DNS amplification attack

Andreoli C. • Ligari D. • Alberti A. • Scardovi M. • Intini K.[1]

[1]*Department of Computer Engineering - Data Science, University of Pavia, Italy*
Course of Enterprise digital infrastructure

Abstract

Only two levels of sectional headings, `\section` and `\subsection`, should be used. Ad nemo aut quae dolores nesciunt reprehenderit occaecati. Optio distinctio at aliquam odit dolores laudantium. Illum et qui iste et laudantium dolorum. Nihil quis qui at quia alias. Quisquam ea sit aspernatur. Labore at hic voluptas cumque eum officia repellat.

Keywords— DNS server • DDoS Attack • Wireshark • Dig • Top • Ping

Dizdar 2021 Fang *et al.* 2021 Wei-min, Lu-ying, and Zhen-ming 2010 Taylor 2021 Dizdar 2022 Yoachimik 2023 Devi 2015 Vries, Schmidt, and Pras 2016 Meitei, kh, and De 2016 Mathews *et al.* 2022

1 DNS based DDoS attacks

The DNS service is a critical part of the Internet infrastructure. Almost every communication exploits the DNS service, and attacking it could lead a significant number of networked applications to run out of service. The DNS service has been designed to provide fast responses and is less oriented towards security, which makes it vulnerable to different types of attacks. According to a recent Cloudflare's report Yoachimik 2023 the most used vector in DDoS is the DNS. The types of attacks involving DNS are of three main types: *DNS query flood*, *TCP flood*, *DNS reflection and amplification*, and *DNS water torture*.

DNS query flood

This is a direct attack aimed at consuming the server resources until run it out of service. The attacker sends a large number of DNS queries to the target recursive DNS server, leveraging a zombie devices army (botnet). The requests are structured in a way that the server has not the record cached and it is forced to perform recursive queries to provide the responses. It is easier to perform this type of attack on smaller DNS servers that may have limited resources to handle a large number of queries.

TCP flood

This is another type of attack aimed at consuming the server resources. These latter are consumed by the attacker sending lots of TCP connection requests without closing them. The server is forced to allocate resources to handle the TCP connections and, when the numbers get larger it may run out of resources.

DNS water torture

This is a type of indirect attack aimed at consuming the resources of a target authoritative DNS server. The attacker sends a huge number of queries about properly constructed hostnames. These are made up by two parts: the domain whose authoritative server is the target, and a random string such that the FQDN cannot exist. That way the recursive NS starts its search until it reaches the authoritative server. This latter notices the non-existence of the FQDN and sends NXDOMAIN response. All the queries travel until the authoritative server, which is forced to handle all of them until it is overwhelmed.

DNS reflection and amplification

This is an indirect attack aimed at consuming the target network bandwidth. It start with the spoofing of the target's IP address, then lots of queries are sent to the DNS server using as the source address the spoofed IP address. This latter will receives the responses from the DNS server (reflection). The queries are structured in a way that the responses are larger in size (amplification). That way the target's bandwidth is fulfilled, with the attacker having used just a small quantity of its resources. The effectiveness of this attack is given by the amplification factor (AF), measured as the ratio between the size of the response and the size of the query. An easy but effective choice for the attacker is to perform a type ANY which provides a large AF.

Since according to the already cited report Yoachimik

2023 the most common type of attack is the DNS reflection and amplification, in this project we focus on this type of attack.

2 Experimental setup

To ensure the success of the project, it is essential to establish a clear methodology and employ a well-defined set of tools. This section aims to provide a detailed explanation of the methodologies utilized to accomplish the project's objectives.
The selected methodologies encompass a systematic approach that allows for the accurate replication of a DDoS attack while maintaining ethical considerations and minimizing the potential impact on live networks. These methodologies were carefully chosen to ensure the reliability and validity of the experimental results. The methodological approach used is the following:

Why
The objective of this study is to assess the impact of a DoS attack, exploiting the DNS protocol and monitor the reachability of the targeted device and other network nodes. By simulating realistic attack scenarios, this study aims to understand the vulnerabilities within the DNS protocol, evaluate network resilience, and identify potential countermeasures.

Which/Who
The chosen target for the DDoS attack is a laptop (HP ENVY x360), which acts as a host for a DNS server running BIND9. Two laptops, specifically a MacBook Pro 14 and another device (to be specified)!!!!!!!!!!!!!!!!, are utilized as vantage points to initiate the attack.

What
The chosen metrics include measuring the response time for each ICMP or DNS message sent, accounting for potential timeouts. Furthermore, the CPU and memory utilization of the DNS server were also monitored during the simulation.

Where
The vantage point is a MacBook Air inside the network and passive to the attack.
To ensure the security and stability of public networks and devices, the DDoS attack simulations were conducted within a local area network (LAN) environment.

3 Tools used

Ping
Ping is a network utility tool used to test the connectivity between two networked devices. It sends a small packet of data to a specific IP address or hostname and measures the time it takes for that packet to be received and returned. The result shows the round trip time (RTT), as well as the number of packets sent and received, and any packet loss that may have occurred.
While it is a useful tool for testing network connectivity, it has some limitations, it uses the ICMP protocol to send and receive packets, which may not always be allowed by network firewalls or routers, and it does not support different protocols like TCP or UDP. This means that if a network is configured to block ICMP traffic, the ping command may not work. Moreover ping provides only basic information about network connectivity, it does not provide information about bandwidth or the structure of the network.

Dig
The dig command (short for "domain information groper") is a popular network administration tool used to perform DNS queries. It allows users to perform DNS lookups to check DNS records and obtain information about DNS configurations. It is a versatile tool that allows users to specify different query types, such as A, AAAA, MX, TXT, and others. It can also be used to perform reverse DNS queries, where an IP address is used to retrieve the corresponding domain name. In addition to provide detailed DNS query results, the dig command can also be used to troubleshoot DNS issues, such as misconfigured DNS servers, slow DNS resolution times, or DNS cache issues.

Top
The top command provides real-time monitoring of system resources, such as CPU usage, memory utilization, running processes, and more. When executed, the top command displays an interactive, dynamic table that continually updates, allowing users to view the current state of their system and identify any processes consuming excessive resources. The top command also provides options to manipulate the displayed information and perform actions on running processes, such as terminating or changing their priority.

Wireshark
Wireshark is a open-source network protocol analyzer. It is designed to capture, analyze, and display network

traffic in real-time. Wireshark allows users to inspect and interpret the data packets transmitted over a network, providing detailed information about the communication between different devices.
In addition to passive packet capturing, Wireshark offers powerful filtering and search capabilities, allowing users to focus on specific types of traffic or specific packets of interest. It also provides features for advanced analysis, such as the ability to reconstruct and view streams of data, perform statistical analysis, and even export captured data for further investigation or reporting

4 DNS Server

For the simulation of the DDoS attack, a dedicated DNS server was established on a virtual machine running the Ubuntu 24.04 LTS operating system. The virtual machine was allocated 2GB of RAM and 2 CPU cores to ensure sufficient resources for handling the simulated traffic.
To create the DNS server, the open-source software BIND9 was employed. This widely adopted DNS server software offers robust functionality and configurability. The server was specifically configured to act as the authoritative server for the domain name "ediproject.com." By assuming authority over this domain, the DNS server can respond to DNS queries and provide legitimate DNS responses during the simulation.
To mimic the characteristics of a genuine DNS server, a total of seven NS records and five MX-type records were meticulously added to the DNS server's configuration. The inclusion of these records introduces diverse amplification factors, enabling the analysis of the DDoS attack's effectiveness based on these factors. By incorporating varying NS and MX records, the simulation can reflect the behavior of a real DNS server and offer insights into the impact of different amplification configurations on the severity of the attack.

5 Mitigation measures

There exist a variety of measures that can be employed to mitigate the effects of DNS amplification attacks. These measures can be broadly categorized into two groups: those that aim to reduce the probability of an attack occurring, and those that aim to minimize the impact of an attack by detecting it early and enhancing the resilience of the DNS service.

5.1 Proactive measures

Rate limiting

Rate limiting is a measure that can be used to mitigate the impact of DNS amplification attacks. The idea behind rate limiting is to limit the number of responses that a DNS server can send to a specific IP address within a certain time period. That way the queries sent by the attacker are dropped by the DNS server, thus reducing the amplification effect.

Trusted sources

When a DNS recursive server is open on the Internet, it can receive queries from any source. The range of IP addresses that can be spoofed is very large and it is not possible to block all of them. However, it is possible to limit the number of sources that can send queries to the DNS server, creating a whitelist of trusted sources. This measure reduce the probability of an attack occurring, however, the trusted sources could be spoofed, thus the attack be performed.

Firewall

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. Setting up a proper firewall both DNS server side and victim side can block unauthorized traffic and reduce the impact of the attack.

5.2 Detection measures

The DNS amplification attack has as core activity the IP spoofing. A mechanism able to discriminate between a original source IP address and a spoofed could detect the attack. This is the main idea behind the *detection* techniques.

Routing hops detection

This mechanism was proposed by Jin and Wang in this paper Jin and Wang 2003. The idea is to exploit the inconsistency between the number of hops of a spoofed IP packet and the spoofed IP address itself. The hops number is inferred by the TTL value in the IP header. This mechanism can detect almost 90% of the spoofed packets.

Machine Learning

In the last decade with the developing of machine learning, some algorithms have been proposed to detect the DNS amplification attack. In 2015 Meitei, kh, and De Meitei, kh, and De 2016 proposed a machine learning

based approach to detect the attacks, using *Random Forest*, *MLP* and *SVM* algorithms. However, a more recent publication Mathews *et al.* 2022 by Mathews *et al.*, shows that using an adversarial neural network approach (EAD) it is possible to easy circumvent the detection. The idea is to train a network to slightly modify the input data (DNS queries) in order to fool the detection algorithm.

5.3 Resilience measures

These measures are more focused on making the DNS more robust to the attack, allowing it to continue to provide the service even during the attack.

Anycast scheme

The DDoS attack is aimed at causing a service outage on a victim server by flooding it with a large number of packets. The idea behind the anycast solution is to have many replicas of the victim server with same logical IP address, and to choose the destination of the packets according to some routing criteria. That way, the packets are distributed among the replicas, thus reducing the load on each of them. In 2015, a large-scale DDoS attack was launched against the DNS root name servers, resulting in denial of service for some of them, as reported by Vries, Schmidt, and Pras 2016. The attack demonstrated that although the use of anycast schema can increase the resilience of DNS servers, it cannot entirely protect against DDoS attacks. However, due to the deployment of anycast technology in 11 out of 13 root servers, the impact of the attack was limited and partially mitigated.

Caching behavior

This approach is discussed by Wei-min, Lu-ying, and Zhen-ming in this paper Wei-min, Lu-ying, and Zhen-ming 2010. They support that a relatively simple change in the caching behavior of a DNS server can significantly improve the DNS performance under a DDoS attack. They propose a DNS server should not evict the cache entries when it detects the relevant DNS servers are unavailable and delete them as soon as this latter become available again. That way, even during an attack running out of service a relevant server, the DNS recursive server can still serve the cached entries, thus providing part of the requested domain names.

References

Devi, G. U. 2015. "Detection of DDoS Attack using Optimized Hop Count Filtering Technique" [in en]. *Indian Journal of Science and Technology* 8, no. 1 (January): 1–6. ISSN: 09746846, 09745645. https://doi.org/10.17485/ijst/2015/v8i26/83981.

Dizdar, A. 2021. *DNS Amplification Attack: How they Work, Detection and Mitigation* [in en-US], October. Accessed May 9, 2023. https://brightsec.com/blog/dns-amplification-attack/.

———. 2022. "5 DNS Attack Types and How To Prevent Them" [in en-US]. *Bright Security* (May). https://brightsec.com/blog/dns-attack/.

Fang, L., H. Wu, K. Qian, W. Wang, and L. Han. 2021. "A Comprehensive Analysis of DDoS attacks based on DNS." *Journal of Physics: Conference Series* 2024:012027. https://doi.org/10.1088/1742-6596/2024/1/012027.

Jin, C., and H. Wang. 2003. *Hop-count filtering: an effective defense against spoofed DDoS traffic,* January.

Mathews, J., P. Chatterjee, S. Banik, and C. Nance. 2022. "A Deep Learning Approach to Create DNS Amplification Attacks." In *2022 4th International Conference on Management Science and Industrial Engineering (MSIE),* 429–435. ArXiv:2206.14346 [cs]. April. https://doi.org/10.1145/3535782.3535838. http://arxiv.org/abs/2206.14346.

Meitei, I., J. kh, and T. De. 2016. *Detection of DDoS DNS Amplification Attack Using Classification Algorithm,* August. https://doi.org/10.1145/2980258.2980431.

Taylor, R. 2021. *Four major DNS attack types and how to mitigate them* [in en-US], August. Accessed May 10, 2023. https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/.

Vries, W. de, R. Schmidt, and A. Pras. 2016. "Anycast and Its Potential for DDoS Mitigation." *ResearchGate* (June). https://doi.org/10.1007/978-3-319-39814-3_16.

Wei-min, L., C. Lu-ying, and L. Zhen-ming. 2010. "Alleviating the Impact of DNS DDoS Attacks." *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing* 1:240–243. https://doi.org/10.1109/NSWCTC.2010.63.

Yoachimik, P. 2023. *DDoS threat report for 2023 Q1_2023* [in en], April. http://blog.cloudflare.com/ddos-threat-report-2023-q1/.