December 1st / 2017

DDoS Attacks

By: Christopher Katsaras & Connor Geddes

Distributed Denial of Service (DDoS) attacks are simply attempts to overwhelm a service by flooding it with large numbers of requests. Such large amounts of requests cause the attacked server to shutdown due to its inability to handle incoming traffic. DDoS attacks are extremely popular due to the simplicity of their implementation and we have even seen a DDoS attack occur a few years ago at the University of Guelph when the campus WIFI went down for over 12 hours. In addition, DDoS attacks can be purchased for relatively cheap on the “dark web” which is another reason why they are so popular (Digital Attack Map, 2017). To better illustrate how severe DDoS attacks can be, during the 2016 presidential election both Hillary Clinton’s and Donald Trump’s websites were attacked. In the case of Trump, all of his brands (campaign, hotel chains, etc) were attacked in an attempt to damage his brands / presidential bid. It’s clear from attacks like these that the ramifications of a DDoS attack can be pivotal and it is imperative that the necessary steps are taken in order to prevent said attacks.

Slowloris Attack

Well-known Attacks :

1. Iranian presidential election attack (2009)
2. River City Media spam (Biggs, 2017)

The Slowloris attack was created in June 2009 by Robert "RSnake" Hansen. This attack is different than most in the aspect that it doesn’t require a large botnet in order to take down a site. The Slowloris attack can be executed from a single computer which is one of the reasons why it is hard to detect. Additionally the Slowloris attack works by opening connections to a web server which then continuously sends information in partial requests (which will never be completed). Information is sent slowly by removing the carriage returns at the end of the HTTP request, which allows it to persist longer than normal.This method works primarily on apache servers because of the fact that apache servers will create a new thread for each incoming connection and destroy the thread upon the completion of the request and since information via a Slowloris attack is being sent so slowly there is no easy way to determine the difference between an attacker and simply a slow connection (Computerphile, 2016). This would not be a problem if there wasn't still a large number of servers running apache, almost 50% of the web servers run via an apache server making them very vulnerable to this type of attack. An example of a Slowloris attack was in 2009 after the Iranian presidential election an Iranian group extensively used the Slowloris attack to target Iranian government websites. Another unique benefit of using a Slowloris attack is that the attackers bandwidth is barely used. This not only allows the attack to make many requests from many different sockets, but also allows them to use the rest of their bandwidth to monitor the attacked site, or do other browsing that is imperative to a successful attack.
The Slowloris is intriguing due to its entirely different approach to the idea of attacking a server and is one that we both thought was an interesting and elegant solution.

December 1st / 2017

NTP Amplification Attack

Well-known Attacks :

1. Snapchat on IOS (NTP Pool, 2016)
2. Netgear and the University of Wisconsin (Plonka, 2003)

Now, unlike the Slowloris attack, the NTP Amplification attack takes a very aggressive approach to taking down a server. This attack exploits a vulnerable protocol called the Network Time Protocol (NTP) which deals with UDP based traffic. It is important to remember with UDP that there is no handshake necessary, which means large amounts of data can be dumped without approval from the receiver. NTP is used to synchronize users clocks with global standard times. While this protocol is necessary, there is a significant flaw in its system. A command in the protocol called monlist returns the addresses of the last 600 people to connect to this protocol. This function has been denounced by many programmers for its security vulnerabilities as well as its general uselessness (Computerphile, 2014). The issue with the protocol is you can spoof your return address and when used in conjunction with monlist (to retrieve users addresses), large amounts of data can be syphoned to other users. The concept of amplification comes from the fact that the response from NTP is dozens of times larger than the data that you send. If done properly and in conjunction with multiple NTP servers, the amount of data sent could bring down many large scale sites / users.

Ping of Death

Well-known Attacks :

1. Microsoft Servers (Jackson, 2013)
2. Cisco (Chirgwin, 2016)

Before we begin, it important to note that most modern computers are now capable of protecting themselves against Ping of Death. In Ping of Death, the user begins by sending an ICMP packet (commonly known as a Ping). However, this packet is “malformed” due to the fact that it exceeds the maximum size (65535 bytes). When the user sends over the large packet, it is fragmented which is necessary when sending large amounts of data. At this point, nothing will go wrong due to the fact that sending fragmented pieces of data like this is completely valid. The real issue with our system is the reassembly phase. When data is sent in fragments, it needs to be reassembled on the other end in order for the receiver to understand the full message. When the receiver tries to reassemble data that is larger than the maximum size, memory overflows and often causes the computer to crash (Imperva Incapsula, 2016). The reason this attack is no longer an issue is due to the fact that a simple error check was implemented. All the receiver must do when reassembling his/her data is check to see if the data being received + the currently received data is larger than our maximum length. If it is, don’t try and reassemble it. It is once again important to note that the inherit issue with this attack doesn’t really have anything to do with the ping and is more closely related to the receivers lack of error checking at reassembly (Sourcefire, 2013).

As we can see from the three attacks examined above, many of the structures the internet is built on are outdated. Most of these attacks have very simplistic structures and are simply exploiting them in ways that most wouldn’t think about when they were initially created. It is our hope that as technology advances, so does our standards for secure protocols and systems that ensure that our data, experiences and sites are kept safe and secure.

December 1st / 2017

Citations:

Biggs, J. (2017, March 06). Spammers expose over a billion email addresses after failed backup. Retrieved November 23, 2017, from https://techcrunch.com/2017/03/06/spammers-expose-billions-of-emails-after-failed-backup/

Chirgwin, R. (2016). Firewalls snuffed by 'BlackNurse' Ping of Death attack. Retrieved November 23, 2017, from https://www.theregister.co.uk/2016/11/14/its_2016_and_a_ping_of_death_can_still_be_a_thing/

Computerphile. (2014, March 14). The Attack That Could Disrupt The Whole Internet - Computerphile. Retrieved November 23, 2017, from https://www.youtube.com/watch?v=BcDZS7iYNsA

Computerphile. (2016, November 09). Slow Loris Attack - Computerphile. Retrieved November 23, 2017, from https://www.youtube.com/watch?v=XiFkyR35v2Y

Digital Attack Map. (2017). What is a DDoS Attack? Retrieved November 23, 2017, from https://www.digitalattackmap.com/understanding-ddos/

Imperva Incapsula. (2016). Ping of Death. Retrieved November 23, 2017, from https://www.incapsula.com/ddos/attack-glossary/ping-of-death.html

Jackson, J. (2013, August 13). Microsoft Patch Tuesday: The Ping of Death returns, IPv6-style. Retrieved November 23, 2017, from https://www.infoworld.com/article/2610243/patch-management/microsoft-patch-tuesday--the-ping-of-death-returns--ipv6-style.html

NTP Pool. (2016, December 19). Recent NTP pool traffic increase. Retrieved November 23, 2017, from https://community.ntppool.org/t/recent-ntp-pool-traffic-increase/18

Plonka, D. (2003). Flawed Routers Flood University of Wisconsin Internet Time Server. Retrieved November 23, 2017, from http://pages.cs.wisc.edu/~plonka/netgear-sntp/

Sourcefire. (2013, April 02). Denial of Service Attacks (Part 2): The Ping of Death. Retrieved November 23, 2017, from https://www.youtube.com/watch?v=Y8k_UGCiA6Y&t=4s