OVERVIEW

Course Level:

Intermediate

Format:

Instructor-Led

Course Code:

APS-TRAIN-DEFEND

Target Audience:

Security and network engineers responsible for the administration, architecture, and operations for monitoring network traffic, mitigating against DDoS attacks and ensuring peak performance of the Arbor APS deployment.

Duration:

16 course hours, 1.6 CEUs

Defending Against DDoS Attacks Using Arbor APS Course

Course Description

This course focuses on using Arbor APS for protection from availability threats such as volumetric, state-exhaustion, and application-layer Distributed Denial of Service (DDoS) attacks. The goal of the course is to build the attendee's confidence by providing hands-on experience in using the Arbor APS to identify and mitigate malicious DDoS traffic. Attendees will learn about the different types of DDoS attacks and how to use the Arbor APS to monitor and analyze the traffic. Then, during lab exercises, students will experience different inbound and outbound DDoS attack types, and will use the Arbor APS to mitigate malicious traffic that is targeting the server they are assigned to protect.

Course Objectives

- Use Arbor APS to identify DDoS Threat activity
- Determine the characteristics of the major attack categories - Volumetric, State-Exhaustion and Application Layer
- Create and tune Protection Groups used to protect critical network resources
- Apply APS-defined countermeasures to mitigate DDoS threats.
- Verify DDoS attacks have been mitigated

Course Syllabus

Module 1: Arbor APS Overview

- Introduce Arbor and identify the products and services that Arbor provides
- Discuss DDoS attack characteristics and explain DDoS defense using Arbor APS
- Identify Arbor APS functionality and deployment options
- Establish familiarity with the Arbor APS User interface (UI)

Module 2: Deploying and Configuring Arbor APS

- Understand the management connections to and traffic flow through the Arbor APS
- Discuss the Deployment options available for the APS platform – Monitor vs. In-Line
- Navigate through the Arbor APS User Interface
- Define Protection Groups and adjust Mitigation Strategies ahead of responding to network attacks
- Understand data reported within the Summary and Protection Group landing pages

Module 3: Viewing and Understanding the Attack Details

- Analyze the Summary and Protection Group Widgets to understand and isolate an attack
- Leverage FCAP filter expressions for effective mitigation
- Understand the functionality of Dropped Packets vs. Blocked Hosts
- Identify Blocked Hosts and how to Whitelist or Blacklist hosts
- Understand when an attack has been mitigated

Module 4: Layer 3/4 DDoS Protections

- How to use Arbor APS to protect from Layer 3/4 DDoS attacks

Module 5: Configuring APS Cloud Signaling

- Describe when to use Arbor APS cloud signaling capabilities
- Configure Arbor APS to connect to your providers cloud-based services
- Monitor the status of your cloud-based mitigation service

Module 6: Protecting against Outbound Attacks

- How to use Arbor APS to protect from outbound attacks

Module 7: Application Layer DDoS Protections

- Understand how to apply countermeasures to protect – Web Servers, SSL secured services, DNS Servers, SIP Servers and Other Servers

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

TCI_078_EN-1801 04/2018