UMA ABORDAGEM PARA IDENTIFICAÇÃO E ANÁLISE FORENSE DE ATAQUES DNS

ARTIGO ORIGINAL

SOUSA, Robson Everton[1], VALE, Samyr[2]

SOUSA, Robson Everton. VALE, Samyr. **Uma abordagem para identificação e análise forense de ataques DNS**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano. 08, Ed. 07, Vol. 01, pp. 24-44. Julho de 2023. ISSN: 2448-0959, link de acesso: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense, doi: 10.32749/nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense

RESUMO

Os servidores de resolução de nomes de domínio (DNS) desempenham uma função chave no estabelecimento de acesso a páginas da web. Devido à sua importância, eles são alvos constantes de ciberataques, que visam apagar ou substituir alguns de seus registros, causando enormes prejuízos para usuários, empresas e instituições em todo o mundo. No Brasil, para prevenir tais ataques, é estabelecida uma disposição legal que tipifica criminalmente a invasão de dispositivos de computador conectados à *World Wide Web*, o que inclui ataques ao serviço de DNS. Ainda assim, a identificação de ciberataques é difícil, pois depende da aplicação correta de meios de proteção, monitoramento de serviços de rede e extração e interpretação de dados que permitem a identificação de elementos criminosos. O presente trabalho propõe uma abordagem de informática forense para detectar automaticamente a ocorrência de um ataque de envenenamento de cache DNS, subsumindo os elementos que constituem o ataque ao dispositivo legal, identificando assim a ocorrência de um crime.

Palavras-chave: Informática forense, Crimes de computador, Redes de computadores.

1. INTRODUÇÃO

Os servidores de resolução de nomes de domínio (DNS) são uma das infraestruturas mais importantes da Internet que mapeiam as conexões entre o nome de domínio (URL) e o endereço de protocolo de Internet (IP) (Wang, Zang e Lan, 2018). Apesar

de sua grande importância, ele apresenta falhas porque algumas questões de segurança foram negligenciadas durante a sua criação.

Os ataques ao DNS são bastante recorrentes; 92% das redes analisadas estão sujeitas a pelo menos um tipo de envenenamento de cache de DNS (Alharbi *et al*., 2019). Isso foi corroborado ao avaliar 97% dos *resolvers* em operação aberta, 74% das redes corporativas por meio de servidores de e-mail e 68% dos Provedores de Serviços de Internet (ISP) medidos por meio de anúncios de rede.

Embora ferramentas de segurança e proteção de rede, como sistemas de detecção de intrusões (IDS), monitorem a atividade e o tráfego da rede, incluindo possíveis ataques, esses registros são armazenados em arquivos de log internos e constantemente atualizados de forma dinâmica. Normalmente, os dados gerados ali permanecem não processados, atuando apenas como informações de ocorrência de eventos para administradores de rede. Muitas vezes, quando ataques repetidos são detectados, os registros de atividades de invasão são invariavelmente perdidos no meio do grande volume de informações gerado por essas ferramentas. Isso ocorre porque elas não são destinadas a realizar investigações forenses, mas apenas a proteger o tráfego de dados.

A abordagem proposta tem como objetivo identificar as características de um crime de intrusão de dispositivo de computador, particularmente ataques a servidores DNS, para reconhecer a invasão e aplicar as leis criminais apropriadas.

Uma vez feito isso, a abordagem propõe registrar a prova de ocorrência de um ataque em um documento elaborado por um especialista qualificado. Em seguida, esses dados podem ser analisados e interpretados para determinar se o tráfego de dados em um servidor DNS é uma atividade padrão ou uma tentativa de invasão. Para isso, os desastres de rede notificados pelo IDS são analisados para identificar o atacante, a técnica de invasão utilizada, o endereço IP de origem e destino, horário da ocorrência do ataque, serviços de computador afetados e o alcance do dano causado.

O restante deste artigo está estruturado da seguinte forma. A seção II descreve o contexto tecnológico do estudo atual; a seção III apresenta trabalhos relacionados na literatura e suas deficiências; a seção IV aborda a análise forense usando ferramentas de DNS; e, finalmente, a seção V apresenta as conclusões.

2. PAISAGEM TECNOLÓGICA

De acordo com Lencse (2020), o DNS (Sistema de Nomes de Domínio) é um recurso tecnológico importante capaz de dar suporte extenso à *World Wide Web*, sendo imperceptível quando está funcionando corretamente. No entanto, quando ocorre uma falha, a desaceleração que afeta a qualidade do serviço rapidamente se torna perceptível.

Conforme mencionado por Naqash *et al*. (2012), a arquitetura do DNS não incluiu os critérios de segurança necessários para bloquear a recepção de dados falsificados no cache do servidor DNS. Hmood *et al.* (2015) e Steinho, Wiesmaier e Araújo (2006) mencionam que criminosos exploram essa vulnerabilidade inserindo informações falsificadas no cache dos servidores DNS e alterando parâmetros de referência para torná-lo indisponível ou redirecionar o tráfego para páginas maliciosas. Esses parâmetros podem ser alterados de recursivo para autoritário durante o fluxo de consulta.

2.1 TÉCNICAS E ATAQUES NO DNS

Kim e Reeves (2020) descrevem os ataques a servidores DNS como atos de adulteração de dados, inundação, abuso de DNS e estrutura de servidor DNS contrária. Essa classificação permite analisá-los por áreas de acordo com os diferentes interesses dos atacantes. O presente trabalho tem como objetivo analisar o envenenamento de cache DNS, que, de acordo com Kim e Reeves (2020), se enquadra no modo de adulteração de dados.

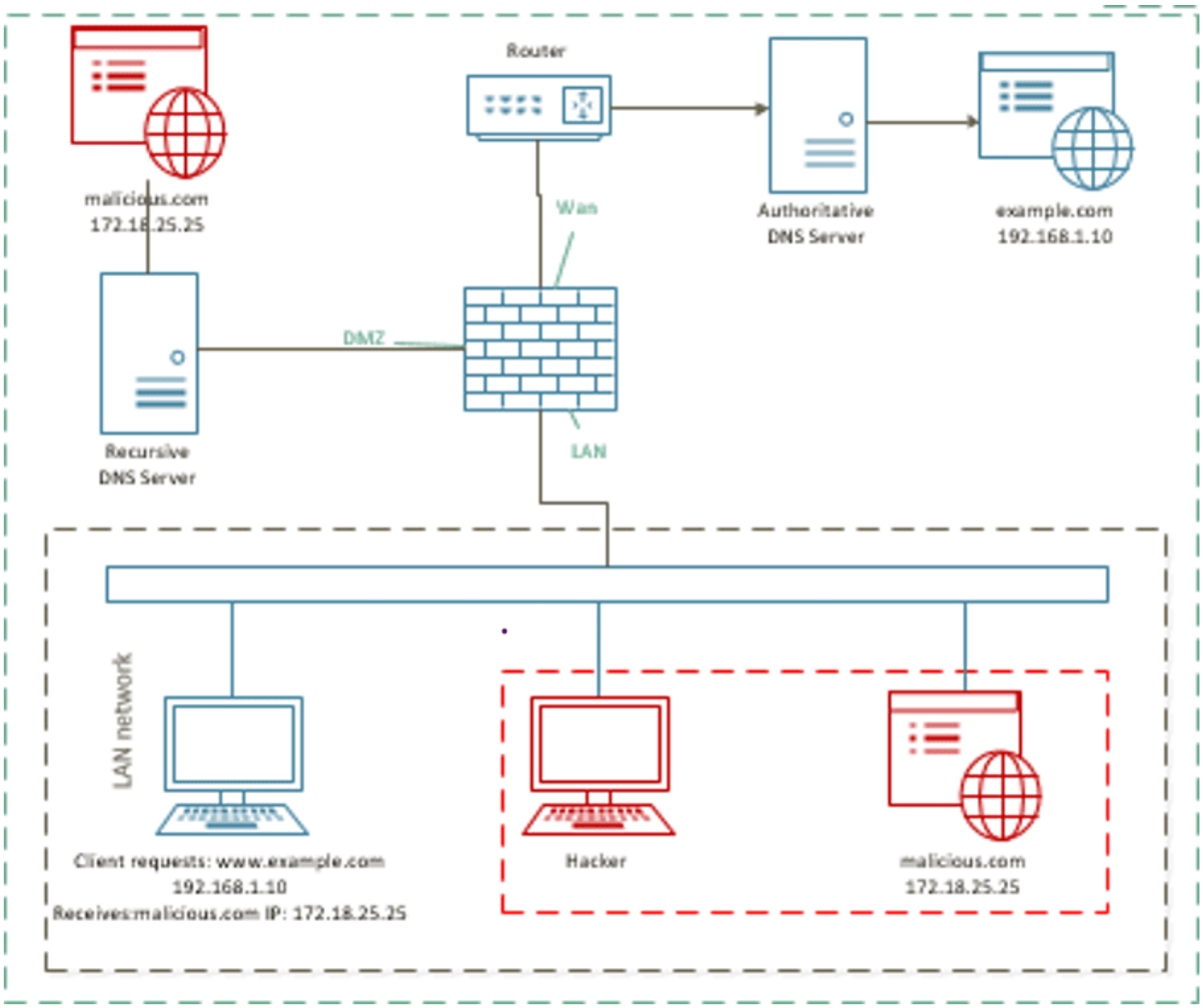
Zhang *et al.* (2021) e Kaminsky *et al.* (2008) mencionam que um dos primeiros casos de envenenamento de cache DNS foi descoberto por Kaminsky em 2008. Ao contrário

do envenenamento de cache local, o envenenamento de cache DNS pode ser realizado remotamente. De acordo com Tripathi, Swarnkare e Hubballi (2018), o envenenamento de cache local é mais simples de implementar do que o envenenamento de cache DNS, já que o atacante precisa estar presente apenas no mesmo segmento de rede para enviar IDs falsificados (Figura 1). Se coincidir com o original, ele pode envenenar o cache do servidor DNS local e fazer o mapeamento incorreto.

Como mencionado por Hussain *et al.* (2016), o envenenamento de cache DNS também pode ser implementado por meio de falsificação de DNS, em que a origem de um pacote de mensagem DNS é falsificada. Essa técnica é vantajosa para os atacantes, pois os campos de origem e destino do IP são alterados (Liska e Stowe, 2016).

De acordo com Tripathi, Swarnkare e Hubballi (2018), esse método permite que os campos do pacote IP sejam preenchidos com um endereço que não corresponde ao IP real, enganando os usuários e levando-os a fazer conexões inseguras (Figura 1).

Figura 1. Envenenamento de cache de servidor DNS recursivo pela técnica de envenenamento de cache DNS



Fonte: Autor (2023).

Wang (2014), Kim e Reeves (2020) e Zhang *et al.* (2021) investigaram o envenenamento de cache DNS usando a técnica de Kaminsky. Os autores destacam que, apesar de essa implementação de ataque ser mais custosa, ela é bastante prejudicial e afeta substancialmente um servidor DNS autoritário que atende a várias redes. Esse tipo de ataque tem atraído considerável atenção entre os pesquisadores devido aos seus impactos e consequências graves.

2.2 SISTEMA DE DETECÇÃO DE INTRUSÃO

Conforme relatado por Eskandari *et al.* (2020), os Sistemas de Detecção de Intrusão (IDS) monitoram e analisam eficientemente o tráfego de rede ou de *host.* Essa análise é conduzida usando assinaturas ou com base em um modelo comportamental.

Vazão (2021) relatou que quando são detectadas violações de regras, elas são salvas em um arquivo de evidência. Esses registros são conhecidos como logs e fornecem informações relevantes necessárias para identificar o momento do ataque, os serviços violados, a identidade do atacante e os danos causados. Esses logs estão disponíveis em formato de texto e são indispensáveis para identificar invasões na infraestrutura de rede e determinar se o crime ocorreu ou não.

3. TRABALHOS RELACIONADOS

Newton e Beliche (2020) propuseram um método forense que detecta e analisa Ataques de Negação de Serviço (DoS) para estabelecer a ocorrência de um crime de perturbação de serviço de computador nos termos da Lei n. 12.737/2012. Essa abordagem se concentrou no crime de perturbação, excluindo a análise do crime de invasão, que é o tema deste artigo. Vazão (2021) comparou quatro soluções de gerenciamento de informações e eventos de segurança que apresentam um framework de registro centralizado de aplicativos e equipamentos de rede para identificar vulnerabilidades. Esses logs serviram como entrada para medidas de reparo e contenção de ameaças. No entanto, apesar dessa iniciativa, a pesquisa não considerou os fatos que afetam a legislação sobre crimes de computador.

Este artigo propõe uma abordagem forense para capturar as evidências de ataques contra servidores DNS por meio de ferramentas de monitoramento e proteção de rede. Primeiro, os dados de ataque coletados são armazenados em um banco de dados de registro de intrusões; em seguida, os fatos são confrontados com a norma; e, finalmente, um relatório forense é gerado como prova legal da ocorrência de um crime.

4. ABORDAGEM FORENSE PARA ATAQUES DE DNS - FORDNS

A abordagem proposta analisa as alegações de rede relatadas pelo IDS para identificar o atacante, a técnica de intrusão, o endereço IP de origem e destino, o horário, os serviços de rede afetados (servidores) e os danos causados. Esses dados são então analisados para identificar atividades criminosas contra o servidor DNS à luz da legislação brasileira (Artigo 154-A do Código Penal). Esse processo gera um relatório que pode auxiliar as autoridades na identificação do atacante, dos fatos, das vítimas, das circunstâncias e das consequências, bem como na determinação de medidas legais apropriadas.

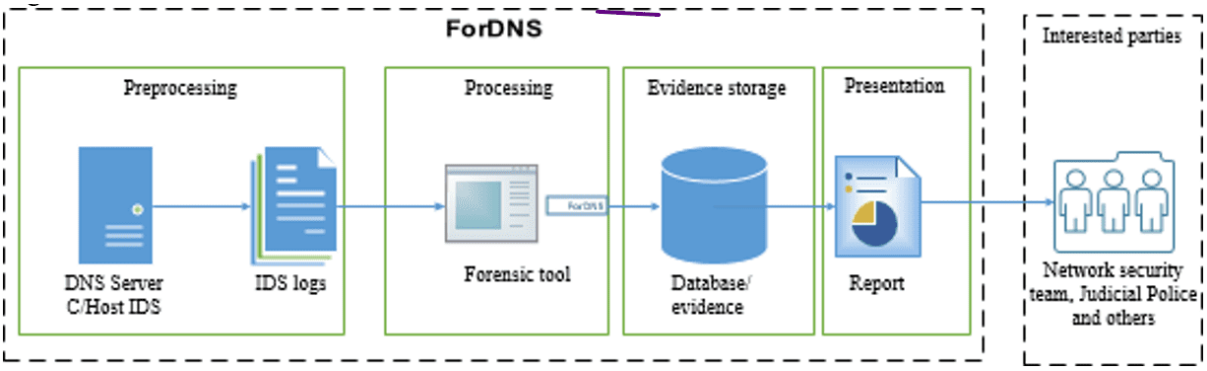
4.1 PROCESSO

As Figuras 2 e 3 ilustram a análise forense de um servidor DNS usando a abordagem proposta. Essa ferramenta coleta dados de infração que corroboram crimes de computador, uma vez que a maioria deles não é investigada devido à falta de evidências ou à volatilidade dos dados registrados no arquivo de log.

Essa ferramenta faz parte de uma arquitetura de computador que automatiza a análise de ataques a servidores DNS. Na maioria dos casos, esses ataques são identificados manualmente por profissionais de segurança da informação, que primeiro localizam a violação (se ainda estiver no arquivo de log do IDS), extraem os dados e os encaminham para quem pode determinar se ocorreu uma infração.

O IDS Suricata pode monitorar o Servidor DNS no modo HIDS, ou seja, ele monitora um servidor *(host)* que fornece serviços DNS (OISF, 2016 e Neto *et al.*, 2017). Para identificar corretamente uma atividade maliciosa, os dispositivos de segurança em redes de computadores, como *Firewall* e IDS, devem ser aplicados e configurados corretamente.

Figura 2. FORDNS



Fonte: Autor (2023).

Na abordagem proposta, uma detecção de intrusão aciona um alerta do IDS. Em seguida, o administrador de rede inicia a ferramenta forense desenvolvida para examinar os registros do IDS. A ferramenta verifica o arquivo de log; se encontrar referências a ataques ao servidor DNS, captura as principais evidências e as armazena em um banco de dados. Este banco de dados gera um relatório que pode ser usado para análises posteriores e servir como prova do crime. Isso é possível devido à forma como o IDS disponibiliza seus dados, permitindo que os dados contidos nos logs sejam lidos e capturados.

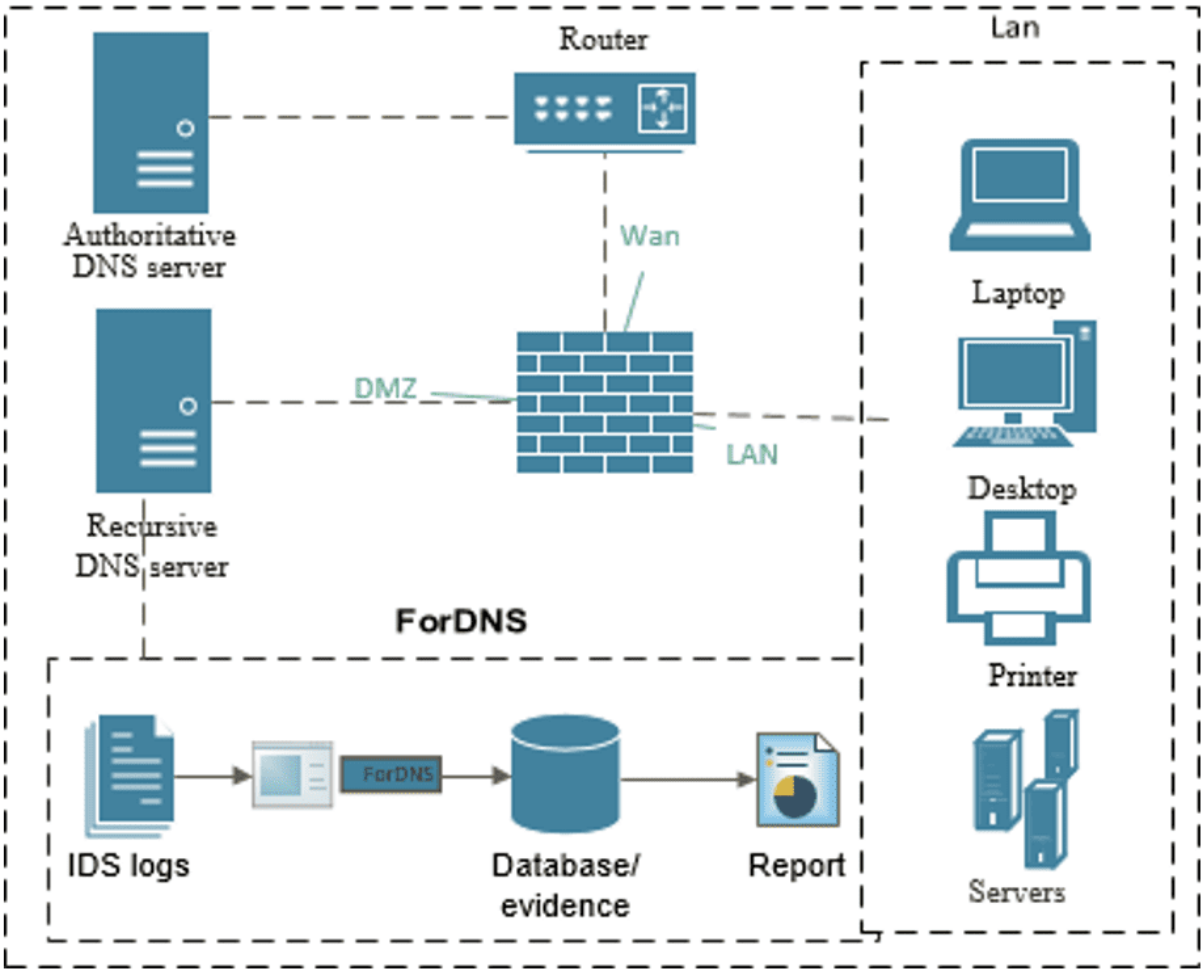
A Figura 2 mostra o fluxo de trabalho da abordagem proposta. O IDS realiza as etapas de pré-processamento do tráfego de rede e processamento de logs do IDS e armazena as evidências criminais. Em seguida, o relatório contendo as principais informações dos crimes é extraído e analisado de acordo com os tipos de crimes.

4.2 ARQUITETURA DO FORDNS

Tipicamente, a arquitetura de uma rede corporativa possui os seguintes elementos: um **roteador** que interconecta a rede WAN (externa), ou seja, a *World Wide Web*, onde o servidor DNS autoritário e outros serviços da Internet estão localizados; a rede **LAN**, que é a rede interna da empresa, onde estão localizados os hosts de usuários que demandam serviços da Internet e outros serviços de rede privada; o ***Firewall***, que é uma ferramenta de segurança de rede; e a **DMZ (Zona Desmilitarizada)**, uma área que compartilha serviços de rede disponíveis para acesso público/privado.

A arquitetura da abordagem *ForDNS* desenvolvida compreende um software que lê e analisa os registros de log do IDS. As informações extraídas destes registros são armazenadas em um banco de dados cujo principal objetivo é gerar relatórios forenses, que podem servir como evidência do ataque.

Figura 3. Arquitetura



Fonte: Autor (2023).

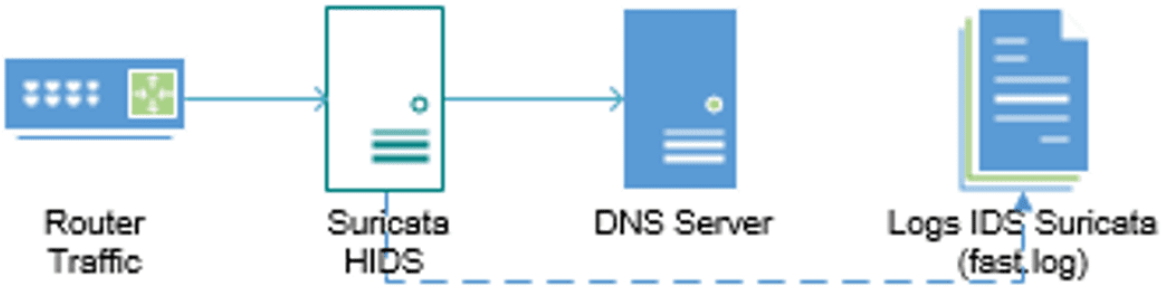
4.3 PRÉ-PROCESSAMENTO DO TRÁFEGO DE REDE PELO IDS SURICATA

Conforme mostrado na Figura 4, o pré-processamento é a primeira fase da investigação em que a fonte de dados será gerada. O arquivo de log do Suricata IDS

RC: 149471
Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense

(OISF, 2023), chamado fast.log, registra todos os incidentes que ocorrem durante a monitoração de pacotes de rede.

Figura 4. Pré-processamento



Fonte: Autor (2023).

O IDS recebe o tráfego de rede, analisa os pacotes de acordo com as assinaturas registradas e, em caso de correspondência entre as regras e os pacotes processados, registra o incidente no arquivo de log (*fast.log*) e alerta a equipe de monitoramento (Eldow *et al*., 2016). Esses logs contêm as informações necessárias para identificar informações, incluindo mensagem, fluxo de rede, referências, números de identificação, classificação e tipo. A Figura 5 descreve cada uma das regras.

Figura 5. Informações da regra

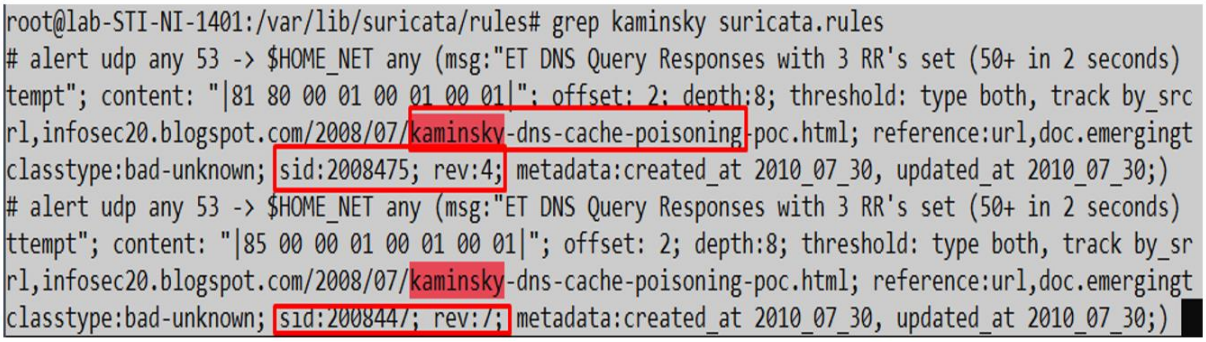
Information managed in each rule	
Msg	Alerts issued by the Suricata IDS
Flow	Contains guidelines on what should be analysed within the traffic
Content	These are rule references. Registered rules usually have a link to identify their source. When the rule is drafted by the network manager, he can describe it
Sid	Rule identification ID, i.e. the identification number
Ver	Rule version
Classtype	Main information and rule classification

Fonte: Autor (2023).

RC: 149471
Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense

A análise dos logs pela ferramenta ForDNS procura por palavras-chave, como o número de identificação (Sid) da regra e o (Msg), que compreendem a mensagem que indica o tipo de ataque. A Figura 6 destaca essas palavras-chave.

Figura 6. Regras de detecção de envenenamento de cache DNS



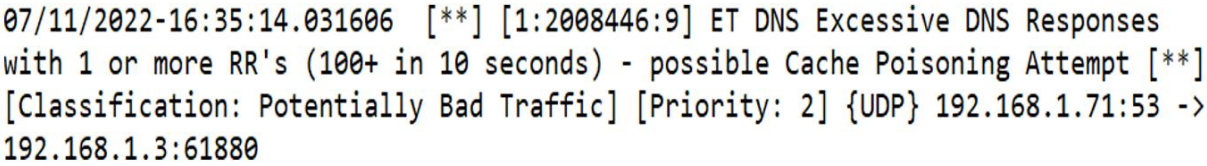
Fonte: Autor (2023).

Essas informações servirão de base para analisar o fato e sua possível conexão com o crime de invasão de dispositivo de computador conectado a uma rede de computadores, de acordo com o Artigo 154-A do Código Penal Brasileiro.

4.4 PROCESSAMENTO DO ARQUIVO DE LOG DO IDS USANDO A FERRAMENTA FORENSE

Conforme mostrado nas Figuras 7 e 8, a ferramenta forense processa a fonte de dados, ou seja, o arquivo fast.log, em busca de palavras-chave (SIDs) das regras responsáveis por identificar ataques.

Figura 7. Registros do IDS Meerkat



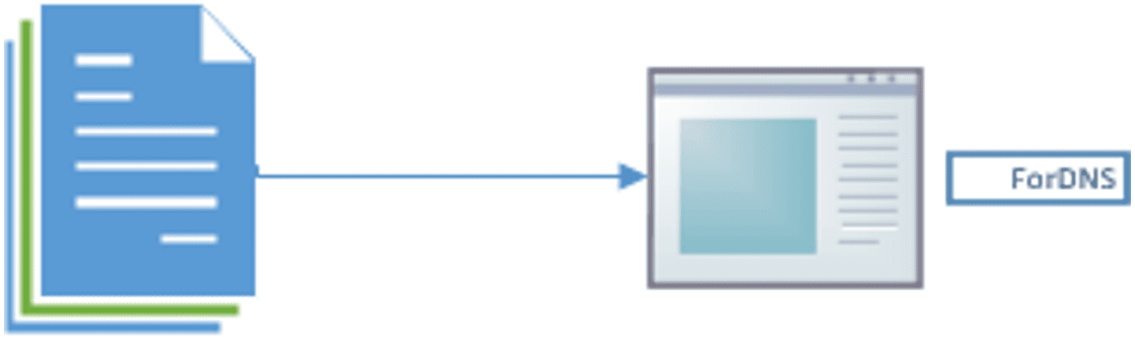
Fonte: Autor (2023).

Se uma intrusão for detectada, a ferramenta coleta os seguintes dados: IP de origem, IP de destino, data/hora, portas de origem e a técnica usada para o ataque; esses

RC: 149471
Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense

dados são então registrados em um banco de dados como evidência de invasão criminosa para análise posterior. Por fim, é gerado um relatório contendo os elementos que constituem o delito.

Figura 8. Processamento de Evidências

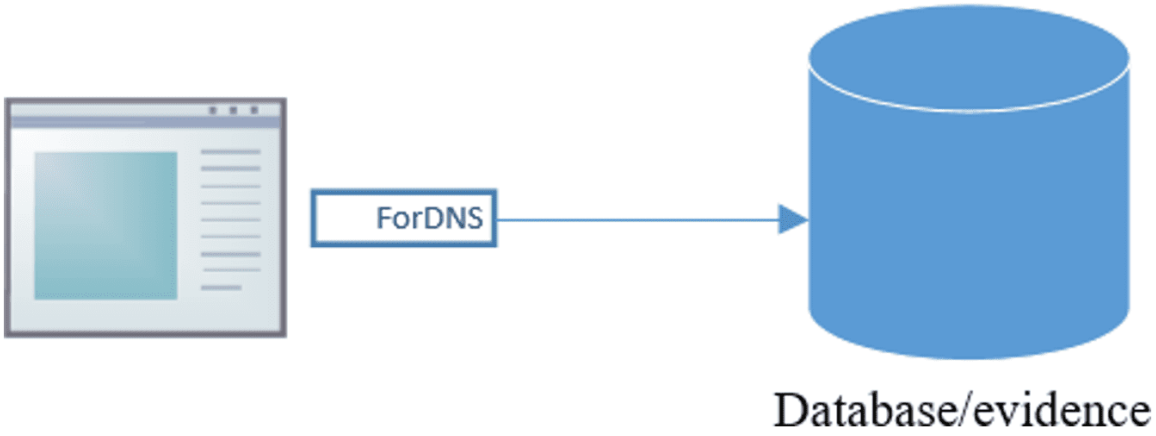


Fonte: Autor (2023).

4.5 REGISTRO DE EVIDÊNCIAS NO BANCO DE DADOS PELA FERRAMENTA FORENSE FORDNS

Conforme mostrado na Figura 12, a inserção de evidências no banco de dados ocorre da seguinte forma: a ferramenta forense (*ForDNS*) analisa a fonte de dados e armazena as seguintes informações no novo banco de dados: tipo da técnica de intrusão, data/hora do ataque, o IP de origem (identifica o infrator), o IP de destino (identifica a(s) vítima(s) e o proprietário do servidor DNS), ou seja, a origem do ataque, quem foi o alvo, que técnica de invasão foi adotada e as consequências técnicas desse ataque. Esses dados são usados para inferir se o referido crime de computador ocorreu de acordo com o Código Penal Brasileiro.

Figura 9. Armazenamento de Evidências



Fonte: Autor (2023).

Figura 10. Banco de Evidências

Result Grid | Filter Rows: | Edit: | Export/Import: | Wrap Cell Content:

iddnsReport	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 s...	Invasion
2	05/15/2022-16:50:01.950319	192.168.100.10:35006	192.168.100.1:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
3	05/21/2022-11:47:28.810665	192.168.100.10:47401	192.168.100.1:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
4	10/25/2022-16:15:15.941984	192.168.0.10:33396	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
5	10/26/2022-22:17:26.184351	192.168.0.10:51114	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
6	10/26/2022-22:17:28.606209	192.168.0.10:36981	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
7	10/26/2022-22:17:28.804180	192.168.0.10:40837	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
8	10/26/2022-22:17:30.412132	192.168.0.10:56182	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
9	10/26/2022-22:35:40.158020	192.168.0.10:45021	181.213.132.2:53	DNS CHACE POISONING	Injection of false data into the cache of a DNS s...	Invasion
10	10/26/2022-22:35:40.276352	192.168.0.10:33766	181.213.132.2:53	DNS HIJACKING	Dns server hijacking. Providing false informatio...	Invasion
NULL	NULL	NULL	NULL	NULL	NULL	NULL

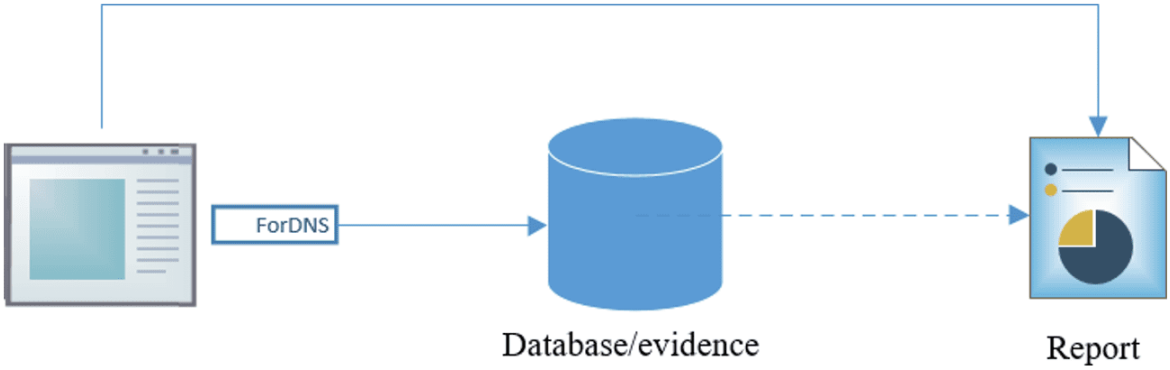
Fonte: Autor (2023).

Apesar da falta parcial de informações no banco de dados, a ferramenta proposta pode não apenas determinar as consequências do ataque, mas também inferir o tipo de crime com base na disposição legal (154-A).

4.6 RELATÓRIO

O relatório gerado pela ferramenta *ForDNS* reúne as informações extraídas e as armazena em um novo banco de dados. Esse relatório servirá como evidência de intrusão criminosa em dispositivo de computador, sendo posteriormente utilizado por investigadores e pela Polícia Judiciária.

Figura 11. Registro de evidências no relatório



Fonte: Autor (2023).

As Figuras 11 e 12 mostram como o relatório reúne informações sobre o delito, registrando-as para a subsequente investigação criminal.

Figura 12. Relatório gerado pela ferramenta *ForDNS*

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: Autor (2023).

4.7 CLASSIFICAÇÃO CRIMINAL DE ATAQUES DE ENVENENAMENTO DE CACHE DNS

O Artigo 154-A do Código Penal Brasileiro (BRASIL, 1940), inserido pela Lei 12.737/2012 (BRASIL, 2012) e recentemente alterado pela Lei 14.155/2021 (BRASIL,

2021), ilustra o crime de invasão de dispositivo de computador, independentemente de estar conectado à World Wide Web.

O IDS, por si só, não pode determinar se ocorreu um crime; ele apenas se concentra na proteção da rede e na emissão de alertas. Outros meios são exigidos por lei para identificar a técnica de invasão, analisar o procedimento de invasão (varredura de portas ou outras técnicas preparatórias para o ataque ao serviço DNS) e identificar todos os elementos criminosos. O presente estudo se concentra em ataques de envenenamento de cache DNS, uma técnica usada para invadir um dispositivo de computador — o Servidor DNS, no caso — para obter, destruir ou adulterar informações que permitem a associação correta do endereço IP de um servidor com seu site, o que constitui um crime de acordo com o Artigo 154-A do Código Penal Brasileiro.

4.8 CENÁRIO DE APLICAÇÃO DA FERRAMENTA FORENSE E ANÁLISE DE LOG DO IDS

Esta abordagem permite a análise de intrusões em servidores DNS sob dois cenários: ataques internos e externos. A abordagem forense foi desenvolvida para a análise de tráfego de rede gerado pelo IDS Suricata. Esse IDS identifica e registra os dados de intrusão, analisando o tráfego de rede e identificando ações alinhadas com as regras que definem várias técnicas de intrusão em redes de computadores (Waleed, Jamali e Masood, 2022).

Apesar de ser capaz de capturar as evidências de ataque, sua identificação e eventuais respostas do IDS (para alertar os serviços de rede atacados ou banir o dispositivo do atacante original), o IDS não identifica se essas ocorrências são atividades criminosas. Esses dados não apenas são voláteis, mas também constantemente sobrescritos por atividades de rede mais recentes.

Nesse contexto, a abordagem proposta pretende ajudar a capturar fatos sinalizados pelo DME e analisá-los sob a perspectiva da lei criminal brasileira, considerando que

nem todo alerta constitui um crime. Nossa abordagem considera os seguintes dois cenários.

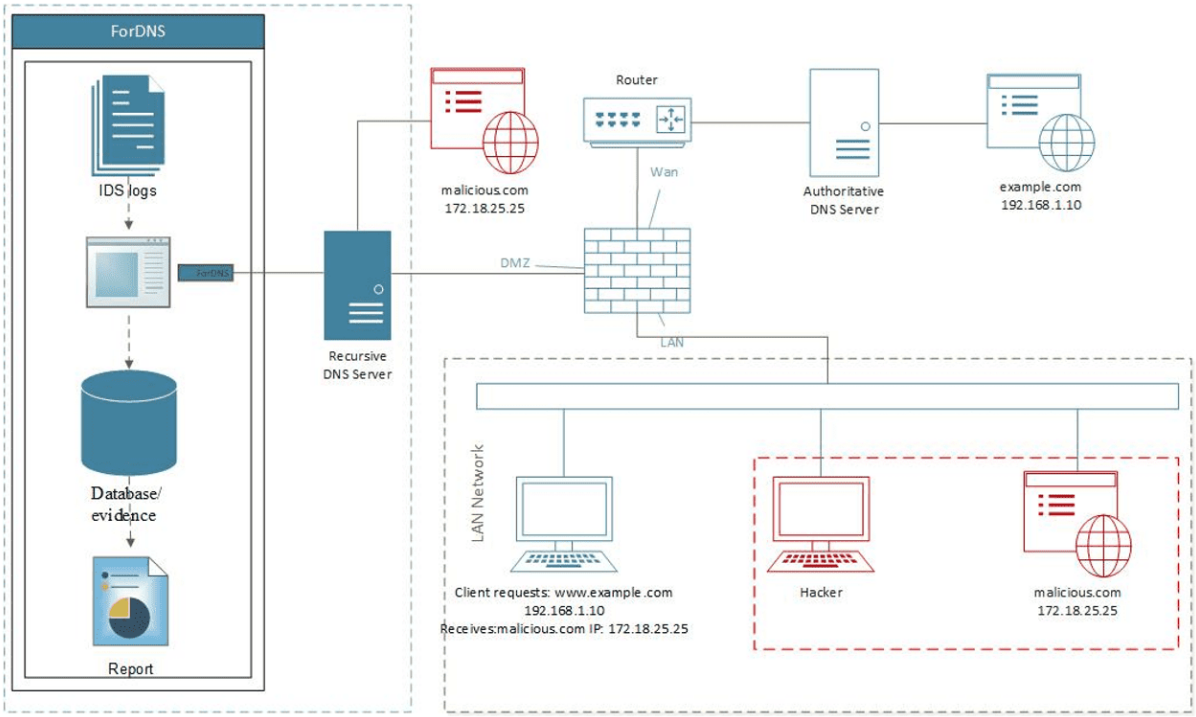
4.8.1 CENÁRIO 1: INVASOR DENTRO DA REDE LAN (USUÁRIO AUTENTICADO) INVADINDO O DNS LOCAL

O Cenário 1 (Figura 13) representa um ataque ao DNS recursivo. O invasor cria uma página da web falsa, semelhante a um site corporativo ou institucional. Aplicando técnicas de invasão, ele captura credenciais privadas de sistemas.

Neste cenário, o invasor envenena o cache DNS inserindo o endereço que leva a uma página da web falsa no cache do servidor DNS recursivo. Ao tentar acessar uma página inserindo uma URL conhecida, os usuários são redirecionados para uma página falsa (quase idêntica à real). Uma vez lá, os usuários se tornam vítimas de outros crimes ao fornecerem dados pessoais.

Na maioria dos casos, as informações em cache têm vida curta e, após algumas tentativas, os usuários conseguem acessar a página real sem perceber os efeitos dos ataques de envenenamento de cache.

Figura 13. Contexto de ataque interno do ForDNS ao DNS recursivo



Fonte: Autor (2023).

Normalmente, as vítimas de envenenamento de cache só percebem os ataques depois que suas consequências se materializaram na forma de perdas financeiras, de trabalho, pessoais ou de outra natureza. As razões mencionadas e a revelação tardia da ocorrência tornam a identificação do autor do crime difícil. Nesse contexto, a necessidade de uma arquitetura de computador especializada na detecção e análise da identificação de fraudes em computadores, bem como no armazenamento das evidências dessas ocorrências, torna-se fundamental.

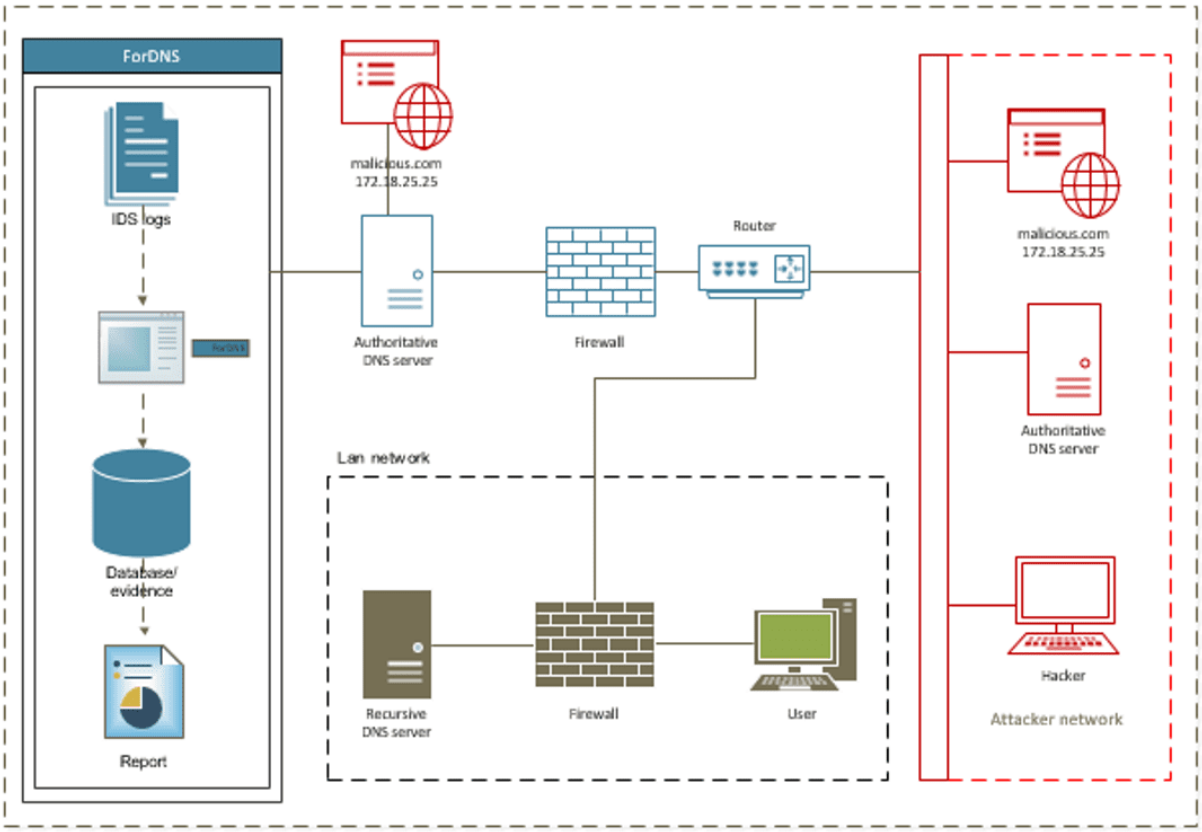
A ferramenta ForDNS, como mencionado, prioriza a análise desse tipo de ataque e extrai evidências criminais, relatando assim crimes que possivelmente se enquadram no Artigo 154-A do Código Penal Brasileiro.

4.8.2 CENÁRIO 2: INVASOR NA REDE WAN (INTERNET) INVADINDO O DNS PRIMÁRIO (AUTORITATIVO)

O Cenário 2, Figura 14, retrata um ataque mais abrangente cujos impactos negativos são maiores do que no Cenário 1, pois não se restringe a um grupo específico, mas se estende a todos os outros usuários dos serviços de resolução de nomes de domínio que acessam um determinado domínio.

Neste caso, trata-se de um ataque remoto ao DNS, que, para alguns 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 sim um servidor recursivo de um provedor de serviços de Internet (ISP) solicitando um domínio a partir de um servidor DNS autoritativo.

Figura 14. ForDNS em um contexto de envenenamento de cache DNS entre um servidor DNS recursivo de um ISP negociando com autoritativo



Fonte: Autor (2023).

RC: 149471
Disponível em: https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/analise-forense

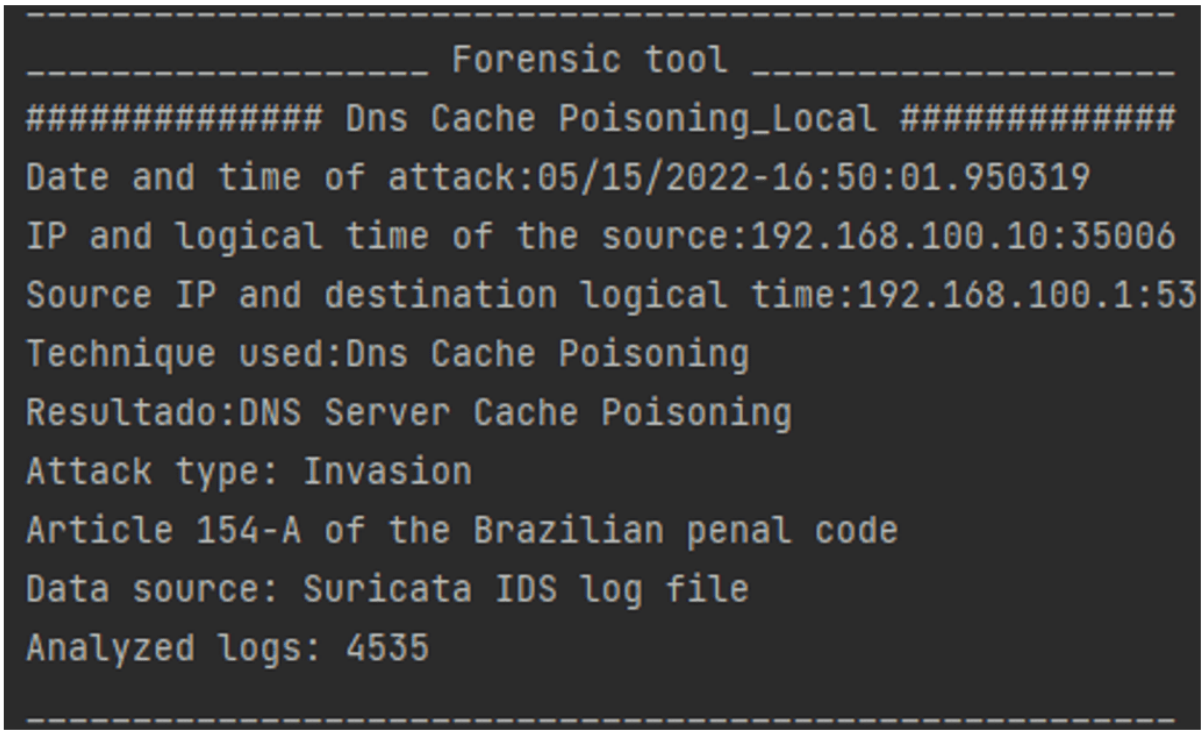
Os atacantes de Kaminsky operam remotamente e não esperam que os usuários em uma rede privada gerem uma consulta DNS para envenenar o cache de um servidor DNS de um ISP. O atacante começa transmitindo a consulta recursiva do ISP a um servidor autoritativo e, se não tiver o endereço de domínio em cache, inicia imediatamente a consulta ao servidor autoritativo para esse domínio. É nesse momento que o atacante compete com o DNS autoritativo porque, enquanto o autoritativo tenta enviar uma resposta autêntica para o recursivo, o atacante, fazendo-se passar pelo autoritativo, envia um grande número de respostas forjadas para o recursivo. Se a resposta falsificada corresponder à enviada durante a consulta DNS, o recursivo aceitará a resposta falsificada e armazenará temporariamente os registros de domínio malicioso em seu cache.

O atacante cria a oportunidade de invadir o servidor DNS falsificando a resposta de validação entre os servidores e interrompendo assim a comunicação entre eles; falsifica o endereço IP do domínio para um malicioso; e finalmente obtém informações de terceiros.

Esse ataque é crítico porque pode ser realizado repetidamente, ou até mesmo sequestrar o DNS ou torná-lo indisponível por meio de um ataque de negação de serviço distribuído (DDoS). Zhang *et al.* (2021) relatam que o envenenamento de cache DNS usando a técnica de Kaminsky inicialmente era direcionado apenas ao envenenamento de cache, mas a partir de 2021, ele tem atuado em conjunto com o sequestro de servidores DNS. Esses ataques têm uma duração maior, resultando em repercussões mais amplas. Tripathi, Swarnkare e Hubballi (2018) afirmam que eles são frequentemente apoiados por ataques DDoS que tornam o servidor DNS original inutilizável.

Semelhante ao Cenário I, os usuários só percebem que foram atacados quando as consequências se materializam em perdas. Portanto, essas estruturas de computador devem ser monitoradas para que o servidor DNS, ou qualquer servidor de uma aplicação de computador, seja monitorado por ferramentas de segurança da informação quando tais fraudes ocorrerem.

Figura 15. Relatório Forense (ForDNS)



Fonte: Autor (2023).

Como descrito, a ferramenta proposta é útil para a detecção de crimes de computador, pois captura e armazena as principais evidências de intrusão no DNS em um banco de dados. Usando isso, um relatório forense pode ser apresentado como evidência de acordo com o Artigo 154 do Código Penal Brasileiro (Figura 15).

5. CONCLUSÃO

As infraestruturas de rede interconectadas com a *World Wide Web* e vários servidores nela contidos exigem um dispositivo de proteção para salvaguardar a integridade de muitos serviços computacionais acessíveis pela Internet. *Firewalls* e IDSs servem a esse propósito de proteção e segurança. O IDS identifica a atividade e a registra em um arquivo de histórico (log), tomando algumas decisões previamente configuradas. Isso constitui, de acordo com a legislação penal brasileira, o crime de invasão de dispositivo de computador. Dado que o arquivo de log registra volatilidade, que é frequentemente atualizada pelo grande volume de dados e alertas gerados pelo

tráfego de rede, tais evidências se perdem, tornando difícil a coleta de provas que permitam o processo criminal dos perpetradores.

Neste estudo, propusemos uma abordagem que utiliza uma ferramenta forense para extrair os dados fornecidos pelo IDS e identificar a ocorrência de um ataque de envenenamento de cache DNS, bem como analisar os vários elementos constituintes dos atos criminosos. Isso também possibilita a disponibilização de evidências para investigar os fatos, o autor, as vítimas e as consequências tecnológicas da invasão do(s) dispositivo(s). Além disso, registra os dados em um banco de dados de evidências fornecido com a arquitetura, que verifica o tipo de ataques em relação à legislação relevante. Por fim, também permite que não especialistas em segurança de rede registrem atividades de ataque, preservando dados históricos para futuras atualizações em sistemas de segurança e proteção de serviços de rede.

REFERÊNCIAS

ALHARBI, F.; CHANG, J.; ZHOU, Y.; QIAN, F.; QIAN, Z.; ABU-GHAZALEH, N. Collaborative Client-Side DNS Cache Poisoning attack. **In: IEEE Conference on Computer Communications (INFOCOM)**, 2019, Proceedings. Piscataway: IEEE, 2019. p. 1153-1161.

BRASIL. **Lei nº 12.737, de 30 de Novembro de 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. Acesso em: 5 jun. 2023.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Diário Oficial da União. 27 de maiode 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm Acesso em: 5 jun. 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Diário Oficial da União, Brasília, DF, 31 dez. 1940. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 5 jun. 2023.

ELDOW, O.; CHAUHAN, P.; LALWANI, P.; POTDAR, M. Computer Network Security IDS Tools and Techniques (Snort/Suricata). **International Journal of Scientific and Research Publications**, v. 6, n. 1, p. 593-597, 2016.

ESKANDARI, M ; JANJUA, Z. H.; VECCHIO, M.; ANTONELLI, F. 'Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices', **IEEE Internet of Things Journal**, Vol. 7 No. 8, pp.6882–6897, 2020.

HMOOD, H. S.; LI, Z.; ABDULWAHID, H. K.; ZHANG, Y. Adaptive caching approach to prevent DNS cache poisoning attack. **Computer Journal**, v. 58, n. 4, p. 973-985, 2015.

HUSSAIN, M. A.; JIN, H.; HUSSIEN, Z. A.; ABDULJABBAR, Z. A.; ABBDAL, S. H.; IBRAHIM. DNS Protection against Spoofing and Poisoning Attacks. **In: International Conference on Information Science and Control Engineering (ICISCE)**, 2016, Proceedings. Piscataway: IEEE, 2016. p. 1308-1312.

KAMINSKY, D. Black Ops 2008**: It's The End Of The Cache As We Know It. Fortune**, 2008, p. 1-18.

KIM, T. H.; REEVES, D. **A survey of domain name system vulnerabilities and attacks. Journal of Surveillance**, Security and Safety, 2020, p. 34-60.

LENCSE, G. Benchmarking Authoritative DNS Servers. **IEEE Access**, v. 8, p. 130224-130238, 2020.

LISKA, A.; STOWE, G. DNS reconnaissance. **In: DNS Security. Cham: Springer**, 2016. p. 75-91.

NAQASH, T.; UBBAID, F. B.; ISHFAQ, A. Protecting DNS from cache poisoning attack by using secure proxy. In: **International Conference on Emerging Technologies (ICET)**, 2012, Proceedings. Piscataway: IEEE, 2012. p. 288-292.

NETO, H.; ÁVILA, C.; LACERDA, W. S. Computer Network Intrusion Detection System Using Artificial Neural Networks. In: **Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)**, 2017, Proceedings. Porto Alegre: SBC, 2017. p. 206-213.

NEWTON, H.; BLICHE, S. Computer Network Forensics Assistance Methodology Focused on Denial of Service Attacks. **International Journal of Computer Applications**, v. 177, n. 33, p. 1-11, 2020.

OISF - Open Information Security Foundation. **Suricata user guide**. p. 206, 2016. Disponível em: <https://suricata.readthedocs.io/ en/suricata-6.0.0/>. Acesso em: 10 out. 2022.

OISF - Open Information Security Foundation. **Suricata IDS V.6**. 2023. Disponível em <https://suricata.io/features/>. Acesso em: 6 jun. 2022.

STEINHO, U.; WIESMAIER, A.; ARAÚJO, R. The State of the Art in DNS Spoofing. **In: International Conference on Applied Cryptography and Network Security (ACNS)**, 2006, Proceedings. Berlin: Springer, 2006.

TRIPATHI, N.; SWARNKAR, M.; HUBBALLI, N. DNS spoofing in local networks made easy. In: **IEEE International Conference on Advanced Networks and**

Telecommunications Systems (ANTS), 2018, Proceedings. Piscataway: IEEE, 2018. p. 1-6.

VAZÃO, 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>. Acesso em: 5 jun. 2021.

WALEED, A.; JAMALI, A. F.; MASOOD, A. 'Which open-source IDS Snort, Suricata or Zeek'. **Computer Networks**, Vol. 213 No. June, pp. 109-116, 2022.

WANG, W.; ZANG, T.; LAN, Y. The Rapid Extraction of Suspicious Traffic from Passive DNS. In: **International Conference on Information Systems Security and Privacy (ICISSP)**, 2018, Proceedings. SciTePress, 2018. p. 190-198.

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.

ZHANG, H.; *et al*. 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>.

Enviado: 14 de junho, 2023.

Aprovado: 29 de junho, 2023.

[1] Mestrando em Ciência da Computação (UFMA), Bacharel em Sistemas de Informação (Estácio), Tecnólogo em Gestão Ambiental (CEST), Especialista em Gestão Pública (UFMA), Especialista em Redes de Computadores (AVM), Tec. Em Informática (IFMA/ETC-BRASIL). ORCID: 0009-0001-1336-4044. CURRÍCULO LATTES: http://lattes.cnpq.br/4129979584830810.
[2] Orientador. Doutor em Informática, Mestre em Engenharia Elétrica com Área de Concentração em Ciência da Computação, Bacharel em Ciência da Computação e Bacharel em Direito. ORCID: 0000-0001-8799-1799. CURRÍCULO LATTES: http://lattes.cnpq.br/1531971102610447.