Denial of Service Attacks

IT-489

March 4, 2016

Honor Pledge: I acknowledge that the Capstone Project is an independent study project to be completed individually. On my honor, I have not received aid on my Capstone Project other than what was provided by my faculty mentor and any persons explicitly cited in my work. I further acknowledge that if I have given any aid to another student in this course, the instructor of this course was made aware of my contributions.

Contents

Objective

Denial of service (DDOS) attacks have become more and more common as technology has advanced which can cause millions of dollars in lost revenue for companies. A denial of service attack happens when an unauthorized user launches an attack against another computer or device by launching an assault on the network that the device is on with so many requests that legitimate traffic is either slowed or completely shut down for a period of time (Basta, p. 96). However, companies and websites are not the only victims of DDOS attacks as residents can be victims of these types attacks just as easily as anyone else can, and I know because I have been the victim of a DDOS attack before. This is why I got interested in Cyber security because in today's age a huge amount of the world uses the internet. The people who initiate these attacks are hackers, but there are different types of hackers such as black hat hackers who carry out attacks for financial gain, white hat hackers who get employed by companies to find faults in their system, and script kiddies who are novices when it comes to hacking and use scripts that are created by really skillful hackers in order to carry out attacks. While script kiddies make up roughly 40% of hackers they are

typically the ones who will launch DDOS attacks against a resident rather than a more skillful hacker as they do this in order to show off more often than not. My goal for this project is to create a way for people who lack knowledge about how computers work to easily combat such an attack, the anti-DDOS version of an anti-virus program like Norton is what I am aiming for.

At the beginning this tool would only be used for online gaming because ever since online gaming has become a thing DDOS attacks involving gamers have become more common. It would probably take a few years in order to get this tool to branch out in order for corporations to be able to use it as I intend for it to start out being useful for attacks against routers rather than servers. When there are less DDOS attacks happening against private residents that use my tool then I will know that my tool works. Plus, my aim is for this tool to not only help prevent a DDOS attack from occurring but for it to also help with holding those who launch such attacks accountable by showing the IP address that the attack is coming from.

Since there is not a guaranteed product that is either digital or physical that can really combat a denial of service attack and also considering how a botnet is structured and how attacks that use a botnet are carried out with potentially thousands of zombie computers, a product that can prevent a denial of service

attack or even provide the victim with the information of where the attack is being launched from would be nearly invaluable in today's market. Even my faculty mentor Dr. Bicak who teaches the Cybersecurity: Attack/Defend course believes that whoever can create such a product would almost definitely become a billionaire. Even the person who did the peer review on my topic would like to see such a device be created because without a doubt the only people who would suffer from such a creation would be the perpetrators who launch such attacks in the first place.

Client

With denial of service attacks growing more common place over the years there needs to be a way that can help combat these kinds of attacks because when a corporation's server comes under a denial of service attack the amount of time that it takes for the server to start having legitimate traffic run on it again can cost a corporation millions in revenue. However, if this device was created the main goal of it would be to hold those who launch these kinds of attacks liable for the damage that they do to others because as it is right now these perpetrators can basically launch large scale attacks with a botnet and no repercussions will follow because the perpetrator uses thousands of zombie

computers that he controls with his own device which makes back tracing the attacker virtually impossible. While creating a device that would help with preventing a denial of service attack or even providing the attackers info would be very beneficial to the world, a device that can infiltrate zombie computers in a botnet in order to find the host computer that is initiating the attack would be an invaluable asset to anyone whether it was an individual, corporation, or even a government.

Content Adivsor

My content advisor is Dr. Ali Bicak who holds a Bachelor's degree from Bilkent University, a Master's degree from Middle East Technical University, and a Ph.D from the University of Maryland (Marymount). He also has the qualifications to teach Computer Networking, Information Security, Cisco Networking and Ethical Hacking (Marymount); and I have taken two Cisco classes where he was the residing professor and I am currently taking Cybersecurity: Attack/Defend which helps prepare students for becoming a certified ethical hacker which I am currently taking.

Resources

The only resources that I need are a couple of computers and two or so fully functioning routers at different IP addresses because within the next two weeks after spring break we have an assignment in Attack/Defend that revolves around denial of service attacks and I cannot wait to do that assignment because it will help me further understand how denial of service attacks work. While I do know that some denial of service attacks rely on sending a large number of packets in order to cause traffic on a site or a private resident's internet to slow down to a crawl or just stop working all together while the attack is being carried out, I have never initiated a denial of service attack against anyone so I do not know the measures that are taken when trying to setup an attack. Since I have been the victim of a denial of service attack before I know what it is like to be on the receiving end of an attack, but I do not know what it is like to be the one behind the attack. Having two computers, both of which are at different IP addresses or virtual machines so that a controlled denial of service of attack can be both initiated and received by either device so that I am able to see just how many packets it takes to basically disable a router from having traffic run through it for a small amount of time.

Project Details

There is no doubting that online gaming has become a very lucrative platform over the past decade and is now a multi-billion dollar industry. However, due to how popular it has become many of the online game providing networks such as Playstation Network and Xbox Live have become targets for hackers with many instances of both being knocked off line from denial of service attacks. This is especially true for Playstation Network which has suffered many breaches over the past few years with the biggest one happening back in 2011 and two of the more recent ones being back in 2014.

The biggest breach that Playstation Network suffered from was back in 2011 when over 77 million accounts where compromised and had information from them stolen (Stuart). Although earlier in that year it was discovered that the encryption for the PS3 had been cracked which is more than likely how the attacker was able to compromise so many accounts (Stuart). In 2014, while it was not a breach of such a large scale like the one back in 2011, Playstation Network and Xbox Live were knocked offline for about a week and a half during the holidays (Wei). However, Lizard Squad claimed to be behind this attack and even stated in August of that year that they were going to be launching an attack on Playstation Network and Xbox Live over the holidays (Kiss). Also when Lizard

Squad launched their attack in August of 2014 they also did a bomb threat on the airplane that the President of Sony Online Entertainment was a part of (Wei).

It is acting like this that should be punished because groups like Lizard Squad can do these attacks or even make bomb threats and they can get away with it with almost no repercussions due to how difficult it is to back track them through all of the zombie computers and most likely the multiple proxies that they have in place to prevent them from getting caught. Let's face it there needs to be ways to combat these kinds of attacks and make those who initiate them take responsibility for their actions. However, when it comes to combating a botnet it is easier said than done due to the vast amount of zombie computers that are a part of the botnet. If a virus can turn a computer into a zombie computer in order to carry out attacks then there must be away to counteract it as well because if the zombie computers are being given commands from a host computer then there has to be a way of tracking down the host computer with their own zombie computers. However, doing something like that might be illegal because what I was thinking of was basically fighting a virus with a virus where I can turn their zombie computers into my zombie computers in order to back trace their signal but that would be breaching into a private device which is illegal. This is why I believe that once the signal has been found and the person's location has

been noted the virus would need to have an autocannibal feature so that it destroys itself after the original attackers information has been found without destroying any data on the zombie computers.

Due to how that idea would most likely be illegal I had another thought, what if there was a tool that while it is active keeps track of all the traffic on a site or a router and when a spike in packets happens that could be a possible denial of service attack the tool denies the packets from coming through. For example say that there is a server that has a cap of 10 people on it and if it exceeds that then it gets overloaded and say that at any given time it has between 4 and 8 devices active on it. Now say that a spike happens that makes it seem as though if the packets got through then it would knock the server out, but instead of knocking everyone who was already on it off it would not allow the packets through which would leave the people who were already on it unaffected.

References

Basta, A., Basta, N., & Brown, M. (2014). Computer security and penetration testing (2nd ed.). Stamford, CT: Cengage Learning. Pg. 96.

Dr. Ali Bicak. Marymountt, 2014. Web. March 4, 2016. http://www.marymount.edu/Home/Contact-Us/Faculty-Staff-Directory?profileid=29

Kiss, Jemima. "Xbox Live and Playstation Attack: Christmas Ruined for Millions of Gamers." The Guardian. Guardian News and Media, 2014. Web. 04 Mar. 2016.

Stuart, Keith, and Charles Arthur. "PlayStation Network Hack: Why It Took Sony Seven Days to Tell the World." The Guardian. Guardian News and Media, 2011. Web. 04 Mar. 2016. <http://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony>.

Wei, Wang. "Sony PlayStation Network Taken Down By DDoS Attack." The Hacker News. 24 Aug. 2014. Web. 04 Mar. 2016.