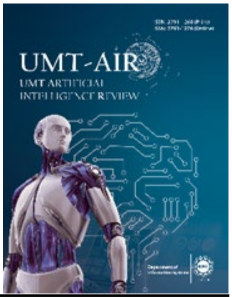
UMT Artificial Intelligence Review (UMT-AIR)
Volume 4 Issue 1, Spring 2024
ISSN$_{(P)}$: 2791-1276, ISSN$_{(E)}$: 2791-1268
Homepage: https://journals.umt.edu.pk/index.php/UMT-AIR

Article QR



Title: **Detection and Prevention of DNS Tunneling Attacks: Exploring Technologies and Methodologies**

Author (s): Usman Inayat[1], and Reamsha Khan[2]

Affiliation (s): [1]University of Management and Technology Lahore, Pakistan
[2]The University of Lahore, Pakistan

DOI: https://doi.org/10.32350.umt-air.41.03

History: Received: March 12, 2024, Revised: April 24, 2024, Accepted: June 07, 2024, Published: June 20, 2024

Citation: U. Inayat and R. Khan, "Detection and prevention of DNS tunneling attacks: Exploring technologies and methodologies," *UMT Artif. Intell. Rev.*, vol. 4, no. 1, pp. 37–45, June 2024, doi: https://doi.org/10.32350.umt-air.41.03

Conflict of Interest: Author(s) declared no conflict of interest

A publication of
Department of Information System, Dr. Hasan Murad School of Management
University of Management and Technology, Lahore, Pakistan

Detection and Prevention of DNS Tunneling Attacks: Exploring Technologies and Methodologies

Usman Inayat[1]*, and Reamsha Khan [2]

[1]Department of Computer Science, University of Management and Technology Lahore, Pakistan
[2]Faculty of Information Technology, Department of Computer Science, The University of Lahore, Pakistan

ABSTRACT DNS tunneling attack is one of the most common and ignored attacks that the current systems are vulnerable to. This study examines the functionality of DNS in terms of DNS hierarchy and the ways through which intruder creates a tunnel. The research used both rule-based and model-based technology tools alongwith other detection-based technologies, namely signature-based and threshold-based technologies. The graphical representation of the tunnel detection technology has been shown to better understand the systematic working of DNS. Based on the review of previous research methodologies, the current research analysed methods for the detection and prevention of DNS tunneling, which includes a location-based model using GPS and observing data packet sizes.

INDEX TERMS attack, DNS, detection, DNS tunneling, spoofing

I. INTRODUCTION

In 1998, DNS tunneling was introduced for the first time to obtain free access to the internet through bypassing all the security hurdles [1]. DNS tunneling has not been considered as an integral attack and sometimes left out unattended as compared to other cyber-attacks [2]. In tunneling, most of the traffic is redirected to a dummy server, which is viewed as a legitimate bypass by security systems. The original data packet is wrapped in various protocols for transmission, allowing the attacker to carry out malicious activities. The network layer protocols are mainly used for this purpose [3].

DNS servers are being monitored continuously to find all the possible vulnerabilities of the attack.

There are a number of ways by which these attacks are made possible.

- Protocol attacks
- Server attacks (based on programs that are running DNS services)
- DNS spoofing
- DNS hijacking [3]

II. LITERATURE REVIEW

A. WHAT IS DNS TUNNELING?

The puncture/disfigurement to any channel of communication through the formation of any restricted or confidential path of communication between any system in the network and any entity outside this network is known as DNS tunneling, which is passed down for observing and getting access to the confidential data within the internet traffic resulting in potential security threat to the organization.

The hierarchy of DNS tunneling is as

*Corresponding Author: usman.inayat@umt.edu.pk follows:

TABLE I
HIERARCHY OF DNS TUNNELING

Level	Description
Root Server	The first one to come in the hierarchy of DNS is the root server which has 13 servers that are labeled as "A to M". The search of the query begins with the root server and thus, it is an essential part of the resolution.
TLD DNS Server (top-level)	The next step after the root server for the query is looking up in the second portion of the domain hierarchy which is the top-level DNS server. It obtains the original IP of the domain name which is requested.
Authoritative DNS Server	The last and final step in the hierarchy of DNS query is the authoritative DNS server. The domain name which has been requested by the user is held at this server. The original IP address will be given to the inquirer.
Recursive DNS Server	As the name suggests, the query is being repeatedly checked. For example, if a user's query is www.umt.edu.pk and the browser let's suppose does not have this IP address, the request will be forwarded to the DNS client which then looks up in the DNS cache and responds accordingly. However, if still the required IP address is not found, the recursive query will look into the DNS hierarchy till it gets the domain which has been requested by the User [4].

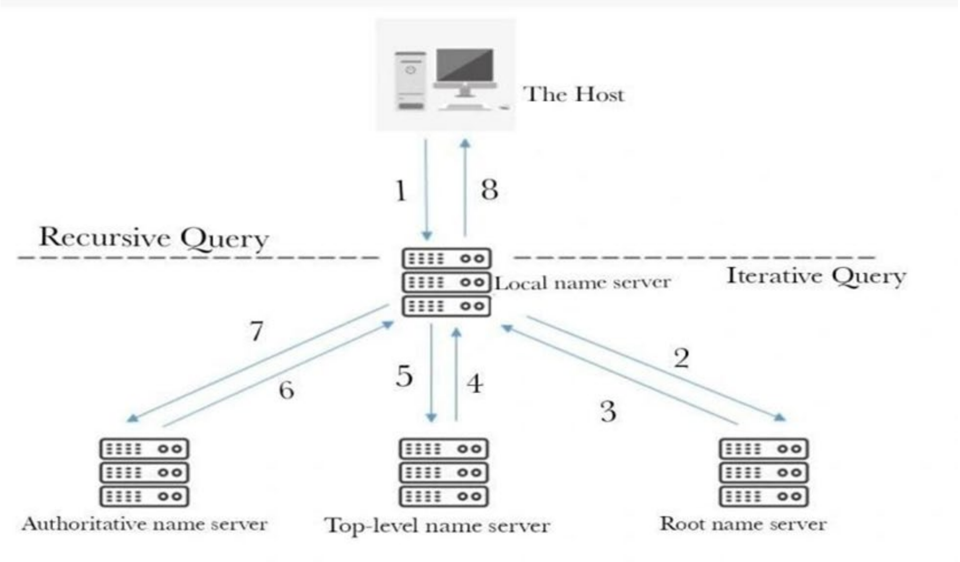


FIGURE 1. Hieracrhy of DNS Tunneling

III. METHODOLOGY

A. QUERY METHOD

The domain is being accessed by two methods as represented in the diagram (Figure 1). As the user sends query to the local server which is said to be recursive, it calls upon for the action to be completed by communicating to the cache if it has surrogated the host to get the IP address.

B. TOOLS FOR ATTACK

The tools used in DNS tunneling so far identified are as follows:

C. RULEBASED TECHNOLOGY

1) DNS2TCP

This tool consists of two main components, Dns2tcpd and Dns2tcpc. The first executes itself on the remote server whereas the latter runs as a client. Any local or remote service relies on TCP connections and the client after listening to the predetermined connection, paves the way for connection requests to an endpoint.

2) DNSCAT

This tool is specifically designed for communication on the internet between two servers. All sorts of firewall and security barrier implemented can be easily overcome.

3) IODINE

The Internet Protocol version 4 (IPv4) traffic is being tunneled where DNS queries are permitted, intercepting the firewalls and keeping itself safe from detection [5]. It's inscribed in C language and run on several other environments, such as Linux, windows, and some other [6].

4)OZYMAN DAN

This tool is based on 4 basic Perl scripts out of which two allow to download and upload the files of end user, whereupon the other two serves as server-client structure. It is a tool utilized either to create a SSH tunnel over DNS or to transfer files.

5) DNSCAT2

The Command and Control (C&C) channel is encrypted by this tool on the DNS protocol. The C2server and client make a communication channel through port 53 of the DNS [7].

6) HEYOKA

This method involves encoding data in the hostname of queries to transfer data between clients and servers using TXT and NULL records. There's a new tool on the horizon called Tunneling and Network Security (TUNS), which works exclusively on UNIX-like systems for both clients and servers. Tunneling and Network Security (TUNS) encapsulates data within the CNAME field. Unlike NSTX and Iodine, it doesn't break up IP packets into smaller DNS packets. The Tunneling and Network Security (TUNS) client sends short queries to the rogue server at regular intervals, preventing DNS servers from making duplicate queries using a caching mechanism. Therefore, TUNS has proven to be effective across a wide range of networks [8].

D. MODEL-BASED TECHNOLOGY TOOLS.

1) FEEDERBOT

It employs authentic DNS syntax for its DNS messages. Messages from the Command and Control (C2) server to the bot are transmitted within the data field of a TXT resource record [9].

2) MORTO

It refers to a type of malware that utilizes DNS tunneling techniques for Command and Control

(C2) communication. DNS tunneling is a method of bypassing network security controls by encoding data within DNS queries and responses, which are typically allowed through firewalls and other network security measures.

E. WHY IS DNS TUNNELING DIFFICULT TO DETECT?

The detection of the DNS tunneling is strenuous as there is no direct relatedness found during the attack which makes it complicated. When a query is created, it is checked recursively or iteratively through the DNS hierarchy to locate the desired domain and retrieve its details, which are then sent back through an authoritative server. DNS traffic is typically brief and contains minimal data. Due to the inherently noisy nature of the DNS protocol, distinguishing normal queries from malicious activities can be challenging for detection systems [4], [10]. C2 communications and data exfiltration are particularly furtive and need to be keenly observed over the time.

The server used by the attacker has malware on it with some similar domain as of the original inquired by the user.

The security was upgraded to a combination of different other protocols to protect the systems. Hypertext Transfer Protocol (HTTP) and Secure Shell (SSH) are the two most commonly used protocols implemented via the application layer [4].

F. DETECTION

The following figure gives an illustration of the DNS tunnel detection technology.

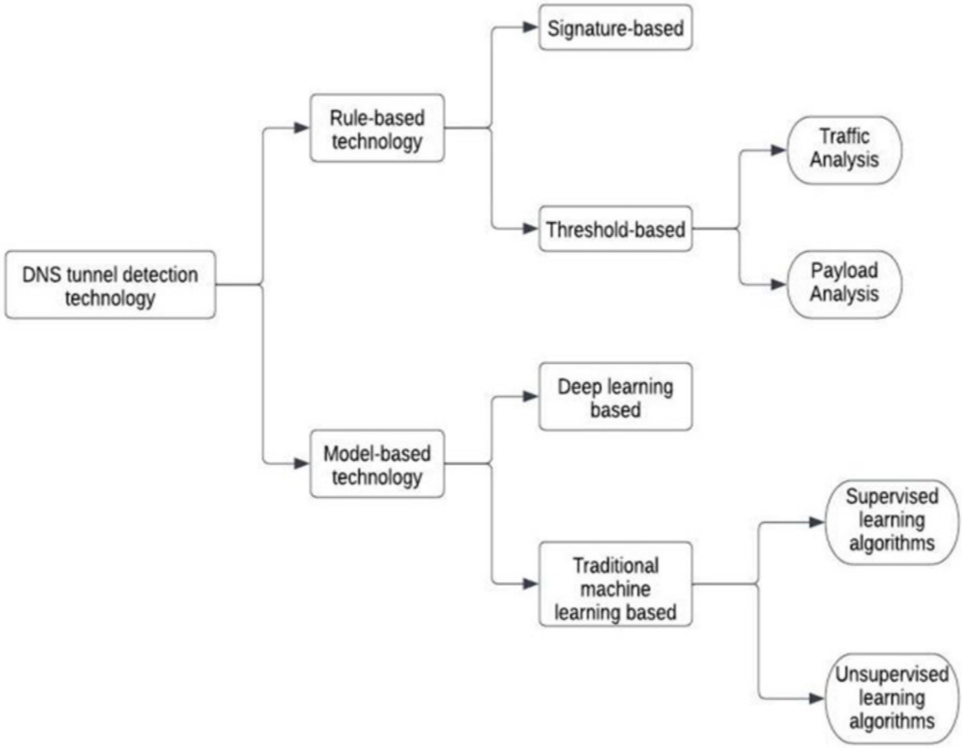

DNS tunnel detection technology
Rule-based technology
Signature-based
Threshold-based
Traffic Analysis
Payload Analysis
Model-based technology
Deep learning based
Traditional machine learning based
Supervised learning algorithms
Unsupervised learning algorithms

FIGURE 2. DNS Tunnel Detection Technology

1) RULE-BASED DETECTION

Rule-based detection involves manually established rules based on the analysis of relevant features. When the monitored traffic matches the predefined rules, the presence of DNS tunnels is detected. The significance of rule-based detection lies in the design of specific criteria, which can be categorized into two types, namely signature-based and threshold-based methods [11].

2) SIGNATURE-BASED METHOD

The signature-based method detects a DNS tunnel by identifying specific signatures. This method relies on well-crafted signatures evaluated by experts. By utilizing deep packet inspection, signatures of DNS tunnel traffic typically found in unique attributes of the DNS header or data content in the payload, can be accurately analyzed. This approach allows for precise detection of DNS tunnels with minimal false positives [3].

3) THRESHOLD-BASED METHOD

The threshold-based method entails detecting DNS tunnels by comparing a pre-established threshold value. This necessitates quantitative analysis of DNS tunnel features to determine a practical threshold. Detecting DNS tunnels involves juxtaposing the preset threshold with the measured value from online traffic recordings. Unlike the signature-based approach, this method identifies DNS tunnels by comparing specific feature values. It aims to pinpoint threshold values for certain features capable of distinguishing between legitimate and tunneling DNS traffic [12].

4) MODEL-BASED DETECTION

Model-based detection automates the creation of identification rules by leveraging various features through a model. Its focal point is training the machine learning model. Machine learning algorithms fall into two main categories, namely traditional machine learning and deep learning. The key disparity between these approaches lies in the feature extraction method and algorithms utilized. Traditional machine learning techniques necessitate experts to manually extract important features during data processing based on their expertise and domain knowledge. In contrast, deep learning methods harness the inherent structure and sequence information within the data to autonomously extract critical features [1].

Various machine learning algorithms are utilized in the field of data science, classified primarily into two categories, namely supervised and unsupervised learning. The supervised learning is giving known labels to instances and it includes algorithms, such as linear regression, classification, and support vector machine. However, for the former one, the instances are not labelled. A familiar algorithm in unsupervised learning is k-means clustering [6].

G. PAYLOAD ANALYSIS

Payload analysis is an analysis of data enclosed within the DNS packets. In payload analysis, the extent of DNS request and response, the entropy of hostnames, and signature analysis via IDS and IPS are done.

1) SIZE OF REQUEST AND RESPONSE

DNS tunneling services often aim to cram as much data as possible into requests and responses. Consequently, it's expected that tunneling requests will exhibit lengthy labels, potentially reaching up to 63 characters.

2) ENTROPY OF HOSTNAMES

DNS tunnels can be identified by assessing the entropy of requested hostnames. Genuine DNS names typically contain dictionary words whereas encoded names show higher entropy. Nonetheless, exceptions exist where DNS names represent specific types of data. Identifying DNS names with elevated entropy levels can suggest tunneling activity.

Threshold-based detection methods typically focus on statistical and domain name-related features of DNS packets. Payload analysis, on the other hand, examines features from a more granular perspective by analyzing the payload data of individual packets or multiple packets. Payload-based features aim to evaluate characteristics related to payload by examining the DNS packets. Payload-based features are frequently employed for real-time detection, with the choice of features in these systems typically linked to the payload—especially those concerning domain names, which serve as input for the system [4].

3) TRAFFIC ANALYSIS

Traffic analysis involves the inspection of DNS packets to discern patterns and anomalies within the traffic. It encompasses various factors, such as the volume of DNS traffic per IP address, per domain, and the number of subdomains or hosts per domain. Additionally, domain history and the volume of replies are analyzed as part of traffic analysis.

The primary focus of traffic analysis is to assess the overall DNS traffic over a given time period, with an emphasis on identifying deviations from expected patterns. Many traffic-based features rely on data collected within specific time windows, making them suitable for non-real-time detection purposes. In contrast, for real-time detection, payload-based features, which examine the content of DNS packets, are often utilized [11].

H. DNS ATTACK DETECTION AND PREVENTION

1) DNS EFFECTS ON DNS PACKET SIZES

In order to identify the DNS tunneling, DNS packet size was observed when the communication took place for the detection of the DNS attack.

Payload and traffic analysis are the two methodologies used for the detection of DNS tunneling.

- Exploring the entropy values A
- Try to differentiate and identify the original DNS name, which typically is short whereas the count of numeric characters was also proposed to look up in the domain name.

A point scoring system is used for detection of DNs attack . In cache poisoning, the attacker gets to manage and upload the spoofed data in DNS server cache, which ultimately leads the traffic to fake IP address, thus landing the user on a malicious site. The word cache poisoning itself suggests that the fake or duplicate data is no less than a poison in the cache.

Its works in the following ways.

1. The fake headers are added to the http obtained from the code of web, after identifying the possibilities for the attack.
2. The original cache server data is deleted and replaced.
3. Fake generated requests similar to the original are being sent to cache server for completing the desired request of user with

the malware.

Up-to-date DNS servers along with the proper configuration of the security updates available is a preventive measure suggested by the above-mentioned system. Domain Name System Security Extensions (DNSSEC) is one of the softwares that provides the authentication of the DNS.

I. DNS AMPLIFICATION

A DDoS attack is a commonly exploited DNS feature that escalates the domain name to a more basic level [3], [12].

1) LOCATION-BASED MODEL FOR PREVENTION OF DNS SPOOFING

The main focus of this model is on DNS spoofing, also known as DNS cache poisoning. The proposal to prevent DNS spoofing was earlier developed under the title A Secure, Flexible Framework for DNS Authentication in IPv6 Auto Configuration in which two (02) protocols were used, namely Transaction Signal (TSIG) and Domain Name System Security Extensions (DNSSEC). Another new technique of the CGA-TSIG algorithm was also introduced, which was executed by the use of three (03) cookies [13], [14].

III. PROPOSED SOLUTION

The use of Global Positioning System (GPS) was made effective for identifying the precise location of the user for the identity authentication. Any intruder attempting to redirect the request away from the specified list of DNS servers will cause delays, making it clear that the request is being handled from a different location, and it will not be accessible.The scenario presented here is based on creating username, password, and user's physical location, which if justified then only the DNS server will be accessed otherwise blocked. The results derived from the practical implementation of this case through a virtual environment showed that many requests were denied access, thus preventing the DNS tunneling [13], [15].

IV. CONCLUSION

DNS is an essential service for regulating the internet's operation. Due to the vast number of networks, DNS traffic is neither limited nor monitored. Therefore, DNS plays a crucial role in maintaining the availability of company websites and online services. This study explored the functioning of DNS, including its hierarchy and how intruders create tunnels within the DNS system. Few of the DNS tunneling detection techniques were viewed that used rule-based method and model-based method. As, these methods cover different scopes of tunneling detection, they were analysed to better specify the scope of research.

CONFLICT OF INTEREST

The author of the manuscript has no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

DATA AVALIABILITY STATEMENT

Data availability is not applicable as no new data was created.

REFERENCES

[1] Y. Wang, A. Zhou, S. Liao, R. Zheng, R. Hu, and L. Zhang, "A comprehensive survey on DNS tunnel detection," *Comput. Net.*, vol. 197, Oct. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108322.

[2] Amazon Web Services. "What is DNS?" AWS.amazon.com. https://aws.amazon.com/route53/what-is-dns/ (accessed June 01, 2022).

[3] U. T. Gudekli and B. Ciylan, "DNS

tunneling effect on DNS packet sizes," *Int. J. Comput. Sci. Mob. Comput*., vol. 8, no. 1, pp. 154–162, 2019.

[4] Sanjay, B. Rajendran, and P. Shetty, "DNS amplification DNS tunneling attacks simulation, detection and mitigation approaches," in *Proc. 5th Int. Conf. Invent. Comput. Technol.*, Feb. 2020, pp. 230–236. doi: https://doi.org/10.1109/ICICT48043.2020.9112413.

[5] Elastic Security Solution. "Potential DNS tunneling via Iodine." Elastic.co. https://www.elastic.co/guide/en/security/current/potential-dns-tunneling-via-iodine.html (accessed July 05, 2022).

[6] S. Yassine, J. Khalife, M. Chamoun, and H. E. Ghor, "A survey of DNS tunnelling detection techniques using machine learning," presented at the International Conference on Big Data and Cyber-Security Intelligence, Hadath, Lebanon, Dec. 13–15, 2018.

[7] Raj. "DNScat2: application layer C&C." Hackingarticles.in. https://www.hackingarticles.in/dnscat2-application-layer-cc/ (accessed June 02, 2022).

[8] D. Tatang, F. Quinkert, N. Dolecki, and T. Holz, "A study of newly observed hostnames and DNS tunneling in the wild," *arXiv*. Feb. 2019, http://arxiv.org/abs/1902.08454

[9] C. J. Dietrich. "Feederbot botnet using DNS as carrier for command and control (C2)." Chrisdietri.ch. https:///post/feederbot-botnet-using-dns-command-and-control/ (accessed July 05, 2022).

[10] ExtraHop. "DNS tunneling attack: Definition, examples, and prevention." ExtraHop.com. https://www.extrahop.com/resources/attacks/dns-tunneling/ (accessed July 05, 2022).

[11] M. Sammour, B. Hussin, M. F. I. Othman, M. Doheir, B. AlShaikhdeeb, and M. S. Talib, "DNS tunneling: A review on features," *Int. J. Eng. Technol.*, vol. 7, no. 3.20, p. 1–5, Sep. 2018, doi: https://doi.org/10.14419/ijet.v7i3.20.17266.

[12] N. Abdelmajid, A. Amin, and S. A. R. Farhan, "Location based model for prevention DNS spoofing," in *ACM Int. Conf. Proc. Ser.*, Jan. 2020, pp. 1–4, doi: https://doi.org/10.1145/3424311.3424329.

[13] U. Inayat, M. F. Zia, F. Ali, S. M. Ali, H. M. A. Khan, and W. Noor, "Comprehensive review of malware detection techniques," presented at Int. Conf. Innov. Comput., Lahore, Pakistan, Nov. 9–10, 2021, doi: https://doi.org/10.1109/ICIC53490.2021.9693072.

[14] M. F. Zia, U. Inayat, W. Noor, V. Pangracious, and M. Benbouzid, "Locational detection of false data injection attack in smart grid based on multilabel machine learning classification methods," presented at IEEE IAS Glob. Conf. Renew. Energy Hydro. Technol., Male, Maldives, Mar. 11–12, 2023, doi: https://doi.org/10.1109/GlobConHT56829.2023.10087717.

[15] U. Inayat, F. Ali, H. M. A. Khan, S. M. Ali, K. Ilyas, and H. Habib, "Wireless sensor networks: Security, threats, and solutions," presented at Int. Conf. Innov. Comput., Lahore, Pakistan, Nov. 9–10, 2021, doi: https://doi.org/10.1109/ICIC53490.2021.9693021