THE CANADIAN SCIENCE FAIR JOURNAL

ARTICLE

How to Mitigate the Effects of Denial of Service Attacks

Muhammad Z. Bharwani

13 | Richmond Hill, Ontario

Local Science Fair Honourable Mention

We all use the internet, on a daily, weekly, or monthly basis. It has become the main focus of our lives. When you use the internet, you communicate with other computers through packets of information. These packets, when sent in large enough quantities, can overwhelm computers. It's as if hundreds of people all came up to you and tried to ask you questions. You wouldn't even be able to hear what they are saying, let alone be able to talk without being interrupted. A similar process happens with computers. Denial of Service (DoS) attacks work by sending large amounts of useless information to a computer. Due to internet access being so crucial, I decided to try and figure out how I can prevent, or mitigate the effects of, Denial of Service attacks. These attacks render computers unable to operate. The solution found was to mask the IP address of one's computer. The IP address acts as a home that receives mail. If the sender can't see the home address, they can't send any mail. Thus, Denial of Service attacks can be prevented by masking the victim computer's IP address, preventing the attacker from reaching the victim's computer.

INTRODUCTION

The Internet. Something which many people are familiar with, and use regularly. Many businesses rely heavily upon it, in order to acquire more business, or to communicate with customers. Schools and universities rely upon it, to contact students and to facilitate the submission of assignments. What if an individual or a company's access to the internet was restricted? They would lose access to contact others, and possibly may be unable to communicate in times of vital importance. Enter, Denial of Service (DoS) attacks. As the name suggests, these cyber attacks work to prevent a computer from accessing the internet, by overwhelming it with information. Computers communicate with each other via "packets." These packets hold information, which will then be passed onto another computer (WIAP?, 2000). However, one can fill these packets with an excess of information, and when sent in large quantities, these packets can overwhelm weaker computers. This restricts internet access, as the afflicted computer will attempt to process all this information at once. Thus, DoS attacks pose a great risk for Internet users, particularly those who need the internet to work, and to go about their daily lives. The purpose of my research is to eliminate or restrict the potential of these attacks, and to create a safer environment for internet users across the world, by enabling them to take action against DoS attacks. By eliminating these attacks, a certain level of security is provided for all internet users.

RUNNING A DENIAL OF SERVICE ATTACK

In an attempt to learn more about how these attacks work, I attempted to perform an attack on my own computer. This would allow me to look at its impact on my computer. I first attempted to use a software called "Nemesy." Nemesy is a piece of software used to send large quantities of packets for a DoS attack. However, I was unable to utilize it, as Nemesy is exclusive to Windows XP, Windows NT, and Windows 2000. I am incapable of accessing any of these Operating Systems, as they are incredibly outdated, and are very difficult to run on newer computers (nemesy13.zip ≈ Packet Storm, n.d.).

The second attempt I made involved the website Low Orbit Ion Cannon. LOIC was used by the hacking group Anonymous to run a Distributed Denial of Service attack, in retaliation to the takedown of popular website MegaUpload ("Anonymous" DDoS Activity | CISA, n.d.). However, I did not use it in the end, as the program is more focused on running a Distributed Denial of Service attack, involving multiple computers (which I do not own). However, as I was able to examine the settings and intricacies of LOIC, I could from there ascertain how a DoS attack would be run and what impacts it may cause. For instance, whilst using LOIC, it provided the user the ability to run Denial of Service attacks against both IP addresses, as well as website URLs. This allowed me to learn that DoS attacks can also be run against websites.

CREATING A SOLUTION TO DENIAL OF SERVICE ATTACKS

Finding a solution to this problem requires one to gain an understanding of how exactly this information is relayed. As stated earlier, information is carried across through packets. One may be inclined to wonder why there is no limitation to the amount of information that can be sent in these messages. The internet relies on protocols for sending this information. One method of running Denial of Service attacks abuse the UDP, or User Datagram Protocol. This protocol is typically used for transferring information in times where one needs vast amounts of information quickly. For instance, when using Voice over IP (VoIP) services to call over the Internet, it would be ideal to have instantaneous com-

munication, sacrificing small amounts of quality. This is accomplished by limiting the number of checks data has to go through (Hoffman, 2017). This can very easily be abused for Denial of Service attacks. Data can be sent with few checks, meaning that large quantities of it can be sent to attack a computer quickly and in large amounts (DoS (Denial of Service) Attack Tutorial: Ping of Death, DDOS, n.d.)

These attacks are directed towards the computer's IP, or Internet Protocol, address. Every computer has one. They are akin to your home address. A home address is needed to send or receive letters. However, one could instead request all letters sent to and from a proxy address, away from your own one. This would allow you to mask your true address behind that which the letters are being sent and received from. You need only to pick up any letters from the proxy.

A similar concept can be applied in the realm of computing. A computer may send packets whilst rerouting them through another computer. This would mask the original sender's identity, as the computer on the receiving end of the packets would simply view the IP address of the computer the packets were rerouted through, i.e the proxy. One would be inclined to believe that this solution would be impossible, due to the fact that the message going back to your computer would not make it, as the final destination is unknown to the receiving computer. This is false. A computer beginning a communication with another computer would have the proxy to facilitate communication. In short, this means that one can maintain anonymity online by hiding one's IP address through a proxy.

This raises the question: how do you access a proxy IP address? There are two solutions. While I did not create these solutions, I am repurposing them for the prevention of Denial of Service attacks. These two are The Onion Router, and Virtual Private Networks.

Firstly, what is The Onion Router? The Onion Router, or TOR, was originally invented by the US government. It encrypts what you send online, by sending it through several different computers, before getting to its final destination. In a very simplified way, TOR sends your packets through multiple proxy computers. These act as layers of anonymity, like the layers of an onion (hence the name). Whilst utilizing TOR, your location will appear as the last computer in the chain, prior to reaching its final destination, the computer you are trying to reach. These computers are other computers, typically volunteers. The speed of using TOR is incredibly slow, in comparison to normal, day-to-day browsing. This is to be expected, as TOR is a free service (Wherry, 2020).

On the other hand, a VPN, or Virtual Private Network, may offer more features a typical computer user is looking for. A VPN is a service that does much the same as TOR. It sends your packets through the VPN's own server/computer, and then onto your final destination. (Norton, 2015). This allows it to be much faster than TOR, as these VPN servers are specifically designated for this purpose. However, it is quite costly to run these VPN services, and so most VPN providers require a user to pay before they may use the product. For an average user who wishes for anonymity, be it for the prevention of Denial of Service attacks, or for another reason, a VPN is often the best solution. They typically provide much faster service then TOR, though they may be less secure as there are fewer proxies in the chain to your final destination.

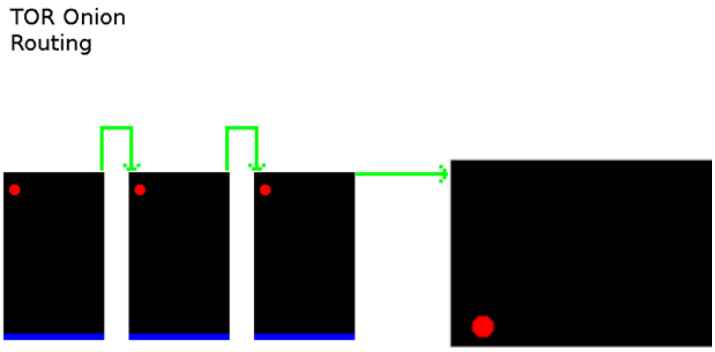

Figure 1

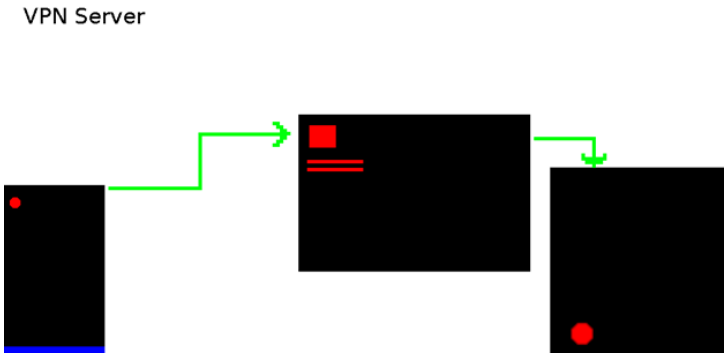

Figure 2

NEXT STEPS

This paper largely focuses on Denial of Service attacks, in which one computer is used to target another computer. However, in the modern world, many individuals are capable of running these attacks from multiple computers, effectively multiplying the power of these attacks, scaling drastically to the extent where major companies' websites can be affected. In the future, working on a solution for large corporations would be a step in the right direction. While there are some solutions, most are not cost effective. Moreover, the current solution proposed by me would not suffice, as a large corporation requires their website (containing their IP address) to be visible to all. Thus, another solution is needed in order to prevent Denial of Service attacks for large websites.

CONCLUSION

DoS attacks are a very major issue for the way in which the internet works. As we become more reliant upon the internet for our day-to-day tasks, we need to remain prepared for attacks such as these. The solution proposed here, namely, is The Onion Router and/or Virtual Private Networks. In conclusion, Denial of Service attacks can be prevented by masking your IP address, through technology originally meant for privacy, TOR or a VPN. While the internet can be easily misused, staying safe allows you to use it without any fear of Denial of Service attacks plaguing you.

ACKNOWLEDGEMENTS

Throughout the course of this solution being found, there are many individuals who have aided me. I'd like to recognize these individuals. Firstly, I'd like to thank my science teacher, Ms.Manji. Without her, I would never have been able to bring my project to fruition. She helped me both in school, as well as in her own time. Secondly, I'd like to thank my Vice Principal, Ms.Rasool. She enabled me to meet all the required submissions, waivers, and other forms, by walking me through them in a very friendly manner. Thirdly, I'd like to thank my mentor, Brother Amjad. Through his help, I was able to ensure the correctness of my project. Lastly, I wish to acknowledge Youth Science Canada, who empowered me to share my passion with the rest of the world.

REFERENCES

Hoffman, C. (2017, June 8). *What's the Difference Between TCP and UDP?* How-to Geek; How-To Geek. https://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/

DoS (Denial of Service) *Attack Tutorial: Ping of Death, DDOS.* (n.d.). www.guru99.com. https://www.guru99.com/ultimate-guide-to-dos-attacks.html nemesy13.zip ≈ Packet Storm. (n.d.). Packetstormsecurity.com. Retrieved June 20, 2021, from https://packetstormsecurity.com/files/25599/nemesy13.zip.html

What is a packet? (2000, December). HowStuffWorks. https://computer.howstuffworks.com/question525.html. Norton. (2015). Norton.com. https://us.norton.com/internetsecurity-wifi-how-does-a-vpn-work.html

Wherry, J. (2020, September 29). *What is Tor (Browser) & How does it work?* CyberNews. https://cybernews.com/privacy/what-is-tor-and-how-does-it-work/

ABOUT THE AUTHOR

Muhammad is a young writer with a passion for science and cybersecurity. From an early age, he became interested in them, participating in many science fairs, and engaging with computers. He recently put his two interests together, to write this paper on Denial of Service attacks. Muhammad lives in Richmond Hill, Ontario with his three sisters, who encourage him to continue learning, and pursuing his interests.