Alexander Cannell

09/24/2016

CSIA 6010

**Reference List**

I am still in the research stage of my final research paper. There is so much information and I’m still trying to figure out how to make it more specialized rather than generalized. I am focusing my paper on what is a DDoS attack, how do they work, What is the risk of successful attacks, and How to defend against such attacks? With greater focus on the question of how to defend against DDoS/DoS attacks.

* Akamai Inc. (n.d.). DDoS Mitigation | Akamai. Retrieved September 25, 2016, from <https://www.akamai.com/us/en/resources/ddos-mitigation.jsp>
  + This is the migration service that the company I work for uses. Doing research on paid DDoS protection services. What benefits do these companies have over other companies? Have a better understanding on how paid services work too. Also understanding the cost behind these services, and what other features they may have.
* Incapsula Inc. (n.d.). Incapsula. Retrieved September 25, 2016, from <https://www.incapsula.com/>
  + More research into other companies, same situation as Akamai. But Incapsula is suppose to be the best product on the market. A great industry standard to compare the other Migration services against.
* TopTenREVIEWS. (2015, October 02). Top 10 DDoS Protection Services of 2016 | Top Ten Reviews. Retrieved September 25, 2016, from <http://www.toptenreviews.com/business/internet/best-ddos-protection-services/>
  + Great website listing a lot of the DDoS Protection Services. Giving great reviews on each of the services. Also giving an explanation on how DDoS works, and how they are migrated. Also giving a great explanation on the merits of having a DDoS Protection service for your company.
* NeustarInc. (2012, June 19). What is a DDoS attack and how does DDoS Mitigation work? Retrieved September 25, 2016, from <https://www.youtube.com/watch?v=ASXmPSE966c>
  + Another Informational video on how DDoS attacks work. Also giving an explaination on how DDoS Migration works. This is a promotional video for Neustar, but the concept still gets across.
* TheTechFeed. (2013, April 14). How To Prevent a DDoS Attack. Retrieved September 25, 2016, from <https://www.youtube.com/watch?v=JzIvpWieBLw>
  + Botnets are cheap, virtually untraceable and improve as the speeds of infected computers improve. This video brings up the point that Botnets can be disabled. For example: Rustock an botnet responsible for 33 percent of spam was taken down by law enforcement. This video also explains what a DDoS attack looks like.
* HackersSecurity. (2013, August 19). DEFCON 20: Javascript Botnets. Retrieved September 25, 2016, from <https://www.youtube.com/watch?v=xDslqMCaLZM>

This is a demonstration on how to create a botnet. In this instance they use a javascript via proxy servers to take control and monitor the bots. At the end he shows us how his web ui can organize all the bots into zombies. Knowing ways to create a botnet is a great way to understand how botnets and DDoS attacks work. This is a very funny video too, worth watching if you have the time.

* A brief history of DDoS... and how to defend yourself and your customers. (2016, May 06). Retrieved September 25, 2016, from <https://www.logicnow.com/blog/brief-history-ddos-defend-customers>
  + A history of how DDoS and DoS attacks first came to be. This article gives a great explanation on what hacktivism is. Also addressing several things we need to take into account when defending against DDoS attacks.
* What are DDoS attacks? DDoS Explained. (2012, September 12). Retrieved September 25, 2016, from <https://www.youtube.com/watch?v=OhA9PAfkJ10>
  + A great little explanation video that explains what an DDoS attacks are. Explains that some DDoS Bot farms are available to hire if you so need. Explains that the average DDoS attack lasts for about 24 hours. Also explaining the motivations behind DDoS attacks. DDoS attacks can lead to financial loss, Image Degradation, bad customer service, and even legal problems for a company.
* C. (2011, October 30). DEFCON 19: Three Generations of DoS Attacks (with Audience Participation, as Victims). Retrieved September 25, 2016, from <https://www.youtube.com/watch?v=1EAnjZqXK9E>
  + Gives several examples of different programs that initiate DDoS attacks LOIC, OWASP, and an example of a RA Flood Attack. They also go over the migration service CloudFlare. Very interesting, I really love these defcon videos. I know this is a statement from 2012 but Sam says something interesting about if you are attacked personally by an DDoS the best policy is to wait out the storm until it is over. He recommends opensource DDoS Protection services like CloudFlare for small businesses with websites. It is more cost effective.
* Vacca, J. R. (2014). *Network and system security*. Amsterdam: Syngress.
  + Class Textbook. Addresses what DDoS and DoS are. Also has a great explaination of what Bots are, and how theGives a great explanation on how redundancies counters SYN or UDP floods, CP, Memory, and storage application attacks. Talks about message flooding.
* Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice*. Syngress.
  + Class textbook perspective addresses DDoS briefly.
* Oriyano, S. (2016). *CEH v9: Certified Ethical Hacker version 9 study guide* (Vol. 9). John Wiley & Sons.
  + Gives a great explanation of what an DoS is, also gives great real world examples. Goes through the different terminology used in DoS attacks. Gives several examples and exercises to practice, and walk through pictures. I think I’m going to have to try some of this on a segregated network. Also gives several diagrams on how a DoS works.
* M. (2015). *Python Penetration Testing Essentials*. Packt Publishing.
  + Describes how dangerous Denial of Service attacks can be. Goes through the programming of a python DoS attacks. Three of them Single IP Single Port, Single IP Multiple Port, and Multiple IP Multiple port. Gives an Idea of how to detect a DDoS. Each of these are given walkthrough and examples of how to program the python.