Distributed Denial of Service

Francisco Francillon

***Abstract*—Denial of service attack is a server attack that attempts to prevent authorized users from accessing a system. Perpetrator overwhelms a computer network or system with a very high number of bogus requests which leads the system becoming unable to respond to legitimate requests. Most DoS attacks that take place today are Distributed Denial of Service (DDoS), which involves hundreds or thousands of devices flooding the server with requests [1]. Victims of DoS attacks are often high-profile organizations such as banking, commerce, and media companies. DoS attacks do not typically result in the theft or loss of significant information or other assets, but they can cost the victim a great deal of time and money to handle, and in today's economy time is money. There are several types of DoS attacks. This paper will focus on flooding of services, these attacks include ICMP flood, and SYN flood [2]. This paper will also cover botnet in the use of a Distributed Denial of Service and explain the Mirai botnet attack. Next, I will explain some of the motivation for cybercriminals to commit a Denial-of-Service attack. I will also explain ways that businesses can mitigate some DDoS attacks. Finally, I will look at a real-life case study of the GitHub Memcached DDoS attack.**

Keywords— Denial of service, Distributed Denial of Service, flooding, ICMP flood, SYN flood, Botnet, Cybercriminals, Memcached, Server, Authorized

I. Introduction

Distributed Denial of Service attack has become a major threat to organization today. In recent years many governmental departments, enterprises and public institutions have suffered denial of service attacks at different levels [3]. Finding the person responsible for a DoS attack can be extremely difficult because of how easily it can be engineered from nearly any location. The first DoS attack was done by David Dennis, a 13-year-old in 1974. Dennis wrote a program using the 'ext' command that forced some computers at a nearby university research lab to turn off. DoS attacks have become more complex and sophisticated over the years, attackers include hacktivist, profit motivated cybercriminals and nation states [4].

II. Denial of Service

It is important to understand the difference between DoS attack and DDoS attack. Denial of Service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the action of a malicious cyber threat actor [5]. A threat actor floods the target host or network with traffic until the target cannot respond or simply crash, preventing access for legitimate users. DoS attacks are a huge cost of time and money for organization while their resources and service are inaccessible. The two general methods of DoS attacks are flooding attacks and crash attacks.

A. *Flooding Attack*

The goal of a flood attack is to send an overwhelming traffic to a system that leads the server to buffer, causing them to slow down and eventually stop. There are several types of flood attacks, but I will be discussing ICMP flood, and SYN flood [2].

B. *ICMP Flood Attack*

ICMP flood is also referred to as a ping flood attack. This attack works by the attacker sending an overwhelming ICMP echo request, also known as a ping to the target. Internet Control Message Protocol (ICMP) is typically used to diagnose the health and connectivity of the device and the connection between the sender and the receiver. Traceroute and the ping command both operate using ICMP. Perpetuator exploits the ICMP to overwhelm a targeted device, causing the device to become inaccessible to normal traffic. ICMP requests require some server resources to process each request and to send a response. Bandwidth is required to process both the incoming message (echo-request) and outgoing message (echo reply), the result is a disruption of normal network activity. In order to hide their IP address, attackers often spoof with a bogus IP address. Modern attackers do not spoof their IP address and instead rely on a large network of un-spoofed bots to saturate a target's capacity [6].

C. *ICMP Flood Attack Category*

In order to execute a DoS, attack the attacker first needs to know the target IP address. ICMP can therefore be broken down into three categories, based on the target and how its IP address is resolved. The first category is called a targeted local disclosure. In this category the attacker targets a single computer on a local network, that he/she has knowledge to its IP address. The second category is called a router disclosed. In this form the attacker floods a router to disrupt communication with computers on the network. The attacker must know the router IP address for this attack to be successful. This attack

Identify applicable funding agency here. If none, delete this text box.

leads to all the computers connected to that router being taken down. Finally, the third category of ping flood attack is a blind ping flood. This involves the attacker using an external program to uncover the IP address of the target computer, and/or router before executing the attack.

D. How ICMP Flood Attack is Commited

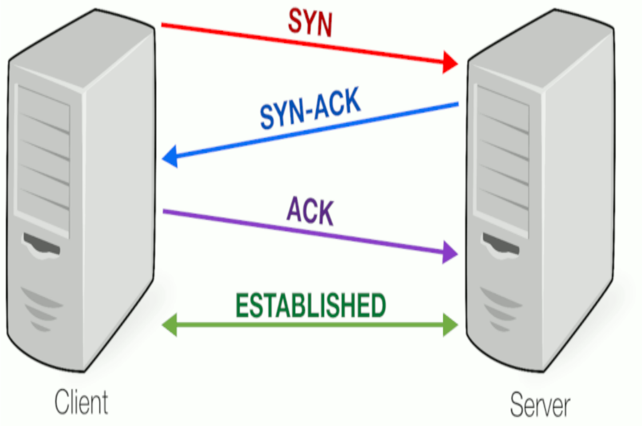
Committing a ICMP flood attack is accessible for anyone with a computer with no knowledge and/or experience to facilitate. The attacker can use the ping command with the option -n which can specify the number of times a request is sent. The attacker can use the -l command to specify the amount of data that is sent with each packet. And the -t command continuously pings the device until it times out. For the ping flood to be sustained, the attacker's computer must have access to more bandwidth than the victim, limiting the ability to commit a large-scale DoS attack. The use of botnet which I will be talking about later has a much greater chance of overwhelming a target device [7].

E. Mitigating ICMP Flood Attack

ICMP flood attack can be mitigated by disabling the ICMP functionality of the targeted router, computer or device. Disabling the ICMP functionality disables the device ability to send and receive any request using ICMP. The consequence of disabling the device ICMP function is the ability to send ICMP requests for testing purposes [6].

F. SYN Flood Attack

SYN flood is similar to ICMP flood as in they are both protocol attacks. The attack aims to flush the target from the network with as much bandwidth as possible. The attacker exploits the three-way handshake of the Transmission Control Protocol (TCP). SYN flood ties up resources by leaving half-open connections. A normal TCP connection the client and server must negotiate a connection, before they can exchange data. A three-way exchange is used for that [8]. The figure below demonstrates how a client must first send a SYN message which the client must acknowledge before establishing a connection.

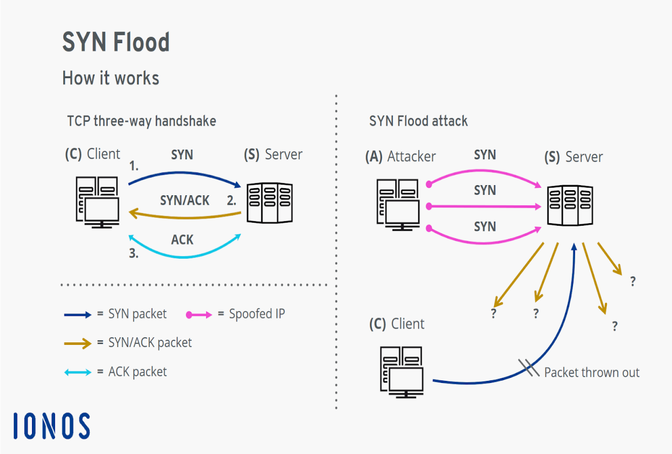


(Fig 1: TCP 3 Way Handshake [9])

A SYN attack exploits this by causing a disturbance of the TCP connection establishment. Specialized software tool is used to trigger a SYN flood. The attack mechanism is as followed:

1. The attacker sends a SYN packet to the server and spoof their IP address
2. Afterwards the server creates a Transmission Control Block data structure for the half-open connection in the SYN backlog. The SYN backlog has a limited memory
3. The server responds to the client with SYN-ACK packets which are never received by the client because the client is using a spoof IP address.
4. The server keeps on sending SYN-ACK messages that it never receives a response back for.
5. During all this the Client continues to send SYN response that the server keeps in its backlog
6. Finally, there comes a point where the server runs out of memory in its backlog and can no longer receive SYN packet causing it to be inaccessible to legitimate requests.

The diagram below summarizes a SYN flood attack.



(Fig 2: SYN Flood Attack [8])

G. Mitigating SYN Attack

There have been several measures put in place to counteract flood attacks. Some of those implementations have some negative side effects or only work under certain conditions. These measures include enlarging the SYN backlog, Recycling the oldest half-open TCP connection, SYN cache and SYN cookies.

1) Enlarging SYN Backlog

This is one of the simplest ways to harden a system against a SYN flood attack. The value of entries for the backlog can have a few hundred of entries, but this can be increased to thousands of entries. This allows more room for SYN backlog.

2) Recycling the Oldest Hald-Open TCP Connection

Companies can make room in the SYN backlog by deleting the older half open connection from the SYN backlog when it is full. Leading to the system remaining accessible during a SYN flood attack. The downside to this is that it does not protect the system from high volume attack.

3) *SYN cache and SYN Cookies*

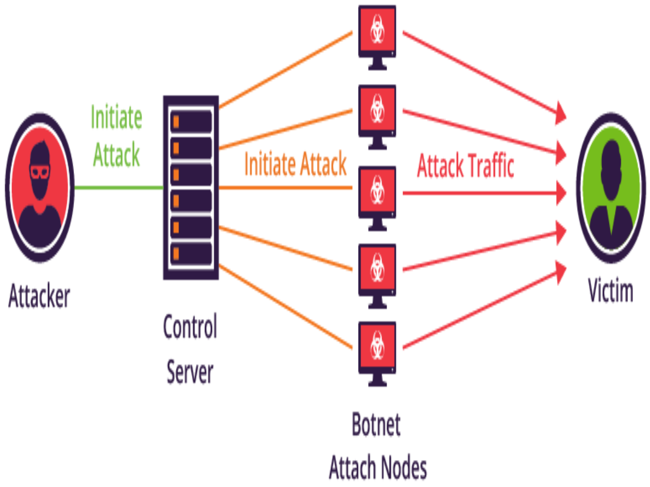
Instead of storing a complete Transmission Control Block in the SYN backlog, the system can choose to keep on a minimum. This is an effective technique; it uses cryptographic hashing to prevent the attack from guessing critical information about the connection. SYN cookies use a specially prepared sequence number to cryptographically verify the connection establishment and to establish a connection. This offers an effective protection against SYN flood attack, but it can also lead to performance losses in certain circumstances. Both techniques can be used together [8].

III. Distributed Denial of service

Distributed Denial of Service on the other hand occurs when multiple machines are operating to attack one target. Threat actor uses botnet to carry out large scale attacks, exploiting security vulnerabilities to control numerous devices using command and control center. Attackers command their botnet to conduct DDoS on a target, the infected devices or botnet are also victims of the crime. With the use of botnet, the attack power significantly increases allowing exponentially more requests to be sent to the target. Due to the huge number of devices being used in the attacks it's even harder to identify the real mastermind behind the actor. The increase of the Internet of Things (IoT) has become more worrisome due to the risk of being part of a botnet. Their use of default passwords and lack of security make them vulnerable to exploitation. Owners of IoT often are not aware that their device is compromised, and an attacker could easily compromise hundreds of thousands of these devices [5].

A. *What is a botnet?*

As stated, before a botnet can be used in a Denial of Service creating a Distributed Denial of service. A botnet is a collection of internet-connected devices that an attacker has compromised. Botnet is used to send large volumes of spams, steal credentials at scale or spy on people and organizations, it is also commonly used in DDoS attacks [10]. Threat actors build botnets by injecting connected devices with malware and a bot herder sends commands through a control center. The malware is often spread by spam, which would leave a backdoor to a device. Botnets are effective because they provide obfuscation, amplification and geographical dispersion. With Obfuscation the attacker can conceal themselves from the victim. Amplification, allow the use of multiple compromise systems gives attacker ability to launch large scale attacks, and geographical dispersion allow for botnets to spam the globe making for a massive, distributed attack that is hard to mitigate [11].



(Fig 3: A Botnet Topology [12])

B. *The Mirai Botnet Attack*

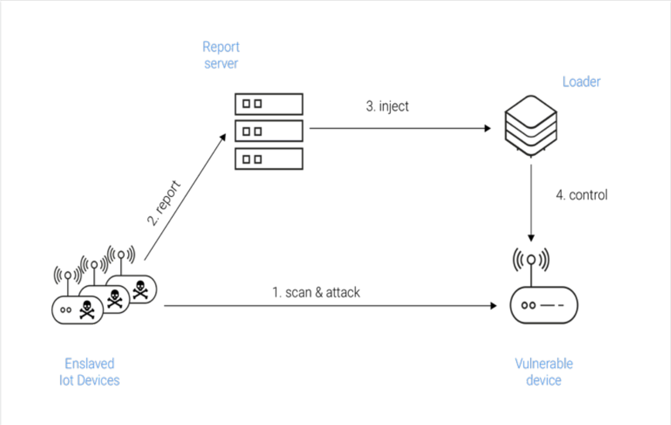
The Mirai botnet attack is an infamous attack that was first reported in late August 2016 and remained in the shadows until mid-September of 2016[13]. Mirai was responsible for taking down a huge swath of websites. These sites include Twitter, Netflix, Spotify, Reddit, and many others. The attack also denied service to all clients of a domain registration service provider called Dyn. Mirai essentially is a malware that scans the internet for IoT devices that still have default or static username and password combination. It takes control of those devices and uses them as bots to overload networks and servers with nonsense requests that slow the speed or shut down the server or service being provided by a host [14].

C. *How Does Mirai Work?*

Mirai is considered both a worm and a botnet. It is a worm because it replicates itself by finding, attacking, and infecting vulnerable IoT devices. And it is a botnet because it is controlled via a central set of Command and Control(C&C) servers that instruct the infected devices on which sites to attack. Mirai consists of a replication module and an attack module.

1) *Replication Module*

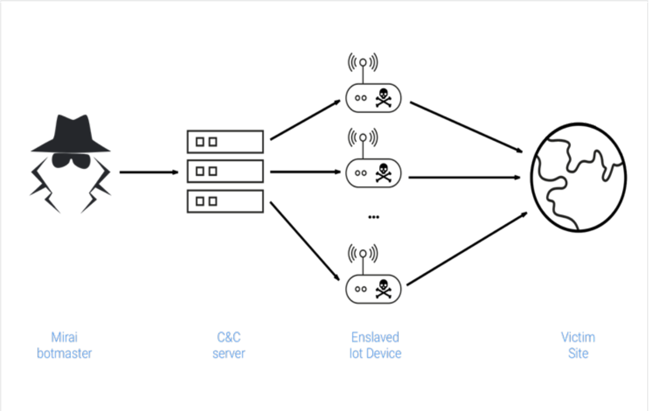
The replication module scans the entire internet for viable targets and attacks. The module then compromises a vulnerable device by using a set of well-known default login/password combinations commonly used by IoT. The module reports it to the C&C servers so it can infect it with the latest Mirai payload. The diagram below illustrates the replication module.



(Fig 4: Mirai Topology [13])

2) *Attack Module*

The attack module carries out the attack against the specific target that the C&C server specified. This module then performs volumetric attack, application-layer attacks, and TCP state-exhaustive attacks, implementing most DDoS techniques such as HTTP flooding, UDP flooding, and all TCP flooding options [13].



(Fig 5: Attack Module[13])

D. *Mirai Attack on Dyn*

Dyn is a DNS server that around 8 percent of the web domains rely on [15]. On October 2, 2016 it was the victim of Mirai. The attack prevented some internet users from accessing Amazon, PayPal, Reddit, and Twitter [13]. The Dyn postmortem reports 23 attack command commands that targeted Dyn infrastructure. The first 21 attacks were about 25 second SYN floods on DNS port 53, along with a few ACK and GRE IP attacks. Afterwards they were hit with a sustained 1-hour attack and 5 hours SYN attack on TCP/53[16]. The Mirai source code was released to the public in a hacker forum leaving it possible for many more similar attacks, and modification to the source code [17]. The rise of copycat is a big concern because Mirai attack can now be conducted my hacker groups, making it hard to discover who is behind those attack.

E. *Mitigating Mirai*

Mirai can be mitigated or averted by IoT vendors. Venders can start by eliminating the default credentials hence preventing hackers from constructing a list of credentials to compromise. Next Venders should mandate auto-patching, this will ensure that no widespread vulnerability can be exploited once discovered. Finally, vendors should implement rate limiting to prevent brute force attacks for users with weak or commonly used passwords [13].

IV. Motivation for Commiting DoS

Attackers commit DDoS attacks against e-commerce sites and banks especially during the holiday season. Extortion or blackmail is another motivation factor to use DDoS attacks, attackers can demand payment in the form of Bitcoin in order to stop the onslaught of traffic [18].

A. *Revenge*

A disgruntled individual or groups behind an attack inflict damages against a company, organization individual for a perceived wrong. Victims include non-profit organization, community college, law enforcement entities, or journalists [18].

B. *Ideological Belief*

Attackers may choose to commit DDoS to demonstrate their technical capability skills. There are a variety of tools, and services available in the dark. Individuals can deploy and experiment with the latest technologies such as automation and botnets against targets [18].

C. *Personal Enjoyment*

Cyberbullying and trolling falls under this category. Actors commit DDoS as a means of enjoyment or vindictive, while also at the same time demonstrating their power to disrupt a web site or a network [18].

D. *Cyberwar*

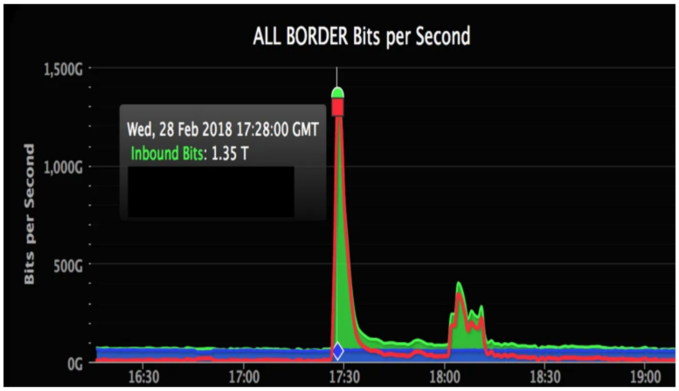
Usually committed with association with a nation state. The goal is to inflict economic or physical impact on its target. Cyber warfare groups are well trained, organized, and are provided with significant resources by the state government to conduct attacks that can disrupt an adversary's critical infrastructure [18].

V. Case Study: Github Memcached DDOS attack

Memcached is an open-source distributed memory caching system that is used for speeding up dynamic web application by reducing database load [18]. A Memcached DDoS attack attempts to overload a targeted victim with internet traffic. The attacker spoofs requests to a vulnerable UDP Memcached server which then floods a target victim with internet traffic. A way to think of a Memcached attack is imagining an attacker calling a restaurant and requesting to order one of everything and telling them to call back and repeat the whole order. The attacker provided the restaurant with a spoof phone number belonging to the victim [19]. Now the victim is now receiving calls from the restaurant with information that they did not request. The victim internet infrastructure is overloaded, and new requests cannot be processed, resulting in a DoS.

A. The GitHub Attack

GitHub is a hosting platform for version control and collaboration. It allows individuals and companies to work together on projects [20]. In February 2018 it was the victim of one of the biggest DDoS attacks that was ever recorded. The attack exploited a vulnerability in the Memcached. According to the GitHub incident report their websites were unavailable from 17:21 to 17:26 UTC and intermittently unavailable from 17:26 to 17:30 UTC due the attack. The attack abused Memcached instances that were inadvertently accessible on the public internet with UDP support enabled. Spoofing of IP addresses allows Memcached responses to be targeted against another address, like the ones used to serve GitHub, it sends more data toward the target than needs to be sent by the spoofed sources. The attack originated from over a thousand different autonomous systems across tens of thousands of unique endpoints. The attack packed at 1.38Tbps via 126.9 million packets per second [21]. The graph below illustrates the attack.



(Fig 6:Github Attack[21])

B. Mitigating Memcached DDoS Attack

In order to prevent such an attack from reoccurring GitHub plans on building more resilient infrastructure that is less dependent on humans. They also plan on measuring their response time to incidents like this to reduce the mean time to recovery (MTTR) [21]. To prevent further Memcached attack Memcached users can disable UDP support if they are not using it. System administrators can check that their Memcached servers are firewalled from the internet [21], in order to prevent entry to network.

VI. Conclusion

This paper explores the aspects of a DDoS attack and explains the difference between DDoS in contrast to DOS attack. ICMP, and SYN flood attacks were deeply described and their impact to organization and individuals. Mitigation for both types of attacks were also stated. Botnet which is considered the power amplification for DDoS was explained, and I discussed the Mirai Attack, which was responsible for taking down a huge swatch of websites. Afterwards I explore the different motivations behind a hacker or individual committing those acts. Finally, I looked at a case study with GitHub Memcached attack, and described some course of action for mitigating that attack.

References

[1] Ciampa, Mark D. *CompTIA Security+ Guide to Network Security Fundamentals*. Cengage Learning, 2018 [accessed April 14, 2020].
[2] "What Is a Denial of Service Attack (DoS)?" *Palo Alto Networks*, www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos [accessed April 14, 2020].
[3] W. Jinhui, "The Current Main Distributed Denial of Service and Defense Methods," 2019 12th International Conference on Intelligent Computation Technology and Automation (ICICTA), Xiangtan, China, 2019, pp. 351-355, doi: 10.1109/ICICTA49267.2019.00081 [accessed April 14, 2020].
[4] Weisman , Steve. "What Are Denial of Service (DoS) Attacks? DoS Attacks Explained." *NortonLifeLock*, 5 Feb. 2020, us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html.
[5] CISA. "Security Tip (ST04-015)." *Cybersecurity and Infrastructure Security Agency CISA*, us-cert.cisa.gov/ncas/tips/ST04-015 [accessed April 14, 2020].
[6] "Ping (ICMP) Flood DDoS Attack." *Cloudflare*, Cloudflare, www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ [accessed April 14, 2020].
[7] "What Is a Ping Flood: ICMP Flood: DDoS Attack Glossary: Imperva." *Learning Center*, Imperva, 30 Sept. 2020, www.imperva.com/learn/ddos/ping-icmp-flood/ [accessed April 14, 2020].
[8] "SYN Flood Attack: Variants and Countermeasures." *IONOS Digitalguide*, 20 Sept. 2021, www.ionos.com/digitalguide/server/security/syn-flood/ [accessed April 14, 2020].
[9] Tudose, Catalin. "The Principles of the TCP Protocol." *Luxoft Training A DXC Technology Company* , www.luxoft-training.com/news/building-java-client-server-applications-with-tcp/ [accessed April 14, 2020].
[10] Korolov, Maria. "What Is a Botnet? When Armies of Infected IoT Devices Attack." *CSO Online*, CSO, 27 June 2019, www.csoonline.com/article/3240364/what-is-a-botnet.html [accessed April 14, 2020].
[11] Fruhlinger, Josh. "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet." *CSO Online*, CSO, 9 Mar. 2018, www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [accessed April 14, 2020].
[12] Imperva. "Mirai DDoS Attack Explained." *Blog*, Imperva, 10 Apr. 2017, www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/ [accessed April 14, 2020].
[13] "Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis." *The Cloudflare Blog*, The Cloudflare Blog, 21 Aug. 2020, blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ [accessed April 14, 2020].
[14] Statt, Nick. "How an Army of Vulnerable Gadgets Took down the Web Today." *The Verge*, The Verge, 21 Oct. 2016, www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained [accessed April 14, 2020].
[15] Roberts, Paul. "Mirai Attack Was Costly for Dyn, Data Suggests." *The Security Ledger*, 9 Feb. 2017, securityledger.com/2017/02/mirai-attack-was-costly-for-dyn-data-suggests/ [accessed April 14, 2020].
[16] Antonakakis, Manos, and Tim April. "Understanding the Mirai Botnet." *USENIX*, USENIX Association, 16 Aug. 2017, www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf [accessed April 14, 2020].

[17] Krebs, Brian. “Source Code for IoT Botnet 'Mirai' Released.” *Krebs on Security*, 1 Oct. 2016, krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ [accessed April 14, 2020].
[18] Brodsky, Zev. “The Psychology Behind DDoS: Motivations and Methods.” *Perimeter 81*, 8 Apr. 2021, www.perimeter81.com/blog/network/the-psychology-behind-ddos-attacks [accessed April 14, 2020].
[18] “What Is Memcached? - KeyCDN Support.” *KeyCDN*, 4 Oct. 2018, www.keycdn.com/support/what-is-memcached [accessed April 14, 2020].
[19] “Memcached DDoS Attack.” *CloudFlare*, www.cloudflare.com/learning/ddos/memcached-ddos-attack/ [accessed April 14, 2020].
[20] “Hello World.” *Hello World · GitHub Guides*, 24 July 2020, guides.github.com/activities/hello-world/ [accessed April 14, 2020].
[21] Kottler, Sam. “February 28th DDoS Incident Report.” *The GitHub Blog*, 1 Mar. 2018, www.github.blog/2018-03-01-ddos-incident-report/ [accessed April 14, 2020].