Towards Understanding Denial of Service Attacks: Identifiers, Propagation, Derivatives and Mitigation

Jyothi Cameron

COM-309: Network Theory & Design

Professor: Dr. Eduardo Bautista

10-17-2021

Abstract

Denial of Service (DoS) attacks are those that overload a sever by inundating it with requests. This can cause a computer to act unexpectedly or even crash because the resources are being pushed beyond their architectural limits. By using a network of infected computers, otherwise called a "botnet," to magnify the effects by both increasing and distributing the requests between nodes, the execution time of the attack is decreased proportionally to the pool of cumulative computing power of the botnet. To better harden critical networks from dangerous attacks like these, whose scale is such that ever larger server systems can be ground to a halt, it is essential to understand the motivations of the individuals who would perform them as well as the mechanics of the attacks themselves.

Keywords: botnets, denial of service, distributed denial of service, networking, malware, information security

Towards Understanding Denial of Service Attacks: Introduction

The author is an undergraduate cybersecurity major at Saint Leo University. To successfully train in network hardening, incident response, and computer forensics, a foundational approach to networking techniques and computer science are embedded into the degree program. The author's interest in distributed computing concepts and network protocols led to a fascination with Distributed Denial of Service attacks, discussed in this paper. Due to the author's current lack of knowledge, this paper could suffer from what is called the "Dunning-Kruger Effect," wherein the ignorance to this topic beforehand undermines its inherent complexity and this will be addressed. This paper is intended as an informative piece aimed at individuals with limited-to-intermediate knowledge of the subject and assumes as much. Topics will be discussed in breadth and only expounded upon at the author's discretion to better refine the relevant concepts.

The Internet today is far more complex than its predecessor built in the 1980's. By 2025, about 463 exabytes of data will be generated daily (World Economic Forum, 2019), and it will be moved between desktops, workstations, mobile and IoT devices through a maze of cables, modems, routers, and servers. Without that Infrastructure life as we know it would be impossible, and the growth of computational devices along with their processing power has been exponential. Due to this dependence, if that same infrastructure were to fail then data communications at many critical endpoints would grind to a halt with potentially catastrophic results.

It is not uncommon for misconfigured networks to fail suddenly, or for hardware to fail and bring a router and by extension an entire Local Access Network, offline; but these are unintentional and unusually not targeted. This same outcome can be reproduced by a Denial of Service (DoS) attack, named as such because it aims to "deny" an organization (represented by a server system) a "service" (the server's ability to perform its function). These attacks by contrast are extremely targeted, and the maliciously induced server crash is the desired outcome.

By understanding the motivations and mechanisms behind these attacks, it is possible to develop techniques to counteract them; both these aspects will be discussed.

Server Fundamentals

A server is a computer that stores network software and shared or private user files (White, 2016), creatively named such because it “serves” data after receiving requests form a “client” device: a web server interacts with a web browser to serve pages, a database server interacts with an application to serve relevant information or perform some work, etc. The client may be in a different network completely, and it is not uncommon for clients from different Wide Area Networks on the planet to send requests to a given server.

Both the client and the server must have the proper encoding software compatible with the Transmission Control Protocol/ Internet Protocol (TCP/IP), along with the proper Network Interfaces to communicate. When a client sends the request, information regarding its location is sent through a modem to the Internet and redirected to the destination LAN’s modem, to a switching platform that redirects it further to the server. The server’s software accepts the request and sends back the necessary data. All of this happens in a fraction of a second (White, 2016).

A given server can handle many requests, even concurrently, but there are both software and hardware limits to every server; once these limits are reached, for example the Random Access Memory reaching capacity or a misconfigured server waiting for an acknowledgement from a client that won’t send one, the server begins to exhibit undesired behavior the least of which is a complete halt of processing called a “hang”.

As the adage goes: “time is money,” and while a server is “hanging,” its organization is unable to provide a service to customers whether that is access to a website or database, ability to stream multimedia or complete transactions and thus loses millions of dollars every second. This makes servers a central point of failure in many business networks and a prime target for DoS attacks.

Denial of Service

Motivations

Before delving into the mechanics of a DoS attack, the motivations of the people behind the attack must be analyzed to grant a more holistic picture of why they deem it necessary to develop the software and infrastructure to conduct the attack in the first place. These “threat actors” can fall into one of three categories: competitors, ideological groups, and nation state actors.

Competitors are business or intellectual rivals who have everything to gain from hindering their opponents’ ability to effectively serve customers, including stealing valuable intellectual property. For example, if a new online service were to be unveiled by Company A but it was covertly overwhelmed by Company B, customers would lose faith in Company A and instead turn to Company B’s more “stable” platform.

Ideological groups do not seek financial gain, but instead perform attacks to forward an agenda. They take aim at organizations they believe to be corrupt and either hinder their effective operations for the sole purpose of causing fiscal damage or go so far as to steal confidential and incriminating sensitive information to expose it and cause defamation. This group may use a DoS attack to shut down an individual or business’ website with which they disagree, then claim responsibility for the attack in order to bring light to that individual or business’ practices. It is not uncommon for a DoS attack to simultaneously act as cover for yet another kind of intrusive attack due to its “noisy” nature, which will be discussed later.

Nation state actors, also called “Advanced Persistent Threats,” are well funded, highly skilled groups that carry out sophisticated, targeted attacks on enemy nations’ infrastructure to cause massive damage, conduct espionage, or both. Of the three categories of threat actors, these are the most dangerous. Their goal is neither money nor fame, but the widespread crippling of critical infrastructure like power grids and air traffic control for the purpose of causing as much damage and chaos to an enemy nation as possible. This is deemed “Cyber Warfare.” **(Ciampa, 2021)**.

Server Exploitation and DoS Attack Types

A DoS attack is an attack on the network: unlike a virus or rootkit it does not aim to steal information and has little need to intrude on a network because its goal is to crash the Internet-facing servers handling data requests, and this can be accomplished from the outside. It is important to note that this is specific to Internet communications, because for a client-server relationship to form, the server must be allowed to receive data from outside of its own LAN in some capacity whereas an Intranet server would be insulated from the internet and only be accessible to devices on an approved LAN. These Internet-facing servers have a high "attack surface," or exposure to being exploited by a threat actor due to their inherently open nature. There are several techniques to effectively halt a server.

A "Smurf Attack" is conducted when an attacker broadcasts a request to several computers but redirects all the traffic back to an unsuspecting victim using a technique called IP spoofing. In this case, the victim was not the one who originally sent the requests but is now being inundated with responses.

A similar technique is called a "DNS Amplification Attack." A Domain Name System (DNS) is a kind of "name resolution protocol" wherein Internet Protocol (IP) addresses are mapped to more identifiable and human-readable addresses. The Internet is integrated with a series of DNS servers that keep an accurate table of all domains and their IP addresses. Because of its role, however, domain servers inherently handle a lot of Internet traffic. In a DNS Amplification attack, the attacker transmits a DNS name lookup request to a public server but spoofs the source to the victim's IP address.

A SYN flood attack exploits the Session Layer of the Open Systems Interconnection (OSI) Model. The Fifth layer, "Session," is responsible for managing open ports and communication windows, or "sessions" between two computers. To initiate a session, computer A first sends a synchronize (SYN) packet to its intended recipient, computer B. B then responds with a unique SYN packet of its own in addition to an acknowledgement (ACK) packet to close A's SYN request, and waits for an ACK packet back from A. Under ideal conditions, the SYN & ACK packet would be received

by A, an ACK would be sent back to B, and the connection would be initiated. However, B must allow for slower computers and internet connections so it implements a period of time where it will wait for an ACK packet. This is what an attacker is exploiting in a SYN flood attack: a sever will “hold” any pending sessions until it receives an ACK response, even while receiving concurrent SYN requests. The attacker knowingly modifies the SYN packet’s source address to fraudulent unreachable hosts and forces the target server to “hold open” several concurrent session requests while receiving yet more spoofed requests. This causes it to run out of memory resources and can induce buffer overflows that severely impact proper functionality (Ciampa, 2021).

Distributed Denial-of-Service

In simple terms, a Distributed Denial-of-Service (DDoS) attack is one that employs all of the aforementioned hallmarks of a DoS attack, multiplied across a network of interconnected devices. By using a network of infected computers, otherwise called a "botnet," and magnifying the effects by both increasing and distributing the requests between them, the execution time of the attack is decreased proportionally to the pool of cumulative computing power of the network. In addition, the scale of the attacks can also be increased meaning ever larger server systems can be ground to a halt, faster.

Botnet Fundamentals

As mentioned above, a botnet is a network of infected devices. As of late, this is not isolated to conventional “computers” but also Internet of Things (IoT) devices. It is highly unlikely that these devices are knowingly compromised by their original owner, so the attacker must first exploit vulnerabilities in these devices to spread malware like worms or use social engineering so that the owner will unwittingly install additional malware like Remote Access Trojans (RATs) that allow the attacker to gain control and use it for nefarious purposes. One such malware is called Mirai, and its goal was to target and infect IoT devices because they are traditionally less secure than other targets. The Mirai botnet consisted of over 300,000 hacked IoT devices and was capable of traffic exceeding 1 Tbps of throughput (Cloudflare, n.d.), allowing it to halt the servers of both Amazon and Twitter, among others (Yamaguchi, 2020).

Once an attacker has gained control over numerous “bots,” they are referred to as a “bot herder.” All the bots must be managed and coordinated from a central point called the Command & Control (C2) server. The misconception that a “server” is synonymous with a large machine in a corporate building betrays the reality that a C2 server can be any computer connected to the internet. In fact, many botnets can scrape HTML pages for their commands, even if that page is hosted on a dedicated hosting service; the bot herder must merely update the web page to issue new commands. Met with the increasing skill of security researchers coupled with the reality that mobile and IoT devices have long eclipsed the number of desktops (O’Dea, 2020), many attackers are shifting to Peer-to-Peer (P2P) C2 architectures wherein any single node can be the server at any given time and it can redirect its traffic through its own network so that “no single point of failure exists within the topology” (Pieterse, 2013).

Mitigation

Firewall Ingress/Egress Filters, NIDS, NIPS

Knowing now a few of the different methods that can result in a Denial-of-Service scenario, it is necessary to discuss ways to mitigate them. Referring again to the OSI model, specialized hardware like firewalls, network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS) are physical devices that provide networking (OSI Layer 3) and Transport (OSI Layer 4) level solutions to generally hardening a computer networks. Specially configuring them to disallow unfamiliar IP addresses, also known as whitelisting, drop packets after a certain buffer time or memory resource ceiling, or even to disallow duplicate requests from the same client or to the same server along with disallowing requests on unauthorized ports prevents congestion and can also drastically increase the perceived efficiency of the network.

Network Load Balancing and Proxy Services

Another Hardware level solution is called Load Balancing. In simple terms this is the concept of employing more hardware; i.e. more compute nodes within a network, that will act as servers and distribute the incoming data requests amongst their resource pool to reduce strain on any individual server. This allows redundancy, because if any

individual node fails then the remaining nodes will absorb its workload and continue to provide uninterrupted service. It also allows for increased efficiency especially in the case of web serving, where any one of thousands of nodes can serve a cached web page to a client in a fraction of a second thus saving bandwidth. In this way, too, a Layer 5 attack such as the SYN Flood described earlier becomes less effective.

Certain Services like Cloudflare do just this, referring to it as a “proxy service”. In addition to this, they also have built in firewalls and network protections along with Application (OSI Layer 7) protection that helps defend against Cross-Site Scripting (XSS) (Cloudflare, n.d.). This Means that Cloudflare is able to provide customers with protection in Layers 3, 4, 5 and 7 of the OSI model, largely insulating their clients’ personal and business websites from DoS and DDoS attack consequences.

Reverse DNS Lookup

In the same way that an attacker can use the DNS service to induce a DoS attack, legitimate entities can utilize a reverse DNS lookup to verify the domain name associated with an IP address that may be flagged for suspicious activity on the network by a firewall or NIDS/NIPS system.

Conclusion

Denial-of-Service attacks are disruptive. They are not meant to be covert, but instead cripple network infrastructure and cause tangible, immediate damage. Sometimes this damage in and of itself is the goal, but many times it is a distraction from another genuinely covert operation from the same attacker. This covert operation can go unnoticed far longer due to the sheer volume of network traffic that the victim would have to sift through to identify it, thus making it an ideal “cover” for attackers. Operations like these not only violate Saint Leo University’s core value of Integrity, but explicitly violate local and federal law and could potentially endanger innocent lives. The continued research of Denial-of-Service techniques along with Distributed Denial-of-Service topographies and methodologies is vital in the defense of interconnected critical infrastructure and Internet services.

References

Ciampa, M. D. (2021). *CompTIA Security+ guide to network security fundamentals* (6th ed.). Cengage MindTap Information Security.

Cloudflare. (n.d.). DDoS Protection with Cloudflare. *Two Pager Rate Limiting Letter*. https://doi.org/https://www.cloudflare.com/resources/assets/slt3lc6tev37/2hIapovmEBdhDq0DLCuwDR/3691243ee090906900ba1a8dce7ddd45/Two_Pager_Rate_Limiting_Letter_EN-US.pdf

Desjardins, J. (2019, April 17). *How much data is generated each day?* World Economic Forum. Retrieved October 10, 2021, from https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

O'Dea, S. (2020, December 18). *Number of mobile devices worldwide 2020-2024*. Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/.

Pieterse, H., & Olivier, M. (2013). Design of a hybrid command and control mobile botnet. *Journal of Information Warfare, 12*(1), 70-82,IV.

White, C. (2016). *Data communications and computer networks: A business user's approach* (8th ed.). Boston, MA: Cengage Custom Publishing. ISBN-13: 978-1-305-76791-1

Yamaguchi, S. (2020). *Botnet defense system: Concept, design, and basic strategy*. Information, 11 (11), 516.