AN APPROACH TO IDENTIFICATION AND FORENSIC ANALYSIS OF DNS ATTACKS

ORIGINAL ARTICLE

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

SOUSA, Robson Everton. VALE, Samyr. **An approach to identification and forensic analysis of DNS attacks**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Year. 08, Ed. 07, Vol. 01, pp. 24-44. July 2023. ISSN: 2448-0959, Access link: https://www.nucleodoconhecimento.com.br/computer-science/forensic-analysis, DOI: 10.32749/nucleodoconhecimento.com.br/computer-science/forensic-analysis

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.

1. INTRODUCTION

Domain name resolution servers (DNS) is one of the most important Internet infrastructures that map the connections between the domain name (URL) and internet protocol (IP) address (Wang, Zang and Lan, 2018). Despite its great importance, it is flawed because some security issues were overlooked during its inception.

DNS attacks are quite recurrent; 92% of the networks analysed are subject to at least one type of DNS cache poisoning (Alharbi et al., 2019). This was corroborated by evaluating 97% of resolvers operating openly, 74% of corporate networks via email servers and 68% of Internet Service Providers (ISP) measured through network Ads.

Although network security and protection tools such as intrusion detection systems (IDS) monitor network activity and traffic, including possible attacks, these records are stored in internal log files and constantly and dynamically updated. Typically, the data generated there remains unprocessed, acting only as an event occurrence information for network administrators. Often, when repeated attacks are detected, hacking activities records are invariably lost among the large volume of information generated by these tools. The reason for this being that these are not meant to perform forensics, but only to protect data traffic.

The proposed approach aims to identify the characteristics of a computer device intrusion crime, particularly DNS server attacks, recognise the intrusion for enforcing appropriate criminal laws.

Once this is done, the approach proposes to record proof of an attack occurrence in a skilled expert document. Then, this data can be analysed and interpreted to ascertain whether the data traffic in a DNS server is standard activity or an attempted intrusion. To this end, the network disasters notified by the IDS are analysed to pinpoint its attacker, the invasion technique deployed, its source and destination IP address, time of the attack occurrence, affected computer services and the extent of the damage caused.

The rest of this paper is structured as the following. Section II outlines the technological background of the present study; Section III presents related works in the literature and their shortcomings; Section IV deals with forensic analysis using DNS tools; and finally, Section V draws conclusions.

2. TECHNOLOGICAL LANDSCAPE

According to Lencse (2020), the DNS (Domain Name System) is an important technological resource capable of widely supporting the World Wide Web, being imperceptible when working properly. However, when a failure occurs, the slowdown that impact the quality of service quickly becomes noticeable.

As mentioned by Naqash et al. (2012), DNS architecture failed to add the necessary security criteria to block spoofed data receipt in the DNS server cache. Hmood et al. (2015) and Steinho, Wiesmaier and Araújo (2006), mention that criminals exploit this vulnerability by inserting forged information into the cache of DNS servers and changing referential parameters to either make it unavailable or divert their traffic to malicious pages. These parameters can be changed from recursive to authoritative during the query flow.

2.1 TECHNIQUES AND ATTACKS ON DNS

Kim and Reeves (2020) describe DNS server attacks as acts of data tampering, flooding, DNS abuse and counter DNS server structure. This classification makes it possible to analyse them by areas according to attackers' different interests The present work aims to analyse DNS *cache poisoning*, which, according to Kim and Reeves (2020), falls under the data tampering mode.

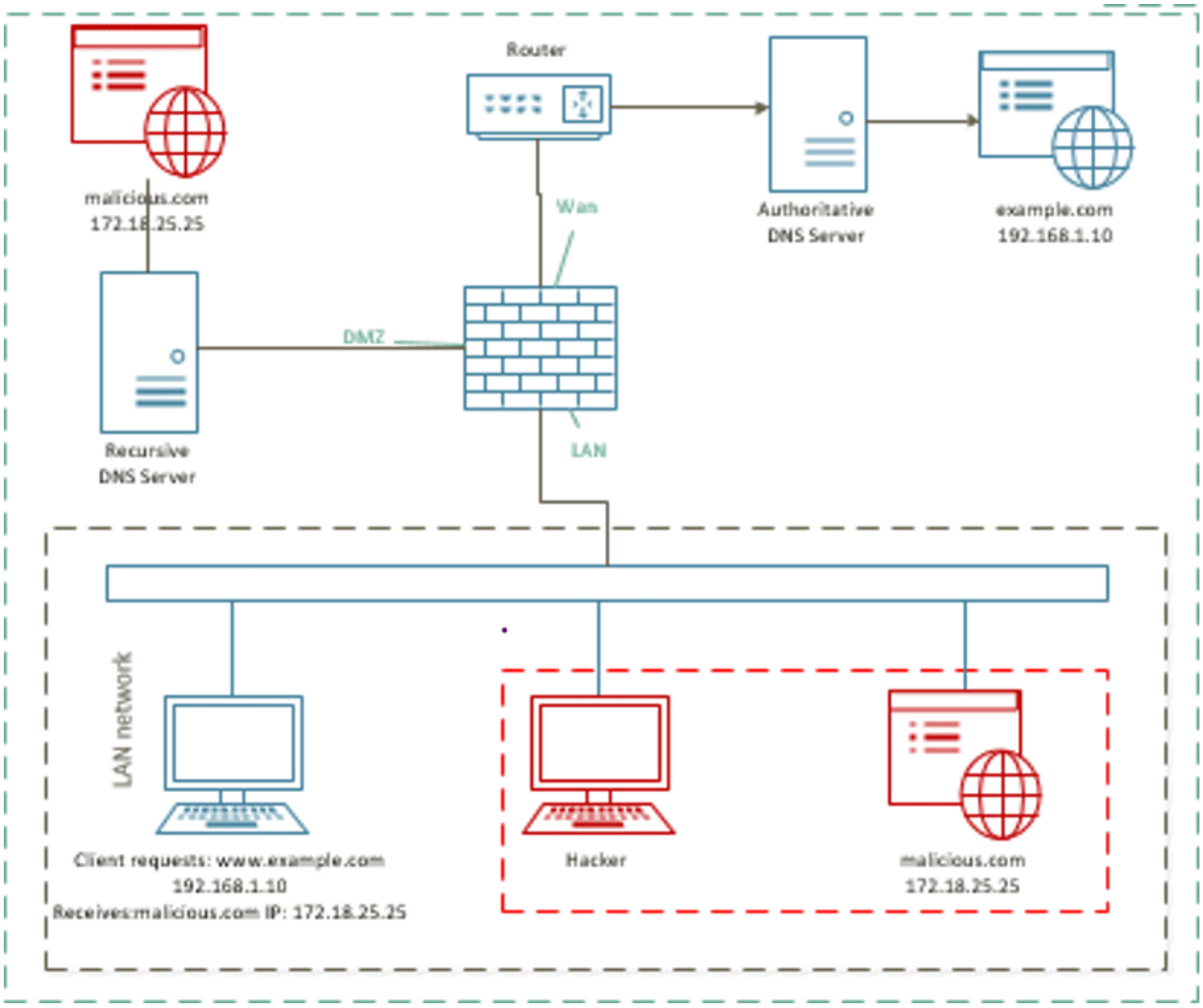
Zhang et al. (2021) and Kaminsky et al. (2008) mention that one of the first DNS cache poisoning was discovered by Kaminsky in 2008. Unlike local cache poisoning, DNS cache poisoning can be performed remotely. According to Tripathi, Swarnkare and Hubballi (2018), local cache poisoning is simpler to implement than DNS cache poisoning as the attacker needs only be present in the same network segment to send forged IDs (Figure 1). If it matches the original, it can poison the local DNS server cache and perform incorrect mapping.

As mentioned by Hussain et al. (2016), DNS cache poisoning can also be implemented via DNS *spoofing*, where the origin of a DNS message packet is spoofed. This

technique is advantageous for the attackers as the source and destination fields of the IP are changed (Liska and Stowe, 2016).

According to Tripathi, Swarnkare and Hubballi (2018), this method allows the IP packet fields to be filled in with an address that does not match the real IP, thereby misleading users into making insecure connections (Figure 1).

Figure 1. Recursive DNS server poisoning by DNS cache poisoning technique



Source: Author (2023).

Wang (2014), Kim and Reeves (2020) and Zhang et al. (2021) have investigated the DNS cache poisoning using the *Kaminsky* technique. The authors emphasise that despite this attack implementation being more costly, it is quite harmful and substantially affects an authoritative DNS server that serves various networks. This

type of attack has attracted considerable attention among researchers because of its severe impacts and consequences.

2.2 INTRUSION DETECTION SYSTEM

As reported by Eskandari et al. (2020), IDSs efficiently monitor and analyse network or host traffic. This analysis is conducted using signatures or based on a behavioural model.

Vazão (2021) reported that when rule breaches are detected, they are saved in an evidence file. These records are known as logs and provide relevant information required to identify the time of the attack, the services violated, the attacker's identity and the damage done. These logs are available in text format and are indispensable to identify network infrastructure invasions and ascertain whether or the crime occurred.

3. RELATED WORKS

Newton and Beliche (2020) proposed a forensic method that detects and analyses Denial-of-Service (DoS) Attacks to establish the occurrence of a computer service disruption offence under the terms of Law n. 12.737/2012. This approach focused on the crime of disturbance, excluding the analysis of the crime of invasion, is the subject matter of this paper. Vazão (2021) compared four security information and event management solutions featuring a centralised logging framework of applications and network equipment to identify vulnerabilities. These logs served as input for threat repair and containment measures. Despite this initiative, the research did not consider facts affecting the legislation on computer crimes.

This paper proposes a forensic approach to capture the evidence of attacks against DNS servers via network monitoring and protection tools. First, the collected attack data is stored in an intrusion registry database; then, the facts are considered to the norm, and finally a forensic report is generated as the legal evidence of a crime's occurrence.

4. FORENSIC APPROACH TO DNS ATTACKS—FORDNS

The proposed approach analyses network claims reported by the IDS to identify the attacker, the intrusion technique, the source and destination IP address, the time, the affected network services (servers) and the damage caused. This data is then analysed to identify criminal activities against the DNS server in the light of Brazilian legislation (Article 154-A of the Penal Code). This process generates a report that can aid the authorities in identifying the attacker, facts, victims, circumstances and consequences and determining appropriate legal proceedings.

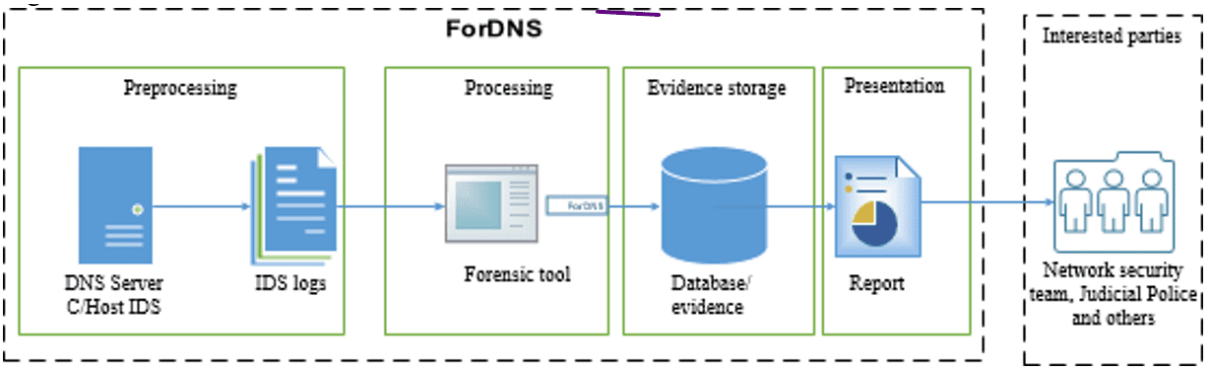
4.1 PROCESS

Figures 2 and 3 illustrate the forensic analysis of a DNS server using the proposed approach. This tool collects infraction data that corroborate computer crimes as most of these are not investigated owing to the lack of evidence, or the volatility of the data recorded in the log file.

This tool is part of a computer architecture that automates the analysis of DNS server attacks. In most cases, such attacks are identified manually by information security professionals, who first locate the breach (if still in the IDS log file), extract the data and forward it to those who can determine whether an offence has occurred.

The Suricata IDS can monitor DNS Server in HIDS mode i.e., it monitors a server (host) that provides DNS services (OISF, 2016 and Neto et al., 2017). To correctly identify a malicious activity, the security devices in computer networks—Firewall and IDS—must be correctly applied and configured.

Figure 2. FORDNS



Source: Author (2023).

In the proposed approach, an intrusion detection triggers an IDS alert. Then, the network administrator starts the forensic tool developed to peruse the IDS logs. The tool scans the log file; if it finds references to DNS server attacks, it captures the main evidence and stores in an database. This database generated a report that can be used for further analysis and act as the proof of the crime. This is rendered possible by the way in which the IDS makes its data available, allowing log-contained data to be read and captured.

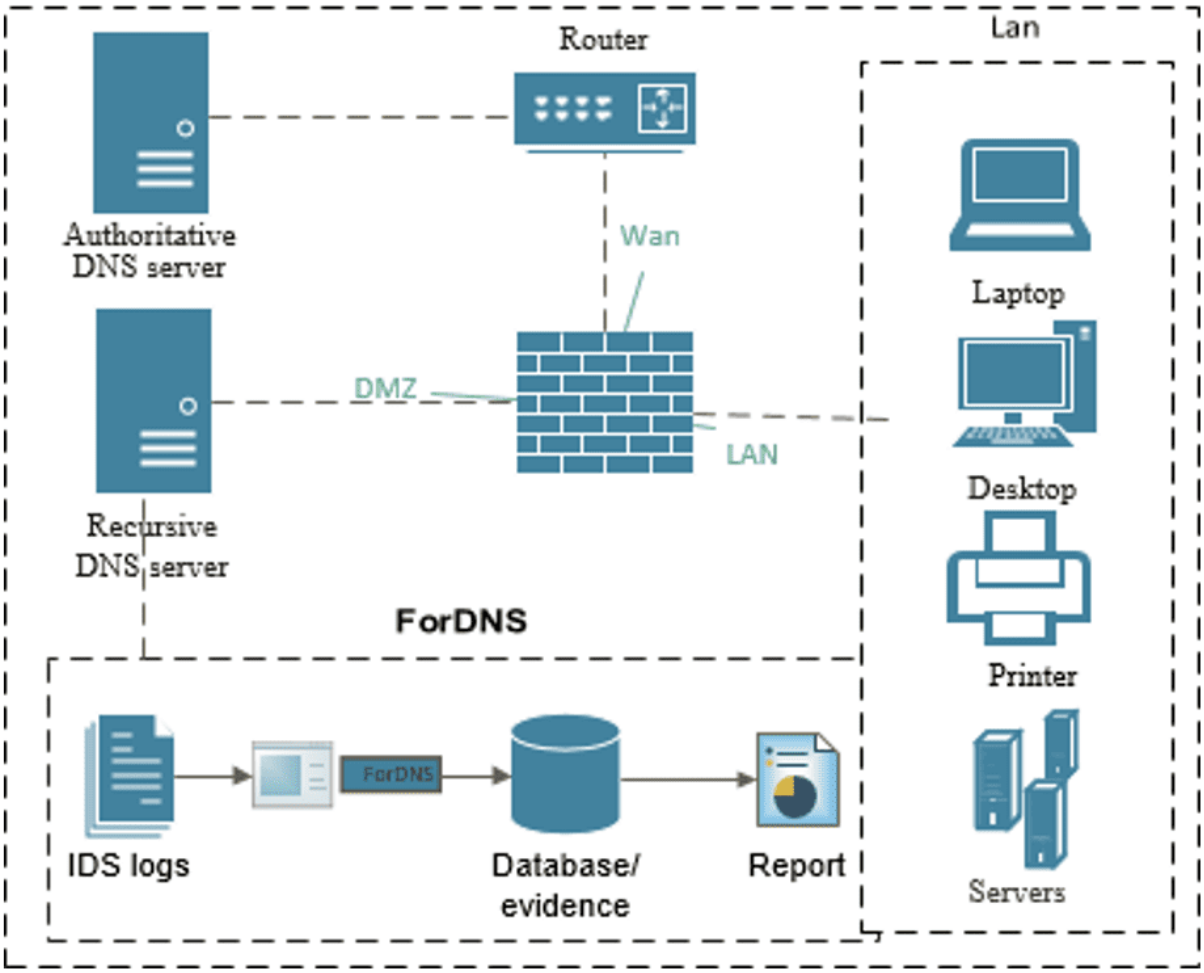
Figure 2 shows the workflow of the proposed approach. The IDS runs the preprocessing of network traffic and processing fro IDS logs steps and stores the criminal evidence. Then, the report containing the main information of the crimes is extracted and analysed according to criminal types

4.2 FORDNS ARCHITECTURE

Typically, a corporate network architecture has the following elements: a **router** that interconnects the WAN (external) network i.e., World Wide Web, where the authoritative DNS server and other Internet services are located; the **LAN** network, which is the internal corporate network where the user hosts who demand Internet services and other private network services are located; the **Firewall**, which is a network security tool; and the **DMZ (Demilitarized Zone)**, an area that that shares network services available for public/private access.

The architecture of the developed ForDNS approach comprise a software that reads and analyzes the IDS log records. Information extracted from the latter is stored in a database whose main purpose is to generate forensic reports, which can serve as the evidence of the attack.

Figure 3. Architecture

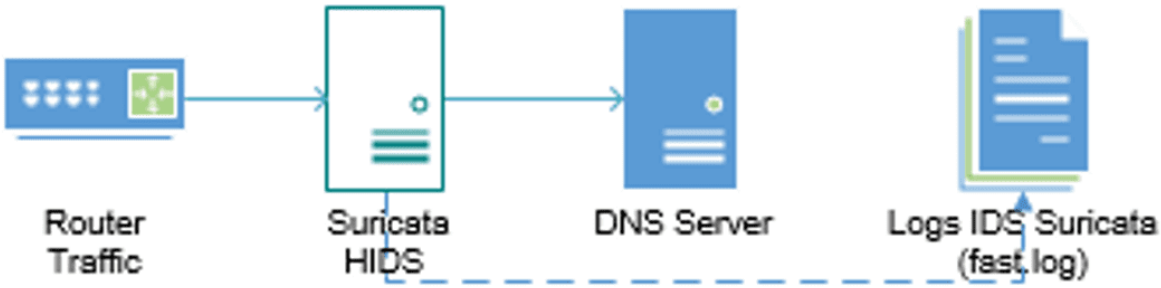


Source: Author (2023).

4.3 NETWORK TRAFFIC PREPROCESSING BY SURICATA IDS

As shown in Figure 4, preprocessing is the first phase of the investigation where the data source will be generated. The Suricata IDS. (OISF,2023) log file (called *fast.log)* records all incidents that occur while monitoring network packets.

Figure 4. Preprocessing



Source: Author (2023).

The IDS receives network traffic analyses the packets according to the registered signatures, and in case of a match between the rules and processed packets, it records the incident in the log file (fast.log) and alert the monitoring team (Eldow et al., 2016). These logs contain the information required to identify necessary information, including message, network flow, references, identification numbers, classification and type. Figure 5 describes each of the rules.

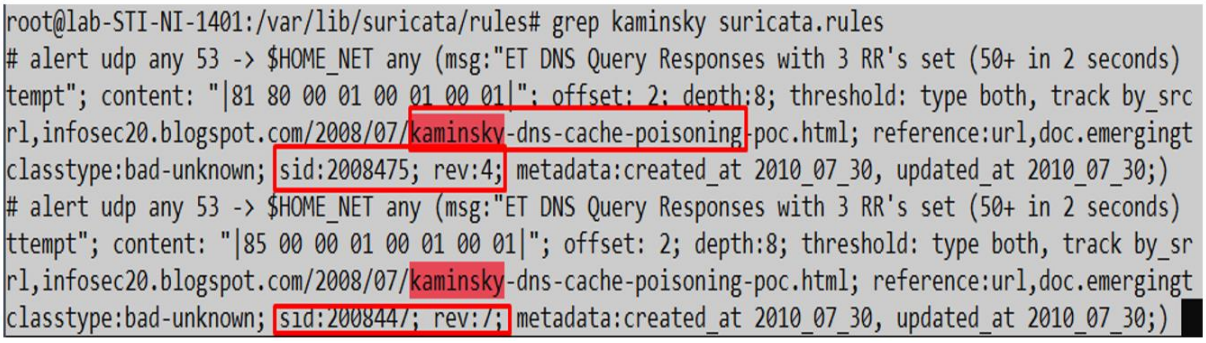
Figure 5. Rule information

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

Source: Author (2023).

The logs' analysis by the ForDNS tool searches key words such as the identification number (Sid) of the rule and the (Msg) which comprise the message that indicate the type of attack. Figure 6 highlights these key words.

Figure 6. DNS cache poisoning detection rules



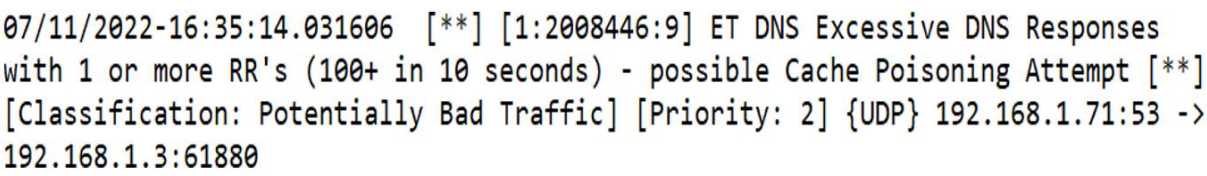
Source: Author (2023).

This information will serve as a basis for analysing the fact and its possible connection to the crime of breaking into a computer device connected to a computer network, pursuant to the Art. 154-A of the Brazilian Penal Code.

4.4 IDS LOG FILE PROCESSING USING THE FORENSIC TOOL

As shown in Figures 7 and 8, the forensic tool processes the data source, i.e., the fast.log file, in search of key words (SIDs) of the rules responsible for identifying attacks.

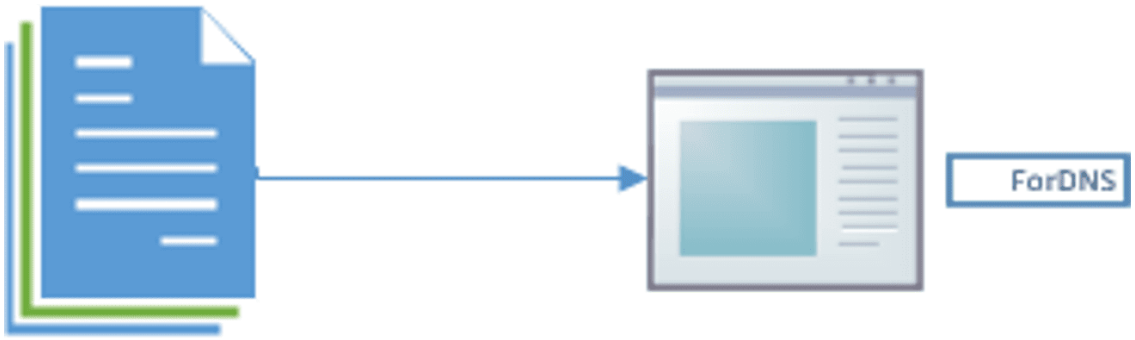
Figure 7. Meerkat IDS logs



Source: Author (2023).

If an intrusion is detected, the tool collects the following data: Source IP, destination IP, date/time, source and ports and the technique used for the attack; these data are then registered in a database as criminal hacking evidence for later analysis. Finally, a report is generated, containing the elements that constitute the offence.

Figure 8. Evidence Processing

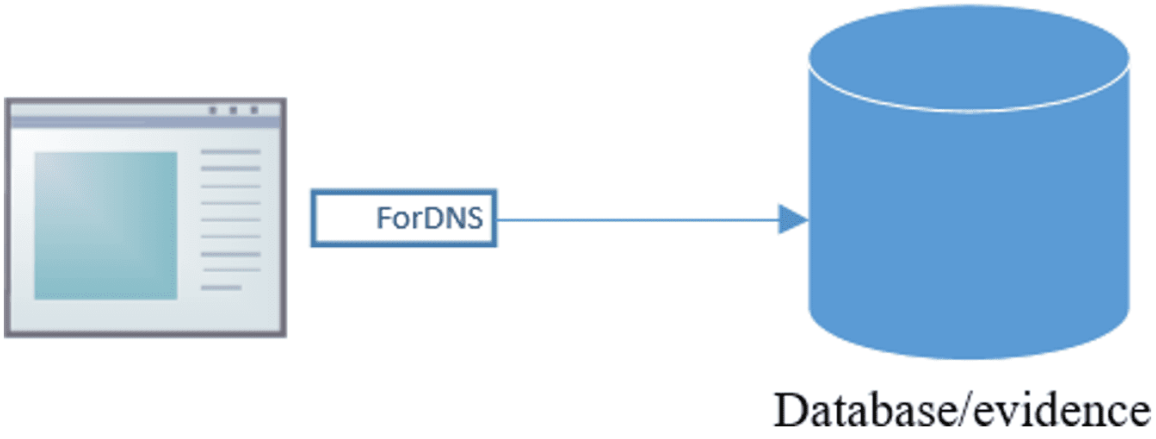


Source: Author (2023).

4.5 REGISTRATION OF EVIDENCE IN THE DATABASE BY THE FORDNS FORENSIC TOOL

As shown in Figure 12, evidence insertion into the database occurs as follows: the forensic tool (ForDNS) analyzes the data source and stores the following data in the new database: type of intrusion technique, date/time of the attack, the source IP (identifies the offender), destination IP (identifies the victim(s) and the DNS server owner), i.e., the attack's origin, who the target was, what invasion technique was adopted and the technical consequences of said attack. These data are used to infer whether the said computer crime –has occurs as per the Brazilian Penal Code.

Figure 9. Storing Evidence



Source: Author (2023).

RC: 146354
Available in: https://www.nucleodoconhecimento.com.br/computer-science/forensic-analysis

Figure 10. Evidence bank

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

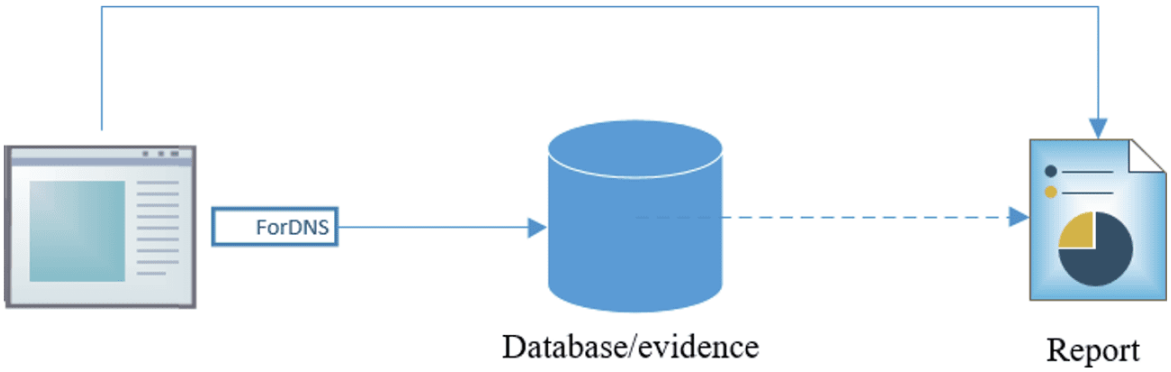
Source: Author (2023).

Despite a partial lack of information in the database, the proposed tool can not only determine the consequences of the attack but also to infer the type of crime based on the legal provision (154-A).

4.6 REPORT

The report generated by the ForDNS tool gathers the extracted information and stores it in a new database. This report will act as the evidence of criminal computer device intrusion, which is subsequently used by investigators and the Judicial Police.

Figure 11. Evidence recording in the report



Source: Author (2023).

Figures11 and 12 show how the report gathers offence information, recording it for the ensuing criminal investigation.

Figure 12. Report generated by the ForDNS tool

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

Source: Author (2023).

4.7 CRIMINAL CLASSIFICATION OF DNS CACHE POISONING ATTACKS

Article 154-A of the Brazilian Penal Code (BRASIL,1940), inserted by Law 12.737/2012 (BRASIL,2012) and recently amended by Law 14.155/2021 (BRASIL,2021) illustrates the crime of hacking into a computer device, regardless of whether it is connected to the World Wide Web.

The IDS, on its own, cannot determine whether a crime has occurred; it only focuses on protecting the network and issuing alerts. Other means are required by law to identify the invasion technique, analyse the invasion procedure (scanning ports or other techniques preparatory to the attack on the DNS service) and pinpoint all criminal factors. The present study focuses on DNS cache poisoning attacks, a technique used to invade a computer device— the DNS Server *in casu*—for obtaining, destroying, or tampering information that allows the correct association of a server's IP address with its website, which is a crime according to the Article 154-A of the Brazilian Penal Code.

4.8 FORENSIC TOOL APPLICATION SCENARIO AND IDS LOG ANALYSIS

This approach enables the analysis of DNS server intrusions under two scenarios: internal and external attacks. The forensic approach was developed for network traffic analysis generated by the Suricata IDS. This IDS identifies and registers the intrusion data by analysing the network traffic and identifying actions aligned with the rules defining various computer network intrusion techniques (Waleed, Jamali and Masood, 2022).

Despite being able to capture the attack evidence, its identification and eventual IDS responses (to alert attacked network services or ban the original attacker device), the IDS does not identify if these occurrences are criminal activities. This data is not only volatile but also constantly overwritten by newer network activity.

In this context, the proposed approach intends to help capture facts flagged by the DME and analyse them under the Brazilian criminal law, considering that not every alert constitutes a crime. Our approach considers the following two scenarios.

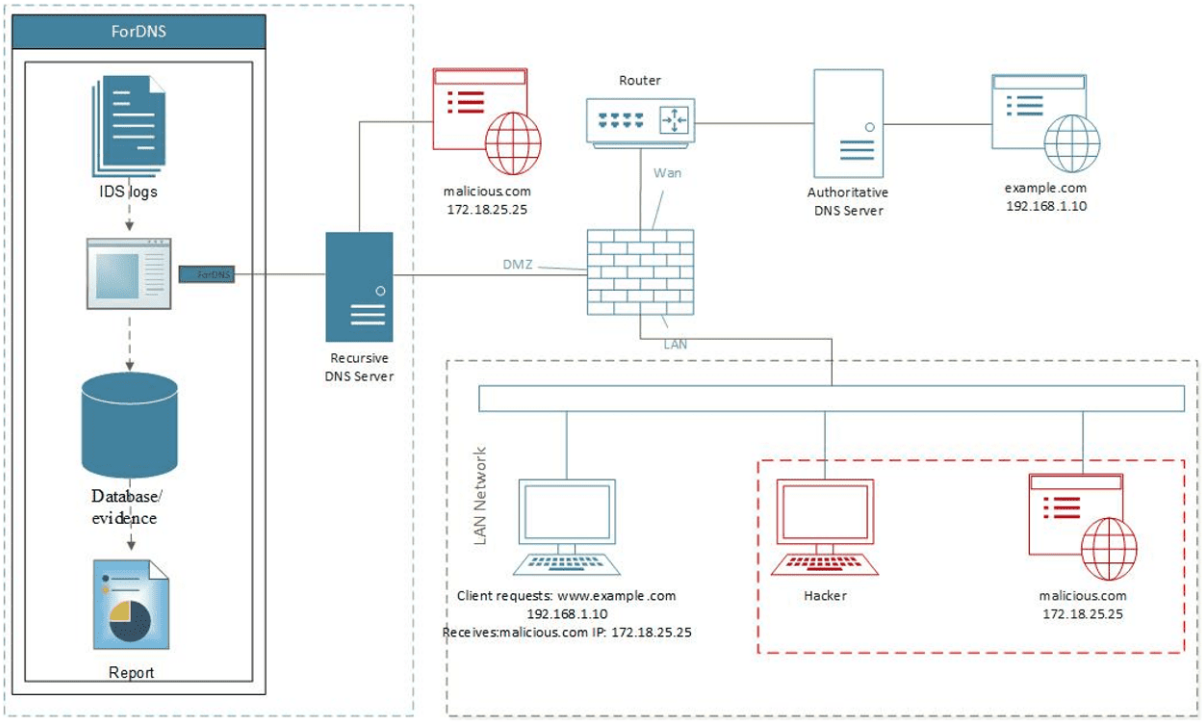
4.8.1 SCENARIO 1: ATTACKER INSIDE THE LAN NETWORK (AUTHENTICATED USER) BREAKS INTO THE LOCAL DNS

Scenario 1 (Figure 13) represents an attack on the recursive DNS. The attacker creates a fake web page, similar to a corporate or institutional site. By applying hacking techniques, it then captures private credentials from systems.

In this scenario, the attacker poisons the DNS cache by inserting the address leading to a fake web page into the recursive DNS server's cache. When trying to access a page by entering a known URL, users are directed to a fake page (almost identical to the real one). Once there, users fall victim to other crimes by entering personal data.

In most cases, cache information is short-lived, and after a few attempts, users manage to access the real page without pecializ the effects of cache poisoning attacks.

Figure 13. ForDNS- internal recursive DNS attack context



Source: Author (2023).

Usually, cache poisoning victims only become aware of attacks once its consequences have pecialized in the form of financial, labour, personal, or other losses. The aforementioned reasons and the delayed revelation of the occurrence make the identification of the perpetrator difficult. Within this context, the need for computer architecture pecialized in detecting and analysing computer fraud identification, as well as storing the evidence of such occurrences, becomes paramount.

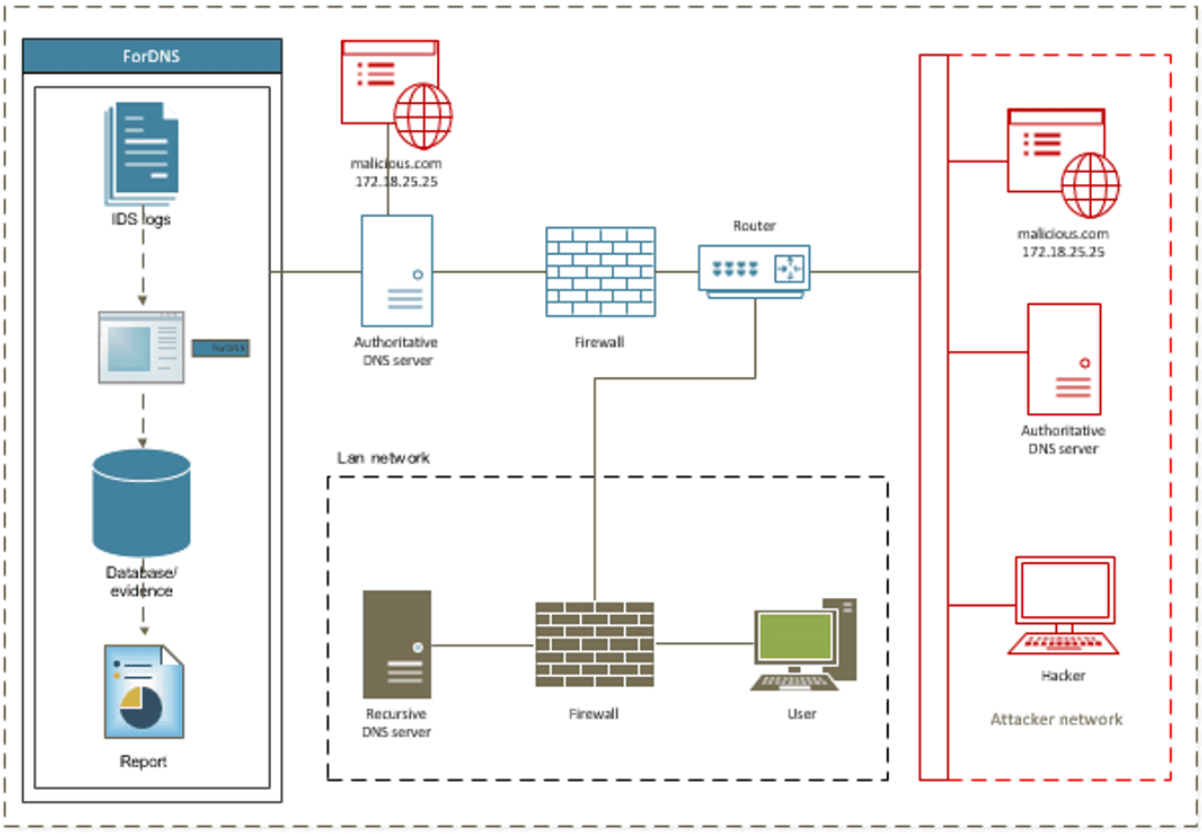
The ForDNS approach tool, as mentioned, prioritises the analysis of this type of attack and extracts criminal evidence, thereby reporting crimes possibly falling under Article 154-A of the Brazilian Penal Code.

4.8.2 SCENARIO 2: ATTACKER ON THE WAN (INTERNET) NETWORK HACKS THE PRIMARY (AUTHORITATIVE) DNS

Scenario 2, Figure 14, depicts an expensive attack whose negative impacts are more than Scenario 1 because it is not restricted to a specific group but extends to all other users of domain name resolution services accessing a certain domain.

In this case, it is a remote DNS attack, which, for some researchers Kim and Reeves (2020) and Zhang et al. (2021), is known as the *Kaminsky* technique where the target is not the recursive server of a LAN, but it is one with the highest rank, a recursive from an ISP requesting a domain from an authoritative DNS server.

Figure 14. ForDNS in a DNS cache poisoning context between an ISP's recursive DNS server negotiation with authoritative



Source: Author (2023).

RC: 146354
Available in: https://www.nucleodoconhecimento.com.br/computer-science/forensic-analysis

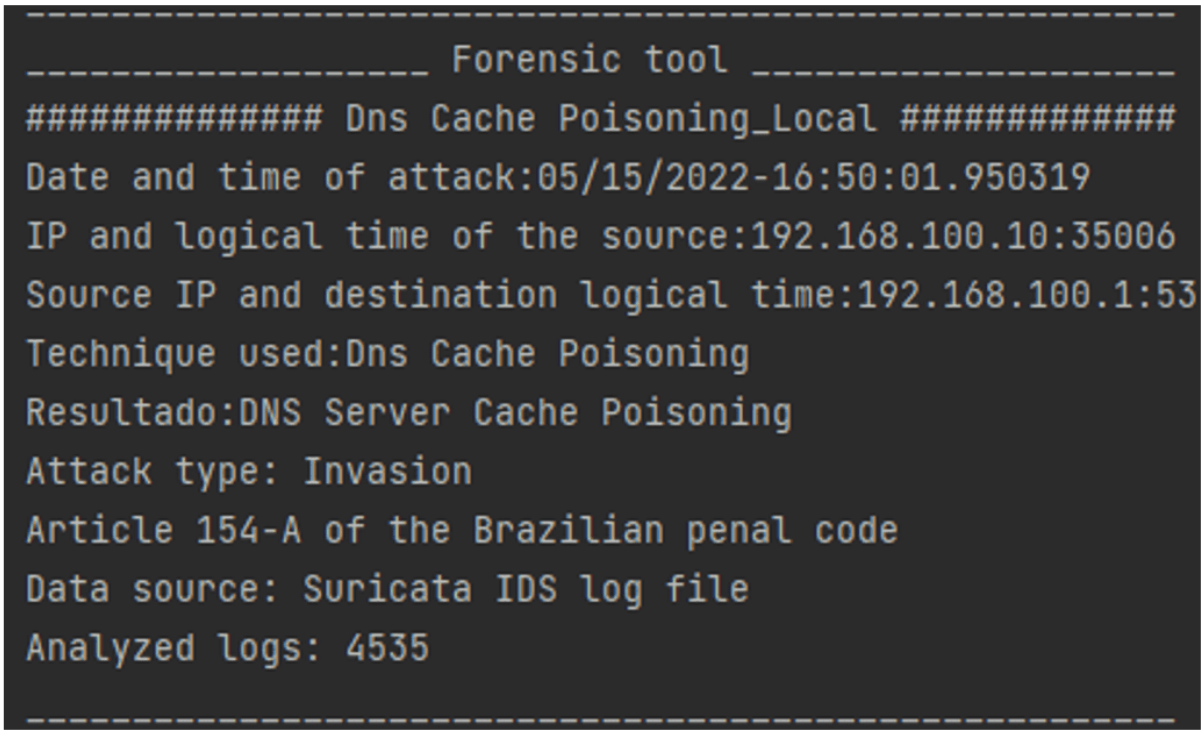
Kaminsky attackers operate remotely and do not wait for users on a private network to generate a DNS query to poison the cache of an ISP's DNS server. The attacker starts by transmitting the ISP's recursive query to an authoritative server and, if it does not have the domain address in cache, it immediately initiates the query to the authoritative server for that domain. It is then that the attacker competes with the authoritative DNS because: while the authoritative tries to send an authentic response to the recursive, the attacker impersonating the authoritative sends a large number of forged responses to the recursive. If the spoofed response matches the one sent during the DNS query, the recursive will accept the spoofed response and temporarily store the malicious domain records in its cache.

The attacker created the opportunity to invade the DNS server by falsifying the validation response between the servers and thereby interrupting the communication between the two; spoofs the IP address of the domain to a malicious one; and finally obtains information from third parties.

This attack is critical because it can be performed repeatedly, or even hijack the DNS or make it unavailable via a distributed DoS (DDoS) attack. Zhang et al. (2021) reports that DNS cache poisoning using the Kaminsky technique was initially directed only to cache poisoning, but that from 2021 it has been acting in tandem with DNS server hijacking. These attacks last longer, thereby resulting in vaster repercussions. Tripathi, Swarnkare and Hubballi (2018) state that they are often supported by DDoS attacks rendering the original DNS server unusable.

Similar to Scenario I, users only realise that they have been attacked when the consequences materialise into losses. Therefore, these computer structures should be monitored so that the DNS server, or any server of a computer application, is being monitored by information security tools when such frauds occur.

Figure 15. Forensic Report (ForDNS)



Source: Author (2023).

As described, the proposed tool is useful for computer crime detection as it captures and stores the main evidence of DNS intrusion in a database. Using this, aforensic report can be filed as evidence under Article154 of the Brazilian Penal Code. (Figure 15).

5. CONCLUSION

The network infrastructures interconnected to the World Wide Web and various servers therein require a protective apparatus to safeguard the integrity of many computational services accessible via the Internet. Firewalls and IDSs serve this protection and security purpose. The IDS identifies the activity and records it in a history file (log), making some previously configured decisions. This constitutes, under Brazilian penal law, the crime of hacking into a computer device. Given that the log file records volatility, which are frequently updated by the large volume of data and alerts generated by network traffic, such evidence is lost, making it difficult collect proof that allows the criminal prosecution of the perpetrators.

In this study, we have proposed an approach that uses forensic tool to extract the IDS-provided data and identify the occurrence of a DNS cache poisoning attack, as well as analyse the various constituent elements of the criminal acts. It likewise enables the provision of evidence for investigations the fact, attacker, victims and technological consequences of hacking the device(s). Additionally, it registers the data in an evidence database provided with the architecture which crosschecks the type of attacks against the relevant legislation. Finally, it also allows non-specialists in network security to log attack activities, preserving history data for future updates in security systems and network services protection.

REFERENCES

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>.

Sent: June 14, 2023.

Approved: June 29, 2023.

[1] Master's student in Computer Science (UFMA), Bachelor in Information System (Estácio), Technologist in Environmental Management (CEST), Specialist in Public Management (UFMA), Specialist in Computer Networks (AVM), Tec. In Informatics (IFMA/ETC-BRASIL). ORCID: 0009-0001-1336-4044. CURRÍCULO LATTES: http://lattes.cnpq.br/4129979584830810.
[2] Advisor. Doctor in Informatics, Master in Electrical Engineering with Concentration Area in Computer Science, Bachelor in Computer Science and Bachelor in Law. ORCID: 0000-0001-8799-1799. CURRÍCULO LATTES: http://lattes.cnpq.br/1531971102610447.