Published on *University of Colorado* (https://www.cu.edu)

Home > DDoS Attacks and Defenses

DDoS Attacks and Defenses [1]

About This Course

In this MOOC, you will learn the history of DDoS attacks and analyze new Mirai IoT Malware and perform source code analysis. you will be provided with a brief overview of DDoS Defense techniques. You learn an Autonomous Anti-DDoS Network called A2D2 for small/medium size organizations to deal with DDoS attacks. A2D2 uses Linux Firewall Rate limiting and Class Based Queueing, and subnet flood detection to handle various DDoS traffic types. You learn the new Intrusion tolerance paradigm with proxy-based multipath routing for DDoS defense. By developing and deploying such a new security mechanism, you can improve performance and reliability of the system at the same time and it does not have to be just an overhead. By the end of this course, you should be able to analyze new DDoS malware, collect forensic evidences, deploy firewall features to reduce the impact of DDoS on your system and develop strategies for dealing with future DDoS attacks.

For the pre-requisites, we recommend the learners take the Design and Analyze Secure Networked Systems course to learn the basic security concepts and principles and take the Secure Networked System with Firewall and IDS courses to learn the basic firewall and IDS systems.

Language
English

User Ratings
4.5

Level
Beginner
Commitment?

Suggested: 8 hours/week

For More Information or to Enroll

[2]

Created by:

Groups audience:
MOOCs
Right Sidebar:
MOOC: DDos Attacks and Defenses

Source URL:https://www.cu.edu/mooc/ddos_attacks_and_defenses

Links
[1] https://www.cu.edu/mooc/ddos_attacks_and_defenses [2] https://www.coursera.org/learn/ddos-attacks-and-defense