e MS DNS, têm vulnerabilidades. Durante o estudo, os autores também demonstram os ataques e suas consequências. Uma das lacunas de pesquisa deixadas neste trabalho é a falta de enquadramento penal para esses crimes. Em contrapartida, este trabalho busca enquadrar os crimes de invasão ao DNS na Lei de Crimes Informáticos.

4. Os pesquisadores Cantanhede e Vale (2020) conduziram uma análise forense em redes de computadores com o objetivo de documentar ataques de negação de serviço e enquadrá-los na Lei 12.737. O foco principal desse estudo foi o enquadramento de ataques de perturbação em sites na internet, um tipo de crime amplamente divulgado na mídia devido aos problemas que causa. Como parte desse esforço, os pesquisadores desenvolveram uma metodologia que permitia diagnosticar esses ataques e gerar relatórios em linguagem acessível, tornando o processo mais compreensível para um público amplo. Essa metodologia também incentivou o uso de um dispositivo automatizado para facilitar a detecção. No entanto, é importante notar que essa metodologia se concentrou em ataques de perturbação, deixando uma lacuna em relação aos ataques de invasão.

   Nesse sentido, o estudo deixou questões em aberto, uma vez que abordou apenas ataques de perturbação. Portanto, é relevante conduzir pesquisas que explorem outros tipos de ataques, incluindo os crimes de invasão a dispositivos informáticos. Diante dessa lacuna, surgiu a oportunidade de realizar um estudo abordando os crimes de invasão a dispositivos computacionais, com ênfase especial nos servidores DNS, com o propósito de enquadrá-los na Lei de Crimes Informáticos.

5. A pesquisa dos seguintes autores Vazao (2021) realizou um estudo comparativo de quatro soluções SIEM (Security Information and Event Management), apresentando

uma estrutura centralizada de armazenamento de logs de segurança das aplicações e dos equipamentos de rede para identificar suas vulnerabilidades.

Esses logs são armazenados e servem de insumo na busca por medidas de reparação e contenção de ameaças para preservar os registros de violação de acessos indevidos. Nesse sentido, o trabalho em questão contemplou apenas o armazenamento dos logs em um único ambiente, o qual é bastante útil, pois os dados dos delitos estão salvos em um ambiente seguro. Apesar dessa iniciativa, é notório que os pesquisadores não enquadram os crimes em um cenário de violação da lei de crimes informáticos.

A lacuna dessas pesquisas nos permite inferir que não basta apenas garantir o armazenamento dos logs, descobrir a origem do ataque e tomar medidas de contenção, mas é relevante a apuração desses crimes. Este trabalho lida com estas questões: uma abordagem forense com o objetivo de capturar as evidências e armazená-las em um banco de dados de delitos para municiar os investigadores em uma possível judicialização dos crimes.

6. CEPIDS é um IDS baseado no Processamento de Eventos Complexos para Internet das Coisas. A referida dissertação apresenta o CEPIDS, um sistema de detecção de intrusão para IoT em tempo real que usa as regras do CEP para identificar ataques que desencadeiam alertas. Cardoso (2018) retrata um cenário onde equipamentos de IoT são alvos de diversos ataques. Apesar de a metodologia desenvolvida direcionar seu objetivo em análise de intrusão em redes de computadores, pode-se observar que não se levou em consideração a questão da análise criminal, pois esses inúmeros ataques são apassivos de investigação e criminalização. Observando essa lacuna, é possível a análise forense nesses logs gerados por essa metodologia.

2.2 Tabela de Trabalhos Relacionados

A tabela 2 apresenta de forma resumida o conteúdo dos trabalhos relacionados, tornando-se uma referência para consulta sobre os principais estudos utilizados, incluindo artigos e outras pesquisas acadêmicas que orientaram este estudo. Isso proporciona ao leitor uma leitura mais rápida e eficiente sobre os tópicos abordados neste pesquisa. Portanto, de maneira dinâmica, são destacadas as principais fontes de pesquisa.

Tabela 2 – Trabalhos Relacionados

Autores	**Nome do Artigo**	**Descrição**
(HOUSER et al., 2021)	A Comprehensive Measurement-based Investigation of DNS Hijacking	Abordam desafios do sequestro de DNS e utilizam relatórios de DNS passivo para identificar características de ataques conhecidos.
(KIM; REEVES, 2020)	A survey of domain name system vulnerabilities and attacks	Este estudo provê uma análise abrangente das vulnerabilidades e ataques direcionados ao Sistema de Nomes de Domínio (DNS), além de fornecer orientações sobre possíveis estratégias de mitigação.
(ZHANG et al., 2021)	Study on the latent state of Kaminsky-style DNS cache poisoning: Modeling and empirical analysis	Apresentam ataques de envenenamento de cache DNS em roteadores domésticos, demonstrando vulnerabilidades em modelos populares.
Cantanhede e Vale (2020)	Computer Network Forensics Assistance Methodology Focused on Denial of Service Attacks	Realiza-se análise forense em redes de computadores para documentar ataques de negação de serviço e, com isso, enquadrá-los na Lei 12.737.
(VAZAO, 2021)	Implementação de sistema SIEM open-source em conformidade com o RGPD	Realiza-se um estudo comparativo de soluções SIEM para identificar vulnerabilidades em aplicações e equipamentos de rede, destacando a importância do armazenamento seguro dos logs de segurança.
(CARDOSO, 2018)	CEPIDS: Um IDS baseado no Processamento de Eventos Complexos para Internet de Coisas	Um sistema de detecção de intrusão para IoT, que pode ser utilizado na análise forense de ataques a equipamentos de IoT.
Studiawan, Sohel e Payne (2019)	A survey on forensic investigation of operating system logs	Afirma-se que os eventos registrados e armazenados em arquivos de sistemas, ou seja, os logs, são provas aproveitáveis para a comprovação de um crime, tornando sua validade aceitável para o judiciário.

2.3 Conclusão

Alguns dos trabalhos mencionados nesta pesquisa discutem conceitos relacionados a ataques em redes de computadores, incluindo ataques DNS, e estratégias para mitigá-los. Outros concentram-se na análise de ataques, registrando evidências em arquivos de logs ou em um concentrador de logs. Um dos trabalhos que se aproxima do escopo desta dissertação foi realizado por Cantanhede e Vale (2020), abordando a relação entre ataques DDoS e a legislação brasileira, embora seu foco seja em ataques de perturbação, deixando espaço para outras abordagens nesse campo de pesquisa.

Observando essas pesquisas, surgiu a oportunidade de desenvolver uma abordagem forense para ataques a servidores DNS, relacionando-a ao artigo 154-A do Código Penal brasileiro, que trata de invasão de dispositivos informáticos.

A baixa produção de trabalhos nesta área do conhecimento nos leva a apresentar poucas referências neste trabalho. Essa escassez de estudos pode ser justificada pela complexidade da interseção entre esses dois campos distintos: um versa sobre análise forense em redes de computadores, uma área técnica e especializada; enquanto o segundo versa sobre o regramento jurídico de um país, que também é bastante complexo. Apesar dessas diferenças, acredita-se que essa área de conhecimento é promissora e pode gerar diversos trabalhos no futuro.

3 Fundamentação Teórica

Em se tratando de redes de computadores, o desafio é fornecer serviços de redes de maneira segura, protegendo informações privadas, pessoais e comerciais. Manter uma rede segura significa garantir a segurança dos usuários da rede e proteger os interesses comerciais. Portanto, para manter uma rede segura, os profissionais de segurança devem estar cientes das novas ameaças e ataques a redes, além das vulnerabilidades dos dispositivos e aplicações, e mitigar as ameaças. No entanto, a segurança da rede é responsabilidade de todos. Conforme destacam Hintzbergen et al. (2018), um dos principais conceitos de segurança deve ser observado: CIA (Confidentiality, Integrity and Availability), considerado o pilar da segurança da informação, de modo que um incidente de segurança é caracterizado quando um desses princípios é afetado. De acordo com Stallings, esses princípios podem ser conceituados da seguinte forma:

> Confidencialidade: esse termo cobre dois conceitos relacionados: Confidencialidade de dados: assegura que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados. Privacidade: assegura que os indivíduos controlem ou influenciem quais informações relacionadas a eles podem ser obtidas e armazenadas, da mesma forma que como, por quem e para quem essas informações são passíveis de ser reveladas. Integridade: esse termo abrange dois conceitos relacionados: Integridade de dados: assegura que as informações e os programas sejam modificados somente de uma maneira especificada e autorizada. Integridade do sistema: assegura que um sistema execute as suas funcionalidades de forma ilesa, livre de manipulações deliberadas ou inadvertidas do sistema. Disponibilidade: assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados (STALLINGS, 2015, p.08).

Diante dessa discussão, é imperativo garantir a segurança em redes de computadores, proteger informações sensíveis e preservar a integridade dos sistemas. Para isso, é necessário que os profissionais de segurança da informação estejam atualizados sobre ameaças emergentes e vulnerabilidades nos dispositivos e aplicações. A segurança da rede é uma responsabilidade compartilhada por todos os envolvidos, e os princípios de Confidencialidade, Integridade e Disponibilidade (CIA) desempenham um papel importante na segurança da informação. Assim, resguardando-se a confidencialidade dos dados, a privacidade dos usuários, a integridade das informações e sistemas, como também a disponibilidade contínua dos serviços, é possível oferecer um ambiente seguro nas redes de computadores.

Em busca de segurança nas redes de computadores e de possibilitar uma comunicação

segura, é necessário adotar medidas efetivas de proteção. No contexto dos padrões de redes, como o modelo OSI (Open Systems Interconnection) e o TCP/IP (Transmission Control Protocol/Internet Protocol), a camada de aplicação desempenha um papel crucial ao disponibilizar protocolos que permitem a interação com o usuário.

Dentre esses protocolos pertencentes a essa camada, destaca-se o DNS (Domain Name System), responsável por facilitar o acesso aos serviços disponíveis nas redes de computadores, convertendo nomes de domínio em endereços IP correspondentes. Sua existência e importância são indiscutíveis, porém, infelizmente, sua ampla influência despertou a cobiça de indivíduos mal-intencionados.

Esses indivíduos se dedicaram a explorar as vulnerabilidades presentes no protocolo DNS e utilizar técnicas maliciosas para capturar dados de terceiros de forma ilegal. Esse comportamento ilícito compromete a confidencialidade, a integridade e a disponibilidade dos dados transmitidos e armazenados nas redes.

No entanto, a resposta a essas ameaças não tardou a surgir. O segmento de segurança da informação percebeu a gravidade da situação e busca alternativas e soluções eficazes para combater esses acessos indevidos. Diante disso, começou uma disputa entre aqueles que buscam melhorar os mecanismos de exploração das vulnerabilidades do protocolo DNS e os que estão empenhados em desenvolver e implementar medidas de segurança mais robustas para proteger as redes de computadores. Esse embate entre atacantes e defensores evidencia a importância de se manter atualizado e vigilante diante das constantes ameaças cibernéticas.

3.1 Contexto Tecnológico

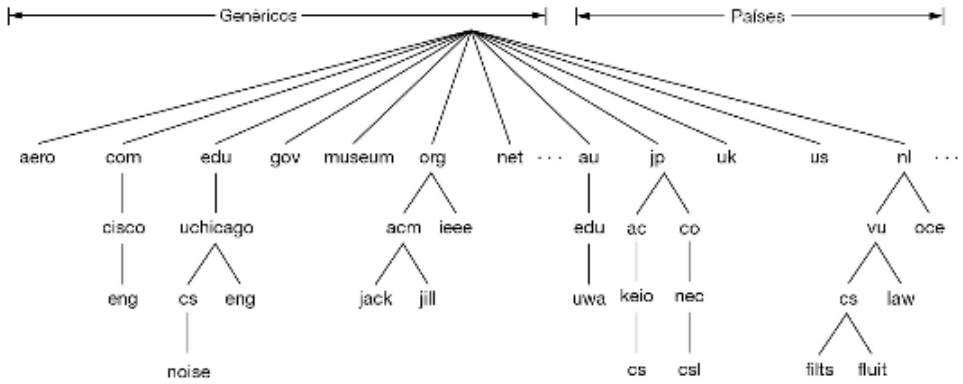
O DNS (Domain Name System) é um importante recurso tecnológico e tornou-se uma parte integrante para o bom funcionamento da Internet. Segundo Lencse (2020), o DNS oferece um amplo suporte aos serviços oferecidos na rede mundial, portanto, parece imperceptível quando funcionando adequadamente. No entanto, quando ocorre uma falha ou os processos de resolução de nome tornam-se mais lentos, logo percebe-se o impacto nos serviços suportados, e a qualidade do serviço torna-se crítica.

De acordo com Silva (2021), o DNS foi criado e regulamentado pelas RFCs 882, 883 e 973, que já estão desatualizadas e foram substituídas pelas RFCs RFCs 1034 e 1035, atualizadas. (TANENBAUM; FEAMSTER; WETHERALL, 2021) afirmam que: “O DNS é um dos protocolos em evolução mais ativo na Internet, sendo definido nas RFCs 1034, 1035, 2181 e elaborado com mais detalhes em muitas outras RFCs”.

Conforme destacado por Kim e Reeves (2020), o sistema DNS segue uma estrutura hierárquica entre seus servidores que são suportados por um sistema de banco de dados

global e distribuído contendo informações de cada domínio. Assim, possibilita que as informações dos DNS possam ser consultadas frequentemente conforme a necessidade do usuário. Para que essa estrutura funcione corretamente, é necessária uma grande interação entre o servidor DNS Raiz, TLDs e servidores DNS Autoritativos.

Figura 1 – Nomes de domínios presentes na internet



Fonte: (TANENBAUM; FEAMSTER; WETHERALL, 2021)

Conforme a obra de Tanenbaum, Feamster e Wetherall (2021), os servidores DNS Raiz são constituídos por 13 servidores DNS redundantes, localizados em diversos países, os quais possuem a capacidade de alcançar todos os TLDs. Esses TLDs podem ser subdivididos em código País Domínio de Nível Superior (ccTLD) e o domínio geral de nível superior (gTLD). A figura 1 demonstra diversos domínios DNS representados por ccTLD e gTLD.

O ccTLD significa nome de domínio de um país e é considerado também como geográfico, representando países, como: .br (Brasil) e .ar (Argentina); e o gTLD representa o tipo de domínio geral, como: .com (comercial), .org (Organizações) e .net (provedores de rede). No geral, os TLDs mais comuns incluem também o .gov (governo), .mil (militar), .edu (educação), .int (organizações internacionais) e outros.

Conforme discutido nas obras de Ramdas e Muthukrishnan (2019) e Kim e Reeves (2020), cada TLD aponta o endereço IP correspondente para o servidor DNS autoritativo consultado. As interações do servidor de DNS são frequentes e com um grande fluxo de mensagens, por conta disso, é indicado que os servidores armazenem, por um tempo determinado, os registros mais recentes. É conhecido como tempo de vida (TTL) esse tempo de armazenamento dos registros no cache, o qual se dá por um tempo específico, determinado pelo administrador do sistema.

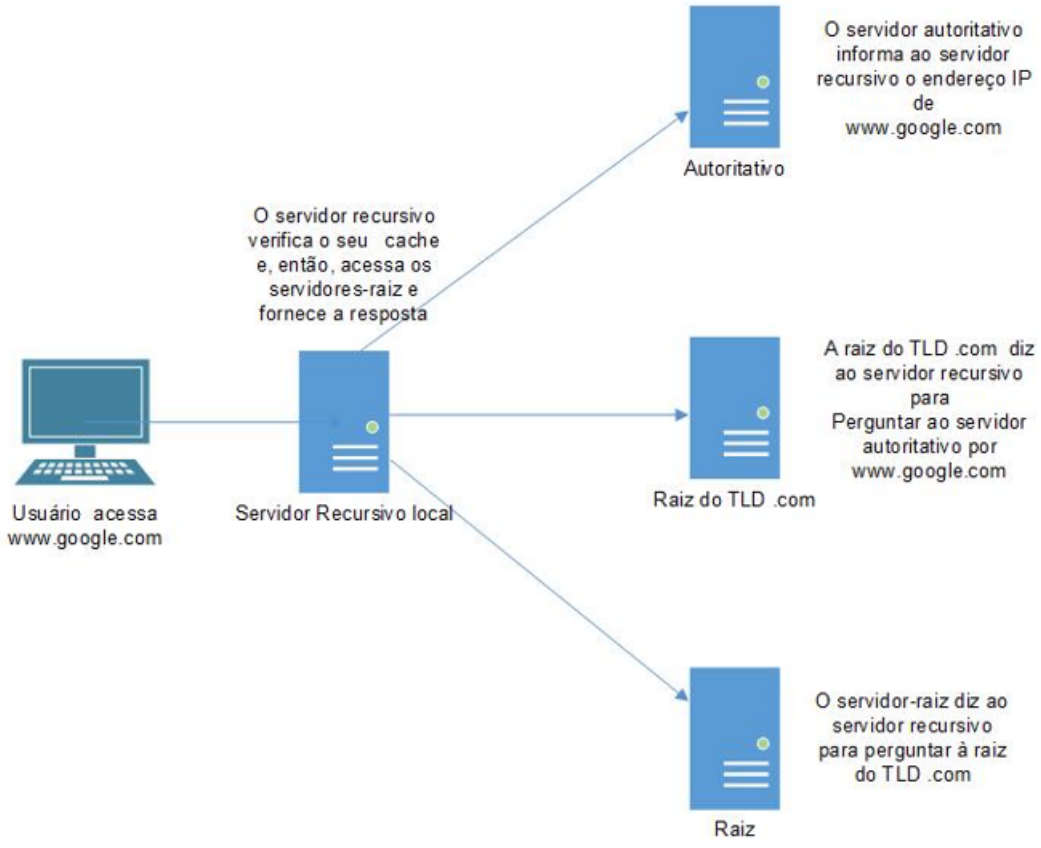
Conforme mencionado pelos autores supracitados Ramdas e Muthukrishnan (2019) e Kim e Reeves (2020), essa procura constante de produtos tecnológicos e novos serviços suportados pelo DNS gerou uma forte demanda sobre os serviços. À medida que o número de domínios aumentava, o número de TLDs disponíveis tornava-se insuficiente. Em decorrência

disso, a ICANN, em 2014, anunciou 1500 novos servidores TLDs que estão sendo mantidos pela IANA.

Conforme destacado por Mendes (2020) e Torres (2014), os servidores DNS servem para converter endereços nominais em endereço IP (A.B.C.D) e vice-versa, tudo em uma estrutura hierárquica global. O nome das máquinas segue um formato chamado FQDN (Full qualilified Domain name), ou seja, um domínio totalmente qualificado que deve ser único na rede.

De acordo com Houser et al. (2021), ao acessar uma página web específica, o cliente primeiramente contata um servidor recursivo que consultará os seus dados armazenados em cache. Caso não obtenha uma resposta, o resolvedor recursivo escala a consulta para os servidores superiores, que percorrerão interativamente toda a hierarquia do DNS até encontrar a resposta e devolvê-la para o cliente.

Figura 2 – Fluxo do tráfego de uma consulta de DNS



Fonte:Próprio autor adaptado de Liska e Stowe (2016)

O DNS realiza a tradução do domínio (google.com) solicitado pelo cliente via browser em um endereço IP válido. Após a tradução do nome em endereço IP, é possível acessar o site solicitado, conforme ilustrado na figura 2. Ao longo dos anos, o DNS tem

sido amplamente utilizado, recebendo atualizações e corrigindo brechas de segurança para tornar a navegação na web mais segura. No entanto, os criminosos continuam aprimorando suas técnicas de ataque, comprometendo, assim, a privacidade dos usuários.

Segundo Liska e Stowe (2016), um exemplo clássico dessa violação ocorre quando hackers exploram brechas de segurança para realizar ataques em um servidor, fornecendo respostas falsas com o intuito de sequestrá-lo e redirecionar os clientes para domínios fraudulentos. Com isso, eles capturam dados pessoais, como senhas de banco, números de cartão de crédito e demais informações sensíveis.

3.1.1 Vulnerabilidades do DNS

De acordo com ESR (2019),os invasores de redes de computadores utilizam de quatro etapas para levantamento de vulnerabilidades: reconhecimento, scanning de vulnerabilidades, investigação das vulnerabilidades e exploração das vulnerabilidades, além da evasão dos sistemas de segurança.

Ainda segundo as explanações da ESR (2019), na etapa de reconhecimento, os invasores buscam identificar redes, hosts e usuários de interesse, coletando informações relevantes sobre a estrutura da rede e seus possíveis alvos. Em seguida, na etapa de scanning de vulnerabilidades, os invasores utilizam ferramentas automatizadas para identificar potenciais falhas e vulnerabilidades nos sistemas-alvo. Após a identificação de vulnerabilidades, ocorre a etapa de investigação, na qual os invasores realizam uma análise mais aprofundada das falhas encontradas, explorando-as manualmente e buscando informações adicionais que possam ser úteis durante a invasão. Por fim, na etapa de exploração das vulnerabilidades, os invasores utilizam as falhas identificadas para obter acesso não autorizado aos sistemas-alvo. Além disso, eles empregam técnicas de evasão para evitar serem detectados pelos sistemas de segurança durante a invasão.

Por outro lado, Kim e Reeves (2020) destacam que o DNS é um dos alvos dos atacantes e apresenta várias vulnerabilidades, as quais podem ser classificadas em três categorias: vulnerabilidade por conceito (conceptual view), por estrutura (structural view) e por comunicação (communication view). Na visão conceitual, as vulnerabilidades estão relacionadas a problemas fundamentais no design e na implementação do DNS. Na visão estrutural, as vulnerabilidades estão relacionadas a falhas na arquitetura e na infraestrutura do DNS. Já na visão de comunicação, as vulnerabilidades estão relacionadas a questões de segurança na transmissão de informações entre os servidores DNS.

3.1.1.1 Conceptual view

De acordo com Kim e Reeves (2020), a vulnerabilidade conceitual do DNS ocorre quando os princípios de confidencialidade, integridade e disponibilidade são violados.

A confidencialidade é comprometida quando as mensagens, requisições e respostas são interceptadas, pois utilizam o protocolo UDP que geralmente não oferece criptografia, tornando o seu conteúdo suscetível à espionagem. O princípio da integridade é violado quando a resposta DNS é alterada e não há mecanismos adequados para verificar a autenticidade das informações — como a falta de assinatura de dados. Por fim, o princípio da disponibilidade é atingido quando os serviços de DNS são colocados como indisponíveis, geralmente como alvo de ataques de negação de serviço.

3.1.1.2 Structural view

De acordo com Bates et al. (2018), os servidores de DNS estão organizados em uma estrutura de árvores hierárquicas, que vai da raiz a um simples servidor de domínio. No entanto, essa organização do DNS desencadeia problemas estruturais, os quais resultam em vulnerabilidades do DNS por falta de DNS redundante.

Conforme mencionado por Bates et al. (2018), um exemplo clássico dessa exploração pode ser visto quando um ataque de negação de serviços deixou gigantes como Netflix, CNBC e Twitter fora de operação tanto na América do Norte quanto na Europa. A Dyn — um importante provedor de serviços de sistemas de nomes de domínio — relatou que a causa foi em decorrência de um ataque DDoS, fazendo uso do malware Miraim, que se utilizou de diversos dispositivos de Internet of Things (IOT).

Ainda com base em Bates et al. (2018), a estrutura de DNS aplica redundância entre o raiz e os vários TLDs (Top Level Domains), que são os domínios de níveis superiores, SLD (Second Level Domain), já o FQDN (Fully Qualified Domain Names) não dispõe de tal redundância e isso o torna vulnerável ao ponto de não se recuperar tão fácil de um ataque.

De acordo com Kim e Reeves (2020), outra vulnerabilidade significativa está relacionada à exposição de informações do DNS, que é frequentemente explorada. As configurações básicas do DNS não são suficientes para garantir sua segurança, o que pode resultar na exposição e exploração dessas configurações, incluindo servidores de hospedagem. Essa vulnerabilidade pode comprometer a navegação na web e afetar os clientes dos servidores DNS.

A navegação por um determinado domínio, ou melhor, por um página web, torna-se comprometida quando um dos serviços de DNS é interrompido por um ataque de negação de serviço (DDoS), o qual pode impedir que os usuários acessem o site, levando a uma interrupção do serviço. Se o cache do servidor DNS for alterado, o servidor fornecerá informações falsas aos clientes.

3.1.2 Communication view

Conforme destacado por Kim e Reeves (2020), nessa modalidade de ataque, leva-se em consideração a fragilidade das consultas e respostas DNS. A forma de operação é basicamente em cima do IP, além do número da porta de origem e destino e do ID de transação das respostas, que são manipuladas para obter sucesso em ataques de DNS spoofing.

O fato de o protocolo UDP não possuir criptografia torna as informações transportadas por ele vulneráveis. E, dentre os utilizadores do protocolo em questão, estão as consultas DNS, que são primordiais para conectar um cliente a um servidor. Quando um atacante captura um pacote UDP e verifica os parâmetros de conectividade entre uma consulta DNS e um servidor qualquer, é possível forjar uma resposta do servidor de nomes numa resposta maliciosa, antes de o resolvedor receber uma resposta válida.

Um dos principais recursos do DNS que são comprometidos por esse tipo de ataque é o cache do DNS — proposto para oferecer mais eficiência para o DNS, mas tornou-se uma vulnerabilidade —, quando criminosos, utilizando-se da técnica de envenenamento de cache, enviam um IP malicioso para que o cliente acesse uma página web maliciosa.

Conforme afirma Kim e Reeves (2020), outra vulnerabilidade identificada no DNS é a falta de proteção contra ataques DDos. Esses ataques representam aproximadamente 93%dos ataques reportados na internet. Com a falta de medidas mais efetivas contra o DDoS, os servidores DNS se tornam vulneráveis a sobrecarga e indisponibilidade quando são vítimas desse tipo de ataque em larga escala. Esse tipo de vulnerabilidade ressalta a importância de implementação de estratégias de mitigação de DDoS para tornar os serviços suportados pelo DNS mais estáveis.

3.1.3 Tecnicas de ataques DNS

Conforme afirmado nos estudos de Kim e Reeves (2020), os ataques aos servidores DNS, apresentado na figura 3 (Tabela), ocorrem através de diversas técnicas, as quais podem ser classificadas em quatro categorias: adulteração de dados DNS, inundação de dados DNS; abuso de DNS: DNS tunneling e estrutura do servidor DNS. Essa classificação possibilita que os ataques sejam analisados por áreas, pois os atacantes possuem interesses diversos. Alguns realizam atividades de adulteração de dados, outros, inundações, com o intuito de perturbar os serviços.

Manter a segurança em um ambiente computacional é bastante desafiador, conforme os “Ataques costumam ocorrer na Internet com diversos objetivos, visando diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via Internet pode ser alvo de um ataque, assim como qualquer computador com acesso a Internet pode participar de um ataque.” BR (2012, p. 17).

Figura 3 – Categorização de 11 tipos de ataque ao servidor DNS.

ATAQUES AO SERVIDOR DNS			
DNS Data Tampering	DNS Data Flooding	Abuse of DNS	DNS Server Structure
DNS Cache Poisoning	DNS Flooding Attack	DNS Tunneling	DNS NXDOMAIN
Kaminsky	DNS Reflection and Amplification	DGA	Phantom Domain
DNS Hijacking	Random Subdomain	Fast Flux	

Fonte: Adaptado de (KIM; REEVES, 2020).

Conforme observado por Kim e Reeves (2020), as seguintes técnicas — como o DNS cache poisoning e o ataque Kaminsky — estão incluídas na modalidade de invasão e adulteração de dados.

3.1.3.1 DNS cache poisoning

A efetivação do envenenamento de cache ocorre quando as tentativas, bem-sucedidas, do invasor são capazes de injetar dados falsos no cache de um resolvedor DNS. Essas investidas são elaboradas meticulosamente pelos atacantes, sendo a precisão um fator fundamental para a execução do ataque.

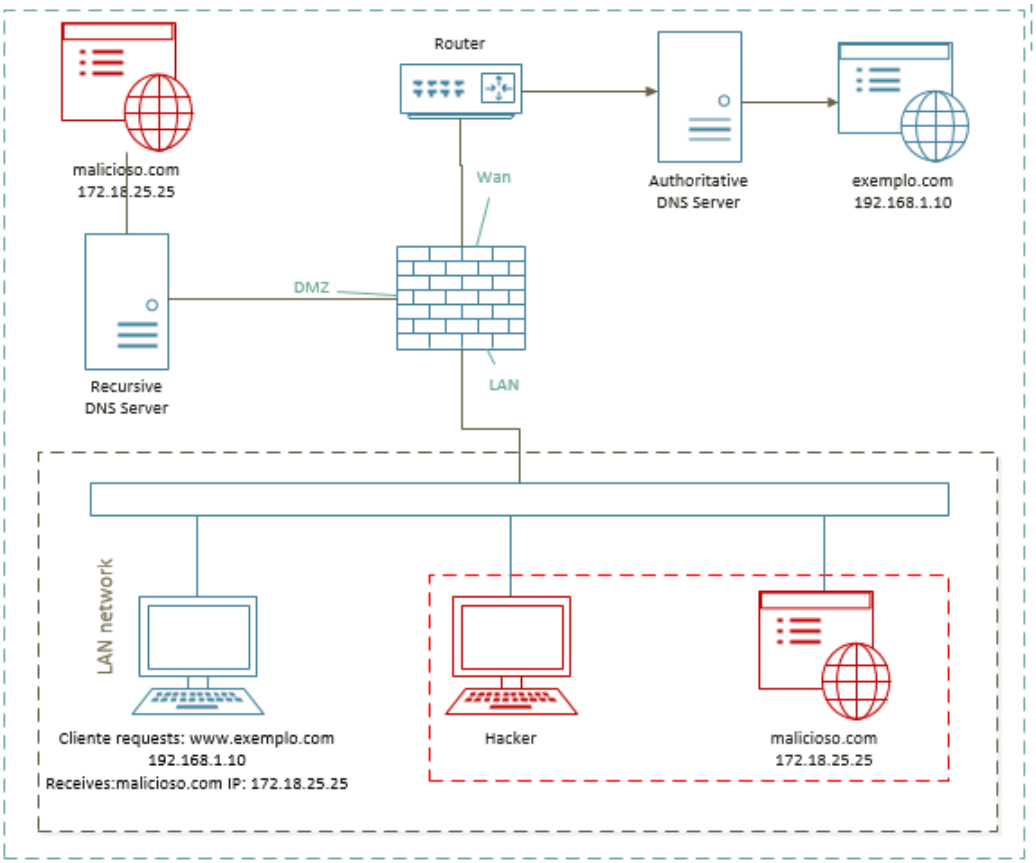
Conforme ressaltado por Wang (2014) e Hmood et al. (2015), as consultas de DNS ocorrem via o protocolo de transporte UDP, o qual não estabelece uma conexão com o destinatário antes de enviar os dados. Utilizando-se dessa vulnerabilidade, um invasor pode comprometer um servidor DNS, introduzindo informações falsas no cache do DNS. Com o resolvedor de nomes envenenado, os usuários do serviço estabelecem conexões com servidores errados e, possivelmente, maliciosos.

O processo de envenenamento do cache , conforme demostrado na figura 4, ocorre durante o mapeamento DNS. Para que isso ocorra, o atacante faz uma requisição ao servidor DNS para saber o endereço IP de um site específico. Caso o servidor local não tenha o endereço em seu cache, envia o pedido para um servidor autoritário. Nesse ponto, o atacante resolve o pedido do servidor DNS através de um servidor autoritário falso implantado por ele, fornecendo o endereço IP do site desejado.

Dependências são estabelecidas para a efetivação desse tipo de ataque. Quando iniciado o ataque, o registro do nome para qual o atacante quer direcionar o ataque não pode constar no cache do servidor de nomes. Além disso, o atacante deve acertar os valores dos parâmetros dos IDs da requisição e porta de origem para a resposta forjada ser aceita.

Conforme apresentado por Carvalho e Pelli (2017), o DNS cache poisoning, para

Figura 4 – Envenenamento DNS cache poisoning local.



Fonte: O autor

ser implementado, antes, precisa do DNS spoofing — que é uma técnica utilizada para falsificar a origem do pacote de mensagens DNS. Essa técnica torna-se útil em decorrência da alteração dos campos de origem e destino do protocolo. Tripathi, Swarnkar e Hubballi (2017) acrescentam que a técnica em questão permite que os campos do pacote IP sejam preenchidos com endereço que não corresponde ao IP verdadeiro e, com isso, leva o usuário a realizar uma conexão insegura.

O ataque pode ser desencadeado de máquinas pertencentes ao mesmo segmento de rede do servidor DNS vítima — ataque a rede local. Tripathi, Swarnkar e Hubballi (2017) asseveram que esse ataque também pode ser implementado de uma rede remota. A efetividade se dá em decorrência de uma resposta falsa enviada para um servidor de nomes, assim o mesmo ID do pacote utilizado em uma pergunta enviada volta na resposta e, com isso, o servidor DNS aceita o endereço IP falso como resposta na resolução de nome de domínio questionado.

Interceptar o tráfego DNS, em uma rede local, não é uma tarefa custosa, considerando que o tráfego DNS não é criptografado, tampouco assinado, pois o cabeçalho do protocolo DNS, em seu campo de ID, de 16 bits. A consulta DNS recebe como resposta, no seu campo ID, o mesmo ID que foi disparado na consulta, ou seja, a consulta e a resposta

possuem o mesmo identificador, portanto tal procedimento abre uma lacuna de segurança, resultando em vulnerabilidades, e os atacantes se valem dessa falha para realizar suas operações de ataque.

3.1.3.2 DNS cache poisoning remoto utilizando a técnica Kaminsky

A literatura indica que um dos primeiros ataques de envenenamento de cache DNS foi descoberto por Kaminsky, em 2008. Essa técnica foi considerada um ataque fora do caminho, ou seja, é possível realizar o ataque remotamente, diferente do envenenamento do cache DNS local, que, em tese, é mais simples de desferir, pois basta que o atacante escute o tráfego da rede para saber a resposta da consulta DNS, que serve de subsídio para o atacante forjar a resposta e, com isso, envenenar o cache do servidor DNS local.

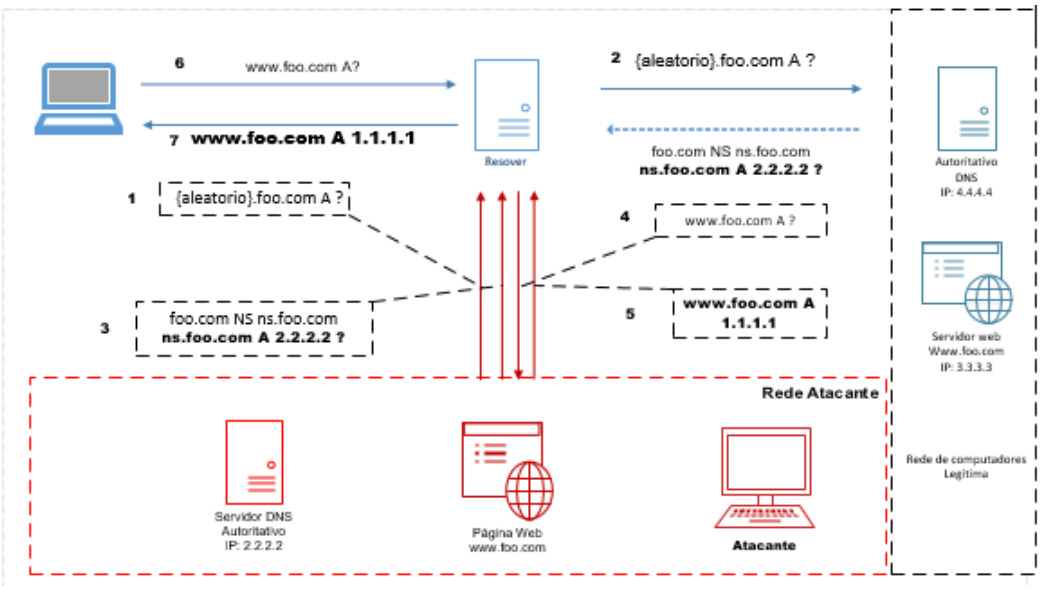
> As coisas podem ficar ainda piores quando os invasores envenenam o mapeamento não apenas para um único site, mas para uma zona inteira. O ataque é conhecido como ataque DNS de Dan Kaminsky e causou um grande pânico entre os responsáveis pela segurança da informação e administradores de rede em todo o mundo. (TANENBAUM; FEAMSTER; WETHERALL, 2021, p. 478)

De acordo com Kaminsky (2008), Wang (2014), Kim e Reeves (2020), Zhang et al. (2021) e Tanenbaum, Feamster e Wetherall (2021), o envenenamento do DNS mediante uso da técnica Kaminsky é mais custoso, porém seu resultado é mais prejudicial, pois seu objetivo é, mormente, alcançar um servidor DNS autoritativo que atende não apenas a uma rede específica, mas a diversas. O ataque em questão, até hoje, vem chamando a atenção dos pesquisadores, pois sua aplicação resulta em forte impacto sobre o protocolo em questão e sua ação afeta quase todos os serviços projetados para trabalhar com o DNS.

O funcionamento do kaminsky, conforme demonstrado na figura 5, ocorre da seguinte forma: 1) O invasor envia uma consulta ao resolvedor de destino para um nome gerado aleatoriamente no formato random .foo.com, onde random denota um valor aleatório; 2) O resolvedor envia uma consulta a um servidor autoritativo, pois há uma pequena chance de que o nome com prefixo aleatório exista no cache; 3) Antes da resposta do servidor autoritário, o invasor inunda o resolvedor com respostas contendo o registro NS de foo.com associado a um registro de cola forjado. Se as palavras de desafio, como TXID na resposta, corresponderem às da consulta, os registros serão aceitos e armazenados em cache pelo resolvedor; 4) Quando o registro A de www.foo.com no cache expira, o resolvedor envia uma consulta externa para o servidor autoritativo falso referido pelo registro de cola falsificado; 5) O falso servidor autoritário responde com um registro A de www.foo.com que aponta o domínio para um site malicioso controlado pelo invasor; 6) Os usuários consultam o endereço IP do nome de domínio ao acessar o site www.foo.com; 7) O resolvedor responde com o registro A de www.foo.com em cache. Deste ponto em

diante, o tráfego será redirecionado para o servidor web do invasor sempre que os usuários visitarem www.foo.com (ZHANG et al., 2021, p.03).

Figura 5 – Diagrama de envenenamento de cache DNS Kaminsky.



Fonte: O autor adaptado de (ZHANG et al., 2021)

O protocolo DNS é baseado em consulta e resposta, em que, em grande maioria dos casos, a autenticidade da resposta não é confirmada. As vulnerabilidades são exploradas por atacantes que investem em inúmeros ataques contra o protocolo. Na pesquisa realizada por Zhang et al. (2021), é apresentada uma técnica que visa melhorar a performance do protocolo DNS. Essa técnica envolve o armazenamento em cache das respostas DNS em servidores locais, por um tempo determinado, para que as consultas futuras desses domínios possam ser obtidas com baixo atraso. No entanto, devido ao melhor desempenho proporcionado por essa técnica, o protocolo DNS também se tornou alvo de ataques de envenenamento de cache DNS.

Pode-se observar a implantação desse ataque em diversos cenários, desde uma rede doméstica, quanto há uma rede corporativa; até empresas de distribuição de energia, hospitais, e instituições bancárias. A figura 6 demonstra (experimentalmente) diversos domínios que foram sequestrados via técnica de Kaminsky. Na ocasião, trazemos como demonstração o sequestro de um domínio de uma grande instituição, a qual investe em tecnologia e segurança.

Conforme discutido em Houser et al. (2021) e Radware (2018), o ataque de sequestro DNS (DNS Hijacking) ocorre quando invasores direcionam o tráfego DNS para sistemas de domínio não autorizados. Nesse contexto, o invasor consegue modificar os registros do servidor para redirecionar o usuário para sites maliciosos. Dessa forma, ocorre a interceptação das solicitações de um usuário e o redirecionamento para o servidor DNS

Figura 6 – Sequestro de Servidores DNS utilizando DNS cache poisoning com a técnica Kaminsky.

Table 7 – Experiment results of various types of domain hijacking.

Target name	max(S)	Success rate of chain hijacking[a] theoretical | experimental	Injected name (chain hijacking)	Type	Injected name (CRNS)	Success rate of real bounce hijacking[a] theoretical | experimental
www.google.com	N/A	100% | 100%	www.google.com	FI-startup	google.com	99.96% | 99.55%
www.youtube.com	N/A	100% | 100%	www.youtube.com	FI-startup	youtube.com	87.50%|86.23%
www.baidu.com	N/A	100% | 100%	www.baidu.com	FI-startup	baidu.com	99.31% | 98.98%
www.paypal.com	N/A	100% | 100%	www.paypal.com	FI-startup	paypal.com	4.17% | 4.55%
www.facebook.com	N/A	100% | 100%	www.facebook.com	FI-startup	facebook.com	98.96% | 96.33%
www.wikipedia.org	N/A	100% | 100%	www.wikipedia.org	FI-startup	wikipedia.org	50.00% | 53.85%
www.taobao.com	N/A	100% | 100%	www.taobao.com	FI-startup	taobao.com	99.65% | 97.75%
www.360.cn	N/A	100% | 100%	www.360.cn	FI-startup	360.cn	95.83% | 96.21%
www.amazon.com	N/A	100% | 100%	www.amazon.com	FI-startup	amazon.com	75.00% | 72.98%
www.jd.com	N/A	100% | 100%	www.jd.com	FI-startup	jd.com	99.93% | 97.92%
www.live.com	N/A	100% | 100%	www.live.com	FI-startup	live.com	4.17% | 3.85%
www.china.com.cn	N/A	100% | 100%	www.china.com.cn	FI-startup	china.com.cn	95.83% | 92.77%
206.220.58.216.in-addr.arpa	N/A	100% | 100%	206.220.58.216.in-addr.arpa	FI-startup	220.58.216.in-addr.arpa	87.50% | 85.99%
195.24.217.172.in-addr.arpa	N/A	100% | 100%	195.24.217.172.in-addr.arpa	FI-startup	24.217.172.in-addr.arpa	50.00% | 47.98%
224.166.102.103.in-addr.arpa	N/A	100% | 100%	224.166.102.103.in-addr.arpa	FI-startup	166.102.103.in-addr.arpa	87.50% | 90.75%
218.134.136.14.in-addr.arpa	N/A	100% | 100%	218.134.136.14.in-addr.arpa	FI-startup	134.136.14.in-addr.arpa	97.92% | 95.83%
11.250.10.106.in-addr.arpa	N/A	100% | 100%	11.250.10.106.in-addr.arpa	FI-startup	250.10.106.in-addr.arpa	50.00% | 47.93%
33.79.0.192.in-addr.arpa	N/A	100% | 100%	33.79.0.192.in-addr.arpa	FI-startup	192.in-addr.arpa	99.48% | 98.75%
252.246.212.88.in-addr.arpa	N/A	100% | 100%	212.88.in-addr.arpa	FI-startup	252.246.212.88.in-addr.arpa	50.00% | 52.01%
4.25.217.172.in-addr.arpa	N/A	100% | 100%	4.25.217.172.in-addr.arpa	FI-startup	25.217.172.in-addr.arpa	95.83% | 90.59%
www.goodreads.com	192	99.74% | 99.59%	com	RE-startup	www.goodreads.com	87.50% | 88.43%
www.webmd.com	288	99.83% | 99.65%	www.webmd.com	RE-startup	www.webmd.com	99.83% | 97.99%
www.interia.pl	2880	99.98% | 99.95%	www.interia.pl	RE-startup	www.interia.pl	50.00% | 49.62%
www.myfreecams.com	2160	99.98% | 99.81%	www.myfreecams.com	RE-startup	www.myfreecams.com	99.98% | 97.11%
www.gmarket.co.kr	288	99.83% | 99.75%	www.gmarket.co.kr	RE-startup	www.gmarket.co.kr	99.98% | 95.85%
www.gusuwang.com	288	99.83% | 99.69%	com	RE-startup	www.gusuwang.com	75.00% | 72.98%
www.gotowebinar.com	2880	99.98% | 99.88%	www.gotowebinar.com	RE-startup	www.gotowebinar.com	99.98% | 95.22%

[a] The results only represent the success rate of hijacking in the second phase of DNS cache poisoning. The overall success rate of poisoning is determined also by the injection success rate in the first phase which is 100% as the MitM injection method is used in the experiments.

Fonte:(ZHANG et al., 2021)

comprometido do invasor.

Esse tipo de empreitada, geralmente, tem a finalidade de adquirir dados sensíveis — o criminoso clona um site de uma instituição financeira que o cliente tenta acessar. E, a partir desse momento, poderá ser desviado para o site falso e ter seus dados bancários capturados. A figura 7 demonstra uma situação de sequestro de domínio de uma instituição financeira de grande renome no Brasil, isso mostra que as grandes instituições com fortes investimentos e pessoal treinado em segurança de redes são alvos de sequestro de servidores DNS.

Ramdas e Muthukrishnan (2019) afirmam que, em decorrência dos inúmeros ataques destinados ao DNS, novas versões de servidores DNS possuem mecanismos de segurança

Figura 7 – Sequestro do Domínio Banco do BRASIL

```
$ dig www.bb.com.br @198.50.222.136
; <<>> DiG 9.10.3 <<>> www.bb.com.br @198.50.222.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49313
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;www.bb.com.br.                  IN      A

;; ANSWER SECTION:
www.bb.com.br.          10800   IN      A       198.50.222.136

;; AUTHORITY SECTION:
www.bb.com.br.          10800   IN      NS      win-eknrp3tthaf.

;; Query time: 94 msec
;; SERVER: 198.50.222.136#53(198.50.222.136)
;; WHEN: Fri Aug 10 02:20:53 CEST 2018
```

Fonte: (RADWARE, 2018)

que dificultam a ação de criminosos, pois os servidores atuais possuem mecanismos que randomizam os valores do campo ID para diversas consultas DNS e, com isso, eliminam a geração automática dos IDs, visto que, com o advento dessas inovações, os riscos com esse tipo de ataque se tornou mais custoso.

3.1.4 DNS Security Extensiong (DNSSEC)

Conforme descreve Tanenbaum, Feamster e Wetherall (2021) devido ao aumento dessas investidas contra a segurança do DNS, medidas de contenção foram desenvolvidas para superar os avanços dos ataques hackers. Umas dessas contenções foi o protocolo DNS Security Extensiong (DNSSEC), apresentado na RFC 2535 e atualizado nas RFCs 4033, 4034 e 4035. Implantou-se mecanismo de assinatura digital de criptografia de chave pública no sistema DNS. A organização dessa nova medida de proteção se vale da infraestrutura de chaves públicas (PKI) que oferece proteção aos dados de comunicação do DNS. Essas chaves são emitidas por autoridades certificadoras (CA) e, assim, garantindo a propriedade das chaves públicas. Por meio dessa técnica, os clientes e resolvedores podem verificar se as respostas de DNS não foram forjadas ou alteradas.

> O DNSSEC oferece três serviços fundamentais: Prova de onde os dados se originaram. Distribuição de chave pública. Autenticação de transação e solicitação.O principal serviço é o primeiro, que verifica se os dados que estão sendo retornados foram aprovados pelo

> proprietário da zona. O segundo é útil para armazenar e recuperar chaves públicas com segurança. O terceiro é necessário como proteção contra ataques por reprodução e spoofing. Observe que o sigilo não é um serviço oferecido, pois todas as informações no DNS são consideradas públicas. Tendo em vista que a implantação do DNSSEC deverá demorar vários anos, a habilidade de servidores conscientes da segurança para interoperar com servidores que ignoram os aspectos da segurança é algo essencial; isso implica que o protocolo não pode ser alterado (TANENBAUM; FEAMSTER; WETHERALL, 2021, p. 533).

Apesar de o DNSSEC oferecer segurança para as transações do DNS, essa extensão, conforme destacam Chung et al. (2017), ainda não foi implantada significativamente para cumprir o seu propósito. Um dos motivos para essa baixa adesão do DNSSEC é a sua complexidade.

3.1.5 Técnicas de proteção

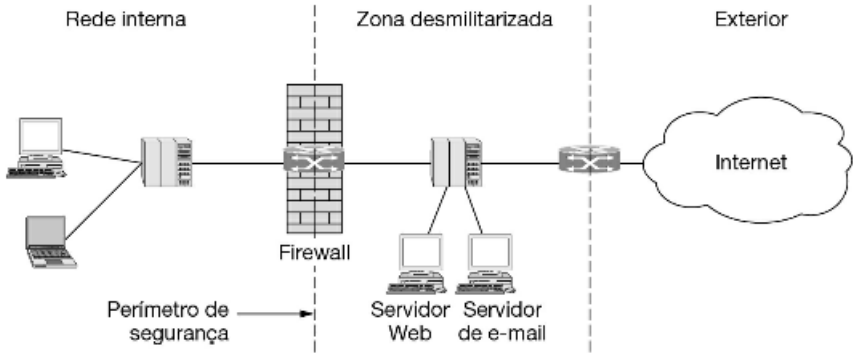
Conforme discutido por Silva e Vale (2021), o monitoramento e a revisão das medidas de segurança de redes de computadores devem ser contínuas para garantir que estão funcionando adequadamente e protegendo de forma adequada os dados que estão em sua posse. Dessa forma, recomenda-se observar os regulamentos da instituição, a legislação sobre a proteção de dados e resguardar-se em utilizar as melhores práticas em segurança de redes de computadores, com a finalidade de garantir que a instituição esteja em conformidade com as exigências legais.

A segurança da informação é montada seguindo técnicas diversas, como: implantação de um firewall que age entre a WAN e a LAN da instituição; sistemas de antivírus que são utilizados para eliminar vírus, cuja eficácia depende de sua base de dados atualizada para verificar a assinatura dos vírus; outra ferramenta bastante utilizada são os IDS, responsáveis por monitorar a rede e emitir alertas ao administrador da rede. Khan e Hasan (2017) afirmam que o sistema de IDS pode ser baseado em Host (voltada para monitorar computadores) ou Rede (trata de monitorar a rede).

Khan e Hasan (2017) definem que o funcionamento de um firewall pode ser uma combinação de componentes (hardware e software) com o objetivo de proteger informações entre uma rede privada e a internet ou outras redes. Para ter um firewall eficiente, é preciso que ele seja configurado corretamente, possua bons recursos implementados e esteja corretamente posicionado na rede.

Os firewalls são definidos por suas diversas capacidades e são classificados de acordo com suas camadas de atuação, ou seja, se um firewall atua no nível da camada de rede, interpreta as informações do cabeçalho dos protocolos dessa camada. Atuando na camada de aplicação, interpreta informações dos cabeçalhos dos protocolos da camada de aplicação

Figura 8 – Elementos essenciais para segurança de redes



Fonte: (TANENBAUM; FEAMSTER; WETHERALL, 2021)

e das camadas inferiores (MORAES, 2021).

IDS (Intrusion Detection System) é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos. Esse equipamento não bloqueia uma ação, mas verifica se a ação é ou não uma ameaça para um segmento de rede, informando a um sistema de gerenciamento de falhas (TANENBAUM; FEAMSTER; WETHERALL, 2021). Assim, a vantagem de se utilizar um IDS é que ele não interfere no fluxo de tráfego da rede, pois ele trabalha em paralelo à rede, apenas monitorando o fluxo de dados, analisando e reportando possíveis ataques ou riscos à segurança.

Essa ferramenta pode ser classificada da seguinte forma: Network Intrusion Detection System (NIDS), cuja função é analisar os pacotes e reportar os ataques detectados (NETO; ÁVILA; LACERDA, 2017); O Host-Based Intrusion Detection Systemt (HIDS) se trata de um sensor que analisa o comportamento de um host com o intuito de detectar anomalias; e, por fim, o Protocolo-Based Intrusion Detection System (PIDS) dedica-se a monitorar um protocolo específico (TORRES, 2014). Algo a se ressaltar sobre o IDS é o fato de não conseguir agir sozinho sobre o problema, dependendo de outros elementos de segurança para eliminar o possível ataque.

IPS (Intrusion Prevention System) surgiu como um complemento do IDS, pois ele tem a capacidade de identificar uma invasão, analisar a relevância do evento/risco e bloquear determinados eventos. O IPS é uma ferramenta com inteligência na maneira de trabalhar, pois reúne componentes que fazem com que ele se torne um repositório de logs e técnicas avançadas de alertas e respostas, voltadas exclusivamente para tornar o ambiente computacional cada vez mais seguro, sem perder o grau de disponibilidade que uma rede deve ter.

O IPS usa a capacidade de detecção do IDS junto com a capacidade de bloqueio de um firewall, notificando e bloqueando de forma eficaz qualquer tipo de ação suspeita ou

indevida. Dessa forma, é uma das ferramentas de segurança de maior abrangência, uma vez que seu poder é de alertar e bloquear, agindo em diversos pontos de uma arquitetura de rede. Um IPS é instalado em modo In-Line.

DMZ (Demilitarized Zone), a ideia é criar uma área de serviços comuns que podem ser acessados tanto por usuários externos (Internet – redes não confiáveis) como por usuários internos (Intranet – rede confiável). A grande vulnerabilidade se encontra nos serviços e servidores que possibilitam acessos externos. Desse modo, tiram-se esses servidores da rede interna para, caso esses sejam comprometidos, não necessariamente implique em comprometimento dos usuários e serviços internos (TORRES, 2014).

3.2 Computação Forense

O crime informático é originado em uma plataforma computacional que perpassa o mundo físico e resulta em impacto negativo aos seus alvos, dessa forma, alterando as condições de funcionamento — seja de um aparelho digital, software ou informações armazenadas em um banco de dados. Conforme destaca Pacheco (2020), esse modelo de comportamento se materializa em prejuízo e violação ao objeto tutelado e protegido pelo Direito Penal.

Conforme Silva et al. (2020), a computação forense reúne um conjunto de procedimentos técnicos com a capacidade de coletar evidências digitais em dispositivos computacionais e, dessa forma, demonstra em que condições um delito informático foi realizado. Para isso, é necessária a atuação de um profissional capacitado, ou seja, um perito em computação forense, que realizará os procedimentos de forma sistemática.

> A Computação Forense tem como objetivo principal determinar a dinâmica, a materialidade e autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhes validade probatória em juízo (ELEUTÉRIO; MACHADO, 2019, p. 12).

Esse tipo de investigação suportada pela computação forense busca avaliar as circunstâncias sob as quais um crime informático ocorreu, a materialidade e a autoria. Para isso, estabelece critérios científicos para validar as provas do delito perante o judiciário (ELEUTÉRIO; MACHADO, 2019). E, dessa forma, a perícia forense pode ser considerada um suporte técnico ao judiciário, realizado preferencialmente por pessoal habilitado.

A análise forense em redes de computadores é uma derivação da forense computacional. Portanto, segundo Galvão (2018, p. loc 297)): “A análise forense em redes de computadores consiste na captura, no armazenamento, na manipulação e na análise de dados que trafegam

(ou trafegaram) em redes de computadores, como parte de um processo investigativo". Dessa forma, conforme mencionam Pilli, Joshi e Niyogi (2010), a forense em redes de computadores rastreia o ataque até a origem e atribui o crime a uma pessoa, host ou rede. Além disso, por meio dos dados coletados, pode construir barreiras e documentar modelos de comportamento de atacantes de redes.

3.2.1 Tipos de Perícia Forense Computacional

Em se tratando de análise forense computacional, Galvão (2018) a classifica da seguinte forma: análise ao vivo e análise off-line. A primeira envolve a análise direta das mídias de prova — não recomendada, pois a análise ocorre diretamente sobre a mídia de prova. Essa prática é adotada em cenários de falta de tempo, recursos ou até mesmo por falta de autorização para replicar a informação em uma nova mídia para análise off-line. Apesar da celeridade que esse tipo de análise oferece na apuração dos resultados, há mais possibilidades de contestação, pois não oferece a possibilidade de uma nova perícia. Isso significa que uma nova perícia não será replicada nas mesmas condições das provas que foram geradas durante a primeira avaliação. Já a segunda forma de perícia (off-line) dedica-se a analisar dados que foram armazenados para uma análise futura, dentre os quais podem ser listados os logs de um sistema de monitoramento de rede, como IPS, IDS, log de um firewall ou até mesmo um concentrador de logs com um SIEM.

> Registros em logs: nesses casos, a perícia não é realizada diretamente sobre os pacotes em tráfego, mas sobre os registros (logs) relacionados a alguma aplicação que utiliza ou utilizou a rede, como logs de: firewalls, sistemas de detecção de intrusões (IDS), servidores de aplicação (logs registrados por servidores web [HTTP], proxies, FTP, e-mails [SMTP, POP3/IMAP], dentre outros serviços), sistemas operacionais, tabelas/registros ARP e registros feitos pelos próprios sistemas operacionais relacionados a uso de recursos de rede.(GALVÃO, 2018, p. 358)

Análise forense pode se beneficiar significativamente dos dados registrados nos logs dos sistemas computacionais, uma vez que esses arquivos são capazes de armazenar informações detalhadas e precisas sobre as atividades executadas pelo sistema. No entanto, esses logs têm um período de retenção limitado e, muitas vezes, são deletados. Portanto, recomenda-se coletá-los o mais breve possível, com a finalidade de garantir a integridade e precisão das evidências coletadas.

3.2.2 Processo Forense

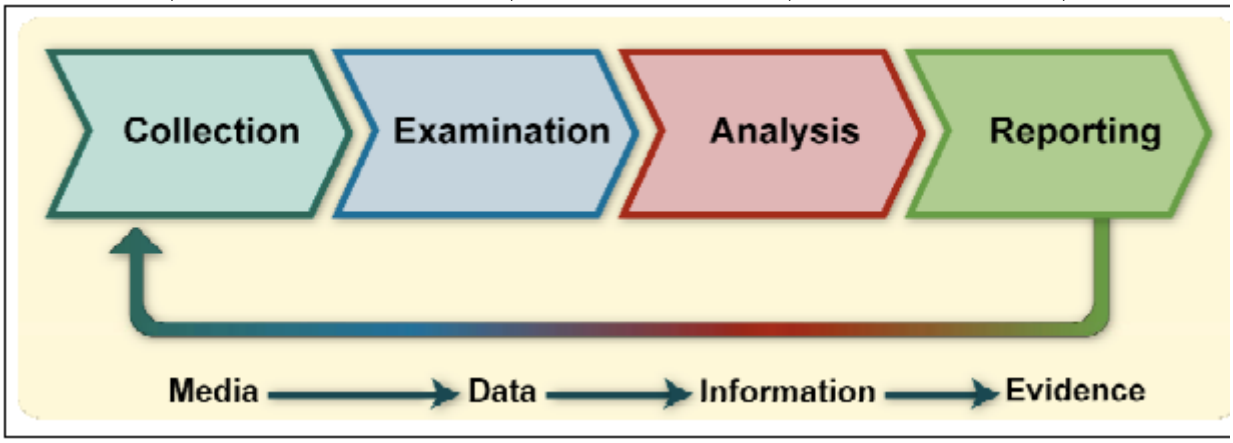
O ciclo de vida do processo forense, segundo Kent, Chevalier e Grance (2006), representado na figura 9, pode ser composto por 4 etapas: coleta, exame, análise e

apresentação. Ao analisar diversos trabalhos forenses, pode-se perceber que, dependendo da pesquisa, são acrescentadas outras etapas. Um exemplo dessa expansão pode ser visto em Martinelli (2013), que lista as etapas de uma análise forense em 5 etapas: obtenção e coleta de dados, preservação, identificação, análise e apresentação. Essa abordagem, de certa forma, está inserida nas etapas estabelecidas por Kent. Dessa forma, os autores em questão buscam elucidar o crime e alcançar os resultados de forma bastante criteriosa, resguardando-se para preservar as provas ao máximo e não comprometê-las.

> A evidência digital é uma das evidências mais voláteis com as quais um investigador pode lidar, e o menor erro ou manipulação indevida da parte do investigador poderá causar sérios impactos na investigação. Pode haver perda permanente ou parcial dos dados. Uma manipulação acidental dos dados pode levar ao questionamento de suas habilidades para investigar, bem como da integridade dos dados da investigação (OETTINGER, 2021, p. 82).

Figura 9 – Processo Forense

Collection / Coleta, **Examination** / Exame, **Analysis** / Analise , **Report** / Relatório



Media / Midia, **Data** / Dados, **Information**/Informação, **Evidence**/ Evidência

Fonte:(KENT; CHEVALIER; GRANCE, 2006)

Conforme destaca Galvão (2018), a perícia forense se mostra como um importante suporte técnico ao poder judiciário. A apuração de um crime é realizada por pessoas capacitadas em diversas áreas do conhecimento, e traz respostas ao questionamento do judiciário quando não dispõem de conhecimento técnico para julgar o caso com precisão. Essa agregação da perícia forense reflete em ação positiva à justiça a qual aplica a lei em prol da sociedade e levando a penalização ou inocência ao acusado.

3.2.2.1 Coleta

Pode-se considerar como fonte de dados, em computação forense, as mídias de provas, dentre as quais podem ser incluídos os diversos tipos de dispositivos informáticos,

incluindo as suas memórias voláteis e não voláteis, como discos rígidos, pendrives, cartões de memória ou qualquer dispositivo capaz de armazenar dados. Além disso, também são considerados dispositivos/meios responsáveis pelo armazenamento e/ou a transmissão de dados voláteis, como memórias voláteis e infraestrutura de redes cabeadas ou sem fio.

Segundo Galvão (2018) e Martinelli (2013), algo importante a ser levado em consideração sobre o armazenamento, ou melhor, a cópia autenticada, dos arquivos a serem periciados é o armazenamento dos dados em suas mídias de destinos. A legislação penal preza pela coleta adequada das provas de um crime e, para isso, estabelece a cadeia de custódia como procedimento padrão a ser seguido durante a coleta de evidências. Dessa forma, a cadeia de custódia preza pelo registro de todas as pessoas que tiveram contato com a evidência e em que momento isso ocorreu. Esses procedimentos são necessários para garantir a integridade e autenticidade da prova coletada.

> A cadeia de custódia é o conjunto de processos direcionados a documentar toda a história cronológica da evidência eletrônica, garantindo a sua integridade, disponibilidade e idoneidade, em todas as etapas da forense computacional, de forma que possa ser utilizada como prova perante a Justiça (WENDT; JORGE, 2021, pp. 265-266)

Ressalta-se que os dados periciais de uma mídia devem ser muito bem armazenados com proteção contra alteração e garantindo a verificação posterior da integridade das cópias, de tal forma que, em caso de outra análise, possa-se chegar ao mesmo resultado, ou seja, a replicação da informação apurada seja comprovada e validada por outros profissionais que se propuserem a investigar, ou melhor, ratificar o que foi considerado como verídico. O fato de o dado estar armazenado de forma segura, garantindo que não houve violação das informações, torna a prova irrefutável.

3.2.2.2 Exame

Uma fase importante na computação forense é a extração dos dados. Nessa etapa, é crucial seguir as etapas dos procedimentos necessários para preservar a integridade do material a ser periciado. É pertinente lembrar que a análise dos dados não deve ser feita no arquivo original, mas sim em uma cópia forense, para garantir a originalidade dos dados. Durante essa análise, é fundamental utilizar ferramentas que comprovem a autenticidade da cópia, assegurando que ela reflita fielmente uma réplica do material original.

> Em uma investigação forense computacional, são utilizados algoritmos hash como instrumento importante para comprovação da integridade de um conjunto de bits – no caso, os arquivos obtidos na fase de coleta. O resultado hash é armazenado e preservado, e na necessidade

> de conferência da integridade dos arquivos se faz possível uma verificação para comprovação de que não foram realizadas alterações, desde que a saída obtida do hash seja a mesma que foi gerada inicialmente (MARTINELLI, 2013, p.43)

Ressalta-se que os dados periciais de uma mídia devem ser muito bem armazenados com proteção contra alteração e garantindo a verificação posterior da integridade das cópias, de tal forma que, em caso de outra análise, possa-se chegar ao mesmo resultado, ou seja, a replicação da informação apurada seja comprovada e validada por outros profissionais que se propuserem a investigar, ou melhor, ratificar o que foi considerado como verídico. O fato de o dado estar armazenado de forma segura, garantindo que não houve violação das informações, torna a prova irrefutável.

3.2.2.3 Análise

Quanto à análise forense, essa é uma etapa muito importante, visto que é o momento de verificar se, de fato, há ocorrência de crime, pois: "A análise de dados é a fase que consiste no exame das informações extraídas na fase anterior, a fim de identificar evidências digitais presentes no material examinado, que tenham relação com o delito investigado", com base no que apontam Eleutério e Machado (2019, p.60). A partir das evidências, é possível a elucidação do crime. Nessa etapa, é importante trabalhar com uma imagem pericial fidedigna das mídias de provas armazenadas com proteção contra alterações (qualquer procedimento de leitura e/ou gravação que implique em modificação de seus dados), de modo a permitir a verificação de sua integridade e quantas cópias forem necessárias.

3.2.2.4 Apresentação

O relatório forense está contido na fase de apresentação, fornecendo as provas necessárias para demonstrar se um crime ocorreu ou não. Através de um relatório completo e bem organizado, é possível apresentar com clareza as descobertas, conclusões e recomendações da investigação, oferecendo-se uma base consistente para a tomada de decisão.

Galvão (2018) destaca que um relatório forense é capaz de demonstrar informações satisfatórias extraídas durante a análise da fonte de dados. Essas informações são muito úteis e reportam o endereço IP do suspeito, quais foram os arquivos acessados durante a ação maliciosa, horário do ataque e outras informações, como: Endereço MAC [host de origem], Endereço MAC [host destino], roteador intermediário, navegador utilizado, Software e sistema operacional utilizados no servidor web, porta lógica utilizada pelo cliente no acesso ao servidor, além de outras informações que podem levar à localização do criminoso.

> Cabe esclarecer que os endereços IP podem não ser de um provedor brazileiro. Nesses casos, será necessário encaminhar representação para o Poder Judiciário determinar que a empresa verifique em seus logs e ferramentas de gerenciamento quais instituição - pessoa jurídica- ou pessoa física estava de posse do endereço IP durante o ataque. Com isso, de posse da informação necessária identificar os responsáveis pelo delito (WENDT; JORGE, 2021, p. 148).

O resultado forense é apenas uma das etapas para elucidar um crime, pois, conforme comentam Wendt e Jorge (2021) dificuldades podem ser encontradas durante a identificação do criminoso, considerando-se que, em muitas situações, o provedor de internet do atacante pode estar em outro país, o que dificulta sua localização. Nesses casos, são necessários acordos formais entre países que permitam a cooperação na investigação de crimes cibernéticos.

Com base em informações do Ministério Público Federal (2021) o Brasil já é signatário do Tratado de Budapeste — um acordo internacional que lida especificamente com esse tipo de crime —, o que pode facilitar a colaboração entre países para identificar e punir os criminosos.

3.2.3 Conclusão

Em resumo, pode-se destacar que as novas versões de servidores DNS tem buscado mitigar os ataques direcionados a esse sistema crucial da Internet. Esses mecanismos, como a randomização dos valores do campo ID para consultas DNS, têm contribuído significativamente para tornar as ações criminosas mais onerosas. À medida que a tecnologia avança e as inovações são implementadas, os riscos associados a esse tipo de ataque foram consideravelmente reduzidos, fortalecendo a segurança do DNS e, por consequência, da Internet.

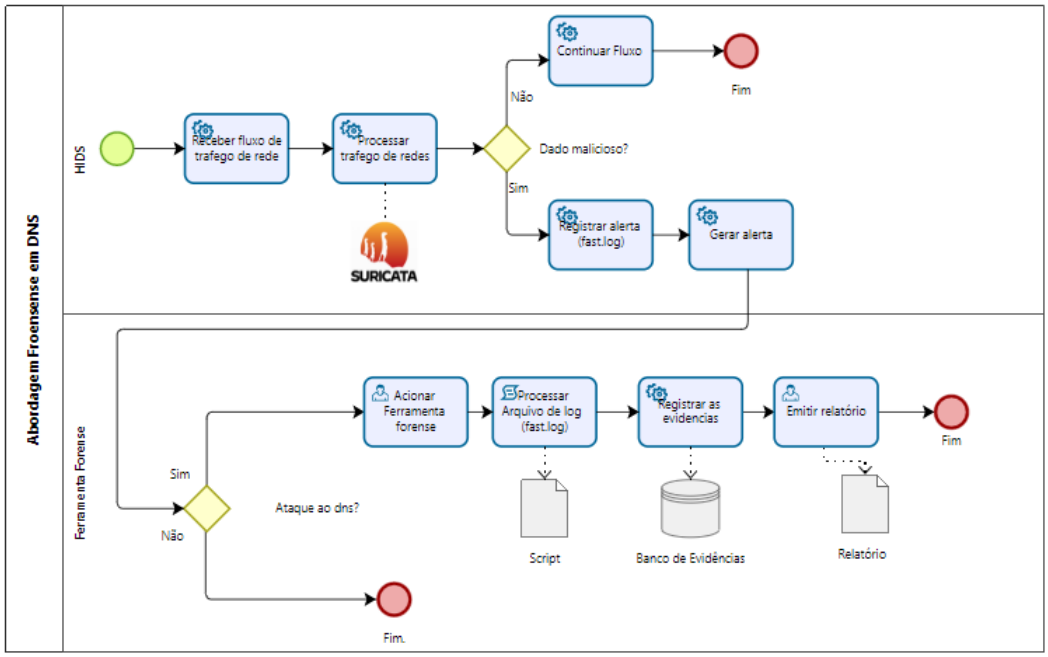
Apesar da disponibilidade da tecnologia, sua adesão não foi plena, pois existe grande número de domínios que ainda não possui o DNSSEC implementado, em vista disso, os atacantes continuam aplicando seus golpes, abusando do servidor de nomes. As investidas maliciosas contra o protocolo DNS.

A computação forense é um importante aliado para as entidades policiais e judiciárias. Seus resultados servem para elucidar crimes informáticos que, em sua grande maioria, são praticados por pessoas que acreditam no anonimato da internet, mas tal fato é refutado, pois os meios informáticos são auditáveis e reúnem informações para elucidação de um crime. A computação forense torna-se importante devido a sua validade perante o judiciário, que tem como fonte de provas as informações coletadas durante a perícia forense e tal fato agrega à justiça, pois criminosos são alcançados pelo rigor judiciário.

4 FORDNS: Análise forense em servidores DNS para ataques de invasão

Este capítulo apresenta uma abordagem forense para analisar ataques de invasão de servidores DNS e identificar elementos que possam caracterizar o crime. A abordagem consiste em associar os fatos ocorridos com a norma penal correspondente — na ocasião, o artigo 154-A do Código Penal Brasileiro —, registrar as evidências em um banco de dados e gerar um relatório forense utilizável como prova crime. Para esse fim, analisam-se os ataques de invasão de DNS cache poisoning, identificam-se a autoria e os detalhes do delito, interpretam-se os dados à luz da legislação brasileira e produz-se um documento que possa ser compreendido por operadores do direito e demais partes interessadas.

Figura 10 – Processos da ferramenta FORDNS



Fonte: O autor.

Neste capítulo apresenta-se também o FORDNS, que é uma ferramenta forense que analisa uma fonte de dados oriunda de um Sistema de Detecção de Intrusão. Essa ferramenta busca evidências de um crime cibernético nos logs gerados pelo IDS suricata, com enfoque nos ataques de DNS cache poisoning. Kim e Reeves (2020) ressalta que esse tipo de ataque é considerado, segundo a literatura, como ataques de invasão .

Na ocasião analisa-se os incidentes de rede notificados pelo IDS (Sistema de Detecção de Intrusão) para identificar a autoria, a técnica de invasão, o endereço IP de origem e destino, horário, serviços de rede atingidos (servidores) e os danos causado ao DNS. Esses

dados são analisados a fim de identificar as atividades criminosas contra o servidor DNS à luz da legislação brasileira (artigo 154-A do Código Penal) (BRASIL, 1940).

Nesse processo, um relatório é gerado, contendo informações sobre o autor, o fato ocorrido, a vítima, as circunstâncias e as consequências, o que pode servir de base para as autoridades procederem com as ações penais cabíveis.

É importante destacar que, embora o FORDNS tenha sido desenvolvido para análise de ataques de DNS cache poisoning, a ferramenta pode ser adaptada para análise de outros tipos de ataques em servidores DNS. A figura 10 apresenta uma visão geral dos processos da ferramenta, incluindo coleta e análise de dados, geração de relatório e análise de contexto para tomada de decisões.

4.1 Processo

A abordagem proposta apresenta um processo de análise forense em servidor DNS, conforme as figuras 10 e 11. Durante esse processo, coletam-se as principais informações da ocorrência do crime. Dessa forma, o desenvolvimento dessa ferramenta possibilita a elucidação de um crime informático, pois muitos não são apurados por falta de provas.

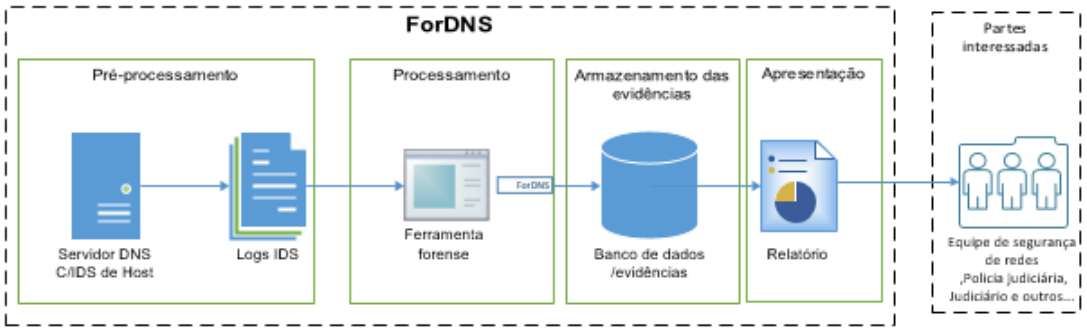
Essa ferramenta faz parte de uma arquitetura computacional que automatiza a análise dos ataques ao servidor DNS. Tais ataques, na maioria dos casos, são identificados manualmente por profissionais de segurança da informação, que precisam identificar os alertas (caso ainda não tenham sido apagados do arquivo de log do IDS), extrair os dados e encaminhá-los a quem possa identificar a ocorrência do delito.

O IDS Suricata, conforme mencionam Open Information Security Foundation (2016) e Neto, Ávila e Lacerda (2017), pode monitorar o servidor DNS em modo HIDS, ou seja, monitorar um Host. Para a correta identificação da atividade maliciosa em estudo, é necessária a correta aplicação e configuração dos dispositivos de segurança em redes de computadores, como o Firewall e o IDS. Nesta abordagem, quando uma invasão é detectada, é gerado um alerta pelo IDS.

Em decorrência disso, o administrador de rede inicia a ferramenta forense para periciar os logs do IDS. A ferramenta faz uma varredura no arquivo de log e, caso encontre referências de ataques ao servidor DNS, captura as principais evidências, armazenando-as em um banco de dados de evidências para posterior análise da atividade e para preservar os dados que caracterizam o crime.

Essa base de dados armazena as informações dos ataques e possibilita a geração de relatório, que poderá servir como meio de prova. Tal procedimento é possível devido à forma como o IDS disponibiliza seus dados, permitindo a leitura e captura dos dados contidos no arquivo de log. A figura 11 demonstra o método utilizado para atingir esse

Figura 11 – Análise Forense (FORDNS).



Fonte: O autor

objetivo: pré-processamento, processamento, armazenamento das evidências do delito e, por fim, o relatório que conterá as principais informações dos delitos e será analisado em relação ao tipo penal.

É importante ressaltar que as partes interessadas nesse processo são as pessoas que darão continuidade às etapas pós-análise forense, como gestores, polícia judiciária, o próprio judiciário e outros. Além disso, é crucial destacar que as partes interessadas nesse processo de análise forense são as pessoas que desempenharão papéis essenciais na continuidade das etapas subsequentes.

4.2 Modelo arquitetural

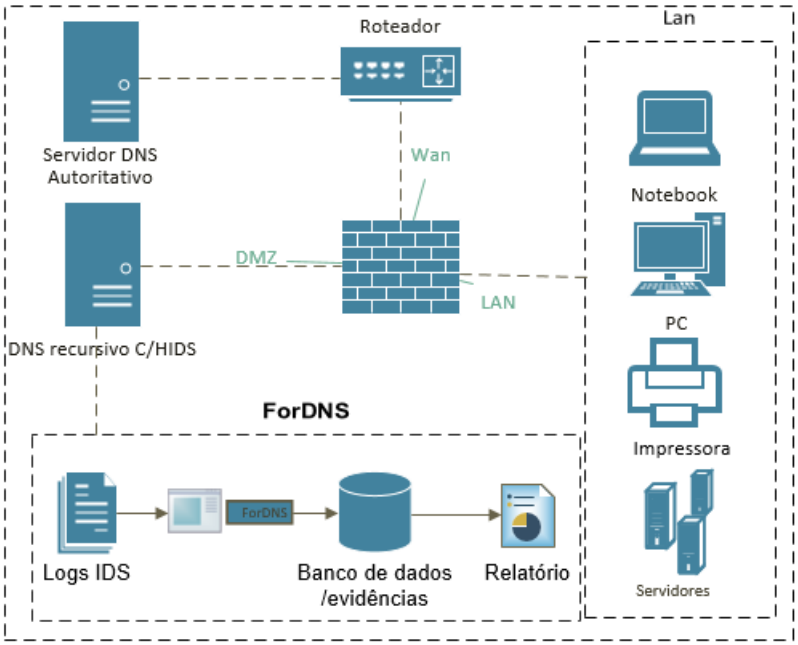
A arquitetura, confome demonstrado na figura 12, possui um roteador que faz divisão entre a rede Wan — rede mundial de computadores onde está o servidor DNS autoritativo e demais serviços da internet; a rede Lan — rede interna onde estão os usuários que demandam serviços da web e de demais serviços privados da rede; o Firewall, que é uma ferramenta de segurança de redes e a segmenta em Wan, Lan e DMZ, zona desmilitarizada que compartilha serviço para acesso público/privado; e, por fim, os elementos da ferramenta forense, que serão explanados ao longo desta seção.

A arquitetura da abordagem desenvolvida para a análise forense é composta por um software especializado, projetado para ler e analisar os registros dos logs do Sistema de Detecção de Intrusões (IDS). Esse software é essencial no processo, pois é responsável por extrair informações dos logs, que serão utilizadas na análise forense.

Ao receber os registros dos logs do IDS, o software realiza uma análise, examinando os eventos registrados. As informações extraídas dos logs são armazenadas em um banco de dados projetado para servir como uma base de dados de evidências. Uma das principais finalidades desse banco de dados é auxiliar o software na geração do documento forense.

Esses documentos forenses são essenciais para a investigação de incidentes cibernéticos.

Figura 12 – Arquitetura proposta.



Fonte: O autor

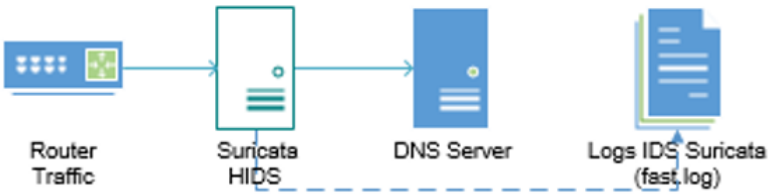
Eles fornecem informações cruciais, permitindo que os investigadores examinem as evidências da análise forense. Além disso, os relatórios podem servir como documentação legal em processos judiciais, fornecendo provas e informações para o devido processo legal.

Portanto, a arquitetura da abordagem desenvolvida para a análise forense baseada nos logs do IDS envolve um software especializado, um banco de dados de evidências e a geração de relatórios forenses. Essa estrutura permite uma análise precisa e eficiente dos eventos ocorridos. É importante enfatizar que a arquitetura proposta aqui serve como diretriz fundamental para uma configuração mínima voltada à segurança de redes. Vale ressaltar que a arquitetura proposta nesta pesquisa orienta sobre as ferramentas necessárias para a segurança em ambientes de redes. É possível uma abordagem ainda mais robusta nesse contexto, inclusive com o emprego de outras ferramentas de segurança.

4.3 Pré-processamento do tráfego de rede

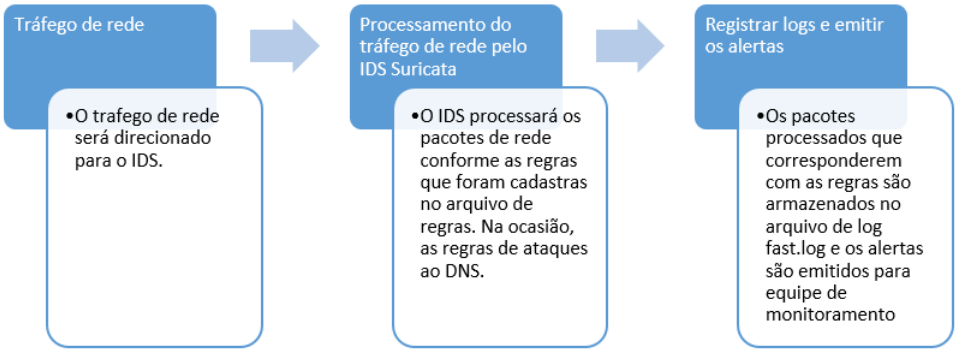
O pré-processamento, conforme demonstrado nas figuras 13 e 14, é a primeira etapa da investigação, onde a fonte de dados gerada é o arquivo de log do IDS Suricata, conhecido como fast.log, responsável por registrar os incidentes durante o monitoramento dos pacotes de rede.

Figura 13 – Visão geral do Pré-processamento.



Fonte: O autor

Figura 14 – Descrição do Pré-processamento.



Fonte: O autor

No modelo em questão, o pré-processamento inicial das evidências de crimes cibernéticos é executado pelo IDS Suricata, que analisa o tráfego de rede e identifica correspondências com assinaturas cadastradas. Quando uma correspondência ocorre, as informações relevantes, como IP de origem, IP de destino, portas de origem e destino, horário de início e término do ataque, tipos de ataques, IDs das regras e outros detalhes, são registradas no arquivo de log (fast.log). Se esses registros incluírem alertas de DNS cache Poisoning, eles são posteriormente analisados usando uma ferramenta forense desenvolvida. Os principais elementos das regras são descritos na tabela 3.

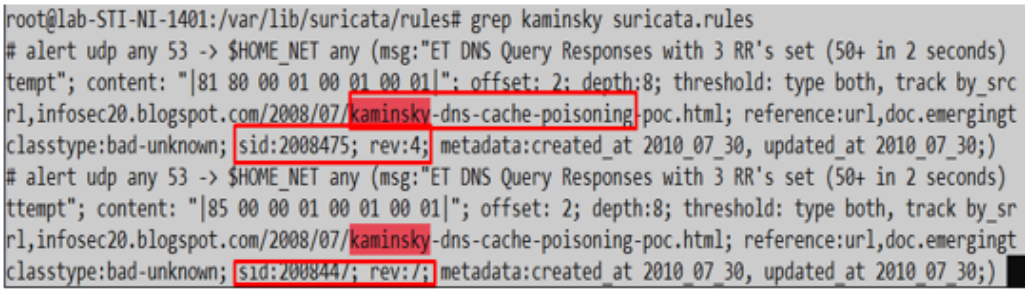
Tabela 3 – Principais informações das regras do IDS suricata

Msg	Mensagem de alerta emitida pelo Suricata
Flow	Fluxo de rede
Content	Contém a cadeia de caracteres que deve ser buscada dentro do tráfego
Sid	ID da regra identificada
Rev	versão da regra
Classtype	Fornece informações sobre a classificação de regras e alertas

Na análise dos logs pela ferramenta FORDNS, buscam-se palavras-chave como o

número de identificação da regra (Sid) e a mensagem (Msg), que indicam o tipo de ataque. Na Figura 15 destacam-se essas palavras-chave.

Figura 15 – Regras de detecção de ataques DNS



Fonte: O autor

Como se observa na figura 16, é possível constatar o alerta gerado pelo IDS Suricata por meio dos seguintes dados: data e horário do ataque, o protocolo utilizado (UDP), classificação do ataque (tráfego malicioso), endereço lógico de origem do ataque (IP 172.1.7.1), porta lógica de origem (53, porta conhecida registrada para o DNS), endereço lógico de destino (192.168.10.3), porta lógica de destino (618880) e descrição da regra. Dessa forma, o IDS Suricata pode ser utilizado como ferramenta de detecção de ataques capaz de reunir evidências criminais para serem analisadas por dispositivos forenses e profissionais da área investigativa da polícia judiciária. Essas informações servirão de base

Figura 16 – Log IDS Suricata

```
07/06/2017-16:35:14.031606  [**] [1:2008446:9] ET DNS Excessive DNS Responses
with 1 or more RR's (100+ in 10 seconds) - possible Cache Poisoning Attempt [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 172.1.7.1:53 ->
192.168.10.3:61880
```

Fonte: O autor

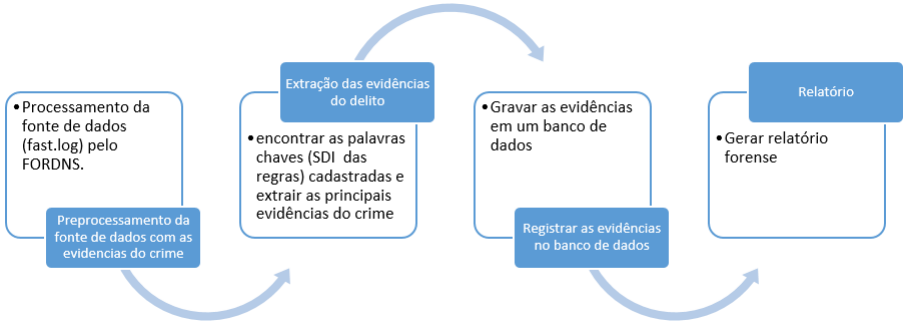
na análise do fato e sua possível subsunção ao delito de invasão de dispositivo informático conectado à rede de computadores, nos termos do art. 154-A, do Código Penal brasileiro.

4.4 Processamento e armazenamento das evidências

Para processar o arquivo de log, a ferramenta forense busca por palavras-chave (os Sid's) das regras responsáveis por identificar os ataques. Ao encontrar registros da ocorrência de um ataque, a ferramenta coleta informações como endereço IP de origem e destino, data/hora, portas de origem e destino e a técnica utilizada. Essas informações são registradas em um banco de dados como evidências do crime para posterior análise, uma vez que constituem provas da ocorrência do crime de invasão de dispositivo informático.

Por fim, a ferramenta gera um relatório contendo os elementos que constituem o delito. Essa sequência é ilustrada na figura 17.

Figura 17 – Processamento.



Fonte: O autor

4.5 Registro das evidências

No banco de dados, as evidências extraídas do log pela ferramenta FORDNS seguem um procedimento de organização preciso para serem armazenadas no banco de dados, conforme demonstrado na figura 18. Inicialmente, é atribuído um ID para cada evidência, garantindo que não ocorra repetição dessa numeração em outras entradas do log. Em seguida, são registrados o timestamp, que inclui a data e o horário exatos em que o ataque ocorreu, juntamente com a duração total do incidente. Posteriormente, são documentados o Source IP, que corresponde ao endereço IP de origem, que possibilita identificar o atacante por trás do incidente, e o Destination IP, que revela o endereço IP do alvo, ou seja, a vítima do ataque. A técnica utilizada no ataque é descrita em "Technique Used", seguida pelo "Result", que apresenta o desfecho ou resultado da operação maliciosa. Por fim, é registrado o tipo específico de ataque, que, neste contexto, é categorizado como um ataque de invasão. Essa organização das evidências facilita a análise e investigação subsequente, bem como a geração do relatório forense.

Figura 18 – Evidências armazenadas

Armazenamento de Evidencias no Banco de Dados						
ID	Timestamp	Source_IP	Destination_IP	Technique_used	Result	Attack_Type
1	05/15/2022-16:50:01.946936	192.168.100.10:47052	192.168.100.1:53	Dns Chace Poisoning	Injection of false data into the cache of a DNS server.	Invasion

Fonte: O autor

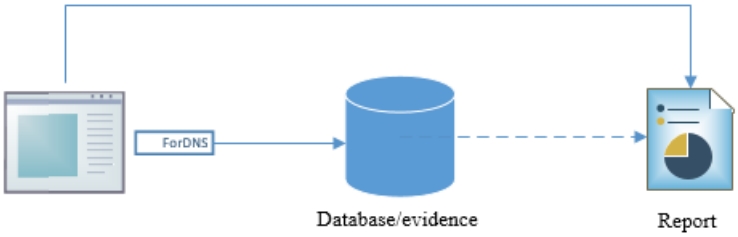
4.6 Relatório Forense

O relatório gerado pela ferramenta FORDNS é de extrema importância nas investigações de invasões de dispositivos informáticos. Ele reúne e consolida informações extraídas e armazenadas em uma nova base de dados, servindo como prova do crime e fundamentando as alegações das autoridades. Ao apresentar as evidências de forma organizada, o relatório contribui para a construção de um caso sólido perante os tribunais.

Além disso, o relatório fornece informações úteis aos investigadores e à Polícia Judiciária, detalhando as técnicas e vulnerabilidades exploradas pelos invasores. Isso permite a compreensão do ocorrido, facilitando a identificação dos responsáveis e a tomada de medidas adequadas para solucionar o caso.

Diante disso, o relatório gerado pela ferramenta FORDNS torna-se indispensável na investigação de crimes cibernéticos, especificadamente em taques de DNS cache poisoning, oferecendo uma visão embasada dos eventos ocorridos durante o ataque de invasão. Sua contribuição como prova do crime destaca sua importância na busca pela justiça.

Figura 19 – Registrando as evidências no relatório.



Fonte: O autor

Conforme as figuras 19 e 20, o relatório concentra as principais informações do delito, registrando-as para as próximas etapas da investigação criminal.

Figura 20 – Registrando as evidências no relatório.

Forensic tool report (ForDNS)	
Date and time of attack	05/15/2022-16:50
IP and logical time of the source	192.168.100.10:35006
Source IP and destination logical time	192.168.100.1:53
Technique used	DNS cache poisoning
Attack type	Invasion
Penal vilation type	Article 154-A of the Brazilian penal code
Data source	Suricata IDS log file

Fonte: O autor

4.6.1 Tipificação penal do DNS cache poisoning

Após a minuciosa análise realizada por Khraisat et al. (2019), que consideram intrusão em dispositivos computacionais qualquer atividade não autorizada que cause danos a um sistema de informação e viole os princípios da confidencialidade, integridade ou disponibilidade; e as definições de Hintzbergen et al. (2018), que definem um ataque como uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a um ativo, torna-se essencial compreender as questões legais associadas aos crimes informáticos.

Conforme ressaltado por Jesus (2017), a configuração de uma conduta como crime requer uma lei específica, pois apenas o que é previsto em legislação pode ser considerado como tal. No contexto dos crimes cibernéticos, antes de 2012, não havia uma lei brasileira específica para tratar dessas questões. Foi somente após a pressão da população e o aumento dos crimes cometidos pela internet que surgiu a Lei nº 12.737, de 30 de novembro de 2012, conhecida como lei de crimes informáticos.

Dentre as disposições dessa legislação, destaca-se o artigo 154-A do Código Penal, que tipifica o crime de invasão de dispositivo informático (BRASIL, 1940). Esse artigo foi inserido no Código Penal pela Lei nº 12.737/2012 (BRASIL, 2012) e passou por alterações recentes, por meio da Lei nº 14.155, de 27 de maio de 2021 (BRASIL, 2021). Segundo Gouvêa (2022), essa alteração ampliou o escopo do crime, passando a considerar invasões de dispositivos informáticos de uso alheio, não se restringindo apenas a dispositivos de propriedade de terceiros. Além disso, a pena atribuída aos delitos previstos no referido artigo também foi agravada, resultando em uma abordagem mais rigorosa contra os infratores.

A tipificação do ataque de DNS cache poisoning torna-se relevante diante desse contexto jurídico, uma vez que esses ataques violam os princípios da segurança da informação, adulterando, destruindo e obtendo informações de terceiros com o intuito de obter ganhos por meio de fraude eletrônica. É fundamental ressaltar que a lei brasileira possui disposições específicas para punir aqueles que praticam essas ações maliciosas, de acordo com a legislação vigente. A figura 21 apresenta um resumo da tipificação do DNS cache poisoning como uma infração ao Código Penal Brasileiro.

Figura 21 – Tipificação penal do DNS cache poisoning conforme art 154-A do C.P

Base legal	Elemento de identificação	Atividade Maliciosa	Resultado	Motivação
Artigo 154-A	Adulterar	**DNS cache poisoning**	Alterar o endereço de um domínio DNS para um domínio malicioso.	Obter vantagem indevida por meio de fraude computacional.
Artigo 154-A	Destruir		Eliminar as resposta de requisição para validar o endereço do domínio no cache do servidor DNS Recursivo ou autoritativo para instalar um domínio malicioso.	
Artigo 154-A	Obter		Levar o cliente a acessar o domínio malicioso com a finalidade de coletar dados (bancários, pessoais, sensíveis e outros)	

Fonte: O autor

Porém, é importante considerar também as limitações técnicas dos servidores DNS quanto ao envenenamento dos servidores recursivos, como apontado por Zhang et al. (2021), visto que o tempo necessário para a atualização entre servidores autoritativos e recursivos permite que os dados injetados no cache dos servidores recursivos sejam utilizados para fornecer serviços até que expirem ou sejam atualizados. Durante esse intervalo de tempo, podem ocorrer implementações de DNS cache local, sequestro do nome do domínio e envenenamento fora do caminho.

4.7 Cenário de implementação

A abordagem possibilita a análise de ataques a servidores DNS em dois cenários: um interno e outro externo. Foi desenvolvida para analisar o tráfego de redes gerado pelo IDS, que, conforme destacado por Waleed, Jamali e Masood (2022), identifica e registra os dados da intrusão por meio da análise do tráfego de rede e da identificação de atividades que se encaixam nas regras que definem diversas técnicas de invasão em redes de computadores

Apesar da captura dessas evidências, da identificação do ataque e de eventuais respostas dadas pelo IDS — como emissão de alertas, interrupção dos serviços de rede atacados ou banimento do dispositivo que originou o ataque —, o IDS não tem como função identificar a ocorrência de delitos.

Nesse contexto, a abordagem proposta pretende contribuir, capturando o fato alertado pelo IDS e analisando-o à luz da legislação penal brasileira, haja visto que nem todo alerta configura a existência de um crime. A seguir, são apresentados os dois diferentes cenários analisados pela abordagem proposta.

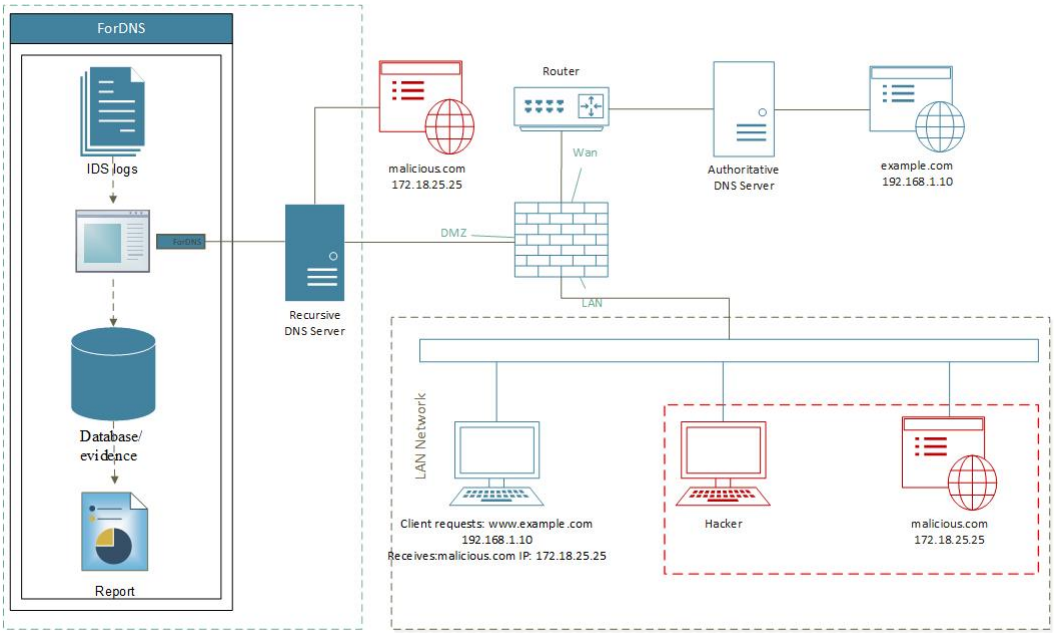
4.7.1 Cenário 1: O atacante encontra-se dentro da rede LAN (usuário autenticado) e invade o DNS local;

O cenário representa ataque ao DNS recursivo, conforme demonstrado na Figura 22. Na ocasião, o atacante criou uma página falsa de uso comum dos usuários da rede. Essa página pode ser de um sistema empresarial/institucional para capturar credenciais de sistemas para obter informações restritas.

O usuário, ao solicitar uma página web, tem o cache DNS envenenado pelo atacante, que insere no cache do DNS recursivo a página web falsificada e leva o cliente a acessá-la e, nela, inserir suas credenciais de sistema — que são capturadas. A página falsificada é semelhante à original.

Em grande maioria, os efeitos deste ataque no cache duram pouco tempo e, logo em seguida, após algumas tentativas, o cliente consegue acessar a página original e não percebe que foi vítima do cache poisoning, pois as informações do cache duram por um curto período de tempo.

Figura 22 – Cenário -1: Analise do DNS cache poisoning



Fonte: O autor

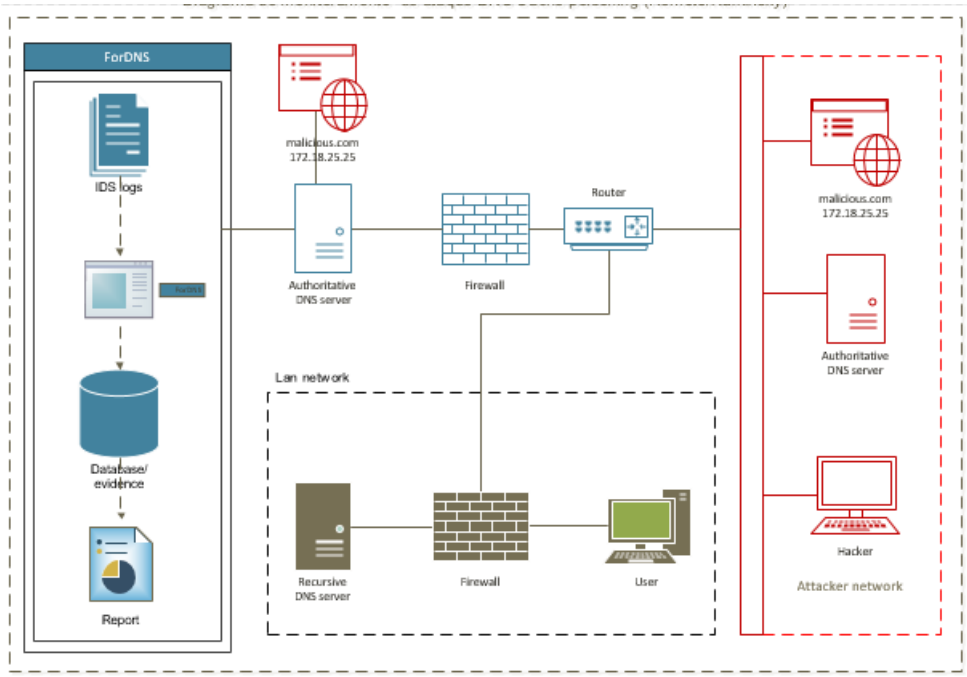
Geralmente, o cliente só percebe que foi vítima de um cache poisoning após as consequências do ataque se materializarem por meio de prejuízos financeiros, laborais,pessoais

e outros. E, a partir dessa percepção, começa a fase de notificação da equipe de segurança da informação e dos órgãos de segurança pública. Nesse contexto, percebe-se a necessidade de uma arquitetura computacional especializada na detecção e análise desses crimes informáticos. A ferramenta da abordagem FORDNS, como mencionada neste trabalho, prioriza a análise desse tipo de ataque, extraindo as evidências do crime e registrando-o como um ataque de invasão, conforme destacado no artigo 154-A.

4.7.2 Cenário 2: O atacante encontra-se na rede WAN (Internet) e invade o DNS principal (autoritativo);

No cenário 2, conforme ilustrado na figura 23, o ataque torna-se mais custoso, mas os impactos negativos causados são mais abrangentes, pois não está restrito a um grupo específico, mas a todos os demais usuários dos serviços de resolução de nomes de domínios que solicitarem o acesso a um domínio específico. Nesse caso, trata-se de um ataque DNS remoto, que, para pesquisadores como Kim e Reeves (2020) e (ZHANG et al., 2021), é conhecido como a técnica de kaminsky, onde o alvo não é o servidor recursivo de uma Lan, mas um com a patente mais elevada, um recursivo de um ISP que solicita um domínio para um servidor DNS autoritativo.

Figura 23 – Cenário -2: Analise do DNS cache poisoning/Remoto



Fonte: O autor

Na implementação do kaminsky, o atacante que está em uma rede remota não aguarda que um cliente de uma rede privada gere uma consulta DNS para envenenar o cache de um servidor DNS de um ISP. O atacante inicia os procedimentos levando o

recursivo do ISP a realizar uma consulta a um servidor autoritativo e, caso não possua o endereço do domínio em cache, este, imediatamente, inicia a consulta ao autoritativo desse domínio. E, nesse momento, o atacante entra em competição com o DNS autoritativo, pois, antes que o autoritativo envie uma resposta autêntica para o recursivo, o invasor, passando-se pelo autoritativo, envia uma grande quantidade de respostas forjadas para o recursivo. Caso a resposta falsificada corresponda à enviada durante a consulta DNS, o recursivo aceitará a resposta falsificada e armazenará temporariamente os registros do domínio malicioso em seu cache.

Dessa forma, verifica-se que o atacante invadiu uma transação do servidor DNS e falsificou a resposta de validação entre os dois servidores e, com isso, interrompeu a comunicação entre os dois; adulterou o endereço IP do domínio verdadeiro para um malicioso e, por fim, obtém informações de terceiros por meio de crime computacional, pois tal procedimento só é possível utilizando um sistema computacional.

Esse tipo de ataque é tão crítico que o atacante pode ficar envenenando o cache do DNS várias vezes ou até mesmo sequestrar um servidor DNS e deixar o original indisponível por meio de ataques DDOS.

Zhang et al. (2021) reportam que o DNS cache poisoning, utilizando a técnica de kaminsky, durante muito tempo, os estudos sobre essa técnica não foram aprofundados e foi direcionado apenas para o envenenamento, mas, em 2021, esses pesquisadores reportam que essa técnica é capaz de agir em consórcio com o sequestro de servidor DNS autoritativo, pois o ataque não perdura apenas com um curto tempo, mas também com um período mais duradouro, resultando em impactos mais severos.

Como reportado no cenário 1, o cliente só percebe que foi vítima do ataque quando as consequências aparecem por meio de prejuízos. Portanto, é importante monitorar essas estruturas computacionais, com o intuito de, quando ocorrer esse tipo de fraude ao servidor DNS, ou a qualquer servidor de uma aplicação computacional, sejam monitorados por ferramentas de segurança da informação. Conforme descrito, mais uma vez, a ferramenta proposta torna-se útil para elucidação de um crime informático. Pois, conforme muito dito, a ferramenta captura as principais evidências de invasão ao DNS e as armazena em uma base de dados, fornecendo um relatório forense que indica esse tipo de ataque como invasão, segundo o artigo 154-A do C.P. Brasileiro.

5 Resultados

Nesta dissertação, é abordada a temática da análise forense em ataques DNS cache poisoning direcionados a servidores DNS. Através da análise forense realizada, obtêm-se evidências que indicam a ocorrência desses ataques. Essas evidências são fundamentais para embasar ações judiciais direcionadas à reparação dos danos causados às vítimas. Ademais, o estudo ressalta a importância da análise forense como uma ferramenta indispensável na investigação e resolução de crimes cibernéticos.

Para a verificação dos ataques de invasão ao servidor DNS, foi efetuado um estudo sobre os tipos de ataques ao servidor DNS, mais precisamente os ataques de invasão, pois buscava-se trabalhar com o artigo 154-A do código penal, que versa sobre invasão a dispositivos computacionais. O estudo focou no ataque DNS cache poisoning, o qual foi considerado como ataque de invasão.

Para detectar esse tipo de ataque, utilizou-se a ferramenta de monitoramento de intrusão de redes O IDS Opens-source Suricata, que trabalha e detecta os ataques por meio de assinaturas, ou seja, regras disponibilizadas ou construídas de acordo com a finalidade do monitoramento. Na ocasião, o trabalho teve como uma de suas fases a geração de uma fonte de dados, ou seja, um arquivo de logs que reunisse as violações ao protocolo DNS que permitia submeter essa fonte de dados à ferramenta forense FORDNS, a qual coletou as principais evidências do delito e as disponibilizou em uma linguagem acessível.

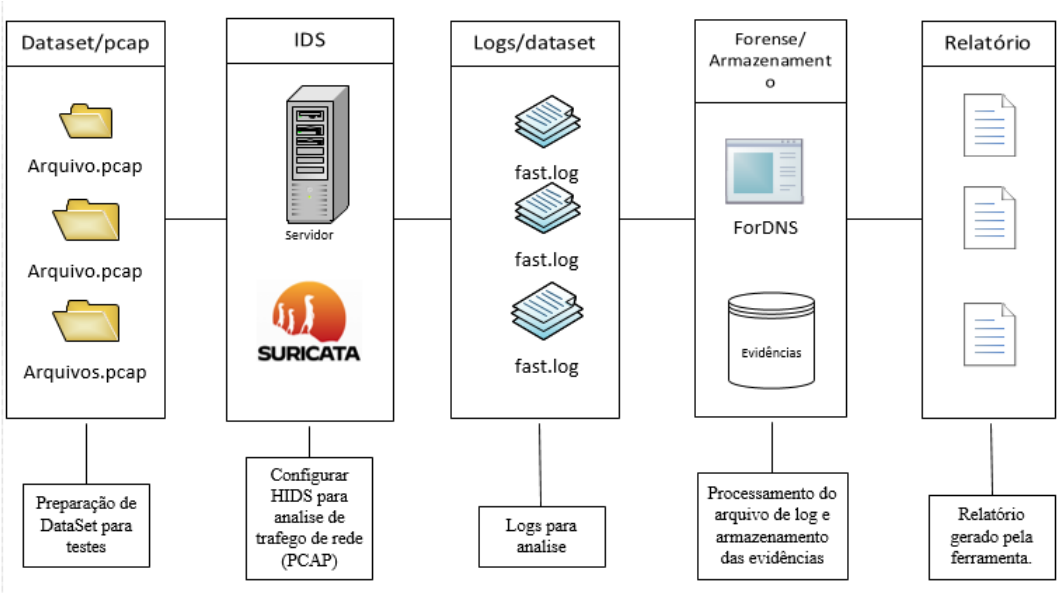
5.1 Teste com a Ferramenta FORDNS

Nesta e nas demais subseções, apresenta-se um ambiente de teste para análise forense em servidores DNS com o auxílio da ferramenta FORDNS. O ambiente utiliza o IDS Suricata para gerar logs e um banco de dados para armazenar as evidências dos ataques, servindo como referência para análises futuras. Com base no arquivo de log, verifica-se a existência de ataques de DNS cache poisoning no arquivo fast.log. Em caso positivo, coletam-se as principais evidências do ataque e as armazenamos no banco de dados. Os testes são necessários para validar as etapas anteriores da pesquisa.

Para realizar essas etapas, foram seguidos os seguintes passos: obtenção e disponibilização dos datasets .pcap para processamento pelo IDS; instalação e configuração do IDS Suricata; pré-processamento dos datasets .pcap pelo IDS Suricata; e, finalmente, submissão dos arquivos de log (fast.log) gerados durante o processamento dos arquivos .pcap à ferramenta forense FORDNS. Essa sequência de etapas está representada na figura 24.

O experimento tem como objetivo submeter os logs do IDS Suricata à ferramenta

Figura 24 – Etapas da execução dos testes



Fonte: O autor

forense. Para isso, utilizou-se um dataSet público de tráfego com intrusão de redes disponibilizado pelo Instituto Canadense de Segurança Cibernética (CIC), com sede na Universidade de New Brunswick. Esse dataset, conforme destacam Sharafaldin, Lashkari e Ghorbani (2018) são capturas de pacotes de tráfego de rede que foram armazenados e tratados e fornecem condições necessárias para a investigação pretendida.

5.2 Definição do Dataset

Conforme analisado por Grajeda, Breitinger e Baggili (2017), dataset é um conjunto de dados relacionados e discretos com significados e finalidades diversas, o qual carrega nos seus resultados muitos dos cenários aos quais foram submetidos. Outro ponto a considerar no estudo foi a análise realizada em diversos artigos que versam sobre cibersegurança e computação forense, nos quais os datasets são criados, porém nem sempre disponibilizados para a comunidade científica. Destaca-se ainda que os datasets, quando disponibilizados, são de extrema importância, uma vez que geram dados analisáveis em diversas pesquisas, otimizando os resultados. Pois, trabalhos realizados com rigor científico são replicáveis e aplicáveis em outros estudos, conferindo respostas que não poderiam ser alcançadas na pesquisa anterior em decorrência de tempo e investimentos.

De acordo com as considerações da IBM (2021)), dataset é um conjunto de dados estruturados, organizados e armazenados, existindo diversos tipos de datasets, cada um com finalidades específicas. Conforme elencam Grajeda, Breitinger e Baggili (2017)), há diferentes tipos de conjunto de dados e alguns utilizados em um contexto de segurança de

redes de computadores (cibersegurança e análise forense), elencando os seguintes tipos de datasets: dados de tráfego de rede, logs de eventos de segurança, conjuntos de dados de malware e vulnerabilidades, dados de autenticação, análise de comportamento e verificação de autenticidade e outros. Esses datasets podem ser utilizados em pesquisas científicas, pois fornecem informações valiosas para análise e desenvolvimento de soluções de segurança. São utilizáveis em pesquisas científicas com o intuito de produzir resultados mais precisos e confiáveis.

Dentre os dadasets utilizados para realização e replicação de novas pesquisas ,inclui-se o tipo de dataset pcap, que, segundo Cunha (2019), é um conjunto de dados coletados a partir de capturas de tráfego de rede em formato pcap (Packet Capture Data). Esses documentos possuem informações sobre os pacotes de rede, como origem, destino, tipo de protocolo, conteúdo do pacote e timestamps.

Como destacado por Open Information Security Foundation (2023) e Open Information Security Foundation (2016), a análise de dataset, utilizando ferramentas de intrusão de redes, é uma prática comum em pesquisas e análise de ameaças computacionais. Uma eficiente é o IDS Suricata, que conta com vários módulos de operação, incluindo a análise de datasets PCAP. Com essa ferramenta, é possível detectar ameaças como malwares, phishing, ataques de negação de serviço e invasões, além de identificar outros padrões de comportamento malicioso. O Suricata possui um vasto repositório de assinaturas para identificação de comportamento malicioso, tornando-o uma poderosa ferramenta para proteção da rede.

A abordagem proposta não tem como foco gerar tráfego malicioso,mas sim analisar uma fonte de dados oriunda da análise de tráfego de rede com um IDS, como o Suricata, que trabalha tanto com dados em tempo real como com arquivos PCAPs, possibilitando análise do tráfego de rede. Um arquivo dessa categoria, analisado em um segundo momento após a sua captura, pode identificar como o ataque foi realizado, trazendo informações como quais vulnerabilidades foram exploradas e qual o comportamento do atacante durante a atividade maliciosa.

Para realizar o teste com a ferramenta forense, seria necessário conectar o IDS Suricata a uma rede e submetê-la a ataques de DNS cache poisoning. Portanto, a análise de tráfego de rede contendo tráfego normal e tráfego malicioso para testar as funcionalidades de análise da ferramenta não foi gerada na pesquisa, mas transferida para um dataset já construído, que forneceu o suporte necessário para realizar os testes. A forma como o dataset foi construído possibilita a validação da abordagem desenvolvida, pois foram utilizados os equipamentos necessários para gerar um tráfego de rede.

O conjunto de dados utilizado tem sua origem na pesquisa realizada por Sharafaldin, Lashkari e Ghorbani (2018) a qual aborda e disponibiliza o CIC-IDS2017, um conjunto de dados simulados contendo ataques realistas. Este estudo também incorpora os resultados

da análise do tráfego de rede ao utilizar o CICFlowMeter, uma ferramenta de análise de fluxo de dados em redes. A referida pesquisa registra informações como horário, IPs de origem e destino, portas de origem e destino, protocolos utilizados e tipos de ataques. Para a elaboração desta pesquisa, foram criados perfis para 25 usuários, abrangendo diferentes protocolos de rede, como HTTP, HTTPS, FTP, SSH e e-mail.

Figura 25 – Dataset PCAP

DataSet.PCAP CIC-DS2017			
Dia da semana	Tipo de trafego de rede	Arquivo pcap	Tamanho arquivo
segunda-feira	normal	Monday-WorkingHours.pcap	11.0G
terça-feira	Ataque + normal	Tuesday-WorkingHours.pcap	11.0G
quarta-feira	Ataque + normal	Wednesday-WorkingHours.pcap	13.0G
quinta-feira	Ataque + normal	Thursday-WorkingHours.pcap	7.8G
sexta-feira	Ataque + normal	Friday-WorkingHours.pcap	8.3G

Fonte: O autor.

No conjunto de dados em questão, demonstrado na figura 25, CIC-IDS 2017, utilizado nos testes deste trabalho, os registros foram coletados durante 5 dias, do dia 3 ao dia 7 de julho de 2017. Os ataques implementados incluem Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet e DDoS. A infraestrutura de rede utilizada contava com os elementos necessários para o funcionamento de uma rede, incluindo Modem, Firewall, Switches, Roteadores e os sistemas operacionais Windows, Ubuntu e Mac OS X.

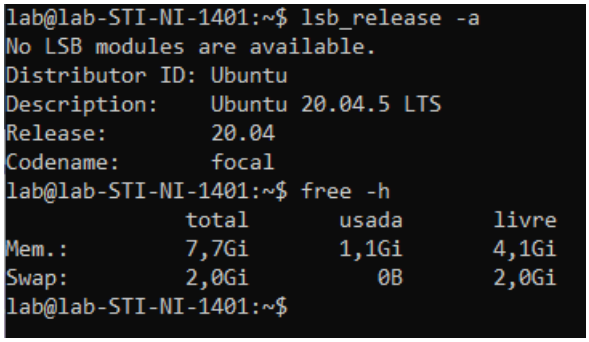
Embora a pesquisa CIC-IDS2017 não faça menção explícita a ataques DNS, ao submeter os arquivos pcaps às regras de monitoramento do protocolo DNS, diversos alertas sobre ataques DNS foram gerados, inclusive o DNS cache poisoning — um tipo de ataque investigado neste estudo.

5.3 Preparação do ambiente

Os logs gerados no monitoramento do tráfego de rede pelo IDS Suricata são a base dessa análise. O Suricata, um IDS consistente e versátil de código aberto, atua também como IPS, garantindo a segurança da rede. Ele analisa pacotes de acordo com regras cadastradas para detectar ameaças durante essa etapa de pré-processamento

Para realização dos testes, utilizou-se um notebook STI NI 1401, equipado com processador Intel Pentium de 2.10GHz e 8GB de memória RAM, para a realização da instalação do IDS Suricata e a análise do dataset específico. Optou-se pelo sistema operacional Ubuntu, na versão 20.04, devido à sua ampla utilização em ambientes de pesquisa e desenvolvimento. A figura 26 mostra as configurações do sistema operacional em questão.

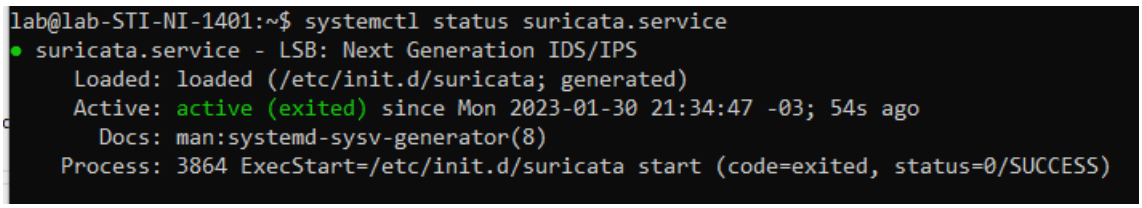
Figura 26 – Informações básicas
do sistema operacional utilizado



Fonte: O autor.

Para realizar a instalação do IDS Suricata, primeiramente foi necessário adicionar o repositório correspondente ao sistema operacional Ubuntu, utilizando o comando "sudo add-apt-repository ppa:oisf/suricata-stable". Em seguida, os arquivos do sistema foram atualizados através do comando "sudo apt-get update". Por fim, o Suricata foi instalado utilizando o comando "sudo apt-get install suricata". Esse processo garante que o Suricata seja instalado a partir de um repositório confiável e atualizado, dessa forma, proporcionando segurança e estabilidade no ambiente de análise.

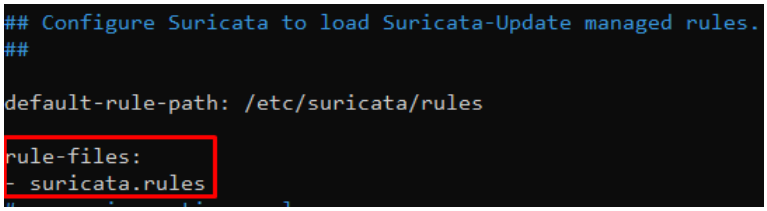
Figura 27 – Versão e Status do IDS suricata utilizado nos testes



Fonte: O autor.

Após a instalação do Suricata, foram realizados ajustes nos parâmetros necessários para rodar os arquivos de dataset. No arquivo de configuração, chamado suricata.yaml, foi configurado o caminho para a leitura das regras, conforme ilustrado na figura 28. Nesse caso, o caminho apontado foi /etc/suricata/rules. Essa configuração é recomendada para que o Suricata acesse as regras de detecção de intrusão e as aplique corretamente durante a análise dos arquivos de dataset.

Figura 28 – IDS suricata utilizado nos testes

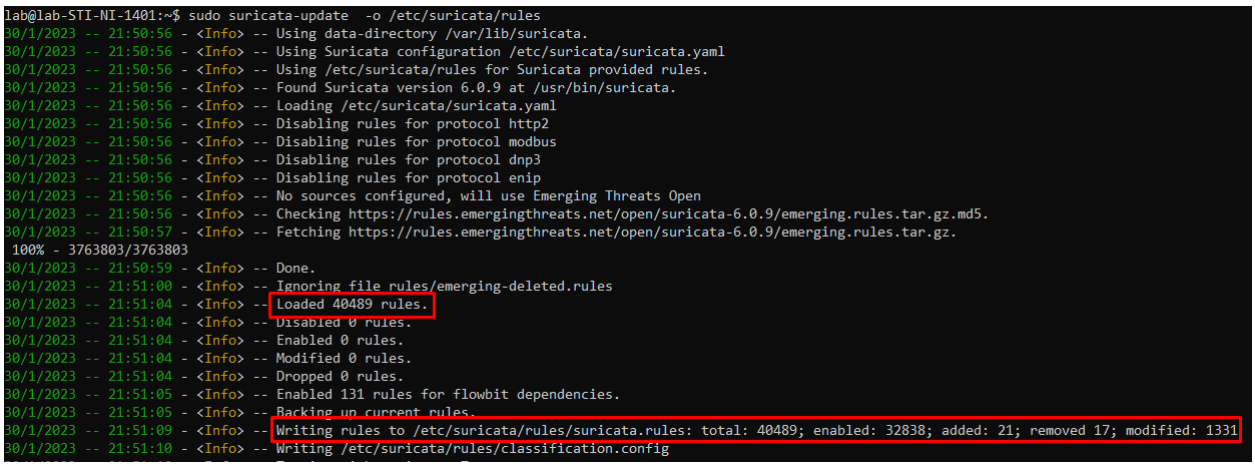


Fonte: O autor.

As regras pré-carregadas na instalação padrão do Suricata são limitadas e genéricas, tornando-as pouco eficientes em detectar ameaças específicas. Por esse motivo, é recomendável instalar ou criar regras mais abrangentes. Para o teste em questão, foram instaladas as regras Emerging Threat (ET) utilizando o comando "suricata-update", que baixa e instala as regras mais recentes. Para direcionar as regras ao diretório correto, utilizou-se o comando "suricata-update -o /etc/suricata/rules". Com isso, as regras mais abrangentes foram carregadas no diretório apropriado, permitindo o uso mais consistente do Suricata para detectar ameaças de forma mais precisa.

Execução do comando suricata-update, conforme figura 29, informa o total de regras baixadas — um total de 40.489 regras. Dessas, apenas 32.838 foram ativadas, 17 removidas e 1.331 modificadas..

Figura 29 – Atualização de regras do IDS suricata



Fonte: O autor.

Após realizar as configurações necessárias e configuração das regras, percebeu-se que o conjunto de logs e alertas reportados era muito grande. Por isso, foi conveniente limitar-se às regras para monitoramento apenas o protocolo DNS, e, dessa forma, baixou-se apenas o arquivo de regras emergentes para DNS, desabilitando o arquivo suricata.rules, deixando habilitadas apenas as regras para DNS. O conjunto de regras emergentes para o protocolo DNS forma um total de 29 regras habilitadas, as quais reportaram ataques

ao protocolo DNS, no entanto, logs diversos constavam no arquivo de log. Assim, para diminuir o escopo de busca e de logs, optou-se por habilitar apenas as 4 regras disponíveis para analisar DNS cache poisoning.

5.4 Aplicando o dataset ao IDS Suricata

Após instalar e configurar o IDS, submeteu-se o dataset.pcap às regras cadastradas. No primeiro teste, com 32.838 regras que foram ativadas durante a instalação das regras emergentes, submeteram-se os 5 arquivos pcap oriundos de 5 dias de monitoramento (segunda-feira a sexta-feira), resultando em 56.250 alertas. Esse total de alertas só foi possível devido ao grande número de protocolos monitorados, conforme regras cadastradas.

Em seguida, resolveu-se submeter os 5 arquivos PCAPS às 29 regras emergentes destinadas a ataques ao servidor DNS, e dessa forma foi possível diminuir o grande número de alertas reportados pelo IDS. Ao submeter esses arquivos às 29 regras, foram registrados menos logs de ataques ao servidor DNS. Até o momento, o arquivo de regras emergentes para DNS do IDS disponibilizado pela comunidade do Suricata não foi modificado.

Após a geração de diversos alertas de diferentes tipos de ataques ao servidor DNS, resolveu-se monitorar apenas os ataques de DNS cache poisoning. Para isso, optou-se por ativar apenas as regras que monitoram o DNS cache poisoning no arquivo "emerging-dns.rules".

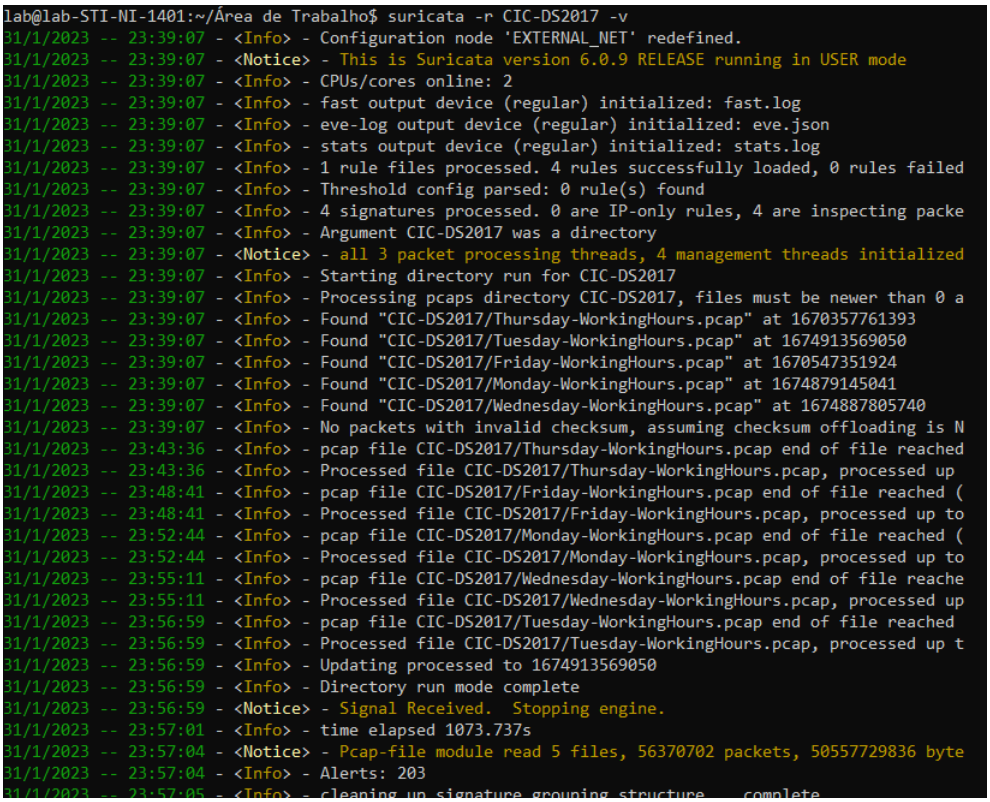
Figura 30 – Regras DNS cache poisoning

```
# This Ruleset is EmergingThreats Open optimized for suricata-5.0-enhanced.

alert udp any 53 -> $DNS_SERVERS any (msg:"ET DNS Excessive DNS Responses with 1 or more RR's (100+
in 10 seconds) - possible Cache Poisoning Attempt"; byte_test:2,>,0,6; byte_test:2,>,0,10; threshold
: type both, track by_src, count 100, seconds 10; reference:url,doc.emergingthreats.net/bin/view/Mai
n/2008446; classtype:bad-unknown; sid:2008446; rev:9; metadata:created_at 2010_07_30, updated_at 201
0_07_30;)

alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) -
possible A RR Cache Poisoning Attempt"; content: "|81 80 00 01 00 01 00 01|"; offset: 2; depth:8; th
reshold: type both, track by_src, count 50, seconds 2; reference:url,infosec20.blogspot.com/2008/07/
kaminsky-dns-cache-poisoning-poc.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008475;
classtype:bad-unknown; sid:2008475; rev:4; metadata:created_at 2010_07_30, updated_at 2010_07_30;)

alert udp any 53 -> $HOME_NET any (msg:"ET DNS Query Responses with 3 RR's set (50+ in 2 seconds) -
possible NS RR Cache Poisoning Attempt"; content: "|85 00 00 01 00 01 00 01|"; offset: 2; depth:8; t
hreshold: type both, track by_src,count 50, seconds 2; reference:url,infosec20.blogspot.com/2008/07/
kaminsky-dns-cache-poisoning-poc.html; reference:url,doc.emergingthreats.net/bin/view/Main/2008447;
classtype:bad-unknown; sid:2008447; rev:7; metadata:created_at 2010_07_30, updated_at 2010_07_30;)

alert udp any 53 -> $DNS_SERVERS any (msg:"ET DNS Excessive DNS Responses with 1 or more RR's (100+
in 10 seconds) to google.com.br possible Cache Poisoning Attempt"; byte_test:2,>,0,6; byte_test:2,>,
0,10; threshold: type both, track by_src, count 100, seconds 10; content:"|06|google|03|com|02|br|00
|"; reference:url,www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil; refe
rence:url,www.zdnet.com/blog/security/massive-dns-poisoning-attack-in-brazil-serving-exploits-and-ma
lware/9780; classtype:bad-unknown; sid:2013894; rev:5; metadata:created_at 2011_11_10, updated_at 20
11_11_10;)
```

Fonte: O autor

Ao submeter todos os arquivos às 4 regras de DNS cache poisoning, foi possível registrar 203 alertas. Dessa forma, gerou-se um conjunto de dados que servirá como prova de ataques ao servidor DNS. Esses logs foram salvos em um arquivo de log denominado "fast.log", que servirá como fonte de dados.

Figura 31 – Total de alertas gerados
com as Regras DNS cache poisoning



Fonte: O autor

Esses testes mostram que, dependendo da abordagem da equipe de segurança, é possível ter uma quantidade maior de eventos de invasão de redes registrados. Isso é útil porque, em um nível mais genérico de segurança de redes, onde são aplicadas regras diversas para monitorar a rede como um todo, essa abordagem pode levar a um grande número de alertas, o que pode exigir mais da equipe de monitoramento da segurança da rede.

Quando uma aplicação depende de um protocolo específico e essa aplicação é crucial para a instituição, ou seja, é o seu nicho de atuação, é recomendado que medidas mais direcionadas sejam tomadas para proteger os protocolos e os serviços que são suportados por eles. É importante ressaltar que a escolha da estratégia de segurança depende do contexto da instituição e dos riscos aos quais ela pode estar exposta.

Diante do exposto, vale apena reduzir o escopo de busca de uma ferramenta de monitoramento de redes para se obter apenas as informações necessária, ou seja, os logs e

alertas de violação de segurança que ela pretende monitorar.

É importante ressaltar que monitorar os demais serviços providos pela rede. Como mencionado na pesquisa, existem dois modelos de IDS: o de rede e o de host. O primeiro faz um monitoramento mais amplo, enquanto o segundo tem um monitoramento mais pontual. Dessa forma, é possível segmentar o monitoramento de tráfego de rede e, com isso, obter resultados mais úteis. A pesquisa tratou de ataques ao servidor DNS, por isso, restringiu as regras apenas ao DNS cache poisoning e, dessa forma, obteve-se um número bem menor de alertas.

5.5 Análise da Fonte de dados (fast.log)

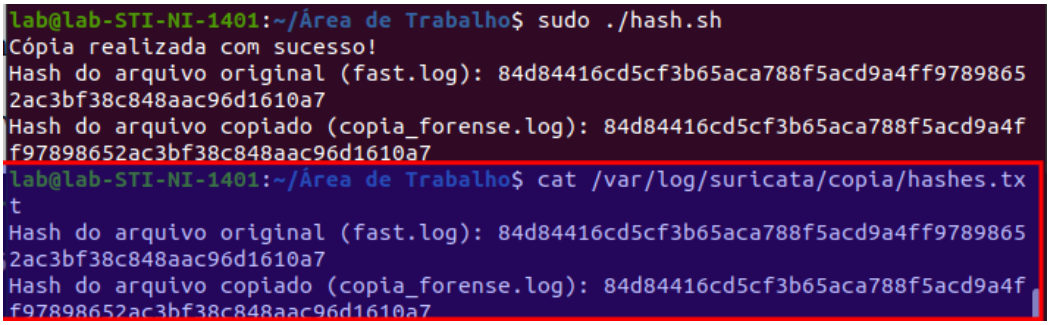
Com a obtenção da fonte de dados gerada pela ferramenta de monitoramento de rede IDS Suricata, adquiriram-se os insumos necessários para esta fase dos testes. Dessa forma, é possível submeter o arquivo de log (fast.log) à ferramenta forense FORDNS, que realizará uma análise minuciosa na fonte de dados em busca de evidências de crimes informáticos. Essas evidências serão processadas por um script que buscará por palavras-chave indicadas. Ao encontrá-las, as evidências serão devidamente armazenadas no banco de dados indicado no script.

No entanto, antes de prosseguir com os procedimentos de análise forense, é essencial seguir os preceitos da computação forense. De acordo com esses preceitos, é recomendado criar uma cópia da fonte de dados para garantir que a prova não seja comprometida. Essa medida de segurança envolve a geração de um hash, que atua como um carimbo legal.

Ao fazer uma cópia da fonte de dados e gerar um hash, estabelecendo um mecanismo de autenticação semelhante a uma autenticação em cartório, esse hash verifica e valida que os dados contidos na cópia refletem fielmente os dados originais. Dessa forma, a cópia do documento é respaldada e a credibilidade nela é garantida. Portanto, ao seguir os princípios da computação forense, estabeleceu-se uma base sólida para a análise forense, preservando a integridade das evidências coletadas e garantindo a validade dos resultados obtidos.

Para cumprir o pré-requisito de integridade exigido na computação forense, utilizou-se um script escrito em Bash. O objetivo desse script é gerar hashes tanto para o arquivo original quanto para a sua cópia, que, no caso, é o fast.log. Em seguida, os hashes gerados são comparados e, caso sejam idênticos, um arquivo contendo esses hashes é criado. Esse procedimento garante que a cópia do arquivo não sofreu alteração e está em conformidade com o original, conforme apresentado na figura 32.

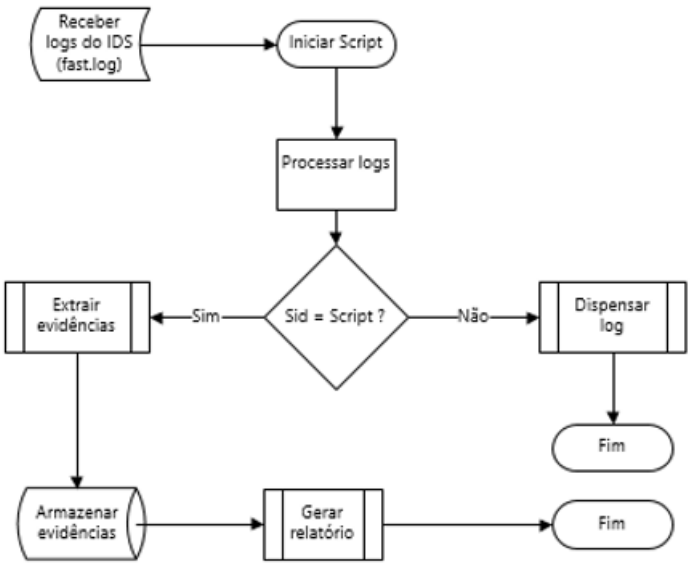
Figura 32 – Hash da fonte de dados original e copia



Fonte: O autor

A ferramenta FORDNS proposta neste trabalho possui um dos seus módulos implementado como um script na linguagem de programação Python, o qual é responsável pelo processamento e análise dos logs presentes no arquivo fast.log, conforme previamente descrito. Com o intuito de viabilizar a leitura e manipulação do arquivo de log do Suricata IDS (fast.log), desenvolveu-se a classe "Log Analyzer", em Python, com o objetivo específico de analisar o referido arquivo de log e extrair informações relevantes durante a análise forense. A figura 33 apresenta uma visão geral da ferramenta FORDNS ao analisar a fonte de dados.

Figura 33 – Visão geral da ferramenta FORDNS ao analisar a fonte de dados



Fonte: O autor

Durante a implementação dessa classe, diversas bibliotecas foram utilizadas para fornecer suporte funcional. Entre elas, destaca-se a biblioteca "re", a qual permite a utilização de expressões regulares. Outra biblioteca de relevância foi a "datetime", utilizada para registrar o momento em que a análise forense foi realizada no log, permitindo assim

que o horário de execução seja incluído no relatório final.

A classe "Log Analyzer"emprega dois métodos essenciais. O primeiro método é responsável por invocar o objeto que recebeu o nome do arquivo de log, possibilitando o registro dos logs gerados pela análise do IDS durante essa ocasião. O segundo método, por sua vez, é responsável pela leitura do arquivo e extração das evidências do delito quando ocorrerem correspondências definidas como parâmetros. A cada linha, são buscadas as palavras-chave ("1:20088446:9", "1:2008475:4", "1:2013894:5", "1:2008447:7") previamente repassadas como parâmetros. Caso sejam encontradas, as informações relevantes são extraídas para posterior análise.

A forma como o script foi desenvolvido permite que as informações presentes no arquivo de log sejam consideradas como uma única linha. Essa forma de separação dos logs, permite que os elementos essenciais para a análise (IP de origem, IP de destino, Porta de origem e destino, horário de início e fim do ataque, tipos de ataques, IDs das regras e outras informações) sejam identificados corretamente, pois não há variação da localização desses elementos.

Na ocasião, escolheram-se apenas os logs gerados durante a análise com as 4 assinaturas habilitadas no arquivo de regras do suricata, que retornou menos alertas. Para validar a ferramenta forense, indicou-se o arquivo de logs (fast.log) que será analisado pela ferramenta.

A busca realizada pela ferramenta visa ao rastreamento dos logs de violação ao servidor DNS com o fim de identificar endereço, informações necessárias para coletar evidências do crime. Caso os logs não correspondam ao conjunto de palavras-chave cadastradas, as informações desses logs são dispensadas.

5.5.1 Armazenamento das evidências no banco de dados

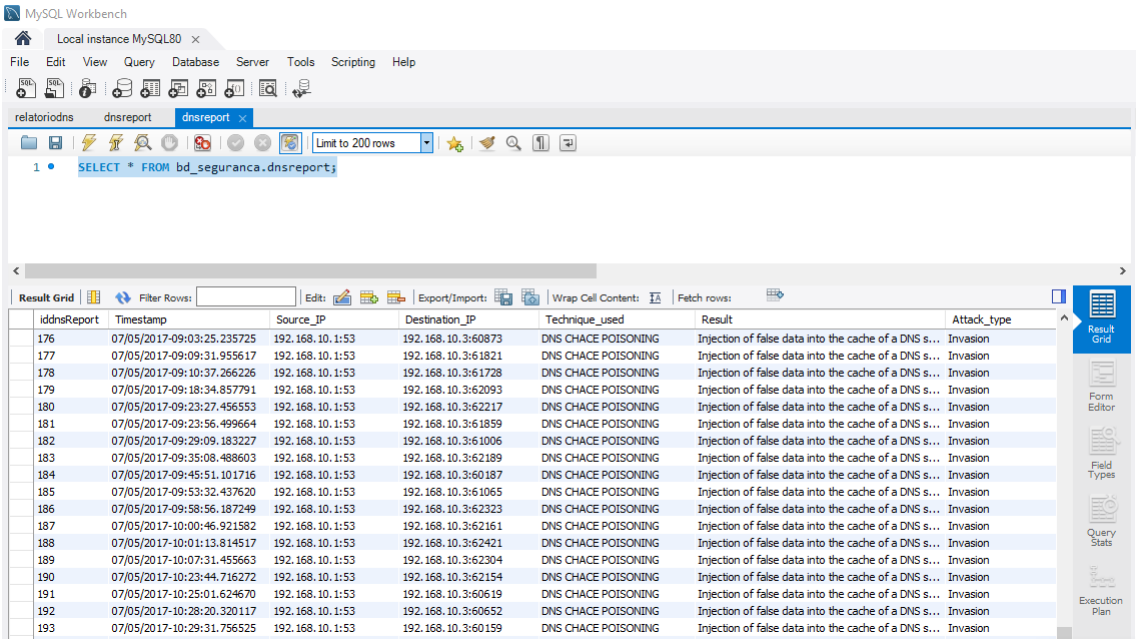
A organização e armazenamento adequados das evidências extraídas durante a análise forense são relevantes, pois possibilitam a geração de um histórico de informações da organização. Quando os dados são adequadamente organizados e analisados, é possível transformá-los em informações e conhecimento.

Conforme destaca Date (2004), qualquer informação pode ser armazenada, desde que faça sentido. Dessa forma, o armazenamento de informações de um delito computacional é extremamente relevante, pois pode auxiliar em procedimentos de investigação e manter uma base de dados pertinente.

Diante da necessidade de armazenar informações referentes a delitos de intrusão em redes de computadores, decidiu-se utilizar a ferramenta FORDNS. Essa ferramenta tem a capacidade de percorrer cada linha de log, encontrar a palavra-chave desejada, extrair os dados que lhe foram recomendados e armazenar no banco de dados. Dessa forma, é possível

extrair um relatório da análise forense realizada. O uso dessa ferramenta é relevante para garantir a eficácia das investigações e o armazenamento correto das informações.

Figura 34 – Banco de evidências



iddnsReport	Timestamp	Source_IP	Destination_IP	Technique_used	Result	Attack_type
176	07/05/2017-09:03:25.235725	192.168.10.1:53	192.168.10.3:60873	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
177	07/05/2017-09:09:31.955617	192.168.10.1:53	192.168.10.3:61821	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
178	07/05/2017-09:10:37.266226	192.168.10.1:53	192.168.10.3:61728	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
179	07/05/2017-09:18:34.857791	192.168.10.1:53	192.168.10.3:62093	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
180	07/05/2017-09:23:27.456553	192.168.10.1:53	192.168.10.3:62217	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
181	07/05/2017-09:23:56.499664	192.168.10.1:53	192.168.10.3:61859	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
182	07/05/2017-09:29:09.183227	192.168.10.1:53	192.168.10.3:61006	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
183	07/05/2017-09:35:08.488603	192.168.10.1:53	192.168.10.3:62189	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
184	07/05/2017-09:45:51.101716	192.168.10.1:53	192.168.10.3:60187	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
185	07/05/2017-09:53:32.437620	192.168.10.1:53	192.168.10.3:61065	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
186	07/05/2017-09:58:56.187249	192.168.10.1:53	192.168.10.3:62323	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
187	07/05/2017-10:00:46.921582	192.168.10.1:53	192.168.10.3:62161	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
188	07/05/2017-10:01:13.814517	192.168.10.1:53	192.168.10.3:62421	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
189	07/05/2017-10:07:31.455663	192.168.10.1:53	192.168.10.3:62304	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
190	07/05/2017-10:23:44.716272	192.168.10.1:53	192.168.10.3:62154	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
191	07/05/2017-10:25:01.624670	192.168.10.1:53	192.168.10.3:60619	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
192	07/05/2017-10:28:20.320117	192.168.10.1:53	192.168.10.3:60652	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
193	07/05/2017-10:29:31.756525	192.168.10.1:53	192.168.10.3:60159	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion

Fonte: O autor.

O armazenamento dos dados foi realizado por meio de um módulo, ou seja, uma classe específica da ferramenta FORDNS responsável pela conexão com o banco de dados e armazenamento das informações em uma tabela. Na ocasião, utilizou-se o gerenciador de banco de dados MySQL, por ser uma ferramenta open source e amplamente utilizada em ambientes empresariais, acadêmicos e outros

Essa base de dados guarda as informações dos ataques e possibilita a geração de um documento forense, para que, na judicialização do caso, sirva de material de prova, e, dessa forma, informe a técnica utilizada pelo criminoso. Tal procedimento é possível devido à forma como o IDS disponibiliza seus dados, permitindo a leitura do arquivo de logs.

De acordo comHintzbergen et al. (2018), a segurança da informação é uma área do conhecimento que visa proteger a informação contra ameaças que possam comprometer sua integridade, disponibilidade, confidencialidade, autenticidade e não-repúdio, independentemente da forma como ela é disponibilizada. No contexto em questão, lida-se com o armazenamento de informações extraídas de uma fonte de dados — na ocasião, os logs do IDS Suricata —, que serão conduzidos para um banco de dados para criar um repositório de dados de intrusão em redes de computadores. Para garantir que esses dados sejam autênticos e confiáveis, é necessário aplicar subterfúgios que os validem.

Para esse fim, existem dispositivos computacionais que podem validar esses dados.

Um dos métodos mais comuns, é a utilização de algoritmo de hashes. Ao gerar os hashes de um arquivo e sua cópia (cópia forense onde será feita a análise dos logs do IDS), é possível verificar de forma consistente que os dados armazenados durante a análise forense são confiáveis e foram armazenados de forma que possam ser utilizados em um processo de apuração de um delito. Com a manipulação correta da fonte de dados, assim como foi justificado, é possível replicar as informações por outros investigadores, pesquisadores ou qualquer outro interessado que ache necessária a verificação da informação.

No entanto, é importante ressaltar que a indicação de culpabilidade ou inocência do acusado é de responsabilidade do judiciário, e que os dados oriundos de um banco de dados relatados em um relatório forense são apenas um suporte técnico aos operadores do direito. É fundamental observar que os profissionais que lidam com esses dados devem ter habilidades em análise forense e segurança da informação para garantir a integridade e confiabilidade das evidências digitais.

5.6 Relatório Forense

Conforme menciona Martinelli (2013), o relatório é resultado de uma análise final de uma perícia forense que será apresentado durante um processo judicial. Geralmente, esse relatório é encaminhado pela equipe de profissionais do direito. Portanto, é fundamental que o relatório seja redigido em uma linguagem acessível às partes envolvidas no processo judicial.

Apesar da necessidade de um documento forense em linguagem bem acessível também é necessário apontar a forma como esse relatório foi gerado. Nesse ponto a abordagem FORDNS deixa isso bem claro, conforme explicado em tópicos anteriores.

Durante a análise forense realizada com a ferramenta FORDNS, foi possível obter informações cruciais, tais como o horário e o endereço IP do atacante, além de outras informações relevantes. Esses dados desempenham um papel fundamental, uma vez que os dispositivos em uma rede dependem de endereços IP para se comunicarem, seguindo as regras de roteamento. Além da identificação associada ao endereço IP, a análise permitiu a obtenção de outros dados que contribuíram para a compreensão do incidente e para a identificação do atacante.

Na análise forense, além da identificação do endereço IP, foram obtidas informações relevantes, como o tipo de ataque, no caso, DNS cache poisoning, e a identificação de uma invasão. Essas informações adicionais contribuíram para a compreensão do incidente e forneceram subsídios para a investigação em andamento. Além disso, a ferramenta FORDNS possibilitou uma análise ágil e segura, reduzindo significativamente o tempo necessário para uma investigação. Destaca-se também a capacidade de obter dados precisos e examinar um grande volume de logs, o que evidencia a eficácia e utilidade dessa ferramenta

Figura 35 – Relatório

ANÁLISE FORENSE (FORDNS)

Hash da fonte de dados: b39ec354e8541fc1ff02c24cc385143a8017556a5c2c461217d4cf5f9d8d64f0

Horário: 2023-07-14 09:52:25

Relatório forense

Na análise forense em questão, foram identificadas informações cruciais para a investigação do incidente, tais como o horário exato do ataque (timestamp), o endereço IP do atacante (Source IP), a porta de origem (source port), o alvo do ataque - endereço IP de destino (Destination IP) - e a porta de destino DNS (Destination Port). Com base nessas informações, foi possível identificar o tipo de ataque como DNS Cache Poisoning, que é considerado um delito de invasão de acordo com o artigo 154-A do Código Penal brasileiro. Vale ressaltar que a fonte de dados utilizada para este laudo forense foram os logs de rede, os quais foram capturados e analisados a partir do IDS Suricata, o qual tem a capacidade de detectar atividades suspeitas na rede, incluindo tentativas de invasão e ataques maliciosos.

EVIDÊNCIAS DO ATAQUE:

Timestamp: 2017-07-06 09:08:13.396930

Source IP: 192.168.10.1

Destination IP: 192.168.10.3

Source Port: 53

Destination Port: 62515

Técnica usada: DNS Cache Poisoning

Tipo de ataque: Invasion

Fonte de dados: logs do IDS Suricata (fast.log)

Violação do artigo 154-A do C.P

Fonte: O autor.

na condução de análises forenses.

Durante os experimentos com os datasets utilizados na pesquisa e no IDS Suricata, considerou-se que não houve ocorrência de falsos positivos ou negativos. Considerando-se que os logs de DNS cache poisoning foram reportados de acordo com as regras citadas. Dessa forma, é possível considerar que esses logs são confiáveis. As regras estabelecidas para análise de tráfego de rede pelo IDS Suricata são maduras e confiáveis, corroborando com a reputação do Suricata como um IDS conceituado na área de segurança de redes de computadores.

Outro ponto relevante a ser destacado é que os logs analisados foram gerados em um ambiente de teste, no qual foi utilizado um dataset público. Esse dataset foi submetido ao IDS (Sistema de Detecção de Intrusões) Suricata, que forneceu os dados necessários para validar a eficácia da ferramenta FORDNS. É importante ressaltar que o endereçamento IP utilizado nos testes corresponde a endereços privados, pois o objetivo era realizar as

análises em um ambiente de teste controlado, evitando qualquer impacto ou complicações durante a pesquisa.

Essa abordagem permitiu a obtenção de resultados confiáveis e a realização de validações adequadas da ferramenta, sem comprometer a segurança ou causar transtornos em ambientes de produção. Ao utilizar um dataset público e endereçamento IP privado, foi possível conduzir a análise de forma segura, explorando diferentes cenários de ataques e avaliando a capacidade da ferramenta em identificar e fornecer insights relevantes.

O trabalho em questão atingiu o objetivo, porém não esgota o assunto, pois existem margens para trabalhos futuros. Existe a possibilidade de adaptar a ferramenta para analisar outros tipos de ataques a redes de computadores ou até mesmo a outros tipos de invasão ao servidor DNS, algo que não foi possível fazer nesta dissertação.

6 Conclusão

A tecnologia da informação é indispensável na sociedade, abrangendo atividades simples e complexas, envolvendo software, hardware, dispositivos de rede e outros elementos. Entre as várias subáreas da computação, destaca-se a rede de computadores como uma das mais relevantes por sua capacidade de conectar recursos computacionais remotamente, contribuindo significativamente em atividades acadêmicas, empresariais, sociais, pessoais e outros.

Entretanto, a tecnologia está sob forte pressão de ataques cibernéticos, o que preocupa a sociedade. Para enfrentar essa agressão, há estudiosos que trabalham no fortalecimento dos sistemas computacionais, desenvolvendo artefatos capazes de resguardar o trânsito de informações e dados nas redes de computadores. Os crimes praticados nesses ambientes computacionais estão sendo combatidos e investigados com o objetivo de identificar os autores das infrações cometidas na internet. Diversos países estão criando leis mais rígidas para enfrentar as ameaças e os crimes cibernéticos.

No Brasil, em virtude de ser um grande alvo de criminosos cibernéticos, os legisladores melhoraram os dispositivos penais para serem mais duros com os criminosos cibernéticos. A pressão e os inúmeros casos de brasileiros sofrendo prejuízos de diversos tipos resultaram no endurecimento do sistema penal brasileiro. Com o fortalecimento de medidas judiciais capazes de punir mais severamente os criminosos computacionais, percebe-se a necessidade de desenvolver artefatos tecnológicos que possam tornar mais célere as investigações criminais destinadas a ataques cibernéticos.

Firewalls e IDSs alinham-se a essa tarefa de proteção e segurança. Na presença de uma tentativa ou de uma invasão a servidores de rede, o IDS identifica a atividade e a registra em um arquivo de histórico (log), tomando algumas decisões previamente configuradas.

Nesse contexto, foi desenvolvida uma abordagem forense com foco em ataques de invasão de dispositivos computacionais, especificamente a análise forense em ataques DNS, tendo como caso de uso o ataque de DNS cache poisoning. Para definir o caso de uso em questão, foi necessária uma pesquisa sobre a importância e as vulnerabilidades do protocolo DNS, que vem sofrendo diversos ataques. Dentre os diversos ataques estudados, escolheu-se o ataque de DNS cache poisoning como caso de uso, considerado um ataque de invasão, violando o artigo 154-A do Código Penal brasileiro.

Nesta abordagem utilizou-se uma ferramenta forense para extração dos dados fornecidos pelo IDS, a identificação da ocorrência de um ataque do tipo DNS Cache Poisoning, bem como a análise dos diversos elementos constitutivos do fato delituoso.

Possibilitando, ademais, o fornecimento de meios de prova, para investigações sobre o fato, sobre o autor, vítimas e consequências tecnológicas da invasão do (s) dispositivo (s). Para além disso, registra os dados em um banco de dados de evidências fornecido com a arquitetura e faz subsunção do tipo de ataque com a norma incriminadora que o prevê. Além disso, possibilita o registro das atividades do ataque por não especialistas em segurança de redes, preservando dados e servindo de histórico para futuras atualizações nos sistemas de segurança e proteção dos serviços de rede.

A pesquisa realizada possui uma grande importância e relevância no campo da análise forense e segurança de redes de computadores. Contribui para avançar o conhecimento nessa área, oferecendo uma abordagem sistemática e eficiente para a análise forense de ataques de invasão de servidores DNS. Com a utilização da abordagem proposta, é possível obter resultados mais precisos e confiáveis na investigação e resolução de incidentes de segurança cibernética.

A abordagem e o protótipo da ferramenta FORDNS, desenvolvida como parte da pesquisa, pode ser uma aliada para profissionais de segurança cibernética, investigadores forenses e operadores do direito. Ela fornece recursos específicos para a análise forense de ataques de DNS cache poisoning, auxiliando na coleta, organização e interpretação dos dados relevantes para a investigação.

Dessa forma, a pesquisa tem um impacto direto na prática, fornecendo uma ferramenta útil e eficaz para lidar com incidentes de segurança cibernética.

Além disso, a pesquisa contribui para o avanço do conhecimento na área de segurança cibernética como um todo. Ao propor uma abordagem inovadora para a análise forense de ataques de invasão de servidores DNS, ela expande o campo de possibilidades e estimula o desenvolvimento de novas técnicas e abordagens para enfrentar os desafios cada vez mais complexos da segurança cibernética.

6.1 Trabalhos Futuros

A pesquisa atual aponta para futuras investigações na área de segurança cibernética e análise forense, com ênfase na criação e melhoria de sistemas computacionais para agilizar investigações em ataques cibernéticos. Isso inclui o desenvolvimento de ferramentas inovadoras e soluções que tornem a coleta, análise e interpretação de dados mais eficientes e eficazes para profissionais de segurança cibernética.

Um caminho de pesquisa relevante envolve o aprimoramento de ferramentas de análise forense digital para identificar evidências digitais com maior precisão e rapidez. Isso requer o desenvolvimento de algoritmos avançados de busca e indexação de dados, além da implementação de técnicas de recuperação de informações em dispositivos e sistemas

afetados. Adicionalmente, a pesquisa pode se voltar para a automação de processos forenses, visando a eficiência ao lidar com tarefas repetitivas, resultando em economia de tempo e recursos.

Outro aspecto importante é a pesquisa em métodos de detecção de ameaças, incluindo sistemas de detecção de intrusões que identifiquem comportamentos maliciosos em tempo real por meio de análises de tráfego de rede e padrões de atividade suspeita, com uso de inteligência artificial e aprendizado de máquina para melhorar a precisão e reduzir falsos positivos.

A pesquisa futura pode analisar tendências e padrões em crimes cibernéticos para compreender as táticas de atacantes, contribuindo para estratégias mais eficazes de prevenção e resposta a incidentes.

6.2 Publicações

Esta dissertação resultou na publicação de um artigo científico da abordagem forense proposta, conforme indicado na tabela 4. O artigo foi publicado na Revista Científica Multidisciplinar Núcleo do Conhecimento, classificada como Qualis B1 em Ciência da Computação.

Tabela 4 – Artigo publicado em Revista Cientifica

Título	**Revista Científica**	**Qualis**
An Approach to Identification and Forensic Analysis of DNS Attacks (SOUSA; VALE, 2023)	Revista Científica Multidisciplinar Núcleo do Conhecimento	B1

Referências

ALHARBI, F.; CHANG, J.; ZHOU, Y.; QIAN, F.; QIAN, Z.; ABU-GHAZALEH, N. Collaborative client-side dns cache poisoning attack. In: IEEE. *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. 2019. p. 1153–1161. Disponível em: <https://ieeexplore.ieee.org/document/8737514>. Citado na página 18.

AQUINO, M. Grupo que atacou saúde diz ter sequestrado 50 terabytes de dados. *Metropoles*, 2021. Atualizado em 2021-12-10 às 13:56. Disponível em: <https://www.metropoles.com/brasil/grupo-que-atacou-saude-diz-ter-sequestrado-50-terabytes-de-dados>. Citado na página 18.

BATES, S.; ZITTRAIN, J.; BATES, S.; BOWERS, J. Evidence of decreasing internet entropy :. 2018. Disponível em: <https://www.nber.org/system/files/working_papers/w24317/w24317.pdf>. Citado na página 33.

BR, C. Cartilha de segurança para internet. 2012. v. 4, p. 142, 2012. ISSN 978-85-60062-54-6. Disponível em: <https://www.nic.br/media/docs/publicacoes/1/cartilha-seguranca-internet.pdf>. Citado na página 34.

BRASIL. *lei nº 2.848, de 7 de dezembro de 1940*. 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Citado 2 vezes nas páginas 50 e 57.

BRASIL. *Lei nº 12.737, de 30 de Novembro de 2012*. 2012. Diário Oficial da União. 03 de Dezembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Citado na página 57.

BRASIL. *Lei nº 14.155, de 27 de maio de 2021*. 2021. Diário Oficial da União. 27 de maio de 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm>. Citado na página 57.

CANTANHEDE, H. N. F.; VALE, S. B. Computer network forensics assistance methodology focused on denial of service attacks. *International Journal of Computer Applications*, v. 975, p. 887, 2020. Disponível em: <http://www.ijcaonline.org/archives/volume177/number33/cantanhede-2020-ijca-919788.pdf>. Citado 4 vezes nas páginas 19, 24, 26 e 27.

CARDOSO, A. M. d. S. CEPIDS: Um IDS baseado no Processamento de Eventos Complexos para Internet de Coisas. 2018. Disponível em: <https://tedebc.ufma.br/jspui/handle/tede/2360>. Citado 3 vezes nas páginas 19, 25 e 26.

CARVALHO, H. C. F. B.; PELLI, E. Técnicas de reconhecimento de padrões para identificação de ataque de dns. *Revista Brasileira de Computação Aplicada*, v. 9, n. 2, p. 99–110, 2017. Disponível em: <https://doi.org/10.5335/rbca.v9i2.6279>. Citado na página 35.

CHUNG, T.; RIJSWIJK-DEIJ, R. van; CHANDRASEKARAN, B.; CHOFFNES, D.; LEVIN, D.; MAGGS, B. M.; MISLOVE, A.; WILSON, C. A longitudinal, end-to-end view of the {DNSSEC} ecosystem. In: *26th {USENIX} Security*

Symposium ({USENIX} Security 17). [s.n.], 2017. p. 1307–1322. Disponível em: <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-chung.pdf>. Citado na página 41.

CUNHA, T. F. M. D. *Detecção de falsos alertas de intrusão em redes de computadores*. 2019. Acesso em: 15 de maio de 2023. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/64480/1/62026-Dissertacao%2bde%2bMestrado_TiagoCunha.pdf>. Citado na página 64.

DATE, C. *Introdução a sistemas de bancos de dados*. ELSEVIER EDITORA, 2004. ISBN 9788535212730. Disponível em: <https://books.google.com.br/books?id=xBeO9LSlK7UC>. Citado na página 72.

ELEUTÉRIO, P. da S.; MACHADO, M. *Desvendando a Computação Forense*. Novatec Editora, 2019. ISBN 9788575227879. Disponível em: <https://books.google.com.br/books?id=jS2oDwAAQBAJ>. Citado 2 vezes nas páginas 43 e 47.

ESR, E. S. *Segurança de Redes e Sistemas*. [S.l.]: Escola Superior de Redes - ESR, 2019. Citado na página 32.

GALVÃO, R. K. M. *Introdução à Análise Forense em Redes de Computadores: Conceitos, Técnicas e Ferramentas para"Grampos Digitais"*. [S.l.]: Novatec Editora, 2018. Citado 5 vezes nas páginas 43, 44, 45, 46 e 47.

GOUVÊA, G. M. d. Crimes informáticos à luz da lei n° 14.155 de 2021. 2022. Citado na página 57.

GRAJEDA, C.; BREITINGER, F.; BAGGILI, I. Availability of datasets for digital forensics – and what is missing. *Digital Investigation*, v. 22, p. S94–S105, 2017. ISSN 1742-2876. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1742287617301913>. Citado na página 63.

HARAN, J. M. *Ataques DNS hijacking em roteadores são usados para baixar um app falso sobre a Covid-19*. 2020. Disponível em:<https://www.welivesecurity.com/br/2020/03/26/>. Acesso em: 01 de fevereiro 2022. Citado na página 18.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. Brasport, 2018. ISBN 9788574528601. Disponível em: <https://books.google.com.br/books?id=1CVFDwAAQBAJ>. Citado 3 vezes nas páginas 28, 57 e 73.

HMOOD, H. S.; LI, Z.; ABDULWAHID, H. K.; ZHANG, Y. Adaptive caching approach to prevent dns cache poisoning attack. *The Computer Journal*, Oxford University Press, v. 58, n. 4, p. 973–985, 2015. Citado 2 vezes nas páginas 18 e 35.

HOUSER, R.; HAO, S.; LI, Z.; LIU, D.; COTTON, C.; WANG, H. A comprehensive measurement-based investigation of dns hijacking. In: IEEE. *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*. [S.l.], 2021. p. 210–221. Citado 5 vezes nas páginas 17, 23, 26, 31 e 38.

IBM. What is a data set? 2021. Accessed on April 6, 2023. Disponível em: <https://www.ibm.com/docs/en/zos-basic-skills?topic=more-what-is-data-set>. Citado na página 63.

JESUS, D. de. *Manual de Crimes Informáticos*. Saraiva Educação S.A., 2017. ISBN 9788502627246. Disponível em: <https://www.amazon.com.br/Manual-Inform%C3%A1ticos-ANTONIO-MILAGRE-OLIVEIRA-ebook/dp/B076CL4WVX/ref=sr_1_1?___mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=MQI18Z94QRZ5&keywords=Manual+de+Crimes+Inform%C3%A1ticos&qid=1677810102&s=digital-text&sprefix=manual+de+crimes+inform%C3%A1ticos+%2Cdigital-text%2C396&sr=1-1>. Citado na página 57.

KAMINSKY, D. Black ops 2008: It's the end of the cache as we know it. *Black Hat USA*, v. 2, 2008. Citado na página 37.

KENT, K.; CHEVALIER, S.; GRANCE, T. Guide to integrating forensic techniques into incident. *Tech. Rep. 800-86*, 2006. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>. Citado 2 vezes nas páginas 44 e 45.

KHAN, R.; HASAN, M. Network threats, attacks and security measures: A review. *International Journal of Advanced Research in Computer Science*, v. 8, n. 8, 2017. Citado na página 41.

KHRAISAT, A.; GONDAL, I.; VAMPLEW, P.; KAMRUZZAMAN, J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, Springer, v. 2, n. 1, p. 1–22, 2019. Disponível em: <https://doi.org/10.1186/s42400-019-0038-7>. Citado na página 57.

KIM, T. H.; REEVES, D. A survey of domain name system vulnerabilities and attacks. *Journal of Surveillance, Security and Safety*, OAE Publishing Inc., v. 1, n. 1, p. 34–60, 2020. Disponível em: <https://jsssjournal.com/article/view/3660>. Citado 13 vezes nas páginas 17, 19, 23, 26, 29, 30, 32, 33, 34, 35, 37, 49 e 60.

LENCSE, G. Benchmarking authoritative dns servers. *IEEE Access*, IEEE, v. 8, p. 130224–130238, 2020. Citado na página 29.

LISKA, A.; STOWE, G. *DNS Security: Defending the Domain Name System*. Elsevier Science, 2016. ISBN 9780128033067. Disponível em: <https://books.google.com.br/books?id=MNNhrgEACAAJ>. Citado 3 vezes nas páginas 18, 31 e 32.

MARTINELLI, V. *Introdução à Computação Forense - Teoria e visão prática: 1ª Edição*. Bookmakers, 2013. 88 p. ISBN 978-85-65242-47-9. Disponível em: <https://www.amazon.com.br/Introdu%C3%A7%C3%A3o-Computa%C3%A7%C3%A3o-Forense-Teoria-pr%C3%A1tica-ebook/dp/B097652X7T>. Citado 4 vezes nas páginas 45, 46, 47 e 74.

MENDES, D. *Redes de Computadores: Teoria e Prática*. Novatec Editora, 2020. ISBN 9786586057164. Disponível em: <https://books.google.com.br/books?id=TWrjDwAAQBAJ>. Citado na página 31.

Ministério Público Federal. *Brasil aprova adesão à Convenção de Budapeste, que facilita cooperação internacional para combate ao cibercrime*. 2021. <https://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-de-budapeste-que-facilita-cooperacao-internacional-para-combate-a
Acesso em: 26 mar. 2023. Citado na página 48.

MORAES, A. D. *Firewalls Segurança no controle de acesso*. Saraiva Educação S.A., 2021. ISBN 9788536515083. Disponível em: <https://www.amazon.com.br/Ciberseguran%C3%A7a-gera%C3%A7%C3%A3o-Firewalls-Alexandre-Fernandes-ebook/dp/B08Y5TKDF7/ref=sr_1_1?___mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=36VV7UUN6EB44&keywords=firewall&qid=1677727219&s=books&sprefix=firewall%2Cstripbooks%2C227&sr=1-1>. Citado na página 42.

NAQASH, T.; UBAID, F. B.; ISHFAQ, A. et al. Protecting dns from cache poisoning attack by using secure proxy. In: IEEE. *2012 International Conference on Emerging Technologies*. [S.l.], 2012. p. 1–5. Citado na página 18.

NETO, H.; ÁVILA, C.; LACERDA, W. Sistema de detecção de intrusão em redes de computadores utilizando redes neurais artificiais. In: SBC. *Anais do XIII Simpósio Brasileiro de Sistemas de Informação*. 2017. p. 206–213. Disponível em: <https://sol.sbc.org.br/index.php/sbsi/article/view/6044>. Citado 2 vezes nas páginas 42 e 50.

OETTINGER, W. *Aprenda Computação Forense: Um guia para iniciantes para buscar, analisar e proteger evidências digitais*. Novatec Editora, 2021. ISBN 9786586057553. Disponível em: <https://books.google.com.br/books?id=iG8sEAAAQBAJ>. Citado na página 45.

Open Information Security Foundation. *Suricata IDS V.6*. 2016. Disponível em <https://suricata.io/features/>. Acesso em 6 de julho de 2022. Citado 2 vezes nas páginas 50 e 64.

Open Information Security Foundation. *Suricata IDS V.6*. 2023. Disponível em <https://suricata.io/features/>. Acesso em 6 de julho de 2023. Citado na página 64.

PACHECO, A. *Crimes digitais: responsabilização penal de hackers, crackers e engenheiros sociais*. [S.l.]: eBook Kindle, 2020. Citado na página 43.

PILLI, E. S.; JOSHI, R.; NIYOGI, R. Network forensic frameworks: Survey and research challenges. *Digital Investigation*, v. 7, n. 1, p. 14–27, 2010. ISSN 1742-2876. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1742287610000113>. Citado na página 44.

RADWARE, T. R. C. *DNS Hijacking Targets Brazilian Banks*. 2018. Disponível em:<https://www.radware.com/security/ddos-threats-attacks/threat-advisories-attack-reports/dns-hijacking-brazil-banks/>. Acesso em: 07 de maio 2022. Citado 2 vezes nas páginas 38 e 40.

RAMDAS, A.; MUTHUKRISHNAN, R. A survey on dns security issues and mitigation techniques. In: IEEE. *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*. 2019. p. 781–784. Disponível em: <https://ieeexplore.ieee.org/abstract/document/9065354>. Citado 2 vezes nas páginas 30 e 39.

SHARAFALDIN, I.; LASHKARI, A. H.; GHORBANI, A. A. Intrusion detection evaluation dataset (cic-ids2017). *Proceedings of the of Canadian Institute for Cybersecurity*, 2018. Disponível em: <https://www.unb.ca/cic/datasets/ids-2017.html>. Citado 2 vezes nas páginas 63 e 64.

SILVA, L. C.; VALE, S. A methodology for network security infrastructure according to the new brazilian general law for personal data protection. *International Journal of Computer Applications*, v. 183, n. 07, p. 2021, 2021. Disponível em: <https://www.ijcaonline.org/archives/volume183/number17/silva-2021-ijca-921520.pdf>. Citado na página 41.

SILVA, P. a. da. *Passo a Passo: DNS e DNSSec*. Amazon Edição do Kindle, 2021. Disponível em: <https://www.amazon.com.br/Passo-DNSSec-Priscila-Silva-Alves-ebook/dp/B08SQNVVNC/ref=sr_1_1?qid=1678453344&refinements=p_27%3APriscila++da+Silva+Alves&s=digital-text&sr=1-1&text=Priscila++da+Silva+Alves>. Citado na página 29.

SILVA, W. d. V. R. da; ADELINO, M. A.; SILVA, M. V. da; SILVA, F. C. da; SILVA-MANN, R. Análise da produção científica e tecnológica acerca da ciência forense digital. *Research, Society and Development*, v. 9, n. 11, p. e45391110224–e45391110224, 2020. Citado na página 43.

SOUSA, R. E.; VALE, S. An approach to identification and forensic analysis of dns attacks. *Revista Científica Multidisciplinar Núcleo do Conhecimento*, v. 01, n. 07, p. 24–44, July 2023. ISSN 2448-0959. Disponível em: <https://www.nucleodoconhecimento.com.br/computer-science/forensic-analysis>. Citado na página 79.

STALLINGS, W. *Criptografia e segurança de redes: princípios e práticas*. 6th. ed. São Paulo: Pearson Education do Brasil, 2015. ISBN 978-85-430-1450-0. Citado na página 28.

STUDIAWAN, H.; SOHEL, F.; PAYNE, C. A survey on forensic investigation of operating system logs. *Digital Investigation*, Elsevier Ltd, v. 29, p. 1–20, 2019. ISSN 17422876. Disponível em: <https://doi.org/10.1016/j.diin.2019.02.005>. Citado 2 vezes nas páginas 23 e 26.

TANENBAUM, A.; FEAMSTER, N.; WETHERALL, D. *Redes de Computadores (coedição Bookman e Pearson)*. Bookman Editora, 2021. ISBN 9788582605615. Disponível em: <https://books.google.com.br/books?id=DNFJEAAAQBAJ>. Citado 6 vezes nas páginas 29, 30, 37, 40, 41 e 42.

TORRES, G. *Redes de computadores*. [S.l.]: Novaterra Editora e Distribuidora LTDA, 2014. Citado 3 vezes nas páginas 31, 42 e 43.

TRIPATHI, N.; SWARNKAR, M.; HUBBALLI, N. Dns spoofing in local networks made easy. In: IEEE. *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. 2017. p. 1–6. Disponível em: <https://ieeexplore.ieee.org/abstract/document/8384122>. Citado na página 36.

VAZ, G. M.; RIZZETTI, T. A.; FILHO, W. P. Um estudo de caso sobre a implantação de um ambiente de prevenção de intrusões com a ferramenta suricata. In: SBC. *Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. 2021. p. 256–263. Disponível em: <estudodecasosobreaimplantaç~aodeumambientedeprevenç~aodeintrus~oescomaferramentasuricata.> Citado na página 19.

VAZAO, A. P. H. *Implementação de sistema SIEM open-source em conformidade com o RGPD*. Dissertação (Mestrado) — Escola Superior de Tecnologia e Gestão, Instituto Politécnico, 2021. Disponível em: <http://hdl.handle.net/10400.8/5567>. Citado 2 vezes nas páginas 24 e 26.

WALEED, A.; JAMALI, A. F.; MASOOD, A. Which open-source ids? snort, suricata or zeek. *Computer Networks*, Elsevier, v. 213, p. 109116, 2022. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1389128622002420?casa_token=AlAegfOxyXgAAAAA:gdR9-Gz4n24axSwJ0hQAAOQyU0k1cSIFEmEDK00B4q6NigdcXzPmvCbO4n9RjwnjvvDaIZIR6R2D> Citado na página 58.

WANG, Z. Poster: on the capability of dns cache poisoning attacks. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. [s.n.], 2014. p. 1523–1525. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/2660267.2662363?casa_token=owTpt53Om_QAAAAA:ePU01iIrGaIe846Ro8BEYjH8VJ0tDJYqXlzk6ZRZ-rI3K2kD_4WCjC8ra5s6ViY-dKEUB-GOPbImSi8>. Citado 2 vezes nas páginas 35 e 37.

WAZLAWICK, R. S. *Metodologia de Pesquisa para Ciência da Computação*. 3rd. ed. [S.l.]: GEN LTC, 2020. 152 p. Livro de bolso. ISBN 9788595151093, 8595151091. Citado 2 vezes nas páginas 22 e 23.

WENDT, E.; JORGE, H. *Crimes Cibernéticos 3a edição: ameaças e procedimentos de investigação*. Brasport, 2021. ISBN 9786588431382. Disponível em: <https://books.google.com.br/books?id=V1FFEAAAQBAJ>. Citado 2 vezes nas páginas 46 e 48.

ZHANG, H.; YE, J.; HU, W.; WANG, Q.; YAN, X.; YUE, Q.; LV, W.; HE, M.; WANG, J. Study on the latent state of kaminsky-style dns cache poisoning: Modeling and empirical analysis. *Computers Security*, v. 110, p. 1–15, 2021. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404821002698>. Citado 9 vezes nas páginas 17, 24, 26, 37, 38, 39, 58, 60 e 61.

A Apêndice

A.1 FORDNS

Listing A.1 – Trecho do Código Fonte: FORDNS

```
class LogAnalyzer:
    def __init__(self, log_file):
        self.log_file = log_file
        self.log_pattern = re.compile(
            r'^(.*?)\s+\[\*\*\]\s+\[(.*?)\]\s+(.*?)\s+\[\*\*\]\s
               +\[(.*?)\]\s+\[(.*?)\]\s+\{(\w+)\}\s+(.*?):(\d+)\s
               +->\s+(.*?):(\d+)\s*$'
        )
        self.info_list = []

    def read_log_file(self):
        with open(self.log_file) as f:
            log_lines = f.readlines()

        for line in log_lines:
            if any(keyword in line for keyword in ['1:2008446:9',
                '1:2008475:4', '2008447', '1:2013894:5']):
                match = self.log_pattern.match(line.strip())
                timestamp = datetime.strptime(match.group(1), '%m
                   /%d/%Y-%H:%M:%S.%f')
                src_ip = match.group(7)
                dest_ip = match.group(9)
                src_port = int(match.group(8))
                dest_port = int(match.group(10))
                data = datetime.now()

                info = {'timestamp': timestamp, 'src_ip': src_ip,
                    'dest_ip': dest_ip, 'src_port': src_port,
                        'dest_port': dest_port, 'data': data}
                self.info_list.append(info)
```

A.2 DOCUMENTO FORENSE (RELATÓRIO)

ANÁLISE FORENSE (FORDNS)

Hash da fonte de dados: b39ec354e8541fc1ff02c24cc385143a8017556a5c2c461217d4cf5f9d8d64f0

Horário: 2023-07-14 09:52:25

Relatório forense

Na análise forense em questão, foram identificadas informações cruciais para a investigação do incidente, tais como o horário exato do ataque (timestamp), o endereço IP do atacante (Source IP), a porta de origem (source port), o alvo do ataque - endereço IP de destino (Destination IP) - e a porta de destino DNS (Destination Port). Com base nessas informações, foi possível identificar o tipo de ataque como DNS Cache Poisoning, que é considerado um delito de invasão de acordo com o artigo 154-A do Código Penal brasileiro. Vale ressaltar que a fonte de dados utilizada para este laudo forense foram os logs de rede, os quais foram capturados e analisados a partir do IDS Suricata, o qual tem a capacidade de detectar atividades suspeitas na rede, incluindo tentativas de invasão e ataques maliciosos.

EVIDÊNCIAS DO ATAQUE:

Timestamp: 2017-07-06 09:08:13.396930

Source IP: 192.168.10.1

Destination IP: 192.168.10.3

Source Port: 53

Destination Port: 62515

Técnica usada: DNS Cache Poisoning

Tipo de ataque: Invasion

Fonte de dados: logs do IDS Suricata (fast.log)

Violação do artigo 154-A do C.P

ANÁLISE FORENSE (FORDNS)

Hash da fonte de dados: b39ec354e8541fc1ff02c24cc385143a8017556a5c2c461217d4cf5f9d8d64f0

Horário: 2023-07-14 09:52:25

Relatório forense

Na análise forense em questão, foram identificadas informações cruciais para a investigação do incidente, tais como o horário exato do ataque (timestamp), o endereço IP do atacante (Source IP), a porta de origem (source port), o alvo do ataque - endereço IP de destino (Destination IP) - e a porta de destino DNS (Destination Port). Com base nessas informações, foi possível identificar o tipo de ataque como DNS Cache Poisoning, que é considerado um delito de invasão de acordo com o artigo 154-A do Código Penal brasileiro. Vale ressaltar que a fonte de dados utilizada para este laudo forense foram os logs de rede, os quais foram capturados e analisados a partir do IDS Suricata, o qual tem a capacidade de detectar atividades suspeitas na rede, incluindo tentativas de invasão e ataques maliciosos.

EVIDÊNCIAS DO ATAQUE:

Timestamp: 2017-07-06 09:11:13.134320

Source IP: 192.168.10.1

Destination IP: 192.168.10.3

Source Port: 53

Destination Port: 62135

Técnica usada: DNS Cache Poisoning

Tipo de ataque: Invasion

Fonte de dados: logs do IDS Suricata (fast.log)

Violação do artigo 154-A do C.P