Readme File for Teachers:  
Case Study on DDoS Attacks

**Abstract:**In this case study, students will look into the detail of a 300Gbps DDoS attack happened in 2012. Students will learn how the attack take place from the beginning to the end. During the process of case analysis, a list of security topics reflecting different aspects of the breach is introduced. Through guided in-class discussion and hands-on lab assignments, student learning in lecture will be reinforced.

**Target audience:**Undergraduate, Graduate

**Objectives:**

* Explain DDoS attacks
* Explain Reflective DDoS attacks
* Explain IP Spoofing and traffic amplification
* Describe common defense mechanisms to defeat DDoS attacks

**Keywords:**DDoS attacks, Reflective DDoS attacks, IP Spoofing

**Description:**This case study provides an in-depth analysis of a significant Distributed Denial of Service (DDoS) attack that occurred in 2012, targeting the Spamhaus website. This attack reached a peak of 300 Gbps, significantly disrupting the service. The presentation outlines the nature of DDoS attacks, including reflective DDoS attacks, IP spoofing, and traffic amplification. It emphasizes the importance of understanding the mechanics of these attacks, such as how attackers exploit multiple compromised systems (forming a botnet) to overwhelm a network or server, thereby making the service unusable. The case study illustrates the challenges of defending against such large-scale attacks and provides real-world insights into the vulnerabilities and responses during the incident.

Moreover, the presentation details the common defense mechanisms against DDoS attacks, including the use of cache servers, mirror servers, anycast routing, IP traceback, and packet filtering. Each method aims to mitigate the effects of a DDoS attack by either distributing the load, tracing the attack's origin, or filtering malicious traffic. The discussion also covers how the attackers used open DNS resolvers to amplify the attack and the significance of maintaining good network practices to prevent IP spoofing. The case study concludes with a reflection on the trends in DDoS attacks and the evolving strategies in cybersecurity to counteract these threats, highlighting the need for continued vigilance and innovation in defense mechanisms.

**Cybersecurity topics:**General topic: DDoS attacks, IP Spoofing  
  
**Teaching resources for the case:**A study package with the following materials was developed for the case:  
a) A PowerPoint presentation explaining technical details and lessons learned for the case: used by the instructor to guide the classroom discussion.   
b) A list of discussion questions: It is suggested to ask students to finish the discussion questions before attending the in-class discussion.  
c) A video tutorial introducing the case: For instructors or online students.   
The video can also be used before the in-class discussion. Students will be asked to finish the video before attending the in-class discussion.

**Additional third-party resources for the case:**[1] LESSONS FROM SURVIVING A 300GBPS DENIAL OF SERVICE ATTACK. Blackhat 2013. https://www.youtube.com/watch?v=w04ZAXftQ\_Y

[2] DDoS data. https://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical

**Language:**English

**Date created:**   
May 1, 2023

**Last update:**   
May 1, 2024