Alexander Cannell

CSIA 6010

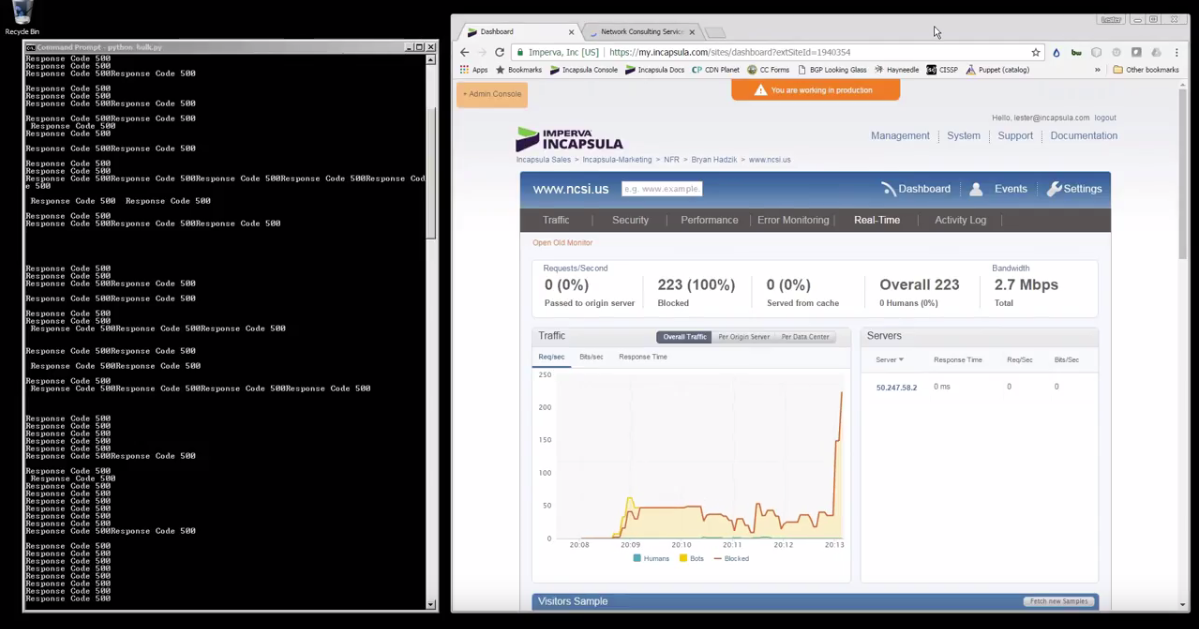
Professor Pogue

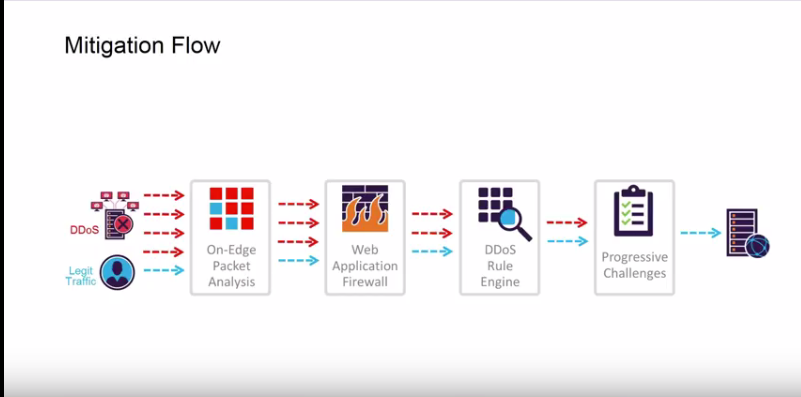
Webinar Attendance 1

**Summarize the Webinar.**

The Webinar I took apart in was the one from Imperva Incapsula titled Imperva DDoS Education Presentation on 09/28/2016. Imperva is a web application for firewalls, database protection, cloud access security, and is a leader is DDoS Mitigation. The presenter was Lester John is a Senior Sales for Imperva. He started his presentation by explaining the two different types of DDoS attacks Volumetric(Layer 3 and 4) attacks and Application layer attacks. Volumetric attacks are DDoS attacks that use a large amount of traffic from multiple sources to one target. It isn't about the Mbps but the amount of packets per second. If we send larger packets we are seeing that networks can handle them, but if we send large amounts of smaller packets than it overloads network equipment. Application layer attacks is a DDoS attack that impersonates human behavior. DDoS are becoming larger, smarter, and more frequent almost doubling from last year. Lester then continued talking about the architecture of Imperva. Talking about a large amount of scrubbing centers around the world. A scrubbing center/Points of Presence(PoP) analysis traffic to determine what is legitimate and mitigates or scrubs out the bad traffic. A peanut is designed to handle anywhere between 500 million packets to just above one trillion packets a second. A sinkhole when you discover traffic that is completely bad, you don't want to terminate that bad traffic on the end point because you are going to be running into the same connection with the requirement of opening up that bad connection to dump it. When you determine that traffic from a specific IP is bad you can transfer that to a sink hole that takes the traffic; confirms the connection, and then throw away. He brings up an excellent point, when we look at a DDoS attack we have the technical cost of the attack, but we need to look at the cost of all the other costs that happen it isn't just the technical cost. You have to include in your cost not just damages/repairs, but stuff like lawyers, hours spend, revenue lost, reputation lost, customers lost, etc…. DDoS is a backdrop to what they are really after if they can focus you on the DDoS attack they can go after the other stuff. The difference between a blocking DDoS service and mitigation DDoS service is a mitigation service allow legitimate traffic in during a DDoS event. During a large DDoS attack that traffic, if needed, can be directed to multiple scrubbing centers to handle the load, this will slow down the response time of legitimate traffic, but it is far better to have your website slow than down.

It was quite interesting, Lester performed a DDoS attack on the www.ncsi.us website using the program hulk(HTTP Unbearable Load King) which is a DDoS hacking tool that generates large volumes of unique requests to a victim. Dave co-presenter from NCSI(Network Consulting Service Inc.) told us that his security team contacted him to tell him that the website was under attack from a DDoS.





**Was the presentation succinct?**

I believe that he was very clear, I thought it was a little too sales pitchy for my good, but I enjoyed to learn how a mitigation service works.

**Was the presenter prepared and knowledgeable about the subject matter?**

I believe that Lester John was prepared he was quite knowledgeable about what he did. He was quite knowledgeable about DDoS and how Mitigation worked. I really enjoyed how he did a live demonstration on an actual site of a DDoS attack. It was quite funny when the Operations Team for that website called the co-presenter Dave Hammer and told them that they were under attack.

**Did the presentation clearly present a defensible position or was it merely a sales pitch?**

At the beginning, it was definitely a sales presentation, but it became more of an educational video towards the end. I really enjoyed it. I’m planning on doing my Capstone on the effects of DDoS attacks on companies, and what it takes for a company to recover. I am currently in the CSIA 6000 and I watched this webinar for a final project in that class.

**What was your opinion of the presentation?**

I really didn’t like the technical difficulties. I think I would have enjoyed the presentation a lot more if I could see all the slides, and without the constant interruptions. Which is something the presenter didn't have any control over, and he did the best he could with all the interruptions he had. But I really enjoyed the live DDoS attack. I thought it was quite funny to watch and interesting. I really thought the presenter was very knowledgeable about how DDoS Mitigation works, and how to best defend against DDoS attacks. I asked the question about the Load Balancer and found it interesting how he answered the question. There was a lot of plugging for his product, but I enjoyed the explanation on how the load balancer and the mitigation service work together to filter and distribute legitimate traffic.

**What could the presenter have done better?**

Again I just didn't like the technical difficulties. Which the presenter had no control over so I can't fault him for interruptions and missed slides. Also, the sales pitch at the beginning and throughout the presentation was not very entertaining, but it was a free webinar.

**References:**

* <http://hacking-tutorials-now.blogspot.com/2013/09/hulk-performing-denial-of-service-attack.html>
* <https://www.youtube.com/watch?v=vh9gxHHdlKI>